Enhancing Hardware Security with Emerging Transistor Technologies

Yu Bi
University of Central Florida
Electrical and Computer Engineering Department
Orlando, FL 32816, USA
yubi@knights.ucf.edu

X. Sharon Hu
University of Notre Dame
Computer Science and Engineering
Notre Dame, IN, 46530 USA
shu@nd.edu

Yier Jin
University of Central Florida
Electrical and Computer Engineering Department
Orlando, FL 32816, USA
yier.jin@eecs.ucf.edu

Michael Niemier
University of Notre Dame
Computer Science and Engineering
Notre Dame, IN, 46530 USA
mniemier@nd.edu

Kaveh Shamsi
University of Central Florida
Electrical and Computer Engineering Department
Orlando, FL 32816, USA
kaveh@knights.ucf.edu

Xunzhao Yin
University of Notre Dame
Computer Science and Engineering
Notre Dame, IN, 46530 USA
xyin1@nd.edu

ABSTRACT

We consider how the I-V characteristics of emerging transistors (particularly those sponsored by STARnet) might be employed to enhance hardware security. An emphasis of this work is to move beyond hardware implementations of physically unclonable functions (PUFs) and random number generators (RNGs). We highlight how new devices (i) may enable more sophisticated logic obfuscation for IP protection, (ii) could help to prevent fault injection attacks, (iii) prevent differential power analysis in lightweight cryptographic systems, etc.

CCS Concepts

•Security and privacy → Hardware-based security protocols; •Hardware → *Emerging architectures;*

Keywords

Hardware security, emerging transistors, tunnel transistor, TFET, SymFET, NCFET, IC camouflaging, polymorphic logic

1. INTRODUCTION

Like performance, power, and reliability, security is becoming a critical design consideration. As a representative example, hardware security threats in the integrated circuit (IC) supply chain, including hardware counterfeiting, IP piracy, and reverse engineering cost the US economy more than $200 billion annually [17]. Problems are further exacerbated by the rapid growth in the "Internet of Things" (IoT). This paper will highlight how *emerging transistor technologies* can enhance existing hardware security primitives, and also lead to new hardware security primitives.

More specifically, we highlight how emerging transistor technologies could impact encryption engines. We consider not only how new devices could lead to more sophisticated and robust encryption ciphers in resource constrained environments, but also how new devices may make said ciphers more resilient to attacks such as differential power analysis (DPA). We also include a discussion of how unique I-V characteristics offered by beyond CMOS transistors can enable new hardware security primitives that could facilitate IC supply chain protection, help prevent/stop side-channel attacks, etc.

Presently, most emerging technologies being studied in the context of hardware security are related to designing physically unclonable functions (PUFs) and random number generators (RNGs) [30]. However, most PUF and RNG designs leverage larger device-to-device variations in emerging technologies. Ironically, said variations often represent shortcomings when viewed through the lens of an original device target – i.e., reliable digital logic or memory. In contrast, we will discuss emerging transistor technologies for hardware security related applications that are not RNGs or PUFs, and do not inherently rely on device variations as a means to an end.

2. BACKGROUND

Here, we review hardware security needs and challenges, and the transistor technologies that form the basis of our work.

2.1 Hardware security needs and challenges

To reduce design costs and increase profits, IC manufacturers are continuing to outsource low-profit services (e.g., manufacturing) to offshore facilities. While such outsourcing may reduce total cost, it has exacerbated security concerns. Below, we review ways that emerging technologies may help to alleviate the following threats: **(1) Hardware fingerprinting and authentication** can protect hardware intellectual property (IP) cores against reverse engineering [10]. PUFs have frequently been suggested for the authentication process [33]. However, modeling methods have been devel-

