Multi-gated Carbon Nanotube Field Effect Transistors based Physically Unclonable Functions as Security Keys

Nitish Kumar, Jialuo Chen, Monodeep Kar, Suresh K. Sitaraman, Saibal Mukhopadhyay and Satish Kumar*
Contact author e-mail: satish.kumar@me.gatech.edu

***Abstract*—Enabling data security from unauthorized access is a major challenge for electronics devices. Most of the conventional cryptographic techniques store 'keys' in non-volatile memory, which is vulnerable to external attacks like physical attacks, side-channel attacks, fault attacks, etc. Physically Unclonable Functions (PUFs) have the potential to overcome these challenges because they do not store keys permanently and are difficult to reproduce. The next generation of electronic and opto-electronic devices may use semiconducting materials like carbon nanotubes (CNTs) or 2-D materials due to their superior electrical, optical, thermal and mechanical properties. There is a need for PUFs, which are low-cost and more efficient than existing silicon-based PUFs and compatible with future electronic technologies. We propose multi-gated CNT Field Effect Transistors (CNT-FETs) based PUFs, where inherent randomness of CNT network and a multi-gated channel are utilized to generate high-quality random keys. We have shown that while conventional single-gate channel FETs can generate binary keys, multi-gated CNT-FETs, where different gate voltages are applied in different sections of the channel, can enable the creation of multiple challenges and current levels to produce not only ternary but up to base-17 (heptadecimal) keys. Such keys can create significantly more entropy than binary or ternary keys of the same size generated by typical PUFs.**

***Index Terms*— CNT, PUF, security keys, random, FET, multi-gate, percolation.**

I. INTRODUCTION

USAGE of electronic devices has increased exponentially in the last few decades and this is expected to further rise due to the rapid growth of IoT. It has made transfer of data and information very fast and simple but increased the risk of privacy and security breach. There are several cryptographic techniques to secure data, but most of the cryptographic primitives use 'keys'. Ideally, they should be able to generate random and unique keys as well as securely store, retrieve and use these keys as an input into an encryption algorithm to encrypt the data without revealing any information about the keys. However, these tasks are not simple. Previous studies have reported that many security systems have poor key generators, which make them vulnerable [1, 2]. In addition, these keys are usually stored in a non-volatile digital memory, e.g., Electronically Erasable Programmable Read-Only Memory (EEPROM). Thus, keeping them secure also becomes a challenge as physical, fault and side-channel attacks (e.g., power consumption, execution time) can be used to steal the key [3-5].

Physically Unclonable Functions (PUFs), physical root-of-trust cryptographic primitives, are an attractive option to overcome the aforementioned challenges. PUF instances, as the name suggests, cannot be replicated due to their complex physical properties, even if all the parameters in the fabrication process are constant. Each instance of PUF receives one or multiple challenges and generates one or multiple responses. The response(s) of each instance will be unique and unpredictable as the physical phenomenon rendering the response cannot be controlled to produce any fixed type of response. These different types of responses can be associated with different key values and multi-level (e.g., binary, ternary) keys can be generated using multiple PUFs together to secure data from the external attacks. PUFs can also be used in other applications e.g., secure RFID systems [6], IP protection [7], device authentication [8]. Several PUF designs have been proposed in the past that exploit electronic, optical, magnetic and many other properties of materials. Some of the conventional PUF designs include Optical PUF, named as Physical One-way Function, proposed in [9], Arbiter PUF

This paragraph of the first footnote will contain the date on which you submitted your paper for review.

Nitish Kumar is with G. W. W. School of Mechanical Engineering, Georgia Institute of Technology, Atlanta, GA 30332 USA (e-mail: nitish.kumar@gatech.edu).

Jialuo Chen is with School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332 USA (e-mail: jlchen@gatech.edu).

Monodeep Kar was with School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332 USA when this work was performed. He is now with the Intel Corporation, Hillsboro, OR 97124 USA (e-mail: monodeepkar@gmail.com).

Suresh K. Sitaraman is with G. W. W. School of Mechanical Engineering, Georgia Institute of Technology, Atlanta, GA 30332 USA (e-mail: suresh.sitaraman@me.gatech.edu).

Saibal Mukhopadhyay is with Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332 USA (e-mail: satish.kumar@me.gatech.edu).

Satish Kumar is with G. W. W. School of Mechanical Engineering, Georgia Institute of Technology, Atlanta, GA 30332 USA (e-mail: satish.kumar@me.gatech.edu).

proposed in [10, 11], Magnetic PUF proposed in [12], Ring Oscillator PUF proposed in [13], Coating PUF proposed in [14], Bitline PUF proposed in [15] SRAM PUF proposed in [7], Glitch PUF proposed in [16], etc. For many applications, we may be moving from conventional silicon-based electronic devices toward nano-materials based flexible, wearable and faster computing devices [17-21]. These devices can help reduce power consumption and cost and are compatible with various new substrates used for the next generation of electronic devices. Carbon nanotube (CNT) based PUFs have been proposed and even fabricated in recent years [22, 23]. Hu et al. [22] fabricated devices on lab-scale where CNTs are selectively self-assembled into HfO_2 trenches to create open and closed connections, which are associated with bit values '0' and '1' respectively. They also showed ternary key generation by further differentiating between semi-conducting and metallic CNT closed connections. It was not clear how to control the yield of semi-conducting and metallic CNT connections to maximize the randomness in ternary keys. Each instance had only one challenge, which also limited randomness and level of security. In addition, these trenches were of nanometer scale and large-scale production may not be reliable and economically viable.

In this work, we introduced a random CNT network-based multi-gated Field Effect Transistor (FET) as PUF, which exploits the randomness of the CNT network in the channel to generate keys. Single-gate transistors with CNT density close to percolation threshold density produced binary keys depending upon whether the CNT network channel was connected or not. We introduced a multi-gate CNT-FET, where the channel was divided into multiple sections and each section could be biased with an independent gate voltage. FETs with four-gates produced three different levels of current including zero current corresponding to an unconnected CNT network and generated six different challenge-response pairs in a single instance. Current levels were separate enough to avoid any bit error. We could also control the distribution of different bit-values easily to maximize the randomness by changing the dimensions of the channel and/or its sections. By combining six challenges and three current levels, it was shown that not only ternary-bit keys but base-17 (hepta-decimal) keys could also be produced. Consequently, a significantly higher level of randomness was achieved by our PUF in comparison with existing PUFs, which could generate only binary or ternary keys.

II. CNT-FET FABRICATION AND ASSESSMENT AS PUFS

We fabricated CNT-FETs using the cleanroom facilities of the Institute for Electronics and Nanotechnology (IEN) at Georgia Tech. The devices' I_{ds}-V_{gs} characteristics were measured to assess their usage as PUFs. The details of the fabrication method are reported in the 'Methods' Section (see 'Experimental' part). CNT-FETs of four different channel lengths–10, 20, 40 and 60 μm were fabricated with a constant width of 100 μm. The CNT solution was from NanoIntegris who reported that the average length of the CNTs is 1 μm and CNTs have semiconducting purity equal to or greater than 99.9%. SEM images of networks indicated that the placement of CNTs in the channel was completely random, see Fig. 1(c). The CNT network density was estimated to be around 13 per μm^2 using SEM images.

