INTERNATIONAL ROADMAP FOR DEVICES AND SYSTEMS

INTERNATIONAL ROADMAP FOR DEVICES AND SYSTEMS

2021 UPDATE

BEYOND CMOS

THE IRDS IS DEVISED AND INTENDED FOR TECHNOLOGY ASSESSMENT ONLY AND IS WITHOUT REGARD TO ANY COMMERCIAL CONSIDERATIONS PERTAINING TO INDIVIDUAL PRODUCTS OR EQUIPMENT.
© 2021 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.
## Table of Contents

Acknowledgments .......................................................................................................................... vi

1. Introduction ................................................................................................................................. 1
   1.1. Scope of Beyond-CMOS Focus Team .................................................................................. 1
   1.2. Difficult Challenges .............................................................................................................. 2
   1.3. Nano-information Processing Taxonomy .............................................................................. 4

2. Emerging Memory Devices .......................................................................................................... 4
   2.1. Memory Taxonomy .............................................................................................................. 5
   2.2. Emerging Memory Devices .................................................................................................. 6
   2.3. Memory Selector Device ..................................................................................................... 17
   2.4. Storage Class Memory ........................................................................................................ 20

3. Emerging Logic and Alternative Information Processing Devices ........................................ 27
   3.1. Taxonomy ........................................................................................................................... 27
   3.2. Devices for CMOS Extension ............................................................................................. 28
   3.3. Beyond-CMOS Devices: Charge-Based ............................................................................ 32
   3.4. Beyond-CMOS Devices: Alternative Information Processing ......................................... 36

4. Emerging Device-Architecture Interaction .................................................................................. 41
   4.1. Introduction .......................................................................................................................... 41
   4.2. Analog Computing .............................................................................................................. 43
   4.3. Probabilistic Circuits .......................................................................................................... 57
   4.4. Reversible Computing ........................................................................................................ 59
   4.5. Device-Architecture Interaction: Conclusions/Recommendations .................................. 64

5. Beyond CMOS Devices for More-Than-Moore Applications ..................................................... 65
   5.1. Emerging Devices for Security Applications ...................................................................... 65

6. Emerging Materials Integration .................................................................................................. 69
   6.1. Introduction and Scope ....................................................................................................... 69
   6.2. Challenges .......................................................................................................................... 70
   6.3. Technology Requirements and Potential Solutions ......................................................... 71
   6.4. Emerging/Disruptive Concepts and Technologies ............................................................... 74
   6.5. Conclusions and Recommendations ................................................................................ 75

7. Assessment ................................................................................................................................. 75
   7.1. Introduction ........................................................................................................................ 75
   7.2. NRI Beyond-CMOS Benchmarking ................................................................................. 76
   7.3. Archive of ITRS ERD Survey-Based Assessment ............................................................... 78

8. Summary ..................................................................................................................................... 80

9. Endnotes/References .................................................................................................................. 82
List of Figures

Figure BC1.1 Relationship of More Moore, Beyond CMOS, and Novel Computing Paradigms and Applications (Courtesy of Japan beyond-CMOS group) ........................................... 1

Figure BC2.1 Taxonomy of Emerging Memory Devices ................................................................. 6

Figure BC2.2 Taxonomy of Memory Select Devices .......................................................... 17

Figure BC2.3 Comparison of Performance of Different Memory Technologies ....................... 23

Figure BC3.1 Taxonomy of Options for Emerging Logic Devices ........................................... 27

Figure BC4.1 Conventional vs. Alternative Computing Paradigms ........................................... 42

Figure BC4.2 A Resistive Memory Crossbar $Ax = b$ Solver is Illustrated ..................................... 45

Figure BC4.3 A Spiking CNN for Gesture Recognition with Local Learning .......................... 47

Figure BC4.4 One Generalized Instantiation of a Photonic MVM unit, with Wavelength Multiplexed Inputs and Outputs and a Coupler-based Tunable Array. Reproduced from .................................................... 55

Figure BC4.5 Energy Dissipation per Stage vs. Frequency in an Adiabatic CMOS Shift Register ................................................................................................................................. 61

Figure BC4.6 Energy dissipation of RQFP and irreversible AQFP 1-b full adders .................... 62

Figure EMI1 Emerging Material Integration Promotes the Advancement of Existing Technologies ......................................................................................................................... 70

Figure EMI2 An Example of the Role of Machine Learning in the Multiscale Simulation ........ 74

Figure BC7.1 (a) Energy versus Delay of a 32-bit ALU for a Variety of Charge- and Spin-based Devices; (b) Energy versus Delay per Memory Association Operation Using Cellular Neural Network (CNN) for a Variety of Charge- and Spin-based Devices ........................................................................................................... 77

Figure BC7.2 (a) Survey of Emerging Memory Devices and (b) Survey of Emerging Logic Devices in 2014 ERD Emerging Logic Workshop (Albuquerque, NM) ....................... 79

Figure BC7.3 Comparison of Emerging Memory Devices Based on 2013 Critical Review ...... 79

Figure BC7.4 Comparison of Emerging Logic Devices Based on 2013 ITRS ERD Critical Review: (a) CMOS Extension Devices; (b) Charge-based Beyond-CMOS Devices; (c) Non-charge-based Beyond-CMOS Devices .................................................. 80
List of Tables

Table BC1.1  Beyond CMOS Difficult Challenges ................................................................. 3
Table BC2.1  Emerging Research Memory Devices—Demonstrated and Projected Parameters ................................................................. 5
Table BC2.2  Experimental Demonstrations of Vertical Transistors in Memory Arrays .......... 18
Table BC2.3  Benchmark Select Device Parameters ............................................................. 18
Table BC2.4a Experimental Demonstrated Two-terminal Memory Select Devices .......... 20
Table BC2.4b Experimentally Demonstrated Self-selecting Memory Devices (self-rectifying) ... 20
Table BC2.5  Target Device and System Specifications for SCM ......................................... 22
Table BC2.6  Potential of Current Prototypical and Emerging Research Memory Candidates for SCM Applications ................................................................. 22
Table BC2.7  Likely Desirable Properties of M (Memory) Type and S (Storage) Type Storage Class Memories ................................................................. 26
Table BC3.1a MOSFETS: Extending MOSFETs to End of Roadmap ..................................... 27
Table BC3.1b Charge-based Beyond CMOS: Non-conventional FETs and Other Charge-based Information Carrier Devices ................................................................. 27
Table BC3.1c Alternative Information Processing Devices .................................................... 28
Table BC4.1  Metrics for Analog Capacitive Vector-Matrix Multiply (VMM) ICs ..................... 54
Table BC4.2  Comparison of Some Electrical Oscillators for Computing ............................. 56
Table EM11  Near-term Difficult Challenges ........................................................................ 70
Table EM12  Long-term Difficult Challenges ......................................................................... 70
Table EM13  Materials for Transistor Scaling and Integration ............................................... 71
Table EM14  Materials for Lithography and Patterning .......................................................... 72
Table EM15  Interconnect Materials ....................................................................................... 72
Table EM16  Heterogeneous Integration, Assembly and Packaging Materials ..................... 72
Table EM17  Emerging Research Materials Needs for Outside System Connectivity ............. 72
Table EM18  Emerging Materials for Memory ........................................................................ 73
Table EM19  Emerging Materials for Memory Select ................................................................ 73
Table EM10  Emerging Materials for Advanced and Beyond-CMOS Logic Devices .......... 73
Table EM11  Spin Devices versus Materials ........................................................................... 73
Table EM12  Spin Material Requirements and Properties ....................................................... 73
Table EM13  Metrology Needs and Challenges for Emerging Research Materials ................ 73
Table EM14  Modeling and Simulation .................................................................................. 74
Table EM15  Summary of Potentially Disruptive Emerging Research Materials Application Opportunities ......................................................................................... 75
ACKNOWLEDGMENTS

Sapan Agarwal          Shy-Jay Lin
Brad Aimone            Tsu-Jae King Liu
Hiro Akinaga          Matthew Marinella
Otitoaleke Akinola     Bicky A. Marque
Mustafa Badaroglu      Yoshiyuki Miyamoto
Gennadi Bersuker       Johannes Muller
Christian Binek         Azad Naeemi
Geoffrey Burr          Mitchell A. Nahmias
Leonid Butov           Emre Neftci
Kerem Camsari          Mike Niemier
Gert Cauwenberghs      Dmitri Nikonov
An Chen                Yutaka Ohno
Winston Chern          Chenyun Pan
Supriyo Datta          Shashi Paul
John Dallesasse        Ferdinand Peper
Shamik Das             Paul R. Prucnal
Erik DeBenedictis      Titash Rakshit
Peter Dowben           Shriram Ramanathan
Tetsuo Endoh           Mingyi Rao
Ben Feinberg           Arijit Raychowdhury
Thomas Ferreira de Lima Graham Rowlands
Akira Fujiwara         Sayeef Salahuddin
Elliot Fuller          Shintaro Sato
Michael Frank          Michael Schneider
Paul Franzon           Bhavin J. Shastri
Michael Fuhrer         Xia Sheng
Mike Garner            Chakku Goplan
Takahiro Shinada       Takahiro Shinada
Bogdan Govoreanu       Urmita Sikder
Cat Graves             Greg Snider
Kohei Hamaya           John-Paul Strachan
Masami Hane            Dimitri Strukov
Jennifer Hasler        Naoyuki Sugiyama
Yoshihiro Hayashi      Tarek Taha
Toshiro Hiramoto       Alexander N. Tait
D. Scott Holmes        Shinichi Takagi
Sharon Hu              Norikatsu Takaura
Francesca Iacopi       Tsutomu Teduka
Danielle Ilmeni        Yasuhide Tomioka
Jean Anne Incorvia     Wilman Tsai
Engin Ipek             Tohru Tsuruoka
Satoshi Kamiyama       Zhongrui Wang
Kiyoshi Kawabata       R. Stanley Williams
Asif Khan              Justin Wong
Hajime Kobayashi       Dirk Wouters
Suhas Kumar            Patrick Xiao
Ilya Krivorotov        Kojiro Yagami
Xiuling Li             J. Joshua Yang
Xiang (Shaun) Li       Noboyuki Yoshikawa
                      Victor Zhirnov
BEYOND CMOS

1. INTRODUCTION

1.1. SCOPE OF BEYOND-CMOS FOCUS TEAM

Dimensional and functional scaling\(^1\) of CMOS is driving information processing\(^2\) technology into a broadening spectrum of new applications. Scaling has enabled many of these applications through increased performance and complexity. As dimensional scaling of CMOS will eventually approach fundamental limits, several new information processing devices and microarchitectures for both existing and new functions are being explored to extend the historical integrated circuit scaling cadence. This is driving interest in new devices for information processing and memory, new technologies for heterogeneous integration of multiple functions, and new paradigms for system architecture. This chapter, therefore, provides an IRDS perspective on emerging research device technologies and serves as a bridge between conventional CMOS and the realm of nanoelectronics beyond the end of CMOS scaling.

An overarching goal of this chapter is to survey, assess, and catalog viable emerging devices and novel architectures for their long-range potential and technological maturity and to identify the scientific/technological challenges gating their acceptance by the semiconductor industry as having acceptable risk for further development. This chapter also surveys beyond-CMOS devices for more than Moore (MtM) applications, e.g., hardware security.

This goal is accomplished by addressing two technology-defining domains: 1) extending the functionality of the CMOS platform via heterogeneous integration of new technologies (“More Moore”), and 2) stimulating invention of new information processing paradigms (“Beyond CMOS”). The relationship between these domains is schematically illustrated in Figure BC1.1. Novel computing paradigms and application pulls (e.g., big data, Internet of Things (IoT), artificial intelligence, autonomous systems, exascale computing) introduce higher performance and efficiency requirements, which is increasingly difficult for the saturating More Moore technologies to fulfill. Beyond-CMOS technologies may provide the required devices, processes, and architectures for the new era of computing.

![Figure BC1.1](image)

**Figure BC1.1** Relationship of More Moore, Beyond CMOS, and Novel Computing Paradigms and Applications (Courtesy of Japan beyond-CMOS Group)

The chapter is intended to provide an objective, informative resource for the constituent nanoelectronics communities pursuing the following: 1) research, 2) tool development, 3) funding support, and 4) investment. These communities include universities, research institutes, and industrial research laboratories; tool suppliers; research funding agencies; and the semiconductor industry. The potential and maturity of each emerging research device and architecture technology are reviewed and assessed to identify

---

\(^1\) Functional Scaling: Suppose that a system has been realized to execute a specific function in a given, currently available, technology. We say that system has been functionally scaled if the system is realized in an alternate technology such that it performs the identical function as the original system and offers improvements in at least one of size, power, speed, or cost, and does not degrade in any of the other metrics.

\(^2\) Information processing refers to the input, transmission, storage, manipulation or processing, and output of data. The scope of the BC Chapter is restricted to data or information manipulation, transmission, and storage.
the most important scientific and technological challenges that must be overcome for a candidate device or architecture to become a viable approach.

The chapter is divided into five sections: 1) emerging memory devices, 2) emerging logic and alternative information processing devices, 3) emerging device-architecture interaction, 4) beyond-CMOS devices for More-than-Moore applications, and 5) emerging materials integration. The former IRDS Emerging Research Materials (ERM) chapter is rolled into this chapter as section 6 renamed to “emerging materials integration”. Some detail is provided for each entry regarding operation principles, advantages, technical challenges, maturity, and current and projected performance. The chapter also discusses applications and architectural focus combining emerging research devices offering specialized, unique functions as heterogeneous core processors integrated with a CMOS platform technology. This represents the nearer term focus of the chapter, with the longer-term focus remaining on discovery of an alternate information processing technology beyond digital CMOS.

1.2. DIFFICULT CHALLENGES

1.2.1. INTRODUCTION

The semiconductor industry is facing some difficult challenges related to extending integrated circuit technology to new applications and to beyond the end of CMOS dimensional scaling. One class relates to propelling CMOS beyond its ultimate density and functionality by integrating a new high-speed, high-density, and low-power memory technology onto the CMOS platform. Another class is to extend CMOS scaling with alternative channel materials. The third class is information processing technologies substantially beyond those attainable by CMOS using an innovative combination of new devices, interconnect, and architectural approaches for extending CMOS and eventually inventing a new information processing platform technology. The fourth class is to extend ultimately scaled CMOS as a platform technology into new domains of functionalities and application, also known as “more than Moore”. The fifth class is to bridge the gap between novel devices and unconventional architectures and computing paradigms. These difficult challenges are summarized in Table BC1.1.

1.2.2. DEVICE TECHNOLOGIES

Difficult challenges gating development of beyond-CMOS devices include those related to memory technologies, information processing or logic devices, and heterogeneous integration of multi-functional components, a.k.a. More-than-Moore (MtM) or Functional Diversification.

One challenge is the need of a new memory technology that combines the best features of current memories in a fabrication technology compatible with CMOS process flow and that can be scaled beyond the present limits of SRAM and FLASH. This would provide a memory device fabrication technology required for both stand-alone and embedded memory applications. The ability of an MPU to execute programs is limited by interaction between the processor and the memory, and scaling does not automatically solve this problem. The current evolutionary solution is to increase MPU cache memory, thereby increasing the floor space that SRAM occupies on an MPU chip. This trend eventually leads to a decrease of the net information throughput. In addition to auxiliary circuitry to maintain stored data, volatility of semiconductor memory requires external storage media with slow access (e.g., magnetic hard drives, optical CD, etc.). Therefore, development of electrically accessible non-volatile memory with high speed and high density would initiate a revolution in computer architecture. This development would provide a significant increase in information throughput beyond the traditional benefits of scaling when fully realized for nanoscale CMOS devices.

A related challenge is to sustain scaling of CMOS logic technology. One approach to continuing performance gains as CMOS scaling matures in the next decade is to replace the strained silicon MOSFET channel (and the source/drain) with an alternate material offering a higher potential quasi-ballistic-carrier velocity and higher mobility than strained silicon. Candidate materials include strained Ge, SiGe, a variety of III-V compound semiconductors, and carbon materials. Introduction of non-silicon materials into the channel and source/drain regions of an otherwise silicon MOSFET (i.e., onto a silicon substrate) is fraught with several very difficult challenges. These challenges include heterogeneous fabrication of high-quality (i.e., defect free) channel and source/drain materials on non-lattice matched silicon, minimization of band-to-band tunneling in narrow bandgap channel materials, elimination of Fermi level pinning in the channel/gate dielectric interface, and fabrication of high-κ gate dielectrics on the passivated channel materials. Additional challenges are to sustain the required reduction in leakage currents and power dissipation in these ultimately scaled CMOS gates and to introduce these new materials into the MOSFET while simultaneously minimizing the increasing variations in critical dimensions and statistical fluctuations in the channel (source/drain) doping concentrations.

The industry is now addressing the increasing importance of a new trend of functional diversification, where added value to devices is provided by incorporating functionalities that do not necessarily scale according to “Moore's Law”. In this chapter, an “Beyond-CMOS devices for More-than-Moore Applications” section covers unconventional applications of existing and novel technologies. The section currently covers emerging devices for hardware security and will be expanded in future update.
A longer-term challenge is invention and reduction to practice of a manufacturable information processing technology addressing “beyond CMOS” applications. For example, emerging research devices might be used to realize special purpose processor cores that could be integrated with multiple CMOS CPU cores to obtain performance advantages. These new special purpose cores may provide a particular system function much more efficiently than a digital CMOS block, or they may offer a uniquely new function not available in a CMOS-based approach. Solutions to this challenge beyond the end of CMOS scaling may also lead to new opportunities for such an emerging research device technology to eventually replace the CMOS gate as a new information processing primitive element. A new information processing technology must also be compatible with a system architecture that can fully utilize the new device. A non-binary data representation and non-Boolean logic may be required to employ a new device for information processing. These requirements will drive the need for new system architectures. The requirements and opportunities correlating emerging devices and architectures are discussed in the “Emerging Device-Architecture Interaction” section.

---

**Table BC1.1   Beyond CMOS Difficult Challenges**

<table>
<thead>
<tr>
<th><strong>Difficult Challenges</strong></th>
<th><strong>Summary of Issues and Opportunities</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Scale high-speed, dense, embeddable, volatile/non-volatile memory technologies to replace SRAM and FLASH in appropriate applications.</td>
<td>The scaling limits of SRAM and FLASH in two dimensional (2D) are driving the need for new memory technologies to replace SRAM and FLASH memories. Identify the most promising technical approach(es) to obtain electrically accessible, high-speed, high-density, low-power, (preferably) embeddable volatile and non-volatile memories. The desired material/device properties must be maintained through and after high temperature and corrosive chemical processing. Reliability issues should be identified and addressed early in the technology development.</td>
</tr>
<tr>
<td>Extend CMOS scaling</td>
<td>Develop new materials to replace silicon (or III-V, Ge) as alternate channel and source/drain to increase the saturation velocity and to further reduce Vth and power dissipation in MOSFETs while minimizing leakage currents. Develop means to control the variability of critical dimensions and statistical distributions (e.g., gate length, channel thickness, S/D doping concentrations, etc.) Accommodate the heterogeneous integration of dissimilar materials. The desired material/device properties must be maintained through and after high temperature and corrosive chemical processing. Reliability issues should be identified and addressed early in this development.</td>
</tr>
<tr>
<td>Continue functional scaling of information processing technology substantially beyond that attainable by ultimately scaled CMOS.</td>
<td>Invent and reduce to practice a new information processing technology to replace CMOS as the performance driver. Ensure that a new information processing technology has compatible memory technologies and interconnect solutions. A new information processing technology must be compatible with a system architecture that can fully utilize the new device. Non-binary data representations or non-Boolean logic may be required to employ a new device for information processing, which will drive the need for new system architectures. Bridge the gap that exists between materials behaviors and device functions. Accommodate the heterogeneous integration of dissimilar materials. Reliability issues should be identified and addressed early in the technology development.</td>
</tr>
<tr>
<td>Extend ultimately scaled CMOS as a platform technology into new domains of functionalities and application (“more than Moore, MiM”).</td>
<td>Discover and reduce to practice new device technologies and primitive-level architecture to provide special purpose optimized functional cores (e.g., accelerator functions) heterogeneously integrable with CMOS. Provide added value by incorporating functionalities that do not necessarily scale according to “Moore’s Law”. Heterogeneous integration of digital and non-digital functionalities into compact systems that will be the key driver for a wide variety of application fields, such as communication, automotive, environmental control, healthcare, security, and entertainment.</td>
</tr>
<tr>
<td>Bridge the gap between novel devices and unconventional architectures and computing paradigms.</td>
<td>Identify suitable opportunities in unconventional architectures and computing paradigms that can utilize unique characteristics of novel devices. Identify emerging devices that can implement computing functions and architectures more efficiently than CMOS and Boolean logic.</td>
</tr>
</tbody>
</table>
4 Emerging Memory Devices

1.2.3. MATERIALS TECHNOLOGIES
The most difficult challenge for Beyond CMOS is to deliver materials with controlled properties that will enable operation of emerging research devices in high density at the nanometer scale. To improve control of material properties for high-density devices, research on materials synthesis must be integrated with work on new and improved metrology and modeling. These important objectives are addressed in the “Emerging Materials Integration” section.

1.3. NANO-INFORMATION PROCESSING TAXONOMY
Information processing systems to accomplish a specific function, in general, require several different interactive layers of technology. One comprehensive top-down list of these layers begins with the required application or system function, leading to system architecture, micro- or nano-architecture, circuits, devices, and materials. A different bottom-up representation of this hierarchy begins with the lowest physical layer represented by a computational state variable and ends with the highest layer represented by the architecture. In this representation focused on generic information processing at the device/circuit level, a fundamental unit of information (e.g., a bit) is represented by a computational state variable, for example, the position of a bead in the ancient abacus calculator or the charge (or voltage) state of a node capacitance in CMOS logic. The electronic charge as a binary computational state variable serves as the foundation for the von Neumann computational system architecture. A device provides the physical means of representing and manipulating a computational state variable among its two or more allowed discrete states. Eventually, device concepts may transition from simple binary switches to devices with more complex information processing functionality, perhaps with multiple fan-in and fan-out. The device is a physical structure resulting from the assemblage of a variety of materials possessing certain desired properties obtained through exercising a set of fabrication processes. An important layer, therefore, encompasses the various materials and processes necessary to fabricate the required device structure, which is a focus of the “Beyond CMOS (BC)” chapter. The data representation is how the computational state variable is encoded by the assemblage of devices to process the bits or data. Two of the most common examples of data representation are binary digital and continuous or analog signal. This layer is within the scope of the BC chapter. The architecture layer encompasses three subclasses of this taxonomy: 1) nano-architecture or the physical arrangement or assemblage of devices to form higher level functional primitives to represent and execute a computational model, 2) the computational model that describes the algorithm by which information is processed using the primitives, e.g., logic, arithmetic, memory, cellular nonlinear network (CNN), and 3) the system-level architecture that describes the conceptual structure and functional behavior of the system exercising the computational model.

2. EMERGING MEMORY DEVICES
The emerging research memory technologies tabulated in this section are a representative sample of published research efforts (circa 2017 – 2019) describing alternative approaches to established memory technologies. The scope of this section also includes updated subsections addressing the “Select Device” required for a crossbar memory application and an updated treatment of “Storage Class Memory” (including Solid State Disks).

Figure BC2.1 is a taxonomy of the prototypical and emerging memory technologies. An overarching theme is the need to monolithically integrate each of these memory options onto a CMOS technology platform in a seamless manner. Fabrication technologies are sought that are modifications of or additions to established CMOS platform technologies. A goal is to provide the end user with a device that behaves similarly to the familiar silicon memory chip.

This memory portion of this section is organized around a set of seven technology entries shown in the column headers of Table BC2.1. These entries were selected using a systematic survey of the literature to determine areas of greatest worldwide research activity. Each technology entry listed has several sub-categories of devices that are grouped together to simplify the discussion. Key parameters associated with the technologies are listed in the table. For each parameter, two values for performance are given: 1) theoretically predicted performance values based on calculations and early experimental demonstrations, 2) up-to-date experimental values of these performance parameters reported in the cited technical references.

The tables have been extensively footnoted, and details may be found in the indicated references. The text associated with the table gives a brief summary of the operating principles of each device and significant scientific and technological issues, not captured in the table, but which must be resolved to demonstrate feasibility.

---

3 Including a particular approach in this section does not in any way constitute advocacy or endorsement. Conversely, not including a particular concept in this section does not in any way constitute rejection of that approach. This listing does point out that existing research efforts are exploring a variety of basic memory mechanisms.
The purpose of many memory systems is to store massive amounts of data, and therefore memory capacity (or memory density) is one of the most important system parameters. In a typical memory system, the memory cells are connected to form a two-dimensional array, and it is essential to consider the performance of memory cells in the context of this array architecture. A memory cell in such an array can be viewed as being composed of two fundamental components: the ‘storage node’ and the ‘select device’, the latter of which allows a given memory cell in an array to be addressed for read or write. Both components impact scaling limits for memory. For several emerging resistance-based memories, the storage node can, in principle, be scaled down below 10 nm,¹ and the memory density will be limited by the select device. Planar transistors (e.g., field effect transistor (FET) or bipolar junction transistor (BJT)) are typically used as select devices. In a two-dimensional layout using in-plane select FETs the cell layout area is \( \text{A}_{\text{cell}} = (6-8)F^2 \). In order to reach the highest possible 2-D memory density of \( 4F^2 \), a vertical select transistor can be used. Table BC2.2 shows several examples of vertical transistor approaches. Another approach to obtaining a select device with a small footprint is a two-terminal nonlinear device, e.g., a diode. Table BC2.3 displays benchmark parameters required for a 2-terminal select device, and Table BC2.4 summarizes the operating parameters for several candidate 2-terminal select devices.

Storage-class memory (SCM) describes a device category that combines the benefits of solid-state memory, such as high performance and robustness, with the archival capabilities and low cost per bit of conventional hard-disk magnetic storage. Such a device requires a non-volatile memory technology that can be manufactured at a very low cost per bit. Table BC2.5 lists a representative set of target specifications for SCM devices and systems, which are compared against benchmark parameters offered by existing technologies (hard disk drive (HDD), NAND Flash, and DRAM). Two columns are shown, one for the slower S-class Storage Class Memory (SCM), and one for fast M-class SCM, as described in Section 2.4. These numbers describe the performance characteristics that will likely be required from one or more emerging memory devices in order to enable the emerging application space of Storage Class Memory. Table BC2.6 illustrates the potential for storage-class memory applications of a number of prototypical memory technologies (Table BC2.1) and emerging research memory candidates (Table BC2.2). The table shows qualitative assessments across a variety of device characteristics, based on the target system parameters from Table BC2.5. These tables are discussed in more detail in Section 2.4.

Table BC2.1  Emerging Research Memory Devices—Demonstrated and Projected Parameters

2.1. MEMORY TAXONOMY

Figure BC2.1 provides a simple visual method of categorizing memory technologies. At the highest level, memory technologies are separated by the ability to retain data without power. Non-volatile memory offers essential use advantages, and the degree to which non-volatility exists is measured in terms of the length of time that data can be expected to be retained. Volatile memories also have a characteristic retention time that can vary from milliseconds to (for practical purposes) the length of time that power remains on. Non-volatile memory technologies are further categorized by their maturity. Flash memory is considered the baseline non-volatile memory because it is highly mature, well optimized, and has a significant commercial presence. Flash memory is the benchmark against which prototypical and emerging non-volatile memory technologies are measured. Prototypical memory technologies are at a point of maturity where they are commercially available (generally for niche applications), and have a large scientific, technological, and systems knowledge base available in the literature. The focus of this section is Emerging Memory Technologies. These are the least mature memory technologies in Figure BC2.1, but they have been shown to offer significant potential benefits if various scientific and technological hurdles can be overcome. This section provides an overview of these emerging technologies, their potential benefits, and the key research challenges that will allow them to become viable commercial technologies.
2.2. EMERGING MEMORY DEVICES

2.2.1. NOVEL MAGNETIC MEMORIES

This section is divided into three categories of devices based on different mechanisms, i.e., spin-transfer torque, spin-orbital torque, and voltage-controlled magnetic anisotropy.

2.2.1.1. SPIN-TRANSFER TORQUE

Spin-transfer torque (STT) MRAM has recently entered the commercial production stage for both embedded and standalone Flash-like applications. Various foundries announce the readiness of embedded MRAM (TSMC, GlobalFoundries, Samsung) for production, and standalone MRAM products with various density (Mb-GB) are also available on the market for IoT and data center applications (Avalanche Tech, Everspin). For embedded applications, STT-MRAM possesses non-volatility, high-endurance, scalability, low power, and fewer masks than the embedded Flash. It also provides great area savings and lower leakage compared with SRAM. A STT-MRAM cell consists of a magnetic tunnel junction (MTJ) with two ferromagnetic layers, i.e. a free layer (FL) and a reference layer (RL) sandwiching a tunnel barrier. When a current enters the RL, the electrons' spin is polarized according to that of the RL. After tunneling through to the FL, the spin momentum of these spin-polarized electrons is transferred to the FL, thus writing the FL orientation to that of the RL. The opposite operation can be achieved by flipping the current polarity. Compared with its in-plane counterpart, perpendicular STT-MRAM has higher density, lower switching current, and is easier to control in large scale manufacturing.

Since Flash-like STT-MRAM is entering mass production at all major foundries, this topic is covered in the More Moore Chapter of IRDS. For cache-level applications, research has shown 3 ns, 63 μA switching of 16-nm perpendicular STT-MRAM with endurance above 10^{12} cycles and write error rate (WER) below 10^{-6}. Reliable 10 ns, 0.12 pJ switching of 50 μA with sub-ppm error rates is also recently demonstrated in 30 nm perpendicular STT-MTJs satisfying the last level cache (LLC) application requirements. A system-level benchmarking study also indicates the use of 34 nm perpendicular STT-MRAM to replace SRAM as a LLC for high performance computing (HPC) at 5 nm node provides significant read and write energy gains at about 43% of the total macro area, achieving a nominal access latency <2.5 ns and <7.1 ns for read and write respectively. (see Table BC2.1)

For SRAM-like STT-MRAM development, a major challenge is to reduce the write power consumption at sub-10 ns write speed. The large write power at sub-ns speed using STT requires a large access transistor, reducing density as well as reduced endurance due to tunnel barrier damage from higher writing current. Multiple factors contribute to this high switching current at sub-10 ns regime including limited spin torque efficiency, incubation delay, and intrinsic magnetization precession frequency on the order of GHz. A great amount of work has been devoted to increasing the switching speed, such as decreasing the FL saturation magnetization, lowering the FL damping factor, and increasing the STT effect via double-RL design. However, because at most 100% of the current can be polarized, there is an upper bound of the write efficiency using the STT effect. In contrast, the use of writing mechanisms of fundamentally different physics, such as spin-orbit torque (SOT) and voltage-controlled magnetic anisotropy (VCMA) effect, may help propel the next-generation of MRAM technologies for SRAM-like cache applications. Secondly, as the critical dimension of STT-MRAM scales down to less than 20 nm, the requirement of thermal stability calls for higher interfacial perpendicular magnetic anisotropy (PMA). Double-MgO barrier MTJs have shown 2x improvement in MTJ...
with diameters above 10 nm,9 whereas the use of shape-anisotropy induced PMA from elongated ferromagnetic pillars may further the scaling of STT-MRAM below 10 nm diameter.10 Lastly, STT-MRAM with higher density to replace DRAM is still an open area for research. Stacking of STT-MRAM dies with logic or memory dies using through silicon vias,11,12 and high density 3-dimensional (3D) integration of STT-MRAM using selector-MTJ crossbar architecture13 are two high potential approaches.

### 2.2.1.2. Spin-Orbit Torque

Spin-orbit torque (SOT)-driven magnetization switching recently emerges as an alternative write mechanism beyond STT for SRAM-like cache-level applications. Though at rather early stage of research, sub-ns SOT writing has been demonstrated at current density of 20-40 MA/cm²14,15 compared with 3-10 ns switching of STT-MRAM at a current density of 7 MA/cm²,5,16 (see Table BC2.1). A SOT-MRAM cell consists of a magnetic tunnel junction (MTJ) with its free layer (FL) sitting on top of a strip of material with large spin-orbit coupling (SOC), such as heavy metal17,18. When current flows through this long strip of SOT material, spin-polarized current emerges and diffuses into the adjacent FL. Like the STT case, the spin-polarized current exerts a damping-like spin torque on the ferromagnetic layer, thus switching the FL orientation. As the write path is separated from the read path, a much larger read voltage can increase read speed. The major advantage of SOT over STT is that unlike STT where the filtered spin-polarized current is smaller than the charge current, the SOT efficiency (spin-polarized current over charge current) can be larger than one in the SOT case.19 From a physics perspective, multiple mechanisms have been found to contribute to this large damping-like SOT, including spin Hall effect (SHE)17, Rashba-Edelstein effect18, and spin-momentum locking from topological protected electronic states19. Most experimental work has discovered a damping-like SOT in the in-plane transverse direction with respect to the current flow direction. However, there also exists a field-like SOT in many of the experimental works, which acts on the free layer like a static magnetic field with a fixed orientation.

There are three types of SOT-MRAM configurations, i.e., in-plane MTJ with easy axis oriented along the current direction (type X), in-plane MTJ with easy axis oriented orthogonal to the current direction (type Y), and perpendicular MTJ (type Z). Note that only type Y can achieve field-free switching, while both type X and Z require the breaking of symmetry for deterministic switching. Experimentally, 0.5-ns switching with a current density of 40 MA/cm² has been demonstrated in a 100 x 400 nm² type X MTJ, which will lead to 51-µA, 0.3-V, and 8-fJ write performance when scaled down to a channel width of 50 nm.14 Another work shows 0.5-ns switching with a current density of 18 MA/cm² in 30 x 190 cm² type Y MTJ with a write error rate (WER) of 10⁻⁷.15 For perpendicular MTJ (type Z), research has shown 0.5-ns and 220-fJ write operation with a current density of 180 MA/cm² of a 60 nm perpendicular MTJ with endurance up to 10¹¹ and WER down to 10⁻⁴. Field-free switching is realized in this work by using an elongated biasing ferromagnet deposited on top of the SOT-MTJ.20

Lowering the write energy while maintaining sub-ns switching speed is the main challenge to push SOT-MRAM into cache-level applications. A multitude of novel SOT materials beyond traditional heavy metal are being intensively investigated for higher SOT efficiency. Several new research directions include heavy metal alloys21, topological insulator and semimetal22,23, antiferromagnets24,25, and complex oxides26,27. The need of high SOT efficiency is especially critical for type Z as it inherently shows a larger switching current than type X and Y.28 Second, SOT-MRAM suffers from a large cell size due to the three-terminal configuration needed to perform separate write and read functions.29 A two-terminal perpendicular SOT-MRAM has been demonstrated by increasing the density of the current flowing in-plane in the SOT underlayer while suppressing that of the current flowing perpendicular in the MTJ.30 Meanwhile, the scheme of multiple SOT-MTJs sharing one single SOT write line can partially alleviate the density disadvantage of SOT-MRAM.31 Third, a tradeoff exists between writing speed and field-free switching. For type Y, the FL aligning to the transverse direction does not experience any SOT; thus, an initial perturbation of the FL away from the easy axis is required for fast switching. A large field-like SOT or Oersted field due to SOT current can provide this perturbation.32 For type X and Z, a maximal SOT exists as the FL is aligned perpendicular to the spin current direction, thus enabling high-speed switching. There have been several approaches to break the symmetry for realizing field-free type X and Z switching, such as lateral structural and shape-induced asymmetry33,34, use of interlayer exchange coupling35, exchange bias36, and dipolar external magnetic field37. Meanwhile, new studies show field-free switching of type Z MTJ using a damping-like SOT with perpendicular polarization arising from crystalline materials with broken in-plane symmetry38 and interfaces with SOC39. Last, the scalability of all three SOT types remains an open question. Type X and Y scaling are challenging due to variations in MTJ shape, while type X and Z scaling face obstacles in implementing field-free switching at scaled nodes.

### 2.2.1.3. Voltage-Controlled Magnetic Anisotropy

Contrary to current-driven writing mechanisms such as STT and SOT, voltage-assisted writing using electron-mediated voltage-controlled magnetic anisotropy (VCMA) effect40 enables lower write energy (~fJ) and smaller cell size due to reduced current, and therefore joule heating and select transistor size.(see Table BC2.1) A VCMA-MTJ is almost the same as an STT-MTJ, except that the tunnel barrier MgO thickness is increased to suppress the tunneling current and enhance the capacitive characteristics of the tunnel barrier.41 When a voltage is applied across the VCMA-MTJ, charge accumulation or depletion takes place at the FL/buffer interface, leading to a change of electron occupancies among different Fe 3d orbitals. Because the interfacial
perpendicular magnetic anisotropy (PMA) originates from the Fe 3d and O 2p orbitals hybridization, this change of electron occupancy results in the modulation of PMA and thus the energy barrier between the two FL stable states.\textsuperscript{40,42,43} The VCMA effect is, therefore, a useful handle to reduce the energy barrier during the write operation, while the energy barrier is restored for retention purposes after writing by simply removing the VCMA bias.

There are two main types of VCMA-assisted magnetization switching schemes. First, removal of the entire energy barrier by the VCMA effect facilitates a precessional motion of the FL along an in-plane bias field direction (built-in or applied). By precise timing of the VCMA pulse width, the FL can switch from one state to the other in half the precession period.\textsuperscript{44} Research has shown switching energy of 6 fJ/bit, switching speed of 0.5 ns, write voltage of 1.96 V, current density of 0.3 MA/cm\textsuperscript{2} with a WER of 10\textsuperscript{13} using perpendicular MTJs with a VCMA coefficient of 30 fJ/V-m.\textsuperscript{45} Another recent work further shows 0.15 ns precessional switching of 120 nm perpendicular VCMA-MTJ at a write voltage of 3.06 V, a current density of 0.3 MA/cm\textsuperscript{2} with a WER of <10\textsuperscript{6}.\textsuperscript{46} Second, the VCMA effect can be utilized to reduce the write energy in in-plane and perpendicular SOT-MTJs further.\textsuperscript{31,47} Research has demonstrated VCMA-assisted (VCMA bias of 1 V) SOT writing of 30 x 80 nm\textsuperscript{2} to 50 x 120 nm\textsuperscript{2} in-plane MTJ using 2-ns pulse with a current density of 12 MA/cm\textsuperscript{2} with a high endurance of 10\textsuperscript{13} write cycles.\textsuperscript{48} Another work shows 5-ns 62 μA SOT current writing (VCMA bias of 1.2 V) of 30 x 80 nm\textsuperscript{2} in-plane MTJ with WER <10\textsuperscript{6} and endurance over 10\textsuperscript{12} cycles, the VCMA coefficient in this device is about 100 fJ/V-m.\textsuperscript{49}

The major roadblock of VCMA in either precessional switching or assisting SOT switching is the rather small VCMA coefficient of around 100 fJ/V-m, as defined by the interfacial PMA change under given electric field applied at the MgO barrier.\textsuperscript{50} Though an approximate level write performance has already been demonstrated, further scaling of MTJs requires higher VCMA coefficient (>300 fJ/V-m) for advanced nodes cache or storage applications.\textsuperscript{51} New materials research using Cr and Ir-based crystalline MTJs have shown a high VCMA coefficient of up to 1000 fJ/V-m.\textsuperscript{52,53} Meanwhile, detailed chemical and structural characterizations of VCMA-MTJs recently reveal that metal-oxides at the FL/MgO interface lead to large VCMA effect.\textsuperscript{55} Another challenge facing VCMA is the longer read time because the thicker MTJ tunnel barrier leads to a much larger MTJ resistance. One way to resolve this is using a large read voltage (V\textsubscript{DD}) which has reverse polarity compared with the write voltage to increase read speed and reduce read disturbance.\textsuperscript{55} In terms of the precessional switching scheme, another significant challenge is the non-deterministic nature of the writing process, which results in large WER and narrow write pulse window. The use of pulse shape engineering and reverse biasing can partially help\textsuperscript{56,57}, whereas combining VCMA with deterministic writing mechanisms such as type Y SOT\textsuperscript{47} and STT\textsuperscript{58} may solve this challenge.

2.2.2. **Oxide-Based Resistive Memory (OxRAM)**

The redox-based nanoionic memory operation is based on a change in resistance of a MIM structure caused by ion (cation or anion) migration combined with redox processes involving the electrode material or the insulator material, or both.\textsuperscript{59,60,61} Three classes of electrically induced phenomena have been identified that involve chemical effects, i.e., effects which relate to redox processes in the MIM cell. In these three ReRAM classes, there is a competition between thermal and electrochemical driving forces involved in the switching mechanism. Two major types of ReRAM exist: i) those based on metal oxide (OxRAM), which involve oxygen ions/vacancies motion, and ii) conducting bridge-based RAM (CBRAM), which involves metal cation motion. This section covers the three categories of OxRAM, and CBRAM is covered in the following section. Beyond CMOS has subcategorized oxide ReRAM (OxRAM) based on the electrical switching type (bipolar versus unipolar) and whether a conductive filament is formed in the device. Most of the literature fits into the three categories: bipolar filamentary, unipolar filamentary, and nonfilamentary.\textsuperscript{52}

In most cases, the conduction is of a filamentary nature, and hence a one-time formation process is required before the bipolar switching can be started. If this process can be controlled, memories based on this switching process can be scaled to very small feature sizes. The switching speed is limited by the ion transport. If the active distance over which the anions or cations move is small (in the <10 nm regime) the switching time can be below few nanoseconds, down to sub-nanoseconds range.\textsuperscript{63,64} Many of the finer details of the ReRAM switching mechanisms are still under investigation. Developing an understanding of the physical mechanisms governing switching of the redox memory is a key challenge for this technology. Nevertheless, recent experimental demonstrations of scalability,\textsuperscript{65} retention,\textsuperscript{66} and endurance\textsuperscript{67} are encouraging.

2.2.2.1. **Bipolar-Filamentary OxRAM**

Bipolar filamentary OxRAM is the most common form of oxide-based ReRAM. At any given defect density, the number of current paths through the dielectric, in the virgin or fresh state, is proportional to the device area, and consequently the total current is area dependent. In addition, the current magnitude tends to fluctuate from device to device due to randomness of the initial distribution of vacancies/ions. However, cell area dependency is eliminated when the current is dominated by a single conductive path, called conductive filament (CF). The CF provides an ultimate scaling advantage since it is only limited to the active filament size, which potentially may be as small as a few nm.
A one-time forming process is required for most types of OxRAM devices to create a conduction filament across the dielectric layer linking the electrodes. A stable preferential conduction path is known to form through oxide films subjected to electrical stress: under the applied voltage, a current abruptly increases at some point in time indicating the occurrence of a dielectric breakdown (BD) resulting in the formation of a CF. During the forming process, electrons injected from the cathode electrode may lead to their trapping at defect sites in the dielectric material inducing chemical bonds breakage and the generation of anion vacancies (Oxygen or Nitrogen). \(^{68,69}\)

Post-forming switching events between high and low conductive states, which are operated at significantly smaller voltages, are believed to modify the filament conductivity by rupturing/recovering a section of the filament (primarily in the vicinity of the metal electrode) or changing the filament cross-section. The specific mechanisms in filament-type switching depend on the materials (dielectric and metal electrodes) employed in the fabrication of the memory cell and may include more than one type of a conduction mode. The operation of these devices involves redox reactions of the dielectrics sandwiched between two electrodes. \(^{70,71,72}\) The dielectrics are mostly comprised of one or a few layers of insulating materials \(^{73}\) (e.g., oxide AlO\(_x\), HfO\(_x\), TaO\(_x\), TiO\(_x\), WO\(_x\), ZrO\(_x\), oxynitrides AlO\(_x\)N\(_y\), or nitrides including AlN\(_x\) and CuN\(_x\)). TaO\(_x\) and HfO\(_x\) are the leading candidates among the aforementioned dielectrics, due to their superior performance (e.g., endurance) and CMOS compatibility.

