Emerging Technology-Based Design of Primitives for Hardware Security

YU BI, KAVEH SHAMSI, and JIANN-SHIUN YUAN, University of Central Florida
PIERRE-EMMANUEL GAILLARDON and GIOVANNI DE MICHELI, 'Ecole Polytechnique Fédérale de Lausanne (EPFL), Switzerland
XUNZHAO YIN, X. SHARON HU, and MICHAEL NIEMIER, University of Notre Dame
YIER JIN, University of Central Florida

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. In this article, emerging technologies are investigated by leveraging their unique properties for applications in the hardware security domain. Security, for the first time, will be treated as one design metric for emerging nano-architecture. Five example circuit structures including camouflaging gates, polymorphic gates, current/voltage-based circuit protectors, and current-based XOR logic are designed to show the high efficiency of silicon nanowire FETs and graphene SymFET in applications such as circuit protection and IP piracy prevention. Simulation results indicate that highly efficient and secure circuit structures can be achieved via the use of non-CMOS devices.

Categories and Subject Descriptors: C.2.2 [**Security and Protection**]: Physical Security

General Terms: Security, Design

Additional Key Words and Phrases: Emerging technology, hardware security, SiNW FET, graphene SymFET

ACM Reference Format:
Yu Bi, Kaveh Shamsi, Jiann-Shiun Yuan, Pierre-Emmanuel Gaillardon, Giovanni De Micheli, Xunzhao Yin, X. Sharon Hu, Michael Niemier, and Yier Jin. 2016. Emerging technology-based design of primitives for hardware security. J. Emerg. Technol. Comput. Syst. 13, 1, Article 3 (April 2016), 19 pages.
DOI: http://dx.doi.org/10.1145/2816818

1. INTRODUCTION

The emergence of hardware Trojans has largely reshaped the traditional view that the hardware layer can be blindly trusted. Hardware Trojans, which are often in the form of maliciously inserted circuitry, may impact the original design by data leakage or circuit

M. Niemier and X. S. Hu were supported in part by the Center for Low Energy Systems Technology (LEAST), one of six centers of STARnet, a Semiconductor Research Corporation program sponsored by MARCO and DARPA.

A preliminary version of parts of this work was published in the 23rd Asia Test Symposium (ATS) in November 2014 under the title "Leveraging Emerging Technology for Hardware Security—Case Study on Silicon Nanowire FETs and Graphene SymFETs."

Authors' addresses: Y. Bi, K. Shamsi, J.-S. Yuan, and Y. Jin, Department of Electrical Engineering and Computer Science, University of Central Florida; emails: yubi@knights.ucf.edu, kaveh@knights.ucf.edu, jiann-shiun.yuan@ucf.edu, yier.jin@eecs.ucf.edu; P.-E. Gaillardon and G. de Micheli, École Polytechnique Fédérale de Lausanne (EPFL), Switzerland; emails: pierre-emmanuel.gaillardon@utah.edu, giovanni.demicheli@epfl.ch; X. Yin, X. S. Hu, and M. Niemier, Department of Computer Science and Engineering, University of Notre Dame; emails: {xyin1, shu, mniemier}@nd.edu.

DOI: http://dx.doi.org/10.1145/2816818

malfunction. Hardware counterfeiting and intellectual property (IP) piracy are another two serious issues costing the U.S. economy more than $200 billion annually [Frontier Economics 2011]. To address such threats, various hardware Trojan detection methods and hardware metering methods have been developed [Agrawal et al. 2007; Alkabani and Koushanfar 2007; Jin and Makris 2008; Potkonjak et al. 2009; Jin et al. 2013]. Besides circuit-level security solutions, cybersecurity researchers also rely on layered security protection approaches and have developed various methods to protect the higher abstraction layer through security enhancement at the lower abstraction layer. Through this chain, cybersecurity protection schemes have been pushed downward from virtual machine to hypervisor [Seshadri et al. 2007]. Following this trend, new methods are under development through which the hardware infrastructure is modified to directly support sophisticated security policies so that a system-level protection scheme will be more efficient [Jin and Oliveira 2014].

It is a rather common practice to think of dedicated hardware primitives that support the various security applications in the multiple layers of the system hierarchy. Physical unclonable functions (PUFs) to produce unique IDs, power regulators to hinder power analysis attacks, or encryption hardware accelerators are examples of these special types of hardware that only find applications in the security context. A large amount of research and experimentation has been carried out on the design of these primitives based on the currently prevailing CMOS technology. However, the security provided by these primitives comes at the cost of large overheads mostly in terms of area.

The development of emerging technologies provides hardware security researchers with opportunities to utilize some of the otherwise unusable properties of emerging technologies in security applications. Originally developed as alternatives to CMOS technology to overcome the scaling limit, emerging technologies also demonstrated their unique features, which, besides improving circuit performance, can simplify circuit structure for security purposes such as IP protection and Trojan detection [Bi et al. 2014]. Traditional metrics, such as power and delay, are the major criteria used to evaluate the merits of emerging devices; however, in this work, we will include the security consideration in the overall performance measurements to fully compare the emerging devices to CMOS technology. Considering the large amount of emerging device models, including graphene transistors, atomic switches, memristors, Mott FET, spin FET, nanomagnetic, and all-spin logic, spin wave devices, OST-RAM, magnetoresistive random-access memory (MRAM), spintronic devices, and so forth [ITRS 2013], two fundamental questions have recently been raised related to their applications in the hardware security domain. First, can emerging technology provide a more efficient hardware infrastructure than CMOS technology in countering hardware Trojans and IP piracy? Second, what properties should the emerging technology-based hardware infrastructure provide so that software-level protection schemes can be better supported?

Most work with emerging technologies for security purposes to date has explored implementations like PUFs [Iyengar et al. 2014]; however, PUFs essentially leverage device-to-device process variation. In some sense, this suggests that noisier devices are more useful. Orthogonal to these efforts, we present a collection of design concepts that leverage the unique properties of emerging technologies, other than those relying on noisy devices, for IP protection and hardware attack prevention. Specifically, the article considers two emerging technologies: silicon nanowire (SiNW) FETs [De Marchi et al. 2012] and graphene SymFETs [Sedighi et al. 2014b], and makes the following contributions. To assist in IP protection, we introduce SiNW FET–based camouflaging layout and polymorphic gates to help obfuscate layouts and netlists (see Sections 3.1 and 3.2). We further propose SymFET circuit protectors to counter fault injection attacks (see Section 3.3). Last, we present a lightweight SymFET-based XOR for implementing cryptographic functions (see Section 3.4). Preliminary experimental results and

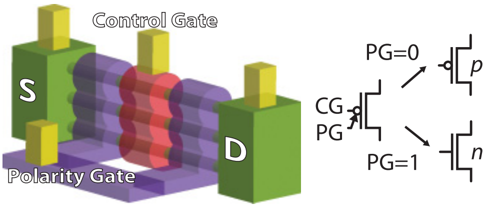

Fig. 1. 3D sketch of the SiNW FETs, featuring two independent gates and their associated symbols [De Marchi et al. 2012].

hardware infrastructure designs are provided. Simulation results demonstrate that these emerging technologies outperform CMOS in area and power while maintaining the same qualitative level of security.

2. EMERGING TECHNOLOGY

Driven by the need for post-CMOS technology, a great deal of research has been concentrated on the invention of new devices and their applications. Various emerging devices have been fabricated, including the FinFETs [Hisamoto et al. 2000; Jan et al. 2012; Ma et al. 2014], tunnel FETs (TFETs), carbon nanotube FETs (CNTFETs) [Appenzeller et al. 2006; Lin et al. 2011], graphene-based symmetric tunneling FETs (SymFETs) [Zhao et al. 2013], and spin-transfer-torque devices [Roy et al. 2014].

