Emerging Reconfigurable Nanotechnologies: Can they support Future Electronics?

(Invited Paper)

Shubham Rai[1], Srivatsa Srinivasa[2], Patsy Cadareanu[3], Xunzhao Yin[4], Xiaobo Sharon Hu[4], Pierre-Emmanuel Gaillardon[3], Vijaykrishnan Narayanan[2], Akash Kumar[1]

(1) CfAED Technische Universität Dresden, Germany, (2) Pennsylvania State University, USA, (3) The University of Utah, USA, (4) University of Notre Dame, USA

ABSTRACT

Several emerging reconfigurable technologies have been explored in recent years offering device level runtime reconfigurability. These technologies offer the freedom to choose between p- and n-type functionality from a single transistor. In order to optimally utilize the feature-sets of these technologies, circuit designs and storage elements require novel design to complement the existing and future electronic requirements. An important aspect to sustain such endeavors is to supplement the existing design flow from the device level to the circuit level. This should be backed by a thorough evaluation so as to ascertain the feasibility of such explorations. Additionally, since these technologies offer runtime reconfigurability and often encapsulate more than one functions, hardware security features like polymorphic logic gates and on-chip key storage come naturally cheap with circuits based on these reconfigurable technologies. This paper presents innovative approaches devised for circuit designs harnessing the reconfigurable features of these nanotechnologies. New circuit design paradigms based on these nano devices will be discussed to brainstorm on exciting avenues for novel computing elements.

ACM Reference Format:

Shubham Rai[1], Srivatsa Srinivasa[2], Patsy Cadareanu[3], Xunzhao Yin[4], Xiaobo Sharon Hu[4], Pierre-Emmanuel Gaillardon[3], Vijaykrishnan Narayanan[2], Akash Kumar[1] (1) CfAED Technische Universität Dresden, Germany, (2) Pennsylvania State University, USA, (3) The University of Utah, USA, (4) University of Notre Dame, USA . 2018. Emerging Reconfigurable Nanotechnologies: Can they support Future Electronics?: *(Invited Paper)*. In *IEEE/ACM INTERNATIONAL CONFERENCE ON COMPUTER-AIDED DESIGN (ICCAD '18), November 5–8, 2018, San Diego, CA, USA*. ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3240765.3243472

1 INTRODUCTION

Runtime-reconfigurable emerging devices show symmetrical p- and n-type functionality at the transistor level just by applying different biases at the gate terminals. Several devices below 45 nm exhibit this ambipolarity. Reconfigurable technology is demonstrated by transistors made with materials like silicon nanowires [19, 31], carbon nanotubes [29], graphene nanoribbons [17], and even 2-D materials such as tungsten diselenide (WSe_2) [47]. Reconfigurable transistors based circuits and systems are a potential solution to complement the existing CMOS technology for fulfilling the requirements of future electronics.

While CMOS scaling has promised higher performance and smaller area from last few decades, the reconfigurable behavior shown by these technologies can enable the circuit designers to pack more functions per computational unit. This leads to reduced delay (smaller critical paths [43]), area [56], and overall energy-delay-product [48] for the entire circuit.

Efficient design flow is imperative to make use of these functionally enhanced transistors for larger circuits. Recently, majority logic was proposed as the natural abstraction for newer nanotechnology and this forms the basis for new majority inverter graph (MIG) synthesis flow [3]. An area optimizing technology mapping flow exploiting functionally enhanced logic gates [56] was proposed in [41]. The authors incorporated inverter minimization to have more area savings specially designed for silicon nanowires FETs-based logic gates. Apart from logic synthesis flow, a crucial aspect is to devise physical synthesis flows which can evaluate the promise which newer nanotechnologies hold, on larger benchmarks. An early evaluation has been carried out in [42] for silicon nanowire reconfigurable FETs based circuits. Such evaluation is necessary to extrapolate how a lab-level research technology competes with CMOS for larger and more complex circuits.

Apart from processing elements like adders which have been shown to exploit features of these re-configurable devices [43, 2], memories also form a critical component. The emergence of new devices and technology enables blurring the gap between memory and logic functionality. Technology support enables configuring the accessing mechanism of a memory either using an address (random access of data) or using a value (CAM). 3D integration process coupled with biasing schemes enhance the memory stability through dynamic assist mechanisms. Emerging nonvolatile memory cells provide the ability to trade-off metrics such as retention-times for factors such as power and access latency. In addition, novel cell structures allow one to incorporate computation at the bit-level, row-level or bank-level.

Another major application in which the reconfigurable devices fit in as a suitable candidate is *Hardware security* owing to their runtime reconfigurability and symmetrical I-V characteristics at the transistor level. Hardware security concerns such as intellectual property (IP) piracy and hardware Trojans have triggered research into circuit protection and malicious logic detection from various design perspectives. Since these reconfigurable nanotechnologies encapsulate multiple functionalities due to ambiploarity and tunable hysteresis, security functions such as logic encryption, camouflaging, resistance from side-channel attacks come naturally cheap [5].

The paper is organized as follows. Section 2 provides details about the various emerging reconfigurable nanotechnologies which are being actively researched. This is followed by Section 3 which lists the challenges being faced by emerging nanotechnology. Section 4 gives details about the recent advancement in the field of electronic design automation (EDA). Section 5 and 6 presents the memory and security applications in which these reconfigurable technology can suitably fit.

2 RECONFIGURABLE NANOTECHNOLOGIES

As CMOS reaches its scaling limits, the imperative pursuit for nanotechnology replacements is under way. While many potential substitute devices exist, the primary requirement for such devices

ICCAD '18, November 5–8, 2018, San Diego, CA, USA

ACM ISBN 978-1-4503-5950-4/18/11…$15.00
https://doi.org/10.1145/3240765.3243472

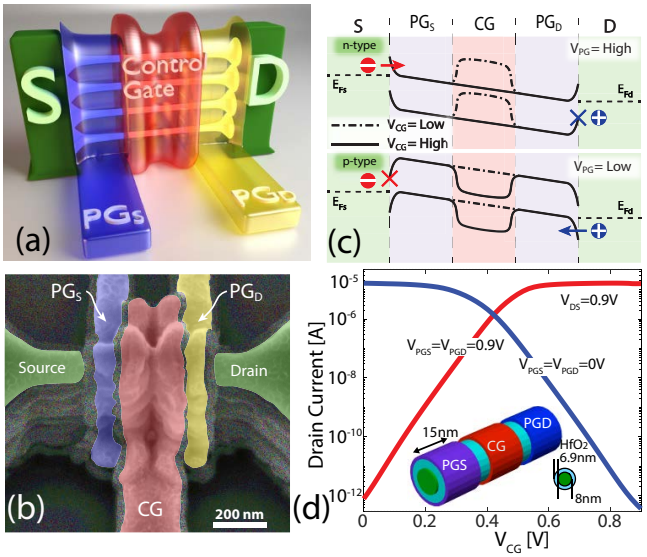

Figure 1: (a) Conceptual sketch of a vertically-stacked nanowire TIGFET. (b) SEM image of the fabricated device. (c) Conceptual band diagrams of the device. (d) TCAD simulated 15-nm TIG NWFET demonstrating a current density of 0.66 mA/μm.

is that they be pragmatic in a fabrication scheme that is still CMOS-driven. Industry will exclusively consider the development of systems compatible with the existing CMOS flow. Device level innovations such as novel geometries and materials introduce improved logic devices [28, 37] which include carbon nanotubes [14], 2D materials (e.g., graphene [38], molybdenum disulfide (MoS_2) [40]) or exploit new physics, such as spintronics [59].