Since the demonstration of a single crosspoint HfO\(_x\) device with a 10 nm dimension in 2011 \(^{74}\), scaling to a smaller size has been achieved by employing a sidewall electrode in a 1x3 \(\mu\)m\(^2\) cross-sectional HfO\(_x\)-based OxRAM device with reasonable performance in terms of both endurance and retention. \(^{75}\) Up to 10\(^{12}\) cycles has been demonstrated with Zr:SiO\(_x\) sandwiched by graphene oxide layers. \(^{76}\) Some of the filament-based metal-oxide RRAMs implemented with metal electrodes and a variety of fab-friendly transition-metal-oxides (i.e., HfO\(_x\), ZrO\(_x\), TiO\(_x\), etc.) and nitride devices demonstrated sub-nanosecond \(^{77,78}\) switching with high (up to 10\(^{12}\) cycles) endurance \(^{79}\) and retention of more than 10 years. Extrapolated retention at 85°C by stressing TaO\(_x\) in the temperature range from 300°C to 360°C is estimated to be years with an activation energy of 1.6 eV. \(^{80}\) Reliable switching operations have been demonstrated at 340°C with devices based on 2D layered heterostructures (e.g., graphene/MoS\(_2\), \(\chi\)O/graphene). \(^{81}\)

Unconventional electrodes such as graphene have been paired with HfO\(_x\) dielectrics to yield a low power consumption, a write/erase energy of 230 fJ per bit for a single programming transition. \(^{82}\) Pt/BMO((Bi, Mn)O\(_x\))/Pt structured OxRAM device was used to demonstrate an even lower write/erase energy per transition, of the order of 3.8 pJ/bit for read and 20 pJ/bit for write operation. \(^{83}\)

Large scale integration of OxRAM switching based on 1T1R schemes has been carried out by Toshiba, Panasonic and IMEC. In 2013, Toshiba announced the 32 Gb RRAM chip integrated with 24 nm CMOS. \(^{84}\) In 2014, Panasonic and IMEC demonstrated the encapsulated cell structure with an Ir/TaO\(_x\)/TaO\(_x\)/TaN stack on a 2 Mbit chip at the 40 nm node. In addition, passive integration of 1S1R scheme has been reported by Crossbar on a 4 Mbit chip, but the material stack of the OxRAM switch has not been revealed. \(^{85}\) Ultra-fast (down to 100 ps), compliance-free, low power (< pJ) switching was demonstrated with 1R devices using TiN/HfO\(_x\)/TaN stack. \(^{86}\)

A number of technical challenges hampering the commercialization of OxRAM still remain despite the significant advancements made in the field. One of the main challenges is the fact that the switching currents for devices based on the currently most mature materials (e.g., HfO\(_x\) and TaO\(_x\)) are still too high (above tens of \(\mu\)A) for large arrays. Apart from that, the filament formation and rupture processes are stochastic in nature, which leads to variation in switching parameters like the voltage and resistance distribution of the switching. This is especially detrimental to certain applications such as multilevel cell memory.

### 2.2.2.2. Bipolar Non-Filamentary OxRAM

The Bipolar Non-Filamentary OxRAM is a non-volatile bipolar resistive switching device composed of one or more oxide layers. One layer is a conductive metal oxide (CMO), which is usually a perovskite such as PrCaMnO\(_x\) or Nb:SrTiO\(_x\). \(^{87}\) In contrast to Unipolar and Bipolar Filamentary OxRAM devices—typically based on binary oxides such as TiO\(_x\), NiO\(_x\), HfO\(_x\), TaO\(_x\) or combinations thereof—the resistance change effect of the Bipolar Non-Filamentary OxRAM is uniform. Depending on the materials choice and structure the current is conducted across the entire electrode area, or at least across the majority of this area. A forming step to create a conductive filament is not needed. Non-volatile memory functionality is achieved by the field-driven redistribution of oxygen vacancies close to the contact resulting in a change of the electronic transport properties of the interface (e.g. by modifying the Schottky barrier height). Oxygen can be exchanged between layers due to the exponential increase in ion mobility at high fields. Low current densities, uniform conduct, and bipolar switching imply that substantial self-heating is not involved. Typical \(R_{OFF}\) to \(R_{ON}\) ratios are on the order of 10.

One class of the Bipolar Non-Filamentary OxRAM includes a deposited ion conductive tunnel layer (Tunnel ReRAM), e.g. ZrO\(_x\). Here, a redistribution of oxygen vacancies causes a change of the electronic transport properties of the tunnel barrier. Low current densities and area scaling of device currents enable ultra-high-density memory applications. Set, reset, and read currents scale...
with device area. In addition, set, reset, and write currents are controlled by the tunnel oxide and hence, can be adjusted by changing the tunnel barrier thickness. Both set and reset IV characteristics are highly nonlinear enabling true 1R cross-point architectures without the need for an additional selector device for asymmetric arrays up to 512×4096 bit. No external circuitry is needed for current control during set operation. A continuous transition between on and off states allow straightforward multi-level programming without the need for precise current control.

The typical thickness of the CMO is greater than 5 nm and the tunnel barrier is typically 2–3 nm. If a tunnel barrier is present, the adjacent electrode needs to be an inert metal such as Pt to prevent oxidation during operation. For the case of PCMO cell, low deposition temperatures of less than 425°C of all layers enables back end integration schemes.

Currently the technology is in the research and development stage. Depending on material system and structure cycling endurance over 10,000 cycles and up to a billion cycles as well as data retention from days to months at 70°C has been achieved on single devices. Within the Bipolar Non-Filamentary OxRAM device family the Tunnel OxRAM is probably the furthest developed technology. Single device functionality is demonstrated down to 30 nm. Set, reset, and read currents scale with area and tunnel oxide thickness facilitating sub μA switching currents with read currents in the order of a few nA to a few 100 nA. BEOL integration schemes and CMOS/OxRAM functionality are verified for 200 nm devices on 200 mm CMOS wafers. True cross-point array (1R) functionality utilizing the self-selecting non-linear device IV characteristics and transistor-less array operation is demonstrated on fully decoded 4kb true cross-point arrays (1R) build on top of CMOS base wafers. SLC and MLC operations are demonstrated within 4kb arrays.

Major challenges to be resolved towards the commercialization of Bipolar Non-filamentary OxRAM are, in order of priority, a) improvement of data retention, b) the integration of conductive metal oxide layer (perovskites) via ALD or the replacement of CMO by more process-friendly materials, and c) the replacement of Pt electrodes by a non-reactive, more process-friendly electrode material.

The most important issue is the improvement of retention and the “voltage-time dilemma.” This dilemma hypothesizes physical reasons as to why it is difficult in a particular device and material system to simultaneously obtain a long retention, with short low read voltages, and fast switching at moderate write voltages. Even though the exact mechanism is still under investigation there is a common agreement that oxygen vacancies are moved by the external electric field resulting in different resistance states of the memory cell. Vacancy drift at room temperature is possible due to a field dependent mobility, which increases exponentially with field at fields of 1 MV/cm and larger. However, current models based on a field-dependent mobility underestimate the experimentally observed ratio between set/reset times and data retention indicating that the mechanism is only partly understood. More theoretical work is needed to understand the kinetics of programming and retention mechanisms. Once understood, materials need to be chosen to maximize the ratio between set/reset and retention times. The goal is to set/reset devices at low temperatures and meet retention requirement of 10 years at 70°C, 85°C, and 125°C, depending on the application. A multi-layer ReRAM structure (HfO2/A2O3) was shown to improve retention by suppressing tail bit failure due to decreased oxygen ion diffusivity.

Memory cells using conductive perovskite material as an electrode have proven to show excellent device-to-device and wafer-to-wafer reproducibility with yields close to 100%. One of the reasons might be that perovskites display high oxygen vacancy mobilities and tolerate large variations in the oxygen content while maintaining its crystal structure. From an integration perspective, ALD is the method of choice for advanced technology nodes and future 3D integration schemes. Key issues are the control of the metals ratio (perovskites are ternary or quaternary oxides), the control of the oxygen stoichiometry in the cell, oxygen loss in the presence of reducing atmospheres like H2, as well as high temperatures required for crystallization. Eventually a migration to binary oxides with comparable properties might be required to resolve the integration challenges.

Platinum or other noble electrodes display superior device performance over fab-friendly electrodes like TiN. On the one hand it was observed that the oxidation resistance of TiN is not sufficient to prevent oxidation and the formation of TiO2 during operation. On the other hand, inert electrodes such as Pt or Pt-like metals are difficult to integrate. New oxidation-resistant electrodes and Pt alternatives are required to reduce integration challenges and enable 3D integration schemes.

### 2.2.2.3. Unipolar Filamentary OxRAM

Note that unipolar filamentary OxRAM has been removed from the memory tracking tables, due to lack of research over the period covered by this Beyond CMOS chapter. However, this text section has been maintained to provide background on earlier unipolar OxRAM work, due to the close relationship and key differences with bipolar OxRAM.

Unipolar OxRAM is another resistive switching device, also referred to in the literature as thermochemical memory (TCM) due to its primary switching mechanism. The device structure consists of a top electrode metal/insulator/bottom electrode metal (MIM) structure. Typical insulator materials are metal-oxides such as NiOx, HfOx, etc., and common metal electrodes include...
TiN, Pt, Ni, and W. In general, the device can be asymmetric (i.e. top electrode material differs from bottom electrode material), but unlike other types of ReRAM, asymmetry is not required.

The first reported resistive switching in these MIM structures after 2000 was unipolar in nature (see reference\(^9\) for the first integrated device work that put metal oxide ReRAM in the spotlight). Unipolar is defined as switching where the same polarity of voltage needs to be applied for changing the resistance from high to low (SET) or from low to high (RESET). Note that in the general case, polarity is still important (e.g. repeatable SET/RESET switching only occurs for one polarity of voltage with respect to one of the electrodes\(^4\)). Only in symmetric structures (e.g. Pt/HfO\(_2)/Pt), nonpolar behavior can be obtained, where SET and RESET are occurring irrespective of voltage polarity.\(^9\)

The switching process is generally understood as being filamentary, where conduction is caused by a filamentary arrangement of defects (e.g. oxygen vacancies) throughout the thickness of the insulator film. As with other filamentary OxRAM devices, an initial high voltage “electroforming” step is required to form the conduction filament, while subsequent RESET/SET switching is thought to occur through local breaking/restoration of this conduction path.

The unipolar character of the switching indicates that drift (of charged defects) in an electric field plays a less important role (than it does in bipolar switching resistive memory), but that thermal effects probably dominate.\(^96,97\) On the other hand, polarity effects indicate anodic oxidation (e.g. at Ni or Pt electrodes) is responsible for RESET.\(^94\) These findings suggest a thermo-chemical “fuse” model for describing this unipolar switching. It has been shown for different MIM structures that both unipolar and bipolar switching mechanisms can be induced, depending on the operation conditions.\(^98,99,100,101\) An interesting work reporting on the Scaling Effect on Unipolar and Bipolar Resistive Switching of Metal Oxides was published.\(^102\)

A unipolar switching device is seen as advantageous for making scaled memory arrays, as it only requires a selector device as simple as a diode that can be stacked vertically with the memory device in a dense crossbar array.\(^93\) In addition, the use of a single program voltage polarity greatly simplifies the circuitry.

On the other hand, as has been exemplified in mixed mode (unipolar/bipolar) operation of memory cells, there are important trade-offs between the unipolar and bipolar switching modes. On the positive side, unipolar switching mode typically shows a higher ON/OFF resistance ratio. On the negative side, unipolar switching is typically obtained at higher switching power (higher currents) than the bipolar mode, and also endurance is much more limited. As a result, major research and development work on resistive memories has shifted towards bipolar switching mechanisms. Yet, some interesting recent development work has been reported.\(^103,104,105,106,107,108\) One paper\(^103\) shows an endurance of over 10\(^6\) cycles with a resistive window of over 5 orders of magnitude (and a reset current ~1mA). Others\(^104,105,106\) demonstrate how unipolar RRAM elements can be integrated in a very simple way in an existing CMOS process (known as Contact ReRAM technology). This may provide a very inexpensive embedded ReRAM technology. Recently, integration unipolar ReRAM with a 28 nm CMOS process was reported.\(^106\) The key attributes were a small cell size (0.03 \(\mu\)m\(^2\)), switching voltage of less than 3V, RESET current of less than 60 \(\mu\)A, endurance > 10\(^6\) cycles, and short SET and RESET times of 500 ns and 100 \(\mu\)s, respectively. One paper\(^107\) shows 4Mb array data using this same Contact-ReRAM technology, fabricated using a 65 nm CMOS process. To accommodate the low logic VDD process, an on-chip charge pump was applied. Set and reset voltages are less than 2 V. Another paper\(^108\) reports on a novel approach using thermal assisted switching to lower the switching current.

As stated above, large OFF to ON resistance ratio is an attribute of unipolar switching. The low resistance window and large intrinsic variability of bipolar switching OxRAM may require complex and time-consuming switching operation schemes (e.g. the so-called verify scheme). Further study of the stability and control of the large resistance window (at low current levels), are required to determine if unipolar OxRAM variability can be improved, potentially even allowing for multi-level cell operation.

Major challenges to be resolved are the high switching current that seems inherent to the unipolar operation mode. Reset currents less than 100 \(\mu\)A are achieved but need further reduction to less than 10 \(\mu\)A.\(^104,105,106\) Recently, a possible solution incorporating thermally assisted switching has been presented.\(^108\)

2.2.3. Conducting Bridge Memory

Conductive Bridge RAM (CBRAM), also referred to as Programmable Metallization Cell (PMC), and electrochemical metallization cells, is a device which utilizes electrochemical control of nano-scale quantities of metal in thin dielectric films or solid electrolytes to perform the resistive switching operation.\(^109\) The basic CBRAM cell is a metal–ion conductor–metal (MIM) system consisting of an electrode made of an electrochemically active material such as Ag, Cu or Ni, an electrochemically inert electrode such as W, Ta, or Pt, and a thin film of solid electrolyte sandwiched between both electrodes.\(^110\) Large, non-volatile resistance changes are caused by the oxidation and reduction of the metal ions by the application of low bias voltages. Key attributes are low voltage, low current, rapid write and erase, good retention and endurance, and the ability for the storage cells to be physically scaled to a few tens of nm. The material class for the dielectric film or the solid electrolyte is comprised of oxides, higher chalcogenides (including glasses), semiconductors, as well as organic compounds including polymers.
CBRAM is a strong emerging memory candidate primarily due to scalability (~10 nm), ultra-low energy operations due to fast read, write and erase times, and low voltage requirements. Maturity of the CBRAM technology development can be assessed by the fact that many companies are either shipping products based on CBRAM or are in advanced stages of commercialization. Recent publications show CBRAM technology application in various markets including SSDs, embedded non-volatile memory (NVM), and serial interface non-volatile memory replacement. In 2012, a CBRAM-based serial NVM replacement product became commercially available. In 2014, a 16 GB CBRAM array based on a CuTe CBRAM cell was demonstrated. Such efforts are critical to identify core technology challenges and fundamental materials and mechanisms. Novel applications such as reconfigurable switch and synaptic elements in Neuromorphic systems based on CBRAM are also gaining prominence and are expected to expand the application base for this technology. An atom-switch-based field-programmable gate array is also released using Cu conduction bridge in a new polymer solid electrolyte.

As with other filamentary ReRAM technologies, CBRAM is challenged by bit level variability, the random nature of reliability failure such as retention or endurance, and random telegraph noise potentially contributing to read disturbs. Such issues require large populations of bits to be studied, which suggests collaboration between universities and industry may be beneficial. Focus on fundamental understanding and simultaneously addressing some mitigation path such as error correction schemes, redundancy and algorithm development would enable closing the technology gap.

Engineering hurdles include the availability and integration of new materials used in CBRAM at advanced process nodes especially when there could be issues with compatibility of thermal budgets and process tooling. The availability of integrated array level information suggests that some of these challenges are being resolved in the recent years. Active participation from semiconductor equipment vendors and material suppliers would assist in overcoming manufacturing hurdles rapidly.

### 2.2.4. Macromolecular (Polymer) Memory

Macromolecular memory is a category of memory which focuses on structures incorporating a layer of polymer—the polymer perhaps containing nano-particles, small molecules and nanoparticles - that is sandwiched between two metal electrodes. This structure allows two different stable electrical states controlled through an external electrical voltage. These two stable electrical states, which are often called ON and OFF states (or 0 and 1), exhibit resistive, ferroelectric or capacitive natures according to the physical properties of the sandwich. The first fully-organic memory devices, based on nano-composite (a blend of poly-vinylphenol (PVP) and Bucky-ball (C60)) was presented in Materials Research Society in 2005. Around the same time, memory devices using gold nano-particles and 8-hydroxyquinoline, dispersed in a polystyrene matrix, were also demonstrated. Since then, the interest to use an admixture of nano-particles, small molecules and polymers in the manufacture of electronic memory devices, is on the rise. Non-volatile memory effects with a non-destructive read have been reported for a surprisingly large variety of polymeric/organic materials and blends of polymers with nanoparticles and molecules. Unlike the other four categories, this category is based on the material used in the switching layer(s) of the cell, but the mechanism is not specified. Both bipolar and unipolar (all pulses of the same polarity) switching have been demonstrated. Macromolecular ReRAM may have a mechanism placing it in one of the four main ReRAM categories listed above. However, the other mechanisms behind the electrical bistability, such as capacitive and ferroelectric, have also been reported.

Depending on the structure of the polymer, a variety of mechanisms can be operative. For polymers supporting transport of inorganic ions, formation of metallic filaments is reported. In semiconducting polymers supporting ion transport, dynamic doping due to migration of inorganic ions occurs. Ferroelectric polymers in blends with semiconducting material give rise to a memory effect-based modification of charge injection barriers by the ferroelectric polarization. However, for many polymeric materials, the origin of the resistive switching is not well understood. To date no specific design criteria for the polymer are known, although clear correlations between memory effect and electronic properties of the polymer have been demonstrated.

Stability of the memory states at high temperatures (85°C, 2 × 10^4 s) has been demonstrated. Programming at very low power (70 nW) has been realized. Assuming a 15 ns switching time for the same system, one might achieve a write energy of 6 × 10^15 J/bit. Furthermore, low programming voltages have been realized: +1.4 and -1.3 V for the two states with good retention time (>10^5 s). Downscaling of polymer resistive memory cell to the 100 nm length scale has been reported. At this length scale, integration of memory cells into an 8 × 8 array could be shown. Polymer memory cells on a flexible substrate have been shown. For amorphous carbon, downscaling to nanometer sized cells has been published (1 × 10^3 nm^2). Using carbon nanotubes as macroelectrode electrodes and aluminum oxide as interlayer, isolated, non-volatile, rewriterable memory cells with an active area of essentially 36 nm^2 have been achieved, requiring a switching power less than 100 nW, with estimated switching energies below 10 fJ per bit. With regards to the mechanism of operation, extensive work on the class of polyimide polymers has shown clear correlations between electronic structure of the polymer and memory effects, although a comprehensive picture for the operation has not yet emerged. A number of studies have indicated an active role of the interface between macromolecular material and (native) oxide layers in the operation of the memory involving charge trapping. The recent and past studies...
show resistive, capacitive (charge storage, based on electric dipole formation) and ferroelectric behavior of such devices. Thus, there is a need to open up a further discussion on the right pathway to realize such memory.

In macromolecular memory, a large variety of operation mechanisms can be operative. A key research question concerns distinguishing different mechanisms and evaluating the potential and possibilities of each mechanism. A second subsequent step would be to identify model systems for each mechanism. Having such a model system then provides a possibility to benchmark the operation of the macromolecular materials. These research steps would be crucial for establishing and securing the collaboration of the chemical industry; for design, synthesis and development of the next generation macromolecular materials for memory applications, clear guidelines on the required structural and electronic properties of the macromolecular material are needed. For instance, memory effect originating for metallization and formation of metallic filaments requires macromolecular materials that support transport of ions and have appropriate internal free volume for ion conduction. Here the field could benefit from interaction with the field of polymer batteries. Ferroelectric polymers have been shown to give rise to resistive memory and could benefit enormously from development of new macromolecular polymeric materials with combined ferroelectric switching and semiconducting structural units. Finally, a number of macromolecular memories involve oxide layers. Here mutually beneficial interaction with the (research) community on metal oxide ReRAM switching could spring, because at the macromolecular / oxide interface trap states can be engineered by tuning the electron levels of the macromolecular material.

In a nutshell, this area certainly needs an attention from theoretical physicists, materials scientists, chemists and device engineers. There are a number of issues that need to be addressed before we can embark on extending these devices to the real world. Such issues involve understanding of the electrical bistability mechanism in nano composite (there are a number of contradicting theories), maintaining the difference between low and high conduction states for a longer period time by ensuring the stability of the high and low states, selecting environmentally friendly materials required for fabrication of nano composite/polymer materials, and developing a cost-effective methodology for the fabrication of devices.

It is not possible to replace silicon-based memory devices with polymers in the foreseeable future. However, there are a number of other applications where “cheap” electronic memory devices can play a vital role. For example, nano-composite based memory devices can be directly printed on medicine bottles/packages and the information about the patient and schedule of taking medicine can be stored on the printed device.

### 2.2.5. Ferroelectric Memory

Coding digital memory states by the electrically alterable polarization direction of ferroelectrics has been successfully implemented and commercialized in capacitor-based Ferroelectric Random Access Memory (covered in Table BC2.1). However, in this technology the identification of the memory state requires a destructive read operation and largely depends on the total polarization charge on a ferroelectric capacitor, which in terms of lateral dimensions is expected to shrink with every new technology node. In contrast to that, alternative device concepts, such as the ferroelectric field effect transistor (FeFET) and the ferroelectric tunnel junction (FTJ), allow for a non-destructive detection of the memory state and promise improved scalability of the memory cell. The current status of and key challenges for these emerging ferroelectric memories will be assessed within this section.

#### 2.2.5.1. Ferroelectric FET

The FeFET is best described as a conventional MISFET that contains a ferroelectric oxide in addition to or instead of the commonly utilized SiO$_x$, SiON or HfO$_2$ insulators. The former case requires the direct and preferably epitaxial contact of the ferroelectric to the semiconductor channel (metal-ferroelectric-semiconductor-FET, MFSFET), whereas the latter and commonly applied case maintains a buffer layer between the channel material and the ferroelectric (metal-ferroelectric-insulator-semiconductor-FET, MIFISFET). When additionally introducing a floating gate in-between the buffer layer and the ferroelectric, a metal-ferroelectric-metal-insulator-semiconductor structure (MFMISFET) may be obtained that shares its equivalent circuit representation with the MFSFET approach. By applying a sufficiently high voltage pulse to the gate of the FeFET (i.e. voltage drop across the ferroelectric layer larger than its coercive voltage $V_C$), the polarization direction of the ferroelectric can be set to either assist in the inversion of the channel or to enhance its accumulation state. This results in a polarization dependent shift of the threshold voltage $V_T$, which allows for a non-destructive read operation and a 1T memory operation comparable to that of FLASH devices.

In order to assess the material and device requirements for a reliable and scalable FeFET technology the following two intrinsic relations in a ferroelectric gate stack need to be considered. First it is important to note that the extent of the aforementioned $V_T$-shift (memory window) in FeFET devices is primarily determined by the $V_C$ of the implemented ferroelectric rather than by its remnant polarization $P_r$. This results in a scaling versus memory window trade-off as $V_C$ is proportional to the coercive field $E_C$ and thickness $d_{FE}$ of the ferroelectric. The inability of the commonly utilized perovskite-based FeFETs to laterally scale beyond the 180 nm node is therewith not solely based on the insufficient thickness scaling of perovskite ferroelectrics, but rather due to their low $E_C$ (SBT: 10-100 kV/cm, PZT: ~50 kV/cm, summarized in Table BC2.1) that in order to maintain a reasonable memory
window requires compensation by a large $d_E$. A solution to this scaling retardation is provided by the high coercive field (1-2 MV/cm) and thickness-scalable FE-HfO$_2$.\textsuperscript{145} This CMOS-compatible material innovation enabled the demonstration of a FeFET technology scaled to the 28 nm node utilizing a conventional HKMG technology and is already used in high volume production.\textsuperscript{146} The close resemblance of the HKMG transistor and the FE-HfO$_2$-based memory transistor proves especially useful for the realization of an embedded memory solution with greatly reduced mask counts as compared to embedded FLASH.

The second noteworthy and important characteristic of the FeFET gate stack is related to its intrinsic capacitive voltage divider, which causes a significant gate voltage drop and buildup of electric field not only across the ferroelectric, but also across the non-ferroelectric insulator in the gate stack. When additionally considering the incapability of the linear insulator to fully compensate the polarization charge of the ferroelectric layer, it becomes apparent that even in the case of no external biasing the capacitive voltage divider leads to a buildup of a permanent electric field. The so-called depolarization field building up in the ferroelectric is opposed to the polarization direction of the ferroelectric and to the electric field induced in the insulator\textsuperscript{147}. The capacitive voltage divider is therefore directly responsible for the retention loss during stand-by as well as for the gate voltage distribution and the corresponding charge injection during write operations. This retention- and endurance-critical distribution of the electric field within the gate stack may be optimized by choosing the insulator capacitance as high as possible and the ferroelectric capacitance as low as possible. In the perovskite-based FeFET this is achieved by utilizing high-k buffer layers and is additionally fostered by the unavoidably large physical thickness of the perovskite ferroelectrics.\textsuperscript{148} In the case of the aggressively scaled FE-HfO$_2$-based FeFET, the small thickness of the ferroelectric is compensated by the comparably low permittivity of HfO$_2$ the possibility to use ultra-thin interfacial layers, and by the depolarization resilience of the high $E_c$.\textsuperscript{144,149} This leads to the situation that despite the markedly different stack dimensions and materials used, the electrically obtained characteristics are quite similar. Fast switching speed ($\leq$100 ns), switching voltages in the range of 4-6 V, and 10-year data retention and endurance in the range of $10^{12}$ switching cycles have been demonstrated for FE-HfO$_2$\textsuperscript{145,146,150,151} as well as for perovskite-based FeFETs.\textsuperscript{141,152,153} In the case of cycling endurance, however, the high $E_c$ of FE-HfO$_2$ and the correspondingly large electric field in the insulator facilitates charge trapping during write operation, which was identified as the root cause for the limited endurance of $10^5$ cycles observed in FE-HfO$_2$-based FeFETs with ultra-thin interfacial layer enabling excellent data retention.\textsuperscript{154} Nevertheless, in an alternative approach utilizing a thicker insulator and sub-loop operation it was demonstrated that at the cost of retention a cycling endurance $>10^{12}$ may still be obtained.\textsuperscript{150} In the current stage of development this endurance versus retention trade-off may be tailored, spanning the application range from embedded NOR-FLASH replacement with high retention requirements to low refresh rate 1T DRAM requiring high cycling endurance.

Entirely overcoming this endurance versus retention trade-off will require an improved stack design that may include a tailored polarization hysteresis (low $P_s$ and high $P/P_s$ ratio)\textsuperscript{141}, a reduced trap density at the interfaces,\textsuperscript{154} an optimized capacitive voltage divider by area scaling in the MFMISFET approach\textsuperscript{155} or the realization of a MFSFET device by implementing recent breakthroughs in the epitaxial growth of FE-HfO$_2$.\textsuperscript{156} Despite promising results obtained for perovskite-based FeFET devices implemented into 64 Kb NAND-Arrays at a feature size of 5 $\mu$m\textsuperscript{157}, little is known about the variability and array characteristics of FeFET devices scaled to technology nodes approaching the grain or domain size of the implemented ferroelectrics. Initial investigations on phase and grain distribution in doped HfO$_2$ based ferroelectric thin films and the effects of such granularity on device level characteristics of scaled FeFETs (such as on the statistical nature of switching) have recently been reported in Refs.\textsuperscript{157,158,159}. Recently, 64 Kb and 32 Mb FeFET arrays were demonstrated in the 28 nm\textsuperscript{160} and the 22 nm FD-SOI CMOS platform\textsuperscript{161}, respectively—in each case, a clear low and high $V_T$ separation at the array level was demonstrated. Nevertheless, in order to fully judge the variability of ferroelectric phase stability at the nanoscale and to guide material optimization and fundamental understanding of the phenomenon, larger array statistics in the Kb to Mb range and high-resolution PFM data will be required. Besides, recent demonstration of non-volatile memory operation based on antiferroelectricity—a phenomenon closely related to ferroelectricity—in work-function engineered ZrO$_2$ thin film capacitors may allude to new way of addressing and potentially solving some of these challenges in FeFETs.\textsuperscript{162}

### 2.2.5.2. Ferroelectric Tunnel Junction

The ferroelectric tunnel junction, a ferroelectric ultra-thin film commonly sandwiched by asymmetric electrodes and/or interfaces, exhibits ferroelectric polarization induced resistive switching by a non-volatile modulation of barrier height. With the tunneling current depending exponentially on the barrier height, the ferroelectric dipole orientation either codes for a high or a low resistance state in the FTJ, which can be read out non-destructively. The resulting tunneling electroresistance (TER) effect of FTJs, the ratio between HRS and LRS, is usually in the range of 10 to 100 (163 and references therein). However, giant TER of $>10^4$ has most recently been reported in a super-tetragonal BiFeO$_3$ based FTJ by Yamada et al.\textsuperscript{164} A similarly high TER was demonstrated by Wen and co-workers\textsuperscript{165} for a BaTiO$_3$ tunnel barrier by replacing one metal electrode of the FTJ with a semiconducting electrode. With this new junction design, the modulation of tunneling current does not only rely on barrier height, but due to a variable space charge region in the semiconductor, also on a barrier width modification. With these most recent findings, two strategies
to achieve giant TER have been identified: either use a ferroelectric barrier with a large polarization such as BiFeO₃ or use a semiconductor as electrode material to modulate the barrier width by field-induced carrier depletion.

The MFM-based structure of FTJs may be able to enable a retention time (> 10 years) and very high cycling endurance (> 10¹⁴) properties of conventional ferroelectric RAM (FRAM). Nonetheless, in order to have a significant tunneling current, ferroelectric films in FTJs usually have a thickness ranging from several unit cells to ~5 nm, which is much thinner than in commercialized 1T-1C FRAM (> 50 nm). Due to larger interface contributions and increased leakage currents at reduced thickness, experimental data of these material systems might strongly deviate from their thick film behavior and need to be assessed separately. However, even though only limited data are available up to this point, promising single cell characteristics have already been demonstrated, such as the most recent demonstration of 4x10⁸ endurance cycles and extrapolated data retention of 10 years at room temperature for a BiFeO₃-based FTJ. In the context of retention, it should be noted that despite improved TER, the newly proposed MFS-FTJ structure will give rise to a depolarization field, which will most likely degrade memory retention in a similar manner as described for the FeFET in Section 2.2.5.1. The highly energy efficient electric field switching, common to all ferroelectric memories, enables fast (10 ns) and low voltage (1.4 V) switching in FTJ devices and results in a minimal power consumption during write operation (1.4 J/bit, calculation based on the device characteristics given). Due to the availability of non-destructive read-out and the further reduced ferroelectric thickness in FTJ devices as compared to conventional FRAM, improved voltage scaling and total energy consumption may be expected from this technology.

Similar to most other two-terminal resistor-based memories with insufficient self-rectification, the elimination of sneak currents in large crossbar arrays is most efficiently suppressed utilizing 1 transistor-1 resistor (1T-1R) or 1 diode-1 resistor (1D-1R) cell architecture. In terms of scaling, this two-element memory cell, as well as the scalability of the selector device itself, has to be considered. Simply based on the lateral dimensions of the FTJ element (assuming unlimited scalability of the selector), scaling below 50 nm² based on PFM data, most likely appears possible. However, with further scaling a simultaneous enhancement of the LRS current density is required to maintain readability in massively parallel memory architectures. A recent breakthrough of 1.4x10⁹ A/cm² current density at 300 nm feature size has been achieved by Bruno et al. utilizing low resistivity nickelate electrodes. Based on these results maintaining 10 µA read current for feature sizes <100 nm appears possible. New FTJ concepts are also emerging; for example, engineered domain walls within the ferroelectric layer in an FTJ structure can lead to exotic quantum phenomenon such as resonant electron tunneling and quantum oscillations in the electrical conductance albeit at low temperatures.

FTJ based memories are currently at a very early development stage, and most of the research activity is focused on perovskite-based ferroelectrics. Further investigations reaching beyond single device characterization will be needed to fully judge the scalability of FTJ as well as its MLC capability suggested in Ref. So far, no conclusions can be drawn on retention and statistical distribution of the polarization induced resistance states in large arrays. However, when considering the collective phenomenon of ferroelectricity with multiple dipoles contributing to a resistance change as opposed to filament-type resistive switching, advanced scalability may be expected. First results have shown that the FTJ is very similar to ReRAM in terms of electrical behavior and memory design, albeit distinct physical mechanisms. It should be noted that current prototypes could actually have both FTJ and ReRAM traits, as resistive switching is common among oxides including ferroelectric perovskites (and references therein). For future development, the ferroelectric film in an ideal FTJ should be as thin as possible to allow scalability (while maintaining sufficient read current) and much less defective than that in ReRAM (e.g., with fewer oxygen vacancies), so that the mechanism of ferroelectric switching can dominate electrical behavior with little influence from mechanisms related to conducting filaments. The manufacturability of the rather complex electrode-perovskite ferroelectric-system of the FTJ concept will largely rely on the availability of high throughput and CMOS-compatible epitaxial growth techniques for large substrates or alternatively on the unrestricted feasibility demonstration of a polycrystalline FTJ. In this context it is worth noting that the CMOS-compatibility and advanced thickness scalability of ferroelectrics based on HfO₂ and its doped variant as well as recent breakthroughs in its epitaxial growth might yield great potential for the manufacturability of competitive FTJs. Experimental demonstrations of FTJs based on doped variant of HfO₂ were recently reported in Refs.

### 2.2.6 Mass Storage Devices

Device scaling has become a matter of strategic importance for modern and future information storage technologies, which motivates an exploration of unconventional materials with competitive performance attributes. By 2040 the conservative estimate the worldwide amount of stored data is 10⁸²⁴ bits, and the high estimate is ~10⁸²⁹ bits (these estimates are based on research by Hilbert and Lopez). In nature, much of the data about the structure and operation of a living cell is stored in the molecule of deoxyribonucleic acid (DNA) and using nucleic acids molecules, such as DNA, for memory storage has been proposed. DNA has an information storage density that is several orders of magnitude higher than any other known storage technology: 1 kg of DNA stores 10⁸²⁴ bits, for which >10⁹ kg of silicon Flash memory would be needed. Thus, a few tens of kilograms of DNA could meet all of the world’s storage needs for centuries to come.
A number of recent studies have shown that DNA can support scalable, random-access and error-free information storage. A state-of-the-art operating system developed at the University of Washington with an industry partner is a DNA-based archival storage framework that supports random access from a DNA key-value store. The DNA-stored files are compatible with mainstream digital format, and large-scale DNA storage up to 200 MB has been demonstrated. There are still many unknowns regarding both DNA operations in cell and with regard to the potential of DNA technology for massive storage applications. DNA volumetric memory density far exceeds ($10^3$–$10^5 \times$) projected ultimate electronic memory densities. Also, in the living cell, the memory read/write operations occur at high speed (<100 µs/bit) and require very low energy of ~$10^{-17}$ J/bit or $10^{-11}$ W/GB. DNA can store information stably at room temperature for hundreds of years with zero power requirements, making it an excellent candidate for large-scale archival storage. Also, DNA is an extremely abundant and totally recyclable material. Recently, a method for efficient encoding of information—including a full computer operating system—into DNA was presented, which approaches the theoretical maximum for information stored per nucleotide. One of the goals for research efforts is to demonstrate miniaturized, on-chip integrated DNA storage. New methods for DNA synthesis and sequencing are key components for these developments.

Two major categories of technical challenges remain:

- **Physical Media**: Improving scale, speed, cost of synthesis and sequencing technologies.
- **Operating System**: Creating scalable indexing, random access and search capabilities.

The key technological and scientific challenges are in improving performances beyond the life sciences industry. In the life science industry applications require perfect synthesis and perfect sequencing, while scale, throughput and cost are secondary considerations. For data storage, high read and write error rates can be tolerated, and information encoding schemes can be used. In this application, scale and throughput cost are primary considerations. Current DNA storage workflows can take several days to write and then read data, due to reliance on life sciences technologies that were not designed for use in the same system. The demonstrated DNA write-read cycle is too slow and costly to support exascale archival data storage. Solving this problem will require: 1) Substantial reductions in the cost of DNA synthesis and sequencing, and 2) Deployment of these technologies in a fully automated end-to-end workflow.

### 2.2.7. MOTT MEMORY

Mott memory is a metal/insulator/metal capacitor structure consisting of a correlated electron insulator (or Mott insulator). Correlated electron insulators often show the electronic phase transition accompanied by a drastic change in their resistivity under external stimuli such as temperature, magnetic field, electric field, and light. Mott memory exploits this electronic phase transition (called Mott metal-to-insulator transition or Mott transition) induced by an electric field. A mechanism of the Mott memory has been theoretically proposed in terms of the interfacial Mott transition induced by the carrier accumulation at a Schottky-like interface between a metal electrode and a correlated electron insulator. The theory also predicted that the resistive switching due to the interfacial Mott transition has a non-volatile-memory functionality, because the Mott transition is a first-order phase transition due to its nature. In addition, a Mott memory based on the Mott transition involving a large number of carriers (more than $10^{22}$ cm$^{-3}$) has in principle an advantage in device scaling, because there are a sufficient number of carries for the Mott transition even in a nanoscale device. In an ideal Mott transition, the electrons localized due to the strong electron-electron correlation come to be itinerant, via the stimuli, such as application of an electric field, and so forth. It needs no dopants, and the mechanism withstands the miniaturization of the (silicon) devices.

The Mott transition induced by an electric field or carrier injection has been experimentally demonstrated in a correlated electron material of Pr$_1$.Ca,MnO$_3$. After this demonstration, two-terminal devices such as switches and memories have been intensively studied using such correlated electron oxides as Pr$_1$.Ca,MnO$_3$, VO$_2$, VO$_3$, SmNiO$_3$, NiO, Ca$_2$RuO$_4$, and NbO$_2$. and using Mott-insulator chalcogenides of AM$_2$X$_3$ (A=Ga, Ge; M=V, Nb, Ta; X=S, Se). In addition to these inorganic materials, reversible and non-volatile resistive switching based on the electronic phase change between charge-crystalline state and quenched charge glass has recently been demonstrated in the organic correlated materials of $\theta$-(BEDT-TTF)$_2$X (where X denotes an anion).

SmNiO$_3$ exhibits a colossal (8 orders in magnitude) resistance jump by hydrogenation. The SmNiO$_3$ channel with the solid state proton gate has demonstrated the electric base gated large ON/OFF switching. The trigger for switching is based on the proton intercalation by electric field, and the DFT calculation explains the large gap opening by additional electron doping via protonation and is the origin for colossal resistance jump phenomena. These results indicate that the device using the metal – insulator (Mott) transition driven by the strong electron-electron correlation is powerful as well as appropriate for the switching devices.

Scalability has been demonstrated down 110 $\times$ 110 nm$^2$ in Mott memristors consisting of NbO$_2$ that shows the temperature-driven Mott transition from a low-temperature insulator phase to a high-temperature metal phase. The switching speed, energies, and...
endurance of the NbO$_2$-Mott memristors have been evaluated to be less than 2.3 ns, of the order of 100 fF, and >10$^9$, respectively.\textsuperscript{200,201} The programing and read voltages reported so far are <2 V and <0.2 V, respectively.\textsuperscript{198} The non-volatile resistive switching of AMX$_5$ single crystals was induced by the electric field of less than 10 kV/cm.\textsuperscript{202,203,204,205} This suggests that if the device consisting of a 10-nm-thick AMX$_5$ film is fabricated, the switching voltage will be less than 0.01 V.

Although non-volatile switching has been reported in the devices based on AMX$_5$ and $\theta$(BEDT-TTF)$_2$X, their retention characteristics are not elucidated in detail.\textsuperscript{202,203,204,205} In addition, the NbO$_2$-Mott memristors and VO$_2$-based devices are volatile switch.\textsuperscript{193,194,195,200,201} The retention is thus a major concern of Mott memory. In principle, the Mott transition can be driven even by a small amount of carrier doping to the integer-filling or half-filling valence states of the transition element.\textsuperscript{188} However, because of disorders, defects, and spatial variation of chemical composition, a rather large amount of carriers of more than 10$^{22}$ cm$^{-3}$ are required to drive the Mott transition in actual correlated electron materials, resulting in a relatively large switching voltage required in the Mott memory. Therefore, one of the key challenges is the control of crystallinity and chemical-composition in the thin films of correlated electron materials, including the integration of the correlated electron materials onto Si platform. There are some theoretical mechanisms proposed for Mott memories such as the interfacial Mott transition\textsuperscript{189} and the formation of conductive filament generated by local Mott transition.\textsuperscript{202,204,205} However, a thorough understanding of the mechanism has not been achieved yet. Therefore, the elucidation of detailed mechanism is also a major research challenge.

### 2.3. MEMORY SELECTOR DEVICE

The capacity (or density) is one of the most important parameters for memory systems. In a typical memory system, memory devices (cells) are connected to form an array. A memory cell in an array can be viewed as being composed of two components: the ‘storage node’, which is usually characterized by an element with switchable states, and the ‘selector’, which allows the storage node to be selectively addressed for read and write. Both components impact scaling limits of memory. It should be noted that for several advanced concepts of resistance-based memories, the storage node could in principle be scaled down below 10 nm,\textsuperscript{208} and the memory density is often limited by the selector devices. Thus, the selector device represents a serious bottleneck for emerging memory scaling to 10 nm and beyond.

The most commonly used memory selector devices are transistors (e.g., FET or BJT), as in DRAM, FRAM, etc. Flash memory is an example of a storage node (floating gate) and a selector (transistor) combined in one device. Planar transistors typically have the footprint around (6-8)F$^2$. In order to reach the highest possible 2D memory density of 4F$^2$, a vertical transistor selector needs to be used. However, transistors as selector devices are generally unsuitable for 3D memory architectures. Two-terminal memory selector devices are preferred for scalability and can be used in crossbar memory arrays to achieve 4F$^2$ footprint.\textsuperscript{209,210} The function of selector devices is essentially to minimize leakage through unselected paths (“sneak paths”). Two-terminal selector devices can achieve this through asymmetry (e.g., rectifying diodes) or nonlinearity (e.g., nonlinear devices).\textsuperscript{211} Volatile switches can also be used as selector devices. Figure BC2.2 shows a taxonomy of memory selector devices. In addition to external selector devices, some storage elements may have inherent self-selecting properties (e.g., intrinsic nonlinearity or self-rectification), which may enable functional crossbar arrays without external selectors.

![Figure BC2.2 Taxonomy of Memory Select Devices](image-url)
2.3.1. **VERTICAL TRANSISTORS**

Several examples of experimental demonstrations of vertical transistors used as selectors in memory arrays are presented in Table BC2.2. While a vertical transistor selector allows for the highest planar array density (4F²), it is challenging to integrate a transistor selector into stacked 3D memory. For example, to avoid thermal stress on the memory elements on the existing layers, the processing temperature of the vertical transistor in 3D stacks must be low. Also, making contact to the third terminal (gate) of vertical transistors constitutes an additional integration challenge, which usually results in cells size larger than (4F²)², although true 4F² arrays can, in principle, be implemented with 3-terminal selector devices.²¹³

| Table BC2.2 | Experimental Demonstrations of Vertical Transistors in Memory Arrays |

2.3.2. **DIODE SELECTOR DEVICES**

General requirements for two-terminal selector devices are sufficient ON currents at proper bias to support read and write operations and sufficient ON/OFF ratio to enable selection. The minimum ON current required for fast read operation is ~1 µA (Table BC2.3). The required ON/OFF ratio depends on the size of the memory block, m x n; for example using a standard scheme of array biasing the required ON/OFF ratio should be in the range of 10⁷–10⁸ for m=10³–10⁴, in order to minimize the ‘sneak’ currents.²¹⁴ These specifications are quite challenging, and the experimentally demonstrated selector devices can rarely meet them. Thus, selector devices are becoming a critical challenge of emerging memory. It should be noted that different application targets of resistance-based memories also impact selector device requirements.

| Table BC2.3 | Benchmark Select Device Parameters |

The simplest realization of diode selectors uses semiconductor diodes, such as a pn-junction diode, Schottky diode, or heterojunction diode. Such devices are suitable for a unipolar memory cell. For bipolar memory cells, selectors with bi-directional switching are needed. Proposed examples include Zener diodes,²¹⁵ BARITT diodes,²¹⁶ and reverse breakdown Schottky diodes.²¹⁷

2.3.2.1. **SI DIODE SELECTOR DEVICES**

Both single-crystal Si²¹⁸ and poly-Si²¹⁹,²²⁰,²²¹ diodes have been developed as selector devices for PCM arrays. To provide high ON current, the contact resistivity needs to be reduced to <10⁻⁷ Ω·cm², which was achieved by engineering the metal electrodes and electrode-Si interface.²¹⁹ A short-time annealing technique helps to reduce the OFF current and enlarge the ON/OFF ratio. Poly-Si technology can achieve ON current density of 10² A/cm² (at ~1.8V) and an ON/OFF ratio of 10⁸. It is believed that Si diodes can be scaled beyond 20 nm or 10 nm. Poly-Si diode selector devices have been integrated in PCM crossbar arrays, 3D vertical chain-cell type PCM,²²⁰ and a 1 Gb PCM test chip.²²¹ A major challenge of Si diodes is the high processing temperature (above 1000°C) required to crystallize Si to reduce contact resistivity and OFF current.