2.1. SiNW FETs

In several nanoscale FET devices (45nm and below), the superposition of n-type and p-type carriers is observable under normal bias conditions. The phenomenon, called *ambipolarity*, exists in various materials, such as silicon [Colli et al. 2007], carbon nanotubes [Martel et al. 2001], and graphene [Geim and Novoselov 2007]. Through the control of this ambipolarity, we can adjust the device polarity during the postdeployment stage. Transistors with a controllable polarity have already been experimentally fabricated in several novel technologies, such as carbon nanotubes [Lin et al. 2005], graphene [Harada et al. 2010], and SiNWs [Appenzeller et al. 2006; Heinzig et al. 2012]. Given an additional gate, the operation of these FETs is enabled by the regulation of Schottky barriers at the source/drain junctions. The example emerging device considered in this article is a vertically stacked SiNW FET, featuring two gate-all-around (GAA) electrodes [De Marchi et al. 2012]. Figure 1 shows the 3D structure of the SiNW FET. Vertically stacked GAA SiNWs represent a natural evolution of FinFET structures, providing better electrostatic control over the channel and, consequently, superior scalability properties [De Marchi et al. 2012].

In this device, one gate electrode, the Control Gate (CG), acts conventionally by turning on and off the device depending on the gate voltage. The other electrode, 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 [De Marchi et al. 2012; Gaillardon et al. 2014b].

Whereas many emerging devices demonstrate the polarity control property (SiNWFETs, graphene transistors, CNTFETs, NEM relays, etc.), we focus on SiNW FETs due to their full process compatibility with the current silicon technology and their high probability of industrial transfer in the near term. In addition, both single transistors and basic logic gates for SiNW FETs have been experimentally demonstrated. Furthermore, a simple compact model is available. However, note that the techniques

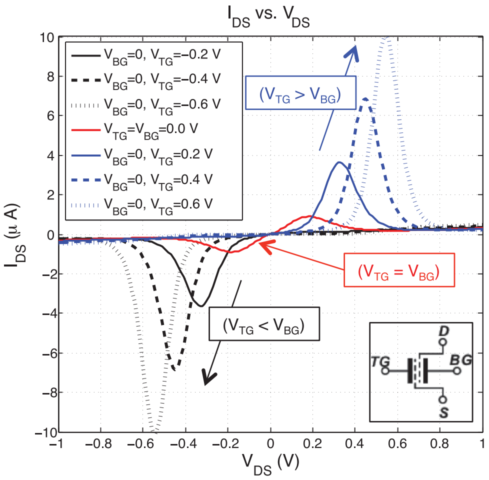

Fig. 2. I-V characteristics of SymFET device for different top and back gate voltage combinations.

presented in this article are not limited only to this device but rather can be applied to any other polarity-controllable transistor devices.

2.2. Graphene SymFETs

As MOSFET alternatives, tunneling-based transistor technologies (e.g., Seabaugh and Zhang [2010] and Lu and Seabaugh [2014]) are being actively investigated by device scientists. Among these devices is a double-layer graphene transistor—often referred to as a SymFET [Zhao et al. 2013]. In the SymFET device, tunneling occurs between the two graphene sheets that are separated by insulating and oxide layers. Possible $I_{DS} - V_{DS}$ characteristics of a SymFET, which are a function of a top gate voltage (V_{TG}) and back gate voltage (V_{BG}) (see the device symbol in the Figure 2 inset), are illustrated in Figure 2. Similar characteristics have also been observed experimentally [Britnell et al. 2013]. More specifically, V_{TG} and V_{BG} change the carrier type/density of the drain and source graphene layers by an electrostatic field, which can modulate I_{DS}. Per Figure 2, the value and position of the peak current depends on the values of V_{TG} and V_{BG}. Note that the I-V curves illustrated in Figure 2 assume a SymFET device with a 100 × 100 nm footprint with a coherence length of 0.75X of the edge side and an insulating layer of boron nitride (h-BN) that is 1.34nm (or four h-BN layers) thick. Although further study is required, tuning the insulator thickness could represent another design lever at the device level. For example, theoretically, by reducing barrier thickness to two layers of h-BN, tunneling current could be increased substantially—albeit at the expense of higher leakage current [Sedighi et al. 2014b].

The unique I-V characteristics of SymFET offer some interesting circuit-level alternatives for realizing both analog and digital circuits [Sedighi et al. 2014a, 2014b]. For example, simply cascading SymFET devices leads to an extremely small majority gate design. Furthermore, different combinations of V_{TG} and V_{BG} can change the shape of the I-V curve dramatically. Devices such as the interlayer tunnel FET (ITFET) have similar behaviors as the SymFET. We use SymFETs as a proxy for all of these types of devices.

3. EMERGING TECHNOLOGY IN HARDWARE SECURITY

The characteristics of both SiNW FETs and graphene SymFETs, shown in Figures 1 and 2, prove to us that these new devices are not drop-in alternatives to traditional

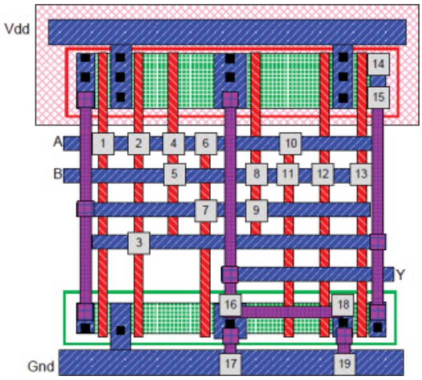

Fig. 3. CMOS camouflaged layout for achieving XOR, NAND, or NOR [Rajendran et al. 2013].

Table I. List of True and Dummy Contacts to Realize Three Functions for the Camouflaged Layout Presented in Figure 3

Function	Contacts	
	True	Dummy
NAND	2,4,6,8,11,12,16,17	1,3,5,7,9,10,13,14,15,18,19
NOR	2,5,6,11,12,18,19	1,3,4,7,8,9,10,13,14,15,16,17
XOR	1,3,4,7,9,10,12,13,14,15,18,19	2,5,6,8,11,16,17

MOSFETs. Instead, these new devices are equipped with unique physical properties that may be leveraged by hardware security approaches to achieve various highly efficient implementations for IP protection, Trojan detection, and side-channel attack prevention. In this section, we introduce SiNW FET– and SymFET-based circuit structures for hardware security applications.

3.1. SiNW FET–Based Camouflaging

Counterfeiting and IP piracy are among the most serious security threats to the IC industry. To prevent attackers from learning the circuit schematic through reverse engineering, various protection methods have been developed, among which camouflaging is a popular solution [Chow et al. 2002; Ronald et al. 2012; Chow et al. 2012]. This method relies on layout-level obfuscation with similar layouts for different gates. As a result, attackers cannot easily recover the circuit structure through reverse engineering [Rajendran et al. 2013]. However, the overhead in applying CMOS camouflaging gates can be rather high such that both power consumption and area would increase significantly for high-level protection.

In Rajendran et al. [2013], a CMOS camouflaging standard cell utilizes 12 transistors and a group of contacts to achieve three logic functions, as shown in Figure 3. There are more contacts than in a normal standard cell, as some of the contacts work as dummies to camouflage the functionality of this logic cell. More specifically, in Table I, different combinations of true and dummy contacts deliver three different logic functions. For example, when contacts 2,4,6,8,11,12,16,17 are true and contacts 1,3,5,7,9,10,13,14,15,18,19 are fake, the camouflaging layout performs the NAND functionality. With more functionalities being achieved by a camouflaging gate, it becomes more difficult for attackers to recover the gate functionality through reverse engineering. Compared to the 4-T NAND, 4-T NOR, and 8-T XOR gates, the area overhead of CMOS camouflaging layout ranges from 50% to 200%.

