Leveraging Emerging Technology for Hardware Security - Case Study on Silicon Nanowire FETs and Graphene SymFETs

Yu Bi*, Pierre-Emmanuel Gaillardon†, X. Sharon Hu‡, Michael Niemier‡, Jiann-Shiun Yuan*, and Yier Jin*
*Department of Electrical Engineering and Computer Science, University of Central Florida
†École Polytechnique Fédérale de Lausanne (EPFL) - Switzerland
‡Department of Computer Science and Engineering, University of Notre Dame

***Abstract*—Hardware security concerns such as IP piracy and hardware Trojans have triggered research into circuit protection and malicious logic detection from various design perspectives. In this paper, emerging technologies are investigated by leveraging their unique properties for applications in the hardware security domain. Three example circuit structures including camouflaging gates, polymorphic gates and power regulators are designed to prove 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 emerging technologies.**

I. 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 malfunction. Hardware counterfeiting and IP piracy is another serious issue costing the US economy more than $200 billion annually [1]. In order to address such threats, various hardware Trojan detection methods and hardware metering methods have been developed to detect hardware Trojans and prevent IP piracy [2]–[5]. Besides circuit level security solutions, cybersecurity researchers also rely on layered security protection approaches and have developed various methods to protect the higher abstract layer through security enhancement at the lower abstract layer. Through this chain, cybersecurity protection schemes have been pushed downward from virtual machine to hypervisor. Following this trend, new methods are under development through which the hardware infrastructure is modified to directly support sophisticated security policies so that system level protection scheme will be more efficient [6].

However, the prevailing CMOS technology does not support security applications naturally. Therefore, developing CMOS-based hardware security solutions, despite circuit optimizations and improved design techniques, still faces a lot of challenges particularly in terms of circuit complexity, performance, and power consumption. That is, MOSFETs are often treated as simple switches in digital designs such that only sophisticated circuit designs, or even software level operations, can achieve the goal of security applications. However, this comes at the cost of high design complexity and decreased performance.

Fortunately, the development of emerging technologies provides hardware security researchers opportunities to change the passive role that CMOS technology plays in security applications. Originally developed as alternatives to CMOS technology to overcome the scaling limit, emerging technologies also demonstrate unique features which, besides improving circuit performance, can simplify circuit structure for security purposes such as IP protection and Trojan detection. 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, etc. [7], two fundamental questions have recently been raised related to their applications in the hardware security domain: 1) *Can emerging technology provide a more efficient hardware infrastructure than CMOS technology in countering hardware Trojans and IP piracy*? 2) *What properties should the emerging technology-based hardware infrastructure provide so that software level protection schemes can be better supported*? Being the first paper introducing emerging technologies in hardware security applications, we try to answer the first question by providing preliminary experimental results and hardware infrastructure designs using two emerging technologies: silicon nanowire (SiNW) FETs [8] and Graphene SymFETs [9]. Design schematics/layouts and testing results will also be provided to uphold our claim that these emerging technologies outperform CMOS in many hardware security applications.

II. 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 [10], tunnel-FETs (TFETs) [11], carbon nanotube FETs (CNTFETs) [12], Graphene-based symmetric tunneling FETs (SymFETs) [13], and spin-transfer-torque devices [14].

A. Silicon Nanowire 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 [15], carbon nanotubes [16] and graphene [17]. Through the control of this ambipolarity, we can adjust the device polarity during the post-deployment stage. Transistors with a controllable polarity have already been experimentally fabricated in several novel technologies, such as carbon nanotubes [18], graphene [19] and Silicon NanoWires (SiNWs) [20], [21]. 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 paper is a vertically-stacked silicon nanowire (SiNW) FET, featuring two Gate-All-Around (GAA) electrodes [8]. Figure 1 shows the 3D structure of the SiNW FET. Vertically-stacked GAA SiNWs

1081-7735/14 $31.00 © 2014 IEEE
DOI 10.1109/ATS.2014.69

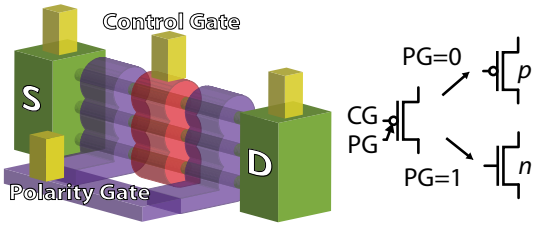

Figure 1: 3D sketch of the SiNWFETs featuring 2 independent gates and its associated symbol [8]

represent a natural evolution of FinFET structures, providing better electrostatic control over the channel and, consequently, superior scalability properties [8].