2.3.2.2. **OXIDE DIODE SELECTOR DEVICES**

Oxide-based heterojunction²²²,²²³,²²⁴,²²⁵ or Schottky junction²²⁸,²²⁹,²³⁰,²³¹ diodes may be fabricated at lower temperatures and used as selector devices. Oxide-based heterojunction devices, in particular suitable for oxide-based RRAM devices. A p-NiO/n-TiOₓ diode has demonstrated a rectification ratio of 10⁵ at ±3 V and ON current density of 5×10⁴ A/cm² (at ~ 2.5 V).²²² A p-CuO/n-InZnO diode achieved higher ON current density of 10⁴ A/cm² (at ~ 1.3 V) and was integrated with NiOx RRAM in a 2-layer 8×8 crossbar array²²³,²²⁴ and with Au₂O₃ antifuse in a one-time-programmable (OTP) memory.²²⁵ Si substrates can be used as a part of heterojunction diodes as demonstrated in n-ZnO/p-Si²²⁶ and n-Ge-nanowire/p-Si diodes.²²⁷ In TiOₓ-based diodes with Pt electrodes, temperature-dependent current-voltage (I-V) characteristics confirm a Schottky barrier of ~0.55 eV at the TiOₓ/Pt interface.²²⁸ The rectification ratio is ~1.6×10⁴ at ±1 V but ON current density is low (~ 13 A/cm²) due to large size. A Pt/TiOₓ/Ti diode with Pt as the Schottky contact and Ti the ohmic contact achieved higher rectification ratio of 10⁷–10⁸ at ±1 V.²²⁹ Another demonstration of Pt/TiOₓ/Ti or Pt/TiOₓ/Ti Schottky diodes improved ON current density to ~3×10⁴ A/cm² at 2 V on 4 µm² area.²³⁰ Measurement showed that current is not uniform across the diode area, probably due to edge leakage. Therefore, current density is higher at smaller diode size. An Ag/n-ZnO Schottky diode with non-alloyed Ti/Au ohmic contact demonstrated a rectification ratio of 10⁵ and forward current density over 10⁴ A/cm² at 2 V.²³¹ In addition to oxide Schottky diodes, Si Schottky diodes are also utilized as selector devices, e.g., Al/p-Si.²³² The ON current of oxide-based heterojunction diodes is often limited by both contact resistance and density of states of the oxide materials.

---

THE INTERNATIONAL ROADMAP FOR DEVICES AND SYSTEMS: 2021

COPYRIGHT © 2021 IEEE. ALL RIGHTS RESERVED.
2.3.3. **Volatile Switch as Selector Devices**

Volatile resistive switching devices can also be utilized as selector devices. They provide access to a selected memory element in their ON state and block sneak paths in OFF state. The device structure and physics of operation of these devices are sometimes similar to those of the storage nodes. The main difference is that nonvolatility is required for the storage node, while for select devices volatile switching characteristics allow them to be switched quickly between ON and OFF states.

2.3.3.1. **Mott Switch**

This device is based on metal-insulator transition (i.e., Mott transition) and exhibits a low resistance above a critical electric field (threshold voltage, $V_{th}$). It recovers to a high-resistance state if the voltage is below a hold voltage ($V_{hold}$). If the electronic conditions that triggered Mott transition can relax within the memory device operation time scale, the Mott transition device is essentially a volatile resistive switch and can be utilized as a selector device. A VO$_2$-based device has been demonstrated as a selector device for NiO$_x$ RRAM element. However, the feasibility of Mott-transition switches as selector devices still needs further research. It should be noted that VO$_2$ undergoes a phase transition to the metallic state at temperature around 68°C, which restricts its operation temperatures and limits practical applications of a VO$_2$ selector as current specifications require operational temperature of 85°C. Suitable Mott materials with higher transition temperatures need to be investigated. Metal insulator transitions at ~130°C, and electrically driven switching were observed in thin films of SmNiO$_3$.

2.3.3.2. **Threshold Switch**

This type of device is based on the threshold-switching effect observed in thin-film MIM structures caused by electronic charge injection. Significant resistance reduction occurs at $V_{th}$, and this low-resistance state quickly recovers to the original high-resistance state when the applied voltage falls below $V_{hold}$. It was reported that chalcogenide-based threshold switches could be used as access devices in PCM arrays. Niobium oxide is found to possess both memory switching and threshold switching properties at different compositions, based on which hybrid memory (W/bi-layer-NbO$_x$/Pt) was demonstrated in a 1 Kb array. NbO$_x$-based selectors have also been integrated with TiO$_2$/TaO$_x$ based RRAM in crossbar arrays at 5nm node. In Si-As-Te ternary alloy, the composition (controlled by the sputtering power during deposition) determines the emergence of threshold switching. Both $V_{th}$ and $V_{hold}$ vary with composition, which may provide a method to optimize the selector device operation window. Another threshold switch device based on chalcogenide AsTeGeSiN was shown to be scalable to 30 nm with current density exceeding 10MA/cm$^2$ and endurance over 10$^6$ cycles. It was integrated with TaO$_x$-based RRAM devices. An unavoidable finite delay time was found in this selector device due to intrinsic properties of the chalcogenide material, which may limit the selector speed. Another doped-chalcogenide (material undisclosed) based selector demonstrates low $V_{hold}$ (0.2 V), large ON/OFF ratio (>10$^3$), fast speed (<10 ns), long endurance (>10$^9$ cycles) and good thermal stability (180°C). A so-called “FAST” (Field Assisted Superliner Threshold) selector was recently reported, with abrupt switching (<5 mV/dec), high ON/OFF ratio (10$^7$), and long endurance (10$^8$ cycles). Unlike other threshold switch selectors, this device does not exhibit recovery to OFF-state at certain $V_{hold}$, which appears more like a nonlinear selector. A 4Mb 1S1R crossbar RRAM array has been demonstrated based on this selector.

2.3.4. **Nonlinear Selector Devices**

Similar to volatile switches, nonlinear selector devices can be used with bipolar memory elements, which is an advantage over rectifying diode selectors.

2.3.4.1. **Nonlinear Selector Devices**

Nonlinearity in device characteristics can be introduced with non-ohmic transport mechanisms, e.g., tunneling. A Ni/TiO$_2$/Ni nonlinear selector device is integrated with HfO$_2$-RRAM to demonstrate a 1S1R memory structure. Another selector device with Pt/TiO$_2$/TiN structure is combined with a bi-layer Pt/TiO$_2$/$\text{TaO}_x$/W RRAM for a functional memory device. A so-called “varistor” selector device is based on a sandwiched TaO$_x$/TiO$_2$/TaO$_x$ structure. It was found that the substitution of Ti$^{4+}$ by Ta$^{4+}$ ions increases the conductivity of the initially insulating TiO$_2$ layer. The ON-current of nonlinear selector devices can be modulated by oxide thickness and oxidation conditions. Another multi-oxide stack (Ta$_2$O$_5$/TaO$_x$/TiO$_2$) based selector also leverages various interface engineering techniques to obtain high ON-current density (>10$^7$ A/cm$^2$), high nonlinearity ratio (~10$^6$), and low OFF-current (~100 nA). It is integrated with CBRAM in a 1 Kb crossbar array. A back-to-back diode structure, n$/p^n+$ poly-Si, is also suggested as a selector device, where the middle p-layer is fully depleted and a drain induced barrier lowering (DIBL) effect causes exponential current increase with applied voltage.

2.3.4.2. **MIEC Switch**

The device is made from Cu-containing “mixed ionic and electronic conduction” (MIEC) materials sandwiched between an inert top electrode (TE) (e.g., TiN, W) and a bottom electrode (BE). Negative voltage applied on TE pulls Cu$^+$ in MIEC away from the BE and creates vacancies near the BE. The hole and vacancy concentrations depend exponentially on the applied voltage. Symmetrical diode-like I-V characteristics are achieved with two inert electrodes. Large fraction of mobile Cu$^+$ enables high...
current density (> tens of MA/cm²). Endurance above 10^8 cycles has been demonstrated on MIEC devices in small arrays. The MIEC selector devices were also integrated with PCM in a 512 Kb testing array using 180 nm CMOS process. The scalability of MIEC select devices was tested to below 30 nm in diameter and below 12 nm in thickness.

2.3.4.3. **Complementary Resistive Switches**

A complementary resistive switch (CRS) provides a self-selecting memory by connecting two bipolar RRAM devices anti-serially. It may be considered as “constructed nonlinearity”. Both states “0” and “1” have high resistance in CRS, which helps to minimize leakage through sneak paths. In either state, one of the two RRAMs is in LRS and the other in HRS. When reading a “1” state, the HRS device is switched to LRS and both devices end up in LRS. When reading a “0” state, no switching occurs and CRS remains in HRS. Notice that the reading operation is destructive, although non-destructive readout method was also proposed. CRS has been demonstrated in different resistive switching devices, e.g., Cu/ SiO_x/Pt bipolar resistive switches, amorphous carbon-based RRAM, TaO_x-based RRAM, multi-layer TiO_x device, HiO_x RRAM, ZrO_x/HiO_x bi-layer RRAM, Cu/TaO_x atomic switch, Nb_xO_y/NbO_y RRAM, etc.

Table BC2.4a summarizes experimentally demonstrated parameters of some two-terminal select devices, including diodes, volatile switches, and nonlinear devices. Table BC2.4b summarizes the parameters of some reported self-rectifying memories. It should be emphasized that these summary tables can only capture a snapshot of selector device characteristics; however, the functionality of these devices depends on their actual voltage in arrays with random data patterns and the balance between selectors and storage elements. Therefore, these parameter tables should only be used for illustration purpose, not for rigorous benchmark or assessment.

It remains a great challenge for the demonstrated selector devices to meet all the requirements in Tables BC2.4a and BC2.4b. For scaled two-terminal select devices, two fundamental challenges are contact resistance and lateral depletion effects. Very high doping concentration is needed to minimize both effects. However, high doping concentrations result in increased reverse bias currents in classical diode structures and therefore reduced I_on/I_off ratio. For switch-type selector devices the main challenges are identifying the right material and the switching mechanism to achieve the required drive current density, I_on/I_off ratio, and reliability.

**Table BC2.4a**

| Experimentally Demonstrated Two-terminal Memory Select Devices |

**Table BC2.4b**

| Experimentally Demonstrated Self-selecting Memory Devices (self-rectifying) |

2.4. **Storage Class Memory**

2.4.1. **Storage Class Memory Devices**

2.4.1.1. **Traditional Storage: HDD and Flash Solid-state Drives**

Conventionally, magnetic hard-disk drives are used for non-volatile data storage. The cost of HDD storage in $/GB is extremely low and continues to decrease. Although the bandwidth with which contiguous data can be streamed is high, the poor random-access time of HDDs limits the maximum number of I/O requests per second (IOPs). In addition, HDDs have relatively high energy consumption, a large form factor, and are subject to mechanical reliability failures in ways that solid state technologies are not. Despite these issues, the sheer number and growth in HDD shipments per year (380,000 Petabytes in 2012, growing at 32% per year) means that magnetic disk storage is highly unlikely to be “replaced” by solid-state drives at any time in the foreseeable future.

Non-volatile semiconductor memory in the form of NAND Flash has become a widely-used alternative storage technology, offering faster access times, smaller size and lower energy consumption when compared to HDD. However, there are several serious limitations of NAND Flash for storage applications, such as poor endurance (10^3–10^5 erase cycles), only modest retention (typically 10 years on a new device, but only 1 year at the end of rated endurance lifetime), long erase time (~ms), and high operating voltage (~15 V). Another difficult challenge of NAND Flash SSD is posed by its page/block-based architecture. By not allowing for direct overwrite of data, sophisticated procedures for garbage collection, wear-leveling and bulk erase are required. This in turn requires additional computation — which reduces performance and increases cost and power because of the need for a local processor, RAM, and logic — as well as over-provisioning of the SSD which further increases cost per effective user-bit of data.
Although Flash memory technology continues to project for further density scaling, inherent performance characteristics such as read, write and erase latencies have been nearly constant for more than a decade. While the introduction of multi-level cell (MLC) Flash devices extended Flash memory capacities by a small integral factor (2–4), the combination of scaling and MLC have resulted in the degradation of both retention time and endurance, two parameters critical for storage applications. The migration of NAND Flash into the vertical dimension above the silicon has continued this trend of improving bit density (and thus cost-per-bit) while maintaining or in some cases, even slightly degrading the latency, retention, and endurance characteristics of present-day NAND Flash.

This outlook for existing technologies has opened interesting opportunities for prototypical and emerging research memory technologies to enter the non-volatile solid-state-memory space.

2.4.1.2. What is Storage Class Memory?

Storage-class memory (SCM) describes a device category that combines the benefits of solid-state memory, such as high performance and robustness, with the archival capabilities and low cost of conventional hard-disk magnetic storage. Such a device requires a non-volatile memory (NVM) technology that could be manufactured at a very low cost per bit.

A number of suitable NVM candidate technologies have long received research attention, originally under the motivation of readying a “replacement” for NAND Flash, should that prove necessary. Yet the scaling roadmap for NAND Flash has progressed steadily so far, without needing any replacement by such technologies. So long as the established commodity continues to scale successfully, there would seem to be little need to gamble on implementing an unproven replacement technology instead.

However, while these NVM candidate technologies are still relatively unproven compared to Flash, there is a strong opportunity for one or more of them to find success in applications that do not involve simply “replacing” NAND Flash. Storage Class Memory can be thought of as the realization that many of these emerging alternative non-volatile memory technologies can potentially offer significantly more than Flash, in terms of higher endurance, significantly faster performance, and direct-byte access capabilities. In principle, Storage Class Memory could engender two entirely new and distinct levels within the memory and storage hierarchy. These levels would be differentiated from each other by access time, with both levels located within more than two orders of magnitude between the latencies of off-chip DRAM (~80 ns) and NAND Flash (20 µs).

2.4.1.2.1. Storage-type SCM

The first new level, identified as S-type storage-class memory (S-SCM), serves as a high-performance solid-state drive, accessed by the system I/O controller much like an HDD. S-SCM must provide at least the same data retention as Flash, allowing S-SCM modules to be stored offline, while offering new direct overwrite and random-access capabilities (which can lead to improved performance and simpler systems) that NAND Flash devices cannot provide. However, because of the modest (perhaps 10x) advantage in read latency over NAND Flash, it is critical that the eventual cost-per-bit for S-SCM be no worse than 3-10x higher than NAND Flash. While such costs need not be realized immediately at first introduction, it would need to be very clear early on that costs could steadily approach such a level relative to Flash.

Note however that such system cost reduction can come from other sources than the raw cost of the device technology: a slightly-higher-cost NVM technology that enabled a simple, low-cost SSD by eliminating or simplifying costly and/or performance-degrading overhead components would achieve the same overall goal. If the cost per bit could be driven low enough through ultrahigh memory density, ultimately such an S-SCM device could potentially replace magnetic hard-disk drives in enterprise storage server systems as well as in mobile computers (subject to the same issues mentioned above in terms of needing numerous IC fabs to ship the many petabytes of HDD delivered to those markets).

2.4.1.2.2. Memory-type SCM

The second new level within the memory and storage hierarchy, termed M-type storage-class memory (M-SCM), should offer a read/write latency of less than ~200 ns. These specifications would allow it to remain synchronous with a memory system, allowing direct connection from a memory controller and bypassing the inefficiencies of access through the I/O controller. The role of M-SCM would be to augment a small amount of DRAM to provide the same overall system performance as a DRAM-only system, while providing moderate retention, lower power-per-GB and lower cost-per-GB than DRAM. Again, as with S-SCM, the cost target is critical. It would be desirable to have cross-use of the same technology in either embedded applications or as a standalone S-SCM, in order to spread out the development risk of an M-SCM technology. The retention requirements for M-SCM are less stringent, since the role of non-volatility might be primarily to provide full recovery from crashes or short-term power outages, requiring non-volatility over a period of perhaps 7–21 days.

Particularly critical for M-SCM will be device endurance, since the time available for wear-leveling, error-correction, and other similar techniques is limited. The volatile portion of the memory hierarchy will have effectively infinite endurance compared to any of the non-volatile memory candidates that could become an M-SCM. Even if device endurance can be pushed well over 10⁹
cycles, it is quite likely that the role of M-SCM will need to be carefully engineered within a cascaded-cache or other Hybrid Memory approach. That said, M-SCM offers a host of new opportunities to system designers, opening up the possibility of programming with truly persistent data, committing critical transactions to M-SCM rather than to HDD, and performing commit-in-place database operations.

### 2.4.1.3. Target Specifications for SCM

Since the density and cost requirements of SCM transcend the straightforward scaling application of Moore’s Law, additional techniques will be needed to achieve the ultrahigh memory densities and extremely low cost demanded by SCM, such as 1) 3-D integration of multiple layers of memory, currently implemented commercially for write-once solid-state memory, and/or 2) Multiple level cell (MLC) techniques.

Table BC2.5 lists a representative set of target specifications for SCM devices and systems compared with benchmark parameters of existing technologies (HDD and NAND Flash). As described above, SCM applications can be expected to naturally separate based on latency. Although S-class SCM is the slower of these two targeted specifications, read and write latencies should be in the 1–5 usec regime in order to provide sufficient performance advantage over NAND Flash. Similarly, endurance of S-class SCM should offer at least 1 million program-erase cycles, offering a distinct advantage over NAND Flash. In order to support off-line storage, 10-year retention at 85°C should be available.

In order to make overall system power usage (as shown in Table BC2.5) competitive with NAND Flash and HDD, and since faster I/O interfaces can be expected to consume considerable power, the device-level power requirements must be extremely minimal. This is particularly important since low latency is necessary but not sufficient for enabling high bandwidth – high parallelism is also required. This in turn mandates a sufficiently low power per bit access, both in terms of peripheral circuitry and device-level write and read power requirements. Finally, standby power should be made extremely low, offering opportunities for significant system power savings without loss of performance through rapid switching between active and standby states.

In order to achieve the desired cost target of within 3–10x of the cost of NAND Flash, the effective areal density will similarly need to be quite similar to 1X-node planar NAND Flash. This low cost structure would then need to be maintained by subsequent SCM generations, through some combination of further scaling in lateral dimension, by increasing the number of multiple layers, or by increasing the number of bits per cell.

Also shown in Table BC2.5 are the target specifications for M-type SCM devices. Given the faster latency target (which enables coherent access through a memory controller), the program-erase cycle endurance must be higher, so that the overall non-volatile memory system can offer a sufficiently large lifetime before needing replacement or upgrade. Although some studies have shown that a device endurance of $10^7$ cycles is sufficient to enable device lifetimes on the order of 3–10 years, we anticipate that the need for sufficient engineering margin would suggest a minimum cycle endurance of $10^8$ cycles. While such endurance levels support the use of M-class SCM in memory support roles, significantly higher endurance values (e.g., $1e12$ or $1e14$ cycles) would allow M-class SCM to be used in more varied memory applications, where the total number of memory accesses may become very large.

### Table BC2.5 Target Device and System Specifications for SCM

<table>
<thead>
<tr>
<th>Specification</th>
<th>S-Class SCM</th>
<th>M-Class SCM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Latency (usec)</td>
<td>1–5</td>
<td>1–5</td>
</tr>
<tr>
<td>Endurance (10^7 cycles)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Endurance (10^8 cycles)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Power per bit (mW/bit)</td>
<td>0.1</td>
<td>0.1</td>
</tr>
<tr>
<td>Power per access (mW/Access)</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Retention (10 years)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Temperature (85°C)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 2.4.1.4. First SCM Products Reach the Market

In July 2015, Intel and Micron jointly announced a new non-volatile memory technology, called “3D-Xpoint.” This technology is said to offer 1000x lower latency and 1000x higher endurance than NAND Flash, at a density that is 10x higher than DRAM. Note that it is most likely that the latency referred to here is write latency rather than read latency, since NAND write latency is much slower than its read latency. 3D-Xpoint technology, said to have been implemented at the 128Gbit chip level, is based on a two-layer stacked crossbar array, with each intersection point containing a non-volatile memory device and a nonlinear access device. The particular non-volatile memory device was not specified, other than that it depends on bulk changes of resistance, nor was the nonlinear access device described. Speculation based on patent searches and job solicitations suggest that the technology may be a combination of some variant of phase change memory and an Ovonic Threshold Switching access device.
While the details of the devices involved may still be uncertain, the projected array specifications and the target applications are, for all intents and purposes, indistinguishable from those described above for S-type Storage Class Memory. Thus we can consider 3D-Xpoint as the first commercial implementation of the Storage Class Memory concept first described in 2008.267,268 Furthermore, in a later presentation, a second, “Performance-focused” form of 3D-Xpoint memory was described as being under active development.277 Compared to the initial “Cost-focused” form of 3D-Xpoint memory, this variant is said to offer even faster latencies and higher endurance (Figure BC2.3). Thus, this second variant of 3D-Xpoint is somewhat similar to M-type SCM as described above, both in terms of its specifications and in terms of potential applications. The only major difference, as observed in Figure BC2.3, is the strong similarity between the expected volatility of Performance-focused 3D-Xpoint and the known volatility of DRAM. In contrast, one of the benefits of M-type SCM was supposed to be its non-volatility. Ideally, retention of data for perhaps 1-3 weeks would permit successful recovery of server data, even after a power outage due to a natural disaster or other major event.

Figure BC2.3  Comparison of Performance of Different Memory Technologies

2.4.2. STORAGE CLASS MEMORY ARCHITECTURES

2.4.2.1. INTRODUCTION

In traditional computing, SRAM is used as a series of caches, which DRAM tries to refill as fast as possible. The entire system image is stored in a non-volatile medium, traditionally a hard drive, which is then swapped to and from memory as needed. However, this situation has been changing rapidly. Application needs are both scaling in size and evolving in scope, and have rapidly exhausted the capabilities of the traditional memory hierarchy.

By combining the reliability, fast access, and endurance of a solid-state memory together with the low-cost archival capabilities and vast capacity of a magnetic hard disk drive, Storage Class Memory (SCM) offers several interesting opportunities for creating new levels in the memory hierarchies that could help with these problems. SCM offers compact yet robust non-volatile memory systems with greatly improved cost/performance ratios relative to other technologies. S-class SCM represents ultra-fast long-term storage, similar to an SSD but with higher endurance, lower latencies, and byte-addressable access. M-class represents dense and low-power non-volatile memory at speeds close to DRAM.

In order to implement SCM, both the emerging memory technologies discussed in Section 2.4.1 as well as new interfaces and architectures will be needed, in order to fully use the potential and to compensate for the weaknesses of various new memory technologies. In this section, we explore the Emerging Research Architecture implications and challenges associated with Storage Class Memory.

2.4.2.2. CHALLENGES IN MEMORY SYSTEMS

Current memory systems range in size from Gigabytes (low-volume application-specific IC (ASIC) systems, field programmable gate arrays (FPGAs) and mobile systems) through Terabytes (multicore systems that manage execution of many threads for personal or departmental computing), to Petabytes (for database, Big Data, cloud computing, and other data analytics applications), and up to Exabytes (next-generation, exascale scientific computing). In all cases, speed (both in terms of latency of data reads and writes as well as bandwidth), power consumption, and cost are absolutely critical. However, the importance of other system aspects can vary across these different application spaces.
Historically, roughly one-third of the power in a large computer system is consumed in the memory sub-system. Some portion of this is refresh power, required by the volatile nature of DRAM. As a result, modern data servers consume considerable power even when operating at low utilization rates. For example, Google has reported that servers are typically operating at over 50% of their peak power consumption even at very low utilization rates. The requirement for rapid transition to full operation precludes using a hibernate mode. As a result, a persistent memory that did not require constant refresh would be valuable.

Many computer systems are not running at peak load continuously. Such systems (including mobile or data analytics) become much more efficient if power can be turned off rapidly while maintaining persistent stored data, since power usage can then become proportional to the instantaneous computational load. This provides additional incentive for the non-volatile storage aspect of SCM.

Some applications such as data analytics and ASIC systems can benefit from having associative memories or content addressability, while other applications might gain little. Mobile systems can become even more compact if many different memory tiers can be combined on the same chip or package, including non-volatile M-class or even S-class Storage Class Memory.

Total cost of ownership is influenced by cost-to-purchase, cost-to-maintain, and system lifetime. Current cost-to-purchase trends are that hard disk drives (HDD) cost roughly an order of magnitude less per bit than Flash memory, which in turn costs almost an order of magnitude less per bit than DRAM. However, cost-to-purchase is not the only consideration. It is anticipated that S-class SCM will consume considerably less power than HDD (both directly and in terms of required cooling), and will take up considerably less floorspace. One early projection what that by 2020, if the main storage system of a data center is still built solely from HDD, the target performance of 8.4 G-SIO/s could consume as much as 93 MW and require 98,568 square feet of floor space. In contrast, the improved performance of emerging memories could supply this performance with only 4 kW and 12 square feet. Given the cost of energy, this differential can easily shift the total cost advantage to emerging memory, away from HDD, even if a cost per bit differential still exists.

These requirements have led to considerable early investigation into new memory architectures, exploiting emerging memory devices, often in conjunction with DRAM and HDDs in novel architectures. These new Storage Class Memories (SCM) are differentiated as whether they are intended to be close to the CPU (M-class) or to largely supplement the hard-drives and SSDs (S-class).

The emergence of SCM leads to the need to resolve issues beyond the device level, including software organization, wear leveling management, and error management. Because of the inherent speed in SCMs, software can easily limit the system performance. Some of these changes have already been initiated by the advent of SSDs. All types of IO software – from the filesystem, through the operating system and up to applications – had to be redesigned in order to best leverage both SSDs and then SCMs. The number of software interactions was reduced, and disk-centric features were removed. Inefficiencies buried deep within conventional software were accounting for anywhere from 70% to 94% of the total IO latency. It is likely to be valuable to give application software direct access to the SCM interface, although this can then require additional considerations to protect the SCM device from malicious software. This direct access has not occurred for SSDs, with manufacturers applying numerous undocumented operations between the input data and the raw storage. (One example is the inversion of entire data blocks, based on the number of 0s or 1s to be stored.) However, this approach is not typically used in current operating systems that use some form of File Address Table as an intermediate index mechanism.

Access patterns in data-intensive computing can vary substantially. While some companies continue to use relational databases, others have switched to flat databases that must be separately indexed to create connections amongst entries. In general, database accesses tend to be fairly atomic (as small as a few bytes) and can be widely distributed across the entire database. This is true for both reads and writes, and since the relative ratio of reads and writes varies widely by application, the optimality of any one design can depend strongly on the particular workload.

A specific issue that arises with SCMs is wear leveling. While DRAMs and HDDs can support a large number of writes to the same location without failure, most of the emerging non-volatile memory device technologies cannot. Thus, there is a need for low-overhead mechanisms to “spread” the writes around uniformly, generally referred to as “wear leveling”. An important issue in any file system is that certain data (such as metadata) is written to quite frequently. It is important to make sure that such storage locations are not subject to fast wear out, e.g., by using a more robust technology for such portions of the file system.

Error management is a broader problem than just wear leveling. While DRAM has traditionally benefited from simple methods such as error correction code (ECC) and error detection codes (EDCs), Flash with its large page sizes and slow accesses can afford more sophisticated algorithms such as low-density parity-check (LDPC). Unfortunately, SCM will need more error correction than DRAM but will need faster error correction than Flash, especially for M-class SCMs. This is an open area for research. Some possible options include exploring codes that exploit specifics of error patterns, such as Tensor codes, and the use of...
of in-situ scrub,\textsuperscript{282} where accumulated errors are periodically eliminated so that one or two-bit error correction can remain sufficient.

### 2.4.2.3. Emerging Memory Architectures for M-Class SCM

Storage Class Memory architectures that are intended to replace, merge with, or support DRAM, and be close to the CPU, are referred to as M-type or Memory-type SCM (M-SCM). The required properties of this memory have many similarities to DRAM, including its interfaces, architecture, endurance, and read and write speed. Since write endurance of an emerging research memory is likely to be inferior to DRAM, considerable scope exists for architectural innovation. It will be necessary to choose how to integrate multiple memory technologies to optimize performance and power while maximizing lifetime. In addition, advanced load leveling that preserves the word level interface and suitable error correction will be needed.

The interface is likely to be a word-addressable bus, treating the entire memory system as one flat address space. Since the cost of adapting to new memory interfaces is sizeable, an interface standard that could support multiple generations of M-SCM devices would be highly preferred. Many systems (such as in automobiles) might be deployed for a long time, so any new standard should be backward-compatible. Such a standard should be compatible to DRAM interfaces (though with simpler control commands) and should reuse existing controllers and PHY (physical layers), as well as power supplies, as much as possible. It should be power efficient, e.g., supporting small page sizes, and should support future directions, such as 3D Master/slave configurations. The M-SCM device should indicate when writes have been completed successfully. Finally, an M-SCM standard should support multiple data rates, such as a DDR-like speed for the DRAM and a slower rate for the NVRam.\textsuperscript{283}

While wear-leveling in a block-based architecture requires significant overhead to track the number of writes to each block, simple techniques such as “Start-Gap” Wear-Leveling are available for direct-byte-access memories such as PCM (Phase Change Memory).\textsuperscript{284} In this technique, a pair of registers are used to identify the location of the start point and an empty gap within a region of memory. After some threshold number of write accesses, the gap register is moved through the region, with the start register incrementing each time the gap register passes through the entire region. Additional considerations can be added to defend against detrimental attacks intended to intentionally wear out the memory.

With such techniques, even an M-class SCM that is markedly slower than DRAM can offer improved performance by increasing available capacity and by reducing the occurrence of costly cache misses.\textsuperscript{285} With proper caching, a carefully-designed M-SCM system could potentially even match DRAM performance despite its lower device latency.\textsuperscript{286} The presence of a small DRAM cache helps keep the slower speed of the M-class SCM from affecting overall system performance in many common workloads. Even with an endurance of $10^7$ cycles, the system lifetime has been shown to be on the order of 3 years. Techniques for reducing the write traffic back to the SCM device can help improve this by as much as a factor of 3 under realistic workloads.

Direct replacement of DRAM with a slightly slower M-class SCM has also been considered, for the particular example of STT-MRAM.\textsuperscript{287} Since individual byte-level writes to STT-MRAM consume more power than in DRAM, a direct replacement is not competitive in terms of energy or performance. However, by re-architecting the interaction between the output buffer and the STT-MRAM, unnecessary writes back to the NVM can be eliminated, producing a sizeable energy improvement at almost no loss in performance. However, the use of write buffers means that the device must be able to complete all writes back to non-volatile memory in the event of power loss. Integrating PCM into the mobile environment, together with a redesigned memory management controller, is predicted to deliver a six times improvement in speed and also extends the memory lifetime six times.\textsuperscript{288}

Caches are intended to ensure that frequently-needed data is located near to the processor, in nearby, low-latency memory. In storage architectures, “hot” or frequently-accessed data is identified and then moved to faster tiers of storage. However, as the number of tiers or caches increases, a significant amount of time and energy is being spent moving data. An alternative approach is to completely rethink the hardware/software interface. By organizing the computational system around the data, data is not brought to the processor but instead processing is performed in proximity to the stored data. One such emerging data-centric chip architectures termed “Nanostores”\textsuperscript{289} was predicted to offer 10–60x improvements in energy efficiency.\textsuperscript{290}

Given the slower than expected deployment of scaled emerging devices for M-class SCM, several projects have employed large amounts of DRAM as a surrogate for and M-class SCM. Though Bresniker et.al. describe a computer enabled by a large non-volatile “Universal memory,”\textsuperscript{291} press reports indicate that early commercial machines will be built with large amounts of DRAM. They point out that an NVMM version allows “occasionally-on computing” but could have the downside that new types of bugs might appear as OSs and programs effectively run indefinitely and cannot “re-create their memory state representations each time they start”. New applications and algorithms might emerge as a result of keeping data in perpetuity, or at least for long periods of time.

### 2.4.2.4. Emerging Memory Architectures for S-Class SCM

S (Storage) type SCMs are intended to replace or supplement hard-disk drives as main storage, much like current Flash-based SSDs, but with even more IOPs (I/O operations per second). Their main advantage will be speed, avoiding the seek time penalty...
of main drives. However, to succeed, their total cost of ownership needs to approach that of HDDs. Research issues include whether the SCM serves as a disk cache or is directly managed, how load leveling is implemented while retaining a sufficiently fast and flexible interface, how error correction is implemented, and identifying the optimal mix of fast-yet-expensive and slow-yet-inexpensive storage technologies. The effective performance of Flash SSD, itself slower than S-SCM, has been strongly affected by interface performance. For instance, the SATA (Serial Advanced Technology Attachment) interface was originally designed for HDD, and was commonly used for early SSD devices despite not being optimized for Flash SSD.292

One possible introduction of these new memory devices to the market would be as hybrid solid-state discs, where the new memory technology complements the traditional Flash memory to boost the SSD performance. Experimental implementations of FeRAM/Flash293 and PCRAM/Flash294 have been explored. It was shown that the PCRAM/Flash hybrid improves SSD operations by decreasing the energy consumption and increasing the lifetime of Flash memory.

Additional open questions for S-SCM include storage management, interface, and architectural integration, such as whether such a system should be treated like a fast disk drive or as a managed extension of main memory. To date, disk-like systems built using non-volatile memories have had disk-like interfaces, with fixed-sized blocks and a translation layer used to obtain block addresses. However, since the file system also performs a table lookup, some portion of SCM performance is sacrificed. In addition, non-NAND-Flash SCMs have randomly accessible bits and do not need to be organized as fixed-size blocks.295

While preserving this two-table structure means that no changes to the operating system are required to use or to switch between new S-SCM technologies, the full advantages of such fast storage devices cannot be realized. There are two alternative approaches to eliminate one of these lookup tables. In the Direct Access mode, the translation table is removed, so that the operating system must then understand how to address the SCM devices. However, any change in how table entries are calculated (such as improvements in garbage collection or wearleveling) would then require changes in the operating system.

In contrast, in an Object-Based access model, the file system is organized as a series of (key, value) objects. While this requires a one-time change to operating systems, all specific details of the SCM could be implemented at a low level. This model leads to greater efficiency in terms of both speed and effective “file” density and also offers the potential for enhanced reliability.

Another issue for SCM-based systems will be addressing the asymmetry between read and write in devices such as PCM or other emerging non-volatile memories.296 Such asymmetry can affect the ordering and atomicity of writes and needs to be considered in system or algorithm design.297 Atomicity is critical for operations such as database transactions properties, so that either all of a series of related database operations occur, or none of them occur.

Longer write latencies, in technologies such as PCM, can be compensated by techniques such as data comparison writes,298 partial writes,299 or specialized algorithms/structures that trade writes for reads.300,301 (These last set of techniques can also help reduce endurance problems.) Write ordering and atomicity problems can be finessed by hardware primitives. These can either be existing hardware primitives – cache modes (e.g., write-back, write-combining), memory barriers, cache line flush,302,303,304 – or newly-proposed hardware primitives, such as atomic 8-byte writes and epoch barriers.305,306

Even first-generation PCM chips, although implemented without a DRAM cache, compare favorably with state-of-the-art SSDs implemented with NAND Flash, particularly for small (<2 KB) writes and for reads of all sizes.307 The CPU overhead per input-output operation is also greatly reduced. Another observation for even first-generation PCM chips is that while the average read latency is similar to NAND Flash, the worst-case latency outliers for NAND Flash can be many orders of magnitude slower than the worst-case PCM access. This is particularly important considering that such S-class SCM systems will typically be used to increase system performance by improving the delivery of urgently-needed “hot” data.

Another new software consideration for both S- and M-class SCM is the increased importance of avoiding memory corruption, either through memory leaks, pointer errors, or other issues related to memory allocation and deallocation.308 Since part of the memory system is now non-volatile, such issues are now pervasive and may be difficult to detect and remove without affecting stored user data.

General libraries and programming interfaces – such as NV-heaps,309 Mnemosyne,310 NVMalloc,311 and recovery and durable structures312 – have been proposed to expose SCM as a persistent heap and thus ease its adoption. Schemes for filesystem support have been developed to transparently utilize as byte-addressable persistent storage, including Intel’s PMFS,313 BPFS, FRASH,314 ConquestFS,315 and SCMFS.316

Table BC2.7 Likely Desirable Properties of M (Memory) Type and S (Storage) Type Storage Class Memories
3. **Emerging Logic and Alternative Information Processing Devices**

3.1. **Taxonomy**

One of the central objectives of this chapter is to review recent research in devices beyond silicon transistors and to forecast the development of novel logic switches that might replace the silicon transistor as the device driving technological development within the semiconductor industry. Such a replacement is thought to be potentially viable if one or more of the following capabilities is afforded by a novel device: 1) an increase in device density (and corresponding decrease in cost) beyond that achievable by ultimately scaled CMOS; 2) an increase beyond CMOS in switching speed, e.g., through improvements in the normalized drive current or reduction in switched capacitance; 3) a reduction beyond CMOS in switching energy, associated with a reduction in overall circuit energy consumption; or 4) the enabling of novel information processing functions that cannot be performed as efficiently using conventional CMOS.

An expanded focus on systems requires also that one evaluate the applicability of these novel devices for new types of systems and architectures, above and beyond the hierarchical influence of devices via small core circuits or functional building blocks. Historically, this evaluation has been conducted in this section in terms of possible applications for alternative information processing devices (i.e., those very unlike CMOS transistors). Beginning with the 2017 Edition of the IRDS, the focus pivoted further toward architectures and applications that depart significantly from the device→circuit→logic gate→functional block→system paradigm.

The organization of this section is intended to reflect a progression of options that might enable an orderly transition from CMOS to devices that depart increasingly from CMOS in terms of structure, materials, or operation. That organization is depicted in Figure BC3.1.

![Figure BC3.1](image-url)

**Figure BC3.1**  Taxonomy of Options for Emerging Logic Devices

*Note: The devices examined in this chapter are differentiated according to 1) whether the structure and/or materials are conventional or novel, and 2) whether the information carrier is electron charge or some non-charge entity. Since a conventional FET structure and material imply a charge-based device, this classification results in a three-part taxonomy.*

<table>
<thead>
<tr>
<th>Table BC3.1a</th>
<th>MOSFETS: Extending MOSFETs to End of Roadmap</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table BC3.1b</td>
<td>Charge-based Beyond CMOS: Non-conventional FETs and Other Charge-based Information Carrier Devices</td>
</tr>
</tbody>
</table>
3.2. DEVICES FOR CMOS EXTENSION

3.2.1. CARBON NANOTUBE FETs

For many researchers, the search for an ideal semiconductor to be used in FETs succeeded when single-walled carbon nanotubes (CNTs) were first shown to yield promising devices over twenty years ago. Owing to their naturally ultrathin body (~1 nm diameter cylinders of hexagonally bonded carbon atoms), superb electron and hole transport properties, and reasonable energy gap of ~0.6 – 0.8 eV, CNTs offer solutions in most of the areas that other semiconductors fundamentally fail when scaled to the sub-10 nm dimensional scale. CNT FETs operate as Schottky barrier transistors with nearly transparent barriers to carrier injection achieved for both n- and p-type transport. They are intrinsic semiconductors and cannot be doped in the traditional sense; hence, no inversion layers of charge form to allow current flow. Rather, the gate field lowers the energy barrier in the CNT channel to allow for carriers to be injected from the metal contacts. The most prominent advantages of CNT FETs over other options for aggressively scaled devices are the room temperature ballistic transport of charge carriers, the reasonable energy gap, the demonstrated potential to yield high performance at low operating voltage, and scalability to sub-10 nm dimensions with minimal short channel effects.

In the past several years, significant advances have been made in understanding and enhancing device performance in CNT FETs. These include (1) realizing end-bonded contacts having an effective contact length of 0 nm with reasonable performance, (2) detailing the impact of contact scalability in CNT FETs, (3) maintaining performance as the channel length is scaled down to 9 nm without observing short channel effects, (4) fabricating complementary gate-all-around FETs, (5) fabricating an FET with an intrinsic fT of 153 GHz, (6) fabricating CMOS inverter and pass-transistor logic operating at 0.4 V with a non-doped CNT, (7) fabricating a carbon nanotube computer composed of 178 FETs, (8) progress towards reducing the variability in CNT FETs, (9) understanding origins of hysteresis, and (10) fabricating CNT FETs with ON-current of 0.5 mA/µm.

In addition to improvements at the device level, continuous progress has been achieved toward overcoming the dominant material challenges, including the need to achieve purified and sorted semiconducting CNTs with a relatively uniform diameter distribution and then position the CNTs into aligned, closely packed arrays with consistent pitch. With a target purity of 99.9999% semiconducting CNTs and placement density of >125 CNTs/µm (<8 nm pitch), much work still remains. However, it is important to note that progress continues to be steady and without fundamental obstacles barring these goals from being realized. There remains a need for further research toward improving other device-level aspects, including further reduction of contact effects at small contact lengths, demonstrated reduction in variability, improved control of gate dielectric interfaces and properties, and the experimental study of devices and circuits fabricated using the most scaled and relevant device structures and materials. In short, much work remains for CNT FETs, but they have some of the most substantial (and already demonstrated) potential in high-performance, low-voltage, sub-10 nm scaled transistor applications.

3.2.2. NANOWIRE AND NANOSHEET FETs

Nanowire field-effect transistors are structures in which the conventional planar MOSFET channel is replaced with a semiconducting nanowire. Such nanowires have been demonstrated with diameters as small as 0.5 nm. They may be composed of a wide variety of materials, including silicon, germanium, various III-V compound semiconductors (III-As, III-Sb, III-P, and III-N), II-VI materials (CdSe, ZnSe, CdS, ZnS), as well as semiconducting oxides (In2O3, ZnO, TiO2), etc. Importantly, at low diameters, these nanowires exhibit quantum confinement behavior, i.e., 1-D ballistic conduction, and match well with the gate-all-around structure that permits the reduction of short channel effects and other limitations to the scaling of planar MOSFETs.

Important progress has been made in the fabrication of semiconducting nanowires for use as FET channels, for which there are two principal formation methods. The first method is top-down, by which semiconducting channels are formed through lithography and etch. The second approach is bottom-up growth including catalyzed vapor-liquid-solid (VLS) growth and template-assisted selective epitaxy (TASE). These mechanisms have been used to realize a variety of nanowire geometries, including core-shell and core-multishell heterostructures. Top-down methods have entered the near-future roadmaps for major commercial entities, including examples such as the Samsung Multi-Bridge Channel FET (MBCFET) and the TSMC N2 gate-all-around (GAA) FET. Bottom-up methods continue to be charted within the Beyond CMOS portion of this roadmap, given the significant existing challenges to large-scale fabrication combined with potential advantages in heterogeneous integration and convenience for in situ passivation through heterostructures. Nanowire gate-all-around geometry is of interest primarily due to its superb gate electrostatics that can allow further gate-length scaling.

