The Pennsylvania State University

The Graduate School

GRAPHENE FIELD EFFECT TRANSISTORS FOR PHYSICALLY UNCLONABLE CRYPTOGRAPHIC PRIMITIVES

A Thesis in

Engineering Science and Mechanics

by

Drew Buzzell

Submitted in Partial Fulfillment
of the Requirements
for the Degree of

Master of Science

May 2019

The thesis of Drew Buzzell was reviewed and approved* by the following:

Saptarshi Das
Assistant Professor of Engineering Science and Mechanics
Thesis Advisor

Mark Horn
Professor of Engineering Science and Mechanics

Osama Awadelkarim
UNESCO Chair Professor of Engineering Science and Mechanics

Judith Todd
Professor of Engineering Science and Mechanics
Head of the Department of Engineering Science and Mechanics

*Signatures are on file in the Graduate School

ABSTRACT

Graphene-based devices and sensors are emerging rapidly over the past decade owing to its unique and fascinating electronic and optoelectronic properties [1-5]. In fact, graphene based wearable sensors and heath monitoring devices can revolutionize emerging technologies such as the Internet of Things (IoT). A critical aspect of IoT edge and end devices is their interconnectivity at a global scale [6, 7]. As such the digital information that are generated, stored or communicated by these IoT devices can becomes vulnerable to cyber-attacks, tampering, hacking, and other security threats [8, 9]. It is imperative that these devices must be made secure against any digital crimes. Here we introduce an on-chip security method for generating physically unclonable challenge response pairs (CRPs) by exploiting the inherent disorders associated with the carrier transport in grain boundary dominated graphene field effect transistors (GFETs). To demonstrate the robustness and strength of the CRP, we employed various statistical measures including hamming distance, correlation coefficient, and entropy calculations. Our results showcase that the GFET based cryptographic primitives are uncorrelated, unclonable, and astronomically difficult to decipher using brute force trials (BFTs) facilitating their use as on-chip secure key generation. Finally, we developed a method for generating a new set of CRP by reconfiguring the GFET arrays that do not involve physical replacement of the devices and/or integration of additional hardware components.

TABLE OF CONTENTS

Table of Contents

LIST OF FIGURES

ACKNOWLEDGEMENTS

I would like to thank my research advisor Dr. Saptarshi Das and graduate student Akhil Dodda.

Chapter 1
Introduction

In recent years, there have been unprecedented advances in graphene based wearable and wireless nanoelectronics, optoelectronics, plasmonics, biomedical, and sensing devices that provide low cost, energy efficient, and high-performance solutions for emerging technologies such as the Internet of Things (IoT). It is expected that the era of the IoT will revolutionize how the world interacts. By 2020, there will be 200 billion smart devices that will be constantly generating and communicating data across the globe [1]. These devices will be deployed for agriculture, healthcare, infrastructure, education, defense, as well as for the optimization of transportation of goods and people and for the optimization of industrial manufacturing and collection of real-time analytics, among various other things. This will lead to a substantial amount of data pertaining to individuals, institutions, governments, and military organizations [2-4]. With so much information, we experience the risk of theft and manipulation of the data through various cyber-terrorism and other cyber-crimes. As society becomes more reliant on information it generates, we are posed with the challenge of securing the same.

Information security is achieved in two ways: either with software, or a hardware-based approach. Software based security relies on what is known as one-way mathematical functions. Some examples include prime factorization, hashing, and discrete logarithms. These functions can easily encrypt data in polynomial time, however extensive resources and an exponential amount of time, what is termed nondeterministic

polynomial time, is necessary to decrypt the data [5]. While one way functions are robust method for data encryption [6, 7], and, under current computing limitations, can withstand successive brute force trials (BFTs), they however produce only pseudo-random numbers. As such, there exists ways to determine the input from the encrypted output. This has already been demonstrated for some one-way functions by organizations such as the National Security Agency [8].

The uncertainty of a software approach has driven industries toward a hardware based security which uses the natural disorders in an unclonable physical system to generate true random numbers [9]. A hardware security approach uses physically unclonable functions or PUFs. A PUF is a unique physical object whose disorder comes from its manufacturing and is impossible to duplicate when given access to the same tools and fabrication techniques. The basis of a PUF is its set of challenge response pairs (CRPs). A challenge is a stimulus (light, voltage, etc.) that can cause a response from the physical object that is based on its unique disorders. Some aspects of a PUF include unclonability, reliability, and reconfigurability. Unclonability means that no two PUFs generate the same CRPs. This is illustrated in Fig. 1 which shows that when the same challenge is introduced to different PUFs there should be different

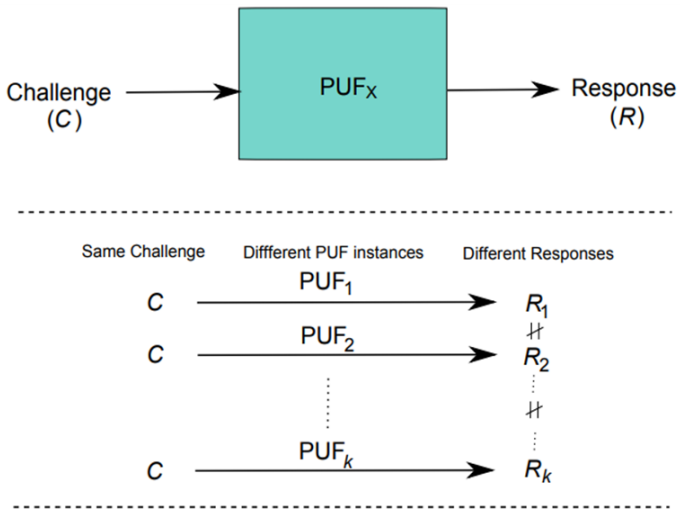

Figure 1: A black box representation of a PUF. The response is determined by the complex physical function of a PUF that is unique to each device and the challenge applied to it. Adapted from Ref. [10].

responses each based on the unique disorders of the PUF [10]. Reliability refers to the fact that the same challenge should produce the same response from a PUF each time it's introduced, regardless of variations in external factors (temperature, time, etc.). Finally, reconfigurability refers to the ability of a PUF to generate an entirely new and uncorrelated set of CRPs by changing some physical characteristic. For a PUF to be considered reconfigurable, the action which causes this physical change must be remote as physical access to the PUF is not always possible or profitable. Note that not every PUF that has been published previously has included the possibility for reconfiguration.

The first iterations of a physically unclonable function (PUF), exploited the speckle patterns generated from light diffracting off randomly dispersed nanoparticles in a transparent medium [11, 12]. This idea of harnessing physical variations was later replicated in the semiconductor industry by exploiting the fluctuations in the physical characteristics of Si complementary metal oxide semiconductor (CMOS) devices to create PUFs [13, 14]. The fabrication of CMOS technology requires multiple complex steps including lithography and doping. When creating billions of these devices, variations in their physical characteristics arise naturally leading to different delay times in the devices which can be harnessed for security applications. Several iterations of Si PUFs are already widely available. The various types can harness the system's disorders at either the device level, circuit level, or architectural level. They include static random-access memory (SRAM) and dynamic random-access memory (DRAM) based PUFs, ring oscillator PUFs, arbiter PUFs, butterfly PUFs, flip-flop PUFs, etc. [15, 16].

Although, ubiquitous, Si PUFs however suffer from low entropy as the device to device variability follows statistical distributions with relatively low standard deviations

[17]. This is expected since the semiconductor industry has invested much resources to improve the reliability of Si devices for the past five decades. Instead Si PUFs use a setup that requires many devices, complex architecture, or extensive post processing to increase the robustness and uniqueness of the PUF response. Post processing methods such as, fuzzy extraction, majority voting, and the addition of helper data [18], not only increase the complexity of Si PUFs, but also add to the area overhead and cost. Further, these techniques introduce vulnerabilities into the system that can be exploited by non-invasive side-channel attacks [19]. Furthermore, Si PUFs are inadequate for IoT applications due to their power hungry nature and difficulties in scaling their complex architecture [20], as well as their incompatibility with flexible and printable substrates [21, 22]. This sets the stage for a new set of security primitives that can be used for IoT devices while maintaining a high level of security.

It is already expected that nanotechnology will play a large part in the era of IoT. As such we look to novel properties of nanotechnology to create conceptually new security primitives with the potential to be more robust and tamper-proof than current Si PUFs [10]. Graphene technology has experienced many advancements due to the attention it has received from the electronics community for applications such as nanoelectronics, optoelectronics, and sensing applications, to name a few [23-27]. Graphene devices are expected to provide low cost, low power, and high-performance solutions to IoT devices. Therefore, we look to graphene for establishing a robust, reliable, high entropy, low power, area efficient, reconfigurable, and non-volatile on-chip security for graphene devices. We accomplish this by harnessing the inherent disorders

associated with the carrier transport in multi domain graphene field effect transistors (GFETs).

Chapter 2
Fabricating GFET PUFs

Here, we introduce an on-chip physical unclonable security primitive for graphene devices which harnesses the variations in the carrier transport of disordered, multi-domain graphene field effect transistors (GFETs). Where, typically, graphene electronic and optoelectronic devices rely on large-area, high-quality, single-domain graphene to achieve high carrier mobilities and ballistic transport, we instead embrace the diffusive transport across graphene grain boundaries, as a source of natural disorders in our system as well as easing out the stringent growth requirements which ultimately provide cost benefits[28-30].