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 [8], [22].

B. Graphene SymFET

As MOSFET alternatives, tunneling based transistor technologies (e.g., [23]) are being actively investigated by device scientists. Among these devices is a double-layer graphene transistor – often referred to as SymFET [24]. In the SymFET device, tunneling occurs between the two graphene sheets – which 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 [25]. More specifically, V_{TG} and V_{BG} change the carrier type/density of the drain and source graphene layers by electostatic 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 nm $\times$ 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 1.34 nm (or 4 h-BN layers) thick. While 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 2 layers of h-BN, tunneling current could be increased substantially – albeit at the expense of higher leakage current [9].

The unique I-V characteristics of SymFET offer some interesting circuit-level alternatives for realizing both analog and digital circuits [9], [26]. 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.

III. Emerging Technology in Hardware Security

The characteristics of both silicon nanowire FETs (SiNW FETs) and graphene SymFETs, shown in Figures 1 and 2,

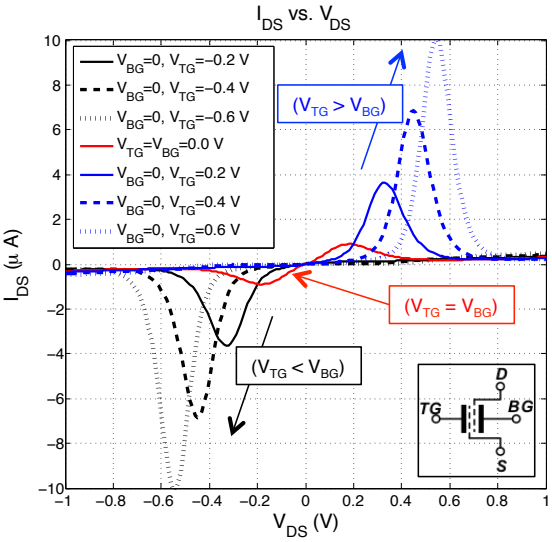

Figure 2: I-V characteristics of SymFET device for different top and back gate voltage combinations.

prove to us that these new devices are not drop-in alternatives to traditional MOSFETs. Instead, these new devices are equipped with unique physical properties which 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 will introduce SiNW FET and SymFET based circuit structures for hardware security applications.

A. SiNW FET based Camouflaging

Counterfeiting and IP piracy are among the most serious security threats to the IC industry. In order to prevent attackers from learning the circuit schematic through reverse engineering, various protection methods have been developed among which camouflaging is a popular solution [27]–[29]. 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 [30]. 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. For example, a generic camouflaged CMOS layout that can perform as an XOR, NAND or NOR gate requires at least 12 transistors along with a large area of metal connections [30]. Compared to the 4-T NAND, 4-T NOR and 8-T XOR gates, the area overhead ranges from 50% to 200%.

It is not surprising that CMOS camouflaging gates consume significantly larger area than normal gates. Because of the fixed polarities of both PMOS and NMOS, designers must prepare spare transistors in order 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 [31], only four SiNW FETs are required to build an XOR or a NAND gate (See Figure 3). A further analysis reveals that by connecting pins with different signals, the four SiNW FETs in Figure 3 can

Table I: List of possible functions from 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

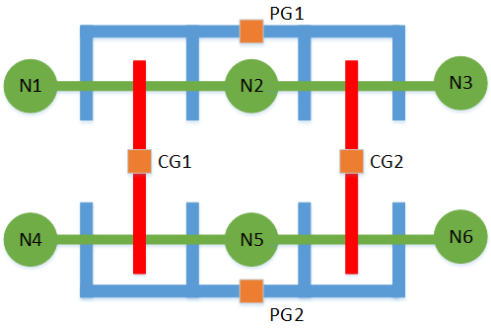

Figure 3: One tile layout for either an NAND or an XOR gate under different pin connections [31]