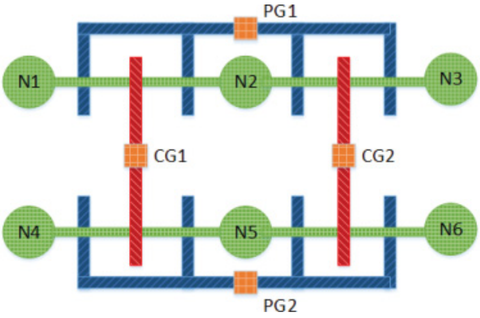

Fig. 4. One-tile layout for either a NAND or a XOR gate under different pin connections [Gaillardon et al. 2014b].

Table II. List of Possible Functions from a One-Tile Layout

PG1	PG2	CG1	CG2	N1	N2	N3	N4	N5	N6	Function (Y)
GND	VDD	A	B	Y	VDD	Y	GND	N/A	Y	NAND
GND	VDD	A	B	VDD	N/A	Y	Y	GND	Y	NOR
Bbar	B	A	Abar	VDD	Y	GND	GND	Y	VDD	XOR
Bbar	B	A	Abar	GND	Y	VDD	VDD	Y	GND	XNOR
Bbar	B	A	Abar	Cbar	Y	C	C	Y	Cbar	XOR3
Bbar	B	A	Abar	C	Y	Cbar	Cbar	Y	C	XNOR3
GND	VDD	A	X	X	VDD	Y	X	GND	Y	Buffer

It is not surprising that CMOS camouflaging gates consume a significantly larger area than normal gates. Because of the fixed polarities of both PMOS and NMOS, designers must prepare spare transistors to build a camouflaging gate. However, the polarity-controllable SiNW FETs, with their unique property, can help build camouflaging gates without using extra FETs. As demonstrated in Gaillardon et al. [2014b], only four SiNW FETs are required to build a XOR or a NAND gate (Figure 4). This one-tile layout includes four SiNW FETs, where circles stand for drain/source pins and bars represent the polarity gate (or control gate). A further analysis reveals that by connecting pins with different signals, the four SiNW FETs in Figure 4 can perform five other meaningful functions besides the NAND and XOR. A list of all of these connections, as well as the corresponding output functions, are presented in Table II. Note that the functionality of the gate is fixed postfabrication, with gate signals being connected to physical terminals. After these connections, the polarity gates perform as normal input gates, and no extra control circuitry is required to maintain the functionality. This structure, or more precisely the polarity-controllable feature, provides an ideal candidate for camouflaging gates, as all of these gates share the same structure with only four SiNW FETs used. In fact, the additional polarity gate is leveraged in the camouflaging gate layout to reduce the transistor count. The overhead of this SiNW-based camouflaging layout is negligible, which is mainly caused by additional insignificant dummy contacts. Following this concept, two SiNW FET–based camouflaging gates are built of different complexities. The first camouflaging gate performs either NAND or NOR functionality if different sets of dummy contacts are selected. Figure 5 shows the layout of the gate where 10 dummy/real contacts are used. As presented in Table III, if we leave 3,6,7,8,9 as dummy contacts, the gate is a NAND gate. If we make 1,2,4,5,10 contacts as dummy contacts, the gate will then perform NOR logic.

Figure 6 shows a more complex camouflaging gate that can act as NAND, NOR, XOR, or XNOR given different sets of dummy contacts. As described in Table IV, different

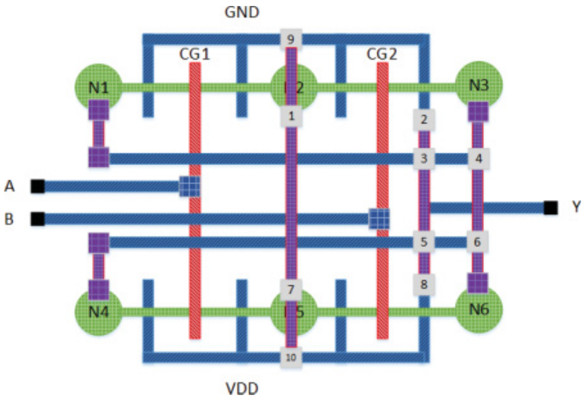

Fig. 5. Camouflaging layout performing NAND or NOR.

Table III. List of True and Dummy Contacts to Realize Basic Functions for the Layout in Figure 5

Function	Contacts	
	True	Dummy
NAND	1,2,4,5,10	3,6,7,8,9
NOR	3,6,7,8,9	1,2,4,5,10

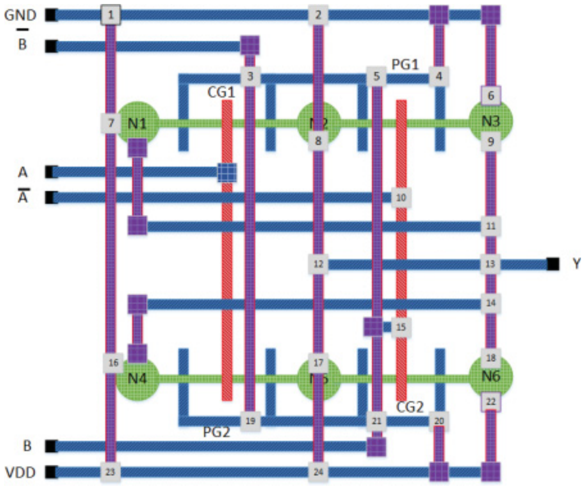

Fig. 6. Camouflaging layout with four possible functions: NAND, NOR, XOR, or XNOR.

connections can result in four different operations for the same input signals. Again, only four SiNW FETs are used in this camouflaging gate. Compared to the CMOS-based camouflaging gate, which needs 12 transistors for a NAND-NOR-XOR gate, the proposed circuit structure can reduce two-thirds of the transistor count. However, five more contacts are used in the SiNW FET–based camouflaging gate, although the area overhead incurred by the extra contacts are negligible considering the transistor count reduction. To further evaluate the security improvement, the security metric has been used to check how easily an attacker can guess the full functionality of given designs containing camouflaging gates. In other words, if one camouflaging layout can achieve

Table IV. List of True and Dummy Contacts to Realize Complex Functions for the Layout in Figure 6

Function	Contacts	
	True	Dummy
NAND	1,4,8,9,11, 13,15,16,18,20,24	2,3,5,6,7,10, 12,14,17,19,21,22,23
NOR	2,4,7,9,13, 14,15,17,18,20,23	1,3,5,6,8,10, 11,12,16,19,21,22,24
XOR	1,3,6,8,10,11,12, 16,17,18,21,22	2,4,5,7,9,13,14, 15,19,20,23,24
XNOR	1,5,6,8,10,11,12, 16,17,18,19,22	2,3,4,7,9,13,14, 15,20,21,23,24

four functions, the chance that the attacker can retrieve the correct result is 25%. Therefore, assuming that there are N SiNW FET camouflaging layouts incorporated in the design, the attacker may have to try up to 4^N times to get the correct design layout. As a consequence, it is promising that the SiNW FET–based camouflaging layout, which has more functionality and less area consumption compared to CMOS counterparts, can achieve a higher level of protection to circuit designs.

3.2. SiNW FET–Based Polymorphic Gates

Polymorphic electronics, which were first introduced in Stoica et al. [2004], are based on the idea of having multiple functionalities built in the same cell and deciding the input-output relation by means of a controllable factor in the circuit. For instance, a polymorphic gate presented in Stoica et al. [2004] would be an AND gate when the VDD is 3.3V and function as an OR gate when VDD is lowered to 1.5V. Such multifunctional gates would prove useful in a number of applications. Circuits that change functionality with temperature variation can find use in aerospace applications, or those that respond to VDD variation could be used to change functionality when the battery is low. In addition, polymorphic electronics could prove useful in evolvable, intelligent, or self-checking hardware [Ruzicka 2007]. For security purposes, adding polymorphic gates to a digital circuit can hide the real functionality of the circuit. Since the circuit functions correctly only in a certain configuration of the control signals known to the designer, even if the adversary knows the whole netlist (including the dummy and true contacts), he or she will not be able to utilize the circuit in his or her own design. Carefully encrypting a logic in this way can ensure that it will take too long for the adversary to find the key (a vector constructed from all morphing signals of the polymorphic gates) [Rajendran et al. 2012]. Therefore, the polymorphic gate becomes a good candidate for integrated circuits protection against IP piracy.