While the conventional drive has been the improvement of independent device performance and size reduction, another viable option, and the interest of this study, is that of enhancing system functionality. This objective is realized through the idea of a reconfigurable transistor. Reconfigurability is the capability of a transistor to switch from *p*-channel to *n*-channel behavior through the application of a signal to an additional gate. Using *Reconfigurable Field Effect Transistors* (RFETs) allows for the development of more complex systems with fewer devices [34].

2.1 Silicon Nanowire Reconfigurable Transistors

The nanowire RFET requires no doping and can be fabricated concurrently to existing technologies in a CMOS fabrication facility. In recent years the use of multiple independent gates (MIGs) to connect FETs in series in a single device has been considered, as seen in [18, 19, 34], allowing for the elimination of interconnect effects. The MIG RFET also provides a wired-AND function to be used in many-input combinational circuits instead of the conventional XOR logic which is useful for transistor-level reconfiguration. These devices were originally made from silicon, though germanium has been used most recently with noticeable improvements; several types of RFETs are discussed in [18, 19, 34].

In the interest of developing high-energy-efficiency computing systems, a promising embodiment of RFET called the Three-Independent-Gate Field Effect Transistor (TIGFET) is considered an effective contemporary solution. TIGFETs have the ability to build compact logic gates that, once used in complex circuits, reduce interconnect parasitics significantly, shifting the technology nodes from interconnect-dominated back to gate-dominated. TIGFETs are capable of three modes of operation: (i) the dynamic reconfiguration of the device polarity [32]; (ii) the dynamic control of the threshold voltage [64]; and (iii) the dynamic control of the subthreshold slope beyond the thermal limit [65].

A TIGFET consists of a semi-conducting channel, metallic source/drain contacts and three gate electrodes: The *Polarity Gate at Source* (PG_S) and the *Polarity Gate at Drain* (PG_D) modulate the Schottky barriers at source and drain; The *Control Gate* (CG) controls the potential barrier in the channel and turns the device on or off.

Figure 1-a shows a typical TIGFET design using vertically-stacked silicon nanowires as the channel, and Figure 1-b shows the corresponding fabricated device as seen top-down by a *Scanning Electron Microscope* (SEM) image. Nickel silicide (NiSi) was used on the source and drain pillars to create mid-gap Schottky barriers. Full details about device fabrication can be found in [32, 64, 65]. The control of carrier injection at the Schottky barriers by the PG_S and PG_D gate terminals gives a lever to determine the operation modes of the device. Figure 1-c presents a conceptual band diagram, when PG_S and PG_D are controlled by the same potential. A positive $PG_{S/D}$ bias enables electron conduction at the source and drain Schottky barriers, setting the device polarity to *n*-type, while a low PG_S/PG_D bias leads to hole conduction and results in *p*-type behavior, giving rise to the dynamic control of the device polarity. This property has been extensively demonstrated experimentally in [32, 30] and further studied using Sentaurus TCAD at the 15-nm technology node, as reported in Figure 1-d.

A single silicon nanowire TIGFET can deliver a current of 16.6 μA, achieving a current density of 0.66 mA/μm. This value, already competitive with FinFET devices [36], can be further improved by using the vertically-stacked nanowire structure [32, 64] to reach current densities larger than the targeted 1mA/μm. When the two PG terminals are biased separately, the independent Schottky biasing facilitates the simultaneous disconnect of carrier injections at both source and drain terminals, leading to a dual-V_T behavior and ultra-low-leakage states [64]. Remarkably, the two V_T configurations share the same *on* state, reducing current drive degradation, a property not achievable with conventional MOSFETs. Full characterization of the dual-V_T capabilities can be found in [64].

Another appeal of TIGFETs is their ability to operate as Super-Steep-Subthreshold-Slope FETs (S4-FETs). This occurs when a positive bias potential $V_{PGS/D}$ is applied, creating a potential well under the gate and causing a noticeable steep-slope behavior, as seen in [65, 66]. This works as follows: When electrons acquire sufficient energy, weak impact ionization is triggered and electron/hole pairs are generated. The generated holes accumulate in the potential well under the gate. This lowers the barrier and provides more electrons for impact ionization, thus establishing a positive feedback. During the transition, the energy band in the PG regions is lowered, maintaining the potential well for the accumulation and improving the average subthreshold slope over the subthreshold region. Due to the weak impact ionization only occurring during transition, the device reliability is not reduced as occurs in other impact ionization devices [65]. Reports of the *n*-type characteristics of a silicon fin-based TIGFET at room temperature and operated in S4-FET mode are seen in [65]. A minimum subthreshold slope of 3.4 mV/dec is achieved, while an average subthreshold slope of 6.0 mV/dec is observed for 5 decades of current. Complete *n*-type and *p*-type characteristics at both room and low temperatures are available in [65, 66].

2.2 2D Reconfigurable Transistors

Alternative channel materials are used in RFETs to allow for improved device-level optimizations. RFETs using graphene p-n junctions have been demonstrated in [54] as early as 2010. The switching

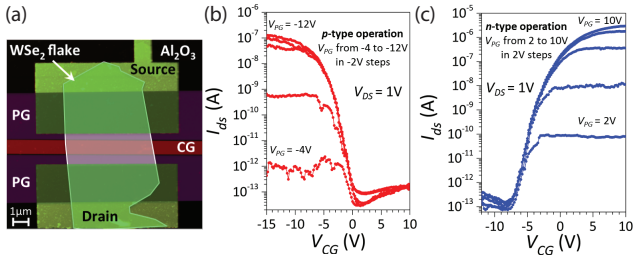

Figure 2: Experimental demonstration of a WSe2 TIGFET [47]. (a) AFM topography image of the experimental device, recolored to highlight the device structure. (b-c) p-type (n-type) transfer characteristics obtained for a negative (positive) bias on PG.