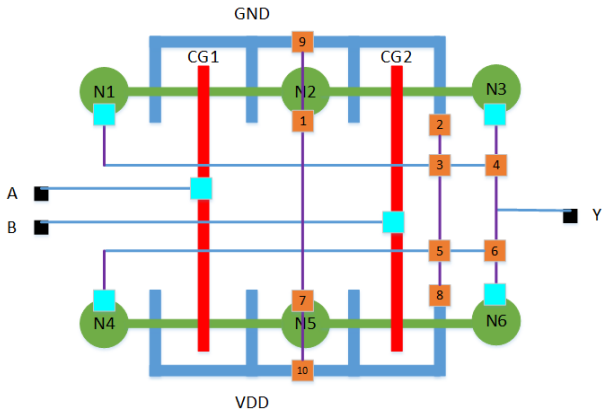

Figure 4: Camouflaging layout performing NAND or NOR

perform five other functions besides the NAND and XOR. A list of all these connections as well as the corresponding output functions are presented in Table I.

This structure, or more precisely the polarity controllable feature, provides an ideal candidate for camouflaging gates since all these gates share the same structure with only four SiNW FETs used. Following this concept, two SiNW FETs 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 4 shows the layout of the gate where 10 dummy/real contacts are used. As presented in Table II, if we leave No. 3,6,7,8,9 as dummy contacts, the gate is a NAND gate. If we make No. 1,2,4,5,10 contacts as dummy contacts, the gate will then perform NOR logic.

Figure 5 shows a more complex camouflaging gate which can act as NAND, NOR, XOR or XNOR given different

Table II: List of true and dummy contacts to realize basic functions for the layout in Figure 4

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

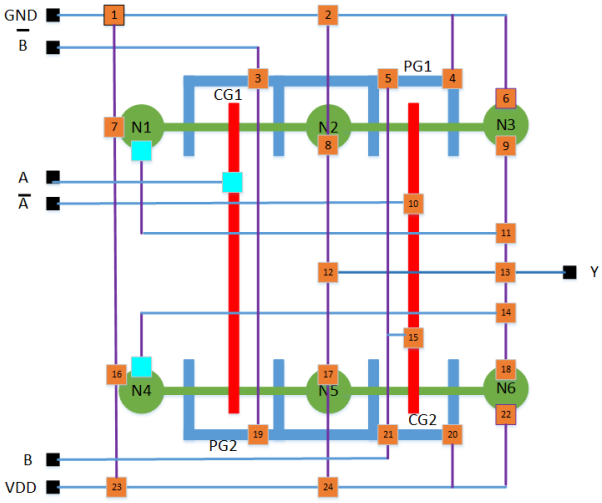

Figure 5: Camouflaging layout with four possible functions: NAND, NOR, XOR or XNOR

sets of dummy contacts. As described in Table III, different 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.

Table III: List of true and dummy contacts to realize complex functions for layout in Figure 5

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

B. SiNW FET based Polymorphic Gates

Different from the layout-level camouflaging, polymorphic gates provide a circuit-level protection against IP piracy. Through the insertion of polymorphic gates, attackers cannot recover circuit functionality even though the entire layout is known. Therefore, this method can also prevent untrusted foundries or workers in the foundry from stealing circuit designs. However, given all the benefits, polymorphic gates are rarely used in CMOS circuits mainly due to the difficulties in designing such gates using CMOS technology. The unique feature of the controllable polarity in SiNW FETs makes polymorphic gates feasible and easy to construct. That is, if we connect the control gate (CG) of a SiNW FET to a normal input while treating the polarity gate (PG) as the polymorphic control input, through different configurations on the polymorphic control inputs, we can easily change the circuit functionality. Since these polymorphic control inputs will only be configured after the circuits are fabricated and delivered, the usage of polymorphic gates can prevent the IC foundry from learning the circuit functionality, providing a powerful protection scheme countering IP piracy[1].

