Twin physically unclonable cryptographic primitives enabled by aligned carbon nanotube arrays

Zhiyong Zhang (zyzhang@pku.edu.cn)
Peking University https://orcid.org/0000-0003-1622-3447
Donglai Zhong
zzatnjuphy@163.com
Jingxia Liu
Peking university
Mengmeng Xiao
Peking University
Yunong Xie
rowenia@163.com
Huiwen Shi
Peking University
Lijun Liu
imec https://orcid.org/0000-0002-3070-3204
Chenyi Zhao
Peking University
Li Ding
Peking University
Lian-Mao Peng
Peking University https://orcid.org/0000-0003-0754-074X

Article

Keywords: twin physically unclonable functions, secure communication, non-volatile memory, aligned carbon nanotube arrays

Posted Date: August 16th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-702485/v1

Version of Record: A version of this preprint was published at Nature Electronics on July 4th, 2022. See the published version at https://doi.org/10.1038/s41928-022-00787-x.

Abstract

Handling the explosion of massive data not only requires significant improvements in information processing, storage and communication abilities of hardware but also demands higher security in the storage and communication of sensitive information. As a type of hardware-based security primitives, physically unclonable functions (PUFs) represent a promising emerging technology utilizing random imperfections existing in a physical entity, which cannot be predicted or cloned. However, if a PUF is exploited to carry out secure communication, the keys inside it must be written into non-volatile memory and then shared with other participants that do not hold the PUF, which makes the keys vulnerable. Here, we show that identical PUFs, e.g. twin PUFs can be fabricated on the same aligned carbon nanotube arrays and optimized to yield excellent uniformity, uniqueness, randomness, and reliability. The twin PUFs show a good consistency of approximately 95 % and are used to demonstrate secure communication with a bit error rate reduced to one trillion through a fault-tolerant design. As a result, our twin PUFs offering a convenient, low-cost and reliable new technology for guarantee information exchange security.

Introduction

In the era of the Internet of Things (IoT), the omnipresent smart devices and human-machine interactions have created an explosion of massive data, which not only demands significant improvements in the handling, storage and communication abilities of hardware but also requires higher security in the storage and communication of personal or sensitive information[1, 2]. Classical cryptography depends on cryptographic algorithms and secret keys to authenticate the electronic devices and encrypt or decrypt the information[3]. The most popular technique for secure communication is RSA encryption, first introduced by Rivest, Shamir, and Adleman in 1978[4]. Factoring a large number with hundreds of digits is extremely difficult for a classical computer, which is the theoretical basis of RSA encryption, but this task has been proven to be accomplishable in polynomial time using a quantum computer[5]. Another strategy is to use random number generators (RNGs) to generate secret keys and then store them for a long time in non-volatile memory, such as erasable programmable read-only memory (EPROM) or static random-access memory (SRAM), for use at any time. Unfortunately, the stored keys are vulnerable to physical and side-channel attacks by observing consumed power or emitted radiation[6, 7] and can thus be revealed to the adversary. Quantum key distribution exploits the quantum theory that the process of measuring a quantum system disturbs the system, which exhibits higher security than classical methods[8, 9], but this technology demands very expensive equipments, e.g., satellites and true single-photon sources[10, 11].

As a type of hardware-based security primitive, physically unclonable functions (PUFs), called physical one-way functions early on[12], represent a promising emerging technology that allows secret keys to be immediately extracted from a reliable and random physical system rather than stored in non-volatile memory[13-15]. The basic idea of PUFs is to utilize random physical imperfections existing in a physical entity caused by the fabrication process variations at a small scale, and these imperfections cannot be predicted or cloned, even by the original manufacturer[16, 17]. Simply, each PUF can be regarded as a