I_{ds}-V_{gs} curves are shown in Fig. 1(d) for four different channel lengths and ON/OFF ratio was observed to be greater than or equal to 10^4. ON/OFF ratio of the order of 10^4 and higher have also been reported in previous studies [24, 25]. The experimental measurement and analysis helped us choose the appropriate conductivity ratio in multi-gate CNT-FETs (discussed later).

Since CNT networks are random, each FET should have a unique CNT network distribution. Therefore, the current should be different for different FETs for a given gate and drain voltage even if all the parameters, e.g., CNT network density; device dimensions and fabrication process are identical. We also wanted to engineer these devices in such a way that different current levels can be obtained to facilitate the development of ternary or higher order bits. However, the measurement of current in the fabricated FETs and numerical simulations revealed that the change in current values of different FETs were not large enough. Two disjoint levels (groups) of currents with enough separation were not present. Environmental effects (e.g., humidity) could affect the current in a device and cause the bit error if the separation between current levels corresponding to different bit values is not large enough. To address this challenge, we decreased the CNT network density close to the percolation threshold density. So, the channel of FETs may or may not conduct depending on whether the CNT network channel is connected or not. Percolation threshold density (ρ_{th}) is a critical number of CNTs per unit area below which the probability that a CNT network would conduct is very low. Although the CNT length-dependent empirical equation for ρ_{th} can be used to estimate ρ_{th}, the same equation may not be applicable to the finite length of channels. So, numerical simulation or experimental analysis is necessary. To predict the dimensions and CNT network density required for highest randomness, we used numerical simulations because fabrication is costly and time-consuming. Numerical simulation could guide us in selecting the appropriate dimensions and CNT network density before we fabricate the devices. Numerical approach is described in the 'Method' Section under 'Numerical' subheading. In addition, passivation layer of dielectric may help in minimizing the effect of environmental factors and improve stability of the devices. Passivation layer could also be used to hide CNT network from adversary in bottom-gate CNT-FETs.

III. SINGLE-GATE CNT-FET AS PUF

Using numerical simulations, we studied the effect of change in channel length, channel width and CNT density on device current and the probability of any device having a connected channel (non-zero current) or an unconnected channel (zero current). When the CNT network density is significantly higher than the ρ_{th} and the network is very dense, as shown in Fig. 2(a), the probability of having an unconnected device in a random sample-set is negligible and there are very few or no

unconnected devices. Even changing the dimensions of the channel does not increase unconnected devices in the sample. Fig. 2(b) and 2(c) present illustrations of CNT-FETs with unconnected and connected channels, respectively. We associated unconnected devices with a bit-value of '0' and connected devices with a bit-value of '1'. The analytical expression for percolation threshold density, $\rho_{th} = 4.236^2 / \pi L_{CNT}^2$, can be used for the estimation of ρ_{th} for large networks [24, 26, 27]. We performed simulations for different network densities close to ρ_{th} using approximately 2,500 random network devices for each density. Length of the CNTs (L_{CNT}) was maintained at 1 µm in simulations, which is the same as the average length of CNTs in experiments. The value of ρ_{th} for this average length of CNTs will be 5.7 per µm^2. Our simulations showed that most of the networks were not connected at this density for small channel dimensions (e.g., channel length/width of 3-50 µm), which is typically used for the fabrication of CNT-FETs. We selected a CNT network density (D) = 7 per µm^2, which is very close to the ρ_{th} of 5.7 per µm^2 and could be used to have about 50% unconnected devices by considering the channel dimensions of interest (e.g., channel length/width of 3-20 µm). Once the density was fixed, we aimed to achieve almost equal numbers of connected and unconnected devices in any given sample to achieve maximum randomness by varying channel dimensions. Fig. 2(d) presents the percentage of unconnected devices as a function of channel length and width at a CNT network density of 7 per µm^2. At this CNT network density (close to ρ_{th}), increasing the length and decreasing the width will increase the percentage of unconnected devices in any given sample. A device with a channel length close to 6.2 µm and width 3 µm or a channel length close to 11 µm and width 4 µm was observed to be suitable for maximum randomness but the former dimensions are more desirable as size of the device is much smaller.

A widely accepted statistical test suit developed by the National Institute of Standards and Technology (NIST) was used to test the quality of random numbers generated by these CNT-FETs. The proposed PUF design passed all the relevant tests. The NIST Statistical Test Suite is a set of algorithmic tests that attempts to identify sequences of binary numbers that do not behave in a truly random manner. The tests calculate a p-value for every sequence of bits. The p-value represents the probability that the given sequence could have been generated by running a truly random number generator once. Each test passes if the p-value is greater than 0.01 as directed in [28]. Details of the test and its results can be found in the supplementary document (see Section S.1).

IV. MULTI-GATE CNT-FET AS PUF

Next, we are introducing a multi-gate CNT-FET design, where the CNT network channel was divided into multiple sections and each section could be biased with a different gate voltage. The conductivity of any of the sections could be independently changed by changing the applied gate voltage in that section. Thus, the path and magnitude of the current in the device could be controlled. The two important advantages of this device were– (1) we could separate connected devices in two or more groups based on the magnitude of current, and; (2) we could create multiple challenges per device. Thus, we could generate n-ary (n>2) keys, which would have more entropy than binary keys for the same key size. Schematic diagrams of a single-gate CNT-FET and a multi-gate CNT-FET are shown in Fig. 3(a) and 3(b), respectively, to highlight the difference in design and operation of the two devices.

Several different multi-gate channel designs can be useful depending upon the application. We are presenting one such design to demonstrate the concept and the advantages of multi-gate CNT-FETs. In this design, we divided the channel into four rectangular sections of the same size, as shown in the Fig. 3(b). We created two different types of sections, namely a high conductivity section (HCS) and a low conductivity section (LCS). The ratio of conductivity between the HCS and LCS is chosen to be 10^4. Following Fig. 1(d), we chose two gate voltages, one corresponding to an ON state and another to an OFF state, such that the current ON/OFF ratio was 10^4. Thus, HCS and LCS mimicked (corresponds to) sections biased with the ON and OFF state gate voltages, respectively.

We simulated around 1600 devices with different random CNT networks. Each device can have 16 (2^4) different combinations (or configurations) of high conductivity and low conductivity sections in the channel. However, we found that in only six out of 16 configurations it was possible to separate the connected, devices into low current devices (LCDs) and high current devices (HCDs) depending on the magnitude of current (shown in Fig. 4(a)). The remaining configurations could produce only one continuous level of non-zero current and were not useful for ternary keys. As shown in Fig. 4(a), we named these configurations Config-1, Config-2, Config-3, Config-4, Config-5 and Config-6. The black sections represent LCSs and white sections represent HCSs. For example, in Config-1, the two black sections in the lower-half are LCSs and the two upper-half white sections are HCSs. Similarly, LCSs and HCSs in other configurations can be identified in Fig. 4(a). We associated unconnected devices with a bit-value of '0', LCDs with a bit-value of '1' and HCDs with a bit-value of '2'. Thus, we generated a ternary key using one of these configurations. Fig. 4(b) demonstrates representative networks and normalized current distribution generating bit-values of '1' and '2' in multi-gate devices for Config-1, Config-2 and Config-3. An HCD is produced by a random network wherein there are one or more connected paths available and at least one connected path is passing only through higher conductivity sections of the channel. An LCD is produced by a random network where there are one or more connected paths available but does not have even a single path passing exclusively through higher conductivity sections of the channel. In that case, current must pass through the low conductivity section and, therefore, current will be much lower in LCDs compared to HCDs. These two disjoint levels of currents are shown in Fig. 5(a).