Traditionally, several CMOS-based polymorphic gates have been reported with different control methods, such as temperature, VDD variation, and external signal level. A summary of the different polymorphic circuits can be seen in Table V. Stoica et al. [2004] designed polymorphic gates by an evolution algorithm. However, the circuits face issues during simulation, as the circuit was evolved to satisfy certain constraints that do not include all aspects of a complete design. For example, the NAND/NOR polymorphic gate based on external signal will experience states where the transistors have to compete over the output, causing the circuit to draw constant current through those paths. Further, since inputs may be shorted to ground or VDD during certain states, it is difficult to connect multiple stages of these gates in sequence. The circuit based on VDD variation is the most practical solution and was fabricated [Stoica et al. 2004]; however, redesigning it in newer technologies where the VDD range is limited would be a difficult task. Another promising solution presented in Ruzicka [2007] is

Table V. Summary of Developed Polymorphic Gates

Function	Morph Method	Number of Transistors	Where Published
AND/OR	27/125 C Temperature	6	Stoica et al. [2001]
AND/OR/XOR	3.3/0.0/1.5V External signal	10	Stoica et al. [2001]
AND/OR	3.3/0.0V External signal	6	Stoica et al. [2001]
NAND/NOR/XOR/AND	0.0/0.9/1.1/1.8V External signal	11	Stoica et al. [2001]
AND/OR	1.2/3.3V Vdd	8	Stoica et al. [2001]
NAND/NOR	3.3/1.8V Vdd	6	(Fabricated) Stoica et al. [2004]
NAND/XOR	0/3.3V External signal	9	Ruzicka [2007]
NAND/NOR	VDD and GND interchange	4	This work

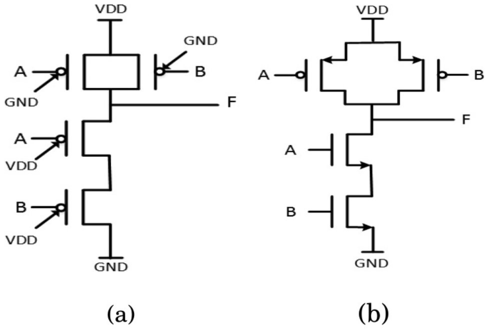

Fig. 7. (a) SiNW FETs NAND. (b) CMOS NAND.

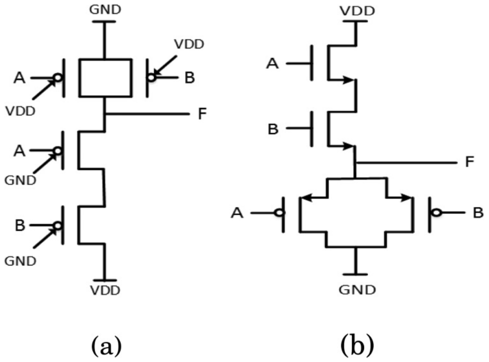

Fig. 8. (a) SiNW FETs NOR. (b) CMOS NOR.

a NAND/XOR gate controlled by a control signal using nine transistors. The gate has good performance even when we redesigned it in the 22nm FinFET technology node.

Here we present a novel approach to designing polymorphic gates using polarity-controllable FETs. The ability to control the polarity of a transistor enables us to build polymorphic cells with a much less number of transistors. As shown in Figures 7 and 8, the basic NAND and NOR gate structure is similar for both the CMOS and the SiNW FET. The polarity control gate does not reduce the number of transistors required to implement NAND and NOR using SiNW FET technology. However, this unique property allows us to change the functionality of the gate simply by interchanging the

Table VI. Simulation Results for NAND/NOR Gates

Gate	Static Power (pW)	Average Dynamic Power for Output Switching at 1GHz (uW)	Delay Averaged on Different Transitions (ps)
FinFET 22nm LSTP NOR	52.19	0.19	28
FinFET 22nm HP NOR	30360	0.67	23.5
FinFET 22nm LSTP NAND	27.19	0.15	23
FinFET 22nm HP NAND	1650	0.652	15.5
SiNW FET 20nm ~~NAND~~/NOR	8.037	1.77	42
SiNW FET 20nm NAND/~~NOR~~	4.127	1.13	56

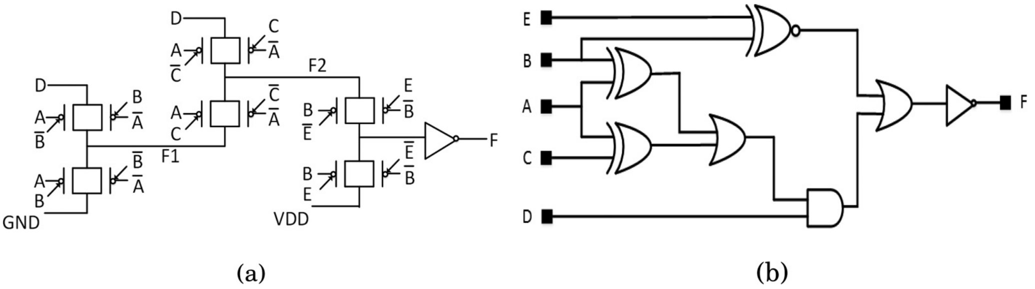

Fig. 9. Original functionality of a SiNW FET complex gate. (a) Transistor schematic. (b) Gate schematic.

VDD and GND. Note that interchanging the VDD and GND connections in any CMOS-based logic will produce the complement of the original function at the output, but full voltage swing at the output will not be achieved due to the presence of PMOS in the pull-down network or NMOS in the pull-up network. Therefore, using this method, one can gather the VDD and GND terminals of the NAND and NOR gates in a combinational logic into a vector and construct a "logic encryption key." As opposed to the work presented in Rajendran et al. [2012], which adds additional XOR or XNOR gates into a logic gate to realize the logic encryption scheme and thus incurs performance overhead, this approach has zero overhead in terms of gate count and trivial wiring cost due to the switching of VDD/GND. The comparison of transistor counts for different polymorphic gates is listed in Table V.

The simulation results for the NAND and NOR generic cells using the EPFL SiNW FET model [Gaillardon et al. 2014b] and the FinFET 22nm low standby power (LSTP) and high performance (HP) configurations of the PTM model [Arizona State University 2014] can be viewed in Table VI. It is not surprising to see that SiNW FET–based NAND (or NOR) gate consumes more dynamic power and has longer delay than the CMOS NAND (or NOR) gate, mainly because of the immaturity of the SiNW FET technology. Note that the leakage power of the SiNW FET is drastically reduced compared to that of FinFET technology.

The performance comparison in Table VI does not take the SiNW FET unique property into consideration. In fact, the benefits of using SiNW FETs can be revealed if the polarity-controllable property is leveraged (e.g., sophisticated polymorphic gates). To validate our claim, a sample polymorphic gate is designed (Figure 9). The two separate functions shown in Figures 9(b) and 10(b) can be implemented by the SiNW FET circuit in its different VDD and GND configurations depicted in Figures 9(a) and 10(a). Table VII lists the simulation results of the designed SiNW FET polymorphic logic and a MUX-based CMOS polymorphic gate that achieves the same functionality.