GLSVLSI '16, May 18-20, 2016, Boston, MA, USA

DOI: http://dx.doi.org/10.1145/2902961.2903041

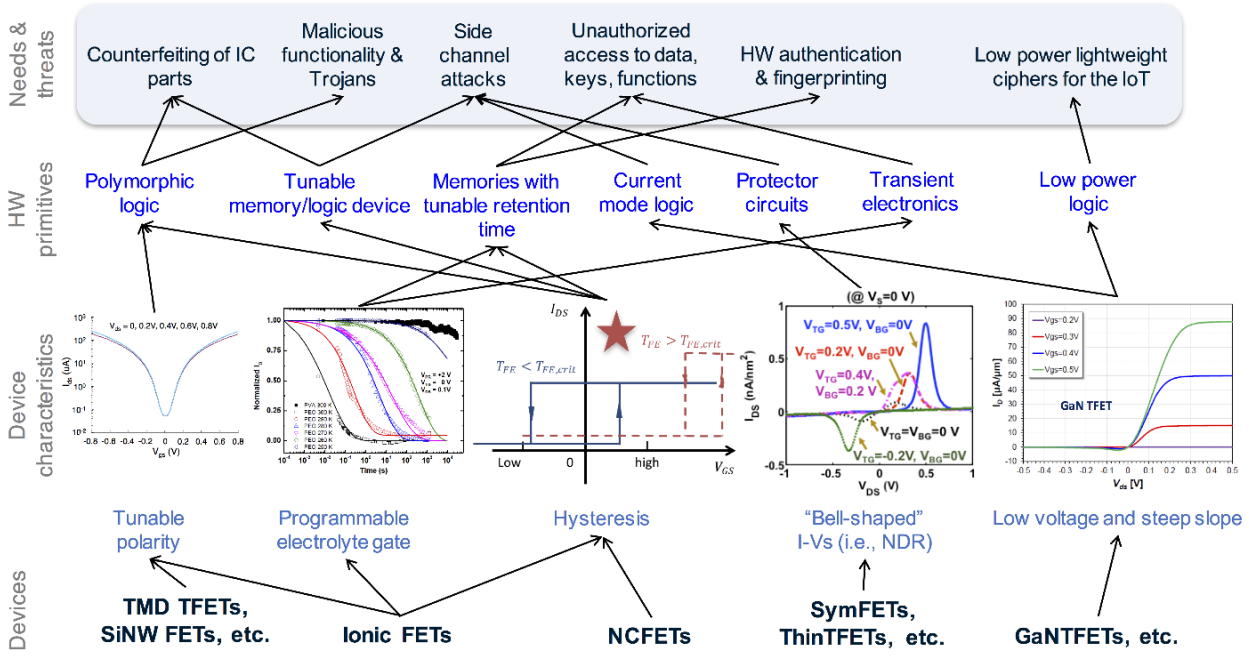

Figure 1: Mapping unique I-V characteristics of emerging transistor technologies to security needs/threats. We particularly note **(a)** the I-V characteristics of a SymFET device for different top, back gate voltage combinations and **(b)** Tunable hysteresis in an NCFET.

oped to predict the PUF responses, which adversely affects this approach [35]. **(2) Camouflaging** [11] relies on layout-level obfuscation that makes it difficult to decipher a circuit's structure via reverse engineering [32]. That said, CMOS camouflaging gates often bring significant performance overhead, area increases, etc – e.g., a XOR+NAND+NOR camouflaging gate has 5.1X-5.5X higher power, 1.1X-1.6X higher delay, and 4X higher area compared to a conventional NAND or NOR gate [32]. Moreover, [27] has suggested that SAT-based techniques could be employed to determine circuit functionality within minutes. **(3) Counterfeit ICs** have recently found their way into safety-critical and military applications [36]. Solutions for detecting counterfeit products are limited. PUFs, aging sensors, etc. [36], often incur high power and area costs. We are also concerned with **(4) side-channel analysis and fault injection attacks** where adversaries can recover internal signals leveraging static/differential analyses on side channels such as timing, power consumption, and electromagnetic emissions – all without any physical intrusion. Again, most countermeasures incur a high performance overhead [7].

2.2 Device characteristics of interest

In Fig. 1 we illustrate how post-CMOS devices could address hardware security needs. **(i)** Security needs/threats are summarized at the top-level, **(ii)** the next level captures what hardware primitives might be employed to address said concerns/needs, **(iii)** the third level illustrates what device I-V characteristics may lead to efficient implementations of said primitives, while **(iv)** the bottom-level indicates what device concepts may lead to desired I-V characteristics. A given device may ultimately address multiple security needs/threats.