The dimensions of sections and channel were chosen such that the probability of producing any of the three bit values is approximately equal to 1/3. An equal distribution of all the bit values corresponds to the maximum possible combinations for

a key of given length. Since the probability of a bit value also depends on configuration, it was not possible to have equal probabilities of bit values in all the six gate configurations simultaneously. Therefore, we chose the dimensions of the device such that the maximum number of configurations has an equal distribution of bit values. We kept the value of CNT network density at 7 per μm^2, same as in the single-gate devices, and selected channel length and width equal to 6.5 µm and 4 µm, respectively. Each of the four channel sections had length and width equal to 3.25 µm and 2 µm respectively. We achieved an approximately equal probability, i.e., close to 33.3%, for all the three bit values in Config-2, Config-3, Config-5 and Config-6 (four out of six configurations) as shown in Fig. 5(b). However, in Config-1 and Config-4, the percentages of bit-values '1' and '2' were close to 45% and 20%, respectively. The increase in bit-value '1' and decrease in bit-value '2' compared to the other four configurations was due to an increase in LCSs compared to the other configurations. For a ternary key with maximum randomness, we can choose one of the four configurations. For example, in a 128-bit ternary key, if all three bit-values are approximately equally distributed, e.g., 42 '0-bit', 43 '1-bit' and 43 '2-bit', then 7.52×10^{58} combinations are possible. However, in a binary key of the same size only 2.40×10^{37} combinations are possible if the bit values are equally distributed. The number of total possible combinations in 128-bit ternary key is 1.18×10^{61} (3^{128}) in comparison to 3.4×10^{38} (2^{128}) of a 128-bit binary key. Thus, ternary keys can significantly increase the possible combinations and randomness level without increasing the size of the key.

Initially, we used only one configuration at a time and were able to generate only ternary keys. Next, we utilized all the six configurations simultaneously as challenges. We were able to generate base-17 (heptadecimal) keys by increasing the total possible combinations and achieved significantly increased randomness in comparison with single challenge multi-gate PUF. Theoretically, each connected device with 'n' different challenges and 'm' current levels can produce m^n different types of outputs. Therefore, a device with six different challenges and two non-zero current levels can produce up to 64 (2^6) different types of outputs e.g., 111222,112121,122111 and so on. For all outputs, the first digit from the left corresponds to the output of Config-1 and the second digit in that order corresponds to the associated output for Config-2 and so on. However, only 16 different types of outputs out of the possible 64 are obtained during simulation, because if Config-2 (or Config-5) and/or Config-3 (or Config-6) rendered bit '1' for a network then Config-1 (or Config-4) would also render bit '1.' This can be understood by the overlap of HCSs in different configurations. For example, if in Config-2 there is no conducting path passing exclusively through HCSs, then Config-1, which has both its HCSs overlapped by two out of three HCSs of Config-2 also produces bit '1'. Fig. 5(c) presents those 16 outputs and their percentage yield in the random sample. Unconnected devices will always have zero current and will, therefore, only produce '0' bit in all the six configurations. Thus, a bit output of '000000' for unconnected devices and 16 different outputs corresponding to the connected devices constitute a total of 17 different outputs in comparison with just 3 outputs, when only one configuration (challenge) was used in multi-gate CNT-FETs. The total number of possible combinations in a 128-bit string is $3.14X10^{157}$ (17^{128}) and the maximum possible combinations if all the states are approximately equally distributed are 3.29×10^{144}. However, in this device design, all the states were not equally distributed, as shown in Fig. 5(c). The number of possible combinations corresponding to this distribution is 1.25×10^{123}, which is significantly larger than the number of possible combinations corresponding to a binary or ternary key of the same length. The calculation details of maximum possible combinations are provided in the supplementary document (see Section S.3). In addition, the entropy generated by these devices can be calculated using the formula:

$$Entropy = -\sum_{i=1}^{N} p_i \log_2(p_i)$$

Here, N is total number of outputs and p_i is the probability of occurrence of the i^{th} output. The entropy generated using single-gate CNT-FETs is 1 bit per device, whereas entropy generated using multi-gate CNT-FETs is 3.47 bits per device for the output distribution shown in Fig. 5. It implies that we need only 'n/3.47' multi-gate devices to generate an n-bit long key, whereas we need 'n' single-gate devices to generate an n-bit long key. The maximum entropy of 4.09 bits per device can be achieved using multi-gate CNT-FETs when all the outputs are equally distributed. Channel area of the single-gate device was 18.6 μm^2 and the multi-gate device was 26 μm^2. But, the total device area is a sum of channel, source, drain and gate area. The source, and drain area constitute a significant proportion of the total area and render the increase in channel area of the multi-gate devices compared to single-gate devices insignificant. The gain in entropy is achieved without any consequential increase in the device area.

For purposes of statistical study and demonstrating capability of simulator to generate random network, we also calculated normalized Inter Hamming Distance for binary and ternary strings produced by single-gate and multi-gate devices respectively. Normalized Inter Hamming Distance is a ratio of the number of positions with different bit values in two different strings of equal length divided by string length (see Section S.2 of supplementary document). It signifies the fraction of corresponding bit positions with different bit values in any two keys. For reasonably long keys (e.g., 64-bit, 128-bit), Inter Hamming Distance for binary keys should be close to 0.5, and for ternary keys it should be close to 0.667 indicating optimal unpredictability and inter-device uniqueness (see Section S.2 of supplementary document). We selected two reasonable key lengths–64-bit and 128-bit–to produce binary and ternary strings from 2560 single-gate and 1600 multi-gate devices, respectively. Fig. 6 presents the distribution of Inter Hamming Distance between strings. For binary strings produced by single-gate devices, Inter Hamming Distances for a 64-bit string are 0.501 with a standard deviation of 0.063. For a 128-bit string it is 0.500 with a standard deviation of 0.045. This means that 99.73% of the time, any two keys generated by multi-gate

devices will have different bit values in at least 31.2% and at most 69% of the bit positions for 64-bit keys and in at least 36.5% and at most 63.5% of the positions for 128-bit keys. For ternary strings produced by multi-gate devices in Config-5, Inter Hamming Distances are 0.665 with a standard deviation of 0.061 for a 64-bit string and 0.666 with a standard deviation of 0.043 for a 128-bit string. This means 99.73% of the time any two keys generated by multi-gate devices will have different bit values in at least 48.2% and at most 84.8% of the bit positions for 64-bit keys and in at least 53.7% and at most 79.5% of the positions for 128-bit keys.