To demonstrate the feasibility of SiNW FET based polymorphic gates and to further point out why CMOS logic is not suitable for such gates, we choose a SiNW FET NAND gate and a CMOS NAND gate for demonstration. Figures 6(a) and 6(b) show the schematic view of the SiNW FET NAND gate and the CMOS NAND gate. Both gates share a similar structure with two PMOS in the pull-up network and two NMOS in pull-down network. The upper two SiNW FETs act as PMOS with the PGs connected to GND while the lower two SiNW FETs act as NMOS with the PGs connected to VDD. If we switch the VDD and GND connections, both gates will be changed to NOR gates (see Figure 7). In SiNW FET based NOR gate, only PMOS is used in pull-up network and only NMOS is used in pull-down network (thanks to the polarity switching). However, the switch of VDD and GND leaves PMOS in pull-down network and NMOS in pull-up network in the CMOS gate. This unique feature makes the SiNW FETs perfect options for polymorphic gate designs.

A more complex polymorphic gate relying on VDD and GND configuration is designed. The original functionality of the gate as well as its transistor-level schematic is shown in Figure 8. A reconfigured version is shown in Figure 9.

C. Graphene SymFET based Circuit Protection

Besides the above-mentioned IP protection, emerging devices may also help improve circuit resilience to counter various hardware attacks such as fault injection, side-channel signal analysis, etc. with extremely low performance overhead and little circuit redesign. For example, the newly developed graphene SymFETs have a special property that the source-drain current will be cut off if the source-drain voltage is outside a narrow voltage band. Figure 2 shows the I-V curve of a SymFET indicating that the I_{DS} only exists for a narrow band of V_{DS}.

[1]Note that the lack of circuit functionality does not hamper chip testing at the manufacturing site if properly selected test patterns are provided.

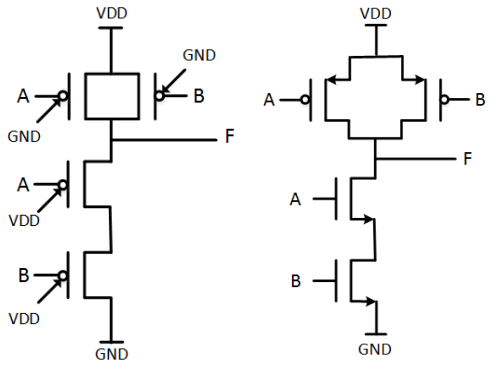

Figure 6: (a) SiNW FETs NAND (b) CMOS NAND

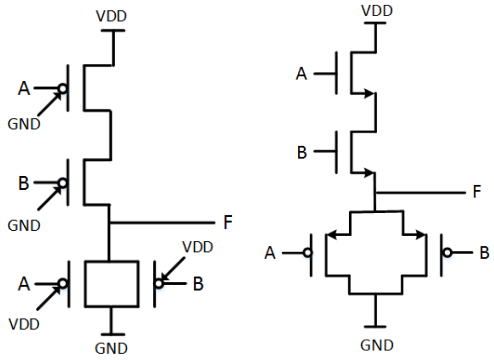

Figure 7: (a) SiNW FETs NOR (b) CMOS NOR

Supported by this property, SymFET-based circuit designs can effectively prevent supply voltage based fault injection. The SymFET logic can also protect the circuit from abnormal power surplus and prevent the circuit from being overheated. Figure 10 shows a typical power regulator relying on the unique properties of SymFETs. In this power regulator, SymFET M1 is the only gate directly connected to the power supply VDD, which is also the source to launch a voltage based fault injection attack. In the circuit parameter setting, V_{TG} is set to 1 V and V_{BG} is set to -1 V for all three SymFETs. 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 input current I_{IN}. The output current I_{OUT} is basically a current source for the circuit under protection. In CMOS technology, the increase of the voltage supply VDD will cause an increase in the output current. However, for SymFET designs, the peak drain current only exists for a narrow range of V_{DS}. If V_{DS} is out of this range, either higher or lower than the pre-defined range, the SymFET will be cut off quickly. In terms of the different settings of top-gate and back-gate voltages, the related V_{DS} range can be changed (see Figure 2).

