Harnessing Nanoscale Device Properties for Hardware Security

(Invited Paper)

Bicky Shakya, Fahim Rahman, Mark Tehranipoor, Domenic Forte
Department of Electrical and Computer Engineering, University of Florida
Email: {bshakya, fahim034}@ufl.edu, {tehranipoor, dforte}@ece.ufl.edu

***Abstract*—Traditional measures for hardware security have heavily relied on currently prevalent CMOS technology. However, with the emergence of new vulnerabilities, attacks and limitations in current solutions, researchers are now looking into exploiting emerging nanoelectronic devices for security applications. In this paper, we discuss three emerging nanoelectronic technologies, namely phase change memory, graphene and carbon nanotubes, to point out some unique features they offer and analyze how these features can aid in hardware security. In addition, we present challenges and future research directions for effectively integrating emerging nanoscale devices into hardware security.**

1. Introduction

Hardware security has become an increasing concern in today's world, where security through software and protocols alone has become insufficient. The past decade has yielded many novel primitives such as physical unclonable functions (PUFs) and true random number generators (TRNGs) for fingerprint and cryptographic key generation, as well as solutions aimed at emerging threats such as integrated circuit (IC) counterfeiting and tampering, to ensure security in a system. Existing security strategies heavily rely on pre-existing CMOS technology that is slowly saturating in development. Further, with new vulnerabilities constantly emerging and longstanding attacks becoming more practical, primitives/countermeasures based on current CMOS technology seem inadequate.

Recently, nanoscale devices and technologies such as phase-change memory (PCM), memristors, graphene and carbon nano-tubes (CNTs) have emerged, with promising improvements in area, speed and power over their CMOS-counterparts. Such devices also show interesting security properties that are largely uninvestigated, especially by the experts in device physics and materials. Research from such groups have mostly focused on device performance and reliability since they are less educated on the nuances of security. The hardware security community has recently adapted some new devices to develop security primitives such as PUFs and TRNGs, but evaluation has been largely restricted to crude simulations. In addition, other equally important security issues such as anti-tampering, counterfeiting detection/avoidance, side-channel attacks, reverse engineering, etc. have hardly been considered. To truly capture and evaluate the properties of emerging devices for security, there is a significant need for multi-disciplinary research which incorporates both device and circuit/system-level security groups. In this perspective paper, we attempt to provide a roadmap for them by discussing important security issues and requirements, and linking emerging devices to them. Since there is already some prior work investigating such links for memristors [1], we have focused on PCM and carbon-based structures (graphene and CNT) in this paper.

This paper is organized as follows. In Section 2, we provide an introduction to PCM, graphene and CNTs, along with some unique features that these devices possess. In Section 3, we discuss security primitives, attacks and countermeasures, and how each can be addressed with emerging nano-devices and their unique features. We also point out the withstanding challenges that need to be overcome to use these nano-devices for security applications. Lastly, in Section 4, we highlight some open questions and future research directions in the emerging field of nanoscale security.

2. Emerging Nanoscale Devices

2.1. Phase Change Memory (PCM)

PCM is an emerging nanoscale device that enables non-volatile storage with high density and fast read/write operations. PCM is primarily based on chalogenide materials such as $Ge_2Sb_2Te_5$ (GST) and their transition to-and-from an amorphous (high resistance) phase and a crystalline (low resistance) phase with a difference in resistance on the order of $10^2 - 10^4$ between the two phases (or states) [2]. For 'resetting' a PCM cell, a high-current pulse is applied over a short duration to melt the GST by localized heating. It is then cooled rapidly, forming an amorphous plug that creates a high resistance between the electrodes of the PCM cell. For the 'set' operation, a moderate current pulse with a longer duration is applied to melt the GST, which is then cooled down slowly for crystallization. A voltage small enough not to disturb the phase is then applied to read the state of the cell, where the amorphous state is considered as logic '0' and the crystalline state is considered a logic '1'. While the set/reset mechanisms and materials remain roughly the same, a PCM cell can be designed in a variety of geometries, e.g. mushroom cell structures (Fig. 1), μ-trench, line cell, and so on, with each geometry exhibiting different current requirements, scalability and thermal properties [2].

We now identify a few features that are inherent in, and in some cases, exclusive to PCM devices.