In this study, we have presented a multi-gate design with only 4 sections having equal dimensions in the channel. There is scope to increase possible combinations and entropy for a fixed array length by increasing the total number of sections in the channel. A higher number of sections can increase the number of challenges in a single device and can enable the creation of more states. In addition, uniform distribution of all states in a bit array will also increase the total number of combinations and entropy, which can be easily controlled by changing the dimensions of the channel and its different sections. Therefore, in future, we aim to investigate the effect by increasing the number of gates per device, gates of different shape and dimensions on the entropy generated per device. In addition, we are working on fabrication of multi-gated CNT-FETs with four gates.

V. Conclusion

We have proposed the design of multi-gate CNT-FET based PUF in this study. An appropriate selection of CNT network channel density and dimensions for the devices enabled us to generate random bit arrays. Single-gate devices with network density close to percolation threshold density produced binary keys. We introduced multi-gate devices, which can have multiple challenges and generate multiple types of outputs. We generated ternary and base-17 (hepta-decimal) keys by using these devices. This study shows that multi-gate CNT-FETs with networks of density close to percolation threshold density can be promising in producing low-cost and high-quality cryptographic primitives.

VI. Methods

A. Numerical

The channel lengths (L_c) of the CNT-FETs studied in this paper were larger than CNT lengths (L_{CNT}). Therefore, numerical analysis of electrical transport in CNT-FETs was based on modified Poisson's and Drift-Diffusion equations [29-32]. Detailed description and assumptions of the model are also available in the literature, where it has been compared and validated with the measurements [24, 29, 30, 33]. The method used to generate random CNT network is also described in [29]. However, for the sake of completeness, we briefly explain the model here as well. The following equations were used to predict current and potential distribution in CNT-FETs.

$$\frac{d^2\psi_i}{ds^2} + \frac{\rho_i}{\varepsilon} - \frac{(\psi_i - V_G)}{\lambda^2} + \sum_{j\neq i} \frac{(\psi_j - \psi_i)}{\lambda_{ij}^2} = 0 \quad (1)$$

$$\nabla . J_{pi} + \sum_{j\neq i} C_{ij}^{p} (p_j - p_i) = 0 \quad (2)$$

$$\nabla . J_{ni} + \sum_{j\neq i} C_{ij}^{n} (n_j - n_i) = 0 \quad (3)$$

The first equation is a modified version of Poisson's equation. Here, ψ_i represents electrostatic potential along i^{th} CNT, ρ is the total charge density, ε is permittivity of CNT and V_G is gate voltage. The third and fourth terms on the left-hand side of Poisson's equation account for CNT-Gate voltage interaction and CNT-CNT interactions respectively, where λ and λ_{ij} are screening lengths. "s" is the length along CNT. The next two equations are Carrier Continuity equations for hole and electrons. Here, J is current density and p and n are hole and electron charge density respectively. The second terms on the left-hand sides of these equations account for hole or electron charge transfer across CNT-CNT at junctions. The numerical values of various parameters are chosen based upon previous studies, where experimental validation was also performed.

B. Experimental

Single-gate CNT-FETs were fabricated using photolithography and lift-off processes at the Institute for Electronics and Nanotechnology (IEN) cleanroom at Georgia Tech. First, Ti and Au layers were deposited as gate electrodes on top of a Si wafer through e-beam evaporation with thickness of 5nm and 50nm, and a deposit rate of 0.2 Å/s and 1 Å/s, respectively. These contacts were patterned in the channel area (between source and drain) to work as back gate. Second, 1.5 nm thick TiO_2 (15 cycles) and 75nm thick HfO_2 (600 cycles) were deposited using atomic layer deposition (ALD), covering the entire wafer surface as a global gate dielectric layer. Before growing a thin film layer of CNT networks, 15~30 seconds of oxygen plasma treatment was indispensable to make the surface hydrophilic. This was followed by 5~15 min of CNT growth by immersing the treated wafer into 0.005-0.01 g/L toluene-based CNT solution (CNT source: >99.9% purity polymer-wrapped CNT solution from NanoIntegris). The resulting CNT network density is a function of both deposition time and CNT solution concentration. Then, Ti and Au pattern with thickness of 5nm and 50nm were defined as the source and drain (S/D) electrodes by photolithography and lift-off processes. This was followed by another photolithography and 30s of oxygen plasma treatment to form the channel area by etching away unwanted parts of the CNT networks. At last, vacuum annealing was performed at 250°C for 2 hours to get rid of surface residue off the wafer.

Electronic Supplementary Information

Supplementary document contains NIST statistical test results, normalized inter hamming distance details, combinations calculations and figures of other possible configuration in multi-gate CNT-FETs and representative networks in Cofig-4, Config-5 and Config-6 generating bit-values '1' and '2'.

REFERENCES

[1] A. K. Lenstra, J. P. Hughes, M. Augier, J. W. Bos, T. Kleinjung, and C. Wachter, "Ron was wrong, Whit is right," 2012, Available: http://eprint.iacr.org/2012/064.

[2] N. Heninger, Z. Durumeric, E. Wustrow, and J. A. Halderman, "Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices."

[3] H. Bar-El, H. Choukri, D. Naccache, M. Tunstall, and C. Whelan, "The Sorcerer's Apprentice Guide to Fault Attacks," *Proceedings of the IEEE*, vol. 94, no. 2, pp. 370-382, 2006.

[4] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," in *Advances in Cryptology — CRYPTO' 99: 19th Annual International Cryptology Conference Santa Barbara, California, USA, August 15–19, 1999 Proceedings*, M. Wiener, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 388-397.

[5] P. C. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems," in *Advances in Cryptology — CRYPTO '96: 16th Annual International Cryptology Conference Santa Barbara, California, USA August 18–22, 1996 Proceedings*, N. Koblitz, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1996, pp. 104-113.

[6] S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola, and V. Khandelwal, "Design and Implementation of PUF-Based "Unclonable" RFID ICs for Anti-Counterfeiting and Security Applications," in *2008 IEEE International Conference on RFID*, 2008, pp. 58-64.

[7] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "FPGA Intrinsic PUFs and Their Use for IP Protection," in *Cryptographic Hardware and Embedded Systems - CHES 2007: 9th International Workshop, Vienna, Austria, September 10-13, 2007. Proceedings*, P. Paillier and I. Verbauwhede, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 63-80.

[8] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," presented at the Proceedings of the 44th annual Design Automation Conference, San Diego, California, 2007.

[9] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical One-Way Functions," *Science*, vol. 297, no. 5589, pp. 2026-2030, 2002.

[10] L. Daihyun, J. W. Lee, B. Gassend, G. E. Suh, M. v. Dijk, and S. Devadas, "Extracting secret keys from integrated circuits," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 13, no. 10, pp. 1200-1205, 2005.

[11] B. Gassend, D. Lim, D. Clarke, M. van Dijk, and S. Devadas, "Identification and authentication of integrated circuits," *Concurrency and Computation: Practice and Experience*, vol. 16, no. 11, pp. 1077-1098, 2004.