We found that during our previous study of graphene heterostructures for photodetection applications, our GFETs demonstrated significant device to device variation in their transfer characteristics. Witnessing this, we leveraged these variations to generate cryptographic primitives. These primitives, our CRP, were tested using standard security metrics to confirm the randomness, unclonability, and stability [13]. Furthermore, we demonstrate the ability to reconfigure our GFETs to generate entirely new and uncorrelated CRP, without the physical replacement of the devices and/or the integration of additional hardware components, a unique feature unparalleled by any state-of-the-art hardware-based security systems.

FET Fabrication

Graphene used here was purchased on Cu foil from the external manufacturer Graphenea. The graphene was grown using chemical vapor deposition (CVD) and, as with most large area growth, the graphene produced is polycrystalline. Graphenea reports their grain size as being "up to 20 μm". The graphene on the Cu foil was pre-spun with a PMMA protective layer, as shown in Fig. 2a. The graphene was transferred from the foil onto a 50nm alumina (Al_2O_3) substrate with a stack of Pt/TiN/p^{++}Si as the back contact. This substrate was initially designed for other 2D material FETs. Use of the high-k dielectric Al_2O_3 gives us an effective oxide thickness of 20nm. The Pt/TiN/p^{++}Si contact is needed to tailor the work function. Together they bring the threshold voltage or Dirac point to lower voltages. The use of the Al_2O_3 substrate for the GFETs was first adopted to lower the operating voltage of the GFET photodetectors compared to those fabricated on a 300nm SiO_2 substrate. Their continued use for the PUF devices was kept for consistency purposes.

To transfer from the Cu foil to the Al_2O_3, the thin PMMA film was used as a sacrificial transport layer. The PMMA/graphene/Cu stack was placed in metal etchant (iron (III) chloride) to release the PMMA/graphene, as in Fig 2b. Ten minutes after the Cu was no longer visible, the PMMA/graphene stack was transferred to three consecutive DI water baths, for ten minutes each, before finally transferring it to the Al_2O_3 substrate (Fig. 2c). Next, a two part process was used to fabricate the device. The first part involved isolating the device channel from the rest of the CVD film. This ensured that the device contacts would not short. The channel was patterned using electron beam

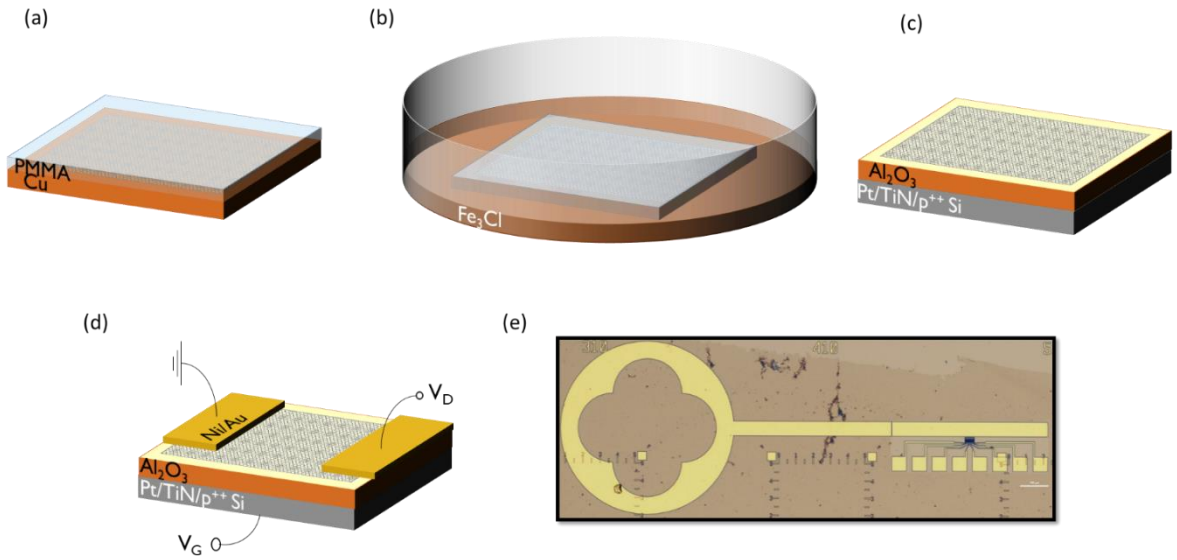

Figure 2: ***Fabrication of Graphene Field Effect Transistors (GFETs) Cryptographic Primitives.*** *a) The graphene bought is CVD grown on a copper foil, and comes with a PMMA layer pre-spun to be used as the sacrificial layer for transferring. b) The Cu/Graphene/PMMA stack is placed in copper etchant solution (Fe_3Cl), separating the metal from the foil. The Graphene/PMMA stack is rinsed in water baths before being c) transferred to the substrate of choice. d) Using electron beam lithography, the source and drain for the device is patterned, and then the Ni/Au contacts are deposited using electron beam evaporation. e) Optical image of the final device with a key like attachment.*

lithography where a 120nm PMMA A3 resist was utilized. After exposure, the resist was developed in a 1:1 MIBK:IPA solution for 1 minute followed by an IPA bath for 45 seconds. A 15 second RF O_2 plasma etch was used to etch away the exposed graphene, leaving only the device channel. The etch was carried out with a 95 sccm flow of O_2 and 8 sccm flow of Ar and a power setpoint was 75W.

The next part was the fabrication of the source and drain contacts. Again, e-beam lithography was used to pattern the contacts. A resist stack of 150nm MMA EL6 and 120nm PMMA A3 was used. Once the exposed sample was developed, with the same process as before, the bottom EL6 layer created an undercut profile for a lift-off process for the contacts. Through electron beam evaporation, 40nm of Ni and 30nm of Au were deposited to be used as the contact metal. After completing a lift-off process the device resembles the structure shown in Fig 2d. An optical image of the final PUF structure is

shown in Fig 2e. The device shown in this image is an array of 8 GFETs which share a source contact. This structure was chosen for ease of measuring.

Demonstrating Randomness

This process of transferring from one substrate to the next introduces dopants, metal contaminants [31], and wrinkles [32] which are defects, along with the grain boundaries, that act to alter the electronic properties of the graphene through intervalley and coulomb scattering, and other mechanisms [33, 34]. Fig. 3 shows the electrical characteristics of a representative GFET device with a channel length of L=1µm and width W= 1µm. The transfer characteristics are shown in Fig. 3a where the drain voltage is stepped from 200mV to 1V in steps of 200mV. The mobility, Fig. 3b, of the device is found with the transconductance, where the device hole and electron mobility are taken as the right and left peak, respectively. Fig. 3c shows the output characteristics of the GFET. We can describe these current characteristics using the following phenomenological expression:

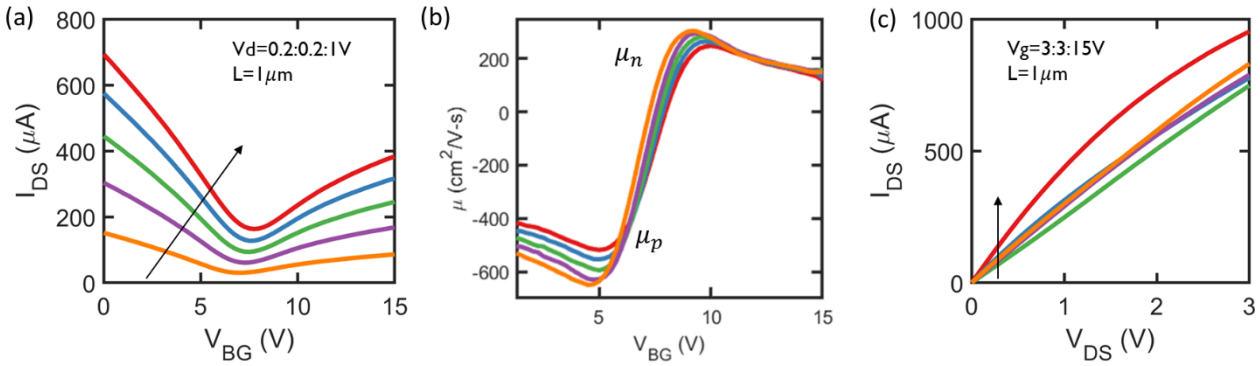

Figure 3: ***Electrical Characteristics of Graphene Field Effect Transistors (GFETs).*** *a) Standard transfer characteristics of a 1µm channel length (L) GFET normalized by width. Drain voltage was stepped from 200mV to 1V in steps of 200mV. b) The hole and electron mobility was plotted from the transconductance of the transfer curves and taken as the peak for a given drain voltage. c) Output characteristics of a GFET with a the gate voltage stepped from 3V to 15V in steps of 3V.*

$$[1] \qquad I = \mu \frac{W}{L} \sqrt{(qn_0)^2 + [qC_{ox}(V_G - V_{Dirac})]^2}\, V_D$$

where, q is the charge of an electron, μ is the carrier mobility, n_0 is the residual number of carriers in graphene due to the presence of charge puddles in the oxide, C_{ox} is the oxide capacitance, V_{Dirac} is the Dirac voltage which corresponds to gate voltage where the current is minimum.

Ideally, the location of V_{Dirac} should occur at $V_G = 0$, however in our devices a ptype doping shifts V_{Dirac} to ~7-8V, depending on the drain voltage, as observed in Fig. 3a. Mechanisms such as substrate induced doping and charge transfer at metal/graphene contact interfaces are typically attributed to the shifted Dirac point [35, 36]. Furthermore, the mobility values extracted for our CVD graphene FETs are at least an order of magnitude smaller than what has been reported in the past for FETs based on exfoliated single crystal graphene flakes, demonstrating that the carrier transport in our GFETs are defect limited [37]. Since the orientation, size and location of the grains are random, as well as the locations of other defects [38-40], we expect that characteristics of all GFETs made with this quality of material will demonstrate significant variations among themselves.