unique and unclonable black-box challenge-response system[13]. In 2002, Rappu et al. first introduced optical PUFs using a laser beam with selected angle and point of incidence as a challenge that goes through a 3D scattering medium to generate a unique speckle pattern as the response[12]. Compared with optical PUFs, electronic PUFs based on electrical properties are preferred owing to their simple connection to key-readout circuits. Conventional silicon (Si) PUFs[18-20], including delay-based PUFs and memory-based PUFs, exploit process variation-induced device and connection mismatches, such as random dopant fluctuations and line edge roughness, which can be easily disturbed by noise. Several nanotechnology-based PUFs, including memristors, using MoS_2 and carbon nanotubes (CNTs), have been demonstrated to be more reliable than conventional Si PUFs[21-28]. Recently, Hu et al. used solution-derived CNTs randomly self-assembled into HfO_2 trenches with a yield dependent on the trench dimensions to demonstrate reliable physically unclonable cryptographic primitives with high immunity to electronic noise (such as supply voltage variations) and environmental (such as temperature) variations[27, 28]. Unclonability ensures that a PUF is very safe since predicting or cloning it is impossible. If a PUF is exploited to carry out secure communication, then the keys inside must be written into non-volatile memory and then shared with other participants that do not hold the PUF[29-31], which makes the keys vulnerable. Therefore, how to clone a PUF or make two identical PUFs is highly desired. Furthermore, mainly owing to recent developments in solution-derived CNT materials[32], great progress has been achieved in CNT-based CMOS field-effect transistors (FETs) and integrated circuits (ICs)[32-35]. Wafer-scale fabrication of CMOS FETs even on an 8-inch wafer[33, 35], high-speed ICs including ring oscillators (ROs) with oscillation frequency up to 8 GHz[32,33], and large-scale digital ICs including a 16-bit MCU consisting of 14000 transistors[34] have been realized on highly semiconducting CNT films, and the feasibility and potential of CNT-based ICs have been demonstrated. Considering the security of CNT ICs in future electronics applications, developing a PUF technology compatible with CMOS ICs based on CNT films is necessary.

In this work, we first demonstrate that pairs of identical PUFs can be fabricated based on chemical vapor deposition (CVD)-grown aligned CNT arrays, and be used for secure communication without key pre-extraction and storage. We name these pairs of identical PUFs “twin PUFs” (as illustrated in Fig. 1), which offer a convenient, low-cost and reliable technology that maintains information exchange security. We use iron (Fe) nanoparticles as catalyst to grow well-aligned CNT arrays on single-crystal quartz substrates[36]. Ideally the characteristics of CNT arrays, including chirality and position, are random in nature perpendicular to the CNT growth direction and identical along the growth direction. Depending on the electrical properties of fabricated back-gate FETs on CNT arrays, three types of FETs are obtained with (1) metallic, (2) semiconducting and (3) no CNTs in the channel (or open channel). As a result, ternary bits can be extracted and used as the secure keys from these CNT FETs. Through simulation and optimization of the purity and device dimensions, the ternary bits are tuned to have maximum randomness. Our PUFs show high uniformity, uniqueness, randomness, unpredictability, and reliability. In particular, twin PUFs show a good consistency of approximately 95 %, which is far higher than the consistency of two independent PUFs of approximately 35 %. Finally, twin PUFs are successfully applied

to demonstrate simple secure communication, and the bit error rate (BER) introduced during the encryption/decryption process can be reduced to one trillion through a fault-tolerant design.

Fabrication Of Cnt Twin Pufs

Well-aligned CNT arrays were CVD-grown on ST-cut quartz substrates using Fe nanoparticles as catalyst (Fig. S1). Deposited via electron beam evaporation (EBE), the Fe nanoparticles in the catalyst stripes were randomly positioned and had different sizes owing to the statistical nature of the EBE process. In addition, the nucleation through the vapor-liquid-solid processes (VLS) is also stochastic; therefore, CNT arrays were randomly distributed perpendicular to the growth direction defined by the gas flow in terms of both chirality and position (Figs. S2 and S3), which is highly unwanted for high-performance electronics applications[37-39]. As shown in Fig. 1a, FETs fabricated on such CNT arrays have three distinct channel types with no CNTs or open channel (O), with pure semiconducting CNTs (S) and with at least one metallic CNT (M). These different channel types lead to distinguishable electronic characteristics, i.e. O channel with very low current, conducting channel with large current on/off ratio (S channel) and small on/off ratio (M channel with metallic CNT). Since the location and type of CNTs in the channel are determined by the stochastic nucleation and random catalyst distribution, FETs fabricated on the CNT arrays (defined by the source/drain contacts) will show O, S, and M characteristics in a random manner perpendicular to the growth direction. The random nature neither predictable unclonable; therefore, in principle one row of FETs meets the requirement of PUFs. Induced by the quartz lattice-CNT interaction[40], CNT arrays grew along the [2 -1 -1 0] crystal orientation for several hundred microns[41], which ensured that the properties of CNT arrays were identical parallel to the growth direction. As shown in Fig. 1b, two rows of FETs fabricated in parallel on the same CNT array show O, S, and M types with the same order, so two identical PUFs can be fabricated together.