[12] J. Das, K. Scott, S. Rajaram, D. Burgett, and S. Bhanja, "MRAM PUF: A Novel Geometry Based Magnetic PUF With Integrated CMOS," *IEEE Transactions on Nanotechnology*, vol. 14, no. 3, pp. 436-443, 2015.

[13] B. Gassend, D. Clarke, M. v. Dijk, and S. Devadas, "Silicon physical random functions," presented at the Proceedings of the 9th ACM conference on Computer and communications security, Washington, DC, USA, 2002.

[14] P. Tuyls, G.-J. Schrijen, B. Škorić, J. van Geloven, N. Verhaegh, and R. Wolters, "Read-Proof Hardware from Protective Coatings," in *Cryptographic Hardware and Embedded Systems - CHES 2006: 8th International Workshop, Yokohama, Japan, October 10-13, 2006. Proceedings*, L. Goubin and M. Matsui, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 369-383.

[15] D. E. Holcomb and K. Fu, "Bitline PUF: Building Native Challenge-Response PUF Capability into Any SRAM," in *Cryptographic Hardware and Embedded Systems – CHES 2014: 16th International Workshop, Busan, South Korea, September 23-26, 2014. Proceedings*, L. Batina and M. Robshaw, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 510-526.

[16] D. Suzuki and K. Shimizu, "The Glitch PUF: A New Delay-PUF Architecture Exploiting Glitch Shapes," in *Cryptographic Hardware and Embedded Systems, CHES 2010: 12th International Workshop, Santa Barbara, USA, August 17-20, 2010. Proceedings*, S. Mangard and F.-X. Standaert, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 366-382.

[17] D. Akinwande, N. Petrone, and J. Hone, "Two-dimensional flexible nanoelectronics," *Nature Communications*, Review Article vol. 5, p. 5678, 12/17/online 2014.

[18] E. Artukovic, M. Kaempgen, D. S. Hecht, S. Roth, and G. Grüner, "Transparent and Flexible Carbon Nanotube Transistors," *Nano Letters*, vol. 5, no. 4, pp. 757-760, 2005/04/01 2005.

[19] Q. Cao *et al.*, "Medium-scale carbon nanotube thin-film integrated circuits on flexible plastic substrates," *Nature*, 10.1038/nature07110 vol. 454, no. 7203, pp. 495-500, 07/24/print 2008.

[20] S. Park, M. Vosguerichian, and Z. Bao, "A review of fabrication and applications of carbon nanotube film-based flexible electronics," *Nanoscale*, 10.1039/C3NR33560G vol. 5, no. 5, pp. 1727-1752, 2013.

[21] K. Bradley, J.-C. P. Gabriel, and G. Grüner, "Flexible Nanotube Electronics," *Nano Letters*, vol. 3, no. 10, pp. 1353-1355, 2003/10/01 2003.

[22] Z. Hu *et al.*, "Physically unclonable cryptographic primitives using self-assembled carbon nanotubes," *Nat Nano*, Article vol. 11, no. 6, pp. 559-565, 06//print 2016.

[23] S. T. C. Konigsmark, L. K. Hwang, D. Chen, and M. D. F. Wong, "CNPUF: A Carbon Nanotube-based Physically Unclonable Function for secure low-energy hardware design," in *2014 19th Asia and South Pacific Design Automation Conference (ASP-DAC)*, 2014, pp. 73-78.

[24] N. Pimparkar, "Nonlinear Electronic and Photovoltaic Characteristics of Nanonet Transistors and Solar Cells," PhD Dissertation, Electrical and Computer Engineering, Purdue University, West Lafayette, IN, USA, 2008.

[25] R. V. Seidel *et al.*, "Bias dependence and electrical breakdown of small diameter single-walled carbon nanotubes," *Journal of Applied Physics*, vol. 96, no. 11, pp. 6694-6699, 2004.

[26] G. E. Pike and C. H. Seager, "Percolation and conductivity: A computer study. I," *Physical Review B*, vol. 10, no. 4, pp. 1421-1434, 08/15/ 1974.

[27] I. Balberg and N. Binenbaum, "Computer study of the percolation threshold in a two-dimensional anisotropic system of conducting sticks," *Physical Review B*, vol. 28, no. 7, pp. 3799-3812, 10/01/ 1983.

[28] A. Rukhin *et al.*, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," 2010.

[29] S. Kumar, J. Y. Murthy, and M. A. Alam, "Percolating Conduction in Finite Nanotube Networks," *Physical Review Letters*, vol. 95, no. 6, p. 066802, 08/01/ 2005.

[30] S. Kumar, N. Pimparkar, J. Y. Murthy, and M. A. Alam, "Theory of transfer characteristics of nanotube network transistors," *Applied Physics Letters*, vol. 88, no. 12, p. 123505, 2006.

[31] C. J. Lobb and D. J. Frank, "Percolative conduction and the Alexander-Orbach conjecture in two dimensions," *Physical Review B*, vol. 30, no. 7, pp. 4090-4092, 10/01/ 1984.

[32] D. J. Frank and C. J. Lobb, "Highly efficient algorithm for percolative transport studies in two dimensions," *Physical Review B*, vol. 37, no. 1, pp. 302-307, 01/01/ 1988.

[33] N. Pimparkar, Q. Cao, S. Kumar, J. Y. Murthy, J. Rogers, and M. A. Alam, "Current–Voltage Characteristics of Long-Channel Nanobundle Thin-Film Transistors: A “Bottom-Up” Perspective," *IEEE Electron Device Letters*, vol. 28, no. 2, pp. 157-160, 2007.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2838580, IEEE Internet of Things Journal