- **Programming Variability:** PCM cells show stochastic programming variability. For example, given two PCM cells, a reset operation on them with the same reset pulse yields two close but different resistance values, where exact resistance is defined stochastically by the geometrical and thermal properties of the specific cell [13].
- **Resistance Drift:** Resistance drift is a phenomenon whereby an amorphized PCM cell may have an increase or 'drift' in resistance over time [3], and eventually change to crystalline phase with a drastic decrease in resistance (Fig. 2). While this may be considered a problematic issue for data retention, it may be useful for security.
- **Random Telegraph Noise:** PCM has recently shown to display random telegraph noise (RTN) (Fig. 3) [4]. RTN occurs in PCM devices as short-term resistance fluctuations, whose power spectral density varies with parameters such as cell contact area, temperature and applied voltage.
- **MultiBit Storage Per Cell and Variability:** PCM is also capable of multi-level cell (MLC) operation, where the resistance window between the amorphous and crystalline states is used to store multiple bits in a single PCM cell.

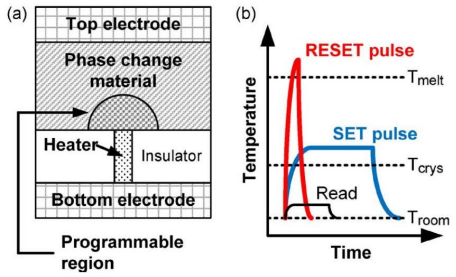

Figure 1: (a) PCM 'Mushroom' cell, (b) Program/Read pulses [2].

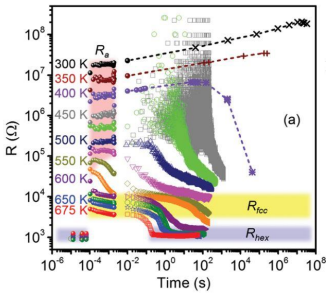

Figure 2: Resistance drift in amorphized PCM cells at various temp [3].

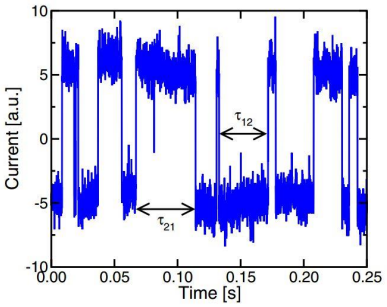

Figure 3: RTN in a PCM cell at room temp [4].

- **Initial Forming Step:** PCMs sometimes require an initial 'forming step'. The resistance of a newly manufactured PCM cell in amorphous phase is much higher than the usual amorphous resistance of a reset PCM cell. Thus, in order to 'form the device', a higher initial programming pulse is required. Note, however, that most PCM devices today are optimized with regard to the interface between the heater area and the chalcogenide material, thereby removing the necessity to 'form' a device [5].

2.2. Graphene and Carbon Nanotube Electronics

Graphene and carbon nanotube (CNT)-based electronics have emerged as promising alternatives to conventional CMOS technologies to maintain the trend set by Moore's law in the nanoscale regime. They also offer a platform to potentially integrate digital logic with nonlogic components such as analog circuitry and sensors [6]. The main advantages for graphene and CNTs arise from their unique physical structures and associated energy-band properties. Ideally, a sheet of carbon atoms sp^2- bonded in a honeycomb lattice forms a large-area graphene, and a CNT can be visualized as a seamless cylinder formed by rolling up graphene. Such structures create interesting energy-band structures, and hence electronic states, that govern the fundamental and unique properties inherent to graphene and CNTs. Studies show that a finely patterned narrow graphene sheet (graphene nanoribbon - GNR) can have similar features like that of CNTs [7]. We note some of the unique features of graphene and CNT below:

- **Bandgap Energy:** Quantization of the electronic states in large area graphene results into quantized wavevectors or subbands passing through the corner points of the Brillouin zone (i.e. *K-points* in reciprocal space), showing semi-metallic properties with no energy bandgap (E_g). Selective patterning of GNR can increase E_g to offer semiconducting behavior. In addition, CNTs have quantized wavevectors in circumferential direction, with subbands having their own sets of 1D dispersion relations. Thus based on the orientation (chirality) of carbon atoms in the lattice, the generated subbands for a CNT may or may not pass through the *K-points*, making it metallic or semiconducting, respectively (Fig. 4) [8].
- **Variability:** Different transistor architectures have been proposed using GNR and CNTs as channel materials (Fig. 5) to design high mobility transistors [6], [7]. Since the property of these GFETs and CNTFETs largely depend on the channel-GNR and CNT properties (e.g., semiconducting or metallic, etc.), length and patterning, drain/source-contact, CNT numbers and placements, and numerous other factors, the inherent sources of variability are quite large and heavily dependent on manufacturing processes.

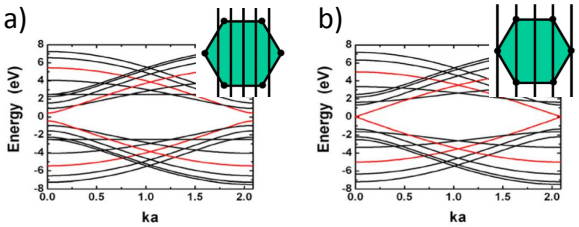

Figure 4: An illustration of bandstructures for (a) semiconducting and (b) metallic CNTs. Allowed wavevector lines are shown in respective insets [8].