To fabricate FETs, CNT arrays were transferred using PMMA as a medium to the target Si/SiO_2 substrate before device fabrication[42], and the substrate served as the global back gate to measure the transfer characteristic characteristics. Pd films were deposited as the source/drain contacts to form p-type FETs with a channel length (L_{ch}) of 1 μm and variable channel width (W_{ch}) controlled by the contact width and etched area, as shown in Fig. 2a. The test units of CNT twin PUFs were designed to be 2×24 or 24 pairs of FETs with an equal spacing of 5 μm, and all FETs were connected to peripheral on-chip pads, as shown in Fig. 2b and Fig. S4. According to the patterned catalyst stripes with a 0.25 mm distance and the pad settings, the test units were batch fabricated in the form of a matrix with a 0.5 mm distance (Fig. 2c and Fig. S4).

We measured the transfer characteristics of three typical pairs of FETs in a test unit with a drain-to-source voltage (V_{ds}) of -1.0 V (Fig. 2d). The FETs with no CNTs in the channel exhibited an on-state current (I_{on}) below 1 pA, while the FETs with CNTs in the channel showed an I_{on} far above 1 μA. Among conducting FETs, the FETs with only semiconducting CNTs showed an on/off ratio of up to 6 decades, while those having at least one metallic CNT showed an on/off ratio of less than 10. Because they were fabricated on

the same CNT array, those FETs pairs with the same order from the two rows of FETs showed transfer characteristics that almost coincide, indicating that they were identical. Five hundred FETs on CNT arrays were readily classified into these three types of O, S and M devices according to their extracted on state current I_{on} and current on/off ratio, by defining O-type FETs be the one with I_{on} below 0.1 nA, S-type FETs with I_{on} above 0.1 nA and an on/off ratio greater than 50, and M-type FETs with I_{on} above 0.1 nA and an on/off ratio of less than 100 (Fig. 2e and Fig. S5)

To utilize CNT PUFs to generate ternary bits and thus keys with maximum randomness and entropy, O-, S- and M-type FETs should be tuned to have an equal occurrence probability of 1/3, which is realized by tuning the CNT arrays density and FET channel width W_{ch} . As shown in Fig. 2f, we extracted CNT positions from SEM images of CNT arrays and then calculated the tube-to-tube spacing (CNT pitch). Through statistical distribution fitting, the CNT pitches (CPs) were found to meet the lognormal distribution, which was verified by other CNT samples we grew with different densities and those published by other groups[38, 43] (Fig. 2g and Fig. S6). According to the simulation with a CP of 1±0.5 μm and an ideal metallic/semiconducting CNT ratio (MSR) of 1/2, Fig. 2h shows that the ratio of O-type FET decreases and M-type FETs increases with increasing W_{ch}, while the ratio of S-type FET first increase and then decrease (see also Fig. S4). The nonmonotonic change in the ratio of S-type FETs results from the fact that the possibility of metallic CNTs appearing in the S-type channel increases rapidly when W_{ch} exceeds 1 μm, which effectively turns the S-type FET into a M-type FET (Fig. S7).

We define the minimal difference (MD) as the sum of the square difference between the ratios of O-, S- and M-type FETs, and assume an ideal value (1/3) for given CP and MSR to maximize randomness. When W_{ch} is set to 0.8 μm, MD is 0.03, with O, S, and M ratios of 0.4, 0.4 and 0.2; therefore, the ratio of S-type FETs needs to be decreased, which can be realized by two strategies. One is to increase the MSR to increase M-type FETs (Fig. S8), and the other is to increase the deviation in the CP to increase mixed FETs (Fig. S9). The MSR can be adjusted by many factors, including catalyst, carbon source, atmosphere, and electromagnetic field[44, 45], while CP is mainly determined by the distribution of Fe nanoparticles. Through co-optimization of CP and MSR, MD is reduced down to 10^{-4} (Fig. S10). Finally, CNT arrays with a CP of 0.65±0.58 μm and an MSR of approximately 0.4 (Fig. S11) were selected to demonstrate CNT twin PUFs with ideal ternary bits, and the experimental result is in good agreement with simulation (Fig. 2h). A total of 1600 FETs with a W_{ch} of 600 nm were fabricated to generate a 40×40 ternary bit map (Fig. 2i), in which 532, 516, and 552 O-, S- and M-bits were counted, respectively.

Security And Reliability Performance Of Cnt Pufs

High-quality PUFs should be uniform, unique, and reliable[46-47], and when applied to cryptography applications, randomness and unpredictability are also indispensable[48]. The optimized ternary bit distribution showed that the three types of FETs have occurrence probabilities of 33.25 %, 32.25 % and 34.5 % and are uniformly distributed in different regions (Fig. S12). The high uniformity substantially increases the combination number (CN) of ternary keys, which can be calculated as C(n,c) times C(c,m),

where n is the total device number, c is the conducting (C)-type device number, and m is the M-type device number. For 300-bit ternary keys, the numbers of O-, S- and M-type FETs are 100, 97, and 103, respectively, and the CN is calculated to be 3.44×10^{140}, which is very close to the maximum value (3.76×10^{140}) and 10^{8} larger than that of previously reported ternary keys made from self-assembled CNTs of the same size (Fig. 3a, see details in Supplementary Information, SI)[28]. Because of one more possibility for every bit than when using binary keys, ternary keys have a much larger CN (10^{50} larger for 300-bit binary keys, as shown in Fig. S13).