Fig. 4a shows the transfer characteristics of one of the GFETs tested. Fig. 4b demonstrates the inherent randomness in the graphene by showing the transfer characteristics of 198 GFETs. Further, Fig. 4c show the distribution (histogram) of I_{Dirac}, i.e. the current at the devices Dirac voltage. Clearly, there exists significant device to device variation within the GFET population. These fluctuations in the device characteristics are direct consequences of the variability in the intrinsic device parameters

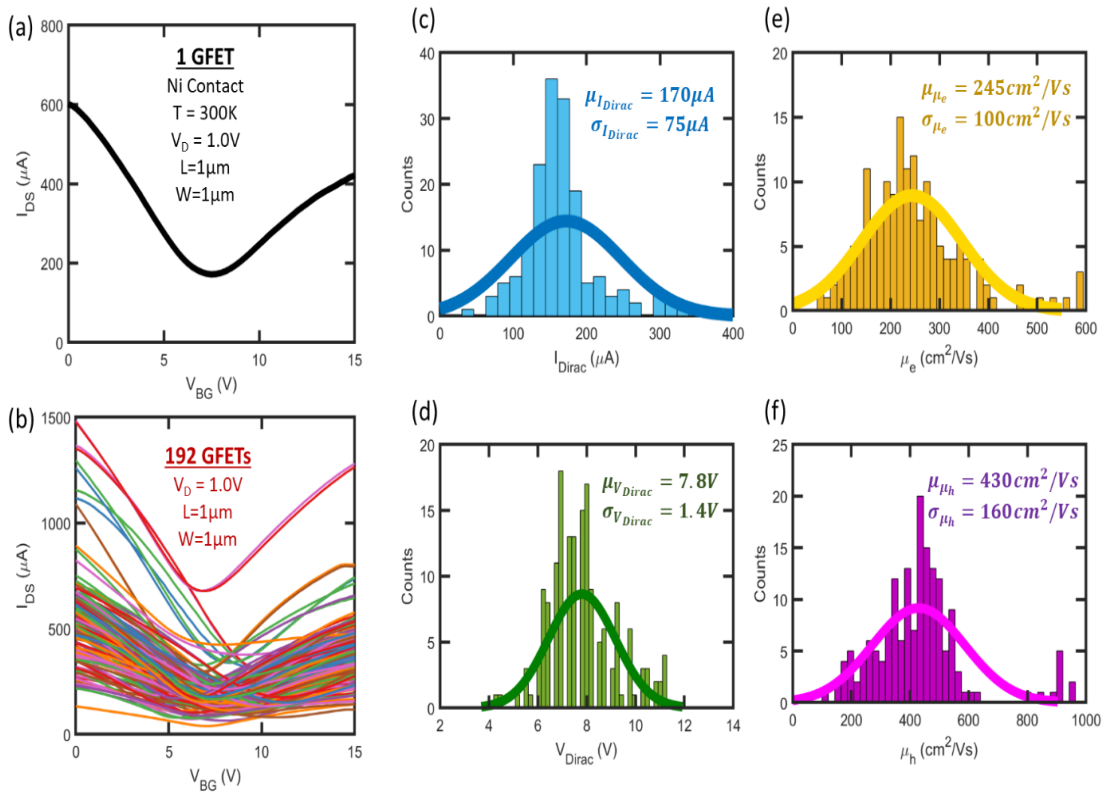

Figure 4: ***Stochastic Fluctuations in Graphene Field Effect Transistors (GFETs).*** *Transfer characteristics of a) single GFET and b) 192 GFETs each with 1µm channel length (L) and 1µm channel width (W), measured at room temperature at a drain bias (V_D) of 1V. Significant device to device variation can be seen. Histogram plot for c) Dirac voltage (V_{Dirac}), d) Dirac current (I_{Dirac}), e) electron mobility (μ_e), and f) hole mobility (μ_h), of these 192 GFETs, which were extracted from their corresponding device characteristics. Clearly, each of these device parameters follow random Gaussian distribution with mean and standard deviation noted in the inset of the associated figures. Note that the mean electron and hole mobility values are found to be 245 cm^2/V-s and 430 cm^2/V-s, respectively, which are orders of magnitude smaller than the best reported room temperature field effect mobility values for GFETs on similar dielectric. Further the standard deviation of electron and hole mobility values are rather large, which is a clear reflection of grain boundary and defect dominated transport in our GFETs. The random size, orientation, and locations of the grain boundaries and defects introduce stochastic fluctuations in the transfer characteristics of the GFETs through the abovementioned parameters forming the basis of on-chip graphene security.*

such as the hole (μ_h) and electron (μ_e) mobility, and V_{Dirac} caused by the random distribution of defects. This is shown by extracting μ_h, μ_e, and V_{Dirac} for the 198 devices as in Fig. 4d, 4e, and 4f, respectively. Here, it is shown that the parameters can be considered as random variables with large distributions quantified by the mean and standard deviation noted in the inset of the associated figure. We then harness these

variations in our device characteristics to form the basis of our graphene security primitive.

Chapter 3
Harvesting Device Randomness

An optical image of the final device structure for the security primitive is shown in Fig. 5a. This arrayed structure consists of 8 GFETs separated by $1\mu m$. The 8 devices share a source contact, which is kept grounded. Each array is treated as a PUF. For this paper, 24 PUFs were measured, where the drain voltage (V_D) is the challenge and the source to drain current (I_{DS}) is the response. For this report, a challenge of 1V was used,

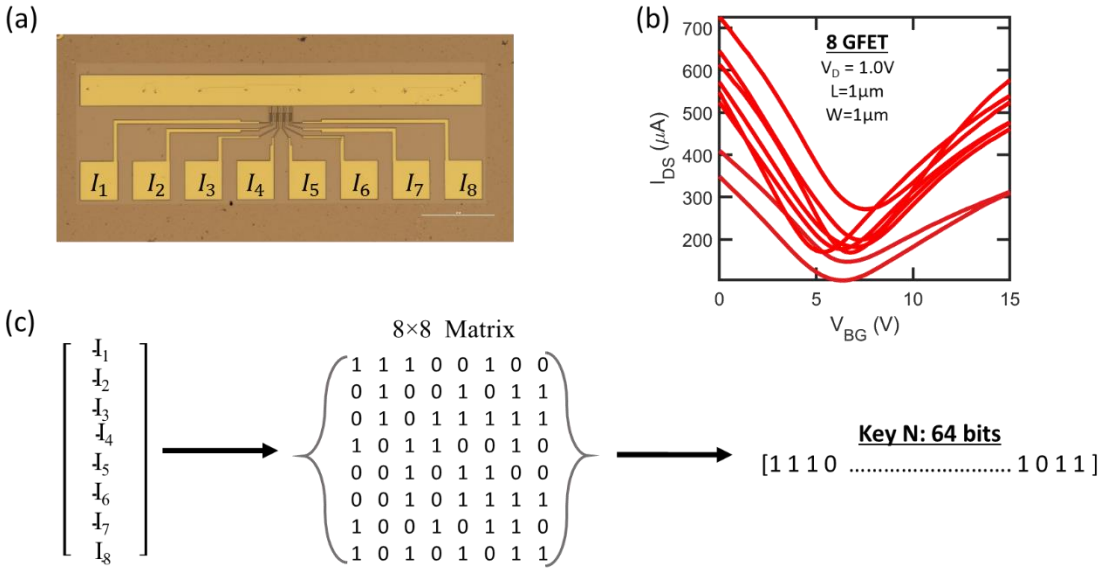

Figure 5: ***Cryptographic Keys Derived using GFETs.*** *a) Cryptographic keys were generated with the GFET arrays shown in the optical image. 8 GFETs, with a separation of 1 μm are contained in an array, whose common source, is kept grounded. b) Transfer characteristics of 8 individual GFETs corresponding to an array. A total of N = 24 arrays were measured. Each array is used to generate a key with the drain bias (**V_D**) as the challenge and source to drain current (**I_{DS}**) as the response. c) Each of the 8 analog current responses, measured at a specified gate voltage, were digitized to 8 bit binary numbers and subsequently appended to generate 8 x 8 = 64 bit long CRPs.*

and corresponding transfer measurements were taken, as shown Fig. 5b. To construct the digital PUF, we first select a gate voltage. The analog current value, at the selected gate voltage, for each of the 8 devices are digitized into 8-bit binary numbers for a total of a 64-bit key as shown in Fig 5c. This measure was taken to ensure a long enough key for a detailed analysis.