Vertical nanowire transistors have been fabricated in this manner using Si, InAs, and ZnO. Core-shell gate-all-around configurations display excellent gate control and few short channel effects. Circuit and system functionality of nanowire devices
has been demonstrated, including vertical InAs MOSFETs with 103 GHz switching speed, a down-conversion mixer based on vertical InAs transistors that showed cut-off frequency of 2 GHz, and extended, programmable arrays (“tiles”) of non-volatile nanowire-based Flash memory that are used to build circuits such as full-adder, full-subtractor, multiplexer, demultiplexer, clocked D-latch and finite state machines. Planar VLS III-As nanowires perfectly aligned in-plane have enabled multigate HEMTs to enhance high frequency performance. Despite the promising results that are mostly obtained from academic research labs, bottom-up nanowire transistors still face significant challenges before commercialization is feasible. There is an urgent need to improve device yield and uniformity, as well as position registry if the nanowires are to be transferred to a different substrate. On the other hand, the potential of bottom-up nanowire transistors for monolithic core-shell architecture and the inherently relaxed lattice matching requirements for heterogeneous integration have not been completely exploited for low power and high speed applications. For top-down fabricated nanowires, with the demonstration of standalone transistors, CMOS integration, and a functional ring oscillator, vertically stacked planar Si nanowires hold enormous potential to succeed FinFETs in sub-5 nm technology nodes.

3.2.3. 2D Material Channel FETs

Two-dimensional (2D) materials transition metal dichalcogenides (TMDCs), including graphene, are promising candidates for future channel materials in LSIs. Since they are layered materials, they can be as thin as one-layer (one-atom) thick without degrading their properties, which cannot be realized with conventional three-dimensional materials. Electrostatic control of such a thin channel is easier than a conventional bulk channel, suppressing “short channel effects” often encountered by scaled transistors. Carrier mobility of such 2D materials can be very high. Furthermore, novel devices based on principles different from that of CMOS can be realized using 2D materials, as discussed later.

Graphene has especially attracted attention as a channel material due to its extremely high mobility since the year of 2004, when a report on monolayer graphene prepared by exfoliation of graphite crystals was published. The report showed that the field-effect mobility of graphene on SiO₂ was as high as ~10,000 cm²/Vs. It was then predicted that the room-temperature mobility of graphene on SiO₂ would be limited to ~40,000 cm²/Vs due to scattering by surface phonons of the SiO₂ substrate. In fact, much higher field effect mobility was obtained using suspended graphene. Values as high as 120,000 cm²/Vs and 1,000,000 cm²/Vs at 240 K and liquid-helium temperature were obtained. Recently, hexagonal boron nitride (hBN), an inert and flat material, has been used as a substrate for graphene-channel transistors, and it has been shown that the field effect mobility of such devices can exceed 100,000 cm²/Vs at room temperature near the charge neutrality point. Furthermore, a device in which graphene was sandwiched between two hBN flakes and edge-contacted with two metal electrodes exhibited mobility even higher than the above. The results indicate that hBN can be an excellent passivation film for graphene devices.

Graphene can also be obtained on SiC surface by annealing a SiC crystal at high temperatures (often called “epitaxial graphene”). The annealing temperatures range from 1200°C to 2000°C depending on the annealing environment. Chemical vapor deposition of graphene on metal foil or film has also been demonstrated. Typical growth temperatures are around 1000°C. It has been shown that monolayer graphene is preferentially formed on Cu foil or film, while multi-layer graphene can be formed on Ni, Co, and Fe catalysts. The quality of epitaxial graphene and CVD graphene is now as good as that of exfoliated graphene.

Efforts have been made to fabricate graphene-channel transistors, where fabrication processes such as doping and contacting to graphene channels have been developed. However, since graphene does not have a bandgap, such transistors cannot have an ON/OFF ratio high enough for digital applications. Several approaches have been proposed to open a bandgap of graphene. One of the two major approaches is to apply an electric field perpendicular to AB-stacked bilayer graphene. Experimentally, a transport gap of 130 meV was obtained at an electrical displacement of 2.2 V/nm, providing an ON/OFF ratio high enough for digital applications. In fact, it has been pointed out that a small stacking fault of AB-stacked bilayer graphene can increase the off current, which is a serious problem.

A promising approach to form a bandgap in graphene is to make it narrow, that is, to form a graphene nanoribbon (GNR). In fact, simulations using a first-principles many-electron Green’s function approach within the GW approximation have predicted that bandgaps can be as large as ~5 eV depending on their widths for armchair-edged GNRs (AGNRs). Formation of GNRs was first attempted by using electron beam lithography and etching. Carrier transport through such a GNR was also investigated. An energy gap of ~200 meV was obtained for a GNR with a width of 15 nm. Devices with multiple GNRs with a sub-10 nm half-pitch were fabricated using patterning with directed self-assembly of block copolymers. The transport characteristics of such top-down GNRs were poor, however. This is mainly because the edges of such GNRs were not well controlled, probably with a lot of defects. Recently, however, attempts to form GNRs with controlled edges have been made using bottom-up approaches. In fact, Cai et al. demonstrated the growth of armchair-edged GNRs (AGNRs) from 10,10’-dibromo-9,9’-bianthryl precursors. In their approach, precursor molecules are deposited onto a
clean Au(111) surface by vacuum evaporation in ultra-high vacuum. The substrate is then heated to 200°C to remove Br from the precursors and to connect them with each other at the Br-removed points, forming polymers. By further heating the substrate to 400°C, the polymers were cyclodehydrogenated to form AGNRs with a uniform width. The AGNR formed is referred to as 7 AGNR, because it has seven dimer lines in the width direction. The band gap of 7 AGNR is 3.7–3.8 eV according to the simulations above and agrees with an experimentally obtained bandgap (~2.3 eV) considering image-charge corrections by Au substrate. Now several types of GNRs have been formed using similar approaches with different precursors. As for AGNRs with a smaller bandgap, 9AGRs with a theoretical bandgap of about 2.2–2.3 eV have been obtained. Formation of 13 AGNRs with a theoretical bandgap of about 2.3–2.5 eV was also demonstrated although the GNRs were rather short, typically less than 10 nm in this case. The successful formation of atomically precise AGNRs paves a way for their application to transistor channels.

Performance of GNR-channel transistors have been predicted by numerical simulations. It was shown that a transistor with multiple-GNR channels (width: 1.47 nm, pitch: 3.47 nm) with a channel length of 15 nm exhibited an on-current exceeding 1 mA/μm with ON/OFF ratio larger than 10^5 and a subthreshold swing of 64 mV at a drain voltage of 0.1 V. Transistors using 7 AGNRs as channels were fabricated and evaluated experimentally. The performance of transistors was, however, poor with a very low on-current and an ON/OFF ratio of 3.6 x 10^3 at a drain voltage of 1 V. The small on-current was attributed to large Schottky barriers at the source and drain contacts caused by the large bandgap of 7 AGNR. Use of 9 AGNRs and 13 AGNRs with smaller bandgaps improved the transistor performance. In fact, transistors using 9 GNRs as channel exhibited ON/OFF ratios as high as 105 and on-current of 1 μA at a drain voltage of 1V, although the number of GNRs in each transistor is unclear. The performance is not yet as good as a counterpart using carbon nanotubes (CNTs) but expected to improve further by, for example, covering GNRs with hBN and realizing better contacts between GNRs and source/drain electrodes.

New principle devices using GNRs have also been proposed. One is a tunneling field-effect transistor (TFET). A higher on-current than that of Si TFET has been predicted. Use of strained graphene as a channel can also realize tunneling-like transport, according to simulations. A Klein-tunneling-based device has also been proposed. Graphene can offer possibilities for employing novel switching mechanism for future electronics.

Transition metal dichalcogenides (TMDCs) are another 2D material attracting attention. TMDCs have the chemical formula of MX_2, where M is a transition metal element and X is a chalcogen. They can be metallic, half-metallic, semiconducting, or superconducting depending on their compositions. Molybdenum disulfide, MoS_2, is probably the most popular semiconducting TMDC, whose single layer was isolated for electrical measurements in 2005. Electrical properties of semiconducting TMDCs depend on the number of layers due to quantum confinement effects and changes in symmetry. For example, single-layer MoS_2 has a direct band gap of 1.9 eV, while bulk MoS_2 has an indirect bandgap of 1.2 eV. The bandgaps also vary with the compositions. For example, first principles calculations performed using the Heyd-Scuseria-Ernzerhof (HSE06) hybrid functional show that MoS_2, MoSe_2, MoTe_2, WS_2, WSe_2, and WTe_2 have bandgaps of 2.02 eV, 1.72 eV, 1.28 eV, 1.98 eV, 1.63 eV, and 1.03 eV, respectively.

Transistors with TMDCs as a channel material have been demonstrated. Kis et al. fabricated a top-gate MoS_2-channel transistor, demonstrating a large ON/OFF ratio (~10^5) and good subthreshold swing (74 mV/decade). Exfoliated single-layer MoS_2 was used in this experiment. However, field-effect mobility was relatively low (60–70 cm^2/Vs). In fact, transport in single-layer TMDC is severely affected by the environment, often degrading its electrical property. It has been demonstrated that mobility of TMDC increases with thickness. This is because the influence of charged impurities in substrate decreases as the thickness increases. As for MoS_2, field-effect mobility as high as 480 cm^2/Vs was obtained for a 47-nm thick MoS_2 channel. MoS_2 is naturally electron-doped, which is possibly caused by chalcogen vacancies, while WSe_2 is hole-doped. It is actually still difficult to control doping level of TMDCs, which is a major challenge to realize TMDC-based electronics. Incidentally, Desai et al. fabricated MoS_2-channel transistor with 1-nm gate lengths by using a CNT as a gate. The ON/OFF ratio and subthreshold swing were ~10^6 and 65 mV/decade, respectively. This is probably the shortest channel transistor ever made.

New principles devices using TMDCs have also been demonstrated. Sarkar et al. fabricated a tunneling FET (TFET) by placing n-type MoS_2 on top of p-type Ge, forming a p-n junction. The TFET was gated by using a solid polymer electrolyte. The subthreshold swing had an average of 31.1 mV/decade for four decades of drain current at room temperature. Britnell et al. prepared stacking structures consisting of graphene/MoS_2/graphene and graphene/hBN/graphene, demonstrating a switching device based on tunneling phenomena. Although the tunneling devices introduced here can offer steep-slope switching properties, on-current is relatively low, which is an important issue to address for real-world applications. Fabrication of a lateral heterojunction of TMDCs, such as MoSe_2 and WSe_2, have also been demonstrated and a p-n junction by such a heterojunction has been made. Valleytronics based on carriers located in two inequivalent valleys in the wave number space also attract attention. New principles devices using TMDCs, as introduced here, may have good opportunities in future electronics.
Growth technology of TMDCs is also in progress. In fact, the synthesis of TMDC film dates back to the 1980’s, when the growth was performed with van der Waals epitaxy. More recently, Lee et al. demonstrated CVD growth of MoS$_2$ using MoO$_3$ and S powder as precursors. The growth temperature was 650°C. Single-crystal monolayer MoS$_2$ flakes were successfully obtained. This method was further improved and single-crystal MoS$_2$ flakes as large as 120 μm in lateral size were obtained. However, uniform growth over a large area is not easy using this powder-based CVD technique. In 2015, Kang et al. succeeded in large area growth of MoS$_2$ by MOCVD using Mo(CO)$_6$ and (C$_2$H$_5$)$_3$S as precursors. The electron mobility of MoS$_2$ in this case was 30 cm$^2$/Vs at room temperature. In general, mobility of CVD MoS$_2$ is lower than that of exfoliated MoS$_2$, which is still an important issue to address. Furthermore, MoS$_2$ deposition by using sputtering is also in progress. The sputtering method is scalable, but it is still difficult to obtain film with a quality as high as that by MOCVD.

3.2.4. Tunnel FETs

Tunnel Field Effect Transistors (TFETs) have the potential to achieve a low operating voltage by overcoming the thermally limited subthreshold swing voltage of 60 mV/decade by utilizing tunneling as a switching mechanism. In its simplest form, a TFET is a gated, reverse-biased p-i-n diode with a gate controlled intrinsic channel. There are two mechanisms that can be used to achieve a low voltage turn on. The gate voltage can be used to modulate the thickness of the tunneling barrier at the source channel junction and thus modulate the tunneling probability. The thickness of the tunneling barrier is controlled by changing the electric field in the tunneling junction. Alternatively, it is possible to use energy filtering or density of states switching; if the conduction and valence band do not overlap at the tunneling junction, no current can flow; once they do overlap, current can flow. Simulations have predicted arbitrarily steep subthreshold swings when relying on density of states switching as the current is abruptly cutoff when the conduction band and valence band no longer overlap. If phonons or short channel lengths are accounted for, simulated subthreshold swings on the order of 20–30 mV/decade are typical. It is possible to use the tunneling switching mechanisms in series with the standard MOSFET thermal switching mechanism to get an overall subthreshold swing that is steeper than 60 mV/decade when no individual mechanism is steeper than 60 mV/decade. The best experimental results to date have relied on a combination of thermal switching and density of states switching. So far, the experimental results are far worse than simulated device characteristics. The review by Lu and Seabaugh shows a comprehensive benchmarking of published experimental results prior to 2014. The benchmarking shows two problems with TFETs as a MOSFET replacement: 1) Devices are unable to achieve SS <60 mV/decade over a large range or at useful current levels and 2) The on-state current is too low for reasonable performance.

The review shows 14 reports of subthreshold swings below 60 mV/decade, and a few additional results have been published since. Most of the results are for group-IV materials such as Si, strained SiGe, Si/Ge, and strained Ge. Nanowire III-V TFETs have shown even steeper swings. An InP/GaAs heterojunction has shown 30 mV/decade at 1 pA/μm. The steepest result ever reported is in a Si/InAs heterojunction of approximately 20 mV/decade at 0.1 pA/μm. However, there are only a few data points defining this result. Even for low power applications, at least 1–10 μA/μm is needed. Recently, a promising InAs/GaAsSb/GaSb nanowire heterostructure TFET with a 48 mV/decade SS at 67 nA/μm and an I$_{off}$ (current at 60 mV/decade) of 0.31 μA/μm was demonstrated.

Researchers attempting to achieve higher on-current TFETs have traditionally relied on reducing the effective mass by using III-V’s and reducing effective bandgap by using a heterostructure. While this has increased the current, the subthreshold swings and off currents have gotten worse. The increase in off-state current and subthreshold swing needs to be decoupled from the increase in on-state current. Unfortunately, this is a fundamental tradeoff when modulating the thickness of the tunneling barrier: barrier thickness modulation only gives a step subthreshold swing at low current densities.

An ideal density of states (DOS) switch would switch abruptly from zero-conductance to the desired on-conductance thus displaying zero subthreshold swing voltage. Practically, the band edges are not perfectly sharp, so there is a finite density of states extending into the band gap. Optimal measurements of intrinsic GaAs imply a band edge steepness of 17 meV/decade. However, the electrically measured joint DOS in diodes has generally indicated a steepness >90 meV/decade. This broadening is likely due to the spatial inhomogeneity and on heavy doping that appears in real devices. Effectively, there are many distinct channel thresholds in a macroscopic device, leading to threshold broadening. Fortunately, it has been experimentally demonstrated that a band edge worse than 60 mV/decade can be combined with a thermal switching mechanism to give an overall subthreshold swing better than 60 mV/decade.

TFETs are reverse-biased diodes hence are subject to generation in the depletion region. These generation events include but are not limited to bulk and interface trap-assisted Shockley-Read-Hall (SRH) and spontaneous and Auger generation. Calculations based upon these mechanisms show that these significantly degrade the subthreshold swing and increase the leakage currents but do not prevent TFETs from achieving sub-60 mV/decade subthreshold swing. Material defects and gate interface traps make these effects worse and result in worse band edges.
To overcome these challenges, better material perfection than ever before is needed. Every defect or dangling bond can create a trap that ruins the band edge or creates a parallel conduction path. The defects due to doping can be eliminated by electrostatically inducing carriers. Proof of concept devices can be made by making the device a few nanometers large so that there is a low probability of having a trap within the device. 2D transition metal dichalcogenides (TMD) heterostructures potentially have better electrostatic control and lower defects as there are ideally no dangling bonds at the semiconductor oxide interface.

3.3. BEYOND-CMOS DEVICES: CHARGE-BASED

3.3.1. SPIN FET AND SPIN MOSFET TRANSISTORS

Spin-transistors are classified as “non-conventional charge-based extended CMOS devices,” and can be further divided into two categories: the spin-FETs proposed by Datta and Das and spin-MOSFETs proposed by Sugahara and Tanaka. The structures of both types of spin transistors consist of a ferromagnetic source and a ferromagnetic drain which act as a spin injector and a detector, respectively. Although the devices have similar structures, they have quite different operating principles. In spin-MOSFETs, the gate has the same current switching function as in ordinary transistors, whereas in the spin-FETs, the gate acts to control the spin direction via the Rashba spin-orbit interaction. Both types of devices behave as a transistor and function as a magnetoresistive device. The important features of spin transistors are that they allow a variable current to be controlled by the magnetization configuration of the ferromagnetic electrodes (spin-MOSFETs) or the spin direction of the carriers (spin-FETs), and they offer the capability for non-volatile information storage using the magnetization configurations. These features are very useful for energy-efficient, low-power circuit architectures that cannot be achieved by ordinary CMOS circuits. Non-volatile logic and reconfigurable logic circuits have been proposed using the spin-MOSFET and the pseudo-spin-MOSFETs, which are suitable for power-gating systems with low static energy.

The full operation suggested for spin-FETs and spin-MOSFETs have not yet been experimentally verified. For realizing fully functional spin transistors, some important progress in the underlying technologies such as electrical spin injection, spin detection, and spin manipulation in semiconductors (SCs) should be required. Lots of theories have predicted that the insertion of a tunnel barrier between the ferromagnet (FM) and SC is a promising method for highly efficient electrical spin injection and detection.

Recently, large spin signals induced by the efficient spin injection and detection were observed in Si-based lateral spin-valve devices with FM/MgO tunnel-barrier contacts even at room temperature. Also, by using a back-gated device structure with FM/MgO tunnel-barrier contacts, a basic read operation of Si-spin-MOSFETs was demonstrated at room temperature. These are important developments for Si-based spin-MOSFETs. However, if an insulator tunnel barrier such as MgO was utilized, the large parasitic resistance can cause the obstacle for the development of source and drain structures in the spin transistors. Another key development for highly efficient spin injection/detection in SCs is half-metallic FM contacts. In particular, electrical spin injection, transport, and detection in SCs without using insulator tunnel barriers have been demonstrated in lateral spin-valve devices with Heusler alloy/SC Schottky-tunnel-barrier contacts. To reduce the value of RA at the source and drain structures in spin-MOSFETs, the delta-doping of dopant impurities near the Heusler alloy/Ge Schottky-tunnel-barrier has been demonstrated, leading to the room-temperature spin transport including local magnetoresistance effect in Ge-based lateral devices with RA values of less than 0.2 kΩμm. Unfortunately, the MR ratio at room temperature in the Ge-based lateral devices is still much low (< 0.001 %) because of an imperfectness of the Heusler alloy/Ge quality. For enhancing the MR ratio in spin-MOSFET structures, it is essential to optimize the formation of high-quality Heusler alloy/SC Schottky-tunnel contacts and to reduce the channel length between source and drain contacts.

Alternative approaches for realizing spin-MOSFETs have been proposed. Pseudo-spin-MOSFETs are circuits that reproduce the functions of spin-MOSFETs using an ordinary MOSFET and a magnetic tunnel junction (MTJ) which is connected to the MOSFET in a negative feedback configuration. Although pseudo-spin-MOSFETs offer the same functionality as spin transistors, such as the ability to drive variable current, pseudo-spin-MOSFETs have larger resistance than spin-FETs or spin-MOSFETs.

For spin manipulation in SCs, channel materials with a strong spin-orbit interaction, such as InGaAs, InAs and InSb, are required in order to sufficiently induce the Rashba spin-orbit interaction by an electric gate voltage. Using InAs and InGaAs D2EG heterostructures with and without FM spin injector and detector, respectively, the spin manipulation was demonstrated by the electric field, meaning the operation of a spin-FET. However, the operation temperature was limited to the low temperature less than 40 K. The experimental proof of electrical spin injection, detection and manipulation in SCs with the strong spin-orbit interaction above room temperature is needed to create spin-FETs.

3.3.2. NEGATIVE GATE CAPACITANCE FET

Salahuddin and Datta originally proposed that, based upon the energy landscape of ferroelectric capacitors, it should be possible to implement a step-up voltage transformer that will amplify the gate voltage of a MOSFET. This would be accomplished by
replacing the standard insulator in the gate stack with a ferroelectric insulator of appropriate thickness. The resulting device is called a negative gate capacitance FET or NCFET. The gate operation in this device would lead to subthreshold swing (STS) lower than 60 mV/decade and might enable low voltage/low power operation. The main advantage of such a device is that it is a relatively straightforward replacement of conventional FETs. Thus, high Ion levels similar to advanced CMOS would be achievable with lower voltages. An early experimental attempt to demonstrate a low-STS NCFET, based on a P(VDF-TrFE)/SiO2 organic ferroelectric gate stack, was reported in 2008, and subsequently in a more controlled structure in 2010. These experiments established the proof of concept of sub-60 mV/decade operation using the principle of negative capacitance.

In addition to these experiments using polymer-based ferroelectrics, negative differential capacitance was demonstrated in a crystalline capacitor stack. Essentially, it was demonstrated that in a bi-layer of dielectric Strontium Titanate (SrTiO3: STO) and Lead Zirconate Titanate (Pb1/2Zr1/2TiO3: PZT), the total capacitance is larger than what it would be for just the STO of the same thickness as used in the bi-layer. This necessarily demonstrates the stabilization of PZT at a state of negative differential capacitance. More recently, in a single PZT capacitor, a direct measurement of negative capacitance was demonstrated. That work determined that when a ferroelectric capacitor is pulsed with an input voltage, it shows an ‘inductance-like’ discharging in addition to a capacitive charging.

As a recent significant result, it is now possible to grow ferroelectric materials using the atomic layer deposition process (ALD) by doping the frequently used gate dielectric HfO2 by constituents such as Zr, Al or Si. Using this doped Hf based ALD ferroelectric, a number of experiments have demonstrated the negative capacitance effect. For example, by using HfZrO2 as a gate dielectric, sub-60 mV/decade STS was demonstrated in finFETs with Lg=30 nm for both nFET and pFET structures. In the last two years, multiple papers have reported this effect for various material systems and channel lengths. Significant among them is the demonstration by GlobalFoundries of NCFETs in their 14 nm finFET technology, with improved subthreshold swing, lower OFF current and lower active power and ring oscillators running at GHz speed.

### 3.3.3. NEMS SWITCH

Nanoelectromechanical (NEM) switches use electrostatic force to mechanically actuate a movable structure to make or break physical contact between current-conducting source and drain electrodes. When the electrodes are separated physically by an air gap, no current flows across the gap, resulting in zero OFF-state current. The NEM switch undergoes an abrupt change in current conduction ability between non-contacting and contacting states, with nearly zero subthreshold swing. While zero OFF-state current provides for zero standby power dissipation, zero subthreshold swing enables very low operating voltages for low dynamic power dissipation as well. Moreover, a NEM switch can be operated with either positive or negative voltage polarity due to the ambipolar nature of the electrostatic force, so that an electrostatically actuated NEM relay can be configured to turn on either with increasing control (gate) voltage or with decreasing gate voltage and can serve as either a pull-down device (passing a low voltage – ground – from the source to the drain, i.e. discharging the voltage at the drain) or a pull-up device (passing a high voltage – VDD – from the source to the drain, i.e. charging the voltage at the drain). Additional advantages of mechanical devices include robust operation across a wide temperature range, down to cryogenic temperatures, and immunity to ionizing radiation. NEM switches can be monolithically integrated with CMOS circuitry by a modular post-CMOS fabrication process with relatively low thermal budget. Since state-of-the-art CMOS technology incorporates air-gapped interconnects, NEM switches can be implemented using multiple interconnect layers formed in the back-end-of-line (BEOL) process. Potential applications for hybrid NEMS-CMOS technology include CMOS power gating, configuration of FPGAs, non-volatile back-up storage of information in SRAM and content addressable memory (CAM) cells, and energy-efficient, fast and reconfigurable look-up tables.

Conventional planar processing techniques (i.e., thin-film deposition, lithography and etch processes) can be employed to fabricate the conducting electrodes of a mechanical switch. The air-gaps between electrodes are formed with a final “release” etch step in which a sacrificial material such as silicon dioxide, photoresist, polyimide or silicon is selectively removed. The switching delay and operating voltage of a NEM switch can be reduced by scaling down the size of these air-gaps. The smallest air-gap demonstrated to date for a functional NEM structure fabricated using a top-down approach is 4 nm, resulting in an actuation voltage of approximately 0.4 V. As expected, it exhibited very low OFF-state current and sub-threshold swing; however, it is only a 2-terminal device, not suitable for logic switch application. SiC nanowires have been used as the movable structure for NEM switches that are suitable for high-temperature operation. Functioning 2-terminal SiC switches with air-gaps as small as 10 nm and switching voltage as low as 1 V have been demonstrated. 3-terminal devices and corresponding logic gates also were demonstrated. Piezoelectric materials have been incorporated in NEM devices to enable sub-1 V switching.

The operating speed of a NEM switch is much slower than that of a transistor because it is dominated by mechanical delay related to the physical motion of the movable structure rather than the electrical (charging/discharging) delay; therefore an optimized relay-based IC design should arrange for all mechanical movements to happen simultaneously, so that the delay per operation is essentially one mechanical delay. For a pass-gate circuit topology, multiple switches are connected together in series to drive
the output signal. This means that the source voltage can vary between the reference voltage (ground) and the supply voltage ($V_{DD}$). For proper pass-gate circuit operation, the state of the switch cannot be dependent on the source voltage; therefore a fourth electrode is necessary to provide a constant reference voltage, such that the voltage applied between the control (gate) electrode and the reference (body) electrode determines the state of the switch, i.e. whether a current path is established between the source and drain electrodes. The contact and actuation air-gaps can be reduced by biasing the body electrode to reduce the magnitude of the gate voltage required to switch the device ON/OFF. Moreover, a constant-field scaling methodology can be applied to miniaturize NEM switches for reduced footprint, switching delay and switching energy. With the aid of body biasing, the minimum switching energy for a nanoscale relay is anticipated to be on the order of 10 aJ, which compares well against the switching energy for an ultimately scaled MOSFET. Piezoelectric NEM devices have demonstrated 10 mV switching operation using body bias, providing for very low energy dissipation per switching cycle (23 aJ), and an extremely small subthreshold slope (0.013 mV/decade). A variety of relay-based computational and memory building blocks have been experimentally demonstrated to date.

The prospective system-level benefits of mechanical logic have been analyzed by performing simulation-based assessments of VLSI circuit blocks implemented with NEM switches. These indicate that relays can provide for more than 10x reduction in energy per operation as compared with MOSFETs, and can reach clock speeds in the GHz regime. Thus, a major potential advantage of NEM switch technology is improved energy efficiency. Moreover, the contact adhesive force and structural stiffness can be engineered to achieve bi-stable operation, which makes mechanical switches attractive for embedded non-volatile memory applications. Recently hybrid CMOS-NEMS circuits have been demonstrated, with non-volatile NEM switches operating at the same $V_{DD}$ as for the CMOS circuitry. The BEOL metallic layers used to form interconnects in a conventional CMOS process can be leveraged to implement compact NV-NEM switches for dynamically reconfigurable circuit functionality.

For all of the aforementioned applications, the NEM switches need to operate reliably and consistently for at least $10^9$ cycles. Due to the extremely small mass of the movable electrode (less than 1 ng), neither gravitational acceleration nor mechanical vibration substantially affects their operation. Structural fatigue or creep can be easily avoided by designing the movable structure/anchor such that the maximum induced strain is well below the yield strength. However, permanent stiction can be a mode of device failure: for soft electrode materials such as gold and platinum, Joule heating at the contacting asperities can lead to atomic diffusion (welding). This issue can be mitigated by using a refractory electrode material such as tungsten to minimize contact wear and by reducing the peak voltage difference between the source and drain electrodes ($V_{DD}$) when they are in contact. NEM switches with tungsten electrodes have been demonstrated to have endurance up to 1 billion ON/OFF cycles at 2.5 Volts for a relatively large load capacitance of 300 pF (i.e. exaggerated electrical delay), and endurance exceeding $10^{16}$ ON/OFF cycles is projected for voltages below 1 Volt and load capacitance below 1 pF. The remaining reliability challenge for NEM logic switches is degradation (dramatic increase) of on-state resistance due to electrode surface oxidation or the formation of friction polymers over the lifetime of device operation. Alternative contacting electrode materials such as Ru/RuO$_2$ and/or hermetic packaging are potential solutions to this issue.

Adhesive force between the contacting electrodes dictates the minimum required stiffness of the movable structure, which in turn determines the minimum gate-to-body voltage required to switch the NEM relay. The adhesion energy is determined by metallic bonding (at the contacting asperities) and by van der Waals force (in the non-contacting regions of the electrodes). Self-assembled molecular (SAM) coating of hydrophobic materials has been demonstrated to reduce the adhesive force and thereby enable switching operation at lower gate voltage. Sub-50 mV operation of relay integrated circuits demonstrating OR, AND, and XOR gate functionality have been demonstrated with body-biased SAM-coated NEM switches. Most recently, operation of NEM switches and integrated circuits at temperatures down to 4K were demonstrated for the first time. Due to reduced adhesion energy and elimination of contact oxidation, relays can be operated reliably with voltages as low as 25 mV for more than $10^8$ cycles at cryogenic temperatures, showing promise for monolithic integration of multiplexing control circuitry with qubits.

In conclusion, the negligible OFF-state current and ultra-low-voltage operation capability of NEM switches make them compelling for ultra-low-power digital computing applications such as the Internet of Things, particularly where resilience to extreme temperatures and/or immunity to radiation are required. Furthermore, hybrid CMOS-NEM technology shows promise for enhanced chip functionality, e.g. with dynamically reconfigurable interconnects. Remaining challenges to realizing the promise of mechanical computing include materials and process optimization to achieve stably low contact resistance with minimal contact adhesive force.

### 3.3.4. MOTT FET

Mott field-effect transistor (Mott FET) utilizes a phase change in a correlated electron system induced by a gate as the fundamental switching paradigm. Mott FETs could have a similar structure as conventional semiconductor FET, with the semiconductor channel materials being replaced by correlated electron materials. Correlated electron materials can undergo Mott insulator-to-metal phase transitions under an applied electric field due to electrostatically doped carriers. Besides electric field excitation,
the Mott phase transition can also be triggered by photo- and thermal-excitations for optical and thermal switches. Defects created by environmental exposure to chemicals or electrochemical reactions can also induce Mott transition via carrier doping. The critical threshold for inducing phase change can be tuned via stress.

Mott FET structure has been explored with different oxide channel materials. Among several correlated materials that could be explored as channel materials for Mott FET, vanadium dioxide (VO₂) has attracted much attention due the sharp metal-insulator transition near room temperature (nearly five orders in single crystals). The phase transition time constant in VO₂ materials is in sub-picosecond range determined by optical pump-probe methods. Device modeling indicates that the VO₂-channel-based Mott FET lower bound switching time is of the order of 0.5 ps at a power dissipation of 0.1 µW. VO₂ Mott channels have been experimentally studied with thin film devices and the field effect has been demonstrated in preliminary device structures. Recently, prototypes of VO₂ transistors using ionic liquid gating have shown larger ON/OFF ratio at room temperature than with solid gate dielectrics like hafnia. The conductance modulation happens at a slow speed, however, due to the large charging time constants. The possibility of electrochemical reactions must also be carefully examined in these proof-of-principle devices due to the instability of the liquid-oxide interfaces and the ease of cations in such complex oxides to change valence state. On the other hand, unlike traditional CMOS that is volatile and digital, electrochemically gated transistors exhibit non-volatile and analog behaviors, which can be utilized to demonstrate synaptic transistors and circuits that mimic neural activities in the animal brains. Voltage induced phase transitions in two-terminal Mott switches have also been implemented to realize neuron-like devices and steep-slope transistors. As a Mott device with purely electrostatic modulation in the solid-state base, the VO₂-FET with a high-k oxide/organic hybrid dielectric gate has been proposed. Their reversible as well as quick resistance switching upon an application of gate bias and the maximum resistance modulation at the Metal-Insulator transition temperature indicate the possibility of purely electrostatic field-induced metal-insulator (Mott) transition. The gate-tunable abrupt switching device based on a VO₂ microwire integrated monolithically with a two-dimensional tungsten diselenide semiconductor by van der Waals stacking has been reported. Nanofabrication engineering has been demonstrated to enhance the performance of Mott FET. The 3-dimensional Fe₂O₃ nanowires on the length scale of 10 nm exhibited the remarkable Verwey transition at about 112 K, which was found to be 6 times larger than that for the thin-film configuration.

Experimental challenges with correlated electron oxide Mott FETs include fundamental understanding of gate oxide-functional oxide interfaces and local band structure changes in the presence of electric fields. Methods to extract quantitative properties (such as defect density) of the interfaces are an important topic that have not been explored much to date. The relatively large intrinsic carrier density in many of the Mott insulators requires the growth of ultra-thin channel materials and smooth gate oxide-functional oxide interfaces for optimized device performance. It is also important to understand the origin of low room-temperature carrier mobility in these materials. Theoretical studies on the channel/dielectric interfacial electronic band structure are needed for the modeling of subthreshold behaviors of Mott FETs. Understanding the electronic transition mechanisms while de-coupling from structural Peierls (lattice) distortions is also of interest and important in the context of energy dissipation for switching.

While the electric field-induced transitions are typically explored with Mott FET, nanoscale thermal switches with Mott materials could also be of substantial interest. Recent simulation studies of “ON and “OFF” times for nanoscale two-terminal VO₂ switches indicate the possibility of sub-ns switching speeds in ultra-thin device elements in the vicinity of room temperature. Such devices could also be of interest to Mott memory. One can, in a broader sense, visualize such correlated electron systems as ‘threshold materials’ wherein the conducting state can be rapidly switched by a slight external perturbation, and hence lead to applications in electron devices. Electronically driven transitions in perovksite-structured oxides such as rare-earth nickelates or cobaltates with minimal lattice distortions would also be relevant in this regard. Three-terminal devices are being investigated using these materials and will likely be an area of growth. Floating gate transistors have recently been demonstrated on silicon. It has been found that non-thermal electron doping in SmNiO₃ can lead to a colossal increase in its resistivity, which has been utilized to demonstrate a solid-state proton-gated transistor with large ON/OFF ratio. Clearly, these preliminary results suggest the promise of correlated oxide semiconductors for logic devices, while the doping process indicates slower dynamics than possible with purely electrostatic carrier density modulation. The non-volatile nature of the Mott transition in 3-terminal devices suggest combining memory operations into a single device and could be explored further. Architectural innovations that can create new computing modalities with slower switches but at lower power consumption can benefit in the near term with results to date while in the longer term transistor gate stacks need to be studied further for these classes of emerging semiconductors.

### 3.3.5. Topological Insulator Electronic Devices

Topological insulators are recently discovered materials that possess a bandgap in their interior. However, the topology of their electronic states necessitates the existence of gapless, conducting modes on their boundaries – one dimensional (1D) edges in the case of two-dimensional (2D) topological insulators, and 2D surfaces in the case of three-dimensional (3D) topological
insulators.\textsuperscript{569,570,571,572} These conducting modes are protected from backscattering by symmetry, and in the case of 1D edge modes of 2D topological insulators, are expected to be ballistic conductors.

Systematic searches of materials databases have found that topological materials are commonplace, representing a significant fraction of all known materials.\textsuperscript{573,574,575} Two-dimensional topological insulators have been realized with very large bandgaps of 360 meV (Na\textsubscript{3}Bi\textsuperscript{576}) and 800 meV (bismuthine\textsuperscript{577}), significantly exceeding the thermal energy at room temperature (25 meV), which indicates that topological phenomena may be robust at room temperature in suitable materials.

Numerous proposals have been put forward to exploit topological materials in transistor design.\textsuperscript{578,579,580,581,582,583,584,585,586,587} One topological transistor design envisions switching a 2D material from topological insulator (“ON” with ballistic edge channels) to a conventional insulator (“OFF”). This switching may be accomplished via electric field through several mechanisms such as Rashba effect,\textsuperscript{578} staggered sublattice potential,\textsuperscript{578,580,586} inversion symmetry breaking,\textsuperscript{581} or Stark effect.\textsuperscript{582,583,584,585,576} Electric field effect switching has been proposed in a number of materials including graphene,\textsuperscript{578} monolayer transition metal dichalcogenides in 1T’ phase,\textsuperscript{582} SnTe and Pb\textsubscript{1-x}Sn,Se(7e),\textsuperscript{581} topological semimetals such as Cd\textsubscript{2}As\textsubscript{3} and Na\textsubscript{3}Bi,\textsuperscript{583,576} and phosphorene.\textsuperscript{584} Electric-field switching of the topological state has been demonstrated in at least one material Na\textsubscript{3}Bi.\textsuperscript{576} Other transistor proposals have focused on electric-field switching of tunneling between topological edges,\textsuperscript{588} or using strong disorder to produce an off state in a bulk conducting topological insulator.\textsuperscript{587} Topology may also be controlled by magnetic fields,\textsuperscript{589,590} strain,\textsuperscript{591} temperature,\textsuperscript{592} or time-dependent electric fields,\textsuperscript{593} hence topological devices have the prospect of adding additional new functionality for “More than Moore” devices.

The deep connection between topological insulators and spin-orbit coupling suggests further synergies between topological electronics and spin electronics. Indeed, 2D topological insulators exhibit a quantized spin Hall effect and can be used to produce completely polarized spin current,\textsuperscript{578} of potential use in spintronics devices. Magnetic 2D topological insulators (quantum anomalous Hall effect) may produce perfectly spin-polarised current with spin direction determined by magnetization direction,\textsuperscript{584} opening new possibilities for spin transistors and non-volatile random-access memory. Near-perfect ballistic conduction in the quantum anomalous Hall regime with current-induced magnetization switching at very low currents (1 nA) was recently demonstrated in graphene/boron nitride heterostructures\textsuperscript{595} albeit at cryogenic temperatures. Analogous topological effects may be realized for other degrees of freedom such as the valley degree of freedom in materials with multiple conduction valleys, with analogous quantum valley Hall effects switchable by electric field.\textsuperscript{596,597,598}

Numerous fundamental research challenges remain before topological transistors may become useful. Topological switching via electric field effect is a fundamentally different mechanism of operation compared to the traditional MOSFET. At present it is unclear what limits the subthreshold swing and therefore the operating voltage of a topological transistor, and how this depends on the specific mechanism of electric field switching. Detailed models and device simulations for topological transistors are needed, as well as experiments on electric-field switching of topological materials in realistic device geometries. It is likely that new topological materials are needed that optimize large bandgaps and sensitive electric field-driven switching, and that also are amenable to device fabrication and processing. Realistic theoretical models will be needed to guide materials discovery and device design.

### 3.4. **BEYOND-CMOS DEVICES: ALTERNATIVE INFORMATION PROCESSING**

#### 3.4.1. **SPIN WAVE DEVICE**

Spin Wave Device (SWD) is a type of magnetic logic devices exploiting collective spin oscillation (spin waves) for information transmission and processing.\textsuperscript{599,600,601,602,603} The basic elements of the SWD include: (i) magneto-electric cells (e.g. multiferroic elements) aimed to convert voltage pulses into the spin waves and vice versa;\textsuperscript{604,605} (ii) magnetic waveguides–spin wave buses for spin wave signal propagation between the magneto-electric cells;\textsuperscript{606} (iii) magnetic junctions to couple two or several waveguides;\textsuperscript{607} (iv) spin wave amplifiers;\textsuperscript{608} (v) phase shifters to control the phase of the propagating spin waves;\textsuperscript{609} and (vi) spin wave phase error correctors.\textsuperscript{510} SWD converts input voltage signals into the spin waves, computes with spin waves, and converts the output spin waves into the voltage signals. Computing with spin waves utilizes spin wave interference, which enables functional nanometer scale logic devices. Since the first proposal on spin wave logic,\textsuperscript{599} SWD concept has evolved in different ways: encompassing volatile\textsuperscript{611} and non-volatile,\textsuperscript{612} Boolean\textsuperscript{612,613} and non-Boolean,\textsuperscript{614} single-frequency and multi-frequency circuits.\textsuperscript{615} The primary expected advantage of SWD over Si CMOS are the following: (i) the ability to utilize phase in addition to amplitude for building logic devices with a fewer number of elements than required for transistor-based approach; (ii) power consumption minimization by exploiting the intrinsically low energy (μeV) of spin waves in ferromagnets as well as built-in non-volatile magnetic memory and magnetic reconfigurability,\textsuperscript{616}, and (iii) parallel data processing on multiple frequencies in a single core structure by exploiting each frequency as a distinct information channel.

Micrometer-scale SWD MAJ gate has been experimentally demonstrated.\textsuperscript{617} It is based on ferromagnetic Ni\textsubscript{81}Fe\textsubscript{19} structure, operates within 1–3 GHz frequency range, and exhibits signal-to-noise ratio of approximately 10 at room temperature.\textsuperscript{617}
internal delay of SWD is defined by the spin wave group velocity (e.g., 3×10^6 cm/s in Ni_{3}Fe_{19} waveguides). Power dissipation in SWD is mainly defined by the efficiency of the spin wave excitation. Recent experiments with synthetic multiferroics comprising piezoelectric (lead magnesium niobate-lead titanate PMN-PT) and magnetostrictive (Ni) materials have demonstrated spin wave generation by relatively low electric field (e.g., 0.6 MV/m for PMN-PT/Ni). The later translates in ultra-low power consumption (e.g., 1 pJ per multiferroic switching). Recent experimental demonstration\textsuperscript{605} of parametric spin wave excitation by voltage-controlled magnetic anisotropy (VCMA) is another promising route towards energy-efficient generation of spin waves.

Recently, a new type of SWD magnonic holographic memory (MHM), was proposed.\textsuperscript{614} The principle of operation of MHM is similar to optical holographic memory, while spin waves are utilized instead of light waves. The first 2-bit MHM prototype based on yttrium iron garnet structure has been demonstrated.\textsuperscript{619} MHM also possesses unique capabilities for pattern recognition by exploiting correlation between the phases of the input waves and the output interference pattern. Pattern recognition using MHM has been recently demonstrated.\textsuperscript{620} The potential advantage of spin wave utilization includes the possibility of on-chip integration with the conventional electronic devices via multiferroic elements. In addition, magnonic holograms can show very high information density (about 1 Tb/cm\textsuperscript{2}) due to the nanometer scale wavelength of spin waves. According to estimates, the functional throughput of magnonic holographic devices may exceed 10\textsuperscript{18} bits/s/cm\textsuperscript{2}.\textsuperscript{614}

There are several important milestones crucial for further SWD development: (i) nanomagnet switching by spin waves;\textsuperscript{621} (ii) integration of several magneto-electric cells on a single spin wave bus. In order to have an advantage over CMOS in functional throughput, the operational wavelength of SWDs should be scaled down below 100 nm.\textsuperscript{612} The success of the SWD will also depend on the ability to restore/amplify spin waves (e.g., by multiferroic elements or spin torque oscillators). Another recent direction of research is antiferromagnetic SWD\textsuperscript{622} that potentially offer a thousand-time increase in operation speed due to THz scale frequencies of antiferromagnetic spin waves.

### 3.4.2. Excitonic Devices

Excitonic devices are based on excitons as computational state variables. Excitonic devices are suited to the development of an advanced energy-efficient alternative to electronics due to the specific properties of excitons: 1) Excitons are bosons and can form a coherent condensate with vanishing resistance for exciton currents and low switching voltage for excitonic transistors. This allows creating energy-efficient computation with power consumption per switch significantly smaller than in electronic circuits. 2) Excitonic signal processing can be directly coupled to optical communication in exciton optical interconnects. 3) The sizes of excitonic devices are scaled by the exciton radius and de Broglie wavelength that are much smaller than the photon wavelength. Furthermore, excitons can be efficiently controlled by voltage. This gives the opportunity to realize excitonic circuits at scales much smaller than for photonic devices.