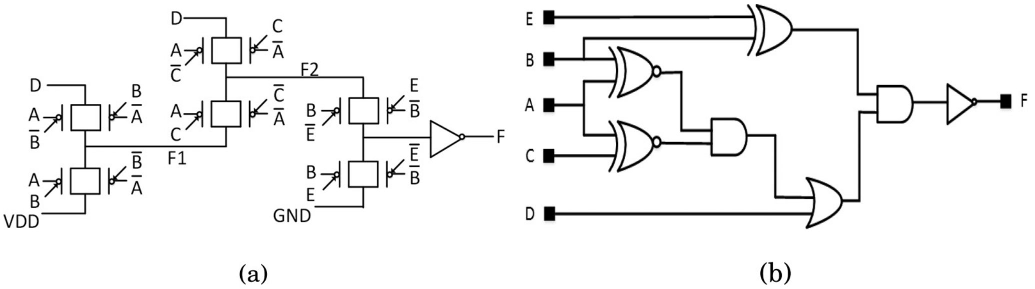

Fig. 10. Reconfigured functionality of a SiNW FET complex gate. (a) Transistor schematic. (b) Gate schematic.

Table VII. Simulation Results of the SiNW FET and CMOS Five-Input Polymorphic Function

Technology	Static Power (nW)	Switching Average Power (uW)	Average Delay (ps)
FinFET 22nm LSTP	0.755	4.04	80
FinFET 22nm HP	491	5.4	60
SiNW 20nm	0.01	2.5	100

As the results suggest, the SiNW FET approach reduces the total dynamic power due to the fewer number of cells while suffering from a longer delay because of the same number of cells available in the critical path. Besides the extremely low leakage power, the overall performance of the SiNW FET polymorphic logic is better than its CMOS counterpart. Consequently, SiNW FET circuits outperform CMOS circuits in terms of power and delay while achieving a similar level of circuit protection. The security metric that we applied measures the difficulty level if attackers want to learn the circuit structure using the brute force method. In other words, if there are N gates each with two possible functions in the schematic, it would take 2^N trials for an attacker to determine the exact functionality of the circuit. The benefits can be more significant in more complex polymorphic logic for large-scale circuits protection. We would like to point that machine learning attacks may be used to speed up the hacking of encryption [Baumgarten et al. 2010]. Thus, judicious placement of these SiNW FET polymorphic gates in a circuit should also be considered to impede such attacks.

3.3. Graphene SymFET–Based Circuit Protectors

Besides the IP protection mentioned previously, emerging devices may also help to improve circuit resilience to counter various hardware attacks, such as fault injection and side-channel signal analysis, with extremely low performance overhead and little circuit redesign. For example, cryptographic circuits are often vulnerable to power supply–based fault injections [Barenghi et al. 2010]. The manipulation of the power supply causes faults due to the rise of the setup time needed for registers to switch into the correct state: this phenomenon particularly affects high-capacitance paths, which are often the slowest paths of the circuit. In this section, we introduce two SymFET-based circuit protectors that leverage the unique I-V characteristics of SymFETs to protect circuits from power supply fault injections.

3.3.1. Current-Based Circuit Protector. As shown in Figure 2, the I-V curve of a SymFET indicates that the I_{DS} only exists for a narrow band of V_{DS}. Supported by this property, we propose a current-based circuit protector, which can effectively prevent supply voltage–based fault injection. Figure 11 shows the proposed structure relying on the unique properties of SymFETs. As shown in the schematic, SymFET M1 is the only

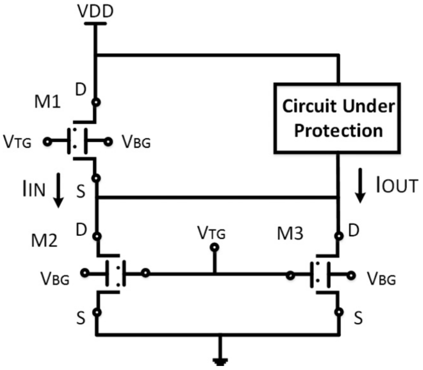

Fig. 11. Schematic of a current-based circuit protector.

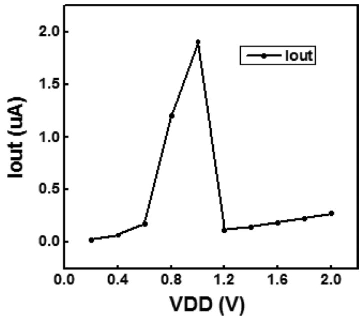

Fig. 12. Simulation of output current changing with VDD.

Table VIII. Power Provided by a Current-Based Circuit Protector

VDD (V)	0.2	0.4	0.6	0.8	1.0	1.2	1.4	1.6	1.8	2.0
Iout (uA)	0.022	0.067	0.176	1.205	1.904	0.114	0.145	0.184	0.227	0.272
Power (uW)	0.009	0.054	0.211	1.928	3.808	0.273	0.406	0.588	0.817	1.087

transistor directly connected to the power supply VDD, which is also the source to launch a voltage-based fault injection attack.

We use a specific parameter setting to explain how the circuit protector works. In our experiment, V_{TG} is set to 0.6V and V_{BG} is set to 0V for all three SymFETs. These gate voltages can be adjusted so that the peak current will appear in different power supply ranges than the one shown in Figure 12. Since M2 and M3 are connected in parallel, source-to-drain voltage V_{DS2} for M2 is equal to V_{DS3} for M3, which makes the output current I_{OUT} the same as the input current I_{IN}. The output current I_{OUT} is basically a current source for the circuit under protection. For this SymFET-based circuit protector, the output current can only exist for a specific drain-source voltage of SymFET M3. If V_{DS3} is out of this range, either higher or lower than the predefined range, the SymFET M3 will be cut off. As a consequence, the circuit under protection will be totally shut down.

The simulation results of the current-based circuit protector in Figure 12 show that only if the VDD is in the range from 0.8V to 1V, the output current will be at its peak values (e.g., 1.928uA when VDD is 1V). The power consumption is also derived and listed in Table VIII. When the supply voltage deviates from its normal value (e.g., 0.6V), the output current will drop down to 0.176uA. This feature can be directly exploited

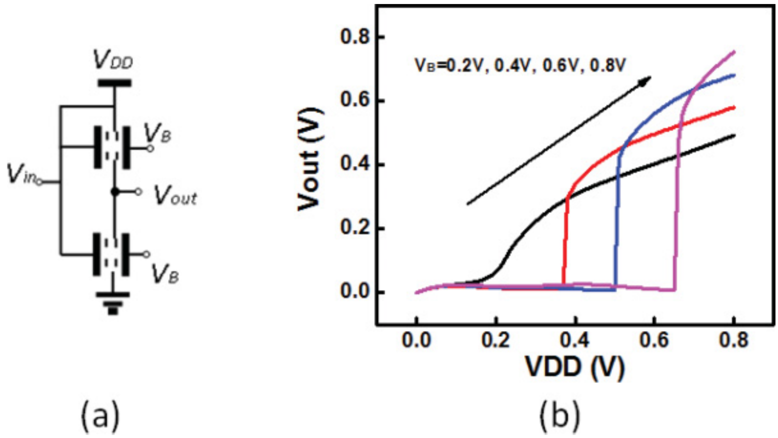

Fig. 13. Voltage-based circuit protector using SymFET. (a) Schematic. (b) Simulation results.

in circuit protection, countering side-channel attacks and fault injections. However, due to the limited maximum current, the current protector can mainly be applied for relatively lightweight cryptographic circuits to prevent fault injections. To handle relatively larger loads, either larger SymFET devices or multiple protectors are needed. If the attackers intend to lower the supply voltage to trigger a single-bit error of an encryption design, the entire circuit can be automatically shut down by the proposed circuit protector before a single-bit error could occur.