New transistor technologies may also offer other "added value." For example, as will be discussed, improved sub-threshold swings can lead to lower power circuits, which could lead to implementations of current mode logic (CML) in resource constrained environments to protect against differential power analysis (DPA). Due to space limitations, in this paper we particularly focus on device technologies that exhibit tunable polarity, hysteresis, and steep slopes.

2.2.1 *Tunable Polarity*

In many nanoscale FETs, the superposition of n-type and p-type carriers is observable under normal bias conditions. The resulting ambipolarity exists in various materials [12], [25], [18]. By controlling ambipolarity, device polarity can be adjusted/tuned post-deployment. Transistors based on carbon nanotubes [22], graphene [19], silicon nanowires (SiNWs) [20], and transition metal dichalcogenides (TMDs) [13] all have configurable polarity.

As representative examples, with SiNW FETs, operation is enabled by the regulation of Schottky barriers at the source/drain junctions. A control gate (CG) turns a device on and off via a gate voltage (i.e., as would be done in a typical MOSFET). A polarity gate (PG) in proximity to the source/drain (S/D) Schottky junctions can then be used to switch device polarity between n- and p-type post-fabrication. Logic gates can still be readily cascaded as input and output voltage levels are compatible [14].

Ambipolarity is also possible with TFETs as different doping types for drain and source are used (i.e., if an n/i/p doping profile is employed [37]). A TFET can function either as an n- or p-type device by properly biasing the n-doped and p-doped regions (as well as the gate). With this approach, no polarity gate is needed in this case.

2.2.2 *Tunable Hysteresis*

The phrase tunable hysteresis implies that (i) a device's I-V curve may contain a hysteresis loop, and (ii) a device's

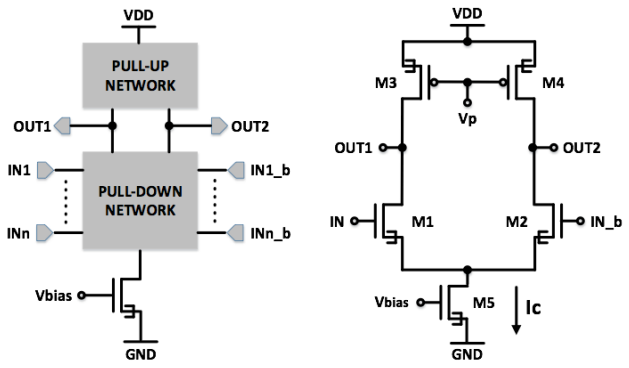

Figure 2: (a) The universal diagram of CML circuits (b) Schematic of the TFET-based CML inverter.

hysteresis loop can be moved to different locations along the applied voltage levels, or be made to disappear altogether. In this work, the negative capacitance FET (NCFET) will be considered as a test bench (see starred plot in Fig. 1). To fabricate an NCFET, a ferroelectric (FE) material is added to the gate stack of a MOSFET. The high polarizability of the FE material provides a nonlinear capacitance which becomes negative under certain electric field values. This in turn enables step-up voltage conversion of the applied gate bias to the surface potential leading to switching slope (SS) steeper than 60 mV/decade. By varying the gate stack material composition, NCFETs can be made with or without hysteretic behavior. One can also fabricate an NCFET that has hysteresis or does not have hysteresis by changing the thickness of the FE material.

2.2.3 *Bell-Shaped I-Vs*

Emerging transistor technologies may also exhibit bell-shaped I-V curves [6, 28, 21]. While useful hardware security primitives may be enabled by such a characteristic (see [3, 4] for further detail), this approach is not considered further in this paper as relative to the other approaches to be discussed, devices are not as mature.

3. TFET CURRENT MODE LOGIC

Current mode logic is a differential digital logic family [38, 7]. A CML gate is essentially comprised of (i) a tail current source, (ii) a current steering core, and (iii) a differential load. The constant current is switched through the differential network of input transistors, and the reduced voltage swing on the two load devices serves as the output. Of particular interest is the fact that the power consumption of a CML circuit is stable, which can serve as a valuable countermeasure when considering a DPA attack [1, 2, 7].