The simulation results of the SymFET power regulator are listed in Table IV proving that only if the VDD is provided close to 1 V, the output current will be at its peak

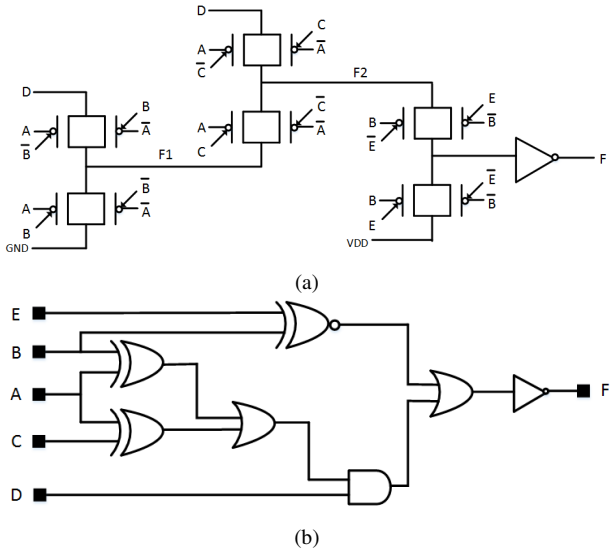

Figure 8: Original functionality of a SiNW FET complex gate (a) transistor schematic (b) gate schematic

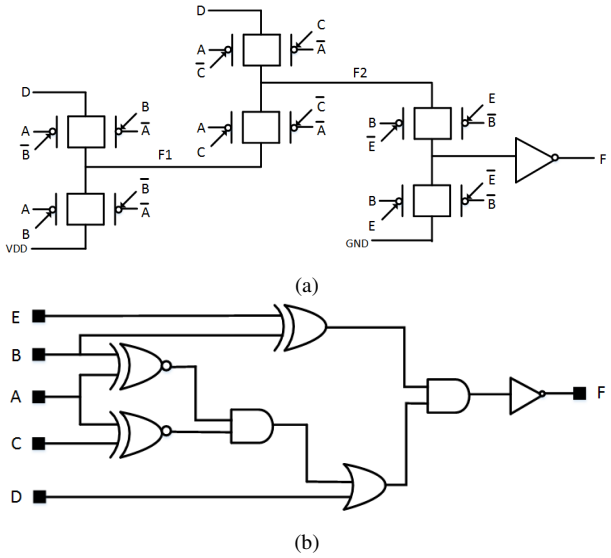

Figure 9: Reconfigured functionality of a SiNW FET complex gate (a) transistor schematic (b) gate schematic

value of 4.2 uA. For any changes to the power supply, the output current will decrease significantly so that the main circuit will be cut off. This feature is very useful in circuit protection countering side-channel attacks and fault injections. For example, cryptographic circuits are often vulnerable to power supply-based fault attack [32]. However, the insertion of the developed power regulator can effectively prevent this attack. When the attackers try to lower the supply voltage to trigger single-bit error of the encryption algorithms, before any single-bit error can occur, the whole circuit is already shut down by the SymFET-based regulator.

This power supply regulator can also help protect the circuit

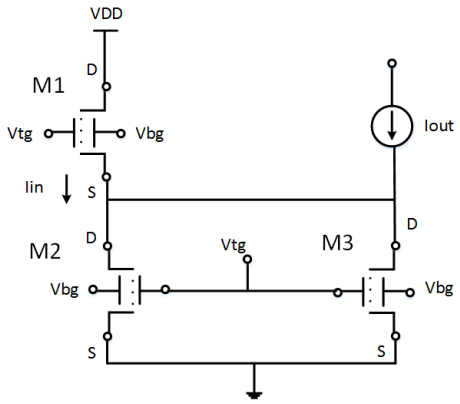

Figure 10: SymFET current regulator for circuit protection

from power surplus. As shown in the Table IV, if the power supply is much larger than 1 V, different from CMOS logic, the supply current will be cut off so that the circuit's lifecycle will be prolonged under extreme working environment.