in the graphene-based logic was accomplished through the use of co-planar split gates, similar to the control gates in TIGFETs. The primary benefit of these devices was that they were fabricated on a large graphene sheet with minimal patterning and thus are extremely compatible with CMOS fabrication schemes. [54] Another channel material used in alternative RFETs is molybdenum ditelluride ($MoTe_2$), as seen in [35]. In this study the transistor polarity was controlled by dual top gates where one gate determined the transistor polarity and the other directly influenced the drain current [35]. Tungsten diselenide (WSe_2) is the only 2D-transition metal dichalcogenide (TMD) for which a stable complementary technology has been demonstrated to date [63] and so is arguably the most promising candidate for the realization of high-performance TIGFET devices and circuits. Polarity-control has recently been demonstrated in TIGFETs with WSe_2 channels in [47]. The fabricated device, shown in Figure 2, was realized using mechanically exfoliated multilayer WSe_2 (7.5 nm thick), that was transferred and aligned on a wafer where buried metal lines were used as polarity gates and the silicon substrate as control gate. The metal contacts (Ti/Pd) were evaporated and provided a band-alignment suitable for the injection of both charge carriers. When using the two gates independently, the transistor polarity could be dynamically changed by the polarity gates, while the control gate controlled the on/off status of the device (Figure 2-bc). The experimental transfer characteristics measured showed a p-type behavior for V_{PG} <-6V, while n-type conduction properties are shown for V_{PG} >4V on the same device. I_{on} / I_{off} ratios of 10^7 and 10^6 were achieved for *n*-type and *p*-type operation respectively.

2.3 Ferroelectric FETs

Newer materials have found a lot of applications in memory technologies. Ferroelectric FETs (FeFET) are one of the newer nanaotechnologies that have found extensive use in such applications. It boasts of a non-volatile element with on-demand backup/restore (B/R) features. It is a three-terminal device that integrates the ferroelectric (FE) in the gate stack of a transistor above the dielectric (DE) providing a unique feature for the device to serve as a logic or memory element. The capacitance of FE couples with that of the underlying FET leading to unique characteristics: FeFET exhibit hysteresis behavior when the absolute value of the negative ferroelectric capacitance is smaller than the capacitance of the underlying MOSFET gate. This unique characteristic enables a FeFET as both a non-volatile storage element and a switch.

3 CHALLENGES FOR THESE EMERGING TECHNOLOGIES

Various newer reconfigurable nanotechnologies have been introduced in the previous section. While most of the devices are different structurally, at the logical abstraction they all exhibit dynamic reconfigurable nature. However, in order to bring them to the mainstream electronics and to push them for commercial use, following challenges have to be addressed:

- Compatibility with the existing CMOS flow as it is easier for the industry to adopt them.
- Early evaluation of the circuit is required in order to be able to assess the benefits and associated costs. A flow is needed that goes all the way down to the layout.
- A design flow is needed that is able to provide feedback to the transistor designers when the devices are used at the system level.
- Novel properties need to be exploited in the design flow. Without that the benefits remain small.
- Foresee how the unique properties of these technologies can be applied to common and known problems and find out the solutions using intelligent and intuitive designs.

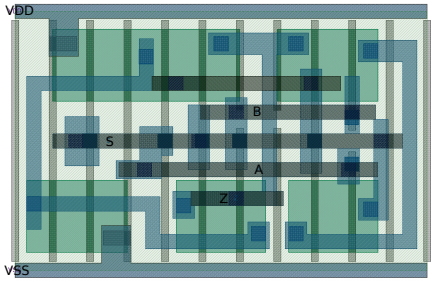

Figure 3: Proposed Layout for reconfigurable MINORITY

4 ENABLING EDA FOR EMERGING TECHNOLOGIES

An efficient electronic design automation (EDA) flow specific to newer nanotechnologies is extremely important as it enables the adoption of a nanotechnology from a lab level research to industrial adoption. It should be comapatible to the existing CMOS flow and be able to harness the true potential of these technologies. This section focusses on recent advances in EDA flow for emerging nanotechnology

4.1 Design Flow for early evaluation of silicon nanowire based reconfigurable FETs

Silicon Nanowire (SiNW) based reconfigurable Field effect transistors (RFETs) are one of the emerging nanotechnologies which has garnered a lot of research in recent years. They are one of the earliest nanotechnologies to demonstrate runtime reconfigurability. For the complete design flow on silicon nanowires based RFETs, an SOI based 22 nm technology to pattern the minimal width of individual nanowire ribbons and to define the half pitch between parallel arranged nanowires was used.

4.1.1 ***Table Model for Silicon Nanowire RFETs.*** The internal structure and material properties of the SiNW transistor is modelled in a TCAD simulator. In early evaluation stages a more simple table model offers a good compromise to link transistor design to electrical simulators. Therefore, we exported a table of current, voltage, and capacitances based on DC simulations inside the TCAD environment. For the electrical transistor model, this table is read inside a Verilog-A module. The parasitic capacitances for a typical transistor structure, upto Metal1, have been included in this model. For library characterization, Synopsys SiliconSmart is used which integrates all required functionality if a cell netlist and transistor model files are provided. While these simulations

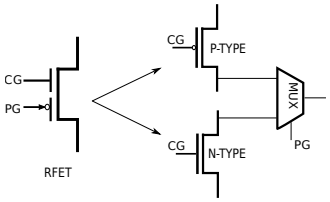

Figure 4: *SiNW* RFET

provide timing and power numbers, the area of the SiNW logic cells needs to be extracted from real cell layouts. Only one operating condition typical at a supply voltage of 1.8V was used. The schematics of the cells are exported as SPICE netlists and are used by the characterization tool.

4.1.2 ***Layout for Reconfigurable Logic Gate.*** The layouts for reconfigurable logic gate based on silicon nanowire based RFETs were proposed based on advanced node design rules and the *LEF* layout abstract files for Place & Route. The MINORITY gate layout, shown in Figure 3 is a reconfigurable ready layout. Depending upon the value of S, this layout of MINORITY gate can function as a NAND gate ($S = 0$) or a NOR gate ($S = 1$).

4.1.3 ***Area Results*** . Experiments using our physical synthesis flow show that SiNW RFETs based circuits for MCNC benchmarks occupy just 17.43% more area as compared to their CMOS counterparts [41]. Even thought the average area is more than CMOS baseline, the results are very encouraging considering the fact that in the used lab-technology, the individual RFETs are almost twice the size of CMOS. This is due to the higher functional encapsulation by reconfigurable emerging technology. The work presents a complete feasibility study of the design flow by taking into account a simplified technology flow. There are other measures which can be employed to reduce the device area like vertical stacking of multiple nanowires [33, 13, 32]. This will lead to a substantial reduction of device width and accordingly to a reduced cell height of the layouts. This will further have a positive impact in the reduction of capacitances and RC delay of the transistor [57].

In terms of circuit speed and power consumption, another promising solution is to use germanium or silicon-germanium nanowire channels instead of silicon nanowires as stated in Section **??**. The above flow can be replicated for any nanowire RFET technology.