We used metrics such as entropy, correlation coefficient and Hamming distance to evaluate the quality of the randomness in our system and the uniqueness of the PUF CRP. The entropy of the system was calculated using the following equation:

$$\text{Entropy} = -[\text{p}\log_2\text{p} + (1-\text{p})\log_2(1-\text{p})] \quad [2]$$

where, p is the probability of finding either a 1 or 0. Ideally, the probability of finding a 1 or 0 should be equal i.e. p=0.5, which ensures a maximum entropy equal to unity. In cases where the entropy favors either a 1 or 0, then the probability of repeated CRP increases. The entropy of the 24 CRP and the corresponding mean as a function of the gate voltage is shown in Fig. 6a and 6b, respectively. With a mean of 0.97, it shows that our GFETs are capable of providing near perfectly random PUF CRP. Fig. 6c and 6d shows the Hamming distance among the ${}^{24}C_2$, or 276, pairs of CRP as a function of gate voltage. The Hamming distance between CRP is defined as the minimum number of bit substitutions required to transform one key into another. With knowledge of one CRP, and the Hamming distance between it and another CRP, it is possible to determine the next key through brute force trials (BFTs) equal to ${}^{N}C_x$, where N is the key length and x is the hamming distance. Note that if the Hamming distance between a pair of CRPs is too short or too long, a very limited number of brute force trails (BFTs) will be required to decipher one CRP from the knowledge of the other CRP. Ideally, a Hamming distance

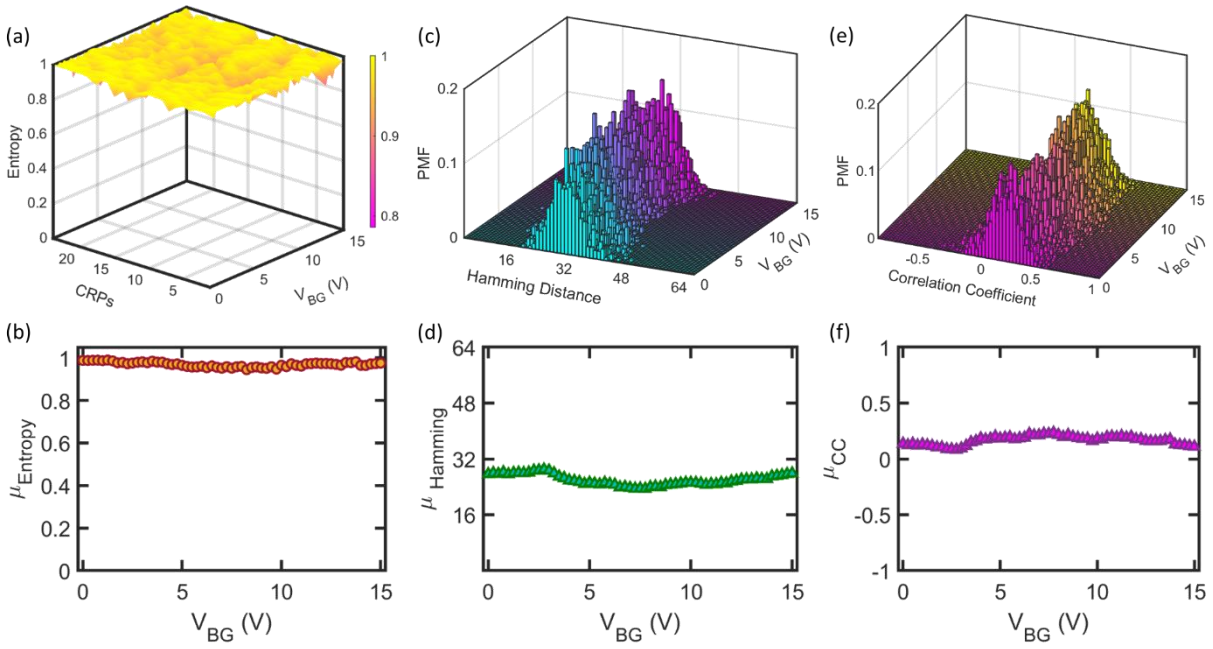

Figure 6: ***Randomness Test for GFET PUF.*** *a) Individual entropy (E) and b) Mean entropy of the CRPs obtained from 24 different GFET arrays, at each applied gate voltage. Clearly the entropy was found to be very close to the ideal value of unity, which confirms that the GFET arrays are perfectly random and unclonable information sources capable of delivering non-volatile on-chip security. c) Normalized distribution or probability mass function (PMF) of the Hamming distance among the* $^{24}C_2$ *or 276 pairs of CRPs as a function of the gate voltage. d) Extracted mean Hamming distance between the CRPs obtained by fitting binomial distributions. The mean Hamming distance ranges from 24 to 30, which is close to ideal Hamming distance of 32 confirming the uniqueness of the CRPs. e) Normalized distribution or probability mass function (PMF) of correlation coefficient among the 276 pairs of CRPs as a function of the gate voltage. f) Extracted mean correlation coefficient between the CRPs by fitting binomial distributions. The mean correlation coefficient is very close to the ideal value of zero, suggesting that the CRPs are uncorrelated. The total number of unique CRPs that can be generated using such graphene PUF is* 2^{64} *or* 1.8×10^{19}.

that is equal to half of the bit length ensures maximum number of BFTs and hence maximum possible uniqueness. For our set of 24 PUFs each with a length of 64 bits, an inter-Hamming distance, the Hamming distance between PUF instances, located at 32 implies a set of CRPs with maximum BFTs needed, and therefore maximum uniqueness. As a function of the gate voltage, V_G, the mean Hamming distance ranges from 24-30. While not ideal, the number of BFTs to decode our CRP is range from $^{64}C_{24}$ to $^{64}C_{30}$ or ~2.5×10^{17}-1.62×10^{18}, which is an astronomical number. Next, we calculated the correlation coefficient between the 24 PUF CRP. The correlation coefficient is a measure of linear correlation between two statistical quantities. For our CRP to be independent

and identically distributed random variables, the correlation coefficient must be zero. Fig. 6e, and 6f show that the correlation coefficients for the 24 PUF CRP are indeed very close to zero reasserting that our GFET PUFs generate CRP that are uncorrelated and random in nature.

Chapter 4
Reliability

As state previously, an essential aspect of a PUF is being able to reproduce the same response each time the same challenge is applied, regardless of external conditions. In the case of our GFET PUFs, CRPs are created by exploiting the variability in carrier mobilities and carrier concentration culminating in fluctuations in conductivity and leading to the high-entropy randomness demonstrated previously. As such, for our PUFs to be reliable, the conductivity of the devices must remain invariant to external stimuli. This includes voltage and temperature, as well as being stable over time (anti-aging). The reliability was thus calculated as the percent change in the conductivity as shown in equation 6:

$$\left|1 - \frac{\Delta G}{G}\right| * 100\% \quad [6]$$

where G is the conductivity of the graphene and ΔG is the change in conductivity. Here we tested the reliability of our PUFs under different supply voltage (V_{DD}), temperature, and hour conditions as a function of the applied gate voltages. To test the reliability of the PUF under varying supply voltage conditions, we varied V_{DD} by ±20%

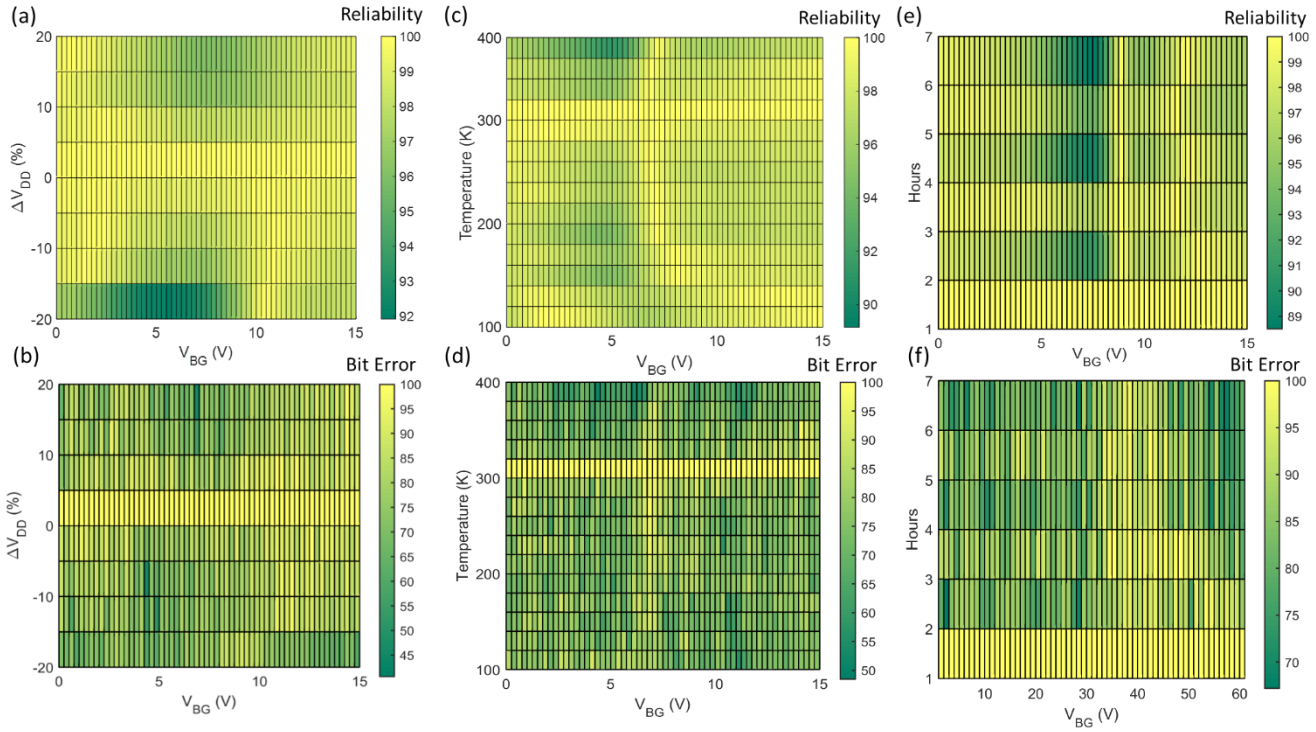

Figure 7: ***Reliability of Graphene PUF.*** *a) Color map showing the reliability of GFET as a function of the supply voltage (V_{DD}) variation. b) Color map showing the bit error rate of the CRPs as a function of the V_{DD}. c) Color map showing the reliability of GFET as a function of temperature. d) Color map showing the bit error rate of the CRPs as a function of the temperature. e) Color map showing the reliability of GFET as a function of temperature. f) Color map showing the bit error rate of the CRPs as a function of the temperature*

of our control of 1V. The results are shown in Fig. 7a as well as the corresponding bit-error rate in Fig. 7b. Fig. 7a shows that our GFET PUFs are remarkably reliable even when V_{DD} varies by 20%, compared to the control value of 1V. However, the bit error rate remains high pointing to instability in or CRPs. The disagreement in our analyses point to a fault in how we are generating our CRPs. Although the variation in the current is minimal, it leads to large changes in the 8-bit strings generated from the current values of each device. This, in turn, leads to sizable changes in the larger 64-bit string each GFET array composes.