Traditionally, power regulators are often used in CMOS technology to protect the main circuit, but they suffer from large area and power consumption. For example, Guo and Leung [2010] proposed an area-efficient regulator based on the 90nm CMOS technology. The regulator includes more than 20 transistors, three capacitors, and one resistor with a total area of 0.019mm^2 and power consumption of 6μW. However, in our proposed structure, only three SymFET transistors are utilized, leading to an area reduction even though one SymFET consumes larger area than one MOSFET in a similar process. The main drawback of the designed circuit protector is the positive voltage at the virtual ground of the main circuit (i.e., the drain voltage of M3 may be larger than 0V). However, the proposed circuit protector can be used as an alternative to the current source, which acts as both a current source and a circuit protector [Li et al. 2014].

3.3.2. Voltage-Based Circuit Protector. Besides the current-based circuit protector, which protects the circuit through current manipulation, SymFETs can also be used to control the supply voltage for fault injection prevention. Figure 13(a) shows the schematic of the proposed voltage-based circuit protector, which is similar to an inverter design [Sedighi et al. 2014b]. However, in this circuit protector, the top gates of the two SymFETs are connected to the voltage source, whereas V_B can be manipulated for different cut-off voltage levels for output V_{out}. For instance, in Figure 13(b), in the case of V_B equal to 0.8V, the output voltage quickly drops to nearly zero when VDD is lowered down to 0.65V, therefore cutting off the voltage supply for the circuit under protection.

To further demonstrate the functionality of the proposed circuit protector, a full adder in the 20nm FinFET technology combined with the protector is implemented and simulated as shown in Figure 14. Note that since the current SymFET technology is not CMOS compatible, 3D stacking is needed to protect a CMOS circuit with the developed protector. That said, we have shown the feasibility of building digital circuits (Inverter, NAND, NOR, etc.) using SymFETs in Sedighi et al. [2014b]. Thus, one can ultimately

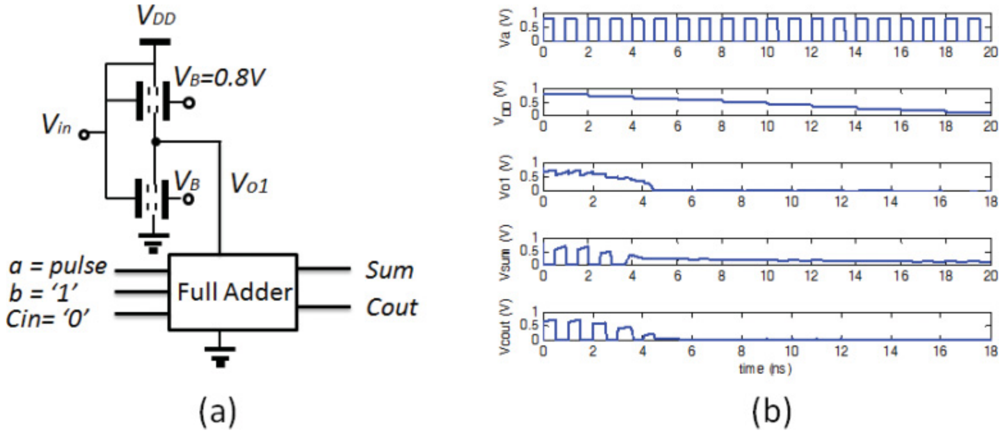

Fig. 14. Voltage-based circuit protector on a one-bit full adder. (a) Schematic. (b) Simulation results.

Table IX. Power Measurement of a SymFET Voltage-Based Circuit Protector

Voltage supply (V)	0.8	0.72	0.64	0.56	0.48	0.40	0.32	0.24
Leakage current (nA)	527	220	219	208	179	80.3	20.9	4.33
Power of the protector (nW)	250.5	135.7	142.9	110.3	76.1	30.3	5.9	0.4
Power of the full adder (nW)	310.9	117.0	1.0	<0.03	<0.02	<0.02	<0.02	<0.02

envision a chip comprised entirely of SymFETs. One input of the full adder is set to logic "1," and the other input is given as a periodic pulse signal. As we can see in Figure 14(b), the universal VDD is manipulated to decrease gradually. When it reaches 0.65V, the output voltage of the circuit protector quickly drops to zero. Consequently, both the sum and carry-out in the full adder output zero. We also measured the power consumption by the circuit protector and summarized the results in Table IX. Because the dynamic power is frequency dependent, input switching is set at 1GHz in the simulation. The leakage current shown here is the current flowing through the two SymFETs instead of the circuit under protection. As shown in Table IX, when the power supply is large enough to make the full adder operate normally, power consumption by the full adder dominates the overall power consumption. However, if the full adder is completely shut off when the supply voltage becomes lower than 0.65V, the majority of the total power is attributed to the static power of the circuit protector. Although high leakage may not be desired in low-power applications, for circuit protection purposes, the power overhead is bearable as long as it can prevent the intentional injection from the supply voltage. More research is needed along this direction to lower the leakage power.

Gomina et al. [2014] evaluated the impacts of power supply attacks where the voltage sensitivity margin is 0.4V. In other words, a bit flip error would only happen if the power supply glitch were larger than 0.4V. In what we have presented, the voltage sensitivity of our designs is less than 0.2V. Before the power glitch attack can be triggered, the SymFET circuit protector already shuts down the circuit to prevent such attacks. Note that the sensitivity of the SymFET projector can be adjusted by altering the top/back gate voltages. Another factor to consider is noise in the power supply. It may be possible that due to environmental variations (e.g., temperature variation and power noise), the supply voltage may fluctuate. If the voltage variation is larger than the design margin, a false alarm will be triggered and the circuit will be shut down even though no attacks are launched. For circuits working under extreme conditions, we may need to tune the circuit protector to increase the allowed supply voltage noise margin.

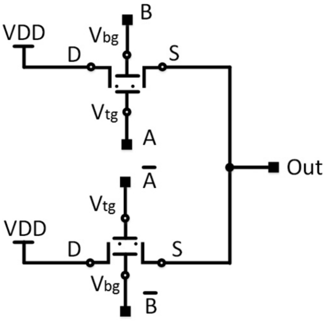

Fig. 15. Schematic of the SymFET XOR logic.

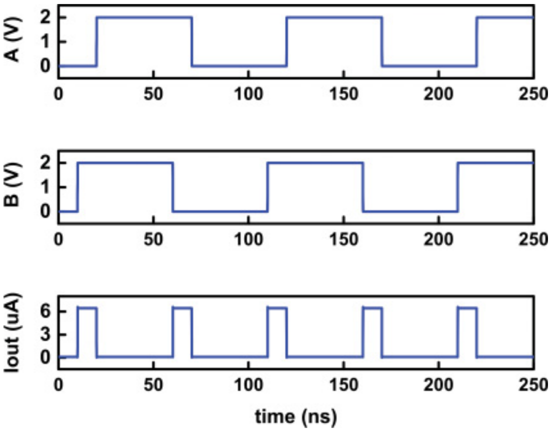

Fig. 16. Simulation results of the SymFET XOR logic.

3.4. Graphene SymFET–Based XOR Logic

In the cryptographic systems, XOR logic serves as a basic computation unit for many of the encryption algorithms. Since CMOS XOR gates often take at least eight transistors, area and power consumption of XOR network becomes the bottleneck to further improve the performance of cryptographic designs. However, in terms of the unique I-V characteristic and low-power feature, the SymFET brings in a new opportunity for hardware security implementation. In Sedighi et al. [2014b], a group of SymFET-based generic logic gates have been investigated, such as inverter, NAND, and majority gates.