4.2 Technology Mapping Flow for silicon Nanowire Based RFETs

While the previous subsection gave a complete design flow for silicon nanowire based RFETs, this section discusses an example optimization which provides an efficient technology mapping for runtime reconfigurable logic gates based on SiNW RFETs [56].

4.2.1 ***Higher Order Functions.*** Changing the polarity of one of the gate terminals for RFETs leads to runtime-reconfigurability. This can be well abstracted in mathematics using a *Higher Order function* (HOF) as described in the following equation [42]:

$$f(x, y, z, w) = g(x, y, z), when\ w = 0$$
$$= h(x, y, z), when\ w = 1$$

In the above expression, f is an *HOF* and can be represented in terms of functions g and h depending upon the value of w. Analogous to the above mathematical function, SiNW RFET has been shown to behave as p-type and n-type as shown in the Figure 4. A SiNW RFET with two gate terminals can be represented as an *NMOS* and an *PMOS* whose outputs are fed into a *2to1 MUX*. Adding to

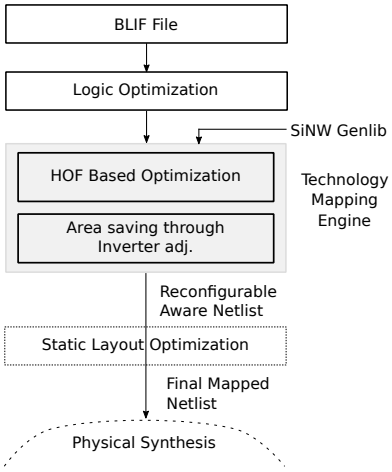

Figure 5: Technology Flow suited for SiNW RFETs

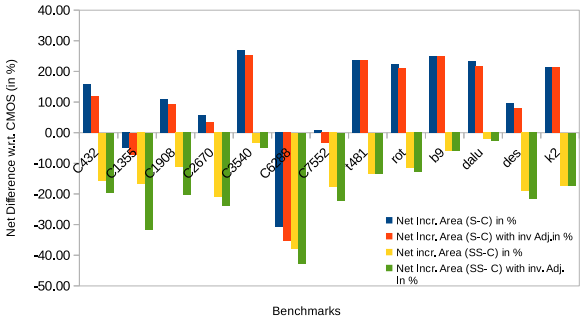

Figure 6: Area Comparison

that, since electrical property ($NMOS \iff PMOS$) can be changed by changing PG, this brings runtime reconfigurability similar to a *MUX*. However, for the above behavior the logic gates need to have a third input which feeds the program gate and requires an inverter logic within the gate boundary [56].

4.2.2 ***Area Optimization through sharing of inverted Fan-ins.*** An important difference to note among the logic gates proposed in [56] are the XOR family of logic gates. In both models of the XOR gate i.e. *2-bit XOR* or *3-bit XOR*, the complemented and actual forms of each input are required in the logic gate. Hence, overall area for the XOR-based logic gates is increased by the area of $Nos\ of\ input\_variables$ x $2(RFETs)$. Hence, we explore the feasibility of harnessing the inverted forms of fan-ins available in the circuit thereby reducing the number of inverters required. We feed these inverted forms to interior gate terminals of multi-input RFETs as they are faster terminals [43]. In XOR both these inputs are fed to these faster gates terminals to compensate the delay caused by the long length of metal wires.

4.2.3 ***Technology Mapping Flow and Area Comparison.*** The complete flow is shown in Figure 5. We used the concept of higher order functions to represent and encapsulate larger functions and use inverter adjustment in our technology mapping. The concept of mutual exclusive function is implemented using ABC tool.

The output of this technology mapping is a netlist which is basically a reconfigurability-aware logic circuit. Until this point, each

component in the circuit is an HOF and can exhibit runtime reconfigurability depending upon input P at program gate for each logic gate [56]. After this, the user has an option to choose a reconfigurability-aware layout or a static layout. For the static layout, the P inputs of all logic gates have to be fixed to either V_{dd} or V_{ss} and the gates behave as CMOS analogous logic gates. In this case, the logic circuit gains in terms of area with fewer transistors but loses dynamic reconfiguration. Circuit designers can utilize this trade-off between the number of transistors and reconfigurability for their designs.

Figure 6 shows the number of transistors post technology mapping step using SiNW transistors as compared to the CMOS. The letters C, S and SS refer to the CMOS flow, SiNW reconfigurability-aware flow and SiNW static flow. Another parameter to evaluate is the area savings due to the availability of inverted fan-ins in case of XOR family gates which are represented as *Inv. Adj.* The reconfigurability-aware logic gates have an area overhead as compared to CMOS baseline because of extra inverters required per logic gate. However, some benchmarks are anomalies as they have less area as compared to CMOS because the mapper uses more higher order functions to match nodes of the logic circuits or if the circuit has more XOR-based nodes and the mapper uses inverter adjustments. For the entire 219 testcases in MCNC benchmark, the average improvement in terms of number of transistors for SiNW RFETs w.r.t CMOS baseline is 17.48% and 16.25% for static and reconfigurability-aware flows respectively. The result is further improved by 9.26 for static flow and 8.2 for reconfigurability-aware flow respectively due to sharing of inverted fan-ins.

The above two contributions related to EDA are applicable to any new reconfigurable nanotechnology which is at the lab-technology level and provide an early evaluation.

5 EMERGING TECHNOLOGIES IN MEMORY

This section will focus on two emerging trends that blur the gap between memory and logic and highlight two specific technologies to highlight enabling innovations.

5.1 Nonvolatile Computing using Ferroelectric FETS

The explosion in the use of wearable electronics is mushrooming technologies that leverage energy harvesting technologies. Hence, non-volatile computing has emerged as a major paradigm, where data retention across power failures is important for instant turn-on and turn-off capability. While initial approaches focused on traditional fault tolerant approaches of systematic backup and recovery to off-chip non-volatile stores, the overheads of data movement limit their viability. Recent approaches have sought to tightly integrate non-volatile memory structures with the compute logic in a distributed fashion. This approach focuses on reducing the energy and time consumed to do backup and recovery in distributed structures. Several NVFF designs using memristors, magnetic tunnel junctions (MTJs), resistive RAMs (ReRAMs), Ferroelectric capacitors and Ferroelectric FETs (FeFET) , as a local non-volatile element have been proposed with on-demand backup/restore (B/R) features.

The hysteresis property of FeFETs is beneficial for introducing non-volatility feature into the flip-flops[58] to enable continued forward progress. However, there is an energy overhead for the non-volatile writes as compared to a volatile write operation. The ability to tune the same FeFET structure to perform a volatile or non-volatile memory operation provides yet another lever for configurability. Recent approaches propose the use of the FeFET structure in conjunction with a CMOS based flipflop which enables need-based non-volatile storage to facilitate a better trade-off [55].