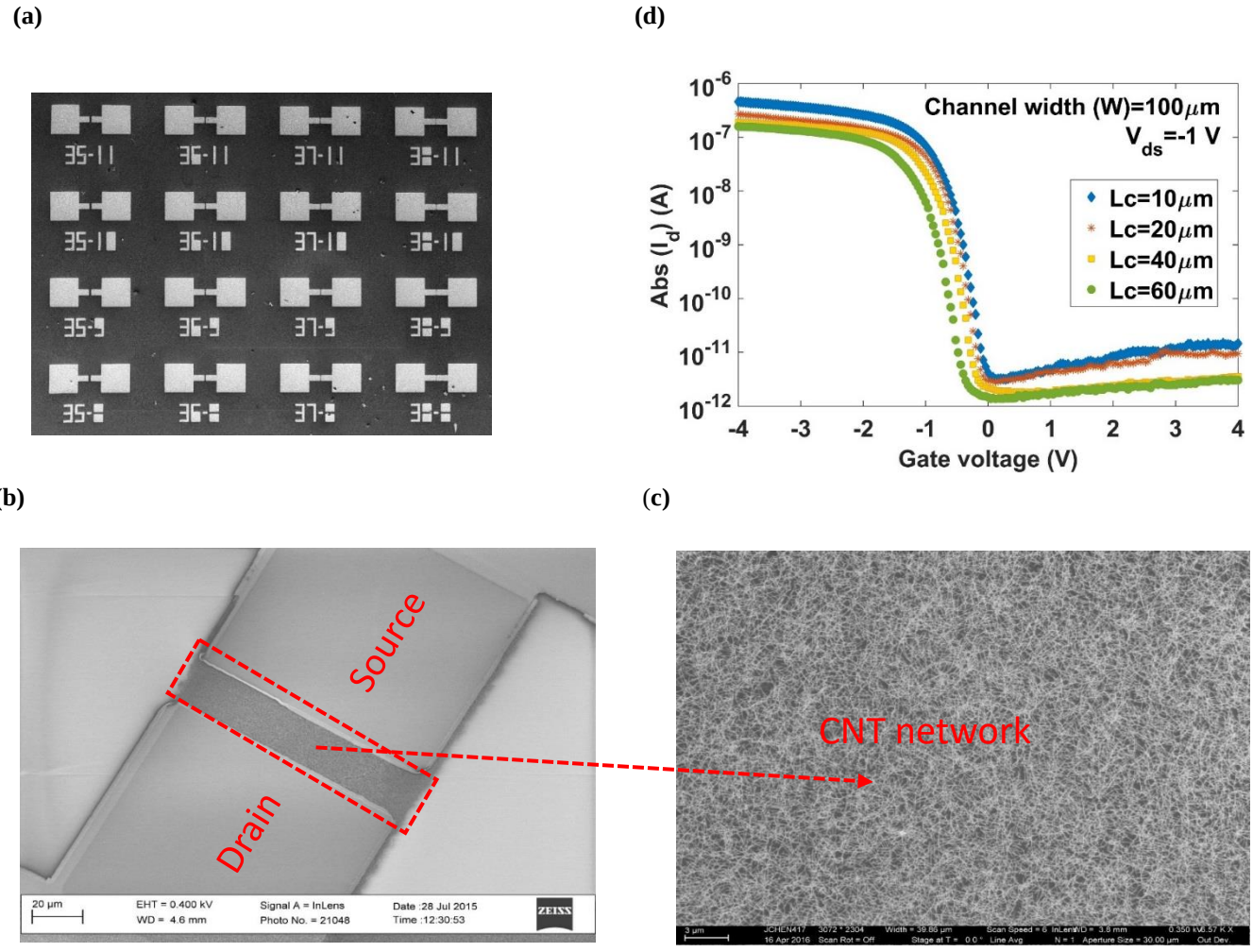

Fig. 1. Fabricated single-gate CNT-FETs. (a) SEM images of the devices fabricated using Georgia Tech's IEN cleanroom facilities. (b) Zoomed-in view of a single-gate CNT-FET. (c) Random CNT network in channel. (d) Transfer characteristics of single-gate CNT-FETs for various channel lengths at V_{ds} = -1 V; channel width = 100 μm.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2838580, IEEE Internet of Things Journal

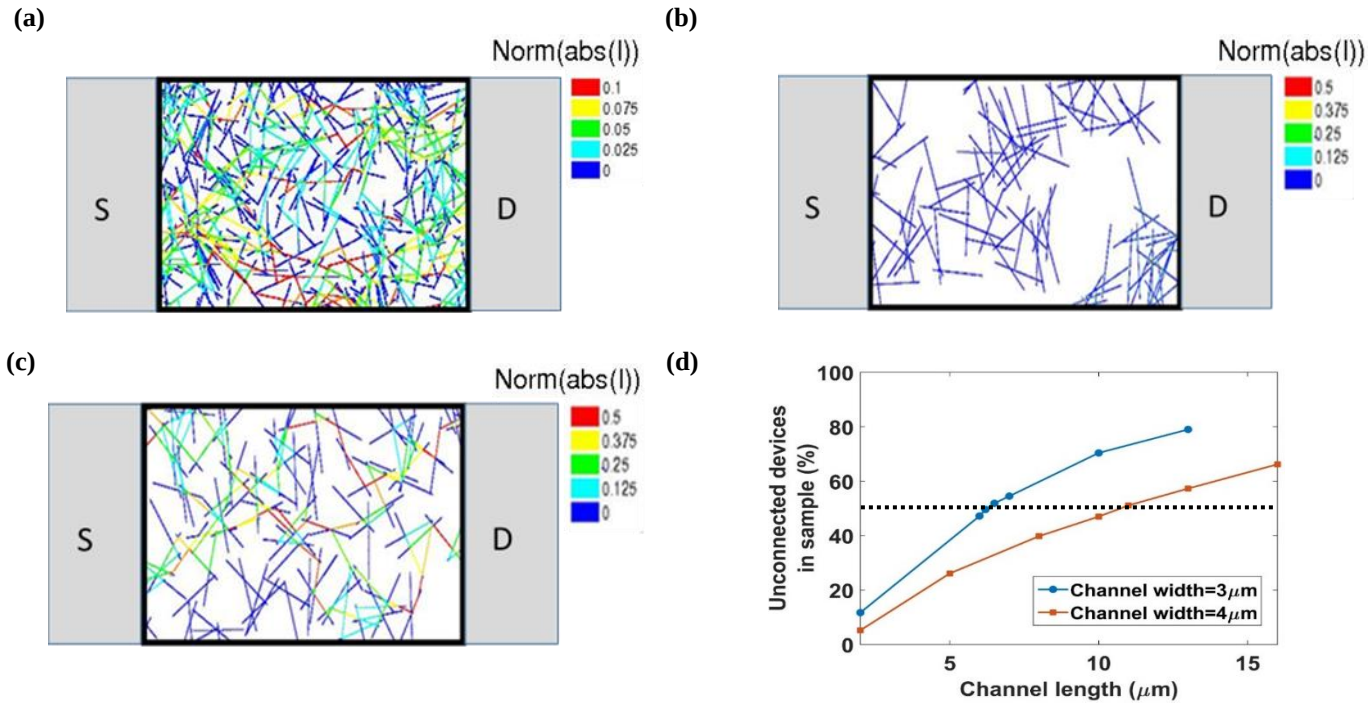

Fig. 2. Network Connectivity in single gate CNT-FETs. (a) A high-density connected network in a CNT-FET. (b) A FET channel with unconnected CNT network (zero current), (c) A FET channel with connected CNT network. Network is generated using same CNT density as in (b). Normalized absolute currents in the channels are also shown for these figures. (d) Percentage of unconnected networks in CNT-FETs with respect to channel length for channel width of 3 μm and 4 μm. Samples are randomly generated with a density of 7 μm^{-2}. Dashed horizontal line corresponds to 50% unconnected devices.