Uniqueness measures the ability of a PUF to be different from other PUFs and is generally characterized by the inter-Hamming distance (HD)[28]. To quantify the uniqueness, ternary bits were divided into 25 64-bit keys. The normalized inter-HD was centred at 66.8 % with a standard deviation of 8.3 % (Fig. 3b), and the mean was close to the ideal value (2/3), determined by the fact that two bits from two different ideal ternary keys differ with a 2/3 probability. To commonly assess CNT PUFs, 1600-bit ternary keys were converted into 3200-bit binary keys by successively extracting two types of bits to form three groups of binary keys and then connecting them (Fig. S14). The normalized inter-HD of the divided 50 64-bit binary keys was centred at 50.1 % with a standard deviation of 8.6 % (Fig. 3c), and the mean was close to the ideal value (1/2). For different size keys, the normalized inter-HDs of ternary and binary keys still approached 2/3 and 1/2, respectively, and the distributions narrowed with increasing key size (Fig. S14). To assess the randomness and unpredictability of CNT PUFs, 3200-bit binary keys were subjected to the National Institute of Standards and Technology (NIST) statistical randomness test suite[44]. For the 1 % significance level, all p-values were larger than 0.01, and most of them were even larger than 0.1, so it is accepted that highly random keys were generated through CNT PUFs.

Reliability measures the ability of a PUF to generate a consistent response to a corresponding challenge and the stability of the bits in the generated key, which is generally quantified by the intra-HD. To demonstrate the long-term stability, we compared the electrical properties of 240 as-fabricated FETs and the same set of FETs after six months. As shown in Figs. 3e-f, the extracted I_{on}s and on/off ratios of these FETs follow the ideal 1:1 guideline, and there was no change among O-type, M-type and S-type FETs. To demonstrate the temperature stability, we compared the electrical properties of 240 FETs at room temperature and at 100 ℃. As shown in Figs. 3g-h, the extracted I_{on}s of these FETs basically followed the ideal 1:1 guideline, while the on/off ratios decreased by approximately a decade on average, which was caused by the high temperature-induced increase in the off-state current (Fig. S16), but there were still no changes among the three types of FETs. Since no FETs changed their types, the intra-HD was equal to the ideal value (zero). The high reliability of CNT PUFs comes from at least three aspects: the intrinsic stability of CNT randomness[49], stable or reliable contacts between electrodes and CNTs[46], and large noise margin between the three types of FETs, ensuring immunity to environmental noise.

Consistency Of Twin Pufs And Secure Communication

Generally, if a normal PUF is utilized for secure communication, the keys inside the PUF must be extracted in advance and shared with other participants or stored in a central server[29-31]. However, this strategy makes the keys vulnerable and greatly reduces the security of communication. Our twin PUFs based on aligned CNT arrays can avoid this problem. After fabrication, twin PUFs are separated and placed in two places. When secure communication starts, the instantly extracted keys from the identical twin PUFs on the two sides of the communication are used to encrypt the plain text and decrypt the cipher text (Fig. 1c). Since the longest CNT array can be up to half a metre, in principle PUFs can be fabricated in a multiple-batch manner and used for multiuser secure communication (Fig. S17).

To study the consistency of keys, we measured the I-V curves of 2×560 FETs in twin PUFs. Figure 4a shows comparison of I_{on} extracted from two sets of PUF pairs, in which 2×543 FETs were the same in terms of conducting or nonconducting types, while 2×17 FETs had different types between the C-type and O-type. Among the 2×385 conducting FETs, 2×12 FETs had different types between the M-type and S-type (Fig. 4b). In total, 2×531 FETs had the same types, making the consistency of twin PUFs approximately 95 %, whereas two independent PUFs had a low consistency of only 35 % (Fig. S18). The small number of inconsistent FETs in twin PUFs was mainly caused by imperfection during CNT growth, including chirality transition, the existence of broken tubes between catalyst stripes and misalignment (Fig. S19). The occurrence probability of CNTs with tube lengths longer than L and unchanged chirality (considering only the chirality transition between metallic tubes and semiconducting tubes) is given by