A schematic of a "generic" TFET-based CML circuit – that includes a pull-up network and a pull-down network – is illustrated in Fig. 2a. In more detail, we consider a TFET-based current mode inverter/buffer circuit (Fig. 2b) as a representative example. As first discussed in [5], IN and IN_b are differential inputs.

A constant drive current is provided by transistor M5, which is also tunable by the gate bias voltage V_{bias}. Together with M5, transistors M3 and M4 can be used to charge and discharge the output pair OUT1 and OUT2. If

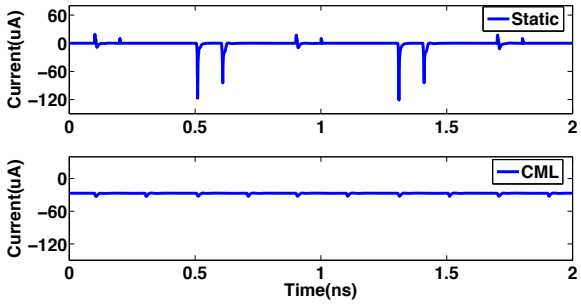

Figure 3: The current traces between static XOR and CML XOR.

IN is logic 1, (i) M1 is turned on, (ii) the constant current I_C flows through the left-handed path, (iii) OUT1 discharges to a value between VDD and GND, and (iv) OUT2 charges to quasi-VDD. (Again, logic 0 is commonly defined as half VDD, and logic 1 is close to VDD.) If OUT1 is extracted as the output pin and the inverted OUT2 is extracted as complementary output pin, the circuit performs a logical inversion. (Alternatively, the structure can serve as a buffer if pin assignments are switched.)

Turning to hardware security, with static CMOS, differential power analysis is based on the power consumption during circuit transition. Power is consumed when a output undergoes a 0→1 (or 1→0) transition. Because of this symbolic characteristic of static logic, a cryptographic algorithm is vulnerable to DPA attack. Alternatively, a CML circuit is naturally resilient to a DPA attack considering the relatively constant power consumption for almost any transitions.

As an example from our prior work [5], we consider the power traces for TFET-based static XOR gates, and the TFET-based differential style XOR gates (see Fig. 3). The TFET CML XOR gate dissipates almost constant power (in contrast to the significant power overshoot of the static XOR gate). Put another way, the TFET static XOR gate leaks information that an attacker may use to identify the internal activity of a cryptographic system, while the CML gate provides little to no information about logical state transitions. When translated to the application-level, a study in [5] suggests that TFET-based current mode logic (CML) can both improve DPA resilience and preserve low power consumption in lightweight cryptographic ciphers (KATAN32). Compared to the CMOS-based CML designs, the TFET CML circuit consumes 80% less power while achieving a similar level of DPA resistance [5].

4. HARDWARE SECURITY VIA TUNABLE POLARITY

The ability to dynamically change the polarity of a transistor opens the door to defining the functionality of a layout or a netlist post fabrication. While field programmable gate arrays (FPGAs) might also be employed, we believe that the above approach offers a path to ASIC-like performance. We briefly review SiNW FET and TFET-based primitives [3, 4] that could be used to enable IP protection, help to prevent IP piracy, and to counter hardware Trojan attacks.

4.1 Polymorphic logic gates

Polymorphic logic circuits (the terms "logic locking" [34,

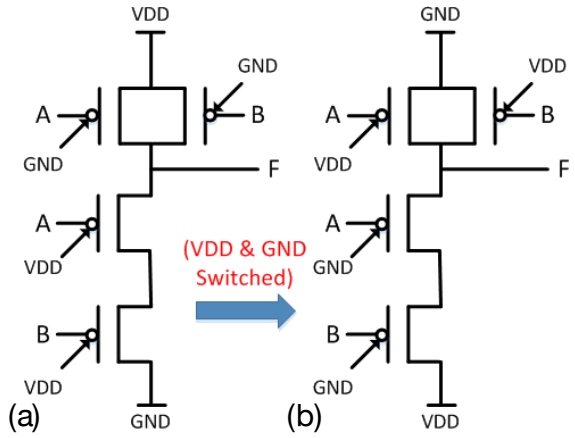

Figure 4: **(a)** SiNW-based NAND [3]; **(b)** SiNW-based NOR [3]

31, 15] or "logic encryption" might also be used) could encrypt logic functionality such that even if an entire netlist were available, an adversary would still not be able to easily decipher a chip's true functionality. With CMOS technology, such circuits have been notoriously difficult to implement efficiently.