IV. 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, etc. 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 paper, we presented examples on how the unique features of emerging technologies can help 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 are proved to be efficient in hardware security applications. These preliminary results lead us towards a new metric for the comparison between CMOS logic and emerging technologies, which will include not only traditional metrics such as power, delay, etc., but also features facilitating specific applications, e.g., security. Only through the new metrics, can we fully evaluate the impact of emerging technologies for future circuit designs.

V. Conclusion

Emerging technologies were investigated in this paper 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 including SiNW FETs and graphene SymFETs. Three different security applications were designed and verified: camouflaging gates, polymorphic gates, and power regulators. Through these 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 evaluate the merits of emerging devices.

Table IV: Output current changes with the sweeping of voltage supply

VDD(V)	0	0.2	0.4	0.6	0.8	1.0	1.2	1.4	1.6	1.8	2.0
Iout(uA)	0	0.033	0.016	0.064	0.028	4.16	0.032	0.055	0.043	0.079	0.076

ACKNOWLEDGEMENTS

Niemier and 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.

REFERENCES

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

[2] Yier Jin, Bo Yang, and Yiorgos Makris, "Cycle-accurate information assurance by proof-carrying based signal sensitivity tracing," in *IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, 2013, pp. 99–106.

[3] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, and B. Sunar, "Trojan detection using IC fingerprinting," in *IEEE Symposium on Security and Privacy*, 2007, pp. 296–310.

[4] Y. Jin and Y. Makris, "Hardware Trojan detection using path delay fingerprint," in *IEEE International Workshop on Hardware-Oriented Security and Trust*, 2008, pp. 51–57.

[5] M. Potkonjak, A. Nahapetian, M. Nelson, and T. Massey, "Hardware Trojan horse detection using gate-level characterization," in *DAC '09: Proceedings of the 46th Annual Design Automation Conference*, 2009, pp. 688–693.

[6] Y. Jin and Daniela Oliveira, "Extended abstract: Trustworthy soc architecture with on-demand security policies and hw-sw cooperation," in *5th Workshop on SoCs, Heterogeneous Architectures and Workloads (SHAW-5)*, 2014.

[7] "International technology roadmap for semiconductors," 2013 EDITION. EMERGING RESEARCH DEVICES.

[8] M. De Marchi, D. Sacchetto, S. Frache, J. Zhang, P. Gaillardon, Y. Leblebici, and G. De Micheli, "Polarity control in double-gate, gate-all-around vertically stacked silicon nanowire fets," in *Electron Devices Meeting (IEDM), 2012 IEEE International*, Dec 2012, pp. 8.4.1–8.4.4.

[9] B. Sedighi, J. Nahas, M. Niemier, and Xiaobo Sharon Hu, "Boolean circuit design using emerging tunneling devices," *Proceedings of IEEE Conference on Computer Design (ICCD)*, p. to appear, 2014.

[10] K. S. Ma, H. C. Liu, Y. Xiao, Y. Zheng, X. Q. Li, S. K. Gupta, Y. Xie, and V. Narayanan, "Independently-controlled-gate finfet 6t sram cell design for leakage current reduction and enhanced read access speed," *Very-large-scale integration(VLSI), 2014 IEEE International Symposium on*, July 2014.

[11] B. Sedighi, X. S. Hu, J. J. Nahas, and M. Niemier, "Non-traditional computation using beyond-cmos tunneling devices," *Emerging & Selected Topics in Circuits and Systems, Journal on*, vol. 12, no. 12, 2012.

[12] Sheng Lin, Yong-Bin Kim, and Fabrizio Lombardi, "Cntfet-based design of ternary logic gates and arithmetic circuits," *Nanotechnology, IEEE Transactions on*, vol. 10, no. 2, pp. 217–225, March 2011.

[13] Pei Zhao, R.M. Feenstra, Gong Gu, and D. Jena, "Symfet: A proposed symmetric graphene tunneling field-effect transistor," *Electron Devices, IEEE Transactions on*, vol. 60, no. 3, pp. 951–957, March 2013.

[14] K. Roy, M. Sharad, D. L. Fan, and K. Yogendra, "Computing with spin-transfer-torque devices: Prospects and perspectives," *Very-large-scale integration(VLSI), 2014 IEEE International Symposium on*, July 2014.