$$P\big|_{\geq L} = (1-\beta L)e^{-\alpha L}, \qquad (1)$$

where l is the tube length and α and β are the probabilities of growth stopping and chirality transition per unit distance, respectively (see details in Supplementary Information). The misalignment is characterized by the angle between CNTs in the array, which is measured to have a standard deviation of 0.09° (Fig. S20). The inconsistency can also be caused by fabrication process, including FET failure and angular deviation (0.05°) between the FET channel direction and CNT growth direction (Fig. S21). We estimated that currently our FET failure would cause a 1 % inconsistency, but this can be reduced to a very low level in a mature device fabrication process. To safely separate twin PUFs, the distance between twin PUFs must be larger than approximately 30 μm, considering that the cut size is approximately 10 μm using plasma dicing[51]. According to the simulated results, the consistency of twin PUFs will decrease to a barely acceptable value of 85 % when the PUF distance is 30 μm (Fig. 4c). Through optimization of the CNT growth and device fabrication, the consistency at long PUF distances can be largely increased to exceed 95 % (Fig. 4d).

To demonstrate secure communication, we generated twin binary keys with 2×1120 bits, in which the solid green, solid red and hollow black circles represent bit ‘1’, bit ‘0’, and inconsistent bit, respectively (Fig. 4e). Effects resulting from these inconsistent or “wrong” bits can be reduced significantly if a fault-tolerant design is used. Assuming the transfer of the word ‘Twin’ (the corresponding binary code is ‘10101001110111110100111011110’ in 7-bit ASCII), the plain text is encrypted into the cipher text

‘10011011011111000111011000 10’ by performing an XOR operation with key A. After transfer from location A to B through a public channel, the cipher text is decrypted into the binary code ‘10101001110111110100111011 10’ by performing an XOR operation with key B, which is translated into the word ‘Twin’ to complete secure communication. However, owing to the non-perfect consistency of twin PUFs, the encryption and decryption process could introduce wrong bits, which is generally measured using the bit error rate (BER). To reduce BER, we designed fault-tolerant cryptography in which multiple key bits (≥3, odd) are used to encrypt one plain text bit into multiple cipher text bits, and the multiple cipher text bits are decrypted and then generate one plain text bit through a majority vote (Fig. 4f). Since inconsistent key bits of more than one half occurring in one group key will cause an incorrect bit, the BER is given by

$$\mathrm{BER} = \sum_{i=k}^{2k-1} C_{2k-1}^{i} p^{2k-1-i}(1-p)^{i}, \qquad (2)$$

where p is the consistency of twin PUFs and k is the number of key bits used to encrypt one plain text bit. According to the calculation, the BER will be exponentially reduced with increasing k for consistency greater than 80 % (Fig. 4g). For our twin PUFs with a consistency of 95 %, the BER can be reduced to one in a trillion when the fault-tolerant number is up to 29; therefore, the accuracy of communication can be greatly strengthened.

Twin PUFs were realized using well-aligned CNT arrays and used to demonstrate secure communication. The properties of the CNT arrays, including chirality and position, are random and impossible to predict or clone perpendicular to the CNT growth direction and are identical along the parallel direction. Through simulation and optimization of the purity and device dimensions, ternary keys were tuned to be maximized in randomness. The PUFs exhibited high uniformity, uniqueness, randomness, unpredictability, and reliability over 6 months and at high temperature of 100 ℃. The twin PUFs showed a good consistency of approximately 95 %, far higher than the consistency of two independent PUFs of approximately 35 %. Finally, twin PUFs were successfully applied to demonstrate simple secure communication, and the BER could be decreased to one trillion through a fault-tolerant design. Our twin PUFs will serve as a higher-security hardware primitive beyond normal PUFs and can also be integrated into CNT ICs as a chip fingerprint.

Declarations

Supplementary Information is linked to the online version of the paper at www.nature.com/nature.

Acknowledgements We are most grateful to the late Miss Jingxia Liu, a talented young scientist and a beautiful girl, for her valuable contribution to this work. This work was supported by the National Key Research & Development Program (Grant No. 2016YFA0201901) and the Beijing Municipal Science and Technology Commission (Grant No. Z181100004418011).

Author Contributions Z. Z. and L. M. P. proposed and supervised the project. D. Z., Z. Z. and L. M. P. designed the experiment. D. Z. fabricated devices. D. Z., J. L., Y. X., H. S. and C. Zhao performed electrical measurements. D. Z. performed the simulations. M. X. grew and characterized aligned CNT arrays. J. L., L. J. and L. D. performed the NIST statistical randomness test. D. Z., Z. Z. and L. M. P. analysed the data and cowrote the manuscript. All the authors discussed the results and commented on the manuscript.