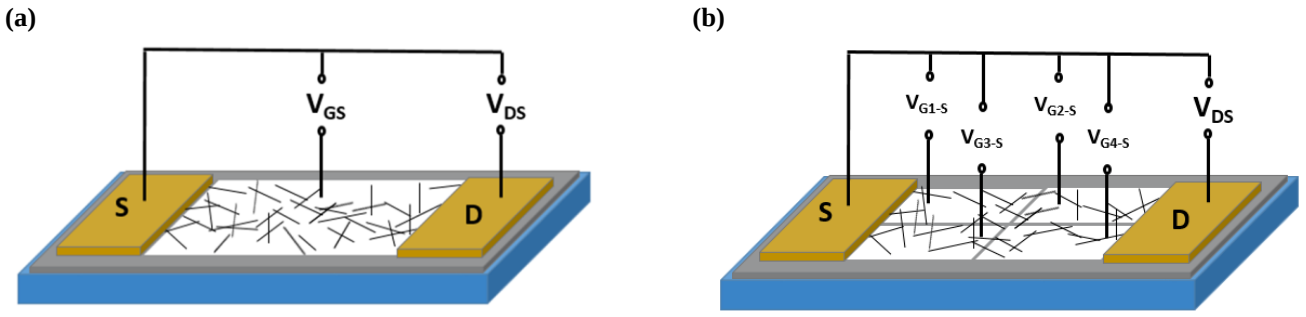

Fig. 3. Comparison between single gate CNT-FETs and multi-gate CNT-FETs. (a) A schematic diagram of single-gate CNT-FET. (b) A schematic diagram of multi-gate CNT-FET.

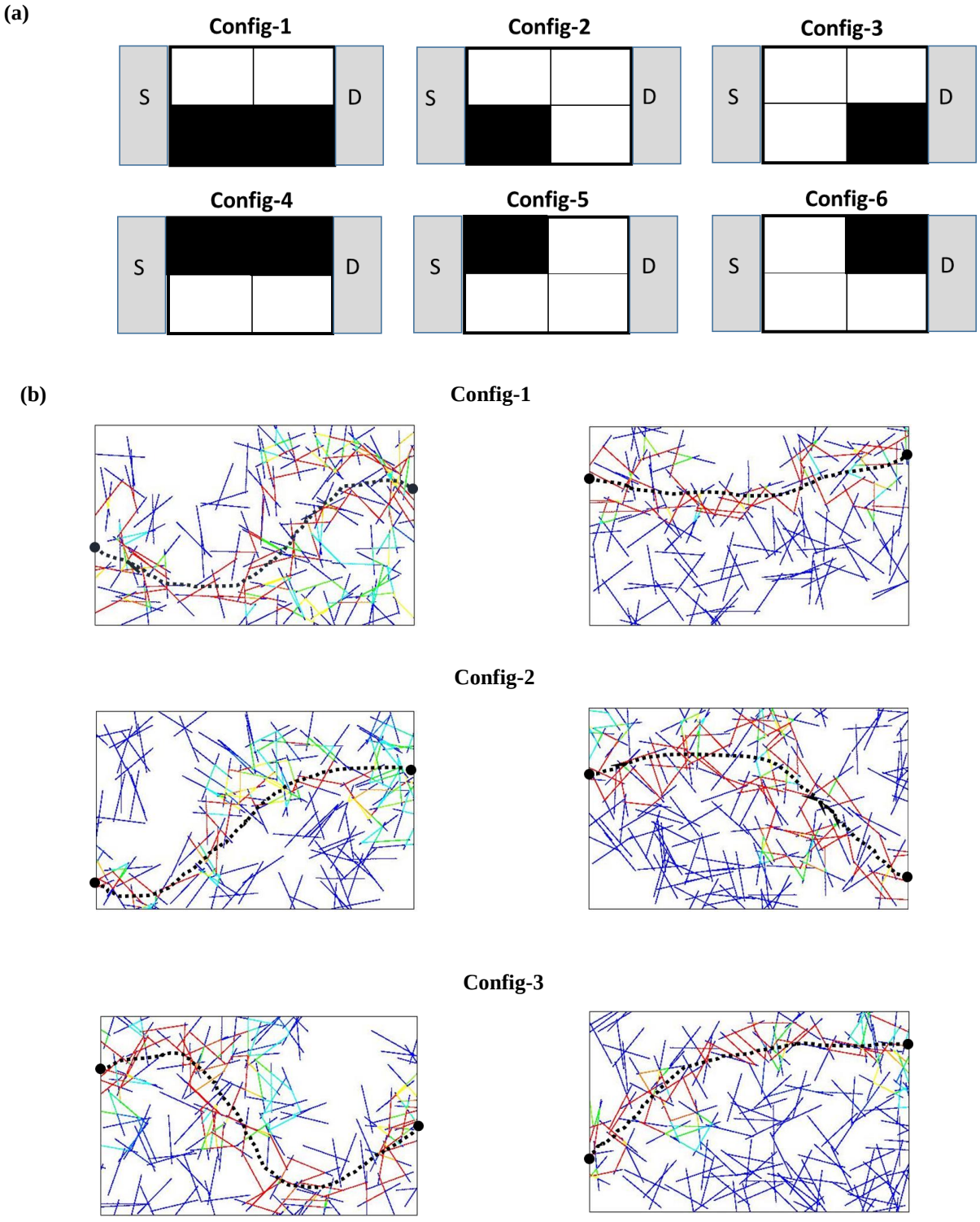

Fig. 4. Multi-gate CNT-FETs. (a) Six different configurations useful in generating ternary bits and creating 6 different challenges per device. HCSs and LCSs of the channel are represented by white and black colors respectively. Configurations in the top row are named Config-1, Config-2, and Config-3 (from left to right) and in the bottom row are named Config-4, Config-5, and Config-6 (from left to right) respectively. (b) Representative networks and normalized absolute currents for three configurations: Config-1, Config-2, and Config-3; bit value '1' (left image) and '2' (right image).