The advantages listed above are realized using specially designed indirect excitons, IXs. An IX is a bound pair of an electron and a hole in separated layers. The properties of IXs make them different from conventional excitons and suitable for the development of energy-efficient computing: 1) IXs have oriented electrical dipole moments. As a result, the IX energy and IX currents are controlled by voltage allowing the realization of a field effect transistor operating with IXs in place of electrons. 2) The IX emission rate can be tuned over many orders of magnitude. Turning the emission off allows the realization of multi-element IX circuits with suppressed losses while turning it on allows fast write and readout. 3) The low overlaps between electrons and holes in IXs allow the realization of a coherent condensate with the suppressed thermal tails and dissipationless IX currents enabling energy-efficient computation.

Experimental proof-of-principle for excitonic devices including IX transistors, diodes, and CCD was demonstrated. IX condensate and coherent IX currents and, recently, long range coherent IX spin currents were observed at low temperatures. New heterostructures based on single-atomic-layers of transition-metal dichalcogenide (TMD) for room-temperature IX circuits were proposed. Recent progress includes the realization of IXs at room temperature in TMD heterostructures, discovery of IX coherent spin currents in GaAs heterostructures, development of first split-gate device for IXs, the basic mesoscopic device, development of advanced platform for high-mobility excitonic devices, development of TMD heterostructures with small IX linewidth and finding charged IXs, indirect trions. At present, the studies are focused on the development of basic concepts of excitonic devices at low temperatures using GaAs heterostructures and development of room-temperature excitonic devices using TMD heterostructures.

### 3.4.3. Transistor Laser

The Light-Emitting Transistor (LET)\textsuperscript{633} and Transistor Laser (TL)\textsuperscript{634,635} utilize a fundamental characteristic of bipolar transistors - that electron-hole recombination in the base is an essential feature of the transistor and that the resulting photon signal in a direct-bandgap base is correlated to the electrical signal driving and being driven by the device. The TL can be thought of as a 5 terminal heterojunction bipolar transistor (HBT) with 3 conventional electrical terminals (emitter, base, and collector) and 2 optical terminals (input-generation and output-recombination).\textsuperscript{636} Very-high-speed transmission and processing are enabled by
the projected capability to achieve over 200 GHz bandwidths in the GaAs- or InP-based devices. An advantage of the TL is that a single epitaxial layer structure can be used for devices that generate photons, detect photons, and perform electronic functions. The layer structure of the TL resembles a heterojunction bipolar transistor with features added to enhance base recombination and control base transit time. When used to realize conventional logic architectures, for example NOR gates, the key advantage is speed. With processing-intensive operations and using the energy-delay product as a metric for comparison, a 30–100 times improvement is expected over conventional CMOS, leading to both faster processing and improved energy efficiency. An even greater benefit might be achieved using architectures that perform electronic-photonic processing in the analog domain.

The first demonstration of lasing in the TL occurred in 2004. Since that time, progress has been made on understanding the device physics and on using the TL for discrete optical interconnects. A key initial objective has been examining factors affecting device bandwidth. Edge-emitting TLs with large active regions (200 μm × 1 μm) have been modulated to 22 Gbps and have shown a measured bandwidth of 10.4 GHz. Relative intensity noise (RIN) as low as -151 dB/Hz has also been demonstrated, showing an approximately 28 dB improvement over diode lasers. To improve speed and enable integration, reducing the size of the active region is critical. For that reason, Vertical-Cavity Transistor Lasers (VCTL) have been examined and demonstrated. Initial VCTLs had limited temperature range due to misalignment of the cavity reflectivity and gain peaks. More recently, work has been underway to show that electronic-photonic logic can be made using the transistor laser. The initial target of an integrated TL-based NOR gate has been demonstrated, but significant work is needed to improve performance.

The ultimate performance in both power and speed will be achieved as the device is size is scaled, as projected performance to bandwidths in excess of 100 GHz has a sound rationale but has yet to be realized. The use of vertical-cavity structures to reduce the device footprint has been a first step in the scaling process but further work is needed on microcavity vertical-cavity transistor lasers (VCTLs). Scaling beyond micron-scale devices such as this is possible, but the key will be the design of optical structures such as photonic crystal cavities that will enable small numbers of photons to be captured and directed to act on other TL structures. As scaling advances, further examination of device physics to reduce the effective minority carrier radiative lifetime will be key, along with the examination of effects that might impact the modulation response. Further work is also needed on InP-based devices (1310 and 1550 nm emission) to facilitate the use of silicon waveguides for optical signal routing. Additional questions at the architecture level involve the best way to use the TL in computer systems. What is enabled by having very high speed optical links? What architectures make sense for electronic-photonic NOR gates? Are other approaches to computation enabled, such as analog methods? Initial work to address how the TL might impact computer architecture has been underway in the Li group at the University of Chicago, in collaboration with the University of Illinois at Urbana-Champaign. Further work on how TLs might be used in machine learning applications is also underway by this group (unpublished). Other noteworthy results include demonstration of blue-emitting light-emitting transistors in the GaN/InGaN system.

3.4. MagnetoElectric Logic

There have been major developments, involving magneto-electric transistor (MEFET) schemes, increasing the range of possible magneto-electric devices, that would serve as "beyond CMOS" plug-in replacement logic. There are also some benchmarking efforts, where there has been an effort to compare the most competitive magneto-electric devices with CMOS. The result is that it is now increasingly clear that magneto-electric field effect transistors are more likely to be competitive or surpass CMOS than the earliest magneto-electric device concepts were based on a magnetic tunnel junction structure. The disadvantage, with the magneto-electric magnetic tunnel junction device structure, is that while much faster than many spintronics devices, there are long delay times in device operation, due to the slow speed of switching a ferromagnet, and the predicted fidelity is likely low, making it difficult to cascade from one device to the next.

Other magneto-electric devices, like the composite-input magneto-electric–based logic technology (CoMET) and a similar magneto-electric device structure, but using spin-orbit coupling, have also been proposed. The concern is that both these device concepts will have long delay times, due to the slow switching speed of the ferromagnetic layer, and in the case of the CoMET device, the additional complications of the slow speed of ferromagnetic domain wall propagation, are limited by the switching speed of the ferroelectric and domain wall motion. The basis of these devices is an input switches a ferroelectric material, in contact with a ferromagnet with in-plane magnetic anisotropy placed on top of an extra-gate ferromagnet interconnect with perpendicular magnetic anisotropy. The input voltage nucleates a domain wall while a current is used to drive the domain wall to the output end of the device. Also using spin orbit coupling, but now explicitly also using a magneto-electric layer for electrical control of exchange bias of a laterally scaled spin valve is the nonvolatile magneto-electric spin-orbit (MESO) logic, but the delay time is limited again by the switching speed of the ferromagnetic layer, although 50 ps switching speeds as short as have been estimated.

Magneto-electric transistor schemes are based on polarization of the semiconductor channel, by the boundary polarization of the magneto-electric gate. The advantage to the magneto-electric field effect transistor is that such schemes avoid the complexity and
detrimental switching energetics associated with magneto-electric exchange-coupled ferromagnetic devices. Spintronic devices based solely on the switching of a magneto-electric, will have a switching speed will be limited only by the switching dynamics of that magneto-electric material and above all are voltage controlled spintronic devices. Moreover, these magneto-electric devices promise to provide a unique field effect spin transistor (spin-FET)-based interface for input/output of other novel computational devices. This is spintronic without a ferromagnet, with faster write speeds (<20 ps/full adder), at a lower cost in energy (<20 aJ/full adder), greater temperature stability (operational to 400 K or more), and scalability, requiring far fewer device elements (transistor equivalents) than CMOS. These do differ from the conventional field transistor in that the ME-FET must be both top and bottom gated, so the result is that these are 4, not 3 terminal transistors.

Obviously, the semiconductor channel will only work if the very thin, so the boundary polarization of chromia effectively polarizes the semiconductor channel. The 2D semiconductors of the trichalcogenide class of quasi one-dimensional semiconductors, such as TiS$_2$, HfSe$_3$, as well as InP, have the potential to be scaled to transistor widths below 10 nm suggesting there is a plausible route forward.

The anti-ferromagnet spin-orbit read (AFSOR) logic device structure has interesting advantages: the potential for high and sharp voltage ‘turn-on’, inherent non-volatility of magnetic state variables; absence of switching currents; large on/off ratios; and multistate logic and memory applications. The design will provide reliable room-temperature operation with large on/off ratios (>10$^3$) well beyond what can be achieved using magnetic tunnel junctions. Again, the core idea is the use of the boundary polarization of the magneto-electric to spin polarize or partly spin polarize a very thin semiconductor, ideally a 2D material, with very large spin orbit coupling.

If the semiconductor channel retains large spin orbit coupling, then the spin current, mediated by the gate boundary polarization, may be enhanced and, to some extent, topologically protected. The latter implies that each spin current has a preferred direction.

The silicon CMOS majority gate (left) requires 13 components. The ME-spinFET majority gate requires, including clocking, of 6 components. This represents an area improvement of over 50%, assuming similar size transistors. This is equivalent to greater than one process node. If we split the magnetoelectric side of the gate so that the channel can independently be spin polarized up or down, this results in a component reduction from the previous best for the MEFET of six, down to four components, a further 50% reduction over the standard MEFET circuit, and a reduction to less than 30% in area compared to CMOS.

A majority gate, in the form of a single transistor like device, has also been proposed and modeled, but depends on the device scaled to dimensions smaller than the natural antiferromagnetic domain size of about 1 to 3 $\mu$m. There is a variant where inversion symmetry is not as strictly broken, that leads to a nonvolatile spintronics version of multiplexer logic (MUX). The magneto-electric spin-FET multiplexer also exploits the modulation of the spin-orbit splitting of the electronic bands of the semiconductor channel through a “proximity” magnetic field derived from a voltage-controlled magneto-electric material. Here, by using semiconductor channels with large spin-orbit coupling, we expect to obtain a transverse spin Hall current, as well as a spin current overall. Depending on the magnitude of the effective magnetic field in the narrow channel, we anticipate two different operational regimes. Like the AFMOR magneto-electric spin FET, the magneto-electric spin-FET multiplexer uses spin-orbit coupling in the channel to modulate spin polarization and hence the conductance (by spin) of the device. There is a source-drain voltage and current difference, between the two FM source contacts, due to the spin-Hall effect when spin-orbit coupling is present. This output voltage can be modulated by the gate or gates, which influences the spin-orbit interaction in the channel especially when it is both top and bottom gated especially. The spin-Hall voltage in the device can be increased by using different FM sources and drain. To increase the spin fidelity of current injection at the source end, one could add a suitable tunnel junction layer (basically a 1 nm oxide layer) between the magnetic source and the 2D semiconductor channel. This latter modification would result in diminished source-drain currents though. Again, there is a reduction is delay time and energy cost because these devices are nonvolatile, there is no magnetization reversal of a ferromagnet involved and the implementation of this device concept would require only 5 components for a majority gate compared to the 13 components required of a silicon CMOS majority gate.

Magneto-electric coupling can be used to excite parametric resonance of magnetization by an electric field. This has been considered for the development of spin wave devices based on voltage controlled magnetic anisotropy in ferromagnetic nanowires. This in turn, in effect, becomes a spin wave field effect transistor. The threshold voltage for parametric excitation in this system is found to be well below 1 V, which is attractive for applications in energy-efficient spintronic and magnonic nanodevices such as spin wave logic.

The challenges in pushing forward these technologies extends not only to the fabrication and characterization of a new generation of nonvolatile magneto-electric devices, but also to ascertaining the optimal implementation of CMOS plug in replacement circuits. Questions that need to be resolved include demonstration that the magneto-electric devices can be scaled to less than 10 nm, and this includes finding a suitable 2D channel material that can be polarized by exchange coupling with the boundary.
polarization of the magneto-electric and yet does not suffer from large scale edge scattering. Experimental demonstration of limits to the switching speeds of any antiferromagnetic magnetic electric remain absent. That said, the magneto-electric transistor has far fewer challenges to implementation than the magneto-electric magnetic tunnel junction, so, not surprisingly, there is a shifting of development effort toward those and related devices for both memory and logic. New device concepts are being considered as well. These device concepts have advantages like reducing the number of leakage pathways to just one and require only one clock cycle. The actual demonstration of such devices appears almost "in hand" suggesting that experimental evidence of promise is not that far away.

### 3.4.5. Domain Wall Logic

The domain wall-magnetic tunnel junction (DW-MTJ) or three-terminal magnetic tunnel junction (3T-MTJ) operates as an in-memory computing nonvolatile logic device through current-driven manipulation of a single domain wall in a ferromagnetic patterned wire, with readout performed using a magnetic tunnel junction. It can be considered as an extension of racetrack memory to a single domain wall racetrack for compute-in-memory applications.

The domain wall track is composed of heavy metal/ferromagnet/oxide thin films patterned into a wire shape. Standard materials examples are Ta/CoFeB/MgO. On top of the track is a patterned MTJ hard reference layer with additional related thin films to promote high switching field of the hard layer compared to the ferromagnetic track.

The ends of the ferromagnetic track can be exchange-biased in opposing directions using antiferromagnets, and/or an additional electrode can be used to ensure a single wire is created in the track.

The simplest form of the device has three terminals: input (IN) and clock (CLK) contacting the ferromagnetic track, and output (OUT) contacting the top of the MTJ. During the write operation, a voltage applied between IN and CLK drives a current and moves the domain wall using either spin transfer torque (STT) and/or spin orbit torque (SOT). During the read operation, a voltage applied between CLK and OUT measures the resistance state of the MTJ relative to the domain wall, which will determine the amount of current to drive subsequent devices. The device can act as an analog universal NAND gate, in addition to other basic logic gates: if IN is connected to the OUT of two previous devices, and only if both are in a low resistance state (logic output 1) will there be sufficient current to depin and move the domain wall to the other side of the MTJ, changing the output of the device from a low resistance state (logic output 1) to high resistance state (logic output 0).

A related device is the mLogic four-terminal version, which has an additional non-magnetic, non-conducting spacer on top of the ferromagnetic track that couples the current-manipulated domain wall to a domain wall or nanomagnet in an electrically-separated layer, which then alters the output MTJ resistance. The additional terminal comes from two terminals connected to the output MTJ. The four-terminal version provides complete input/output isolation.

The device operation has been modeled in micromagnetics including NAND, shift register, and full adder functions, and initial benchmarking was performed up to a full adder simulation. A SPICE model has been developed to enable larger scale circuit simulations. Single device operation and three-device circuit operation has been shown in experimental prototypes, including inverter, buffer, and concatenation operation. The prototypes showed in experiment one of the first examples of concatenable magnetic logic devices for building larger circuits. The four-terminal mLogic spacer coupling has also been demonstrated.

Larger scale system-level simulations have been performed to determine the benefits and drawbacks of DW-MTJ logic. One circuit-level energy-performance analysis showed that while very low voltage can be used to operate the essentially all-metallic devices, it comes with increased extrinsic DW pinning effects and thermal noise. They predicted the energy reduction from increasing the tunnel magnetoresistance (TMR) will saturate when TMR > 100%, but further increasing TMR can mitigate predicted thermal noise limits. Recent work simulated a 32-bit adder communicating with registers with all DW-MTJ devices and shows SOT switching can make the technology competitive with a comparable CMOS sub-processor component.

The device has recently been extended by many in the community to non-Boolean logic applications in neuromorphic circuits, including spike-timing-dependent-plasticity synapses and leaky, integrate, and fire neurons.

Major challenges exist in understanding and improving the device-to-device and cycle-to-cycle variation of the devices, which arise from variation in the domain wall location and pinning landscape. A discussion of influence of device variability on circuit performance is presented in Xiao et al. Better understanding of experimental viability of the technology is needed, given TMR variability and constraints and scaling-induced variability and errors. Example ideal applications of the device technology are still needed, with some potential areas being radiation-hard environments, lower latency hardware accelerators, and low-area, low-energy needs of edge-computing internet of things devices.
3.4.6. Spin Torque Majority Gate

A majority gate is a logic gate used to simplify circuit complexity to carry out the majority function where the output is a HIGH if and only if more than half of its inputs are HIGH, otherwise the output is a LOW. A majority gate can have any number of inputs. However, the most common ones referred to as 3-input majority gates or MAJ3 are implemented with three inputs and one output. A majority gate can implement an AND by tying one of its inputs to a 0, or an OR by tying the input to a 1. A minority gate can be derived from a majority gate by appropriately using an inverter according to De Morgan’s rule. In a full adder, the carry output is the majority function of the three inputs. Implementations of majority gates are currently done using complementary metal oxide semiconductor (CMOS), quantum cellular automata (QCA), spin-wave majority gate (SWMG), and domain-wall or spin-torque majority gate (STMG).

Spin Torque Majority Gate (STMG) is a 3-input majority gate that operates based on domain wall motion driven by either spin transfer torque (STT) or spin orbit torque (SOT) in magnetic tunnel junctions (MTJs) usually with perpendicular magnetic anisotropy (PMA). This has an advantage of energy efficiency, non-volatility, small area, low power, reconfigurability, and radiation hardness compared to other types of majority gate devices. In an STMG, three MTJs set the input states with STT and SOT while the fourth device reads the output state through tunneling magnetoresistance (TMR).

Much of the work on STMGs has been in micromagnetic simulations. The most common implementation consists of four discrete PMA ferromagnetic nanopillars of independent fixed layers placed on a common free cross-shaped PMA ferromagnetic layer. It is observed that there is a minimum critical current density required to switch the device, which is inversely proportional to the applied pulse width. Attempts have been made to concatenate multiple STMGs to implement a full adder circuit. The STMG operates at a smaller drive current compared to its CMOS counterpart, but with slower switching.

Majority gates with in-plane magnetic anisotropy have been demonstrated with Permalloy to have errors in the antiparallel configuration due to thermal noise introduced by the clocking field pulses. Hence, implementation with PMA are more stable and energy efficient.

Other types of implementation include a five-input majority gate with lateral spin valve, and a fabricated 3-input majority gate in which the input and output nanomagnetic logic devices are field-coupled together rather than monolithically integrated.

There is currently a lack of an efficient spin torque inverter (STI). It is also still difficult to cascade multiple STMGs, though some proposals exist. Because the optimal functioning of the STMG occurs below some critical sizes, more work needs to be done experimentally in patterning devices with smaller dimensions.

4. Emerging Device-Architecture Interaction

4.1. Introduction

Many new emerging Beyond-CMOS devices will require co-design between devices and higher levels of computer design (e.g., circuit, architecture and application). These emerging devices are not intended simply as “drop-in” replacements for standard CMOS devices, but will require new types of circuit designs, new functional module architectures, and even new software to best utilize the new devices’ capabilities.

Novel design issues that span the device and architecture levels especially need to be considered when adopting new low-level computing paradigms. Devices may be organized in radically new ways to carry out computation in a very different style from what we may consider the most “conventional” computing paradigm, which has relied on standard combinational and sequential irreversible Boolean logic. Examples of such unconventional or alternative computing paradigms include the following:

Analog computing (§4.2) – This broad category of non-digital computing paradigms uses physical phenomena to do the computing and includes the following:

- Crossbar Based Computing Architectures (§4.2.1): Several different computational kernels can be built on analog crossbars or memory arrays including matrix-vector multiplication (§4.2.1.1), outer product updates (§4.2.1.2), field programmable analog arrays (§4.2.1.3), crossbar based matrix solvers (§4.2.1.4), and ternary content addressable memory (§4.2.1.5). These crossbars perform low-precision matrix operations in parallel, by processing analog data directly at each memory element.
- Neuro-Inspired Computing (§4.2.2): These computing architectures take direct inspiration from the brain to develop more efficient systems. Local learning rules (§4.2.2.1) are a neuro-inspired method of training neural networks that keeps all communication local. Hyperdimensional computing (§4.2.2.2) is a cognitive computing model based on the high-dimensional properties of neural circuits in the brain. Spiking neural networks (§4.2.2.3) minimize communication energy by using sparse spike-based communications. Reservoir computing (§4.2.2.4) nonlinearly transforms time...
dependent signals into a new, random high-dimensional basis and then a conventional machine learning algorithm is used to make predictions from the new basis set.

![Figure BC4.1 Conventional vs. Alternative Computing Paradigms](image)

**Note:** The conventional computing paradigm is explicitly designed to be digital, deterministic, irreversible, and classical. Typical classical analog computing schemes (the focus of this section), including the neural approaches, relax the digital requirement while leaving determinism optional, and they are typically physically irreversible. In classic probabilistic computing, we abandon the requirement for determinism, while preserving the irreversible, digital nature of the computation. And typical classical reversible computing techniques maintain the digital and usually deterministic nature of computation while attempting to minimize irreversibility. Quantum computing machines, as they are conceived and engineered today, are highly thermodynamically irreversible at the system level, and many useful quantum algorithms are nondeterministic. Although achieving digital stabilization of quantum information via fault-tolerant error correction is a major goal of the field, it remains very challenging. Quantum machines that are also thermodynamically reversible at the system level are rarely considered, but may be conceivable.

- **Computing with Dynamical Systems** (§4.2.3): Analog dynamical systems can be used to solve a variety of problems. Optimization problems can be solved using simulated annealing (§4.2.3.1) or coupled-oscillator-based approaches (§4.2.3.2). Dynamical systems can be used to encode associative memories (§4.2.3.3) or to solve differential equations (§4.2.3.4). Chaotic logic can theoretically enable sub-\(kT\) computing (§4.2.3.5).
- **Analog Memory and Compute Devices** (§4.2.4): There are many different types of analog devices that form the building blocks of the computational kernels above. These devices include ReRAM, phase change memory, ion insertion redox transistors, floating gate transistors, capacitive or charge based analog devices, single flux quantum devices, photonic devices, magnetic devices, and more.

**Probabilistic/stochastic circuits** (§4.3) – Devices and circuits that produce truly nondeterministic or random outputs at the hardware level may be useful for accelerating probabilistic algorithms such as Monte Carlo or simulated annealing, for generating secure cryptographic keys, and for other applications.

**Reversible (adiabatic and/or ballistic) computing** (§4.4) – Computing paradigms that approach *logical and physical reversibility* offer the potential to greatly exceed the energy efficiency of all other approaches for general-purpose digital computation. While devices for reversible computing may perform fairly conventional functions (such as switching or oscillating), they should be optimized to utilize quasi-reversible physical processes such as near-adiabatic state transitions, near-ballistic signal propagation, highly elastic interactions, and highly underdamped oscillations. For maximal efficiency, circuits and architectures must approach reversibility at the logical as well as physical level. Careful fine-tuning and optimization of analog circuit characteristics (e.g., resonator quality factors, elasticity of ballistic interactions) remains a difficult and crucially important engineering challenge that must be met in order to fully realize the promise of the reversible computing paradigm. In the meantime, potentially commercially viable near-term applications of reversible computing are beginning to emerge for specialized cryogenic applications.

**Quantum computing** – Quantum computing offers the potential to carry out exponentially more efficient algorithms for a variety of specialized problem classes. Devices for quantum computing are very different from conventional devices, and fine-tuning device characteristics to avoid decoherence while organizing them effectively into scalable architectures has so far proved...
4.2. Analog Computing

Analog computing attempts to “let physics do the computation” by using physical processes directly (as opposed to, by going through the traditional digital abstraction barrier) to compute complex functions. Historically, this required inefficient analog circuitry for all elements, and expensive analog to digital conversion, resulting in limited applications, specifically those requiring analog signal processing. Recently, new analog devices have enabled a new generation of efficient analog architectures. This is especially true for hybrid analog and digital systems where efficient designs may exploit analog preprocessing and computation prior to digitization. Analog preprocessing can reduce the required A/D precision and therefore reduce the system energy consumption by orders of magnitude. Additionally, new architectures can be used for ultra-low-power co-processors for conventional CMOS designs. A key challenge is that analog signals are typically low-precision, with energy and latencies increasing exponentially with higher bit precision. Fortunately, many machine learning and other applications are being developed that can tolerate such lower precision computation.

In this subsection, we review a number of recent examples of analog computational technologies, starting at the architectural level with (in §4.2.1) some currently popular neural-inspired architectures that also have broader applications in linear algebra. Then §4.2.2 broadens the scope to other neural-inspired computing approaches, and §4.2.3 looks at an even broader variety of approaches to “physical computing” with analog dynamical systems. Finally, §4.2.4 reviews device technologies that have some utility in the context of one more of the various analog architectures.

4.2.1. Crossbar-Based Computing Architectures

Analog crossbars or memory arrays can perform low-precision matrix operations in parallel, by processing analog data directly at each memory element. Thus, in 1990, Carver Mead projected that custom analog matrix vector multiplications would be thousands of times more energy efficient than custom digital computation. Because a digital memory must individually access each memory cell and move the data to a separate computation unit, digital systems consume more energy and incur longer latencies. Computing on larger crossbars/matrices allows for any analog overhead to be averaged out over many matrix elements. Any two- or three-terminal device that features a modifiable internal physical state variable (which might be, for example, a variable resistance, a variable capacitance, a stored charge, or a stored magnetic field) that modifies the device’s behavior can be used as a building block for analog operations. Several different types of crossbar architectures are summarized in the following sections.

4.2.1.1. Matrix Vector Multiplication (MVM) and Vector Matrix Multiplication (VMM)

MVM and VMM are key computational kernels underlying many different algorithms. There are several approaches to accelerating these kernels. Any programmable resistor such as a two-terminal resistive memory or a three-terminal floating gate cell can be used. Alternatively, a capacitive MVM can be designed by adding charge from capacitive memory elements.

For many algorithms such as neural network inference (of an already-trained network), accelerating MVM accelerates the bulk of the computation, allowing for large system level gains. An \( N \times N \) crossbar accelerates \( O(N^2) \) operations, leaving only \( O(N) \) inputs and outputs that need to be processed and communicated. This allows each unit of communication and processing costs to be amortized over \( N \) memory elements. This changes the tradeoff for some neural-network algorithms as larger crossbars are more efficient than smaller ones.

Analog VMMs have been used for experimental demonstration of threshold logic, compressed sensing initial filtering, robotic navigation and control, adaptive filtering, Fourier transforms and more. Additionally, Analog VMM techniques have been used for ultra-low power classification and neural networks.

4.2.1.1.1. Resistive MVM and VMM

Resistive MVMs are based on using Ohm’s law, \( V = I \times R \), to perform multiplication, and Kirchhoff’s current law to perform addition by summing currents. Programmable resistors are used to program the weights. Arranging the memory elements in an array allows for the entire operation to be performed in a single parallel step, giving a fundamental \( O(N) \) energy and latency advantage over a standard digital memory that, at best, must access a memory array one row at a time. An MVM and the transpose VMM can be performed on the same memory array, by changing whether the rows of an array are driven and the columns are read, or vice versa.
The key metrics for a resistive MVM are 1) the energy per multiply-accumulate (MAC), 2) latency per MVM, 3) crossbar and supporting circuitry area per matrix element, 4) crossbar dimensions, 5) input/output bit precision for digitally driven MVMs, and 5) the standard deviation of the noise or error per weight when programmed as a percentage of the weight range.

If high-resistance memory elements \( (R_{\text{on}} = 100 \, \text{M}\Omega) \) with good analog properties are developed, one ReRAM based crossbar design projects that each multiply and accumulate operation will require 12 fJ when using 8-bit A/Ds and only 0.4 fJ when using 2-bit A/Ds.\(^{720}\) The latency for a 1024 \times 1024 MVM will only be 384 ns or 11 ns for 8-bit or 2-bit A/Ds respectively. This is over 100x better than an optimized SRAM-based accelerator, which would require 2,700 fJ and 4,000 ns for 8 bits. The area per weight for the 8-bit A/D ReRAM accelerator is 0.05 \( \mu \text{m}^2 \), 16x better than the 0.8 \( \mu \text{m}^2 \) needed for an SRAM accelerator. The energy and latency are dominated by the A/D circuitry and not by the crossbar itself, with the A/D converters and digital circuitry occupying 10x the area of the ReRAM array itself.

To allow for large arrays and minimize parasitic resistance drops, high resistance (~100 M\( \Omega \)) memory elements are needed. The higher the resistance, the larger the array possible, and the more any A/D costs and system level communication costs are amortized out. However, such high resistances would prolong and potentially complicate the process of programming each conductance value accurately to encode already-trained neural network weights or matrix element values.

A key design choice is the bit precision of the inputs and outputs to the crossbar. The fewer bits are needed by an algorithm, the more efficient the crossbar is. If analog or binary inputs/outputs can be used, the A/D costs can also be avoided. The inputs to the crossbar can be encoded in voltage, time, or digitally. Voltage encoding applies different voltages to represent different analog input values. This requires circuitry to create different input voltages, and it requires that the memory elements have a linear I-V relationship, greatly complicating the use of nonlinear access devices.\(^{721}\) Encoding inputs in variable length pulses requires longer reads and an integrator to sum the resulting current. Digital encoding applies each bit of the input sequentially and then combines the result digitally. For digital encoding, the usefulness of the lower-order bits in the input is limited by the noise/errors on the highest-order bit. To save on ADC costs, each bit position can also be combined in analog using successive integration and rescaling.\(^ {722}\)

The precision with which each resistor needs to be programmed depends on the application. For neural network inference, the algorithm can be robust to read noise of up to 5% of the weight range or more.\(^ {723}\) To extend the precision of computation beyond the limits of reliable programming, a technique called bit slicing can be used.\(^ {724}\) With bit slicing, a matrix of wide operands is striped across multiple crossbars, enabling the crossbars to collectively perform computation on arbitrarily wide operands at the cost of additional digital circuitry to reduce partial results from multiple bit slices. When bit slicing is combined with digital input encoding, each bit of the input must be applied to each slice, analogous to multibit scalar multiplication. Leveraging bit slicing, accelerators for a wide range of applications have been proposed, including combinatorial optimization,\(^ {724}\) neural network inference,\(^ {725,726}\) graph analytics,\(^ {727}\) and scientific computing.\(^ {728}\)

### 4.2.1.2. Outer Product Update (OPU)

Analog resistive memory crossbars can also perform a parallel write or an outer product, rank 1 update where all the weights are incremented by the outer product of a vector applied to the rows and a different vector applied to the columns. This is a key kernel for many learning algorithms such as backpropagation\(^ {723}\) and sparse coding.\(^ {719,729}\) Row inputs are encoded in time and column inputs are encoded in either time\(^ {726}\) or voltage.\(^ {723}\)

When a VMM and MVM are combined on the same crossbar, extremely efficient learning accelerators can be designed.\(^ {720,730,731}\) with the potential to be 100–1000x more energy efficient and faster than an optimized digital ReRAM or SRAM based accelerator.\(^ {720}\)

The same figures of merit and design considerations for a VMM apply to the OPU. Additionally, the 1) write noise and 2) asymmetric write nonlinearity are important for determining how well a learning algorithm will perform. The 3) ability to withstand failures, and 4) endurance are also important for training systems. To have an efficient learning accelerator, parallel blind updates are needed where weights are updated without knowing the previous value and without verifying that the correct value is written. To obtain ideal accuracies, a low write noise is needed, less than 0.4% of the weight range. Even more important is having low asymmetries in the write process. The change in conductance for a positive pulse should be the same as that for a negative pulse for all starting states.\(^ {723}\) Often the conductance will saturate near a maximum where a positive pulse will not change the conductance, while a single negative pulse will cause a large decrease in conductance. This significantly lowers accuracy as it only takes a single negative write pulse to cancel many positive pulses.

Several devices have been examined for neural network training, including phase change memory,\(^ {730}\) resistive memory\(^ {720,732}\) and novel lithium-based devices.\(^ {733,734}\) Currently no devices meet all the ideal requirements for training (high resistance >10 M\( \Omega \), low write noise <0.4%, low write asymmetry).\(^ {725}\) Nevertheless, algorithmic approaches such as periodic carry,\(^ {735}\) Local Gains,\(^ {736}\) Tiki-Taka,\(^ {737}\) or the inclusion of semi-volatile capacitor-on-gate devices\(^ {738}\) can be used to help compensate and achieve ideal...
accuracies. Several co-design tools have been developed to model the impact of device level properties on algorithmic performance,\textsuperscript{730, 739, 740} which have allowed for the algorithmic development needed. Additionally, lower resistance devices can be used to give smaller near-term gains in performance.

The need for high on-state resistance and good analog characteristics means that filamentary resistive memories may not work as well as non-filamentary devices. A resistance higher than a quantum of conductance, 13 kΩ, requires current to tunnel through a barrier. This presents a fundamental problem for a filamentary device: a single atom can halve the tunneling barrier, resulting in huge variability and poor analog characteristics.

### 4.2.1.3. Large-Scale Field Programmable Analog Arrays (FPAAs)

A field programmable analog array has configurable analog components, digital components, configurable interconnects between those components and off-chip communications.\textsuperscript{741, 742, 743} FPAAs allow users to build analog applications without having expertise in IC design. FPA\textsuperscript{A} I/O lines can transmit or receive analog signals, digital signals and create direct connection lines typical of analog circuits. The routing between analog and digital blocks can occur between the blocks of devices, with converters between these blocks, or more finely connected heterogeneous analog and digital component populations. The components are often organized into regions called computational analog blocks (CABs). CAB components vary considerably between implementations but often include nFET and pFET transistors, transconductance amplifiers [TA or operational transconductance amplifier (OTA)], other amplifiers, passives (e.g., capacitors), as well as more complicated elements (e.g., multipliers). The most advanced FPAAs to date utilize Floating-Gate (FG) devices, dramatically improving the analog parameter storage and therefore the resulting computational capability.\textsuperscript{744} FPAAs include aspects of digital computation, such as FPGA blocks or shift registers or microprocessors, to complete the full end-to-end configurable system.\textsuperscript{744}

The fundamental breakthrough was recognizing that a switch matrix of single floating gate elements could be used for analog computation. The routing crossbar networks were, in fact, crossbar networks that could support VMM and other computations.\textsuperscript{745} Routing was no longer dead weight, as perceived for FPGA architectures. The floating gate cells could also allow for mismatch calibration at the mismatch source.\textsuperscript{746, 747} The density for VMM in FPA\textsuperscript{A} architectures is nearly the level of custom IC design. These analog computations can be made robust to temperature fluctuations.\textsuperscript{748} These techniques have been utilized by a number of students in university courses.\textsuperscript{749, 750} FP\textsuperscript{A} Based VMMs can be scaled to small geometry (e.g. 40 nm and smaller) and operated at RF frequencies.\textsuperscript{751, 752} FPAAs have been used for command-word recognition in less than 23 μW with standard digital interfaces.\textsuperscript{743} The full classification results in less than 1 μJ per classification (or inference), which has 1000× improvement over similar digital neuromorphic solutions requiring roughly 1 mJ or higher for just an inference.\textsuperscript{753}

### 4.2.1.4. Resistive Memory Crossbar Solver

Resistive memory crossbars can be used to solve matrix problems, such as the linear system of equations \( Ax = b \), where \( x \) is the unknown vector and \( b \) is the known vector, represented by output voltage and input current, respectively, in Figure BC4.2(a).\textsuperscript{754, 755} Each resistive memory element is a programmable resistor that represents an element in the coefficient matrix \( A \). (Alternatively, any programmable analog element can also be used.) The equation \( Ax = b \) can be mapped to Ohm’s law, \( \sum G_{ij}(V_j - V_i) = I_i \). The \( V_i \) are set to zero by the virtual ground of the op-amps. Currents, \( I_i \), are applied to the crossbar and the resulting voltages, \( V_j \), are measured. The op-amps provide feedback allowing the \( V_j \) to be determined.

\[
-A \cdot V = I \\
-A \cdot V/G = -V \Rightarrow A \cdot V = G \cdot V
\]

**Figure BC4.2** A Resistive Memory Crossbar \( Ax = b \) Solver is Illustrated

*Note: The op-amps are used to provide feedback to find the solution and force the row voltages to zero.*
Similarly, eigenvectors of a matrix $A$ can be calculated according to the circuit in Figure BC4.2(b). Here, the maximum eigenvalue is mapped in the feedback conductance $G_{\lambda}$, while the voltage yields the corresponding eigenvector $x$. To solve problems with positive/negative coefficients in $A$, two crossbars can be used in the circuits of Fig. BC4.2. In all cases, crossbar solvers yield their solution in one computational step, without any iteration, and the solution is generally obtained in less than 1 $\mu$s, depending on the poles of the analogue feedback circuit. The same scheme can be extended to one-shot learning by linear/logistic regression.

The biggest challenge in taking advantage of analog solvers for HPC is that analog operations only offer low precision, ~8 bits fixed point, while HPC applications often demand 32 or more bits of floating-point precision. This can be potentially overcome by hybrid analog/digital systems where the computationally intense parts of a calculation can be done in analog, while the required precision can be achieved by refining the solution in digital using a method with lower computational complexity. This allows for some digital computation, while still getting a reduction in the overall computational complexity. The precision can potentially be improved by using iterative refinement or by using the crossbar to initialize a digital solver. The analog solution can also be used as a preconditioner within a Krylov method like CG or GMRES. Large matrices can be broken down into smaller blocks compatible with the accelerator and scaling can be used to compensate for finite on/off ranges. Work is still needed to show how noisy crossbar solvers can be used with ill-conditioned matrices. In general, iterative refinement will only converge if the noise is less than $1/\kappa$ where $\kappa$ is the condition number of a matrix.

### 4.2.1.5. TERNARY CONTENT ADDRESSABLE MEMORY (TCAM)

Similar to resistive crossbar arrays, content addressable memory (CAM) arrays operate in a highly parallel manner but have a distinct operation which compares a given search word to a set of stored words in parallel within the circuit, and returns the index of the matched entry. This CAM array compare operation takes only one or a few clock cycles, enabling massively parallel high-throughput and low-latency lookups. In addition, Ternary CAMs (TCAMs) have the additional functionality of storing a “don’t care” or “X” value which acts as a wildcard to match regardless of input, enabling compression of stored CAM entries. While very powerful, today’s CAMs based on SRAM suffer from high cost, area, and power, limiting their modern usage to networking (QOS/ACL/IP routing lookup tables) and applications which must trade-off power and cost for high throughput and speed.

To address this gap, a significant body of work has developed TCAM circuits using ReRAM or non-volatile memory (NVM) devices to replace the large and power-hungry SRAM storage devices in conventional CAM circuits for reduced power and area, and potential for larger array sizes. Work on design, simulation and physical silicon tapeouts have been conducted for phase change memory, metal-oxide memristors, and spin-transfer torque devices. While several designs have drastically reduced the transistor count per TCAM cell (conventional 16T reduced to 4T, 3T, 2T versions), the limited ON-OFF ratio of NVM and the relatively high device conductance has led to larger power consumption than desired originating from high DC currents during search operations and design work is still underway to optimize area (i.e. transistor count), power and device requirements (ON-OFF ratio, write voltage and conductance state stability). Key challenges for the practical realization of TCAM arrays remain, such as the need for highly reliable devices, error correction schemes, scaling of array sizes and balance of devices requirements (ON-OFF ratio, write voltages) and latency-power optimization for different use cases. For example, smaller ON-OFF ratios can lead to longer latency but may be beneficial for certain applications. Despite these challenges, recent work in this area is promising with competitive reported values of 0.5 fJ/bit/search and as NVM technologies become more available at commercial foundries, further performance improvements and tuning of NVM CAM circuits are anticipated.

In addition, as increasing work on NVM CAM circuits progresses sufficiently to lower the (power/area) barrier to widespread usage, the development of NVM TCAM circuits as a new in-memory computation primitive presents great potential in future computing systems. Like with the much-studied resistive crossbar array architecture, the large performance benefit for using CAMs in in-memory computation comes from the vast reduction of data movement for target applications with large numbers of compare or lookup operations. While resistive arrays enable in-situ vector-matrix multiplication acceleration for applications in areas such as machine learning, analog signal processing, and scientific computing, CAM circuits provide an orthogonal functionality. Recent work in this area has proposed using CAMs as in-memory computation blocks for applications such as associative processing, approximate computing, spiking NNs, string matching and regular expression matching finite state machines. Further application areas are expected to emerge as NVM CAM circuits mature to make their use advantageous compared to GPU and FPGA approaches.

### 4.2.2. NEURAL-INSPIRED COMPUTING

There are several characteristics of how the brain computes that have been proposed for efficient computing technologies. Architecturally, there are two attractive approaches: processing in memory, which is analogous to the analog computation that occurs at synapses within the brain, and event-based communication, which is analogous to neuronal spiking. Both approaches potentially yield considerable energy savings, and the brain clearly benefits from both. As discussed
in §4.2.1, analog crossbars can be used as building blocks for conventional neural networks to give significant improvements in energy, latency and area over digital accelerators. For accelerators specialized to a particular algorithm, various analog neurons can be used to process the crossbar outputs and avoid the need for and high cost of analog-to-digital conversion.

There is also a lot of work on more biologically inspired neural hardware. For biologically inspired neurons, connections are often designed to be persistent on short timescales, but (depending on the model) may exhibit mutability/plasticity in their strength and/or topology on longer timescales to facilitate, for example, adaptive in-situ learning. Connections between neurons can be modeled as discrete events or spikes (often implemented using an address event representation) or continuous-valued analog signals such as voltage or current. A key challenge for more biologically inspired architectures is the need for algorithmic co-design. For many neuro-inspired computational models, further research is needed to demonstrate state of the art machine-learning performance.

4.2.2.1. Local Learning Rules

Recent breakthroughs suggest that local, approximate gradient descent learning is compatible with Spiking Neural Networks (SNNs) implemented in neuromorphic hardware.\(^{774,775,776,777,778,779}\) Spiking neural networks can be viewed as a type of recurrent neural network, where activities are binary and recurrence is both due to connections and the leak of the neurons.\(^{772}\) This analogy enables the transfer of algorithms of deep learning into local synaptic plasticity dynamics in SNNs. The synaptic plasticity dynamics that result from these derivations are “three-factor rules.” Three factor rules are popular among computational neuroscientists for reward-based learning.

Credit assignment for (deep) hidden parameters in SNNs under tight constraints of information locality is a very challenging issue. All states other than spikes, such as neurotransmitter concentrations, synaptic states, and membrane potentials are local to the neuron. If a non-local quantity is required for a computational process (e.g. learning), a communication channel is required to convey it.\(^{780}\) The cost of this channel is non-negligible regardless of the substrate: axons (white matter) take up most of the volume in the brain. Similarly, in modern computers, data movement is the major energy requirement.\(^{781}\)

One strategy is to train a SNN using local loss functions and the three-factor rule. An example of a loss function that is local to the layer of neurons\(^{773}\) is shown in Figure BC4.3 in diamonds. Local loss functions can be either designed,\(^{782,783}\) trained using Back-Propagation (BP)\(^{784}\) or evolved.\(^{778}\)

Using this approach, it is possible to perform learning in crossbar arrays using temporal dynamics of SNNs in an error-triggered fashion.\(^{785}\) Furthermore, the mathematical derivation shows that circuits used for inference and training dynamics can be shared, which renders the learning circuits insensitive to the mismatch in the peripheral circuits. Using error-triggered learning, the number of updates can be reduced a hundredfold compared to the standard rule while achieving performances that are on par with the state-of-the-art.

![Figure BC4.3](image)

**Figure BC4.3** A Spiking CNN for Gesture Recognition with Local Learning

*Note: (Left) Deep Continuous Local Learning (DECOLLE) network for gesture recognition. DECOLLE is a forward trained spiking Convolutional Neural Network (CNN) using local loss functions. The network consisted of three convolutional layers with max-pooling. A local classifier (colored diamond) is attached to every layer via a fixed random projection, i.e. each layer is trained to classify the gesture. The fixed random projection enables the network to find increasingly disentangled representations as the data flows through the hierarchy. DECOLLE is fed with 1-ms integer frames recorded from a neuromorphic vision sensor. (Right) Classification Error for the DvsGesture task during learning for all local errors associated with the convolutional layers. C3D is a 3D CNN commonly used for sequence learning.\(^{786}\) See Ref. 775 for details.*

4.2.2.2. Hyperdimensional Computing

Hyperdimensional (HD) computing is a cognitive computing model based on the high-dimensional properties of neural circuits in the brain.\(^{787}\) Information is encoded into high-dimensional distributed representations in the form of high-dimensional vectors or hypervectors.\(^{787,788}\) A hypervector distributes information uniformly across all of its dimensions, resulting in a distributed or
holo
graphic representation. This contrasts with conventional positional representations in which different digits or bits can convey vastly different amounts of information depending on their position. Consequently, incurring bit errors in particular positions can result in catastrophic failure. In contrast, the distributive nature of hypervectors combined with high dimensionality provides a robustness to bit errors: errors that occur in any dimension result in the same information loss, and this information loss is small due to the large number of dimensions. Thus, HD computers exhibit graceful degradation as hardware components fail, analogous to in the brain when neurons die.