The FeFET device has also been used to provide flexible memory structures that better match the access patterns of the interacting

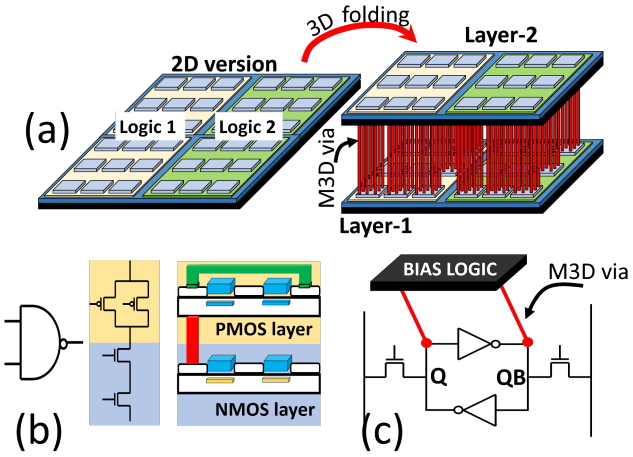

Figure 7: Popular design styles using M3D-IC.

processing elements [61]. Specifically, the array organization and the cell structure can be well utilized for multi-dimensional data access required in machine learning and data analytics accelerators. The single cycle row-wise and column-wise data access capability by harnessing the FeFET properties will accelerate the performance of matrix computations. 11% faster executions of matrix operations are achieved by two-dimensional data access enabled by FeFETs [16]. Reliable multirow activation made possible by the read disturb free configuration has been further utilized in computations in FeFET as part of data readout [46]. FeFET devices have also been demonstrated to serve as analog memory exhibiting partial polarization states and both potentiation and depression behavior. This feature also supports FeFET configurations in cross-point configurations for supporting multiply-accumulate behavior for convolutional kernels [24, 8].

In summary, the FeFET technology holds an immense promise for multiple functionality realization from ultra-low voltage logic design to energy efficient computing in high density NVMs.

5.2 In Memory Compute using Monolithic 3D Integration

Monolithic 3D integration (M3D-IC) is an alternative to TSV based 3D process. M3D-IC enables transistor stacking on different layers through sequential integration process. Sequential integration process offers scalable and high-density vertical interconnects (M3D via). With M3D via dimensions similar to metal routing vias, fine grain integration is possible. Three popular design styles using M3D-IC are shown in Figure 7. Figure 7(a) shows the logic or block level M3D integration. In this technique, 2D IC is folded into 3D and the folding takes place at the block level. Long distance routings are now in 3D using M3D vias, thereby reducing the overall routing latency. The second design style (Figure 7(b) is a standard cell level M3D integration. In this approach, PMOS and NMOS transistors are in two different layers and the connectivity between the NMOS and PMOS cells of the standard cells are through the M3D vias. The third approach is to design 3D SRAM using M3D-IC for various memory related design optimizations (Figure 7(c)). Due to the fact that the dimension of M3D vias enable direct access to the storage nodes of the cell, various design strategies can be employed. M3D-IC process ensures footprint preservation when designing a multi ported 3D SRAM. This technique provides additional routing resources from layer-2. A 3D multidimensional data access capable SRAM [50] enables energy efficient matrix operations by reducing the number of data accesses. A multi-layer 3D FPGA design with a

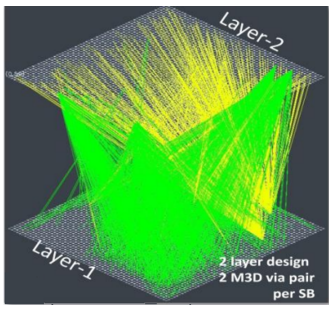

Figure 8: Signal traversal through M3D vias in a 3D FPGA

pair of configuration memories supports rapid dynamic reconfiguration in FPGAs [51]. A two-layer FPGA design will help reduce long distance routings by appropriately configuring the logic elements and routing them through M3D vias. Figure 8 shows the 3D routings which were otherwise long distance or critical delay paths if designed in 2D.

Growing performance gap between logic and memory due to scaling can be blurred with computing where the data is located. 3D SRAMs designed using M3D-IC offer computational support as part of the data readout [20]. Designs such as [52] effectively utilize the layer-2 area over the SRAM cell located in layer-1 to make the read and write process more immune to noise while offering in-memory computational support. A combination of cell level and array level computing facilitates arithmetic operations for layer-2 [23]. Multimode memories which can be configured as SRAM and content addressable memories (CAM) enable various search related in-memory computations across banks in parallel [23]. These designs take advantage of reduced data movement in and out of the memory when designed using M3D-IC. Overall, low latency and scalable M3D vias with sequential M3D-IC process enables novel circuit and memory design opportunities which are either not feasible with TSV based 3D technology or impractical with 2D design process.

In addition to the above-mentioned efforts, there are other approaches that continue to blur the gap between logic and memory. The use of look-up table based computations for complex functions, the use of content-addressable memories (refer CORNELL related papers) as compute engine, the design of custom MAC operations using cross-point based resistive memories.

6 HARDWARE SECURITY BASED ON EMERGING RECONFIGURABLE NANOTECHNOLOGIES

Hardware security threats in the IC supply chain, including counterfeiting of semiconductor components, side-channel attacks, invasive/ semi-invasive reverse engineering, and IP piracy cost the US economy more than $200 billion annually [15]. A rapid growth in the "Internet of Things" (IoT) only exacerbates these problems [49]. While CMOS-based hardware security enhancements and circuit protection methods (e.g., [1, 25, 9, 26, 22]) can mitigate security threats in protected components, these methods often incur high cost with respect to performance, power and/or area. Raising the resilience of hardware systems with minimal compromise to other figures of merit is a daunting challenge.

Advances in emerging, post-CMOS technologies may provide hardware security researchers with new alternatives to change the passive role that CMOS technology currently plays in security applications. While many emerging technologies aim to sustain the performance scaling trends attributed to Moore's Law and/or

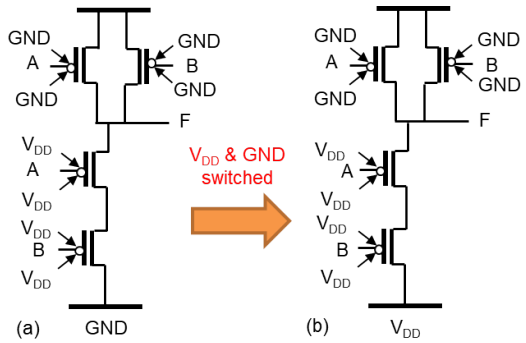

Figure 9: (a) SiNW FET-based NAND; (b) SiNW FET-based NOR.

to improve energy efficiency [37], emerging technologies often demonstrate unique features that could drastically simplify circuit structures for protection against hardware security threats. For example, in [5], we have shown that a bell-shaped I-V characteristic demonstrated by some 2D tunnel FETs (TFETs) can be readily exploited to protect against power supply tampering for launching a fault injection-based side channel attack.