To help prevent IP piracy, in [3, 4], we introduced SiNW FET based polymorphic gates. If the control gate (CG) of a SiNW FET is connected to a normal input, while the polarity gate (PG) is treated as the polymorphic control input, we can easily change the circuit functionality (without a performance penalty). For example, per Fig. 4a and Fig. 4b, a SiNW FET based NAND gate can be converted to a NOR gate. However, a CMOS-based NAND cannot be converted to a fully functioning NOR by switching power and ground.

We have recently designed TFET-based polymorphic logic circuits as well [9]. Fig. 5a and Fig. 5b show a 2-input polymorphic NAND/NOR gate. By properly biasing the gate, the n-doped region, and the p-doped region, a TFET device can function either as an n-type or p-type transistor. The circuit behaves like a NAND gate if the n-doped region of the two parallel TFETs is connected to V_{DD}, and the p-doped region of the bottom TFET is connected to *GND*. With opposite connections, the circuit functions as a NOR gate. By using two MUXes (one at the top and the other at the bottom) to select between the two types of connections, the circuit then functions as a polymorphic gate where the control to the MUXes forms a 1-bit key. Simulation results [9] indicate that the circuit functions as intended.

Using low-cost polymorphic logic gates based on SiNW FETs or TFETs, we can design functional modules that only perform a desired computation if properly configured – e.g., if one were to design an ASIC's datapath using said modules, it would only function correctly if a "key" (configuration bits) were supplied. Thus, IP cloning and IP piracy could be prevented with extremely low performance overhead.

4.2 Camouflaging Layout

IC camouflaging is used to secure the CMOS fabrication process. However, with CMOS camouflaging layouts, significant increases to both power and area (in order to achieve useful levels of protection [32]), and adverse effects such

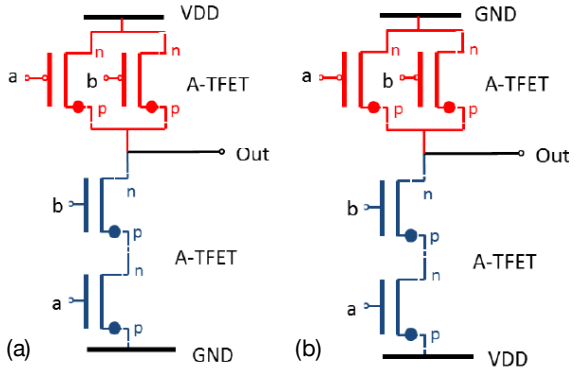

Figure 5: TFET polymorphic **(a)** NAND/ **(b)** NOR gate and simulation result [9]

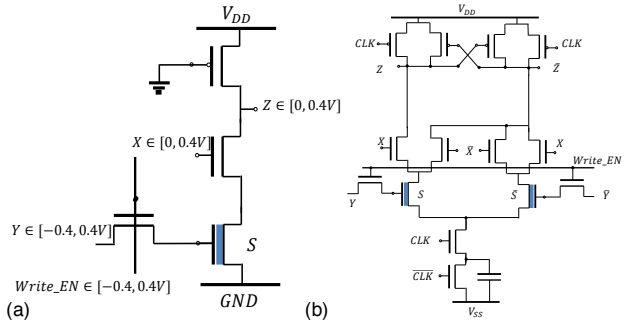

Figure 6: **(a)** NAND-LiM based on pseudo-NMOS logic; **(b)** AND/NAND-LiM based on DyCML.

as decreased circuit reliability are typically incurred. More quantitatively, a CMOS camouflaging layout that can function either as an XOR, NAND or NOR gate requires at least 12 transistors. In our recent work [3, 4], we have shown that by leveraging tunable polarity, just 4 SiNW FETs are required to build a camouflaging layout that can perform NAND, NOR, XOR and XNOR operations.