Fig. 7c and 7d show the temperature reliability and corresponding bit-error rate of the PUF from 100K to 380K compared to the control of 300K. Again, the reliability

remains higher than 90% while the bit error rate suffers. Finally, Fig. 7e and 7f show the reliability colormap for the temporal stability and its corresponding bit-error rate. The devices were measured over a period of 7 hours. It is of note that every other hour there is a distinct drop in reliability around the same gate voltages. Currently, there is no explanation for this periodic decrease in the reliability. Still, the devices remain reliable, demonstrating have a high stability of the graphene overall. However, they are not ideal under all conditions owing to hysteresis[41], temperature dependence of mobility in graphene[42], etc., all of which can cause further changes in the transfer characteristics of our GFETs. This is reflected more so in our bit-error calculations. Measures such as fuzzy authentication protocols [19, 43, 44], where a certain degree of bit-error is tolerated among responses from the same challenge, may need be implemented.

Chapter 5
GFET Reconfigurability

The ability to reconfigure a cryptographic key generator significantly enhances the strength of its security protocols [45]. Reconfiguring the primitive helps to overcome reliability degradation and re-securing the system after a security breach. A primitive is considered reconfigurable if, through some physical mechanism, a given input produces different outputs before and after the reconfiguration action. Typically, reconfigurability is not an included feature in Si PUF systems due to the limitations in energy, cost and complexity. Here, however, we propose a lower power reconfiguration mechanism that

relies only on the established device structure produce a new set of CRPs. This is accomplished by applying a relatively higher voltage across the source and drain, while keeping the gate voltage at zero.

Fig. 8a shows the transfer characteristics of an as-fabricated GFET array. The device transfer characteristics are primarily hole dominant. Once we apply a large drain bias pulse is a, 5V for 10 seconds, the device experiences a dramatic shift in characteristics, to a more electron dominant transport as shown in Fig. 8b. Currently, we believe that the reconfiguration is due to the increased current in our channel leading to changes in the density of charges in our oxide The devices can be reconfigured again by applying a similar pulse of opposite polarity, i.e. -5V drain bias for 10s duration, as demonstrated in Fig. 8c. This time, the device characteristics shift back to the right, becoming more ambipolar. The CRPs generated from the reconfigured device (Fig. 8a-c) were tested using the metrics introduced previously, primarily the entropy, Hamming distance, and correlation coefficient. Fig. 8d shows that the entropy of the twice reconfigured device remains high as a function of the gate voltage. Fig. 8e shows that the Hamming distance remains close to 32 pre- and post- reconfiguration. Finally, Fig. 8f shows that correlation remains low, allowing us to conclude that the GFETs can be easily reconfigured without losing randomness.

To explore the extent of the reconfigurability of the GFETs the devices were reconfigured a total of 16 times, switching between positive and negative pulses. Again, the PUFs were tested using the same metrics as before. Fig. 8g shows that even after the

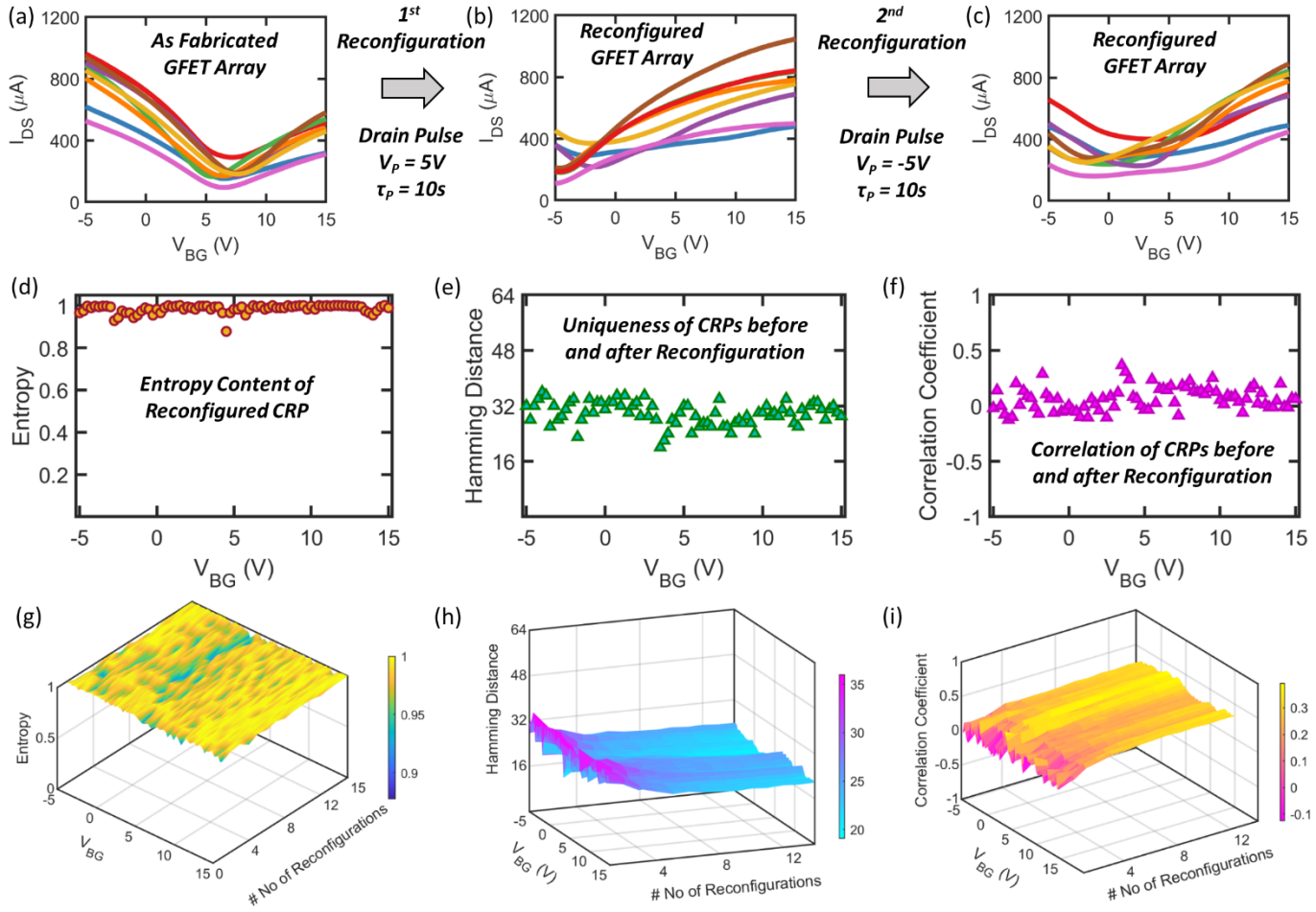

Figure 8: ***Reconfigurability of Graphene PUF.*** *a) Transfer characteristics of an as-fabricated GFET array, where the individual devices exhibit dominant hole transport. b) Transfer characteristics of the same GFET array after 1st reconfiguration using a positive drain voltage pulse of magnitude 5V, which is applied for 10s. The device characteristics change dramatically and randomly and show dominant electron transport that is stable and do not revert back to original characteristics over time ensuring permanent reconfiguration, which is desired for a strong PUF. c) Transfer characteristics of the same GFET array after 2nd reconfiguration using similar magnitude i.e. 5V but reverse polarity i.e. negative drain bias applied for 10s. In this instance the devices recovered partial p-type conduction and become more ambipolar. d) Entropy of the reconfigured CRP remains close to unity. e) The Hamming distance and f) the correlation coefficient between the pre- and post- reconfigured CRPs are also close their ideal value of 32 and 0, respectively, irrespective of the gate voltage, which confirms that the GFET PUFs can be seamlessly reconfigured without any loss of randomness. It is possible to reconfigure the GFET PUF multiple times by cycling between positive and negative drain voltage pulses. g) Entropy of the CRPs obtained from multiple (16) reconfigurations of the same GFET PUF. h) The average Hamming distance between the reconfigured CRPs decreases and i) correlation coefficient between the reconfigured CRPs increases as the system is continually reconfigured. This shows some loss in uniqueness with successive reconfiguration.*

multiple reconfigurations the entropy remains high, confirming that the GFETs remain random. However, in Fig. 8h the average Hamming distance experiences a decrease as the number of reconfigurations increases before plateauing around 22. This tells us that the CRPs begin to lose uniqueness; a penalty for continued reconfiguration. The

correlation shown in Fig. 8i confirms this as it shows in increase in correlation among the CRPs as reconfiguration continues.