Emerging reconfigurable nanotechnologies discussed in Section 2 have great potential towards no/low-overhead techniques for *protection of circuit designs and IP cores* and *protection against counterfeit ICs*. In the rest of this section, we present several case studies that demonstrate the use of emerging reconfigurable nanotechnologies for hardware security, particularly for IP protection.

6.1 Logic Locking via Polymorphic Gates

In order to protect circuit schematics from reverse engineering for IP piracy, various IP protection methods have been developed among which camouflaging is a popular solution [10, 11, 9]. This method relies on layout-level obfuscation that develops similar layouts for different gates, making it difficult to recover the circuit structure [45]. However, CMOS-based camouflaging gates typically consume much higher power and area, and thus incur significant overhead. For example, a generic XOR, NAND and NOR camouflaging CMOS gate requires at least 12 transistors along with a large area of metal connections, which results in about 3X/3X/1.5X increase in terms of the number of transistors compared to the 4T NAND/4T NOR/8T XOR gate.

Logic locking (also referred to as logic obfuscation) that employs polymorphic logic circuits provides an effective way to encrypt logic gate functionality against reverse engineering even given the entire netlist/layout. Polymorphic gates are based on the idea of realizing multiple functionalities in the same cell and the actual functionality is chosen by means of a control signal in the circuit. However, polymorphic logic gates have never been widely used in CMOS circuits mainly due to the difficulties in designing such circuits using CMOS technology.

Leveraging the reconfigurable SiNW FETs discussed in Section 2.1, we have developed low-overhead, SiNW FET based polymorphic gates [5, 6, 7]. As shown in Figure 9, the control gate (CG) of a SiNW FET is connected to a normal input, and the polarity gates (PGs) are treated as the polymorphic control input. By adjusting the polymorphic control input to either V_{DD} or GND, we can easily change the circuit functionality without any performance penalty. Figure 9 demonstrated a SiNW FET based polymorphic gate that can be converted between a NAND gate and a NOR gate. On the contrary, a CMOS-based NAND cannot be converted to a fully functioning NOR by simply switching power and ground.

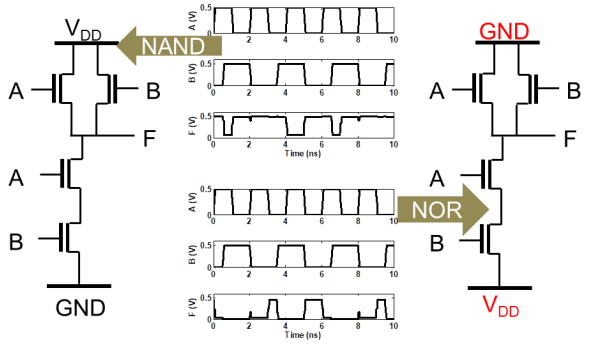

Figure 10: TMDTFET polymorphic NAND/NOR gate and simulation results.

Any device that exhibits ambipolarity, which is the case for many TFETs being studied, can be considered as a candidate for implementing polymorphic gates with low overhead. As another example, Transition Metal Dichalcogenide (TMD) TFET, also exhibits ambipolarity and can be reconfigured for designing polymorphic logic gates [21]. Figure 10 illustrates a 2-input polymorphic NAND/NOR gate. By properly biasing the gate, the n-doped region, and the p-doped region, a TMDTFET device can function either as an n-type transistor or p-type transistor, depending on the gate-source and drain-source voltage drop on the device. For the schematic in Figure 10, if the two parallel TMDTFETs are connected to V_{DD}, and the bottom TMDTFET is connected to GND, the circuit behaves as a NAND gate. If the two parallel TFETs are connected to GND and the bottom TMDTFET is connected to V_{DD}, the circuit behaves as a NOR gate. Simulation results based on a 1D ballistic quantum capacitance limit (QCL) model (representative of TMD devices) show the expected polymorphic functionality (see Figure 10).

6.2 Tunable Hysteresis for IP Protection

An alternative way to protect IP is through logic encryption implemented by key gate-based approaches. Different combinational logic gates are inserted in a circuit to conceal the functionality of a design. These gates can be XOR/XNOR gates or MUXes (e.g., [44, 60, 39]), where one of the inputs to these key gates serves as a key. The key values are stored in a tamper-proof, non-volatile memory and loaded to on-chip SRAM when the chip is powered up. To prevent attacks such as data interception and side-channel attacks at the chip boundary, data encryption is a must for the non-volatile memory chip, leading to large power, area, and performance overheads [27, 53]. To reduce security vulnerabilities,it is suggested that key values should be stored in some on-chip non-volatile memory to eliminate the security vulnerabilities due to off-chip key storage.

The FeFET device discussed in Section 2.3 is a good candidate for on-chip key gate-based logic encryption. FeFETs are reconfigurable in terms of their hysteresis property, referred to as tunable hysteresis. That is, an FeFET can be dynamically configured as either a switch or a non-volatile storage element, which can be achieved by adjusting the coupling between the FE capacitance and the underlying MOSFET capacitance. This tunable hysteresis makes FeFETs a natural choice for power and area efficient logic-in-memory (LiM) designs [62, 61, 4]. FeFET LiMs, when used as both on-chip key storage and logic gates, eliminates key transfers between CPU and off-chip non-volatile memory, thus reduces the vulnerability to memory communication attacks [12]. FeFET LiMs also help reduce circuitry overhead associated with key access and verification.

We show two examples FeFET based LiM circuit blocks whose functions appear often in security circuits, i.e., XOR/XNOR and

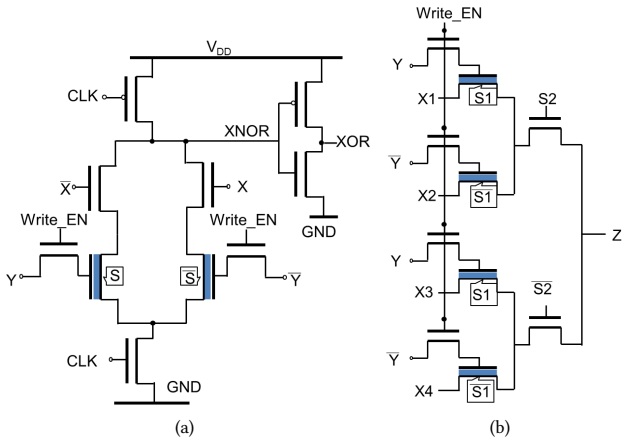

Figure 11: Schematic of (a) XOR/XNOR dynamic logic LiM; (b) MUX dynamic current mode logic LiM.