5. HARDWARE SECURITY LEVERAGING ATYPICAL SWITCHING BEHAVIORS

Post-CMOS devices with tunable hysteresis could enable a device to be dynamically configured as either a switch or a non-volatile storage element. An immediate consequence of such a device is the potential to design simpler and more power efficient logic-in-memory (LiM) cells. From the perspective of security, this could reduce communication between a CPU and memory, which in turn could make a circuit less vulnerable to memory-based attacks during communication [16]. LiM cells can also help to reduce overhead incurred by key access and verification via storing the keys in LiM cells.

We have recently designed several different LiM cells using NCFETs. Fig. 6a shows an example of a LiM cell (performing a NAND function) based on the pseudo-NMOS logic style. The circuit has two modes – update mode and hold mode. In the update mode (i.e., `Write_EN`= 1), the `Y` input is written into the NCFET, and the output realizes the logic function of `Z`= $\overline{\texttt{X} \cdot \texttt{Y}}$. In the hold mode (i.e., `Write_EN`= 0), the circuit outputs `Z`= $\overline{\texttt{X} \cdot \texttt{S}}$, where `S` is the bit value stored in the NCFET which remains unchanged. The pseudo-

NMOS design may lead to relatively large leakage, but similar CMOS-like designs can also be obtained. Fig. 6b shows an AND/NAND-LiM cell design based on the dynamic current mode (DyCML) style. Similar to the circuit in Fig. 6a, this circuit also has an update and hold mode. In the hold mode (i.e., `Write_EN`= 0), the circuit outputs `Z`= $\overline{\texttt{X} \cdot \texttt{S}}$ and $\overline{\texttt{Z}}$ = `X`·`S` where `S` is the bit value stored in the NCFET. In the update mode (i.e., `Write_EN`= 1), `Y` and $\overline{\texttt{Y}}$ are written into the two NCFETs, respectively, while output does the same evaluation as in the hold mode.

Our preliminary work in exploiting atypical switching behaviors for hardware security reveals exciting opportunities that certain post-CMOS devices can provide to enhance Design for Assurance (DFA). As suggested in [9], devices with tunable hysteresis offer several unique functionalities that are difficult to obtain from MOSFETs. For example, a device can be readily changed from being a non-volatile storage element to a switch. This property could help achieve logic obfuscation. Also, the retention time of such a device as a non-volatile storage element can also be tuned which may be exploited for tamper resistant circuitry.

To exploit the capability of NCFETs being either a storage element or a switch, we will investigate NCFET-based efficient design obfuscation on both combinational logic and sequential logic. In [8, 29, 23], the authors have proposed techniques that use finite state machines (FSMs) together with some combinational logic to help obfuscate an IP design. Thus, one possible approach is to employ NCFETs to implement such FSMs. For example, if we leverage the design concepts of the LiM cells discussed above to construct a FSM, the FSM behavior can be tuned, hence providing another level of obfuscation. The mode control (between being a storage element or a switch) then becomes the encryption key. To ensure that this approach is effective, a thorough study is required to address challenges that include: (i) developing more area and power efficient NCFET based FSMs, and (ii) determining how the placements of these NCFETs impact security levels and other traditional metrics such as power and delay.

The other security need that this work could address is resisting denial-of-service (DoS) attacks and differential power analysis (DPA). DoS attacks can be deployed on energy constrained systems. Sleep deprivation attacks [26] and multilevel authentication methods [24] have been proposed to counter such attacks. LiM cells, if used both to store the security key and for authentication, could provide an extremely energy efficient authentication process through close integration of memory and logic. Also, as noted earlier, DyCML has been widely studied for countering DPA based side channel attacks (e.g., [38, 7]). The DyCML based NCFET LiM cells introduced in our recent work not only achieves balanced power traces but also can be readily integrated with memory components. In future work, we will evaluate these LiM based security primitives in terms of their ability to satisfy the identified security needs as well as energy and performance.