- **Channel Sensitivity:** The channel material in GFETs and CNTFETs is highly sensitive to external excitation causing unwanted variations in transistor performance for conventional logic operation. Such excitations may arise from mobility variation due to operating conditions (such as exerted electric field and temperature), channel contamination, physical deformation in channel nanotubes, by photons, and other phenomena. Hence, the issue of controlling channel quality has received much attention. However, researchers have also leveraged this high sensitivity for many nanoscale sensor applications since these effects can easily be translated to digital data for sensing.
- **Flexibility and Printability:** Solution processable graphene sheets can be used for bulk scale printing, for example using ink-jet printers, on both hard and flexible substrates to create transparent and functional electronic circuits that can potentially work as processing blocks with proper active interface. Fig. 6 depicts a simple structure of a single transistor constructed using printable graphene via ink-jet printing [9]. Here graphene works as the channel material and can offer similar functionality as that of a conventional CMOS transistor.

It should be noted that the major difficulty regarding graphene and CNT electronics is integrating them to conventional CMOS platform with high processing yield. However, with the help of state of the art technology in nanoscale regime, for example with a focused ion beam (FIB) system that can operate in sub-10 nm region [10], it is much easier now to have such a circuitry or sensor architecture put in place for selective and critical applications.

3. Securing Hardware using Nanoscale Devices

3.1. Building Hardware Security Primitives

3.1.1. Physical Unclonable Functions (PUFs). PUFs are identically designed architectures that produce non-deterministic keys/signatures using inherent physical variations resulting from the manufacturing process in elements such as transistors, interconnects, etc. Since PUFs (e.g. an arbiter PUF in Fig. 7) can generate responses on the fly, they offer a volatile, less-expensive, and tamper-resistant

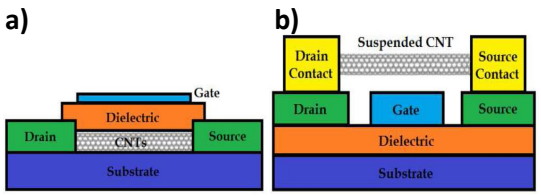

Figure 5: (a) Top-gated CNTFETs, (b) Suspended-channel CNTFETs [7].

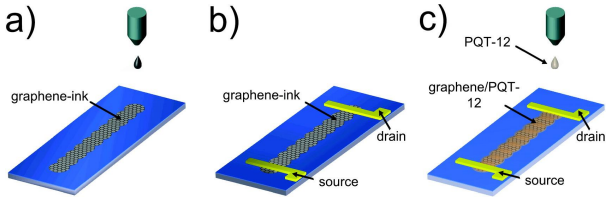

Figure 6: Printable Graphene Electronics: (a) Ink on Si/SiO_2 to define channel, (b) Cr-Au pads define the source and drain contacts, (c) A layer of PQT-12 is printed on top to define gate [9].

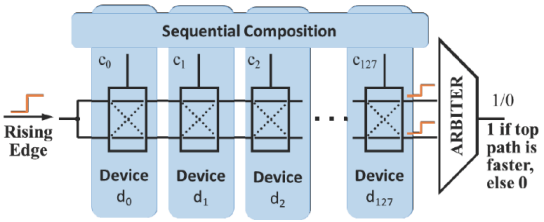

Figure 7: A delay-based 128-stage arbiter-PUF.

alternative to conventional approaches that rely on storing keys in non-volatile memory [11].

Despite promising advantages, current PUFs suffer from several quality issues, most notably, reliability degradation due to temporal variations. Ideally a PUF should generate the same signature over time and different environmental conditions, i.e. maintain 100% reliability, to avoid any error in cryptographic operations. Unfortunately, *environmental variations*, i.e. power supply noise and temperature variations, have adverse, though temporary, effect on CMOS-transistor performance by impacting threshold voltage (V_{th}), mobility (μ) and other critical parameters, making the PUF less robust [12]. In addition, *Aging* creates permanent degradation to the critical parameters due to *Bias Temperature Instability* (BTI), *Hot Carrier Injection* (HCI), *Time Dependent Dielectric Breakdown* (TDDB), and *Electromigration* (EM). To improve PUF reliability, researchers have proposed powerful error correcting codes (ECC), and other novel architectures and algorithms. However they often result in high area and power overhead, and may pose other vulnerabilities. Approaches that take advantage of inherent device properties and optimize them for higher quality PUFs are still being sought.