MUX. Figure 11(a) shows an example of dynamic logic LiM performing XOR/XNOR logic. The circuit has two modes: update mode and hold mode. In the update mode (i.e., $Write\_EN$= 1 and CLK=1), the Y and $\overline{Y}$ inputs are written into the FeFETs, respectively. In the hold mode (i.e., $Write\_EN$= 0, CLK=0 in precharge phase and CLK=1 in evaluate phase), the circuit outputs $X \oplus S / \overline{X \oplus S}$, where S (=Y) and $\overline{S}$ (=$\overline{Y}$) are the bit values stored in the FeFET and remain unchanged even without power supply. Figure 11(b) shows a 4:1 MUX LiM design. Similar to the circuit in Figure 11(a), this circuit also has an update and hold mode. In the hold mode (i.e., $Write\_EN$= 0), the circuit outputs one of the four inputs $X1$, $X2$, $X3$ and $X4$, depending on the value of $S1$ and $S2$, while $S1$ and $\overline{S1}$ are the bits stored in FeFETs. In the update mode (i.e., $Write\_EN$= 1), Y and $\overline{Y}$ are written into the two FeFETs, respectively, while output delivers the output from one of the four inputs depending on the value of Y and $S2$.

Looking forward, devices with tunable hysteresis offer unique functionality that is difficult to obtain with MOSFETs. (i) Such a device can be switched between a nonvolatile storage element and a switch. This property could help achieve logic obfuscation. (ii) With three terminals, such a device can be more flexible when acting as a storage element as compared with a ferroelectric capacitor. This opens the door for simpler LiM cells, which could lead to efficient memory protection strategies.

7 CONCLUSIONS

Emerging reconfigurable technologies indeed offer exciting feature sets which can truly complement or supplement existing electronic designs. These feature sets clearly provide even more functionality per computational unit. Yet, these novel nanotechnologies pose some challenges which need to be taken care of to realize their true potential. These technologies have the potential to be the stepping stones to imitate capabilities of the human brain by bringing memory and logic together. Additionally, some hardware security functions that come naturally are the cherry on top for the systems based on these functionally enhanced emerging technologies.

8 ACKNOWLEDGEMENTS

This work is supported in part by the German Research Foundation (DFG) within the Cluster of Excellence Center for Advancing Electronics Dresden, the NSF Career Award number 1751064, SRC

JUMP Center for Research on Intelligent Storage and Processing-in-memory, and Indiana Innovation Institute through the ASSURE Program.

REFERENCES

[1] Yousra Alkabani and Farinaz Koushanfar. "Active Hardware Metering for Intellectual Property Protection and Security". In: *USENIX Security*. 2007.

[2] Luca Amarù, Pierre-Emmanuel Gaillardon, and Giovanni De Micheli. "Efficient arithmetic logic gates using double-gate silicon nanowire FETs". In: *NEWCAS*. 2013.

[3] Luca Amarú, Pierre-Emmanuel Gaillardon, and Giovanni De Micheli. "Majority-Inverter Graph: A Novel Data-Structure and Algorithms for Efficient Logic Optimization". In: *DAC*. 2014.

[4] A. Aziz et al. "Computing with ferroelectric FETs: Devices, models, systems, and applications". In: *DATE*. 2018.

[5] Yu Bi et al. "Emerging technology-based design of primitives for hardware security". In: *JETC* (2016).

[6] Yu Bi et al. "Enhancing hardware security with emerging transistor technologies". In: *GLSVLSI*. 2016.

[7] An Chen et al. "Using emerging technologies for hardware security beyond PUFs". In: *DATE*. 2016.

[8] Xiaoming Chen et al. "Design and optimization of FeFET-based crossbars for binary convolution neural networks". In: *DATE*. 2018.

[9] Lap Wai Chow et al. "Camouflaging a standard cell based integrated circuit". Pat. 8151235. 2012.

[10] Lap-Wai Chow, James P Baukus, and William M Clark Jr. *Integrated circuits protected against reverse engineering and method for fabricating the same using an apparent metal contact line terminating on field oxide*. US Patent 7,294,935. 2007.

[11] Ronald P Cocchi et al. *Building block for a secure CMOS logic cell library*. US Patent 8,111,089. 2012.

[12] Duncan Elliott et al. "Computational RAM: Implementing processors in memory". In: *IEEE Design & Test of Computers* (1999).

[13] T. Ernst et al. "Novel 3D integration process for highly scalable Nano-Beam stacked-channels GAA (NBG) FinFETs with HfO2/TiN gate stack". In: *IEDM*. 2006.

[14] A. D. Franklin et al. "Sub-10 nm Carbon Nanotube Transistor". In: *Nano Letters* 12.2 (2012), pp. 758–762.

[15] Frontier Economics Ltd, London. *Estimating the global economic and social impacts of counterfeiting and piracy*. 2011.

[16] S. George et al. "Symmetric 2-D-Memory Access to Multidimensional Data". In: *TVLSI* (2018).

[17] Naoki Harada et al. "A polarity-controllable graphene inverter". In: *Applied Physics Letters* (2010).

[18] André Heinzig et al. "Dually Active Silicon Nanowire Transistors and Circuits with Equal Electron and Hole Transport". In: *Nano Letters* 13.9 (2013). PMID: 23919720, pp. 4176–4181. eprint: http://dx.doi.org/10.1021/nl401826u.

[19] André Heinzig et al. "Reconfigurable silicon nanowire transistors". In: *Nano Letters* (2012).

[20] F. Hsueh et al. "TSV-free FinFET-based Monolithic 3D+-IC with computing-in-memory SRAM cell for intelligent IoT devices". In: *IEDM*. 2017.

[21] Hesameddin Ilatikhameneh et al. "Tunnel field-effect transistors in 2-D transition metal dichalcogenide materials". In: *IEEE Journal on Exploratory Solid-State Computational Devices and Circuits* 1 (2015), pp. 12–18.

[22] Meenatchi Jagasivamani et al. "Split-Fabrication Obfuscation: Metrics and Techniques". In: *HOST*. 2014.

[23] N. Jao. "Harnessing Emerging Technology for Compute-In-Memory Support". In: *ISVLSI*. 2018.

[24] Matthew Jacob Jerry et al. "A Ferroelectric field effect transistor based synaptic weight cell". In: *Journal of Physics D: Applied Physics* (2018).

[25] Y. Jin and Y. Makris. "Hardware Trojan detection using path delay fingerprint". In: *HOST*. 2008.

[26] Yier Jin, Bo Yang, and Yiorgos Makris. "Cycle-accurate information assurance by proof-carrying based signal sensitivity tracing". In: *HOST*. 2013.

[27] S. Kannan et al. "Security Vulnerabilities of Emerging Nonvolatile Main Memories and Countermeasures". In: *TCAD* (2015).

[28] K.Bernstein et al. "Device and Architecture Outlook for Beyond CMOS Switches". In: *Proceedings of the IEEE* 9.12 (2010), pp. 2169–2184.