6. CONCLUSIONS

In closing, we have discussed some of our initial work to leverage the unique I-V characteristics of emerging transistor technologies to help enhance/improve hardware security. We emphasize that it is of the utmost importance that any such design space exploration work be done in close conjunction with scientists and engineers working to develop new devices – i.e., to ensure that (i) any circuit design efforts, etc. reflect the true capabilities of the device (e.g,. with respect to reproducible behavior) and (ii) useful and reproducible I-V characteristics (for the purposes of hardware security) are not "optimized away" as a device evolves.

Acknowledgement: This work was supported in part by the Center for Low Energy Systems Technology (LEAST), an SRC STARnet center sponsored by MARCO and DARPA.

7. REFERENCES

[1] K. Baddam and M. Zwolinski. Evaluation of dynamic voltage and frequency scaling as a differential power analysis countermeasure. In *VLSI Design, 2007. Held jointly with 6th International Conference on Embedded Systems., 20th International Conference on*, pages 854–862, Jan 2007.

[2] S. Badel, E. Guleyupoglu, O. Inac, A. Martinez, P. Vietti, F. Gurkaynak, and Y. Leblebici. A generic standard cell design methodology for differential circuit styles. In *Design, Automation and Test in Europe, 2008. DATE '08*, pages 843–848, March 2008.

[3] Y. Bi, P.-E. Gaillardon, X. Hu, M. Niemier, J.-S. Yuan, and Y. Jin. Leveraging emerging technology for hardware security - case study on silicon nanowire fets and graphene symfets. In *Asia Test Symposium (ATS)*, pages 342–347, 2014.

[4] Y. Bi, K. Shamsi, J.-S. Yuan, P.-E. Gaillardon, G. De Micheli, X. Yin, X. Hu, M. Niemier, and Y. Jin. Emerging technology based design of primitives for hardware security. *ACM Journal on Emerging Technologies in Computing Systems (JETC)*. (to appear).

[5] Y. Bi, K. Shamsi, Y.-S. Yuan, Y. Jin, M. Niemier, and X. S. Hu. Tunnel fet current mode logic for dpa-resilient circuit designs. *IEEE Transactions on Smart Grid*, page under review, 2016.

[6] 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. *Nature Communications*, 4(1794):1–5, 2013.

[7] A. Cevrero, F. Regazzoni, M. Schwander, S. Badel, P. Ienne, and Y. Leblebici. Power-gated mos current mode logic (pg-mcml): A power aware dpa-resistant standard cell library. In *Proc. of the 48th Design Automation Conference*, DAC '11, pages 1014–1019, 2011.

[8] R. Chakraborty and S. Bhunia. Harpoon: An obfuscation-based soc design methodology for hardware protection. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 28(10):1493–1502, Oct 2009.

[9] A. Chen, X. S. Hu, Y. Jin, M. Niemier, and X. Yin. How emerging devices can address hardware security needs and challenges. In *Design, Automation and Test in Europe, 2016. DATE '16*, page to appear, 2016.

[10] Chipworks. Chipworks: Patent and technology partner, Accessed November 17, 2015. http://www.chipworks.com/.

[11] L.-W. Chow, J. Baukus, and W. Clark. Integrated circuits protected against reverse engineering and method for fabricating the same using an apparent metal contact line terminating on field oxide, 2002.

[12] A. Colli, S. Pisana, A. Fasoli, J. Robertson, and A. C. Ferrari. Electronic transport in ambipolar silicon nanowires. *physica status solidi (b)*, 244(11):4161–4164, 2007.

[13] S. Das and J. Appenzeller. Wse2 field effect transistors with enhanced ambipolar characteristics. *Applied physics letters*, 103(10):103501, 2013.

[14] 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*, pages 8.4.1–8.4.4, Dec 2012.

[15] S. Dupuis, P. S. Ba, G. D. Natale, M. L. Flottes, and B. Rouzeyre. A novel hardware logic encryption technique for thwarting illegal overproduction and hardware trojans. In *On-Line Testing Symposium (IOLTS), 2014 IEEE 20th International*, pages 49–54, July 2014.

[16] D. G. Elliott, M. Stumm, W. M. Snelgrove, C. Cojocaru, and R. McKenzie. Computational ram: Implementing processors in memory. *Design & Test of Computers, IEEE*, 16(1):32–41, 1999.