Computation is performed by systematically transforming hypervectors into other hypervectors (i.e., closure is satisfied) using operations such as multiplication, addition, and permutation. Due to the distributed nature of hypervectors, these operations become local to individual dimensions (or bits, in the case of binary hypervectors). Multiplication, for example, becomes element-wise multiplication and can be used to “bind” hypervectors together into a single hypervector representing a key-value pair. Multiplying by the multiplicative inverse of the key hypervector will “unbind” the key hypervector from its corresponding value hypervector. Similarly, other operations such as addition and permutation can be used to construct sets and sequences respectively. These simple operations together enable the construction of more complex compositional representations, which are ultimately stored in an autoassociative memory for item “cleanup” as hypervectors become noisy during computation.

Constructing a physical HD computer will require innovations at all levels of the computing stack but could result in an energy efficient “thinking” machine. The robustness to noise and bit errors provided by the high-dimensional distributed representations reduces requirements on signal-to-noise ratio. This enables lower supply voltages and greater tolerance for device variability than in conventional computers. Furthermore, HD computing operations are local to individual digits or bits and are, consequently, highly parallelizable. The trade-off is large word sizes, which necessitate processing-in-memory. Fortunately, HD computing algorithms are geared towards one-shot or few-shot learning and do not require frequent weight updates. As a result, hypervectors may lie dormant for extended periods of time, allowing for a greater portion of inactive components for reduced power consumption.

### 4.2.2.3. Spiking-based Neural Networks (SNNs)

Like the brain which couples both the processing in memory and spike-based communication for maximal space and energy efficiency, a good spiking based neural network needs to couple both. Ultimately, the spiking function by neurons has two features that must be captured by a proposed device or circuit: its non-linearity and its efficient long-distance communication. First, it must accomplish the analog-to-spiking conversion, which in its simplest form is a compact 1-bit analog-to-digital conversion, but ideally would also enable holding some additional state or history from the analog inputs. There have been many proposed devices for spiking neurons including neuristors, spin torque based devices, stochastic phase change neurons, and others. Second, future spiking systems must be able to communicate this information efficiently to downstream neurons.

Currently, CMOS systems rely on event-driven communication of packets that contain some source or destination address relevant to routing the spike to appropriate destinations. Thus, CMOS systems do benefit from the relative rarity of the communication (only transmit when an event occurs), and are already achieving considerable savings from that, but do not benefit significantly from the theoretical 1-bit precision of the spike as a multibit address is needed. In this respect, more efficient mechanisms for direct point to point communication, such as superconducting systems, 3D-nanowires, or perhaps optical interconnects are needed. The challenge in these systems is how to achieve the necessary level of fan-in / fan-out (i.e., number of synapses per neuron) between non-local regions and how to deliver that information in a suitable form for processing in the analog memory circuits used as synapses.

### 4.2.2.4. Hardware-Based Reservoir Computing and Liquid State Machines

Software-based reservoir computing (RC) arose from the surprising insight that a single randomly connected recurrent neural network can be tailored to solve various tasks solely by means of adjusting its output weights. Time dependent signals are nonlinearly transformed into a new, random high-dimensional basis and then a conventional machine learning algorithm is used to make predictions from the new basis set. Hardware-based RC uses physical systems whose temporal evolution—much as in dynamical systems computing (see §4.2.3 below) — form the basis of computation. Such hardware need not implement tunable weights that add considerable complexity to hardware accelerators of neural networks. These systems are well-suited to time-series data processing and forecasting tasks such as learning to emulate a chaotic attractor, though they are generally limited to supervised learning. Naturally a wide variety of systems have been pressed into service as reservoirs, including photonic, mechanical, electronic, spintronic and more recently superconducting systems among many others. An active area of research is extending RC into the quantum regime whose large Hilbert space dimensions may afford additional reservoir performance. Spiking neural networks (see sec. 4.2.2.3 above) can also be used for RC, though this is typically referred to
as liquid state machine (LSM) computing.\textsuperscript{816} The possibility also exists to create “deep” hardware RC architectures,\textsuperscript{817} and to otherwise combine RCs with other novel computing paradigms in order to combine their strengths.

Other approaches such as recurrent neural networks (and structured variants such as long short-term memory) are also suitable for processing temporal data. However, these approaches are difficult to train and may struggle with complex nonlinear dynamics across many timescales.

4.2.3. \textbf{Computing with Dynamical Systems}

In computing with dynamical systems, the built-in dynamical behavior of a physical system exhibiting continuous degrees of freedom is used to compute. The entire computational process can be analog, with only the results being digitized. The following subsections give a few examples of different types of dynamical systems-based approaches. Also exemplifying this category are the hardware-based reservoir computing or liquid-state machines, which were already discussed above in §4.2.2.4.

Although some of the below methods target NP-hard problems and provide approximate solutions, it’s important to note that, to date, no general physical computing method (including analog and quantum approaches) has yet been clearly demonstrated to be capable of exactly solving NP-hard problems without requiring exponential physical resources (energy and/or time) to be invested in the physical process performing the computation. The prevailing belief among computational complexity theorists\textsuperscript{818} is that solving NP-hard problems efficiently would require uncovering new physics (\textit{i.e.}, beyond standard quantum mechanics). (Note that quantum computers can efficiently solve prime factorization since it is not believed to be an NP-hard problem)

4.2.3.1. \textbf{Stochastic/Chaotic Optimization—Simulated Annealing}

Many of the optimization problems that are found in modern operations research—such as routing, scheduling, and other types of resource allocation—are intractably hard. Consider this example: finding an optimal route among three cities can be done using the digits on two hands, but with 15 cities, we are left with more than 40 billion routes to choose from. As the size of the problem grows, the resources needed to solve the problem increases exponentially. Finding even approximate solutions to large combinatorial optimization problems are prohibitively resource-intensive with the best supercomputers we have. Exact solutions to these problems are known in computational complexity theory to be NP-hard (non-deterministic polynomial time hard), meaning that it is too hard for any computer, analog or digital, to solve exactly, in general, and specifically at large scale. However, there are many ways to compute approximate solutions, meaning finding a good solution but not necessarily the best one. In recognition of this, there have been many analog hardware approaches that exploit the inherent computational ability and parallelism in physical processes to solve these hard optimization problems.

An example solution uses energy minimization using multiple runs on a Hopfield network.\textsuperscript{819} A Hopfield network is a popular neural network with its output being calculated via a simple decision system (e.g.: thresholding of input), which is then weighted and fed back to its input. The feedback weights define an energy landscape based on values emerging from the output. If a Hopfield network is initialized to a particular value, the network will follow a trajectory that will take it to a minimum, or local minimum, of the energy landscape.

As an example, consider using a Hopfield network to solve the Traveling Salesman Problem. The Traveling Salesman Problem is to find the best route for a salesman that needs to visit a series of cities, each pair separated by some distance. The salesman seeks the shortest route that visits each city exactly once and then returns to the starting city. In an analog system the weights are set to encode the intercity distances. The system drives the outputs to a starting point for the salesman’s route. The system will settle into a candidate salesman’s route in an amount of time equal to a few time constants of the feedback loop.

The method described above may find the ideal solution, or just a better but suboptimal solution. To improve the odds of finding the best solution, the circuit can include either a true random noise generator or a chaotic pseudo-random noise generator. Under control of an external digital computer, the Hopfield network is driven to a random starting point and released many times in a cycle. The randomness causes many of the starting points to be different, making it more likely that the system will find the global minimum. The digital computer collects all the results, checking each to see which is best.

Such a system leverages multiple new circuit blocks including both a crossbar to encode the n intercity distances (that can be built using memristors), an analog neuron to run the Hopfield network and either chaos or noise generator to get randomness. As the Traveling Salesman problem is NP-hard, no solution method can solve it exactly at scale. Nevertheless, the analog solution seems to be at least comparable in efficiency with some software algorithms. For instance, a memristor based Hopfield network has been built.\textsuperscript{820}

Another important application for combinatorial optimization, specifically graph coloring, was described\textsuperscript{821} and developed theoretically with support from experimental demonstrations using relaxation oscillators based on phase-change insulator-metal transition (IMT) materials. An architecture based on non-repeating phase relations\textsuperscript{822} between fabricated CMOS oscillators tries to emulate stochastic local search (SLS) for constraint satisfaction problems.
4.2.3.2. Coupled-Oscillator Based Optimization

Coupled-oscillator machines are another class of analog accelerators for combinatorial optimization that share a similar architecture: they are composed of a network of decentralized nonlinear oscillators, and the programmable strength of the coupling between them encodes the specific problem to be solved. These networks have been proposed and demonstrated with electrical, \(^{823,824,825,826,827}\) optical \(^{828,829,830}\) and electromechanical \(^{831}\) oscillators. These systems are often called “Ising machines” because they map readily to the Ising graph optimization problem, with each oscillator representing one bistable spin. Any combinatorial optimization problem can be converted into an equivalent Ising problem that is programmed onto and solved by the machine. The energy minima of such networks correspond to the solutions of an NP-hard combinatorial optimization problem and can model other NP-hard problems as well.\(^{827}\)

Networks of coupled oscillators have been shown to embed the energy (cost function) of the Ising problem in their physical dynamics and relax to configurations that minimize this energy. They can thus rapidly sample the local minima of a problem,\(^{824}\) and can potentially also be used to arrive at solutions close to the global minimum.\(^{823,826}\) The sampling speed is determined fundamentally by the oscillator frequency. The accuracy of the different architectures has been benchmarked using large instances of the Ising or Max-Cut problems generated by the operations research community. Solutions have been found that match those obtained by state-of-the-art digital algorithms.\(^{825,828}\) Energy and delay benchmarking remain a future step.

Of the proposed coupled oscillator optimization schemes, the systems which use electrical (LC) or electronic (ring oscillator) oscillators are the most compatible with CMOS technology. Since the Ising problem is specified by a connectivity matrix, the oscillators can be densely connected using a resistive crossbar.\(^{823,826}\) In these networks, the oscillators take on a discrete nature by synchronizing to a second-harmonic master oscillator through a circuit nonlinearity. The nonlinear oscillator properties can be easily provided by semiconductor components such as diodes, MOS capacitors, or amplifiers. In fact, phase-based Boolean computing using such nonlinear oscillator circuits was proposed decades ago.\(^{832}\)

The physical limits of coupled oscillator systems are governed by the achievable level of weight precision and circuit delay. The resistive connections must be linear, programmable to high precision, and have minimal drift. The precision and retention of the resistive connections limit the accuracy to which a problem can be programmed onto the hardware, and the precision requirements for an adequate representation increase with problem size. For very large problems, device or process limitations will impose an upper bound on the quality of the solution: the target error bound depends on the application, but it must be superior to bounds that are guaranteed by digital approximation algorithms. Since a coupled oscillator network relies on synchronization between the oscillators, signal delays can also impact performance, especially in high-frequency circuits needed for rapid optimization. In particular, variability in the distribution delay of the second-harmonic master oscillator by more than a half-cycle are detrimental: this will be a significant problem in large networks. To this end, architectures have been proposed that separate the oscillators in time rather than space,\(^{829}\) but this comes at the loss of continuous-time communication among the oscillators, leading to slower convergence.

Related constraint satisfaction systems have been built.\(^{833}\) An interesting approach based on memory co-processors was introduced as Memcomputing.\(^{834}\) Useful insights can also be obtained by looking into dynamical systems like iterated maps,\(^{835}\) and 0-1 continuous reformulations of discrete optimization problems.\(^{836}\)

4.2.3.3. Associative Memories

Hopfield networks are attractor networks proposed for associative memories\(^{837}\) where the fixed points (or stable states) of the system correspond to memories, and the dynamics of the network is such that the system settles to the fixed point which is closest to the initial state the system starts from. \(^{838,839,840}\) These networks can be implemented with coupled oscillators.

The associative memory application is widely used in the tasks of voice and image recognition, which can be performed in a cellular neural network architecture.\(^{841,842}\) Five decimal digits, ‘1’–‘5’, are associated with the other five digits, ‘6’–‘0’. Hebbian learning is used for storing patterns.\(^{843}\) Patterns with noisy input pixels can still be recalled. The delay per cellular neural network operation is dependent on the input pattern, input noise, and thermal noise.

A key challenge for oscillator-based associative memories is storage capacity. \(^{844}\) A fully connected net with \(N\) units can only store around 0.15\(N\) memories while requiring \(N^2\) weights, resulting in a poor memory density.

4.2.3.3.1. Cellular Neural Networks

The cellular neural network,\(^{845}\) (CeNN) is a non-Boolean computing architecture that contains an array of computing cells that are connected to nearby cells. Since interconnects are major limitations in modern VLSI systems, CeNN systems take advantage of the local communication and encounter fewer constraints imposed by interconnects. The CeNN is a brain-inspired computing architecture that relies on neurons to integrate the incoming currents. The accumulated and activated output signal drives nearby neurons through weighted synapses. CeNNs can be used to create associative memories for voice and image recognition.
CMOS based CeNNs can be implemented by analog circuits using operational amplifiers and operational transconductance amplifiers (OTAs) as neurons and synapses, respectively. Some recent work has also investigated CeNN using beyond-CMOS charge-based devices, such as TFETs, to potentially improve energy efficiency thanks to their steep subthreshold slope and low operating voltage.

Using novel devices such as all-spin logic (ASL) charge-coupled spin logic (CSL), and domain wall logic (mLogic) whose dynamics match the dynamical state of cells in CeNN can be far more efficient than op-amp and OTA based CeNNs. The use of these different devices has been benchmarked. It was shown that the digital CeNNs are quite power hungry and slow. This is because multiple cycles are required to read out the weights from the register and perform the summation in the adder, which is energy and time consuming. In general, analog CeNNs implemented by TFETs dissipate less energy thanks to their steep subthreshold slope and lower supply voltage. In contrast to Boolean circuits, spintronic devices are more competitive. This is because a single magnet can mimic the functionality of a neuron, and these spintronic devices operate at a low supply voltage. The domain wall device provides the best performance, in terms of Energy-Delay Product, thanks to its low critical current requirement.

4.2.3.4. **Differential Equation Modeling**

Analog computation aligns well with the solution of differential equations, both Ordinary Differential Equations (ODE) and Partial Differential Equations (PDE). A key limitation of digital ODE and PDE solution accuracy is the need to discretize time and amplitude. Continuous time analog solutions eliminate this. Analog summation by charge or current is also ideal and not subject to round off error. Similarly, analog integration can be ideal and is typically performed as a current sum on a capacitor. The result of the final computation will have some noise distortion, but the noise is added at the end of the resulting computation and does not affect the core numerics.

Analog computation builds on an analog numerical analysis techniques, analog algorithm complexity theory, where these directions provide guidance on the relative numerical performance, as well as relative architectural performance, for designs abstracted at multiple levels of representation, respectively. Analog solution of differential equation computes using real valued quantities, often computing over continuous amplitude and time.

Analog solution of PDEs often utilize spatially coupled ODEs where the physical system is continuous in space, but practically the parameters change in discrete points with a finite granularity of parameter resolution setting, as well as output measurement capability. Often differential equations are solved using programmable and reconfigurable techniques enabling utilization of many coupled ODEs or PDEs operating over a range of room-temperature conditions. Differential equations have also been mapped to cellular automata-based networks.

Solving an application in analog such as the optimization problems in Section 4.2.3.2, can be thought of as solving a differential equation. These analog solutions involve a transformation between the physical system to be computed to the analog computing substrate. Efficient transformation to an analog computing system can result in a 1000x or larger computational efficiency improvement compared to similar digital approaches. Differential equations utilize superposition over the linear operating region of the particular physics being used. Computational complexity when solving applications using differential equations is still unclear. Although it seems likely that real-valued analog solutions provide an improved computational ability over standard, discrete-valued Turing machines, as of this writing, such capabilities have not been convincingly experimentally demonstrated to date and is an active research area. As a result, physical algorithms, such as the recently proposed ODEs to solve the 3-SAT problem must be developed and verified only through physical hardware, and not discrete simulation or analysis of physical algorithms.

4.2.3.5. **Sub-KT Chaotic Logic and Chaos Computing**

Shannon’s noisy channel coding theorem shows that one can reliably communicate information on a channel subject to noise (at a sufficiently low bitrate) even when the transmitted signal power is below the noise floor (i.e., at a signal-to-noise ratio of less than 1). Moreover, any computational process can be viewed as just a special case of a communication channel, namely, one that simply happens to transform the encoded data in transit—since the derivation of Shannon’s theorem relies solely on counting distinguishable signals, and nothing about how the signals are being counted in Shannon’s argument precludes the encoded data from being transformed as it passes through the channel. This observation suggests that performing reliable computation utilizing signal energies (that is, energies associated with the information-bearing variability in the dynamical degrees of freedom in the system) that are at average levels \( \ll kT \) (i.e., well below the thermal noise floor) should theoretically also be possible—although the output bit rate (per unit signal bandwidth) will scale down with the average signal energy.

In 2016, Frank and DeBenedictis investigated a theoretical approach for implementing digital computation using chaotic dynamical systems which provided evidence that the above theoretical observation is correct. In that approach, the long-term average value of a chaotically evolving dynamical degree of freedom encodes a digital bit. The interactions between degrees
of freedom are tailored such that the bit-values represented by different degrees of freedom correspond to the results that would be computed in an ordinary Boolean circuit. This method can also be considered to be related to analog energy-minimization-based approaches (§4.2.3.1). However, this method does not require cooling the system to low noise temperatures for annealing, as is frequently done in energy-minimization approaches. Instead, the dynamical network uses a variation on reversible computing principles (§4.4) to adiabatically cause the system to transition between different warm, chaotic “strange attractors” that represent different computational states; this transformation can take place reversibly, without energy loss. The dynamical energy of the signal variables is itself conserved within the (Hamiltonian) dynamical system, and so the total energy dissipated per result computed can approach zero in this model as the rate of transformation decreases.

One disadvantage of the particular approach explored in that work is that it exhibits an apparent exponential increase in the real time required for convergence of the results as the complexity of the computation (number of logic gates) increases. However, as far as is known at this time, it is possible that faster variations on this or similar techniques may be found with further investigation.

An earlier, more extensively-developed proposal that is similar to the chaotic logic concept is called chaos computing.875

4.2.4. **ANALOG MEMORY AND COMPUTE DEVICES**

This section lists some specific device technologies that are useful in analog computing.

4.2.4.1. **ReRAM**

ReRAM memory is very dense and can be integrated in the back end of the line, avoiding the use of transistor area for the memory. Several ReRAM crossbars have been demonstrated for inference.876,877,878 A key challenge is maintaining good analog properties and high resistance at the same time. Nanoscale oxide-based cross-bar memristors with analog properties at high resistance were demonstrated owing to a natural thermal-confinement-effect when reducing the cross-point area.879,880 ReRAM for training remains a challenge due to the non-ideal electrical characteristics of synaptic devices.

4.2.4.2. **Phase Change Memory**

Phase-change memory (PCM) offers a wide range of analog memory states due to the large contrast between the amorphous and crystalline phases.881 For memory applications, PCM devices can be switched between a high-resistance RESET state, formed by melting and quenching an amorphous plug that blocks a narrow constrictive within the device; and a low-resistance SET state created by a crystallizing voltage pulse, which frequently ramps down in amplitude over a long duration to produce an extremely low-resistance state.

In contrast, for VMM applications where “device history” is a desirable feature, PCM devices programmed into the RESET state can be slowly brought to a much lower resistance SET state using many repeated partial-crystallization pulses.882 Careful choice of pulse condition can stretch this procedure out to many hundreds of pulses.883 Some recent work has shown some evidence for gradual increases in resistance with multiple successive pulses,884 although the operating regime must be carefully prepared, and the underlying mechanisms are not fully understood.

Many early VMM results using PCM focused on in-situ training (see §4.2.1.2 on Outer-Product Update above).720 Challenges for training include the one-sided nature of PCM programming, the nonlinear evolution of conductance with partial crystallization pulses, and the stochastic nature of PCM programming.

More recent VMM results using PCM have turned to inference of previously trained weights. Key challenges for inference include accurate programming of synaptic state despite the inherent stochasticity observed in PCM device programming.885,886 reducing resistance drift due to long-term relaxation of the amorphous phase, and ensuring long retention at high operating temperatures. PCM unit-cell designs that sacrifice some of the inherently large resistance contrast in order to suppress resistance drift have been proposed and demonstrated, in both memory and VMM contexts.887,888,889 It turns out that intra-device (e.g., shot-to-shot) variability in the rate at which devices drift over time (the “drift coefficient”) is more problematic than the actual drift itself.890 This is because any highly-predictable signal loss can be compensated by signal amplification, at least until background noise becomes strongly amplified.

4.2.4.3. **Ion-Insertion Redox Transistor:**

Ion-insertion redox transistors (IIRT) have recently emerged as promising candidates for analog memory.891,734 IIRTs are three-terminal devices where charge sent to the gate electrode causes an electrochemical redox reaction in the bulk of the channel. The reaction modulates the source drain conductance. IIRT channel and gate electrodes are made of redox-active materials (organic or inorganic) that conduct both electrons and ions (i.e. mixed conductors) and an ionically-conducting, electron-blocking electrolyte. To maintain global charge neutrality in the device, a counter-ion, typically lithium ions or protons, moves between the gate and channel and compensates for the changing oxidation state of the gate and channel. To retain the analog state and prevent the IIRT from discharging, an access device such as a diffusive memristor is required on the gate.
In contrast to traditional semiconductor devices where dopants are static after manufacturing, IIRT represents a class of devices with dynamic dopant control. For analog memory, a major advantage of IIRT is the large, charge-neutral volumetric capacity that can be exploited to support gradual tuning of the transistor source-drain conductance. Such properties have promise for synaptic memory for artificial intelligence applications. The storage capacity can be several orders of magnitude larger than traditional semiconductor devices where information is stored at oxide interfaces. For example, flash-based memory store roughly 50 aC for a 14/16 nm node. By comparison, lithium containing metal oxides report volumetric capacities at ~5,000 C/cm³. Additionally, IIRTs may offer promise for low voltage digital logic. Dynamic doping can lead to sharp metal insulator transitions, e.g. due to correlated electron effects in redox-active oxides, and may result in abrupt low voltage switching.

4.2.4.4. Floating Gate

Floating gate synapses (so-called "synaptic transistors") were first developed in 1994. They are modified EEPROM devices which can be fabricated in a standard CMOS process and programmed to within 0.2% accuracy. A number of sophisticated systems have been developed based on the arrays of synaptic transistors. The main advantage of analog and mixed-signal VMMs based on floating gate memories are very high input and output impedances, which help reducing overhead of peripheral circuitry. The main drawback of synaptic transistor approach is the relatively large cell area, i.e., > 1000F², where F is the minimum feature size, leading to higher interconnect capacitances and hence larger energy losses and time delays in analog computing circuits.

Recently, it was shown that much better area may be obtained re-designing, by simple re-wiring, the arrays of the ubiquitous NOR flash memories with their highly optimized cells. One representative example is Embedded SuperFlash (ESF) memory from Silicon Storage Technology, Inc. The areas of the modified arrays of the ESF1 and ESF3 NOR flash memories, with the latter technology scalable to F = 28 nm, are close to 120F² and may be further reduced to ~40F². (Note that such areas are much smaller compared to the contemporary 1T1R ReRAM.) Modified 180 nm ESF1 technology was successfully utilized to demonstrate a medium-scale (28x28-binary-input, 10-output, 2-layer, 101,780-synapse) network for pattern classification. The measured delay and energy dissipation compared very favorably with digital approaches, while the results for chip-to-chip statistics, long-term drift, and temperature sensitivity of the network were also very encouraging. Simulations have shown that similarly superior energy efficiency may also be reached in mixed-signal neuromorphic circuits based on industrial-grade SONOS floating gate memories.

Even higher density floating gate neuromorphic circuits can be achieved by utilizing NAND flash memories. 2D NAND memory devices designed for digital memory application are already capable of storing 4 bits (16 levels) in a single transistor of 100 nm × 100 nm area in 32nm process. Commercial NAND manufacturers have shown devices at 15 nm and 19 nm, EEPROM devices are found at every CMOS IC node, including 7 nm and 11 nm nodes. At these nodes, we still expect very small capacitors to retain 100s of quantization levels (7–10 bits) limited by electron resolution; in practice, larger capacitors are used, resulting in sufficiently high potential resolution. One expects EEPROM linear scaling down to 10 nm process to result in a 30 nm × 30 nm or smaller array pitch area. Perhaps, the most exciting opportunity is presented by the modern 3D NAND circuits. 3D NAND memories already feature 96 layers of floating gate cells. The number of layers is projected to further increase to 512 to enable 10 Tb/in² density, which will be essential for storing large-scale neuromorphic models. The very high density of 3D NAND circuits is achieved at the cost of certain restrictions at the circuit level, such as cells connected sequentially in strings and shared gate (word) voltages for the cells in the same level. The sequential structure of NAND flash memory can be efficiently exploited by using time multiplexed computations at the architecture level, in which one cell from a string being utilized at a particular time step in a distributed VMM circuit. Time-domain encoding of inputs was proposed to implement VMM circuits based on the existing 3D-NAND flash memory blocks with common word plane structure, not requiring any modification.

4.2.4.5. Capacitor-on-Gate

A recent proposal called for a small capacitor that can be programmed with standard CMOS devices to be tied to the gate of a read transistor. In contrast to DRAM, where the charge on the capacitor is transferred through a select transistor onto a bit-line for readout, here the voltage on the capacitor modulates the conductance of a read transistor by direct attachment to its gate terminal. Although the charge leaks away with a time-constant of milliseconds, the training process can succeed if the time-per-example is at least 100,000× smaller than the decay constant (e.g., 20 ms decay constant and 200 ns per training example). One method to obtain good update linearity, so that the amount of charge added and subtracted are balanced, is to use multiple large transistors to supply the current in each unit cell. Additional transistors are then added in order to ensure that, as per the weight-update algorithm, charge is added or subtracted only when both the upstream neuron (say, along the same row) and the downstream neuron (along the same column) agree that weight update should occur in a particular synapse shared by those two neurons. Recently, Ambrogio et al. introduced a combined PCM+capacitor-on-gate unit-cell, in which the PCM provided the non-volatile storage in a “higher significance” conductance, and the capacitor-on-gate devices provided high update linearity.
in a “lower significance” conductance, with periodic weight transfer from the lower to higher significance devices. The number of transistors associated with the capacitor could be reduced to three: The read transistor, an NFET for charge subtraction and a PFET for charge addition. This was made possible by giving the downstream neuron control over the NFET and PFET gates, and having the upstream neuron control the source contacts of these same two charge addition/subtraction transistors. Furthermore, variability between charge-addition and charge-subtraction due to process nonuniformity was compensated upon weight transfer from capacitor-on-gate cell to the PCM devices using a “polarity inversion” technique. Later, it was shown that this same technique could suppress fixed device variabilities in other kinds of lower-significance conductances, including PCM devices. This combined PCM+capacitor-on-gate unit-cell was shown to allow GPU-equivalent training accuracies, despite the known imperfections of PCM devices and typical fab-level CMOS variability in the capacitor-on-gate devices.

4.2.4.6. Charge-Based Analog Arrays for VMM

Charge-based analog arrays are amenable to very low energy and high-density parallel implementations of vector-matrix multiplication (VMM). Efficient charge storage and weighting in array-based analog computing are achieved through the use of capacitive reactive elements or other charge-based linear weighting elements such as charge-coupled devices (CCDs) and charge-injection devices (CID). Their efficiency stems from inherent charge conservation throughout the computational cycle.

Charge injection device (CID) arrays store each bit of the matrix element in a DRAM storage element. The charge for each bit in a weight is stored in one of two locations. If the input bit that is multiplying the weight bit is 1, the charge is non-destructively shifted between locations during readout causing a charge to be capacitively induced on the bit line. The charge induced by multiple weights can be summed and sensed allowing the entire matrix to be read out in a single operation. Multi-bit inputs are processed serially. Furthermore, charge is recycled during the computation, and so adiabatic techniques can be used to further lower the energy (at the cost of speed).

High-density mixed-signal adiabatic processors using CIDs have been developed using these principles. To optimize for resonant adiabatic energy recovery a stochastic encoding and decoding scheme can be used to ensure a constant capacitive load of the CID array. This has resulted in better than 1.1 TMACS/mW efficiency excluding on-chip digitization.

Alternatively, several approaches have combined a capacitive charge based VMM with analog-to-digital conversion to maintain high overall system efficiencies. Many analog multiply-and-accumulate operations can be performed for each digitization. High precision implementations of capacitive charge based VMM have achieved low-pJ/MAC energy efficiencies, while low-precision versions have achieved efficiencies at the level of 100 fJ/MAC. Comparison of key metrics with the state-of-the-art in analog capacitive VMM ICs is given in Table BC4.2 above.

Table BC4.1  Metrics for Analog Capacitive Vector-Matrix Multiply (VMM) ICs

4.2.4.7. Single Flux Quantum Neural Network Inference

Josephson junctions assembled into single flux quantum (SFQ) circuits form a natural neuromorphic system. In this technology, SFQ pulses act as the action potential for a spiking neuron, and superconducting transmission lines act as axons. The synaptic or weighting function can be implemented with a flux-biased Josephson junction or with a clustered magnetic Josephson junction. These elements represent the basic functionality of an artificial spiking neural network (SNN).

Superconducting and magnetic device technologies are relatively mature among emerging devices. On the magnetic device side, large non-volatile memories based on magnetic tunnel junctions, using spin-polarized currents to write, have been commercialized. On the superconducting device side, high speed microprocessors and communication systems have been developed, mostly on superconducting tunnel junctions.

When implementing the synaptic function with a magnetic nanocluster Josephson junction, the superconducting order parameter is modulated by the magnetic state of the nanoclusters in the barrier. The magnetic state of embedded nanoclusters can be changed by applying small current or field pulses, enabling both unsupervised and supervised learning. Maximum operating frequencies of these systems are above 100 GHz, while spiking and training energies have been demonstrated at roughly $10^{-20}$ J and $10^{-18}$ J, respectively. High speed and low-power operation are promising for direct hardware implementation of neural networks that could perform inference at higher speeds and potentially lower power than alternatives even when including the cooling overhead to operate at 4 K.

4.2.4.8. Photonic Vector-Matrix Multiply (VMM)

There are currently two major bottlenecks in the energy efficiency of artificial intelligence accelerators: data movement, and the performance of multiply-accumulate (MAC) operations, or matrix multiplications. Light is an established communication
medium and has traditionally been used to address data movement on a larger scale. As photonic links are scaled smaller and some of their practical problems addressed, photonic devices have the potential to address both of these bottlenecks on-chip simultaneously. Such photonic systems have been proposed in various configurations to accelerate neural network operations (see 929,930,931). However, their main advantage comes from addressing MAC operations directly. Here, we will look at the advantages of a simple matrix vector multiplication (MVM) unit made of integrated photonic components, in which inputs and outputs are encoded as light signals, and analog matrix multiplications are performed using a passive optical array.

One possible instantiation of a photonic MVMs is shown in the figure above. Power or phase can be used to encode information, while wavelength or phase selectivity can be used to program the network into a desired configuration. Wavelength division multiplexing (WDM) can further increasing the compute density of the approach. Classic examples include arrays of resonator weight banks 930,932,933 or Mach Zehnder interferometers 931. The most important metrics are energy efficiency (energy/MAC), throughput per unit area (MACs/s/mm²), speed (MVM/s), and latency (s), where both speed and latency are measured across an entire matrix-vector (MVM) operation. In CMOS, MVM operations are typically instantiated using systolic arrays 934 or SIMD units 935 although there are some other architectures that use aspects of both 936. Digital systems are limited by the use of many transistors to represent simple operations and require machinery to coordinate the data movement involved in both weights and activations. The state-of-the-art values typically hover around 0.5–1 pJ/MAC, 0.5–1 TMACs/mm², 0.5–1 GMVM/s, and 1–2 µs, respectively. In contrast, photonics MVM units could perform in range 2–10 fJ/MAC, 50 TMACs/mm², and ~3 ps (1 clock cycle) per MVM operation. This performance depends on solving a number of practical problems which are possible to address in the short term. These are discussed below.

The largest bottleneck in efficient photonic MVM operations is the use of heaters for coarse tuning. Typically, the thermo-optic coefficient (dn/dT) is the strongest effect in most materials of interest (i.e., silicon), leading to heavy use of heaters in almost any tunable passive photonic system. There are several ways these can be eradicated, via the use of post-fabrication trimming 937,938 or devices with an enhanced electro-optic coefficient (dn/dT, dalpha/dT) such that heaters are not as necessary 939,940. The second largest problem is fabrication variation, which can result in parameter drifts for devices in an array. Resonators, for example, are highly sensitive to such variation, particularly across a wafer. This can also be remedied by enhancing the electro-optic coefficient of devices and some other tricks (see 941,942 for resonators). Third, the signal-to-noise ratio of the output must be optimized by reducing the intrinsic loss of photonic components together with the noise on the receiver. There are a variety of technologies that can address this—for example, lasers can be coupled on-chip with < 1 dB of loss 943, photonic devices in state-of-the-art silicon foundries can be designed with low scattering 944 while detectors such as avalanche photodiodes 945 can reduce the relative contribution of thermal noise to the signal at the receiver.

Photonic arrays ultimately have very similar limits to analog electronic crossbar arrays, as analyzed in Ref. 946: single-digit aJ/MAC efficiencies, and 100s of PMACs/s/mm² compute densities. However, photonic MVMs garner an advantage for larger MVM units, both in the size of the matrix and in the physical footprint of the core. Generally speaking, optimized photonic systems tend to perform worse than their electrical counterparts for smaller arrays (distances approximately < 100 µm), but perform better for larger arrays (distances approximately > 100 µm) 946. In that sense, photonic MVM arrays have a similar profile to photonic communication channels, with better performance over larger distances. However, photonic systems tend to have worse signal-to-noise ratios, as a result of several factors: (1) photonic channels are ultimately shot noise limited, which is more than an order of magnitude greater than the thermal noise limits on resistors 946 and (2) to achieve similar compute densities to electronics, photonic MVMs must run faster to compensate for their larger device sizes, and noise is speed dependent. That being said, there are some architectural tricks to reduce this issue—for example, optical unitary operations 931 can conserve the variation of the input and output signals, in contrast to other approaches such as resistive crossbar arrays 719, which by default, see a √N decrease in effective signal variation from input to output for an N × N matrix operation.
Although photonic arrays exhibit some fundamental advantages over analog electronics (particularly for large matrix sizes or large physical sizes), a more important question is whether photonics arrays are practical. Thankfully, the transceiver industry has created a silicon photonic ecosystem fully compatible with high volume manufacturing (HVM). Compared to CMOS chips, photonics has costlier packaging, largely because light generation cannot be done easily in silicon—in fact, the cost of a production photonic chip is dominated by packaging. In addition, the tools required for the design and testing of large-scale photonic systems (>10k components) are still early in early development—analog photonic systems must grapple with the challenge of addressing yield, variability, precision, and tunability. Nonetheless, the total cost to produce a photonic chip package at high volume is dipping below one hundred dollars, and it is expected that the trend will continue. The orders of magnitude advantages offered by photonics, and its potential for HVM scalability, makes it a viable inroad for the breakneck performance and innovation required by artificial intelligence algorithms in the years to come.

**4.2.4.9. Magnetic Neural Network Devices**

Several types of magnetic circuits can be used to implement neural networks including spin-diffusion-based devices, charge-coupled spin logic (CSL), and domain wall logic (nLogic). The use of these different devices has been benchmarked.

Magnet switching dynamics that follow the Landau-Lifshitz-Gilbert (LLG) equation with a spin-transfer-torque term are quite similar to the cell dynamics in a Cellular Neural Network (CeNN). CeNNs have been designed based on spin diffusion using all-spin logic (ASL) with PMA magnets as the basic building block. A CeNN cell can also be implemented by using MTJs as synapses and using spin Hall effect or domain wall propagation-based devices as the neuron. In all these cases, the read-out circuit consists of read and reference MTJs and an inverter that amplifies the voltage division between the two MTJs.

In contrast to Boolean circuits, spintronic devices are more attractive compared to charge-based devices. This is because a single magnet can mimic the functionality of a neuron, and these spintronic devices operate at a low supply voltage. The domain wall device provides the best performance, in terms of Energy-Delay Product (EDP), thanks to its low critical current requirement. The spin diffusion based CeNN with (in-plane magnetic anisotropy (IMA) magnets consumes more energy due to the large critical current required to switch the magnet.

For optimal circuit-level performance using spintronic devices, several properties are desired including: MTJs with a large TMR and a moderate resistance-area product, large spin injection coefficient $\beta$, large perpendicular anisotropy $K_u$ for PMA magnets, large spin Hall angle $\theta$ for SHE materials, and small critical depinning current for domain wall magnets.

**4.2.4.10. Device Technologies for Coupled Oscillator Systems**

It is challenging to build compact, low-power oscillators that can also be coupled together to give predictable phase or frequency dynamics. Standard digital ring oscillators based on CMOS inverter feedback loops, as well as the typical transistor-driven LC oscillators used in RF designs, are both less than ideal, due to device nonlinearities in the digital regime and the high biasing currents used in linear-regime analog small-signal oscillators, as well as relatively large oscillator sizes in both cases. Thus, various “Beyond CMOS” oscillator technologies have been explored. Such technologies can use and manipulate the charge, spin, or quantum properties of electrons, or use photons. Important examples include spin-torque, insulator-metal-transition, optical, and quantum. Memristor-based oscillators have also been constructed.

Non-silicon electrical oscillators include two important kinds which are currently being developed. One prominent effort is the use of spin torque oscillators (STOs) coupled with using spin diffusion currents, or electrical signals, for providing a computational platform for machine learning, spiking neural networks, and others. However, the high current densities of STOs and the limited range of spin diffusion currents continue to pose serious challenges in creating coupled networks of such oscillators. Optical oscillators have been studied and used for computing, but challenges include bulky components, difficult interfacing between the electrical and optical domains, and lack of programmability to enable an optical computing apparatus. Another promising non-silicon technology for very compact oscillators is the IMT (insulator-metal transition) material-based oscillator technology. As the oscillation mechanism is completely electrical, the coupling of oscillators can be done easily using electrical components. There have been other implementation efforts for electrical oscillators, but the focus has been to build high frequency and low power individual oscillators, as opposed to the demonstration of coupled systems of oscillators, or the generation of interesting dynamics for computing. A comparison of some computing-focused electrical oscillators is shown in Table BC4.2 below.

**Table BC4.2  Comparison of Some Electrical Oscillators for Computing**

**4.2.4.11. Analog Neuron Functional Block**

Depending on the algorithm being accelerated, analog neurons can accelerate a variety of functions such as:

1. Spatial and temporal integration of input signals.
2. Stochastic firing of an action potential after a threshold is reached.
3. Relaxation to the resting potential if the time delay between excitations is too long.  
4. Non-linear activation functions. In many neural networks, after a linear multiply accumulate is performed on a set of inputs, or in a hidden layer, a non-linear activation or transfer function is applied. The presence of this function prevents the network from mathematically collapsing into a single linear equation, which helps improve the computational capabilities as the number of layers increases. Common functions include sigmoid, tanh and rectified linear (ReLu). In an analog network it is desirable that this function be performed by a single device.

These analog blocks are often with other building blocks such as crossbars, §4.2.1, to accelerate neural networks, to build dynamical systems, §4.2.3, create energy minimization circuits, §4.2.3.1 and enable probabilistic circuits, §4.3. Stochastic neurons/ devices are discussed in §4.3 rather than here. Using an analog neuron allows analog data to be processed directly, obviating the need for time- and energy-consuming ADC/DAC in the circuits.

Recently, Mott memristors, phase change based memristive switches, and chalcogenide threshold switches have all been reported to be capable of performing temporal voltage signal integration in which the effects of non-simultaneous unitary post-synaptic potentials add in time. Device candidates to perform the transfer function include STT-MRAM.

Ionic diffusion dynamics or electrical instabilities enable a single memristive device to perform analog functions like resistance tuning or pulse generation after accumulating input, which typically requires a large number of CMOS transistors. These analog functions are critical in emulating synaptic and neuronal behavior. Taking into account the simple structure and scalability of a two-terminal memristor, both the complexity of a circuit and the area consumed to build a neuron network will be much less compared to a CMOS circuit. Being a passive device, the memristor offers stimulation-dependent electric conductance. However, the passive nature results in a lack of power to maintain sustainable neural signal propagation in a network if passive synaptic blocks are employed. Additional power sources are mandatory for neural networks with multiple layers.

The benchmarks used to evaluate electronic spiking neurons generally measure the energy per operation, the fabrication cost, or the chip area of the integrated functional block, and the fidelity to the desired neuron function (e.g. integrate and fire). High reliability and low variation of devices are two key factors for the viability of a neuron technology. Device failure will require a lot more circuitry for error detection and correction. Large variation increases the difficulty for designing peripheral circuits and degrades the adaptability of the block.

To achieve unsupervised learning in a network, particularly those based on spike-timing-dependent plasticity, neuron blocks should be capable of programming the synaptic blocks. A key design challenge will be engineering the forward and backward propagating action potentials from the analog neuron blocks to potentiate or depress synapses for real time and in situ learning.

**4.2.5. Analog Computing—Closing Remarks**

Analog computation, as surveyed above, presents us with an intriguing and varied array of options for transcending the limitations that apply to the present-day digital approaches to computing. However, more work is needed to better characterize the range of applications for which analog computation can provide significant advantages over digital.

Enormously complex digital information-processing systems have been constructed by leveraging hardware description languages and programming languages that enable encapsulation, composability, and hierarchical design. To enable complex analog systems, more flexible, powerful languages (graphical and/or textual) for representing general classes of analog circuits and architectures are needed, to allow for a similar “modular” design approach.

Even the most advanced and sophisticated analog computational structures reviewed above in this section are only just the beginning. It appears that analog computing represents a vast field of future study, one that would likely benefit from a much more intensive level of exploration than it has received to date.

**4.3. Probabilistic Circuits**

Traditionally, conventional computational processes are designed to be deterministic, with computational results determined by the machine’s initial state and inputs. Nevertheless, computations that are intentionally designed to behave randomly or stochastically, even at the level of individual bit-operations, are of interest and can have many useful applications such as simulated annealing, Monte Carlo simulation, machine learning or Boltzmann machines, randomized algorithms as studied in computational complexity theory, and cryptographically secure random number generation for generating secure private keys. Noise in biological neurons is beneficial for information processing in nonlinear systems, and is essential for computation and learning in cortical microcircuits.

Obtaining randomness in traditional CMOS is difficult and typically relies on a pseudo-random number generator. This requires a large circuit block and significant computational effort to obtain high quality random numbers. Several new devices have been
proposed to obtain true randomness as discussed in §4.3.1. These allow for a random bit to be generated with a single device. Chaotic devices can be used to turn poor quality randomness into high quality random numbers. Novel architectures such as probabilistic p-logic (§4.3.2) or a traveling salesman solver (§4.2.3.1) can be designed using the new true random number generators.

### 4.3.1. Device Technologies for Random Bit Generation

New devices based on memristors, avalanche breakdown, and magnetic tunnel junctions and other technologies have been proposed for generating random bits. A key enabling functionality for some architectures like probabilistic (p)-logic is the ability to tunably control the probability of a zero or one based on an input current or voltage. Several proposed devices are listed below.

#### 4.3.1.1. Magnetic Tunnel Junctions (MTJ)

Existing Embedded MRAM technology can be used to create a tunable random bit, provided that the Magnetic Tunnel Junctions are engineered to be thermally unstable. Such thermally unstable magnets have been experimentally observed. As MTJ dimensions are scaled, keeping them thermally stable becomes a hard challenge for memories, therefore destabilizing them in a controllable manner should be feasible in current technology.