PCM and PUFs: Zhang et. al [13] have used the programming variability of PCM cells to generate keys. In this approach, two PCM cells from a memory array are invoked by a challenge C, and a key is produced by a simple resistance comparison. For example, if $R(PCM_{ref}) < R(PCM_{sel}) \rightarrow 0, else \rightarrow 1$. Another advantage of this scheme is that the generated response also depends on the specific programming pulse used, as the current-magnitude of the pulse changes the amorphous resistance of the PCM cell [14]. Thus, a different programming pulse can potentially yield another fresh set of challenge-response pairs (CRPs). They also demonstrate their concept with $180nm$ PCM chips. However, this approach requires significant post-processing in order to produce unbiased responses (i.e., equally likely outcomes of '0' and '1'). Kursawe et. al [15] have suggested the use of MLC-PCM cells in making reconfigurable PUFs, in which one can write into a certain resistance interval of the PCM cell and read out where exactly the resistance value lies in the interval . Here, the exact position in the interval is dictated by process variations and thus, it can vary, even for the same write operation. However, no demonstration was provided.

Like silicon PUFs, the biggest challenge for PCM-based PUFs is *reliability*. To date, PCM-PUFs have only been as reliable as their CMOS counterparts, if not less. Since crystallization and amorphization are thermally activated processes [2], the impact of temperature (along with the associated resistance drift) and environmental variations on PCM-PUFs is of significant concern. In addition, the relatively high amorphization temperature produced during programming a PCM cell can cause neighboring PCM cells to be disturbed [16]. This is made worse by the fact that thermal disturbance changes over time, hence the generated signature may change over time as well. Although countermeasures for both resistance drift and thermal disturbance have been proposed [16], [17], these solutions need to be considered in the scope of security primitives, not conventional memory applications, where the constraints for area/power overhead might be very different. Further, helper data algorithms and ECCs need to be analyzed for PCM-PUF implementations, as the area advantage provided by high-density PCM may be countered by the high area overhead of the post-processing required.

Lastly, we also mention the longstanding issues and opportunities with PCM as a traditional non-volatile memory (NVM) for key storage. NVMs are still widespread in smart cards, embedded systems and other applications for cryptographic key storage. Traditional NVMs such as flash have an array of vulnerabilities to data remanence attacks and imaging attacks. These vulnerabilities are yet to be assessed with PCM. Intuitively, we could point out a few advantages of having PCM as the NVM for security. For example, PCM based memory will be inherently immune to electromagnetic emission-based attacks for key extraction (since amorphization/crystallization are purely thermal processes). Also, they could be more immune to data remanence attacks, compared to SRAM, as the set/reset operation changes the physical characteristics of the PCM cell, leaving behind little to no evidence of the previous state of the cell. However, to date, no experimental analysis of such features of PCM have been analyzed for security applications.

Graphene/CNT and PUFs: In addition to showing non-trivial properties, graphene and CNT-based FETs are prone to higher process variations, making them intriguing candidates for building PUFs. As discussed in Section 2.2, the inherent random variations present in a GFET/CNTFET can degrade the performance in terms of conventional logic application; however, those can be greatly exploited to generate PUF-based signatures. Konigsmark et al. [18] proposed a carbon nanotube based PUF (namely CNPUF, see Fig. 8) relying on the fact that the lack of chirality control in the manufacturing process yields metallic CNTs over semiconducting CNTs in a non-deterministic way. Utilizing the characteristic variation between semiconducting and metallic properties of CNTs can lead to distinguishable, but random states since the off-current for semiconducting CNTs is considerably lower than that of metallic CNTs. Simulated

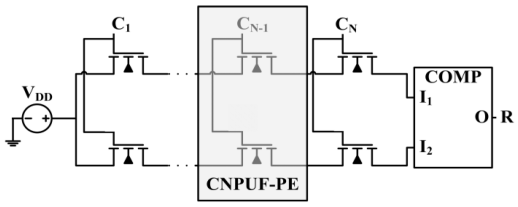

Figure 8: CNPUF proposed in [18]. Characteristics of CNPUF parallel element varies due to process variation.

results of CNPUF show reduced area and power footprint, and higher robustness against environmental variations with respect to selected CMOS-PUFs. However, major barriers to evaluate graphene and CNT-based PUF architectures have to be overcome since we lack proper and reliable models that incorporate such stochastic natures as well as predict the impact of environmental variations and aging. CNT-based PUFs may also suffer from degraded performance and lower reliability due to poor-quality channel formation and contamination. Furthermore, mass-production of such architectures still lacks technological maturity, and integration scheme with CMOS platform still needs thorough investigations.