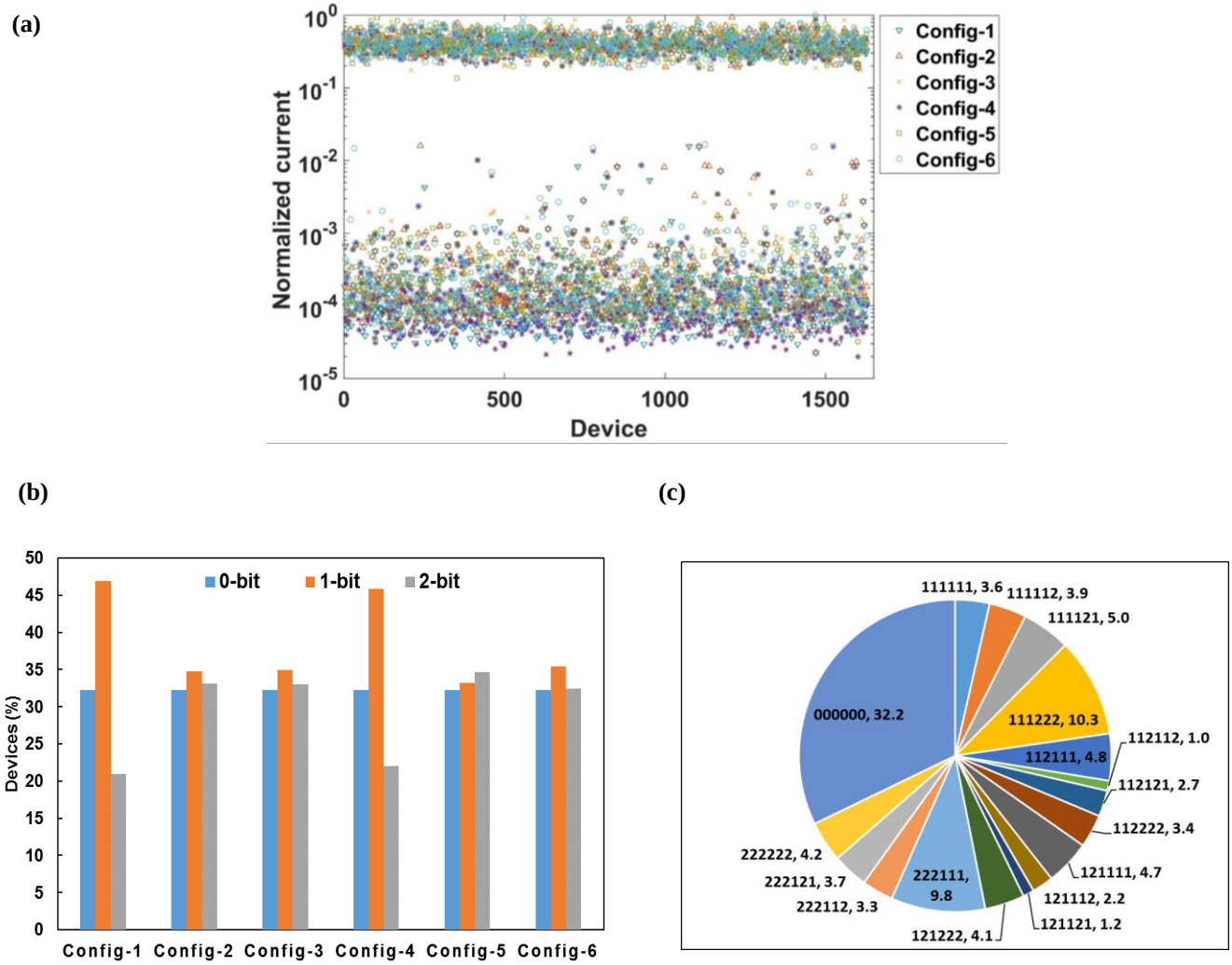

Fig. 5. Multi-gate CNT-FETs. (a) Two disjoint levels of non-zero currents associated with bit-value '1' and '2' in all six configurations generated by connected devices. Third current level associated with bit-value '0' corresponds to 'zero current' generated by unconnected devices. Zero current devices could not be shown on logarithmic scale. CNT networks are randomly generated in the channel region of FETs and current is obtained from the device simulations (b) Percentage of devices with bit values (0, 1 and 2) produced by different configurations of multi-gate CNT-FETs. (c) Percentage yield of different possible composite states produced in around 1600 four-gated CNT-FETs whose networks are randomly sampled. First value represents unique composite output state and second value represents corresponding yield. Each CNT-FET is tested for six gate configurations shown in Figure 4(a). The digits from left to right in six-bit string (composite output state) correspond to the output states (0, 1 or 2) for gate Config-1 to Config-6.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2838580, IEEE Internet of Things Journal

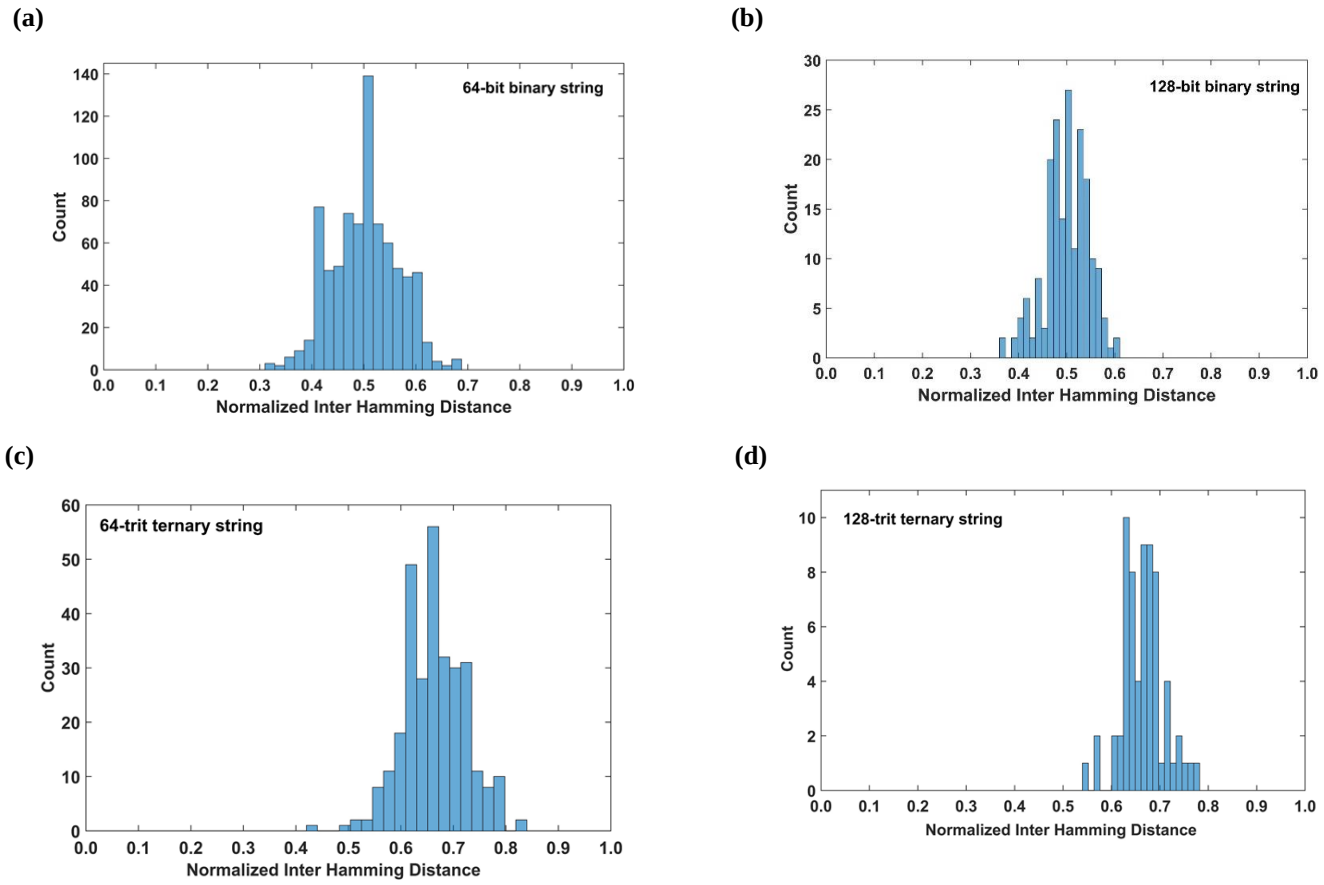

Fig. 6. Histograms of Normalized Inter Hamming Distance for single-gate and multi-gate devices. (a) 64-bit binary string generated by single-gate devices. (b) 128-bit binary string generated by single-gate devices. (c) 64-bit ternary string generated by multi-gate devices. (d) 128-bit ternary string generated by multi-gate devices.