Low-barrier MTJs can convert ambient thermal noise on nanomagnets into a fluctuating resistance, which is then used to build a device with tunable randomness when integrated with minimal CMOS periphery. The fluctuating resistance change due to thermal magnetic noise in MTJs can be measured by tunnel magnetoresistance (TMR). State-of-the-art TMR values range from upwards of 100% to 600% demonstrated by the Tohoku Group, and commercial STT-MRAM devices exhibit >100% TMR. A large TMR would enable a robust functional unit for controllable randomness. The theoretical limit for TMR in MgO-based MTJs has been reported to be 1,000% and can presumably be larger. There is currently intense research activity in half-metallic ferromagnets to increase TMR.

#### 4.3.1.2. Single-Electron Bipolar Avalanche Transistor (SEBAT)

The single-electron bipolar avalanche transistor (SEBAT) is a novel Geiger-mode avalanche bipolar transistor structure. The device generates Poisson-distributed digital output pulses at rates between 1 kHz and 20 MHz. The pulse rate is linearly proportional to the emitted current. A MOS transistor is also formed within the base region of the device, allowing for voltage control of the pulse rate. The device is fully compatible with low-voltage CMOS circuits and standard digital process steps.

#### 4.3.1.3. Memristors/Resistive RAM

The intrinsic variability of memristive switching, particularly the switching delay time of memristors, can be a good source of stochasticity. Such stochasticity originates from the intrinsic dynamics within the memristors.

#### 4.3.1.4. Contact-Resistive Random Access Memory (CRRAM)

CRRAM can be used for random number generation. A CRRAM device may be based on a layer of silicon dioxide that is sandwiched between two electrodes; the bottom electrode could simply be the drain of a CMOS transistor. During operation, the current flowing in a filament channel will be impacted by any electrons trapped in the insulating layer. If a high voltage is applied to a device, the current in the filament channel will be large and not impacted by trapped electrons. However, with the application of a lower voltage, the width of a filament will shrink, and the trapped electrons will influence output current.

#### 4.3.1.5. CMOS

There are different ways to obtain random number generators (RNG) in CMOS using different physical noise sources, one being “jitter” in ring oscillators. These TRNGs can be tuned into tunable random number generators as required but require significant amounts of area when compared to single device alternatives.

#### 4.3.1.6. Stochastic Josephson Junction

Single flux quantum (SFQ) logic relies on voltage pulses generated by 2π phase slips of the superconducting order parameter across a Josephson junction. These voltage pulses have a time-integrated amplitude given by the flux quantum \( \Phi_0 = 2\times10^{-15} \text{ Wb} \). A standard circuit model of a Josephson junction is the parallel connection of a supercurrent up to \( I \), the critical current, a normal state resistor, a capacitor, and a channel for the thermal noise term. The resulting dynamics are the same as a forced damped pendulum. The energy barrier is given by \( (I_c I_0)/(2\pi) \). For stochastic operation one can operate with junctions that meet the condition \( \delta = (2\pi k_B T)/(I_c I_0) \sim 10 \), where \( \delta \) is the stochasticity, \( k_B \) is the Boltzmann constant and \( T \) is the temperature in kelvin. The exact value of the stochasticity is an important circuit parameter as it determines the frequency of spiking events. In this regime, the energy in a single flux quantum spike is sub-attojoule while the frequency can be greater than 100 GHz.

Because Josephson junctions can be operated near the thermal stability limit, the amount of stochasticity can be varied by changing the temperature a few degrees. For values of the stochasticity less than 10, the dynamics are basically deterministic,
whereas when the stochasticity is larger there is a significant stochastic component. The value of the stochasticity can be effectively tuned between the deterministic state and the stochastic state by changing the temperature of the circuit by a few degrees.\textsuperscript{998} Circuits based on these devices have many promising potential applications. For example, stochastic Josephson junctions have been shown to make effective pseudo-sigmoid generators,\textsuperscript{999} and stochastic Josephson junction spiking can perform the neural accumulate operation at speeds up to 70 GHz.\textsuperscript{1000}

4.3.2. **Probabilistic (P)-Logic**

In a series of recent papers, Camsari, Datta and collaborators proposed a type of probabilistic computing model introducing the concept of p-bits and p-circuits.\textsuperscript{1001,1002} The authors explored how p-bits can be compactly realized by leveraging existing Magnetoresistive RAM (MRAM) technology\textsuperscript{1003} and showed different applications of p-circuits including image recognition (inference),\textsuperscript{1004} combinatorial optimization,\textsuperscript{1005} Bayesian networks,\textsuperscript{1006} and an enhanced type of Boolean logic that allows invertible operation.\textsuperscript{1002} More recently, potential applications have been extended to include emulation of a class of quantum systems\textsuperscript{1007} and on-chip learning for stochastic neural networks.\textsuperscript{1008} Further, a prototype realization of an 8 p-bit circuit demonstrating a quantum-inspired integer factorization algorithm that uses MRAM-based p-bits has recently been realized.\textsuperscript{1009}

The main function of a p-bit is to provide tunable randomness of a digitized voltage at its output terminal controlled by an analog input terminal.\textsuperscript{1002,1003} The tunability allows a network of p-bits (p-circuits) to be able to get correlated with one another when appropriately connected through a programmable feedback circuit. Even though the p-bit concept is hardware agnostic and digital implementations of invertible logic have been realized,\textsuperscript{1010,1011} the main advantage of an MRAM-based p-bit comes from its compact, low-power implementation of a complex functionality (tunable randomness) compared to digital implementations.\textsuperscript{1009}

In the context of Machine Learning, this functionality is an approximate hardware representation of a binary stochastic neuron, allowing a natural mapping of powerful algorithms developed for such stochastic neural networks. Secondly, the generic p-circuit consists of autonomously operating p-bits without any digital clocking circuitry, leading to a massively parallel architecture whose performance increases with the number of p-bits in the system.\textsuperscript{1012} Recent breakthroughs in modern MRAM industry has led to production-ready integrated chips with up to 1 Gb cell densities, thus leveraging this technology could lead to application specific probabilistic coprocessors with broad applications for the active fields of Quantum Computing and Machine Learning.\textsuperscript{1013}

4.4. **Reversible Computing**

Besides analog computing (§4.2) and probabilistic computing (§4.3), a third dimension along which we may explore departures from the conventional computing paradigm is reversible computing.\textsuperscript{1014} In the present context, when we say that a computation is reversible, we mean that the lowest-level physical computational processes should be arranged to approach a condition of being both logically reversible and thermodynamically reversible. To say that a computational process is logically reversible means that known or deterministically computed information is not obliviously discarded from the digital state of the machine and ejected to a randomizing thermal environment. To say that the computation process approaches being thermodynamically reversible here means that the total increase in physical entropy incurred by the machine’s operation per useful computational operation performed should be extremely small, with the vision that this quantity can approach zero asymptotically as the technology continues to be improved.

In 1961, Rolf Landauer of IBM argued\textsuperscript{1015} that there is a fundamental physical limit on the energy efficiency of conventional irreversible digital operations, meaning those that carry out a many-to-one transformation of the space of computational states that is used. Landauer’s limit states that an amount $kT \ln 2$ of available energy (where $k$ is Boltzmann’s constant and $T$ is the temperature of the heat bath) must be (irreversibly) dissipated to heat per bit’s worth of (known or correlated) information that is lost from the computational state. Landauer’s limit can be rigorously derived from fundamental physical considerations.\textsuperscript{702,1016}

An important caveat to be aware of is that Landauer’s limit only applies to computational information that is correlated with other available information, as opposed to independent random information.\textsuperscript{702,1017} A computational bit that bears no correlations with other available bits is, in effect, already entropy, and thus it can be transferred back and forth between a stable, digital form in a computer and a rapidly-fluctuating physical form in a thermal environment with asymptotically zero net increase in total entropy, by, for example, adiabatically raising and lowering a potential energy barrier separating two degenerate states.\textsuperscript{703}

However, most bits in a digital computer are correlated bits, having been computed deterministically from other available bits. Performing a many-to-one transformation such as destructively overwriting or erasing such a bit obliviously (i.e., without regards to its existing correlations) therefore typically increases total entropy by one bit’s worth ($k \ln 2$) and thus implies at least $kT \ln 2$ energy consumption (loss of available energy). Fundamentally, then, the only way to avoid Landauer’s limit, in a deterministic computational process, is to avoid many-to-one transformations of the computational state. Bennett\textsuperscript{1018} showed that indeed, this is always possible; that is, any desired irreversible computation can always be embedded into a functionally equivalent reversible one. Such an embedding generally appears to incur some algorithmic overheads,\textsuperscript{1019,1020} in terms of (abstract) time or space complexity, but if reversible devices continue to become cheaper and more energy-efficient over time, then, in principle, these
resource overheads can be outweighed by the achievable energy savings, and total cost may be reduced compared to an irreversible design.\textsuperscript{1021} In the long run, reversible computing is the only physically possible path by which the amount of general digital computation that can be performed per unit energy (and cost!) might continue to be increased indefinitely, without any known fundamental limit.\textsuperscript{703}

In existing adiabatic implementations of reversible computing in today’s device technologies (see §§4.4.1–4.4.2 below), one typically finds that there is a linear tradeoff, at the device level, between the energy dissipation $E_{\text{diss}}$ resulting from, and the time interval or delay $t_{\text{del}}$ required to carry out, a given primitive digital operation in the adiabatic limit. We can express this tradeoff relation by stating that the dissipation-delay product (DdP) of the technology is a constant, over some range of achievable delay values, \textit{e.g.}, within that range, we can write

$$E_{\text{diss}} \cdot t_{\text{del}} \cong c_E,$$

where $c_E$ is the constant DdP, which we may also call the energy coefficient of the technology. However, there is no fully general proof that this same linear tradeoff relation must extend to all possible implementation technologies for reversible computing, and in fact, recent results suggest that an exponential downsizing of energy dissipation with delay may sometimes be possible when quantum effects are leveraged and the system is well-isolated from the thermal bath.\textsuperscript{1022} Further, even among cases where the linear relation still applies, there are no known technology-independent lower bounds on the value of the dissipation-delay constant. Although there are indeed firm quantum lower limits on the product of energy invested in performing an operation times the delay,\textsuperscript{1023} there are no known fundamental lower limits above zero on energy dissipated for any given delay value. Further, even when a fixed value of the constant is given, thermally limited parallel processors can still benefit from reversible computing in terms of their aggregate performance. For example, in cooling-limited stacked 3D logic scenarios, the per-area performance advantage of time-proportionally adiabatic technologies increases with the square root of 3D processor thickness.\textsuperscript{1024,1021} And in loosely-coupled, arbitrarily-massively-parallelizable applications with fixed power budgets, the aggregate performance gain from adiabatic computing scales up with energy efficiency arbitrarily.\textsuperscript{1021}

However, as of today, experimentally realizing reversible computing’s promise to vastly exceed the system-level energy efficiency of all conventional computers in practice remains a difficult engineering challenge. Although a variety of different adiabatic\textsuperscript{1025,1026,1027,1028,1029,1030,1031,1032,1033,1022} and ballistic\textsuperscript{1034,1035,1036,1037,1038,1039,1040,1041,1042,1043,1044,1045,1046,1047,1048,1049,1050,1051} schemes for the realization of reversible computation have been proposed, it has so far turned out to be challenging to actually achieve large energy efficiency gains at the system level in practice while accounting for all of the complexity overheads that are incurred from using a mostly-reversible design discipline, together with a variety of real-world parasitic energy dissipation mechanisms that exist and would need to be systematically eliminated or reduced. (See §4.4.4 for further discussion.) There is not yet any “magic bullet” physical implementation strategy that automatically addresses all the many possible energy-loss mechanisms in a complete system all at once. Logical reversibility (when suitably generalized\textsuperscript{704}) is indeed a necessary condition for approaching physical reversibility in deterministic digital computations, but it is by no means a sufficient one.

However, while approaching the ideal of physically reversible computing is by no means an easy path forward, it is at least a way that general digital computing can move forward. Plausibly, even in CMOS, adiabatic circuits might be able to demonstrate useful energy efficiency gains for highly energy-limited applications (such as spacecraft) even in the relatively near term if sufficiently high-$Q$ resonators can be developed.\textsuperscript{1052,1053} Further, even some of the existing reversible superconducting logic styles (such as RQFP\textsuperscript{1054,1055,1056,1057,1058,1059} and nSQUID\textsuperscript{1060,1061,1062}) logic) already appear to be capable of achieving energy dissipation below the Landauer limit in principle, although the available analyses don’t include dissipation in the clock-power supply. However, in cryogenic applications, if the dissipation in the power supply can take place in a higher-temperature exterior environment, this can translate to a significant and highly practically useful reduction in the amount of power that is dissipated \textit{internally} within the low-temperature system.\textsuperscript{705,706,1053} Finally, superconducting technologies operate with extremely small signal energies, which, if transferred nondissipatively to the room-temperature environment, become relatively insignificant in absolute terms; this can reduce pressure on AC supply design even for general HPC applications. See §4.4.2 below for further discussion of superconducting reversible computing technologies.

Reversible computing can also be potentially usefully combined with probabilistic computing (§4.3); if random digital bits are obtained by taking in entropy from the thermal environment and capturing it in a stable form, this can actually reduce environment entropy temporarily—albeit without reducing total entropy, of course, since the entropy of the digital state is increased.\textsuperscript{760} Once a randomized reversible computation utilizing such bits of “true” entropy has completed, those random bits can later be returned to the thermal environment with no net thermodynamic cost.\textsuperscript{703} Thus, the requirement for such a nondeterministic computation to be thermodynamically reversible is somewhat looser than is the case for a deterministic computation; many-to-one (irreversible) transformations can be permitted together with compensating one-to-many (nondeterministic) transformations in a computation.\textsuperscript{1063} so long as, overall over the course of the computation, previously-established correlations are not lost.
Reversible computing is normally conceived of as a strategy for making digital computation more energy efficient. More generally, can a broad variety of analog computing schemes be developed that are also thermodynamically reversible? Record energy efficiencies for charge-based analog vector-matrix multiplication have been demonstrated using adiabatic principles as discussed in §4.2.4.6. Further, fundamental physics is reversible at the microscale, which suggests that a sufficiently carefully-engineered analog computer might be made to approach macroscopic reversibility, and that its energy efficiency might be increased without limit as its technology is further refined. The degrees of freedom utilized for the analog physical computation would likely have to be very well-isolated from the system’s thermal degrees of freedom, and the usual tendency for complex dynamical systems to devolve towards chaotic behavior would have to be suppressed in some way, or else made into a useful feature of the computational process, such as in reservoir computing (see §4.2.2.4 above). The previously mentioned work on chaotic logic (§4.2.3.4) suggests one potential technique for harnessing the chaotic analog behavior of conservative dynamical systems usefully for general digital computational purposes, but many other, more sophisticated methods may be possible.

4.4.1. **Reversible Adiabatic CMOS**

As mentioned above, currently the most well-developed implementation technologies for reversible computing are those that utilize classical quasi-adiabatic transformations to carry out digital state transitions. Among such technologies, the most well-developed class of them at present has been referred to variously as adiabatic CMOS, adiabatic transistor circuits, or just adiabatic circuits. In traditional (irreversible, non-adiabatic) CMOS circuits, the full digital circuit-node signal energy of $\frac{1}{2}CV^2$ is dissipated to heat on every digital switching event. In contrast, the use of classical quasi-adiabatic transitions for switching reduces the associated local dissipation by a factor of $\pi t/2RC$, where $t$ is the transition time for a linear voltage ramp and $R$ is the resistance of the charging path. This reduction yields a linear tradeoff between speed and energy dissipation per operation over a certain range of frequencies, where the dissipation-delay product or energy coefficient scales as $c_E \propto C^2V^2R$.

The earliest complete circuit families for sequential, pipelined reversible computing with adiabatic CMOS were developed in the 1990s in Tom Knight’s group at MIT. These methods did not gain widespread traction at the time, perhaps because, to save energy, adiabatic CMOS must operate relatively slowly compared to the inherent $RC$ propagation delay of the gates. However, in the period since the end of Dennard scaling in ~2005, multi-core processor performance has become increasingly limited by power dissipation rather than by raw gate delays (witness the increasing amounts of “dark silicon” in modern processor designs), so, revisiting the adiabatic energy-delay tradeoff appears timely at present. Adiabatic switching holds promise as a design technique for the future, since it offers a means by which the dissipation-delay frontier of any given CMOS technology might be expanded beyond the limits of what can be achieved using more conventional low-power design techniques, such as subthreshold operation.

Subsequent to the original MIT adiabatic logic families cited above, a number of other adiabatic logic design styles were also explored, such as two-level adiabatic logic (2LAL), positive feedback logic (PFAL), and efficient charge recovery logic (ECRL). In addition, applications to the design of secure circuits have also been explored, since the unique electrical behavior of adiabatic CMOS circuits can help to prevent non-invasive side channel attacks. And general-purpose computing has been pursued in the design of adiabatic microprocessors. The simulation results shown in Figure BC4.5 indicate that, when operated adiabatically, advanced CMOS nodes such as 28 nm technology can dissipate less energy per cycle.

![Energy Dissipation per Stage vs. Frequency in an Adiabatic CMOS Shift Register](image-url)

**Figure BC4.5** Energy Dissipation per Stage vs. Frequency in an Adiabatic CMOS Shift Register
than prior nodes at relatively high frequencies, at which dynamic power dissipation exceeds the leakage losses. In contrast, if the same circuit is operated irreversibly, it dissipates an energy orders of magnitude higher at all frequencies up into the GHz range.

Another very recent development is the introduction of fully adiabatic CMOS logic families that are also fully static, meaning that all nodes are at all times connected to a supply reference, which eliminates voltage-level drift from leakage and capacitively-induced voltage sag, which could otherwise occur on floating notes and contribute to non-adiabatic losses. In principle, as leakage is reduced, these “perfectly adiabatic” logic styles should be capable of exceeding the energy efficiency of any other semiconductor-based form of digital logic.

4.4.2. REVERSIBLE ADIABATIC SUPERCONDUCTING LOGIC

After adiabatic CMOS, currently the second most well-developed type of hardware technology for reversible computing based on classical adiabatic transformations is the class of adiabatic superconducting logic families. A significant motivation for the consideration of superconducting circuits for energy-efficient computation is the lossless nature of charge transport in Josephson junctions and superconducting wires, which act as switching elements and interconnects, respectively. Also, the naturally discrete phenomenon of flux quantization facilitates the restoration and stabilization of digital signals.

Two basic families of superconducting reversible digital elements, the parametric quantron (PQ) and quantum flux parametrond (QFP) were proposed in early studies. Both approaches were based conceptually on the abstract physical model of adiabatic digital operations introduced by Landauer, in which the potential energy function of the digital element is transformed adiabatically between single-well and double-well configurations in the course of the operation. As with adiabatic CMOS, superconducting reversible logic gates utilizing this approach require AC driving waveforms, in this case to provide a time-dependent flux bias to each gate. More recently, a DC-powered superconducting reversible logic gate based on a negative-inductance SQUID (nSQUID) was proposed and its energy dissipation was estimated to be a few kT per reversible bit-operation.

Recently, a further reduction of the energy dissipation of the QFP approach was achieved by appropriately optimizing the circuit parameters for the adiabatic mode of operation and eliminating the junction shunt resistance. The energy dissipation of this improved adiabatic QFP (AQFP) was investigated numerically, taking thermal noise into account, and found to be well below kT with a low error rate. The energy dissipation of a single AQFP gate was estimated to be 10 zJ per gate at 5 GHz by measuring the scattering parameters of a superconducting resonator coupled to an AQFP gate. The energy dissipation per operation of an (irreversible) AQFP 8-b carry-lookahead adder was experimentally evaluated to be 24 kT per Josephson junction.

The first demonstration of logically and physically irreversible operation of superconducting logic was performed using a newer reversible QFP (RQFP) design style. The basic RQFP element is a logic gate having three binary inputs x0, x1, x2 and three outputs y0, y1, y2 that are related by

$$ (y_0, y_1, y_2) = (\text{MA}(\overline{x_0}, x_1, x_2), \text{MA}(x_0, \overline{x_1}, x_2), \text{MA}(x_0, x_1, \overline{x_2})) $$

where $\text{MA}(i, j, k) = (i \lor j) \land (j \lor k) \land (k \lor i)$. This logically reversible element is composed of three AQFP splitter gates and three AQFP majority gates. The bidirectionality and time reversal symmetry of the RQFP gate were investigated, revealing the cause of the energy dissipation in logically irreversible AQFP logic. Using RQFP gates, the functionality of a 1-bit reversible full adder was demonstrated, and its energy dissipation was numerically calculated, while accounting for thermal noise. Figure BC4.6 shows the simulation results for the energy dissipation of the reversible and irreversible full adders as a function of the frequency of the driving clock. It was found that the energy dissipation of the reversible full adder is much lower than that of the irreversible full adder; it becomes lower than the kT thermal energy at 4.2 K at frequencies below 20 MHz.

![Energy Dissipation of RQFP and Irreversible AQFP 1-b Full Adders](image)

The International Roadmap for Devices and Systems: 2021
Copyright © 2021 IEEE. All rights reserved.
4.4.3. Other Reversible Technology Concepts

Beyond the adiabatic semiconductor/superconductor technologies discussed in §§4.4.1–4.4.2 above, over the years, a rather wide variety of disparate aspirational concepts for physical implementation technologies for adiabatic reversible computing have been described in the literature, although typically without accompanying physical demonstrations as of yet.

In the 1980s, the pioneering nanotechnology visionary K. Eric Drexler at MIT outlined a variety of concepts for nanoscale computing technologies, including adiabatic reversible versions, that were based on nanoscale mechanical, rather than electrical, interactions. More recently, a group led by Ralph Merkle at the Institute for Molecular Manufacturing (IMM) has been developing an even more advanced nanomechanical reversible logic concept based on (single-atomic-bond) rotary bearings, which were analyzed to dissipate as little as $4 \times 10^{-26}$ J per operation at room temperature at speeds of 100 MHz. This is roughly 74,000× lower energy than the Landauer limit at 300 K, and roughly 10× smaller dissipation-delay product (DdP) than even end-of-roadmap CMOS. Although we do not yet have a nanomanufacturing technology that is capable of fabricating the atomically-precise nanostructures envisioned in the IMM designs, this analysis nevertheless suggests how much farther the dissipation-delay frontier might someday be extended, beyond what is possible in today’s semiconductor- and superconductor-based technologies.

Back in the electronic domain, since the 1990s, a number of adiabatic reversible computing concepts based on single-electron devices have been proposed. Notable among these is the quantum-dot cellular automata (QCA or QDCA) technology concept pioneered at Notre Dame, which has been taken up to the level of complete simulated processor designs. However, there is not, as of yet, a viable manufacturing process for fabricating scalable QCA-based processors.

To conclude our review of the adiabatic approaches, we mention an interesting concept for adiabatic capacitive logic.

In addition to the various adiabatic approaches to reversible computing, there are also a number of ballistic reversible computing concepts. These are based on a rather different picture of the basic physical mechanism of reversible computing than the adiabatic approach suggested by Landauer. In the adiabatic approach, some external system (i.e., separate from the logic circuits) drives the adiabatic transformations of the computing system that carry out transitions between digital states. Whereas, in the ballistic picture, first conceived by Ed Fredkin, the physically-reversible dynamics of the system is instead self-contained; in other words, individual entities (such as particles or pulses) carrying information-bearing degrees of freedom evolve forwards reversibly under their own (generalized) inertia, as it were, with no direct external influence.

We should note that the distinction between the two classes of approaches is not a perfectly crisp one, since, even in the adiabatic approach, the driving system (such as a resonant oscillator) can be viewed as evolving ballistically, and even in the ballistic approach, the interactions (e.g., elastic collisions) between individual ballistically-propagating information-bearing entities can be analyzed, on a sufficiently fine timescale, as adiabatic processes. So, to some extent, the distinction between the approaches is primarily just one of perspective and emphasis. However, generally speaking, the adiabatic approaches are characterized by a large-scale separation of the ballistic driving systems from the adiabatic logic, whereas in the ballistic approaches, the ballistic properties are distributed throughout the system, and are associated to the lowest-level information-bearing entities themselves. We can also imagine that other, future approaches could interpolate between these two extremes; e.g., one could imagine systems comprising large numbers of small ballistic oscillators, each driving just a small region of local adiabatic logic, with the various subsystems communicating timing information and data to each other via elastic interactions transmitted via (short- or long-range) couplings between individual oscillators.

In terms of practical realizations of a (fully-distributed) ballistic approach to reversible computing, the approaches to this that have been developed most intensively to date are based on superconducting electronics. This is a particularly convenient technology for ballistic computing, because, unlike in semiconductors, superconductors exhibit the phenomenon of naturally-discrete single flux quanta (SFQ), which can propagate near-ballistically along interconnects consisting of passive transmission lines (PTLs) or long Josephson junctions (LJs). Currently active efforts to develop reversible computing technologies focused on SFQ-based approaches include the synchronous ballistic approach which has been explored since around 2010 at U. Maryland, and the asynchronous ballistic approach which has been in development since 2016 at Sandia National Laboratories.

4.4.4. Challenges for Reversible Computing

Despite the great long-term promise of reversible computing, many fundamental engineering challenges associated with the development of a practical reversible computing technology remain to be solved at this time. These include the following:

Note: Figure is from Ref. 1087. Simulation results are plotted as a function of the frequency of the excitation (driving) clock. Lines are calculation results at 0 K, markers show results accounting for thermal noise at $T = 4.2$ K.
Emerging Device-Architecture Interaction

- Even at the level of very basic physics, a more complete understanding is needed of the fundamental (technology-independent) physical limitations of important cost metrics for reversible computing, such as the dissipation-delay product (DdP), or, more generally, energy dissipation as a function of delay, \( E_{\text{diss}}(t_{\text{del}}) \). An important question is: Are there universal lower bounds on this quantity that we can derive based on parameters such as temperature, or the length scale of devices, or perhaps based on some kind of generalized viscosity characteristics, or on other fundamental physical or materials-dependent parameters? \(^{1098,1099}\)

- New, more complete abstract (but still realistic) physical models of reversible computing should be crafted to illustrate how we might more closely saturate the above fundamental limits in real artifacts, pointing the way to new device and circuit concepts for reversible computing. Are there quantum-mechanical approaches or phenomena that could be usefully harnessed, such as shortcuts to adiabaticity (STA), \(^{1100}\) topological invariants, dynamical variations of the quantum Zeno effect (QZE) \(^{1101,1102}\) or others, to help reversible computing technologies to further suppress the rate of entropy increase while still operating as quickly as possible?

- Facilitated by fundamental advances such as the above, new device and circuit concepts for reversible computing need to be developed that significantly reduce \( E_{\text{diss}}(t_{\text{del}}) \) at useful operating speeds while still being inexpensively manufacturable. New physical mechanisms for computing need to be developed with \textit{reversible operation in mind from the start.}

- Meanwhile, to advance the achievable energy efficiency of adiabatic CMOS for cryogenic applications, novel FET device structures that are optimized to minimize leakage at particular cryogenic temperatures of interest with minimal impact on device performance (expressed in terms of, say, DdP) need to be developed. \(^{1103}\)

- For adiabatic reversible computing technologies operating at room temperature, the logic signal energy (e.g., \( \frac{1}{2}CV^2 \) in CMOS) remains a concern, since it still exists even in adiabatic circuits, and is merely transferred dynamically to the power-clock generator system, rather than being dissipated locally within the logic. Thus, to achieve significant overall energy savings at the system level, compared to the corresponding irreversible technology, this generator must be designed to efficiently recover a large fraction of this signal energy, e.g., by comprising a resonant oscillator with a high \textit{quality factor} \( Q \). Designing extremely high-\( Q \) resonators and clock distribution networks already demands advanced, high-precision engineering. Further, as RF designers know, achieving high \( Q \) implies narrow bandwidth. This in turn implies that the returned clock waveform must be extremely pristine—e.g., any data-dependent back-action from the logic must be avoided. Thus, we must maintain a careful load balancing discipline, e.g., through complementary signaling. And if bulk semiconductors are used, this adds another level of challenge relating to time-varying loads during transitions, since device capacitances are more voltage-dependent if depletion regions are not structurally constrained. Thus, fully-depleted SOI, thin-film, or nanosheet FET geometries may be preferred.

- At higher levels, many advances in areas such as reversible architectures, EDA tool enhancements to support reversible design styles, reversible algorithms\(^{1020}\) and so forth still need to be developed. As useful reversible computing hardware technologies emerge and develop, systems engineering practice will also need to evolve to best leverage the opportunities and tradeoffs offered by reversible design. \(^{1021}\) However, all these R&D areas remain in their infancy at this time.

4.5. \textbf{Device-Architecture Interaction: Conclusions/Recommendations}

In this section, we have surveyed a variety of concepts and R&D directions for the development of novel Beyond CMOS computing technologies that represent an effort to think “outside the box,” in the sense of looking beyond just developing simple drop-in replacements for traditional logic and memory cells. More broadly, new hardware designs spanning multiple levels from the devices up through circuits and architectures must be considered, and the interactions between the various levels explored. More specifically, we expand the scope of future computing technologies beyond traditional irreversible, deterministic digital logic to include a broad range of alternative, unconventional computational paradigms, such as analog, probabilistic, and (classical) reversible computing paradigms.

\textbf{Recommendations}

In general, computing paradigms outside of the traditional irreversible, deterministic, digital paradigm are still very underdeveloped, compared to the conventional paradigm. This is not surprising, considering that the conventional paradigm historically facilitated the development of a design abstraction hierarchy that permitted enormously complex systems to be constructed. As a result, the complexity and efficiency of those systems increased exponentially as Moore’s Law made the underlying devices cheaper and more efficient. However, Dennard scaling has now ended, the end of the CMOS roadmap appears to be in sight, with no clear successor having been identified, and fundamental thermodynamic limits are also coming into view. Thus, today there is an increasing level of interest in expanding the scope of our investigations to include unconventional computing paradigms that may transcend the limits of the traditional computing paradigm.

\textbf{THE INTERNATIONAL ROADMAP FOR DEVICES AND SYSTEMS: 2021}

\textbf{COPYRIGHT © 2021 IEEE. ALL RIGHTS RESERVED.}
Overall, the potential utility of new styles of “Beyond CMOS” computing that rethink computation—not just at the device level, but also in terms of the entire computing paradigm, with changes to the machine design also at the circuit level, the architecture level, and higher levels—is vast. It is our recommendation that these alternative computing styles deserve a greatly increasing amount of attention and investment as the apparent end of the CMOS roadmap draws closer.

5. **BEYOND CMOS DEVICES FOR MORE-THAN-MOORE APPLICATIONS**

5.1. **EMERGING DEVICES FOR SECURITY APPLICATIONS**

5.1.1. **INTRODUCTION**

Like performance, power, and reliability, hardware security is becoming a critical design consideration. Hardware security threats in the IC supply chain, include 1) counterfeiting of semiconductor components, 2) side-channel attacks, 3) invasive/semi-invasive reverse engineering, and 4) IP piracy. A rapid growth in the “Internet of Things” (IoT) only exacerbates problems. While hardware security enhancements and circuit protection methods can mitigate security threats in protected components, they often incur a high cost with respect to performance, power and/or cost.

Advances in emerging, post-CMOS technologies may provide hardware security researchers with new opportunities to change the passive role that CMOS technology currently plays in security applications. While many emerging technologies aim to sustain Moore’s Law-based performance scaling and/or to improve energy efficiency, emerging technologies also demonstrate unique features that could drastically simplify circuit structures for protection against hardware security threats. Security applications could not only benefit from the non-traditional I-V characteristics of some emerging devices, but also help shape research at the device level by raising security measures to the level of other design metrics.

At present, many emerging technologies being studied in the context of hardware security applications are related to designing physically unclonable functions (PUFs). Many post-CMOS devices have been suggested as a pathway to a PUF design. (More detailed reviews are also available.) With a PUF, challenge/response pairs are mapped (typically in a trusted environment). Responses are derived from natural/random variations and disorders in an integrated circuit that cannot be copied (or cloned) by an adversary. PUFs have been employed for tasks such as device authentication, to securely extract software, in trusted Field Programmable Gate Arrays (FPGAs), and for encrypted storage. Post-CMOS devices also find utility as random number generators (RNGs) that may be employed for secure communication channels (e.g., to generate session keys). That said, while intriguing, PUFs and RNGs may only cover a small part of the hardware security landscape. (Furthermore, one must be careful that PUF designs based on emerging technologies do not depend on device characteristics that a designer would like to eliminate when considering utility for logic or memory.)

Given the many emerging devices being studied and that few if any devices were proposed with hardware security as a “killer application,” this document also reports initial efforts as to how the unique I-V characteristics of emerging transistors that are not found in traditional MOSFETs could benefit hardware security applications.

Below, we review the efforts described above, beginning with efforts to design PUFs and RNGs with emerging technologies. How device characteristics can enable novel circuits to achieve hardware security-centric ends such as IP protection, logic locking, and the prevention of side channel attacks are also discussed.

5.1.2. **PHYSICALLY UNCLONABLE FUNCTIONS (PUFS) AND EMERGING TECHNOLOGIES**

A variety of different emerging logic and memory technologies have been considered in the context of PUFs. As has been reviewed, variations in the required write time in spin torque transfer random access memory (STT-RAM) was proposed to create a domain wall memory PUF. Other structures based on magnetic tunnel junctions have also been proposed. Variations in write times have also been exploited to produce unique responses in phase change memory (PCM) arrays. The variability of ReRAM presents a natural opportunity for PUF implementation, and array demonstration has been reported. At the array-level, variations in diode resistivity have also been used to derive challenge/response pairs from crossbar structures. PUFs based on graphene and carbon nanotubes have also been proposed/considered.

As a more representative case study, prior work considers an array structure based on process variation in memristors to create a PUF structure (referred to as NanoPUF). NanoPUF is based on 1) a crossbar with memristors. 2) A challenge is applied to the memristor array by using a row decoder to apply a voltage amplitude (Vad) to a given row that can vary in duration; a column decoder connects a given column to a resistance R_load. All other rows and columns remain floating. 3) A response circuit (to collect outputs to different challenges) would consist of R_load and a current comparator that compares Iout from a given column to a reference current I_ref. A logic 1 might be recorded if Iout > I_ref, while a logic 0 might be recorded if Iout < I_ref. With respect to PUF functionality, when a write pulse is applied, natural process variations will cause some memristors to turn on (leading to a
logic 1), and others to remain off (leading to a logic 0). While the time of the right pulse serves as one variable, the pulse’s duration and amplitude may also be varied.\(^{1121}\)

### 5.1.3. Random Number Generators (RNGs) and Emerging Technologies

The inherent randomness in emerging devices can also be used to generate random numbers.\(^{1109}\) As a representative case study, prior work\(^{1109}\) explores an approach based on contact-resistive random access memory (CRRAM).\(^{1122}\) (Note that a CRRAM device may be based on a layer of silicon dioxide that is sandwiched between two electrodes; the bottom electrode could simply be the drain of a CMOS transistor — which in turn suggests that RNGs based on emerging technologies can be CMOS compatible.\(^{1123}\))

During operation, the current flowing in a filament channel will be (randomly) impacted by any electrons trapped in the insulating layer. If a high voltage is applied to a device, the current in the filament channel will be large and not impacted by trapped electrons. However, with the application of a lower voltage, the width of a filament will shrink, and the trapped electrons will (randomly) influence output current.\(^ {1125}\) Indeed, RNGs based on emerging devices\(^ {1125}\) can successfully pass randomness tests such as those provided by the National Institute of Standards and Technology (NIST).

As random number are derived from current passing through filaments, memristors, PCM, and RRAM devices can also be leveraged to build similar RNGs.\(^ {1109}\)

### 5.1.4. Other Hardware Security Primitives based on Emerging Technologies

Below, other security-centric primitives (non-PUFs and non-RNGs) based on emerging technologies are also discussed. How new devices might be employed for IP protection and to prevent side channel attacks are considered. In each section, device characteristics of interest are discussed first. Subsequent discussions then consider how device characteristics can be employed to achieve a security centric end.

#### 5.1.4.1. Emerging Technologies for IP Protection

**Tunable Polarity:** In many nanoscale FETs (45 nm and below), the superposition of n-type and p-type carriers is observable under normal bias conditions. The ambipolarity phenomenon exists in various materials such as silicon,\(^ {1124}\) carbon nanotubes\(^ {1125}\) and graphene.\(^ {1128}\) By controlling ambipolarity, device polarity can be adjusted/tuned post-deployment. Transistors with a configurable polarity — e.g., carbon nanotubes,\(^ {1127}\) graphene,\(^ {1128}\) silicon nanowires (SiNWs),\(^ {1129}\) and transition metal dichalcogenides (TMDs)\(^ {1130}\) — have already been experimentally demonstrated.

As more detailed examples, SiNW FETs have an ultra-thin body structure and lightly-doped channel which provides the ability to change the carrier type in the channel by means of a gate. FET operation is enabled by the regulation of Schottky barriers at the source/drain junctions. The control gate (CG) acts conventionally by turning the device on and off via a gate voltage. The polarity gate (PG) acts on the side regions of the device, in proximity to the source/drain (S/D) Schottky junctions, switching the device polarity dynamically between n- and p-type. The input and output voltage levels are compatible, enabling directly-cascadable logic gates.\(^ {1131}\)

Ambipolarity is an inherent property of TFETs due to the use of different doping types for drain and source if an n/i/p doping profile is employed.\(^ {1132}\) By properly biasing the n-doped and p-doped regions as well as the gate, a TFET can function either as an n- or p-type device, and no polarity gate is needed. As the magnitude of ambipolar current can be tuned (i.e., reduced) via doping or by increasing the drain extension length,\(^ {1132}\) one can envision fabricating devices that could be better suited for logic as well as security-related applications. Given that the screening length in TMD devices scales with their body thickness, one can achieve substantial tunneling currents.

**Polymorphic logic gates:** The ability to dynamically change the polarity of a transistor opens the door to define the functionality of a layout or a netlist post fabrication. Though one may use field programmable gate arrays (FPGAs) to achieve the same goal, FPGAs cannot compete with ASICs in terms of performance and power, and an FPGA’s reliance on configuration bits being stored in memory introduces another vulnerability. Security primitives to be discussed can serve as building blocks for IP protection, IP piracy prevention, and to counter hardware Trojan attacks.

Polymorphic logic circuits provide an effective way for logic encryption such that attackers cannot easily identify circuit functionality even though the entire netlist/layout is available. However, polymorphic logic gates have never been widely used in CMOS circuits mainly due to the difficulties in designing such circuits using CMOS technology.

SiNW FET based polymorphic gates to prevent IP piracy have been introduced.\(^ {1133,1134}\) If the control gate (CG) of a SiNW FET is connected to a normal input while the polarity gate (PG) is treated as the polymorphic control input, we can easily change the circuit functionality through different configurations on the polymorphic control inputs without a performance penalty. For
example, a SiNW FET based NAND gate can be converted to a NOR gate, whereas a CMOS-based NAND cannot be converted to a fully functioning NOR by switching power and ground.

TFET-based polymorphic logic circuits have also recently been developed.\textsuperscript{1135} By properly biasing the gate, the n-doped region, and the p-doped region, a TFET device can function either as an n-type transistor or p-type transistor. If the n-doped region of the two parallel TFETs is connected to $V_{DS}$, and the p-doped region of the bottom TFET is connected to GND, the circuit behaves like a NAND gate. If the n-doped region of the two parallel TFETs is connected to GND and the p-doped region of the bottom TFET is connected to $V_{DS}$, the circuit behaves as a NOR gate. By using two MUXes (one at the top and the other at the bottom) to select between the two types of connections, the circuit then functions as a polymorphic gate where the control to the MUXes forms a 1-bit key.\textsuperscript{1135}

One can readily design polymorphic functional modules using the low-cost polymorphic logic gates built from either SiNW FETs or TFETs that only perform a desired computation if properly configured. If some key components (e.g., the datapath) in an ASIC are designed in this manner, the chip is thus encrypted such that a key, i.e., the correct circuit configuration, is required to unlock the circuit functionality. Without the key, invalid users or attackers cannot use the circuit. Thus, IP cloning and IP piracy can be prevented with extremely low performance overhead. A 32-bit polymorphic adder using SiNW FETs has been designed and simulated. Two pairs of configuration bits (with up to 32-bits in length) are introduced and the adder can only perform addition functionality if the correct configuration bits are provided.

**Camouflaging Layout:** Split manufacturing and IC camouflaging are used to secure the CMOS fabrication process, albeit with high overhead and decreased circuit reliability. With CMOS camouflaging layouts, both power and area would increase significantly in order to achieve high levels of protection.\textsuperscript{1136} A CMOS camouflaging layout that can function either as an XOR, NAND or NOR gate are designed at least 12 transistors. Emerging technologies help reduce the area overhead. Recent work has demonstrated that only 4 SiNW FETs with tunable polarity are required to build a camouflaging layout that can perform NAND, NOR, XOR or XNOR functionality.\textsuperscript{1137,1138} Again, the SiNW FET based camouflaging layout has more functionality and requires less area than CMOS counterparts and could offer higher levels of protection to circuit designs.

**Security Analysis:** Logic obfuscation is subject to brute-force attacks. If there are $N$ polymorphic gates incorporated in the design, it would take $2^N$ trials for an attacker to determine the exact functionality of the circuit. As the value of $N$ increases, the probability of successfully mounting a brute-force attack becomes extremely low. In a preliminary implementation of 32-bit adder, the incorporated key size is 32 bit.\textsuperscript{1135} The probability that an attacker can retrieve the correct key becomes $1/2^{32}$ (2.33x10$^{-10}$). Obviously, polymorphic based logic obfuscation techniques are resistant to a conventional brute-force attack. With respect to camouflaging layouts, given that our proposed SiNW based camouflaging layout can perform four different functions, the probability that an attacker can retrieve the correct layout is 25%. Therefore, if $N$ SiNW FET camouflaging layouts are incorporated in a design, the attacker has to compute up to $4^N$ times to resolve the correct layout design. Compared to polymorphic gate-based logic obfuscation, camouflaging layout embraces higher security level but with larger area overhead.

### 5.1.4.2. Emerging Technologies to Prevent Side-Channel Attacks

Many post-CMOS transistors aim to achieve steeper subthreshold swing, which in turn enables lower operating voltage and power. Many devices in this space also exhibit I-V characteristics that are not representative of a conventional MOSFET. An example of how to exploit said characteristics for designing hardware security primitives is discussed.

**Steep slope transistors:** TFETs have been exploited to design current mode logic (CML) style light-weight ciphers.\textsuperscript{1139,1140} The high energy carriers in TFETs can be filtered by the gate-voltage-controlled tunneling such that a sub-60 mV/decade subthreshold swing is achievable at room temperature.\textsuperscript{1141} With improved steep slope and high on-current at a low supply voltage, TFETs could enable supply voltage scaling to address challenges such as undesirable leakage currents, threshold voltage reduction, etc. Different types of TFETs have been developed and fabricated.\textsuperscript{1141,1142}

**Bell-Shaped I-Vs:** Emerging transistor technologies may also exhibit bell-shaped I-V curves. Symmetric graphene FETs (SymFETs) and ThinTFETs are representatives of this group. In a SymFET, tunneling occurs between two, 2-D materials separated by a thin insulator. The $I_{DS}$-$V_{GS}$ relationship exhibits a strong, negative differential resistance (NDR) region. The I-V characteristics of the device are “bell-shaped,” and the device can remain off even at higher values of $V_{DS}$. The magnitude of the current peak and the position of the peak can be tuned via the top gate ($V_{TO}$) and back gate ($V_{BG}$) voltages of the device.\textsuperscript{1133} Such behavior has been observed experimentally.\textsuperscript{1143,1144} More specifically, $V_{TG}$ and $V_{BG}$ change the carrier type/density of the drain and source graphene layers by the electrostatic field, which can modulate $I_{DS}$. ITFETs or ThinTFETs may exhibit similar I-V characteristics.\textsuperscript{1145}

**Preventing fault injection:** Side-channel analysis, such as fault injection, power, and timing, allows attackers to learn about internal circuit signals without destroying the fabricated chips. Countermeasures have been proposed to balance the delay and power consumption when performing encryption/decryption at either the algorithm or circuit levels.\textsuperscript{1146} These methods often
cause higher power consumption and longer computation time in order to balance the side-channel signals under different conditions. Thus, an important goal is to prevent fault injection and to counter side-channel analysis by introducing low-cost, on-chip voltage/current monitors and protectors. Graphene SymFETs, which have a voltage-controlled unique peak current can be used to build low-cost, high-sensitivity circuit protectors through supply voltage monitoring.