[15] A. Colli, S. Pisana, A. Fasoli, J. Robertson, and A. C. Ferrari, "Electronic transport in ambipolar silicon nanowires," *physica status solidi (b)*, vol. 244, no. 11, pp. 4161–4164, 2007.

[16] R. Martel, V. Derycke, C. Lavoie, J. Appenzeller, K. K. Chan, J. Tersoff, and Ph. Avouris, "Ambipolar electrical transport in semiconducting single-wall carbon nanotubes," *Phys. Rev. Lett.*, vol. 87, 2001.

[17] A. K. Geim and K. S. Novoselov, "The rise of graphene," *Nature Materials*, vol. 6, pp. 183–191, 2007.

[18] Yu-Ming Lin, J. Appenzeller, J. Knoch, and P. Avouris, "High-performance carbon nanotube field-effect transistor with tunable polarities," *Nanotechnology, IEEE Transactions on*, vol. 4, no. 5, pp. 481–489, 2005.

[19] Naoki Harada, Katsunori Yagi, Shintaro Sato, and Naoki Yokoyama, "A polarity-controllable graphene inverter," *Applied Physics Letters*, vol. 96, no. 1, 2010.

[20] J. Appenzeller, J. Knoch, E. Tutuc, M. Reuter, and S. Guha, "Dual-gate silicon nanowire transistors with nickel silicide contacts," in *Electron Devices Meeting, 2006. IEDM '06. International*, 2006, pp. 1–4.

[21] André Heinzig, Stefan Slesazeck, Franz Kreupl, Thomas Mikolajick, and Walter M. Weber, "Reconfigurable silicon nanowire transistors," *Nano Letters*, vol. 12, no. 1, pp. 119–124, 2012.

[22] P.-E. Gaillardon, S. Bobba, M. De Marchi, D. Sacchetto, and G. De Micheli, "Nanowire systems: Technology and design," *Philosophical Transactions of the Royal Society of London A*, vol. 372, no. 2012, 2014.

[23] Alan C. Seabaugh and Qin Zhang, "Low-voltage tunnel transistors for beyond cmos logic," *Proceedings of the IEEE*, vol. 98, no. 12, pp. 2095–2110, Dec 2010.

[24] Pei Zhao, R.M. Feenstra, Gong Gu, and D. Jena, "Symfet: A proposed symmetric graphene tunneling field-effect transistor," *Electron Devices, IEEE Transactions on*, vol. 60, no. 3, pp. 951–957, March 2013.

[25] 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, "Resonant tunnelling and negative differential conductance in graphene transistors," *Nat Commun*, vol. 4, pp. 1794, 04 2013.

[26] B. Sedighi, Xiaobo Sharon Hu, J. Nahas, and M. Niemier, "Nontraditional computation using beyond-cmos tunneling devices," *Journal of Emerging and Selected Topics in Circuits and Systems*, p. to appear, 2014.

[27] Lap-Wai Chow, James Baukus, and William Clark, "Integrated circuits protected against reverse engineering and method for fabricating the same using an apparent metal contact line terminating on field oxide," 2002.

[28] P. Ronald, P. James, and J. Bryan, "building block for a secure cmos logic cell library," 2012.

[29] Lap Wai Chow, James P. Baukus, Bryan J. Wang, and Ronald P. Cocchi, "Camouflaging a standard cell based integrated circuit," 2012.

[30] Jeyavijayan Rajendran, Michael Sam, Ozgur Sinanoglu, and Ramesh Karri, "Security analysis of integrated circuit camouflaging," in *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, 2013, CCS '13, pp. 709–720.

[31] Shashikanth Bobba, Michele De Marchi, Yusuf Leblebici, and Giovanni De Micheli, "Physical synthesis onto a sea-of-tiles with double-gate silicon nanowire transistors," in *Proceedings of the 49th Annual Design Automation Conference*, 2012, DAC '12, pp. 42–47.

[32] A Barenghi, G.M. Bertoni, L. Breveglieri, M. Pellicioli, and G. Pelosi, "Fault attack on aes with single-bit induced faults," in *Information Assurance and Security (IAS), 2010 Sixth International Conference on*, 2010, pp. 167–172.