3.1.2. True Random Number Generators (TRNGs). TRNG is a primitive used in a wide variety of security applications - most notably, generation of nonces, LFSR seeds, and cryptographic keys. A TRNG consists of an entropy source, entropy extraction/sampling unit and in most cases, a cryptographic conditioning unit. The entropy source is the focal point of a TRNG. As opposed to pseudo-random number generators, a TRNG relies on electrical and/or thermal processes that are inherently random to serve as its entropy source. The sources may include RTN found in scaled transistors, power supply noise, radioactive decay, latch metastability, jitter in ring oscillators and so on. The analog entropy source is then sampled using the entropy extraction/sampling unit. This could be in the form of a latch sampling a ring oscillator signal or a voltage comparator producing a digital output from comparison of a RTN-prone signal to a reference voltage. The most notable problem with entropy sources is that, although they may seem to be 'intuitively random', statistical tests run on the output (e.g., NIST Test Suite, DieHARD, etc.) may show a certain level of bias and predictability, especially under environmental and process variations. To combat this, cryptographic hash functions, von Neumann corrector, and stream ciphers are employed to the TRNG outputs to achieve more uniformity and statistical randomness, albeit at the cost of throughput and area. However, harvesting entropy and generating unbiased random numbers by making better use of inherent device properties could lower these costs considerably.

PCM/CNT and TRNGs: Regarding PCM, several entropy sources embedded within the device structure and functionality might help with random number generation. Firstly, PCM displays RTN (Fig. 3), as pointed out in Section 2.1. However its suitability for random number generation is yet to be assessed. In addition, the amorphous phase of a PCM cell could possess a good source of entropy. Similar to the approach in [13], a PCM cell could be repeatedly amorphized by a constant current pulse. Since amorphization is an intrinsically random phenomenon, the amorphization resistance reached by a PCM cell varies stochastically from cycle-to-cycle. Hence a resistance comparison to a nominal amorphization resistance set as a reference value could potentially generate random bits. Regarding CNTFETs, random variations that occur due to channel-tubes' chirality, placement, spacing and dimensions, as well as other physical variations can be exploited as entropy sources for TRNGs. For example, a metastable ring oscillator [19] implemented with CNTFETs may produce higher entropy due to numerous sources of variations. However, for CNTFETs as well as PCM, digital extraction of entropy from such an inherent phenomenon is challenging and may be biased by the extracting circuitry due to lack of resolution and operational limitations.

3.2. Attacks and Countermeasures

3.2.1. Design-for-Anti-Counterfeiting. Counterfeit ICs are an increasingly common problem in today's globalized semiconductor industry. There are several distinct counterfeit types: recycled, remarked, cloned, overproduced, defective or tampered, with each type posing its own challenge [20]. Overproduced and cloned chips may cause legal issues and loss of profit for legitimate chip designers. On the other hand, chips that are recycled, remarked or defective pose an even riskier threat, as they can compromise critical infrastructures (transportation, military, health, etc.). Detection mechanisms for counterfeit ICs usually involve the identification of the defects produced by counterfeiting. In the case of recycled ICs, embedded sensors can detect prior usage of ICs by measuring device aging [20]. The Supply Chain Hardware Integrity for Electronics Defense (SHIELD) program from DARPA [21] is currently developing miniature dielets that can be inserted into an IC package and then read in a contactless manner to detect cloned and remarked ICs. With nanoscale devices, there might exist opportunities to miniaturize and/or find new modes of developing counterfeit detection sensors and mechanisms for supply chain traceability.

PCM and Anti-Counterfeiting Sensors: The phenomena of resistance drift in PCM cells could be used to design passive aging-sensors for detecting how long an IC or electronic system has been in the supply chain. This is highly desirable, as a passive sensor does not need to be powered on for detecting the age of the chip/system. Prior approaches such as the sensors suggested in [20] require the IC to be turned on and used for a period of time in order to age the sensor, which limits its applicability in low-power/passive applications such as RFID tags. Note that for this passive sensor to work, PCM cells must be isolated and protected against any form of set/reset operations, as its resistance values can be reverted back. Further, the amount of time that can be detected is highly subjective to device geometry and the stochastic nature of the PCM cell. Alternatively, data retention failure can also be used to detect arbitrary durations of time. This is possible in PCM as the gradual process of seed crystal nucleation and formation of percolation paths causes a PCM cell to crystallize and fail, while the resistance continually drops with the gradual crystallization [22]. However, such a failure mechanism is too slow to be practical at room temperature (10 years at 85^oC for complete crystallization) [22]. Design optimization is needed to accelerate this behavior in a controlled way.