Recent work has developed a SymFET-based power supply protector.\textsuperscript{1133,1134} With only two SymFETs, the power supply protector can easily monitor the supply voltage to ensure that the supply voltage to the circuit-under-protection is within a predefined range. In the event of a fault injection, the decreased supply voltage will power down the circuit rather than injecting a single-bit fault,\textsuperscript{1134} and can thus protect the circuit from fault injection attacks. If one uses $V_{\text{out}}$ as the power supply to a circuit under protection (e.g., an adder), due to the bell-shaped I-V characteristic of the SymFET, an intentional lowering of $V_{\text{DD}}$ cuts off the power supply. Thus, the sum and carry-out of the full adder output is '0', and no delay related faults are induced. A similar CMOS power supply protector would require op-amps for voltage comparison. As a result of the voltage/current monitors developed thus far, voltage/current-based fault injections can be largely prevented. By inserting the protectors in the critical components of a given circuit design, the power supply to these components can be monitored and protected.\textsuperscript{1135} (SymFET-based Boolean logic is also possible.\textsuperscript{1147})

**Preventing differential power analysis (DPA):** As an advanced side-channel attack scheme, DPA employs analysis of statistic power consumption measurements from a crypto system to obtain secret keys. Since the introduction of DPA\textsuperscript{1149}, there has been many efforts to develop low-cost and efficient countermeasures. Countermeasures are generally classified into two categories: 1) algorithm-level solutions and 2) hardware-level solutions.

**Algorithm-level solutions** aim to design cryptographic algorithms that can withstand a certain amount of information leakage,\textsuperscript{1148} e.g., frequently changing the keys to prevent the attacker from collecting enough power traces\textsuperscript{1149} or using masking bits during the internal stages to limit information leakage.\textsuperscript{1150}

A more practical circuit-level method for preventing DPA attack leverages a *sense amplifier-based logic* (SABL) or *current mode logic* (CML) for cryptographic algorithm implementations.\textsuperscript{1151} A CML gate includes a tail current source, a current steering core and a differential load. A CML gate will switch the constant current through the differential network of input transistors, utilizing the reduced voltage swing on the two load devices as the output. Although CML is not widely used in mainstream circuit design, its unique features, namely low latency and stable power consumption, can be leveraged to serve as a countermeasure against a DPA attack.

The strength of the CML-based approach is the constant power consumption of differential logic which can counter power-based attacks as operation power is independent of processed data. The drawback with these (mostly CMOS-based) logic designs, is their large area and power consumption when compared to static single ended logic. When considering hardware for the IoT (where the systems can be severely power constrained), system designers are presented with a dilemma in which they need to choose either high security or low power consumption. Emerging transistor technologies could help mitigate risks of DPA attacks while maintaining low power consumption.

Recent work has implemented a standard cell library of TFET CML gates and conducted a detailed study of their performance, power and area with respect to CMOS equivalents.\textsuperscript{1152} Standard cells were used to implement and evaluate TFET-based CML on a 32-bit KATAN cipher (a light-weight block cipher). All KATAN ciphers share the same key schedule with the key size of 80 bits as well as the 254-round iteration with the same non-linear function units.\textsuperscript{1153}

The two CML implementations consume less gate equivalents and area compared to the two static counterparts given that the majority of KATAN32 is made up by the D flip flops. The area of TFET CML KATAN32 is 1.441 $\mu$m\textsuperscript{2}, which is about 60% less than the Static TFET KATAN32. The power consumption of TFET CML (9.76 $\mu$W) is slightly lower than static CMOS (9.96 $\mu$W). It also outperforms CMOS CML.

Moreover, the correlation coefficient of a TFET static KATAN32 reaches its highest when the correct keys are applied. By comparison, the correlation coefficient of TFET CML KATAN32 is much more scattered, and all four hypothetical keys are equally distributed. Thus, the TFET CML KATAN32 implementation can successfully counteract CPA. Because the power consumption is mainly determined by AND/XOR logic gates of two nonlinear functions – and the effect of CPA is maximized – the correlation coefficients for KATAN32 are higher on average than other block ciphers, e.g., CPA on S-box\textsuperscript{1154}. 

---

**THE INTERNATIONAL ROADMAP FOR DEVICES AND SYSTEMS: 2021**

© 2021 IEEE. All rights reserved.
6. EMERGING MATERIALS INTEGRATION

6.1. INTRODUCTION AND SCOPE

6.1.1. CURRENT STATE OF TECHNOLOGY

The semiconductor industry was historically driven by a strong correlation between technology scaling and performance of most integrated circuits. The PC market required more complex and faster microprocessors that largely drove the development and scaling of transistors and memory. These devices required new materials and processes such as strained silicon, high-k gate dielectrics and metal gate electrodes that are now widely, and will continue, to be used in IC manufacturing. In the past decade, a completely new ecosystem has emerged. New system integrators, from mobile to data centers to the Internet of Everything, have appeared with new and complex technology requirements. These system integrators will have impact that includes microprocessors, but extends towards new applications including medicine, energy and the environment.

6.1.2. DRIVERS AND TECHNOLOGY TARGETS

As transistors and memory begin to run out of horizontal space and ICs continue to be limited by power, device technologies will enter a phase characterized by vertical integration and performance specifications driven towards reduction of power. New transistor, memory, interconnect, lithography materials and processes will be required to enable this new More Moore scaling paradigm. As conventional information processing and storage technology reaches its ultimate limits, entirely new non-CMOS logic and memory devices and even new, non-Von Neumann circuit architectures are potential Beyond CMOS solutions. Such solutions ideally can be integrated onto the Si-based platform to take advantage of the established processing infrastructure, as well as being able to include Si devices such as memories onto the same chip. However, while these technologies will likely be integrated on a Si-based platform, the vast majority of these Beyond CMOS technologies are based on entirely new materials and physics. Finally, new system integrators require materials that enable potentially trans-disciplinary advances in monolithically integrated complex functionality, i.e. functional scaling. Significant challenges must be overcome for these emerging materials to provide viable solutions for future integrated circuit technologies. To deliver these capabilities, enhanced Metrology will be needed to accelerate material evaluation, improvement and capabilities. The ultimate goal is to provide timely guidance on emerging material and process performance, cost, reliability, and sustainability options that will drive breakthrough advances in future manufacturing technology.

6.1.3. SCOPE

The IRDS represents a strategic repositioning of the community’s scope, needs, and set of emergent opportunities. In alignment with this new perspective, this edition of the emerging materials integration (EMI) sub-chapter represents a work in transition with a primary goal of aligning with the needs of related IRDS working groups. Much of the associated information in the detailed requirements and solutions tables comes from prior ERM chapters and input from current IRDS working groups, and will be updated in future editions. The chapter emphasizes strategic difficult challenges and/or enabling of novel, breakthrough and potentially disruptive opportunities for emerging material properties, synthetic methods, and metrology, organized in the following areas:

1. **Scaled technology materials needs for More Moore**: transistors, memory, interconnects, lithography, heterogeneous integration, assembly and packaging.
2. **Novel materials for Beyond CMOS**: emerging logic and information processing devices, emerging memory and storage devices, and novel computational paradigms and architectures.
3. **Potentially disruptive material opportunities for functional scaling and convergent applications**: Heterogenous components, outside system connectivity, and high impact application areas such as energy, environment, agriculture, health, medical, etc.

For all areas, the advancement requires an integration of emerging materials as illustrated in Figure BC-EMI 1.
6.2. CHALLENGES

6.2.1. NEAR-TERM CHALLENGES

Table EMI1 Near-term Difficult Challenges

<table>
<thead>
<tr>
<th>Near-Term Challenges: 2019–2024</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Materials and processes that achieve performance and power scaling of lateral fin- and nanowire FETs (Si, SiGe, Ge, III–V).</td>
<td>Integrated high-k dielectrics with EOT &lt;0.5nm and low leakage. Integrated contact structures that have ultralow contact resistivity. Achieving high hole mobility in III–V materials in FET structures. Processes for achieving low dislocations and anti-phase boundary generating interface between Ge/III–V channel materials and Si. Dopant placement and activation i.e. deterministic doping with desired number at precise location for Vth control and S/D formation in Si as well as alternate materials.</td>
</tr>
<tr>
<td>Materials and processes that improve copper interconnect resistance and reliability</td>
<td>Mitigate impact of size effects in interconnect structures. Patterning, cleaning, and filling at nano dimensions. Cu wiring barrier materials must prevent Cu diffusion into the adjacent dielectric but also must form a suitable, high quality interface with Cu to limit vacancy diffusion and achieve acceptable electromigration lifetimes. Reduction of the k value of inter-metal dielectrics.</td>
</tr>
<tr>
<td>Materials and processes that extend lithography to sub-10 nm dimensions with reproducible properties</td>
<td>Novel resists to extend 193 nm lithography and support EUV lithography. Directed self-assembly (DSA) with materials such as block-copolymers to potentially extend lithography though pattern rectification and pattern density multiplication.</td>
</tr>
<tr>
<td>Materials for heterogeneous integration of multi-chip, multi-function packages.</td>
<td>Materials to modify polymer properties to enable increased product reliability. Novel electrical attaching materials to allow lower assembly temperatures and improved product reliability. Simultaneously achieve package polymer CTE, modulus, electrical and thermal properties, with moisture and ion diffusion barriers. Nanosolders compatible with &lt;200C assembly, multiple refloows, high strength, and high electromigration resistance. Nanoinks that can be printed as die attach adhesives with required electrical, mechanical, thermal, and reliability properties.</td>
</tr>
</tbody>
</table>

6.2.2. LONG-TERM CHALLENGES

Table EMI2 Long-term Difficult Challenges

<table>
<thead>
<tr>
<th>Long-term Challenges: 2025–2032</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Materials and processes that achieve 3D monolithic and vertical integration of high mobility and steep subthreshold transistors</td>
<td>Processes for sequential 3D vertical integration of transistors. Methods to lower the synthesis temperature of vertical semiconductor nanowires. Methods to dope and contact vertical semiconductor nanowire transistors. Lithography-free and low-temperature methods to achieve gate stack on vertical transistors.</td>
</tr>
<tr>
<td>Materials and processes that replace copper interconnects with improved reliability and electromagnetic performance at the nanoscale</td>
<td>Synthesis or assembly of CNTs in predefined locations and directions with controlled diameters, chirality and site-density. Carbon and collective excitations. Novel interlayer dielectrics: Metal Organic Framework (MOF) and Carbon Organic Framework (COF). Metals with less size effects such as silicides.</td>
</tr>
<tr>
<td>Materials and processes for charge-based and non-charge-based beyond CMOS logic that replaces or extends CMOS</td>
<td>Achieving a bandgap and full interfaces control in graphene in FET structures and alternative FETs (TFETs etc.). Synthesis of CNTs with tight distribution of bandgap and mobility. Complex metal oxides with low defect density. High mobility transition metal dichalcogenides with low defect density and low resistance ohmic contacts. Spin materials: characterization of spin, magnetic and electrical properties and correlation to nanostructure. Topological materials: large bandgaps much greater than $kT$ at room temperature, ability to modulate bandgap efficiently with electric field. BiSFET heterostructures: achieving exciton condensation at room temperature.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Materials and processes for emerging memory and select devices to replace DRAM/NVM.</td>
<td>Multiferroic with Curie temperature $&gt;$400K and high remnant magnetization to $&gt;$400K. Ferromagnetic semiconductor with Curie temperature $&gt;$400K. Complex Oxides: Control of oxygen vacancy formation at metal interfaces and interactions of electrodes with oxygen and vacancies. Switching mechanism of atomic switch: Improvements in switching speed, cyclic endurance, uniformity of the switching bias voltage and resistances both for the on-state and the off-state.</td>
</tr>
<tr>
<td>Materials and processes that enable monolithically 3D integrated complex functionality including thermal and yield challenges</td>
<td>Integration on CMOS Platforms. Integration with flexible electronics. Biocompatible functional materials. Leveraging convergent materials expertise in adjacent sectors, including More than Moore functionalities (photonic, optics/metamaterials, outside connectivity, energy transfer/storage, power circuits).</td>
</tr>
</tbody>
</table>

### 6.3. TECHNOLOGY REQUIREMENTS AND POTENTIAL SOLUTIONS

#### 6.3.1. SUMMARY

The IRDS seeks a framework for managing the convergence of scaled information processing and storage, i.e., More Moore (MM) and Beyond CMOS (BC), with the next emerging era of monolithically integrated systems that achieve enhanced overall functional density. The trend towards the convergence of monolithically integrated functional diversification with miniaturization manifests as increasing complexity in the road-mapping process. The IRDS reflects this growing complexity, with an increasing number of projected roadmap parameters and requirements associated with new functionalities. While EMI continues to support the evolutionary, and semiconductor centric needs of the traditional semiconductor community, emerging architectures could benefit from new device functionality, which may require new materials and new physical mechanisms. New waves of emerging materials technologies may represent potentially disruptive opportunities.

Candidate EMI materials and processes exhibit unique and useful properties that may require atomic level structural, interface, defect and compositional control. In some cases, current synthetic or manufacturing technologies are not yet capable of producing such materials with the required level of control. The difficulties could be due to: 1) The inability of a research environment to produce materials with the required level of control that would express the desired properties; or 2) scaling up the synthetic and fabrication processes to satisfy commercial manufacturing requirements. In some cases, current materials growth processes effect unacceptable levels of defect formation, which drive the need for new and more robust fabrication methods. In other cases, synthetic methods exist for producing high quality materials, but these processes cannot be scaled to the higher growth rates, yields, or purity needed for insertion into viable commercial applications. While these materials may provide proof of concept and suggest a potential solution, new cost effective fabrication technologies may be required to warrant a candidate material’s insertion into high volume manufacturing.

#### 6.3.2. SCALED TECHNOLOGY MATERIALS FOR MORE MOORE

As described in the More Moore chapter, after 2027 there is no headroom for 2D geometry scaling and 3D VLSI integration of circuits and systems using sequential/stacked integration approaches will likely begin. Whether one is considering 2D geometry scaling or 3D integration, there are numerous materials challenges to achieving increasing device density and integrated performance. The following outlines key materials challenges for transistor scaling and integration, lithography, interconnects, heterogenous integration, assembly and packaging, and outside system connectivity.

#### 6.3.2.1. MATERIALS FOR TRANSISTOR SCALING AND INTEGRATION

Continued increases in transistor device density require a variety of new materials and processes including new channels (Ge, III-V), improved doping techniques, gate stacks and contacting structures. Table EMI3 provides a set of materials and processes priorities for transistor scaling and integration.

|Table EMI3| Materials for Transistor Scaling and Integration|
6.3.2.2. MATERIALS FOR LITHOGRAPHY AND PATTERNING

The future of scaled technologies depends upon emerging patterning materials (resist or self-assembled) to enable extensible lithographic capabilities. New resist materials must concurrently exhibit higher resolution, higher sensitivity, reduced line edge roughness, and sufficient etch resistance to enable robust pattern transfer. 193nm and EUV extension materials are being developed which can improve LWR, pattern shrink materials, and topcoats for EUV to ameliorate issues with out-of-band optical flare and outgassing. Evolutionary approaches for enhancing positive, negative, and chemically amplified families of resists will continue to be evaluated. Leading process approaches to pitch division include multiple patterning (MP) and spacer patterning (SP) as options for extending 193nm immersion lithography. Alternate technologies are utilizing patterning materials to create guide patterns for directed self-assembly, which can include resists to form chemoepitaxy and graphoepitaxy guides, or directly patternable brushes and SAMs. Directed self-assembly (DSA) with block-copolymers or polymer pairs has made significant progress in characterizing sources of defect formation and in applications such as contact rectification, fin patterning, and pattern density multiplication. Table EMI4 provides a set of materials and processes priorities for lithography and patterning.

Table EMI4  Materials for Lithography and Patterning

6.3.2.3. INTERCONNECT MATERIALS

Key challenges for continued increased performance of future integrated circuit interconnects consist of maintaining reductions of RC time constants for delivery of signals and power with high reliability. For copper interconnects, the sidewall copper barrier thickness must continue to be reduced, which is a significant challenge. For post copper interconnect scaling, novel interconnects, such as carbon nanotubes, are being explored. Also, lower dielectric constant (κ for both intra and inter level dielectric are needed; however, each of these emerging families of materials must overcome significant challenges for them to warrant adoption. Airgap, another approach to reducing the effective κ, places additional requirements on barrier layers or novel interconnects. Table EMI5 provides a set of materials and processes priorities for interconnects.

Table EMI5  Interconnect Materials

6.3.2.4. HETEROGENEOUS INTEGRATION, ASSEMBLY AND PACKAGING MATERIALS

The EMI and Heterogeneous Integration teams are in the process of prioritizing key heterogeneous integration and assembly & packaging EMI challenges, which include:

- New engineered materials: substrate, mold, underfill, wafer bond alloys, solder alloys
- Conductors: Nanomaterials (CNT, graphene, NWs), metals (Cu, Al, W, Ag, etc.), composites
- Dielectrics: Oxides, polymers, porous materials, composites
- Semiconductors: Elemental (Si, Ge), Compounds (SiC, III-V, II-VI, tertiary), polymers
- Critical factors: Cost, CTE differential, thermal conductivity, fracture toughness, modulus, processing temperature, interfacial adhesion, operating temperature, and breakdown field strength

Table EMI6 provides a set of heterogeneous integration and assembly and packaging priorities for EMI.

Table EMI6  Heterogeneous Integration, Assembly and Packaging Materials

6.3.2.5. MATERIALS CHALLENGES FOR OUTSIDE SYSTEM CONNECTIVITY

Table EMI7 provides a set of top Outside System Connectivity material priorities for EMI.

Table EMI7  Emerging Research Materials Needs for Outside System Connectivity
6.3.3. **Emerging Materials for Memory, Beyond CMOS Logic and Computing**

Beyond 2030, MOSFET scaling will likely become ineffective and/or very costly. As described in this chapter, completely new, non-CMOS types of memory, logic devices and maybe even new circuit architectures are potential solutions. Such solutions ideally can be integrated onto the Si-based platform to take advantage of the established processing infrastructure, as well as being able to include Si devices as memories onto the same chip. The following outlines key materials challenges for emerging materials for memory, beyond CMOS logic and alternative information processing.

6.3.3.1. **Emerging Materials for Memory**

Emerging memory devices includes capacitive memories (Fe FET), and resistive memories including ferroelectric devices, resistance change devices, devices based on Mott transitions and novel magnetic memories. Another key requirement for memory technology is the development of corresponding select devices that access only the selected memory cell of interest without perturbing non-selected cells. Table EMI8 provides a set of materials and associated challenges for emerging memory materials, and Table EMI9 provides materials and associated challenges for memory select.

![Table EMI8](#)

**Table EMI8**  
Emerging Materials for Memory

![Table EMI9](#)

**Table EMI9**  
Emerging Materials for Memory Select

6.3.3.2. **Emerging Materials for Advanced and Beyond-CMOS Logic Devices**

There are generally two classes of devices/materials for advanced and beyond-CMOS logic devices. The first are those that do not involve spin or magnetism such as ferroelectric FETs, nanoelectromechanical (NEM) switches, topological FETs, and transistors based on collective electron phenomena such as Mott effect or exciton condensation (BiSFET). The second are those based on spin and magnetism that each uses a variety of materials. Table EMI10 contains materials and associated challenges for the non-spin devices. Table EMI11 maps various spin device concepts to associated materials types and Table EMI12 describes the requirements of these materials.

![Table EMI10](#)

**Table EMI10**  
Emerging Materials for Advanced and Beyond-CMOS Logic Devices

![Table EMI11](#)

**Table EMI11**  
Spin Devices versus Materials

![Table EMI12](#)

**Table EMI12**  
Spin Material Requirements and Properties

6.3.3.3. **Emerging Materials for Novel Computing**

Emerging materials spur developments of novel computing, such as neuromorphic computing, reinforcement learning, topological quantum computing, and reversible computing, and probabilistic computing. Since the performance of the computing is considered to be dependent on the intrinsic properties of the emerging material, the material research will further boost the performance, such as the energy efficiency.\(^{1155,1156,1157,1158,1159,1160}\)

6.3.4. **Metrology Needs and Challenges for Emerging Research Materials**

Metrology is needed to characterize composition, properties, and understand structure of emerging research materials, at nanometer dimensions and below. The most difficult EMI metrology challenges would be those associated with the introduction of directed self-assembly (DSA), such as evaluating critical material properties, size and location of features, registration, and defects. Also needed are non-destructive methods for characterizing embedded materials and interfaces defects, as well as platforms that enable simultaneous measurement of complex nanoscopic properties, and modeling of probe-sample interactions. Table EMI13 summarizes the current set of continuing and prioritized metrology related EMI challenges and needs.

![Table EMI13](#)

**Table EMI13**  
Metrology Needs and Challenges for Emerging Research Materials
6.4. EMERGING/DISRUPTIVE CONCEPTS AND TECHNOLOGIES

As mentioned at the beginning of the chapter, new system integrators, from mobile to data centers to the Internet of Everything, have appeared with new and complex technology requirements. These application domains require a highly interdisciplinary set of expertise, e.g., electrical and mechanical engineering; as well as materials, biological, medical, energy, aerospace, transportation, communication, and sustainability sciences. The trend towards the convergence of monolithically integrated functional diversification with miniaturization manifests as increasing complexity in the road-mapping process. Collaborative transdisciplinary research is needed to identify materials and processes that catalyze breakthrough and convergent advances in these technologies. Initiatives that leverage the expertise of colleagues in adjacent spaces who know the local environment, e.g., biology, energy, etc., will help to drive novel approaches and more optimal materials, process, manufacturing, and performance solutions to emerging IoT challenges than can be achieved by semiconductor centric approaches. As examples, (6.4.1) transient concept and (6.4.2) development aided by machine learning (Table EMI14) are shown. Table EMI15 identifies several emerging application opportunities that will drive and enhance future EMI working group activities.

6.4.1. TRANSPORT ELECTRONICS

Transient electronics is an emerging field that requires materials, devices, and systems to be capable of disappearing with minimal or non-traceable remains in a controllable period of time. The spontaneous and transient function appears after the stable operation. This emerging electronics with the disintegrating capability will bring about intelligent applications in various scenes, such as bioelectronics, environmentally friendly electronics. The conductance change with the controllable decay characteristics was demonstrated in molecular gap atomic switches. Meanwhile, a performance of fuel cell can be derived from macro-model originated from the rate equation of chemical reactions of individual molecules. Multiscale view of carrier transport in organic devices were treated by considering molecular orbital levels to mesoscopic scale of electron-hopping. Beside the direct approach on multiscale physics, aid of machine learning can bridge the difference scales phenomena in composite material. These approaches will accelerate the simulation, while proper modeling with understanding of natural physics in difference scales of time and space are still necessary. Finite element analysis (FEA) models will have to be further developed so that they can adequately represent 2D and other nanomaterials.

Table EMI14  Modeling and Simulation

<table>
<thead>
<tr>
<th>Multiscale simulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiscale physics</td>
</tr>
<tr>
<td>Phenomena</td>
</tr>
<tr>
<td>Continuum level</td>
</tr>
<tr>
<td>Length scale (in log)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Multiscale physics and informatics</th>
</tr>
</thead>
<tbody>
<tr>
<td>(an example)</td>
</tr>
<tr>
<td>Phenomena</td>
</tr>
<tr>
<td>Continuum level</td>
</tr>
<tr>
<td>Length scale (in log)</td>
</tr>
</tbody>
</table>

Figure EMI2  An Example of the Role of Machine Learning in the Multiscale Simulation
Note: The left shows conventional multiscale physics where physics to explain mesoscopic level phenomena is required to link molecular and continuum level phenomena. The right shows a potential role of machine learning that provides output of continuum level phenomena from inputs of molecular level phenomena.

Table EMI15  Summary of Potentially Disruptive Emerging Research Materials Application Opportunities

6.5. CONCLUSIONS AND RECOMMENDATIONS

The IRDS represents a strategic repositioning of the community’s scope, needs, and set of emergent opportunities. In alignment with this new perspective, this edition of the EMI chapter represents a work in transition that has aligned difficult challenges with the needs of related IRDS working groups. Much of the information in the detailed tables comes from prior ERM chapters and current IRDS working groups. Future editions of EMI will provide additional detailed descriptions and continue to adapt its scope to engage with a new set of EMIs, many of which will be identified by the IRDS working groups.

7. ASSESSMENT

7.1. INTRODUCTION

It is important to assess beyond-CMOS devices considered in this chapter against current CMOS technologies. Two methods of assessments have been reported previously in the ITRS ERD chapter: a “quantitative emerging device benchmarking” conducted by the Nanoelectronics Research Initiative (NRI) and a “survey-based assessment” conducted by the ERD working group.

In the “NRI benchmarking”, each emerging device is evaluated by its operation in conventional Boolean Logic circuits, e.g., a unity gain inverter, a 2-input NAND gate, and a 32-bit shift register. Metrics evaluated include speed, areal footprint, power dissipation, etc. Each parameter is compared with the performance projected for high performance and low power 5 nm CMOS applications. This “beyond CMOS” chapter will update the quantitative benchmarking section with the latest NRI results.

Up to the 2013 ERD Chapter, a survey-based critical review was conducted based on eight criteria to compare emerging devices against their CMOS benchmark. Spider chart has been used to visualize the perceived potential of these technology entries. However, the limited number of survey results sometimes raises questions of the accuracy of this survey. The most recent “survey-based assessment” was conducted in the 2014 ERD Emerging Memory and Logic Device Assessment Workshops (Albuquerque, NM). The survey collects voting on emerging technologies evaluated in the workshops in the categories of the “most promising” and the “most need of resources” to assess the potential of these technology entries perceived by ERD experts. A summary of previous survey-based assessments is included in this chapter as an archive.

An important issue regarding emerging charge-based nanoelectronic switch elements is related to the fundamental limits to the scaling of these new devices, and how they compare with CMOS technology at its projected end of scaling. An analysis concludes that the fundamental limit of scaling an electronic charge-based switch is only a factor of 3 times smaller than the physical gate length of a silicon MOSFET in 2024. Furthermore, the density of these switches is limited by a maximum allowable power dissipation of approximately 100W/cm², and not by their size. The conclusion of this work is that MOSFET technology scaled to its practical limit in terms of size and power density will asymptotically reach the theoretical limits of scaling for charge-based devices.

Most of the proposed beyond-CMOS devices are very different from their CMOS counterparts, and often pass computational state variables (or tokens) other than charge. Alternative state variables include collective or single spins, excitons, plasmons, photons, magnetic domains, qubits, and even material domains (e.g., ferromagnetic). With the multiplicity of programs characterizing the physics of proposed new structures, it is necessary to find ways to benchmark the technologies effectively. This requires a combination of existing benchmarks used for CMOS and new benchmarks which take into account the idiosyncrasies of the new device behavior. Even more challenging is to extend this process to consider new circuits and architectures beyond the Boolean architecture used by CMOS today, which may enable these devices to complete transactions more effectively.

7.1.1. ARCHITECTURAL REQUIREMENTS FOR A COMPETITIVE LOGIC DEVICE

The circuit designer and architect depend on the logic switch to exhibit specific desired characteristics in order to insure successful realization of a wide range of applications. These characteristics, which have since been supplemented in the literature, include:

- Inversion and flexibility (can form an infinite number of logic functions)
Devices with intrinsic properties supporting the above features will be adopted more readily by the industry. Moreover, devices which enable architectures that address emerging concerns such as computational efficiency, complexity management, self-organized reliability and serviceability, and intrinsic cyber-security are particularly valuable.

### 7.2. NRI BEYOND-CMOS BENCHMARKING

The Nanoelectronics Research Initiative (https://www.src.org/program/nri/) has been benchmarking several diverse beyond-CMOS technologies, trying to balance the need for quantitative metrics to assess a new device concept’s potential with the need to allow device research to progress in new directions which might not lend themselves to existing metrics. Several of the more promising NRI devices have been described in detail in the Logic and Emerging Information Processing Device Section. Some results of this benchmark study were included in 2015 ITRS ERD chapter.

While all these efforts are still very much a work in progress – and no concrete decisions have been made on which devices should be chosen or eliminated as candidates for significantly extending or augmenting the roadmap as CMOS scaling slows – this section summarizes some of the data and insights gained from these studies. Further benchmarks may alter some of the conclusions here and the outlook on some of these devices, but the overall message on the challenge of finding a beyond CMOS device which can compete well across the full spectrum of benchmarks of interest remains.

#### 7.2.1. QUANTITATIVE RESULTS

NRI benchmarking analyzes the potential of major emerging switches using a variety of information tokens and communication transport mechanisms. Specifically, the projected effectiveness of these devices used in a number of logic gate configurations was evaluated and normalized to CMOS at the 5nm generation (projection). The initial work has focused on “standard” Boolean logic architecture, since the CMOS equivalent is readily available for comparison. It should be noted that the majority of devices are evaluated via simulations since many of them have not yet been built, so it should be considered only a “snapshot in time” of the potential of any given device. Data on all of them are still evolving.

At a high level, the data from these studies corroborates qualitative insights from earlier works, suggesting that many new logic switch structures may have some advantages over CMOS in terms of power or energy, but they are also inferior to CMOS in delay. This is perhaps not surprising; the primary goal for nanoelectronics and NRI is to find a lower power device since power density is a primary concern for future CMOS scaling. The power-speed tradeoffs commonly observed in CMOS are also extended into the emerging devices. It is also important to understand the impact of transport delay for the different information tokens these devices employ. Communication with many non-charge tokens can be significantly slower than moving charge, although this may be balanced in some cases with lower energy for transport. The combination of the new balance between switch speed, switch area, and interconnect speed can lead to advantages in the span of control for a given technology. For some of the technologies (e.g., nanomagnetic logic), there is no strong distinction between the switch and the interconnect, indicating the need for novel architecture to exploit unique attributes of these technologies.

A simplified 32-bit arithmetic logic unit (ALU) was built from these devices to evaluate their performance and the result is summarized in Figure BC7.1(a). While tunneling devices (e.g., TFET) show limited advantages over CMOS in terms of energy-delay product, most beyond-CMOS devices are inferior to CMOS in energy and/or delay. For example, the majority of spintronic devices are slower than CMOS and also show no energy advantage.
At the architecture level, the ability to speculate on how these devices will perform is still in its infancy. While the ultimate goal is to compare at a very high level—e.g., how many MIPS can be produced for 100 mW in 1 mm²?—the current work must extrapolate from only very primitive gate structures. One initial attempt to start this process has been to look at the relative “logical effort” for these technologies, a figure of merit that ties fundamental technology to a resulting logic transaction. Several of the devices appear to offer advantage over CMOS in logical effort, particular for more complex functions, which increases the urgency of doing more joint device-architecture co-design for these emerging technologies.

The direction of device-architecture co-optimization has driven NRI benchmarking to explore non-Boolean applications of beyond-CMOS devices. Cellular Neural Network (CNN) has been utilized as a benchmarking model that has been implemented with various novel devices. The energy and delay of CNN based on beyond-CMOS devices are compared with CMOS-based CNN in Figure BC7.1(b). Tunneling devices have significant performance improvement because of their steep subthreshold slopes and large driving current at ultra-low supply voltage. Interestingly, spintronic devices are much closer to the preferred corner in CNN implementation in comparison with 32-bit ALU. This is because some characteristics of spintronic devices (e.g., spin diffusion, domain wall motion) may mimic the functionality of a neuron (e.g., integration) more naturally in a single device.

7.2.2. Observations
A number of common themes have emerged from these benchmark studies and in the observations made during recent studies of beyond-CMOS replacement switches. A few noteworthy concepts:

1. The low voltage energy-delay tradeoff conundrum will continue to be a challenge for all devices. Getting to low voltage must remain a priority for achieving low power, but new approaches to getting throughput with ‘slow’ devices must be developed.

2. Most of the architectures that have been considered to date in the context of new devices utilize binary logic to implement von Neumann computing structures. In this area, CMOS implementations are difficult to supplant because they are very competitive across the spectrum of energy, delay and area—not surprising since these architectures have evolved over several decades to exploit the properties of CMOS most effectively. Novel electron-based devices—which can include devices that take advantage of collective and non-equilibrium effects—appear to be the best candidates as a drop-in replacement for CMOS for binary logic applications.

3. As the behavior of other emerging research devices becomes better understood, work on novel architectures that leverage these features will be increasingly important. A device that may not be competitive at doing a simple NAND function may have advantages in doing a complex adder or multiplier instead. Understanding the right building blocks for each device to maximize throughput of the system will be critical. This may be best accomplished by thinking about the high-level metric a system or core is designed to achieve (e.g., computation, pattern recognition, FFT, etc.) and finding the best match between the device and circuit for maximizing this metric.
4. Increasing functional integration and on-chip switch count will continue to grow. To that end, in any logic architectural alternative, both flexible rich logic circuit libraries and reconfigurability will be required for new switch implementations.

5. Patterning, precision layer deposition, material purity, dopant placement, and alignment precision critical to CMOS will continue to be important in the realization of architectures using these new switches.

6. Assessment of novel architectures using new switches must also include the transport mechanism for the information tokens. Fundamental relationships connecting information generation with information communication spatially and temporally will dictate CMOS’ successor.

Based on the current data and observations, it is clear that CMOS will remain the primary basis for IC chips for the coming years. While it is unlikely that any of the current emerging devices could entirely replace CMOS, several do seem to offer advantages, such as ultra-low power or nonvolatility, which could be utilized to augment CMOS or to enable better performance in specific application spaces. One potential area for entry is that of special purpose cores or accelerators that could off-load specific computations from the primary general purpose processor and provide overall improvement in system performance. If scaling slows in delivering the historically expected performance improvements in future generations, heterogeneous multi-core chips may be a more attractive option. These would include specific, custom-designed cores dedicated to accelerate high-value functions, such as accelerators already widely used today in CMOS (e.g. Encryption/Decryption, Compression/Decompression, Floating Point Units, Digital Signal Processors, etc.), as well as potentially new, higher-level functions (e.g. voice recognition). While integrating dissimilar technologies and materials is a big challenge, advances in packaging and 3D integration may make this more feasible over time, but the performance improvement would need to be large to balance this effort.

As a general rule, an accelerator is considered as an adjunct to the core processors if replacing its software implementation improves overall core processor throughput by approximately ten percent; an accelerator using a non-CMOS technology would likely need to offer an order of magnitude performance improvement relative to its CMOS implementation to be considered worthwhile. That is a high bar, but there may be instances where the unique characteristics of emerging devices, combined with a complementary architecture, could be used as an advantage in implementing a particular function. At the same time, the changing landscape of electronics (moving from uniform, general purpose computing devices to a spectrum of devices with varying purposes, power constraints, and environments spanning servers in data centers to smart phones to embedded sensors) and the changing landscape of workloads and processing needs (Big Data, unstructured information, real-time computing, 3D rich graphics) are increasing the need for new computing solutions. One of the primary goals then for future beyond-CMOS work should be to focus on specific emerging functions and optimize between the device and architecture to achieve solutions that can break through the current power/performance limits.

7.3. Archive of ITRS ERD Survey-Based Assessment

Although survey-based emerging device assessment has not been continued after the 2015 ITRS ERD chapter, previous survey-based assessments in ERD chapters are summarized here for references.

**7.3.1. Emerging Device Assessment in 2014 ERD Workshops**

In August 2014, ERD organized an “Emerging Memory Device Assessment Workshop” and an “Emerging Logic Device Assessment Workshop”, where nine memory devices and fourteen logic devices were evaluated. A survey was conducted in the workshops for the experts to vote on the “most promising” devices and devices “needing more resources”. Figure BC7.2 shows the relative number of votes received by emerging devices in these two categories, ranked from high to low in the “most promising” category (red color bars).

In the “most promising” memory device category, the vote clearly accumulated to a few well-known memory devices: STTRAM, ReRAM (including CBRAM and oxide-based ReRAM), and PCM, ranked from high to low. Some memory devices received few vote, due to lack of progress. Results in this category reflect consensus among experts based on R&D status of these devices. The “need more resources” category reflects perceived value of these devices in the view of the experts and also experts’ consideration of R&D resource allocation based on existing investment (or lack of investment) for each device. For example, with heavy R&D investment on STTRAM that is considered most promising, it is not surprising that it ranks low in the need of resources. The strong interest in emerging FeFET memory is closely linked to the discovery of ferroelectricity in doped HfO$_x$. Among emerging logic devices, “carbon nanomaterial device” (mainly carbon nanotube FET), tunnel FET, and nanowire FET were ranked as one of the most promising emerging logic devices. Notice that they are all charge-based devices, but involve novel materials, structures, and mechanisms. “Piezotronic transistors”, “negative-capacitance FET”, and “2D channel FET” were considered top choices for enhanced research investment.
7.3.2. 2013 ERD Survey Criteria, Methodology, and Results

In the traditional survey-based assessment conducted by ERD, a set of relevance or evaluation criteria, defined below, are used to parameterize the extent to which “CMOS Extension” and “Beyond CMOS” technologies are applicable to memory or information processing applications. The relevance criteria are: 1) Scalability, 2) Speed, 3) Energy Efficiency, 4) Gain (Logic) or ON/OFF Ratio (Memory), 5) Operational Reliability, 6) Operational Temperature, 7) CMOS Technological Compatibility, and 8) CMOS Architectural Compatibility. Description of each criterion can be found in 2013 ERD chapter.

Each CMOS extension and beyond-CMOS emerging memory and logic device technology is evaluated against these criteria according to a single factor. For logic, this factor relates to the projected potential performance of a nanoscale device technology, assuming its successful development to maturity, compared to that for silicon CMOS scaled to the end of the Roadmap. For memory, this factor relates the projected potential performance of each nanoscale memory device technology, assuming its successful development to maturity, compared to that for ultimately scaled current silicon memory technology which the new memory would displace. Performance potential for each criterion is assigned a value from 1–3, with “3” substantially exceeding ultimately-scaled CMOS, and “1” substantially inferior to CMOS or, again, a comparable existing memory technology. This evaluation is determined by a survey of the ERD Working Group members composed of individuals representing a broad range of technical backgrounds and expertise. Details of the assessment values are also included in 2013 ERD chapter.

Although this survey-based critical review has been conducted in ERD for several versions and has been widely cited in literatures, the decreasing number of votes of some less popular devices has raised concerns about the accuracy of some of the results. Figures BC7.3 and BC7.4 summarize the last critical review conducted in 2013 for emerging memory devices and emerging logic devices, respectively. Notice that the technology entries in these figures are based on the 2013 ERD chapter, while some of them have been removed in this chapter (e.g., molecular memory, atomic switch, etc.) and several new technologies are added in this chapter (e.g., novel magnetic memory, transistor laser, etc.).
Since “3” represents the best result and “1” the worst in the spider chart, devices with larger circle area represent more promising devices. In Figure BC7.4 for emerging logic devices, the perceived potential of “beyond-CMOS devices” is generally poorer than “CMOS-extension devices”. Within “beyond-CMOS devices”, “non-charge-based devices” area also perceived slightly less promising than “charge-based devices”. The general trend is consistent with the quantitative NRI assessment in section 7.2. Multiple factors contribute to this result, including the strength of CMOS as a platform technology, the challenges of beyond-CMOS devices in materials, fabrication, and even mechanisms, the lack of memory and interconnect solutions for beyond-CMOS devices, etc.

8. SUMMARY

The “Beyond CMOS” chapter systematically surveys emerging memory and logic devices (sections 2 and 3), novel technologies (section 4), and alternative architectures and computing paradigms (section 5), to explore potential solutions beyond the conventional scaling of CMOS technologies. Although high performance at low power consumption has been a primary objective of beyond-CMOS devices, novel functionalities and applications have become increasingly important. The recent emergence of energy-efficient data-intensive cognitive applications is also shifting the emphasis from high-precision computing solutions to novel computing paradigms with massive parallelism and bio-inspired mechanisms. Research opportunities exist in the co-optimization of beyond-CMOS devices and architectures to explore unique device characteristics and architectural designs.

Although a beyond-CMOS device competitive against CMOS FET has not been identified, beyond-CMOS devices with dramatically enhanced scalability and performance while simultaneously reducing the energy dissipation per functional operation would still be fundamentally important and a worthwhile research objective. In considering the many disparate new approaches proposed to provide order of magnitude scaling of information processing beyond that attainable with ultimately scaled CMOS,
the following set of guiding principles are proposed to provide a useful structure for directing research on “Beyond CMOS” information processing technology.

- **Computational State Variable(s) other than Solely Electron Charge**
  These include spin, phase, multipole orientation, mechanical position, polarity, orbital symmetry, magnetic flux quanta, molecular configuration, and other quantum states. The estimated performance comparison of alternative state variable devices to ultimately scaled CMOS should be made as early in a program as possible to down-select and identify key trade-offs.

- **Non-thermal Equilibrium Systems**
  These are systems that are out of equilibrium with the ambient thermal environment for some period of their operation, thereby reducing the perturbations of stored information energy in the system caused by thermal interactions with the environment. The purpose is to allow lower energy computational processing while maintaining information integrity.

- **Novel Energy Transfer Interactions**
  These interactions would provide the interconnect function between communicating information processing elements. Energy transfer mechanisms for device interconnection could be based on short range interactions, including, for example, quantum exchange and double exchange interactions, electron hopping, Förster coupling (dipole–dipole coupling), tunneling and coherent phonons.

- **Nanoscale Thermal Management**
  This could be accomplished by manipulating lattice phonons for constructive energy transport and heat removal.

- **Sub-lithographic Manufacturing Process**
  One example of this principle is directed self-assembly of complex structures composed of nanoscale building blocks. These self-assembly approaches should address non-regular, hierarchically organized structures, be tied to specific device ideas, and be consistent with high volume manufacturing processes.

- **Alternative Architectures**
  In this case, architecture is the functional arrangement on a single chip of interconnected devices that includes embedded computational components. These architectures could utilize, for special purposes, novel devices other than CMOS to perform unique functions.
9. ENDNOTES/REFERENCES


X. Tian, and A. Toriumi, “New opportunity of ferroelectric tunnel junction memory with ultrathin HfO2-based oxides,” *Electron Devices Technology and Manufacturing Conference (EDTM), 2017 IEEE* (pp. 36-64). IEEE.


90 Endnotes/References


Endnotes/References


272 www.micron.com/about/innovations/3d-xpoint-technology


283 K. H. Kim, “Memory Interfaces for M-Class SCMs,” ITRS SCM workshop, July 2012.


E. Memisevic, J. Svensson, M. Hellenbrand, E. Lind, and L. E. Wernersson, "Vertical InAs/GaAsSb/GaSb tunneling field-effect transistor on Si with S = 48 mV/decade and Ion = 10 $\mu$A/$\mu$m for Ioff = 1 nA/$\mu$m at Vds = 0.3 V," *2016 IEEE International Electron Devices Meeting (IEDM)*, 2016, p. 19.1.1–19.1.4.


U. E. Avci *et al.*, "Study of TFET non-ideality effects for determination of geometry and defect density requirements for sub-60mV/dec Ge TFET," *2015 IEEE International Electron Devices Meeting (IEDM)*, 2015, p. 34.5.1–34.5.4.


K. Kato, V. Stojanović and T. H. Fariborzi et al., “Analysis and demonstration of MEM


104 Endnotes/References


Endnotes/References 111


112 Endnotes/References


M. D. Pickett, G. Medeiros-Ribeiro, and R. S. Williams, “A scalable neuristor built with Mott memristors.”


Endnotes/References

1024 M. P. Frank and T. F. Knight Jr., “Ultimate theoretical models of nanocomputers.” Nano
technology 9, no. 3, 1998.


120 Endnotes/References