Author Information Reprints and permissions information is available at www.nature.com/reprints. Correspondence and requests for materials should be addressed to (Z. Y. Z.) zyzhang@pku.edu.cn; (L. M. P.) lmpeng@pku.edu.cn.

References

1. Riahi Sfar, A., Natalizio, E., Challal, Y. & Chtourou, Z. A roadmap for security challenges in the Internet of Things. *Digit. Commun. Networks* **4**, 118–137 (2018).
2. Mendez Mena, D., Papapanagiotou, I. & Yang, B. J. Internet of things: Survey on security. *Information security journal: A global perspective* **27**, 162–182 (2018).
3. Goldreich, O. Foundations of Cryptography: Basic Tools. Cambridge University Press, New York, NY, USA, 2001.
4. Rivest, R., Shamir, A. & Adleman, L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Commun. ACM.* **21**, 120–126 (1978).
5. Shor, P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM J. Comput.* **26**, 1484–1509 (1997).
6. Sadeghi, A.R. & Naccache, D. Towards Hardware-Intrinsic Security: Foundations and Practice (Springer: New York, NY, 2010).
7. Kömmerling, O. & Kuhn, M. G. Design principles for tamper-resistant smartcard processors. *Smartcard* **99**, 9–20 (1999).
8. Shor, P. W. & Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **85**, 441–444 (2000).
9. Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N. & Peev, M. The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301–1350 (2009).
10. Beveratos, A., Brouri, R., Gacoin, T., Villing, A., Poizat, J. -P. & Grangier, P. Single Photon Quantum Cryptography. *Phys. Rev. Lett.* **89**, 187901 (2002).
11. Aspelmeyer, M., Jennewein, T., Pfennigbauer, M., Leeb, W. R. & Zeilinger, A. Long-distance quantum communication with entangled photons using satellites. *IEEE J. Sel. Top. Quantum Electron.* **9**, 1541–1551 (2003).
12. Pappu, R., Recht, B., Taylor, J. & Gershenfeld, N. Physical one-way functions. *Science* **297**, 2026–2030 (2002).

13. Herder, C., Yu, M.-D., Koushanfar, F. & Devadas, S. Physical unclonable functions and applications: a tutorial. Proc. IEEE 102, 1126–1141 (2014).
14. Roel, M. Physically Unclonable Functions: Constructions, Properties and Applications. PhD thesis, Univ. KU Leuven (2012).
15. Kang, H., Hori, Y., Katashita, T., Hagiwara, M. & Iwamura, K. Cryptographic key generation from PUF data using efficient fuzzy extractors. *16th Int. Conf. Adv. Commun. Tech.* (2014). DOI: 10.1109/ICACT.2014.6778915
16. Maes, R., Van Herrewege, A. & Verbauwhede, I. PUFKY: a fully functional PUF-based cryptographic key generator. *Int. Workshop Cryptographic Hardware Embedded Syst.* (2012). DOI: 10.1007/978-3-642-33027-8_18
17. Ruhrmair, U. & Holcomb, D. E. PUFs at a glance. 2014 *Des. Autom. Test Europe Conf. Exhibit.* (2014). DOI: 10.7873/DATE.2014.360
18. Gassend, B., Clarke, D., van Dijk, M. & Devadas, S. Silicon physical random functions. In Proc. 9th ACM Conf. Comput. Commun. Secur. (Ed. Atluri, V.) 148–160 (ACM Press, 2002).
19. Bolotnyy, L. & Robins, G. Physically unclonable function-based security and privacy in RFID systems. In Fifth Ann. IEEE Int. Conf. Pervasive Comput. Commun. 211–220 (IEEE, 2007).
20. Guajardo, J., Kumar, S. S., Schrijen, G.-J. & Tuyls, P. FPGA intrinsic PUFs and their use for IP protection. In Cryptogr. Hardw. Embed. Syst. - CHES 2007 (eds Paillier, P. & Verbauwhede, I.) 63–80 (Springer, 2007).
21. Rahman, F., Shakya, B., Xu, X. L., Forte, D. & Tehranipoor, M. Security beyond CMOS: fundamentals, applications, and roadmap. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* **25**, 3420–3433 (2017). DOI: 10.1109/TVLSI.2017.2742943
22. Waser, R., Dittmann, R., Staikov, G. & Szot, K. Redox-based resistive switching memories-nanoionic mechanisms, prospects, and challenges. *Adv. Mater.* **21**, 2632–2663 (2009).
23. Chen, A. Comprehensive assessment of RRAM-based PUF for hardware security applications. *In Proc. 2015 IEEE Int. Electron Devices Meet.*
10.7.1–10.7.4
(IEEE, 2015); DOI: 10.1109/IEDM.2015.7409672 (2015).
24. Liu, R., Wu, H. Q., Pang, Y. C., Qian, H. & Yu, S. M. Experimental characterization of physical unclonable function based on 1 kb resistive random access memory arrays. *IEEE Electron Device Lett.* **36**, 1380–1383 (2015).
25. Nili H. *et al.* Hardware-intrinsic security primitives enabled by analogue state and nonlinear conductance variations in integrated memristors. *Nat. Electron.* **1**, 197–202 (2018).
26. Alharbi, A., Armstrong, D., Alharbi, S. & Shahrjerdi D. Physically unclonable cryptographic primitives by chemical vapor deposition of layered MoS_2. *ACS Nano* **11**, 12772–12779 (2017).
27. Hu, Z. *et al.* Physically unclonable cryptographic primitives using self-assembled carbon nanotubes. Nat. Nanotech. 11, 559–565 (2016).