Graphene-based Printable Electronics and Supply Chain Security: Graphene based printable electronics exhibit high potential in hardware security applications, especially in electronic supply chain security. The main advantage of printing electronics over conventional logic circuitry is that the circuit does not need to be fabricated only in the die

in the manufacturing steps. Instead, it can be printed on the package by the authorized personnel. This means that when chips return from the untrusted foundry, the IP owner can "print" necessary circuits on the chip package - circuits that can generate digital fingerprints for identification and tracking - to ensure the security of the product in the supply chain. Such a printed circuit can potentially make a touch-and-go solution for chip authentication, and to some extent, make a counterfeit and tamper evident architecture since any polishing of package for recycled and remarked chips, or delayering, will destroy the printed circuit on the package. Major obstacles of this approach come from the low mobility of carriers in the printed channel limiting it to a low speed application, resolution of the printable architectures and power supply circuitry. Since the demonstrations of printable circuits are still limited to only a few transistor [9], a more detailed investigation is required on digital fingerprint circuitry and interface.

3.2.2. Design-for-Anti-tamper. Design-for-anti-tamper plays a crucial role in preventing secrets (cryptographic keys or other valuable data) from being stolen, IP theft, cloning, and denial of service attacks. Adversaries can carry out such attacks through probing, reverse engineering, remote attacks, etc., that may be invasive, semi-invasive or non-invasive in nature. Prevention of such attacks requires a proper understanding of the threat model as well as developing adequate protection mechanisms [23].

Attacks that involves physical tampering, such as microprobing, may be invasive or semi-invasive. Protection against them can broadly be classified into two categories [23]: (1) A *tamper-evident* security scheme that allows the authorized user to check whether a chip has gone through any physical tampering, but does not actively prevent the data or secret key from being stolen; (2) A *tamper-resistant* security scheme that has the capabilities to sense attacks and 'respond' accordingly. Sophisticated tamper-sensing mechanisms largely depend on creating power-net based active shields, and/or on mechanical and light-based sensors. Whenever an adversary tries to delayer and/or mill through the chip, perform optical imaging, etc. the active net and surrounding sensors get triggered and the sensitive data/IP is erased [24]. However, the active power net may easily be bypassed by state of the art FIB attacks, and physical sensors and optical sensors may also be fruitless since the small exerted mechanical force may not activate the sensors placed in the die and powerful tools may do imaging outside the operational bandwidth of the optical sensors.

PCM and Tamper-Detection: The formation step of PCM can be used to check if a PCM memory is 'fresh' or has been tampered with. A quick check of the amorphous resistance of new PCM cells (provided that correct resistance value is known), or a count of the number of pulses required to crystallize the cell (for example, 20 pulses being required instead of 5 if the cell is new), can help to detect any tampering attempt on new PCM cells. However, as mentioned in Section 2.1, optimized PCM devices today do not require the forming-step. Thus PCM with older heater architectures might be useful for this tamper-detection feature. In addition, self-powered light sensors, coupled with PCM as a NVM, can be used for effective tamper-resistance. As illustrated in [25], an energy-harvesting photovoltaic sensor is coupled along with a portion of the PCM memory (possibly storing secret keys) and highly reactive materials deposited as metal multi-layers (e.g. $Si + 2B, Cu + Pd$).

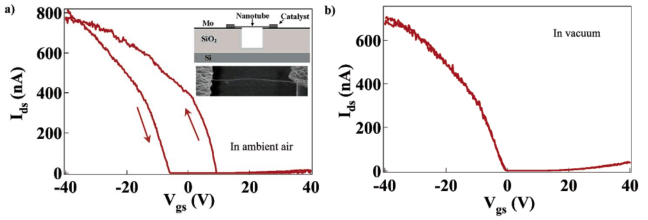

Figure 9: $I_{DS} - V_{GS}$ **curve for a CNTFET exposed to ambient (a) air, and (b) vacuum [29].**

When an invasive attack is attempted, the current pulse generated by the sensor can ignite the reactive material, causing heat generation to set/reset the PCM cell, which effectively 'destroys' its information content. Challenges regarding such tamper-resistant schemes include spatial and temporal stochastic nature of the PCM cell and integration.

Graphene/CNT and Tamper-Detection: Graphene and CNT, although currently unfit for logic applications, can be used to design a variety of sensors that can help in detecting mechanical force, light, or chemical exposure. This opens up opportunities for designing tamper detection sensors. Such sensors and actuators can be used to create a shield around the critical components (e.g. crypto-module, secure data bus, etc.) of the circuit to prevent physical tampering and eavesdropping [24]. As discussed in Section 3.2.2, a design with anti-tampering in mind can leverage sensors that captures unauthorized activities inside the chip to detect and resist physical attacks such as delayering, probing, milling and imaging. Keeping that in mind, we can utilize graphene and CNT-based mechanical, optical and chemical sensors to thwart invasive and semi-invasive attacks.