Although the Hamming distance after successive reconfigurations has a value closer to ideal, the Hamming distance decreases after each reconfiguration, to a value of 22 for our 64-bit CRPs. As such, it can be argued that the system becomes less resistant to attack if an adversary were to keep track of all CRPs across several reconfigurations. To make the PUF more robust we increased the number of GFETs in the PUF, increasing the bit length. After reconfiguring these devices, the Hamming distance falls to 45, as shown in Fig. 9, after successive reconfigurations. As expected the hamming distance was doubled with the number of total bits. By increasing the bit length, we can get a quantitative improvement in performance as the number of brute force trials increases from $^{22}C_{64}$ to $^{45}C_{128}$ or ~$8*10^{16}$ to ~$4*10^{34}$. Therefore, we can make the PUFs more robust by increasing the number of devices, however this comes at a cost of area and power efficiency. These costs can be combatted by reductions in device size and the applied voltage, which will be discussed in later chapters.

After a reconfiguration action the PUF must be able to maintain the reconfigured characteristic in order to be a viable security primitive.

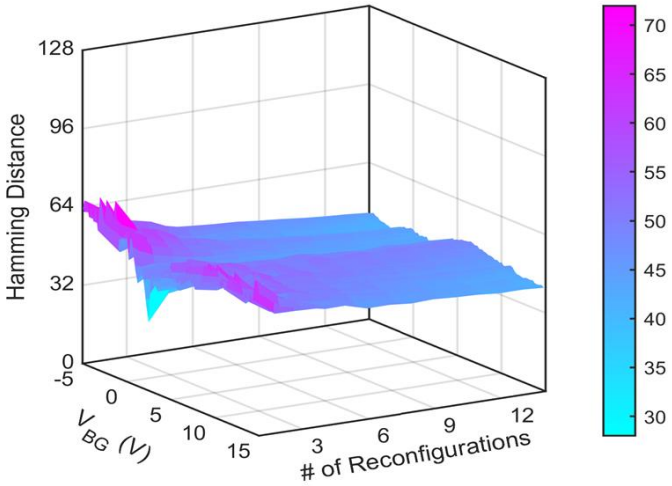

Figure 9: ***128-bit CRP Reconfiguration*** *PUF with twice the number of bits has a Hamming distance between the CRPs that falls to a value that is twice what it was previously. This shows that while there is still some loss in uniqueness with successive reconfiguration, we can improve robustness of the PUF by requiring a larger number of brute force tirals to decrypt.*

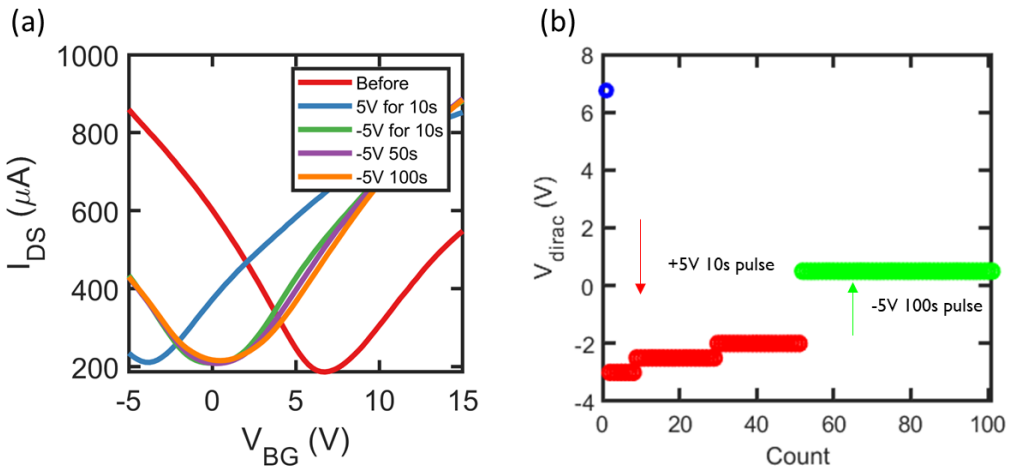

Figure 10: ***GFET Reconfiguration Reliability*** *a) GFET that has before and after a +5V pulse for 10s and -5V pulse for 10s, 50s, and 100s duration. This demonstrates that the pulse duration has relatively little effect on the post-reconfiguration characteristics. b) Position of the Dirac voltage after reconfiguration. Transfer characteristics were measured every 10s for a total of 50 times.*

First, we reconfigured a GFET twice, once with a +5V, 10s pulse and then with a -5V, 10s pulse. Furthermore, to demonstrate the effect that the pulse duration has on the shift in transfer characteristics, after the initial -5V, 10s pulse, we applied -5V pulses with durations of 50s and 100s. This is shown in Fig. 10a. The duration of the pulse is shown to have a relatively small effect on the current. To test the stability of the post-reconfiguration GFETs, the transfer characteristics were measured every 10s a total of 50 times after the positive bias reconfiguration and again after the final 100s negative bias reconfiguration. The Dirac voltage was extracted from each measurement and plotted in Fig. 10b. The pre-reconfiguration device has a Dirac voltage initially around 6V. After the application of the positive bias pulse, the Dirac voltage shifts to -3V before slowly rising and settling at a value of -2V. When the negative bias pulse was applied the Dirac voltage increased to ~0.5V, where it stayed for the duration of the measurements. These measurements show that our reconfigured devices remain stable.

Chapter 6
Implementation

An important challenge for PUF systems is how to extract the PUF properties form the material. Here, we propose a circuit on how the intrinsic randomness of the GFETs can be extracted. Fig. 11 shows the circuit level implementation of the GFET PUF. Using an operational amplifier (op-amp) the analog output current is converted to an analog output voltage. Then, using an analog to digital converter (ADC) the output voltage is converted to an 8-bit binary output.

The performance of the circuit was estimated by evaluating the power consumption and readout timing calculations. Fig. 12a shows the color map of the power consumption of the 24 GFETs as a function of the gate voltage applied. This was calculated using the equation:

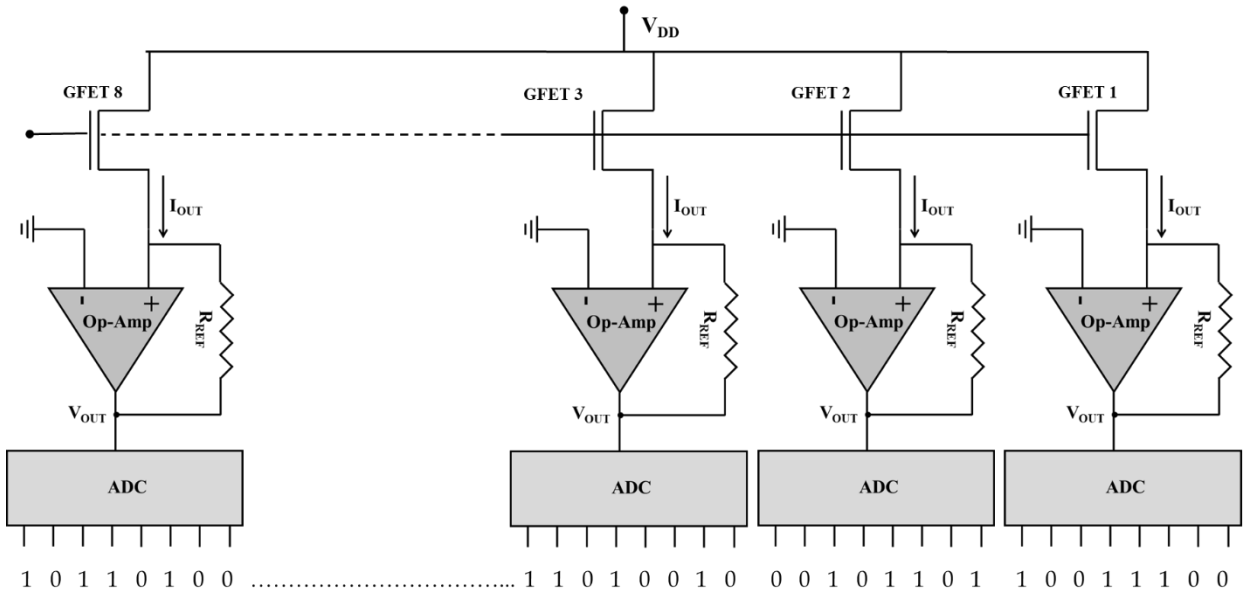

Figure 11: ***Circuit level implementation of GFET PUF*** *The analog output current (I_{OUT}) from each individual GFET is converted to analog output voltage (V_{OUT}) by using an operational amplifier (Op-Amp) and subsequently converted to 8 bit binary output using an analog to digital converter (ADC).*

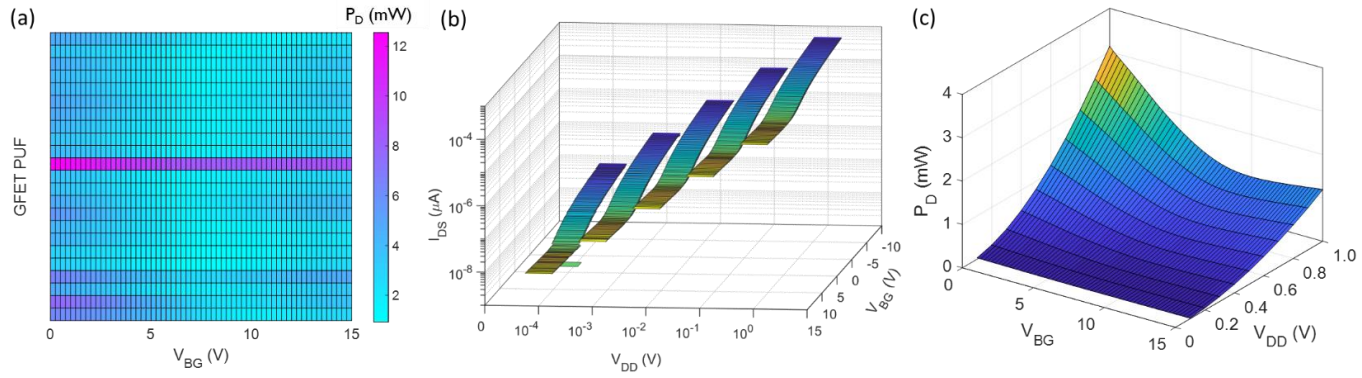

Figure 12: ***Power Consumption of Graphene PUF*** *a) Color map of power consumption by 24 GFET PUFs at different V_{BG}. Each row represents 1 GFET PUF. Power dissipation is minimum with an average value of 2.3mW when the GFET PUFs are operated near the Dirac point. b) Transfer characteristic of GFET as the supply voltage (V_{DD}) is scaled over 4 orders of magnitude from 1V down to 100μV. c) Power dissipation in a GFET PUF as a function of V_{DD} at different V_{BG}.*