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

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

[19] N. Harada, K. Yagi, S. Sato, and N. Yokoyama. A polarity-controllable graphene inverter. *Applied Physics Letters*, 96(1), 2010.

[20] A. Heinzig, S. Slesazeck, F. Kreupl, T. Mikolajick, and W. M. Weber. Reconfigurable silicon nanowire transistors. *Nano Letters*, 12(1):119–124, 2012.

[21] M. Li, D. Esseni, J. Nahas, D. Jena, and H. Xing. Two-dimensional heterojunction interlayer tunneling field effect transistors (thin-tfets). *Electron Devices Society, IEEE Journal of the*, 3(3):200–207, May 2015.

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

[23] B. Liu and B. Wang. Embedded reconfigurable logic for asic design obfuscation against supply chain attacks. In *Design, Automation and Test in Europe Conference and Exhibition*, pages 1–6, 2014.

[24] D. Liu and P. Ning. Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks. In *The Network and Distributed System Security Symposium*, 2003.

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

[26] T. Martin, M. Hsiao, D. Ha, and J. Krishnaswami. Denial-of-service attacks on battery-powered mobile computers. In *Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications*, pages 309–318. IEEE, 2004.

[27] M. E. Massad, S. Garg, and M. V. Tripunitara. Integrated circuit (ic) decamouflaging: Reverse engineering camouflaged ics within minutes. In *Network and Distributed System Security Symposium (NDSS)*, 2015.

[28] A. Mishchenko, J. Tu, Y. Cao, R. Gorbachev, J. Wallbank, M. Greenaway, V. Morozov, S. Morozov, M. Zhu, S. Wong, F. Withers, C. Woods, Y.-J. Kim, K. Watanabe, T. Taniguchi, E. Vdovin, O. Makarovsky, T. Fromhold, V. Fal'ko, A. Geim, L. Eaves, and K. Novoselov. Twist-controlled resonant tunnelling in graphene/boron nitride/graphene heterostructures. *Nature Nanotechnology*, 9(10):808–13, 2014.

[29] S. Narasimhan, R. Chakraborty, and S. Bhunia. Hardware ip protection during evaluation using embedded sequential trojan. *Design Test, IEEE*, PP(99):1–1, 2013.

[30] J. Rajendran, R. Karri, J. Wendt, M. Potkonjak, N. McDonald, G. Rose, and B. Wysocki. Nano meets security: Exploring nanoelectronic devices for security applications. *Proceedings of the IEEE*, 103(5):829–849, May 2015.

[31] J. Rajendran, Y. Pino, O. Sinanoglu, and R. Karri. Security analysis of logic obfuscation. In *Design Automation Conference (DAC), 2012 49th ACM/EDAC/IEEE*, pages 83–89, June 2012.

[32] J. Rajendran, M. Sam, O. Sinanoglu, and R. Karri. Security analysis of integrated circuit camouflaging. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, CCS '13, pages 709–720, 2013.

[33] M. Rostami, M. Majzoobi, F. Koushanfar, D. Wallach, and S. Devadas. Robust and reverse-engineering resilient puf authentication and key-exchange by substring matching. *Emerging Topics in Computing, IEEE Transactions on*, 2(1):37–49, March 2014.

[34] J. A. Roy, F. Koushanfar, and I. L. Markov. Epic: Ending piracy of integrated circuits. In *Design, Automation and Test in Europe, 2008. DATE '08*, pages 1069–1074, March 2008.

[35] U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, and J. Schmidhuber. Modeling attacks on physical unclonable functions. In *Proceedings of the 17th ACM Conference on Computer and Communications Security*, CCS '10, pages 237–249, 2010.

[36] M. M. Tehranipoor, U. Guin, and D. Forte. *Counterfeit Integrated Circuits: Detection and Avoidance*. Springer, 2015.

[37] T. Vasen. Investigation of III-V tunneling field-effect transistors. In *A Dissertation submitted to the University of Notre Dame*, 2014.

[38] M. Yamashina and H. Yamada. Mos current mode logic mcml circuit for low-power ghz processors. *NEC Res. Develop.*, 36:54 – 63, Jan 1995.