Mechanical Pressure Sensors: CNTs offer several MEMS/NEMS structures, and floating gate CNTFET structures, that work as mechanical pressure (or force) sensors. In such cases, the properties such as carrier mobility within the channel of the CNTFET, or resonant frequency of a cantilever structure, change as a result of physical deformation due to exerted physical force [26]. Such a pressure/force sensor may be used to detect physical force given on the die while delayering and polishing.

Optical Sensors: Imaging is one of the key steps in invasive/semi-invasive attacks, and hence optical/image sensors are necessary to combat such attacks. Graphene photodetectors and single wall CNT optical sensors provide high sensitivity in a broad range of optical and near infrared wavelengths [27]. As for security applications in ICs, these sensors will trigger an alert flag if light falls on them while delayering, milling or probing, and will erase any secret key or data stored in NVM. A key obstacle in preventing invasive-attacks is to generate the alert flag in passive mode (with no external power given to the chip). This may be solved by using graphene-based supercapacitors for charge storage, or other lightweight energy-harvesting mechanisms that can work as an on-chip power-source [28].

Chemical Sensors: Researchers have proposed several chemical and biochemical sensors using CNTs to provide high selectivity and sensitivity to detect chemical/biochemical materials and their amount [30]. Placement of such chemical sensors within the die can potentially detect chemical activities occurring while delayering and polishing. These sensors tend to drive different currents since the type and amount of associated chemicals change the electrical properties (e.g. conductance, carrier mobility, threshold voltage, etc) of the channel of, for example, a sus-

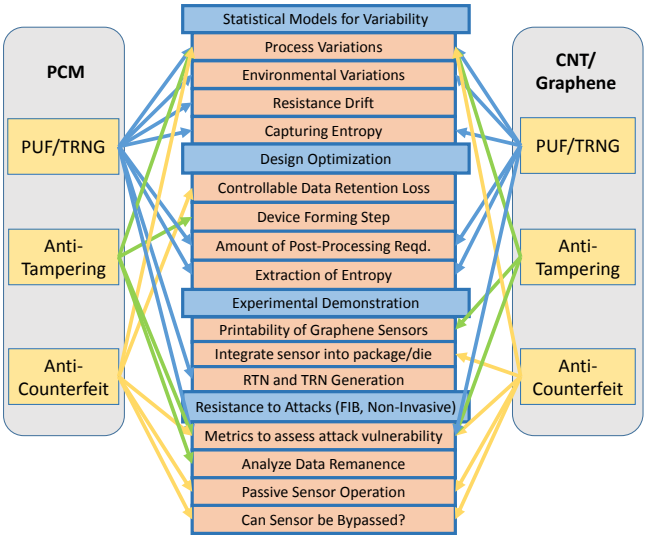

Figure 10: Security primitives, countermeasures for attacks and respective challenges.

pended channel CNTFET shown in Fig. 5. Fig. 9 shows an example of how such a CNTFET may experience changes in its electrical properties due to exposure to air and humidity, for example, while delayering [29].

It is apparent that graphene, CNTs and PCM all possess unique features that enable them to be used for designing sensors to detect/prevent attempts at physical tampering. However, challenges remain in the form of integrating these sensors onto actual IC die or packages, ensuring that their detection capabilities or responses remain robust across different environmental conditions and making sure that they are not vulnerable to attacks that can bypass them (such as FIB-based attacks).

4. Summary

So far, we have identified a plethora of features inherent in emerging nano-scale technologies that open up new opportunities for hardware security. These features enable applications ranging from printable electronics for supply chain security, new PUF/TRNG mechanisms to a variety of sensors capable of detecting different modes of tampering.

However, much of the ideas presented in this paper and others are yet to be experimentally demonstrated and integrated as part of a security-enabling system. Some of the currently withstanding challenges we have presented in this paper are summarized in Fig. 10. In order to overcome these challenges, the following aspects must be considered.

- *Evaluation:* For evaluation of devices, we would need metrics that can quantify parameters such as variability, entropy, vulnerability to tampering, etc. specifically for devices, as opposed to system/output/circuit-level metrics that are currently prevalent.
- *Modeling:* For modeling, good statistical models capturing security features of devices, such as sources of entropy, process variation, changes to parameters by tampering/environmental variations etc. are required.
- *Design and Integration:* Integration challenges, such as harvesting entropy effectively from nano-devices for TRNGs or integrating tamper-detection sensors based on graphene/CNT into IC die/package, also need further investigation.

Towards this three-fold approach, hardware security researchers could contribute to metrics, while device researchers could use those metrics to guide the design and modeling of devices; this clearly points to the need for a multi-disciplinary effort in this field.