28. Hu, Z. Y. & Han, -S. J. Creating security primitive by nanoscale nanipulation of carbon nanotubes. IEEE International Symposium on Hardware Oriented Security and Trust (HOST) 29–34 (2017); DOI: 10.1109/HST.2017.7951733.
29. Huang, M. G., Yu, B., & Li, S. S. PUF-assisted group key distribution scheme for software-defined wireless sensor networks. *IEEE Commun. Lett.* **22**, 404–407 (2018).
30. Delavar, M., Mirzakuchaki, S., Ameri, M. H. & Mohajeri, J. PUF based solutions for secure communications in advanced metering infrastructure AMI. *International Journal of Communication Systems* **67**, 74–88, (2017).
31. Chatterjee, U., Chakraborty, R. S. & Mukhopadhyay, D. A PUF-based secure communication protocol for IoT. *ACM Trans. Embedded Comput. Syst.*, **16**, 67 (2017).
32. Liu, L., Han, J., Xu, L., Zhou, J., Zhao, C., Ding, S., Shi, H., Xiao, M., Ding, L., Ma, Z., Jin, C., Zhang, Z., Peng, L.-M., Aligned, high-density semiconducting carbon nanotube arrays for high-performance electronics. *Science*, **368**, 850–856 (2020).
33. Liu, L., Ding, L., Zhong, D., Han, J., Wang, S., Meng, Q., Qiu, C., Zhang, X., Peng, L.-M., Zhang, Z., Carbon Nanotube Complementary Gigahertz Integrated Circuits and Their Applications on Wireless Sensor Interface Systems. *ACS Nano*, **13**, 2526–2535(2019).
34. Bishop, M. D., Hills, G., Srimani, T., Lau, C., Murphy, D., Fuller, S., Humes, J., Ratkovich, A., Nelson, M., Shulaker, M. M., Fabrication of carbon nanotube field-effect transistors in commercial silicon manufacturing facilities. *Nature Electronics*, **3**, 1–10 (2020).
35. Hills, G., Lau, C., Wright, A., Fuller, S., Bishop, M. D., Srimani, T., Kanhaiya, P., Ho, R., Amer, A., Stein, Y., Murphy, D., Arvind, Chandrakasan, A., Shulaker, M. M., Modern microprocessor built from complementary carbon nanotube transistors. *Nature*, **572**, 595–602 (2019).
36. Si, J. *et al.* Scalable preparation of high-density semiconducting carbon nanotube arrays for high-performance field-effect transistors. *ACS Nano* **12**, 627–634 (2018).
37. Kang, S. J. et al. High-performance electronics using dense, perfectly aligned arrays of single-walled carbon nanotubes. *Nat. Nanotechnol.* **2**, 230–236 (2007).
38. Zhang, J., Patil, N., Hazeghi, A. & Mitra, S. Carbon nanotube circuits in the presence of carbon nanotube density variations. *Proc. IEEE/ACM Des. Autom. Conf.* pp. 71–76 (2009) DOI: 10.1145/1629911.1629933.
39. Franklin, A. D. The road to carbon nanotube transistors. *Nature* **498**, 443–444 (2013).
40. Xiao, J. L. et al. Alignment controlled growth of single-walled carbon nanotubes on quartz substrates. *Nano Lett.* **9**, 4311–4319 (2009).
41. Kocabas, C., Kang, S. J., Ozel, T., Shim, M. & Rogers, J. A. Improved synthesis of aligned arrays of single-walled carbon nanotubes and their implementation in thin film type transistors. *J. Phys. Chem. C* **111**, 17879–17886 (2007).
42. Zhong, D. *et al.* Solution-processed carbon nanotubes based transistors with current density of 1.7 mA/μm and peak transconductance of 0.8 mS/μm. *In Proc. 2017 IEEE Int. Electron Devices Meet.* 5.6.1–5.6.4 (IEEE, 2017); DOI: 10.1109/IEDM.2017.8268335.