Following a similar design method, a lightweight current-based XOR gate is then developed that uses only two SymFETs. In Figure 15, the Vtg of the upper SymFET is connected to input signal A, whereas the V_{bg} is connected to input signal B. The drain and source of the upper SymFET are connected to the voltage supply and the output port, respectively. In the lower SymFET, the V_{tg} and V_{bg} are tied up to complement A and complement B, respectively. The drain and source connections of the lower SymFET are the same as the upper one. The simulation results are shown in Figure 16, which illustrates that when input signals A and B are different, there will be a steady output current through the output port. When A and B are of equal value, the output current drops to nearly zero. In this demonstration, input signals are set as square pulses with the peak voltage of 2V, whereas the supply voltage remains at 500mV. Since the peak current happens due to the different configurations of drain-source voltage and

Table X. Summary of SiNW FET and SymFET in Security Applications

	SiNW FETs	Graphene SymFETs
Benefits over CMOS	Polarity configurable, low static power, fewer transistors for applications	Low power, built-in negative differential resistance
Challenges	Larger area per-transistor, large dynamic power	Current-based designs, non-Boolean computation
Opportunities	IP protection, logic encryption, other security applications	Side-channel attack prevention, cryptographic circuits

gate voltage (see Figure 2), the design also works with the settings of lower VDD and top/back gate voltage through the same configuration on all terminals.

To fully compare the performance between CMOS XOR and SymFET XOR, delay and power consumption of both gates are also measured. We implemented an eight-transistor XOR gate in CMOS 130nm technology with the nominal voltage of 1.5V [Sedighi et al. 2014b]. (The 130nm CMOS technology is chosen since this feature size is close to the feature size used by the SymFET device: 100 × 100 nm.) The CMOS XOR gate consumes 0.632μW. Although the SymFET-based XOR gate consumes 0.68μW, both gates are comparable in power consumption. However, the average delay of the SymFET XOR gate is 48ps. Compared to the 135ps delay of the CMOS XOR gate, the speed of the SiNW FET XOR gate is much faster. With slightly larger power consumption, the SymFET XOR gate outperforms the CMOS XOR gate significantly in delay and area. Moreover, the power consumption of the SymFET XOR gate can be further reduced by lowering the nominal voltage to less than 2.0V.

Although the XOR gate is the basic gate for many cryptographic circuits, other gates (e.g., inverter and NAND gates) may also be required. Sedighi et al. [2014b] and Gaillardon et al. [2014a] have already developed logic gates using SymFET and SiNW FET, respectively. Therefore, the developed XOR gate along with other logic gates can make the cryptographic circuits perform better than their CMOS counterparts.

4. DISCUSSION

Emerging technologies, acting as alternatives to CMOS logic, have already shown promising features for high-performance circuit design. However, the metrics to evaluate different technologies often follow the traditional criteria, focusing only on power, delay, area, and so forth for general-purpose computation modules. Special applications, such as hardware security, are rarely considered, mainly because MOSFETs do not support security and circuit protection naturally.

In this article, we presented security primitives on how the unique features of emerging technologies can help to protect circuits and prevent IP piracy. Unlike CMOS logic, the proposed protection schemes are of much lower overhead because security is not an add-on feature but a built-in feature. Through the simulation results, the two example devices proved to be efficient in hardware security applications. These preliminary results lead us toward a new metric for the comparison between CMOS logic and emerging technologies. Whereas traditional metrics, such as power and delay, are the major criteria to evaluate the merits of emerging devices, in this work, we include the security metric in the overall performance evaluation to fully compare the emerging devices with CMOS technology. A summary of the two emerging devices in hardware security applications is shown in Table X, which lists the benefits and challenges of the emerging-device–based designs compared to CMOS designs and can help to guide future designs in the hardware security area.

5. CONCLUSIONS

Emerging technologies were investigated in this article for their applications in the hardware security domain. Instead of simply replacing CMOS transistors with emerging devices, our work, for the first time, evaluated the unique properties of new devices in helping protect circuit designs and countering IP piracy. Two emerging technologies were used: SiNW FETs and graphene SymFETs. Five different security applications were designed and verified, ranging from IP protection to efficient cryptographic computation. Through our examples, we demonstrated that the unique properties of emerging technologies, if used properly, can provide high-level circuit protection with extremely low performance overhead. Along this direction, new evaluation metrics will be developed in our future work to better evaluate the merits of emerging devices. Besides the simulation results, as emerging technologies become more mature, measurements from fabricated devices will also be collected to verify the claim thatcircuit protection methods can benefit from emerging technologies.

REFERENCES

D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, and B. Sunar. 2007. Trojan detection using IC fingerprinting. In *Proceedings of the IEEE Symposium on Security and Privacy*. 296–310.

Yousra Alkabani and Farinaz Koushanfar. 2007. Active hardware metering for intellectual property protection and security. In *Proceedings of the USENIX Security Conference*. 291–306.

J. Appenzeller, J. Knoch, E. Tutuc, M. Reuter, and S. Guha. 2006. Dual-gate silicon nanowire transistors with nickel silicide contacts. In *Proceedings of the International Electron Device Meeting (IEDM'06)*. 1–4.

Arizona State University. 2014. PTM Model. Retrieved March 18, 2016, from http://ptm.asu.edu/.

A. Barenghi, G. M. Bertoni, L. Breveglieri, M. Pellicioli, and G. Pelosi. 2010. Fault attack on AES with single-bit induced faults. In *Proceedings of the 2010 6th International Conference on Information Assurance and Security (IAS'10)*. 167–172.

A. Baumgarten, A. Tyagi, and J. Zambreno. 2010. Preventing IC piracy using reconfigurable logic barriers. *IEEE Design Test of Computers* 27, 1, 66–75.

Y. Bi, P.-E. Gaillardon, X. S. Hu, M. Niemier, J.-S. Yuan, and Y. Jin. 2014. Leveraging emerging technology for hardware security—case study on silicon nanowire FETs and graphene SymFETs. In *Proceedings of the 2014 IEEE 23rd Asian Test Symposium (ATS'14)*. 342–347.

L. Britnell, R. V. Gorbachev, A. K. Geim, L. A. Ponomarenko, A. Mishchenko, M. T. Greenaway, T. M. Fromhold, K. S. Novoselov, and L. Eaves. 2013. Resonant tunnelling and negative differential conductance in graphene transistors. *Nature Communications* 4, 1794. http://dx.doi.org/10.1038/ncomms2817.

Lap-Wai Chow, James Baukus, and William Clark. 2002. Integrated circuits protected against reverse engineering and method for fabricating the same using an apparent metal contact line terminating on field oxide. Patent US 7294935 B2. http://www.google.com/patents/US7294935.

Lap Wai Chow, James P. Baukus, Bryan J. Wang, and Ronald P. Cocchi. 2012. Camouflaging a standard cell based integrated circuit. Patent US 8151235 B2. http://www.google.com/patents/US8151235.

A. Colli, S. Pisana, A. Fasoli, J. Robertson, and A. C. Ferrari. 2007. Electronic transport in ambipolar silicon nanowires. *Physica Status Solidi (b)* 244, 11, 4161–4164.

M. De Marchi, D. Sacchetto, S. Frache, J. Zhang, P.-E. Gaillardon, Y. Leblebici, and G. De Micheli. 2012. Polarity control in double-gate, gate-all-around vertically stacked silicon nanowire FETs. In *Proceedings of the 2012 IEEE International Electron Devices Meeting (IEDM'12)*. 8.4.1–8.4.4.

Frontier Economics. 2011. *Estimating the Global Economic and Social Impacts of Counterfeiting and Piracy*. Technical Report. Frontier Economics Ltd., London, England.

Pierre-Emmanuel Gaillardon, Luca Amaru, Jian Zhang, and Giovanni De Micheli. 2014a. Advanced system on a chip design based on controllable-polarity FETs. In *Proceedings of the Conference on Design, Automation, and Test in Europe (DATE'14)*.

P.-E. Gaillardon, S. Bobba, M. De Marchi, D. Sacchetto, and G. De Micheli. 2014b. Nanowire systems: Technology and design. *Philosophical Transactions of the Royal Society of London A* 372, 20130102.