Acknowledgments

This project was supported in part by an AFOSR MURI grant under award number FA9550-14-1-0351.

References

[1] J. Rajendran et al., "*Nano meets security: Exploring nanoelectronic devices for security applications,*" Proc. of the IEEE, May 2015.
[2] H.-S. Wong et al., "*Phase change memory,*" Proc. of the IEEE, Dec 2010.
[3] F. Dirisaglik et al., "*High speed, high temperature electrical characterization of phase change materials: metastable phases, crystallization dynamics, and resistance drift,*" RSC Nanoscale, 2015.
[4] D. Fugazza et al., "*Random telegraph signal noise in phase change memory devices,*" IEEE IRPS, May 2010.
[5] A. Pirovano et al. "*Reliability study of phase-change nonvolatile memories,*" IEEE Trans. on Device & Materials Reliability, Sept 2004.
[6] A. Chen et al., *Emerging Nanoelectronic Devices*, 2014.
[7] R. Vargas-Bernal et al., "*Carbon nanotube-and graphene based devices, circuits and sensors for VLSI Design,*" IOAP, 2012.
[8] M. Anantram et al., "*Physics of carbon nanotube electronic devices,*" Reports on Progress in Physics, vol. 69, 2006.
[9] F. Torrisi et al.,"*Inkjet-printed graphene electronics,*" ACS Nano, 2012.
[10] "*ORION NanoFab - Helium Ion Microscope (HIM).*" [Online]. Available: http://www:zeiss:com/microscopy/enn us/products/ multiple-ion-beam/orion-nanofab-for-materials:html
[11] C. Herder et al., "*Physical Unclonable Functions and Applications: A Tutorial,*" Proc. of the IEEE, 2014.
[12] M. T. Rahman et al., "*An Aging- Resistant RO-PUF for Reliable Key Generation,*" IEEE TETC, 2015.
[13] L. Zhang et al., "*Exploiting process variations and programming sensitivity of phase change memory for reconfigurable physical unclonable functions,*" IEEE TIFS, June 2014.
[14] A. Redaelli et al., "*Electronic switching effect and phase-change transition in chalcogenide materials,*" IEEE Elec. Dev. Letters, 2004.
[15] K. Kursawe et al., "*Reconfigurable physical unclonable functions - enabling technology for tamper-resistant storage,*" IEEE HOST, 2009.
[16] S. Kim et al., "*Thermal disturbance and its impact on reliability of phase-change memory studied by the micro-thermal stage,*" IEEE IRPS, May 2010.
[17] W. Zhang et al., "*Helmet: A resistance drift resilient architecture for multi-level cell phase change memory system,*" IEEE DSN, 2011.
[18] S. Konigsmark et al., "*CNPUF: A carbon nanotube-based physically unclonable function for secure low-energy hardware design,*" ASP-DAC, 2014.
[19] I. Vasyltsov et al., "Fast Digital TRNG Based on Metastable Ring Oscillator," CHES 2008.
[20] M. M. Tehranipoor et al., *Counterfeit Integrated Circuits: Detection and Avoidance*. Springer, 2015.
[21] K. Bernstein, *Supply chain hardware integrity for electronics defense (SHIELD)*. Online: http://www:darpa:mil/program/supplychain-hardware-integrity-for-electronics-defense
[22] U. Russo et al., "*Intrinsic data retention in nanoscaled phase-change memories mdash; Part I: Monte carlo model for crystallization and percolation,*" IEEE Trans. on Elec. Dev., Dec 2006.
[23] S. Skorobogatov, "*Semi-invasive attacks-a new approach to hardware security analysis,*" Technical report, University of Cambridge, Computer Laboratory, 2005.
[24] D. Shahrjerdi et al., "*Shielding and securing integrated circuits with sensors,*" IEEE ICCAD, 2014.
[25] J. O. Chu et al., "*Integrated circuit tamper detection and response,*" Oct. 14 2014, uS Patent 8,861,728.
[26] C. Hierold et al., "*Nano electromechanical sensors based on carbon nanotubes,*" Sensors and Actuators A: Physical, 2007.
[27] P. W. Barone et al.,"*Near-infrared optical sensors based on single-walled carbon nanotubes,*" Nature Materials, 2004.
[28] J. Liu et al., "*High performance all-carbon thin film supercapacitors,*" Journal of Power Sources, 2015.
[29] W. Kim et al., "*Hysteresis caused by water molecules in carbon nanotube field-effect transistors,*" Nano Letters, 2003.
[30] P. Bondavalli et al., "*Carbon nanotubes based transistors as gas sensors: State of the art and critical review,*" Sensors and Actuators B: Chemical, Jun. 2009.