[7] $$P_{D,j=\sum_{i=1}^{N} I_{ij} V_{DD}}$$

where P_{Dj} is the power dissipation in the j-th PUF, N is the number of GFETs in a given PUF, V_{DD} is the supply voltage and I_{ij} is the response current in the i-th GFET of the j-th PUF. The power dissipation reaches a minimum 2.3mV near the Dirac point. The power dissipation can be minimized further by reducing the supply voltage. Fig. 12b shows the transfer characteristics of a GFET at different supply voltage over 4 orders of magnitude, from 1V to 100μV. The semi-metallic nature of graphene allows us to aggressively scale the supply voltage by forming near ohmic contacts [46]. We can scale up to the presence of thermal noise, which can distort the bit values, at any finite temp. Fig. 12c shows the change in power dissipation as the supply voltage is scaled down. It demonstrates that we can scale the power linearly irrespective of the gate voltage.

Finally, we estimated the timing delay (τ_{PUF}) for obtaining a CRP from the GFET array using the circuit described in Fig. 11 using the equation:

[8] $$\tau_{PUF} = \tau_{GFET} + \tau_{op-amp} + \tau_{ADC}$$

where τ_{GFET} is the intrinsic delay of the GFET, τ_{op-amp} is the delay for the op-amp and τ_{ADC} is the delay associated with the analog to digital converter. Assuming the carriers in graphene move at the Fermi velocity (~10^6 m/s) the τ_{GFET}=1ps for our 1µm channel devices. τ_{op-amp} is estimated as ~1-2τ_{clc} while τ_{ADC}~$4-6\tau_{clc}$, where τ_{clc} is the clock cycle of the processor. Typically the clock cycle is in the range of nanoseconds. Therefore, the total timing delay can be estimated to bin the 10s of nanoseconds range.

Chapter 7
Discussion

Other nanomaterial based PUFs have been proposed in the past including randomly dispersed nanoparticles **[47-49]**, MoS_2 [50], self-assembled carbon nanotubes **[17]**, and block copolymers and phase change materials (memresistor) [10, 51, 52]. The first two require optical systems limiting their practicality in integrated circuitry. However, PUFs fabricated by Hu, Z *et al.* using 2D array of self-assembled carbon nanotube (CNT) are suitable for circuit integration and shows near ideal stochastic PUF performance.[17] Similarly, RRAM or memristor based PUFs have also been intensely investigated in recent years and have shown promising results [53-55]. Still, the GFET PUFs proposed here have advantages over the emerging nanomaterial based PUFs.

CNT PUFs generate CRP by exploiting the random placement and alignment of CNTs on predefined trenches of specific widths between the leads of a crossbar array. CNTs are randomly placed in the trenches using a self-assembled process [56]. Bit values

are then assigned based on the connection type between the CNT and the array leads. The fabrication process flow for CNT PUF involves more lithography steps compared to GFET PUF incurring additional cost. Furthermore, since the bits are determined by the CNT placement, an adversary with access to the PUF can use high-resolution imaging tools such as electron microscope do determine CNT location and hence the bit information. For our GFET PUFs, being able to image the defects in our material does not impart any bit information since determining the transfer properties such as field effect mobility, Dirac voltage, etc., which compound to add variability to our current, is impossible. Moreover, the ambipolar nature of transport and the option to tune the gate voltage further strengthen GFET PUF against reverse engineering attacks. Finally, CNT PUF lacks reconfigurability as it is not possible to change the location of the CNT post fabrication.

A memristor consists of a metal/oxide/metal stack where the oxide is a sub-stoichiometric dielectric such as TaO_x, HfO_x. Memresistors have two states; a high resistance state (HRS) due to insulating nature of the oxide and a low resistance state (LRS) which is formed by applying a sufficiently large electric field. The conduction mechanism in the HRS is dominated by quantum mechanical tunneling, where a small variation in the tunneling gap distance results in a significant variation in resistance, whereas, conduction mechanism in LRS is mostly Ohmic and translates into lesser resistance variation. To program these devices, first, a pulse forming process is performed on each device to ensure uniform LRS distribution across the array. Next a reset attempt is made on each device to restore the HRS. The operating voltages for forming, reset, set and readout are in the range of 1-5V even for only few nm thick

oxides.[55] Typically, the HRS is exploited in most for PUF demonstration because of the need for a high-entropy state. The variation that occurs in the HRS after this reset operation is subsequently used as the random entropy source for the memristive PUF. Therefore, the implementation of such PUFs are power hungry and defies energy scaling. On the contrary GFET PUFs offer aggressive voltage and hence energy scaling. Although it's been proposed, there is also no experimental demonstration of on-chip reconfiguration of memristive PUF. Finally, there exists several other challenges associated with implementing memristors PUFs including the need for complicated probability tracking, careful tuning of the applied voltage/current, post-processing of data, sophisticated algorithms and circuits, which do not appear to limit GFET PUF.[57-59]

Chapter 8
Future Work

While the GFET PUFs have demonstrated the ability to generate random and largely uncorrelated CRP, which require an astronomical number of BFTs to decode, they still require work before reaching a more ideal stochastic performance and achieving stability in the CRP. As we have shown earlier, the GFETs have a high intrinsic variability in their characteristics. A possible reason the CRP are not reflecting this is in how we are extracting that randomness and constructing CRPs from it. The process of converting the analog output current to a digital 8-bit number involves mapping the device current values to a 256-bit range which can have unattended effects on our CRP

and, consequently, the Hamming distance between the CRPs (inter-Hamming distance). Our CRP generation may also cause the Hamming distance for any CRP under different external stimuli (intra-Hamming distance) to become larger than intended. This would be due to the small changes in current leading to large switching in bits in the 8-bit string. For example, going from 7 to 8 involves a switching of 4 bits. In order to get the true performance of the GFET PUFs we have to develop a system where each device is treated as 1-bit. Bit values would be assigned based on where the current value falls compared to the average of all devices. The circuit design for this would replace the ADC with a voltage comparator to convert V_{out} from each GFET to a 1-bit binary output.

Another method for increasing the hamming distance between generated CRP is by introducing nanoparticles which can further dope the material. By randomly distributing the particles over the device, each would ideally experience a different shift to their current characteristics based on the number of nanoparticles on top of the channel material. Currently we hope to explore CdSe, Pbs, and Au nanoparticles, all of which we have experienced to cause shifts in the transfer characteristics due to a charge transfer mechanism between the channel material and the nanoparticle. Finally, we would like to explore other two-dimensional material such as MoS_2, WSe_2, etc., as possible PUFs to secure devices featuring other emerging nanomaterials.

Chapter 9
Conclusion

In the conclusion, we have demonstrated a reliable and robust graphene PUF that exploits the inherent disorders associated with the carrier transport in grain boundary dominated GFETs. CRP generated demonstrated near ideal entropy and uniqueness through various security metrics. Furthermore, the GFET primitives were reliable under different external stimuli as well as nonvolatile. Finally, we demonstrated that these devices can be reconfigured using the existing device structure. While these PUFs, in their current form, do not match the near ideal stochastic performance demonstrated by other emerging PUFs, our graphene PUFs still have several advantages over other PUFs. For example, the GFET PUFs are effortless and sport a design that can be seamlessly integrated with any substrate-rigid or flexible. This is in contrast with the precise control or placement of the nanomaterial, optimization of device operating conditions and other challenges needed to be overcome to ensure high-quality randomness that other featured nanomaterials PUFs deal with. With the increasing presence of graphene-based electronics in the era of IOTs, the introduction of an on-chip graphene cryptography, is an important step in data security.