A. K. Geim and K. S. Novoselov. 2007. The rise of graphene. *Nature Materials* 6, 183–191.

K. Gomina, J.-B. Rigaud, P. Gendrier, P. Candelier, and A. Tria. 2014. Power supply glitch attacks: Design and evaluation of detection circuits. In *Proceedings of the 2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST'14)*. 136–141.

Jianping Guo and Ka Nang Leung. 2010. A 6-μW chip-area-efficient output-capacitorless LDO in 90-nm CMOS technology. *IEEE Journal of Solid-State Circuits* 45, 9, 1896–1905.

Naoki Harada, Katsunori Yagi, Shintaro Sato, and Naoki Yokoyama. 2010. A polarity-controllable graphene inverter. *Applied Physics Letters* 96, 1, Article No. 012102.

André Heinzig, Stefan Slesazeck, Franz Kreupl, Thomas Mikolajick, and Walter M. Weber. 2012. Reconfigurable silicon nanowire transistors. *Nano Letters* 12, 1, 119–124.

Digh Hisamoto, Wen Chin Lee, Jakub Kedzierski, Hideki Takeuchi, Kazuya Asano, Charles Kuo, Erik Anderson, Tsu Jae King, Jeffrey Bokor, and Chenming Hu. 2000. FinFET—a self-aligned double-gate MOSFET scalable beyond 20nm. *IEEE Transactions on Electron Devices* 47, 12, 2320–2325.

ITRS. 2013. Emerging research devices and emerging research materials. In *International Technology Roadmap for Semiconductors* (2013 ed.). ITRS, New York, NY, 43.

A. Iyengar, K. Ramclam, and S. Ghosh. 2014. DWM-PUF: A low-overhead, memory-based security primitive. In *Proceedings of the 2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST'14)*. 154–159.

C.-H. Jan, U. Bhattacharya, R. Brain, S.-J. Choi, G. Curello, G. Gupta, W. Hafez, M. Jang, M. Kang, K. Komeyli, T. Leo, N. Nidhi, L. Pan, J. Park, K. Phoa, A. Rahman, C. Staus, H. Tashiro, C. Tsai, P. Vandervoorn, L. Yang, J.-Y. Yeh, and P. Bai. 2012. A 22nm SoC platform technology featuring 3-d tri-gate and high-k/metal gate, optimized for ultra low power, high performance and high density SoC applications. In *Proceedings of the 2012 IEEE International Electron Devices Meeting (IEDM'12)*.

Y. Jin and Y. Makris. 2008. Hardware Trojan detection using path delay fingerprint. In *Proceedings of the IEEE International Workshop on Hardware-Oriented Security and Trust*. 51–57.

Y. Jin and D. Oliveira. 2014. Extended abstract: Trustworthy SoC architecture with on-demand security policies and HW-SW cooperation. In *Proceedings of the 5th Workshop on SoCs, Heterogeneous Architectures, and Workloads (SHAW-5)*.

Yier Jin, Bo Yang, and Yiorgos Makris. 2013. Cycle-accurate information assurance by proof-carrying based signal sensitivity tracing. In *Proceedings of the IEEE International Symposium on Hardware-Oriented Security and Trust (HOST'13)*. 99–106.

X. Li, W.-Y. Tsai, V. Narayanan, H. Liu, and S. Datta. 2014. A low-voltage low-power LC oscillator using the diode-connected SymFET. In *Proceedings of the 2014 IEEE Computer Society Annual Symposium on VLSI (ISVLSI'14)*. 302–307.

Sheng Lin, Yong-Bin Kim, and Fabrizio Lombardi. 2011. CNTFET-based design of ternary logic gates and arithmetic circuits. *IEEE Transactions on Nanotechnology* 10, 2, 217–225.

Y.-M. Lin, J. Appenzeller, J. Knoch, and P. Avouris. 2005. High-performance carbon nanotube field-effect transistor with tunable polarities. *IEEE Transactions on Nanotechnology* 4, 5, 481–489.

H. Lu and A. Seabaugh. 2014. Tunnel field-effect transistors: State-of-the-art. *IEEE Journal of the Electron Devices Society* 2, 4, 44–49. DOI: http://dx.doi.org/10.1109/JEDS.2014.2326622

K. S. Ma, H. C. Liu, Y. Xiao, Y. Zheng, X. Q. Li, S. K. Gupta, Y. Xie, and V. Narayanan. 2014. Independently-controlled-gate FinFET 6T SRAM cell design for leakage current reduction and enhanced read access speed. In *Proceedings of the 2014 IEEE International Symposium on Very-Large-Scale Integration (VLSI'14).*

R. Martel, V. Derycke, C. Lavoie, J. Appenzeller, K. K. Chan, J. Tersoff, and P. Avouris. 2001. Ambipolar electrical transport in semiconducting single-wall carbon nanotubes. *Physical Review Letters* 87, 25, 256805.

M. Potkonjak, A. Nahapetian, M. Nelson, and T. Massey. 2009. Hardware Trojan horse detection using gate-level characterization. In *Proceedings of the 46th Annual Design Automation Conference (DAC'09)*. 688–693.

J. Rajendran, Y. Pino, O. Sinanoglu, and R. Karri. 2012. Logic encryption: A fault analysis perspective. In *Proceedings of the Conference on Design, Automation, and Test in Europe*. 953–958.

Jeyavijayan Rajendran, Michael Sam, Ozgur Sinanoglu, and Ramesh Karri. 2013. Security analysis of integrated circuit camouflaging. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications Security (CCS'13)*. 709–720.

P. Ronald, P. James, and J. Bryan. 2012. Building block for a secure cmos logic cell library. Patent US 20100301903 A1. http://www.google.com/patents/US20100301903.

K. Roy, M. Sharad, D. L. Fan, and K. Yogendra. 2014. Computing with spin-transfer-torque devices: Prospects and perspectives. In *Proceedings of the 2014 IEEE International Symposium on Very-Large-Scale Integration (VLSI'14).*

R. Ruzicka. 2007. New polymorphic NAND/XOR gate. In *Proceedings of 7th WSEAS International Conference on Applied Computer Science*, Vol. 2007. 192–196.

Alan C. Seabaugh and Qin Zhang. 2010. Low-voltage tunnel transistors for beyond CMOS logic. *Proceedings of the IEEE* 98, 12, 2095–2110. DOI:http://dx.doi.org/10.1109/JPROC.2010.2070470

B. Sedighi, X. S. Hu, J. J. Nahas, and M. Niemier. 2014a. Nontraditional computation using beyond-CMOS tunneling devices. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems* 4, 4, 438–449.

B. Sedighi, Xiaobo Sharon Hu, Joseph J. Nahas, and M. Niemier. 2014b. Boolean circuit design using emerging tunneling devices. In *Proceedings of the International Conference on Computer Design (ICCD'14)*. 355–360.

Arvind Seshadri, Mark Luk, Ning Qu, and Adrian Perrig. 2007. SecVisor: A tiny hypervisor to provide lifetime kernel code integrity for commodity OSes. In *Proceedings of the 21st ACM SIGOPS Symposium on Operating Systems Principles (SOSP'07)*. 335–350.

A. Stoica, R. S. Zebulum, and D. Keymeulen. 2001. *Polymorphic Electronics*. Springer.

A. Stoica, R. S. Zebulum, D. Keymeulen, M. I. Ferguson, and V. Duong. 2004. Taking evolutionary circuit design from experimentation to implementation: Some useful techniques and a silicon demonstration. *IEE Proceedings—Computers and Digital Techniques* 151, 4, 295–300.

P. Zhao, R. M. Feenstra, Gong Gu, and D. Jena. 2013. SymFET: A proposed symmetric graphene tunneling field-effect transistor. *IEEE Transactions on Electron Devices* 60, 3, 951–957. DOI:http://dx.doi.org/10.1109/TED.2013.2238238

Received December 2014; revised August 2015; accepted August 2015