[29] Yu-Ming Lin et al. "High-performance Carbon Nanotube Field-effect Transistor with Tunable Polarities". In: *IEEE Trans. Nanotechnol.* (2005).

[30] M. De Marchi et al. "Configurable Logic Gates Using Polarity Controlled Silicon Nanowire Gate-All-Around FETs". In: *IEEE Electron Device Letters* 35.8 (2014), pp. 880–882.

[31] M. De Marchi et al. "Polarity control in double-gate, gate-all-around vertically stacked silicon nanowire FETs". In: *IEDM*. 2012.

[32] M. De Marchi et al. "Polarity control in double-gate, gate-all-around vertically stacked silicon nanowire FETs". In: *IEDM Tech. Dig.* (2012), pp. 8.4.1–8.4.4.

[33] H. Mertens et al. "Vertically stacked gate-all-around Si nanowire CMOS transistors with dual work function metal gates". In: *IEDM*. 2016.

[34] Thomas Mikolajick et al. "The RFET a reconfigurable nanowire transistor and its application to novel electronic circuits and systems". In: *Semiconductor Science and Technology* (2017).

[35] S. Nakaharai et al. "Electrostatically Reversible Polarity of Ambipolar α MoTe2 Transistors". In: *ACS Nano* 9.6 (2015), pp. 5976–5983.

[36] S. Natarajan et al. "A 14nm logic technology featuring 2nd-generation FinFET, air-gapped interconnects, self-aligned double patterning and a 0.0588 μ m^2 SRAM cell size". In: *IEDM Tech. Dig.* (2014), pp. 71–73.

[37] D. E. Nikonov and I. A. Young. "Benchmarking of Beyond-CMOS Exploratory Devices for Logic Integrated Circuits". In: *JESSCDC* (2015).

[38] K. S. Novoselov et al. "Electric Field Effect in Atomically Thin Carbon Films". In: *Science* 306.5696 (2004), pp. 666–669.

[39] S. M. Plaza and I. L. Markov. "Solving the Third-Shift Problem in IC Piracy With Test-Aware Logic Locking". In: *TCAD* (2015).

[40] B. Radisavljevic et al. "Single-layer MoS2 transistors". In: *Nature Nanotechnology* 6.3 (2011), pp. 147–150.

[41] S. Rai et al. "A physical synthesis flow for early technology evaluation of silicon nanowire based reconfigurable FETs". In: *DATE*. 2018.

[42] S. Rai, M. Raitza, and A. Kumar. "Technology mapping flow for emerging reconfigurable silicon nanowire transistors". In: *DATE*. 2018.

[43] M. Raitza et al. "Exploiting transistor-level reconfiguration to optimize combinational circuits". In: *DATE*. 2017.

[44] J. Rajendran et al. "Fault Analysis-Based Logic Encryption". In: *TOC* (2013).

[45] Jeyavijayan Rajendran et al. "Security analysis of integrated circuit camouflaging". In: *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. ACM. 2013, pp. 709–720.

[46] Dayane Reis, Michael Niemier, and X. Sharon Hu. "Computing in Memory with FeFETs". In: *ISLPED*. New York, NY, USA: ACM, 2018.

[47] Giovanni V. Resta et al. "Polarity control in WSe2 double-gate transistors". In: *Scientific Reports* (2016).

[48] J. Romero-Gonzalez and P. E. Gaillardon. "BCB Evaluation of High-Performance and Low-Leakage Three-Independent-Gate Field Effect Transistors". In: *JESSCDC* (2018).

[49] A. Sadeghi, C. Wachsmann, and M. Waidner. "Security and privacy challenges in industrial Internet of Things". In: *DAC*. 2015.

[50] S. Srinivasa et al. "Compact 3-D-SRAM Memory With Concurrent Row and Column Data Access Capability Using Sequential Monolithic 3-D Integration". In: *TVLSI* (2018).

[51] S. R. Srinivasa et al. "Improving FPGA Design with Monolithic 3D Integration Using High Dense Inter-Stack Via". In: *ISVLSI*. 2017.

[52] Srivatsa Rangachar Srinivasa et al. "A Monolithic-3D SRAM Design with Enhanced Robustness and In-Memory Computation Support". In: *ISLPED*. 2018.

[53] S. Swami, J. Rakshit, and K. Mohanram. "SECRET: Smartly EnCRypted Energy efficienT non-volatile memories". In: *DAC*. 2016.

[54] S. Tanachutiwat et al. "Reconfigurable multi-function logic based on graphene p-n junctions". In: *DAC*. 2010.

[55] S. K. Thirumala et al. "Dual Mode Ferroelectric Transistor Based Non-Volatile Flip-Flops for Intermittently-Powered Systems". In: *ISLPED*. Seattle, WA, USA, 2018.

[56] J. Trommer et al. "Reconfigurable nanowire transistors with multiple independent gates for efficient and programmable combinational circuits". In: *DATE*. 2016.

[57] Jens Trommer et al. "Functionality-Enhanced Logic Gate Design Enabled by Symmetrical Reconfigurable Silicon Nanowire Transistors". In: *IEEE Transactions on Nanotechnology* 14.4 (2015), pp. 689–698.

[58] Danni Wang et al. "Ferroelectric Transistor Based Non-Volatile Flip-Flop". In: *ISLPED*. New York, NY, USA: ACM, 2016.

[59] S. A. Wolf et al. "Spintronics: a spin-based electronics vision for the future". In: *Science* 294.5546 (2001), pp. 1488–1495.

[60] M. Yasin et al. "On Improving the Security of Logic Locking". In: *TCAD* 35.9 (2016), pp. 1411–1424.

[61] Xunzhao Yin, Michael Niemier, and X Sharon Hu. "Design and benchmarking of ferroelectric fet based tcam". In: *DATE*. IEEE. 2017.

[62] Xunzhao Yin et al. "Exploiting ferroelectric fets for low-power non-volatile logic-in-memory circuits". In: *ICCAD*. ACM. 2016, p. 121.

[63] L. Yu et al. "High-Performance WSe2 Complementary Metal Oxide Semiconductor Technology and Integrated Circuits". In: *Nano Letters* 15.8 (2015), pp. 4928–34.

[64] J. Zhang et al. "Polarity-Controllable Silicon Nanowire Transistors With Dual Threshold Voltages". In: *IEEE Transactions on Electron Devices* (2014).

[65] Jian Zhang et al. "A Schottky-Barrier Silicon FinFET with 6.0mV/dec Subthreshold Slope over 5 Decades of Current". In: *IEDM Tech. Dig.* (2014), pp. 339–342.

[66] Jian Zhang et al. "On Temperature Dependency of Steep Subthreshold Slope in Dual-Independent-Gate FinFET". In: *JEDS* 3.6 (2015), pp. 452–456.