References

1. IDC, I.U.N. *A Guide to the Internet of Things Infographic*. 2015.
2. Atzori, L., A. Iera, and G. Morabito, *The internet of things: A survey.* Computer networks, 2010. **54**(15): p. 2787-2805.
3. Ning, H. and S. Hu, *Technology classification, industry, and education for Future Internet of Things.* 2012. **25**(9): p. 1230-1241.
4. Xia, F., et al., *Internet of Things.* 2012. **25**(9): p. 1101-1102.
5. Katz, J. and Y. Lindell, *Introduction to modern cryptography*. 2014: CRC press.
6. Cook, S., ed. *The P versus NP Problem*. Millenium Prize Problems, ed. A.J. James Carlson, Andrew Wiles. 2006, American Mathematical Society: Providence, RI.
7. Fortnow, L., *The Status of the P Versus NP Problem*, in *Communications of the ACM*. 2009, ACM: New York, NY. p. 78-86.
8. Sullivan, N. *How the NSA (may have) put a backdoor in RSA's cryptography: A technical primer*. arsTechnica, 2014.
9. van der Leest V., v.d.S.E., Schrijen GJ., Tuyls P., ,Handschuh H. , ed. *Efficient Implementation of True Random Generator Based on SRAM PUFs*. Cryptography and Security: From Theory to Application. Lecture Notes in Computer Science, ed. N. D. Vol. 6805. 2012, Springer, Berlin, Heidelberg.
10. Gao, Y., et al., *Emerging Physical Unclonable Functions With Nanotechnology.* IEEE Access, 2016. **4**: p. 61-80.
11. Pappu, R., et al., *Physical One-Way Functions.* Science, 2002. **297**(5589): p. 2026-2030.
12. Marangon, D.G., G. Vallone, and P. Villoresi, *Random bits, true and unbiased, from atmospheric turbulence.* Scientific Reports, 2014. **4**: p. 5490.
13. Maes, R. and I. Verbauwhede, *Physically unclonable functions: A study on the state of the art and future research directions*, in *Towards Hardware-Intrinsic Security*. 2010, Springer. p. 3-37.
14. Ruhrmair U., D.S., Koushanfar F., *Security Based on Physical Unclonability and Disorder*, in *Introduction to Hardware Security and Trust*, W.C. Tehranipoor M., Editor. 2012, Springer: New York, NY.
15. Gassend, B., et al. *Silicon physical random functions*. in *Proceedings of the 9th ACM conference on Computer and communications security*. 2002. ACM.
16. Suh, G.E. and S. Devadas. *Physical Unclonable Functions for Device Authentication and Secret Key Generation*. in *2007 44th ACM/IEEE Design Automation Conference*. 2007.
17. Hu, Z., et al., *Physically unclonable cryptographic primitives using self-assembled carbon nanotubes.* Nature nanotechnology, 2016. **11**(6): p. 559.
18. Helfmeier, C., et al., *Physical vulnerabilities of physically unclonable functions*, in *Proceedings of the conference on Design, Automation & Test in Europe*. 2014, European Design and Automation Association: Dresden, Germany. p. 1-4.
19. Yu, M.-D. and S. Devadas, *Secure and robust error correction for physical unclonable functions.* IEEE Design & Test of Computers, 2010. **27**(1): p. 48-65.
20. Frank, D.J., et al., *Device scaling limits of Si MOSFETs and their application dependencies.* Proceedings of the IEEE, 2001. **89**(3): p. 259-288.
21. Akinwande, D., N. Petrone, and J. Hone, *Two-dimensional flexible nanoelectronics.* Nature communications, 2014. **5**: p. 5678.
22. Kim, D. and J. Moon, *Highly conductive ink jet printed films of nanosilver particles for printable electronics.* Electrochemical and Solid-State Letters, 2005. **8**(11): p. J30-J33.
23. Bae, S., et al., *Roll-to-roll production of 30-inch graphene films for transparent electrodes.* Nature nanotechnology, 2010. **5**(8): p. 574.
24. Kim, J.T. and S.-Y. Choi, *Graphene-based plasmonic waveguides for photonic integrated circuits.* Optics express, 2011. **19**(24): p. 24557-24562.

25. Torrisi, F., et al., *Inkjet-printed graphene electronics.* ACS nano, 2012. **6**(4): p. 2992-3006.
26. Wang, Y., et al., *Wearable and highly sensitive graphene strain sensors for human motion monitoring.* Advanced Functional Materials, 2014. **24**(29): p. 4666-4670.
27. Xia, F., et al., *Ultrafast graphene photodetector.* Nature nanotechnology, 2009. **4**(12): p. 839.
28. Lee, Y., et al., *Wafer-scale synthesis and transfer of graphene films.* Nano letters, 2010. **10**(2): p. 490-493.
29. Lin, Y.-M., et al., *Wafer-scale graphene integrated circuit.* Science, 2011. **332**(6035): p. 1294-1297.
30. Kim, K.S., et al., *Large-scale pattern growth of graphene films for stretchable transparent electrodes.* nature, 2009. **457**(7230): p. 706.
31. Yang, X., et al., *Clean and efficient transfer of CVD-grown graphene by electrochemical etching of metal substrate.* Journal of Electroanalytical Chemistry, 2013. **688**: p. 243-248.
32. Suk, J.W., et al., *Transfer of CVD-Grown Monolayer Graphene onto Arbitrary Substrates.* ACS Nano, 2011. **5**(9): p. 6916-6924.
33. Chen, J.-H., et al., *Defect Scattering in Graphene.* Physical Review Letters, 2009. **102**(23): p. 236805.
34. Yazyev, O.V. and S.G. Louie, *Electronic transport in polycrystalline graphene.* Nature Materials, 2010. **9**: p. 806.
35. Lafkioti, M., et al., *Graphene on a Hydrophobic Substrate: Doping Reduction and Hysteresis Suppression under Ambient Conditions.* Nano Letters, 2010. **10**(4): p. 1149-1153.
36. Nagashio, K., et al. *Metal/graphene contact as a performance Killer of ultra-high mobility graphene analysis of intrinsic mobility and contact resistance*. in *2009 IEEE International Electron Devices Meeting (IEDM)*. 2009.
37. Kim, S., et al., *Realization of a high mobility dual-gated graphene field-effect transistor with Al 2 O 3 dielectric.* Applied Physics Letters, 2009. **94**(6): p. 062107.
38. Yu, Q., et al., *Control and characterization of individual grains and grain boundaries in graphene grown by chemical vapour deposition.* Nature Materials, 2011. **10**: p. 443.
39. Huang, P.Y., et al., *Grains and grain boundaries in single-layer graphene atomic patchwork quilts.* Nature, 2011. **469**: p. 389.
40. Li, X., et al., *Graphene Films with Large Domain Size by a Two-Step Chemical Vapor Deposition Process.* Nano Letters, 2010. **10**(11): p. 4328-4334.
41. Wang, H., et al., *Hysteresis of Electronic Transport in Graphene Transistors.* ACS Nano, 2010. **4**(12): p. 7221-7228.
42. Tan, Y.W., et al., *Temperature dependent electron transport in graphene.* The European Physical Journal Special Topics, 2007. **148**(1): p. 15-18.
43. Schrijen, G.-J. and V. Van Der Leest. *Comparative analysis of SRAM memories used as PUF primitives*. in *Proceedings of the conference on design, automation and test in Europe*. 2012. EDA Consortium.
44. Katzenbeisser, S., et al. *PUFs: Myth, fact or busted? A security evaluation of physically unclonable functions (PUFs) cast in silicon*. in *International Workshop on Cryptographic Hardware and Embedded Systems*. 2012. Springer.
45. Kursawe, K., et al. *Reconfigurable Physical Unclonable Functions - Enabling technology for tamper-resistant storage*. in *2009 IEEE International Workshop on Hardware-Oriented Security and Trust*. 2009.
46. Byun, K.-E., et al., *Graphene for True Ohmic Contact at Metal–Semiconductor Junctions.* Nano Letters, 2013. **13**(9): p. 4001-4005.
47. Yoon, B., et al., *Recent functional material based approaches to prevent and detect counterfeiting.* Journal of Materials Chemistry C, 2013. **1**(13): p. 2388-2403.
48. Demirok, U.K., J. Burdick, and J. Wang, *Orthogonal multi-readout identification of alloy nanowire barcodes.* Journal of the American Chemical Society, 2008. **131**(1): p. 22-23.

49. Kim, J., et al., *Anti-counterfeit nanoscale fingerprints based on randomly distributed nanowires.* Nanotechnology, 2014. **25**(15): p. 155303.
50. Alharbi, A., et al., *Physically Unclonable Cryptographic Primitives by Chemical Vapor Deposition of Layered MoS2.* ACS Nano, 2017. **11**(12): p. 12772-12779.
51. Rajendran, J., et al. *Nano-PPUF: A memristor-based security primitive*. in *VLSI (ISVLSI), 2012 IEEE Computer Society Annual Symposium on*. 2012. IEEE.
52. Rose, G.S., et al. *A write-time based memristive PUF for hardware security applications*. in *Computer-Aided Design (ICCAD), 2013 IEEE/ACM International Conference on*. 2013. IEEE.
53. Chen, A., *Utilizing the Variability of Resistive Random Access Memory to Implement Reconfigurable Physical Unclonable Functions.* IEEE Electron Device Letters, 2015. **36**(2): p. 138-140.
54. Gao, L., et al., *Physical Unclonable Function Exploiting Sneak Paths in Resistive Cross-point Array.* IEEE Transactions on Electron Devices, 2016. **63**(8): p. 3109-3115.
55. Liu, R., et al., *Experimental Characterization of Physical Unclonable Function Based on 1 kb Resistive Random Access Memory Arrays.* IEEE Electron Device Letters, 2015. **36**(12): p. 1380-1383.
56. Park, H., et al., *High-density integration of carbon nanotubes via chemical self-assembly.* Nature Nanotechnology, 2012. **7**: p. 787.
57. Balatti, S., et al., *Physical Unbiased Generation of Random Numbers With Coupled Resistive Switching Devices.* IEEE Transactions on Electron Devices, 2016. **63**(5): p. 2029-2035.
58. Balatti, S., et al., *True Random Number Generation by Variability of Resistive Switching in Oxide-Based Devices.* IEEE Journal on Emerging and Selected Topics in Circuits and Systems, 2015. **5**(2): p. 214-221.
59. Uddin, M., et al. *Techniques for Improved Reliability in Memristive Crossbar PUF Circuits*. in *2016 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*. 2016.