43. Xie, X. et al. Microwave purification of large-area horizontally aligned arrays of single-walled carbon nanotubes. *Nat. Commun.* **5**, 5332 (2014).
44. Shah, K.A. & Tali B.A. Synthesis of carbon nanotubes by catalytic chemical vapour deposition: a review on carbon sources, catalysts and substrates. *Mater. Sci. Semicond. Process* **41**, 67–82 (2016).
45. Wang, J. T. et al. Growing highly pure semiconducting carbon nanotubes by electrotwisting the helicity. *Nature Catalysis* **1**, 326–331 (2018).
46. Maiti, A. Gunreddy, V. & Schaumont P. A systematic method to evaluate and compare the performance of physical unclonable functions. *In Embedded Systems Design with FPGAs* 245–267 (Springer, 2013).
47. Gao, Y., Ranasinghe, D. C., Al-Sarawi, S. F., Kavehei, O. & Abbott, D. Memristive crypto primitive for building highly secure physical unclonable functions. *Sci. Rep.* **5**, 12785 (2015).
48. A. Rukhin et al. A statistical test suite for random and pseudorandom number generators for cryptographic applications. NIST, McLean, VA, USA, Tech. Rep. 800 – 22 (2001).
49. Saito, R., Dresselhaus, G. & Dresselhaus, M. S. Physical properties of carbon nanotubes. Imperial College Press, (1998).
50. Pei, T. et al. Temperature performance of doping-free top-gate CNT field-effect transistors: potential for low- and high-temperature electronics. *Adv. Funct. Mater.* **21**, 1843–1849 (2011).
51. Westermana, R. J.et al. Plasma dicing: current state & future trends. *ECS Trans.* **69**, 3–14 (2015).

Figures

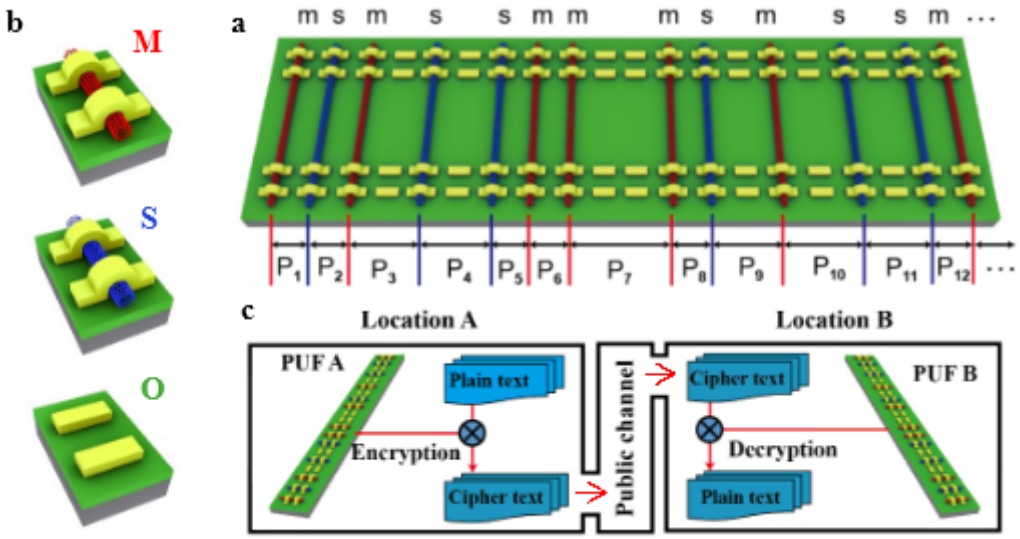

Figure 1

Twin physically unclonable cryptographic primitives based on CNT arrays. a, Schematic of twin PUFs based on CVD-grown CNT arrays. The letters ‘m’ and ‘s’ represent metallic or semiconducting CNT, while letter ‘P’ represents interspacing between two adjacent CNTs. b, Schematic of three distinct types of

devices according to their conduction type. Letter ‘O’ represents device with open channel, and ‘S’ and ‘M’ represent devices channel with semiconducting or metallic CNT, respectively. c, Schematic of secure communication utilizing CNT twin PUFs. PUFs A and B are separated from a pair of twin PUFs.

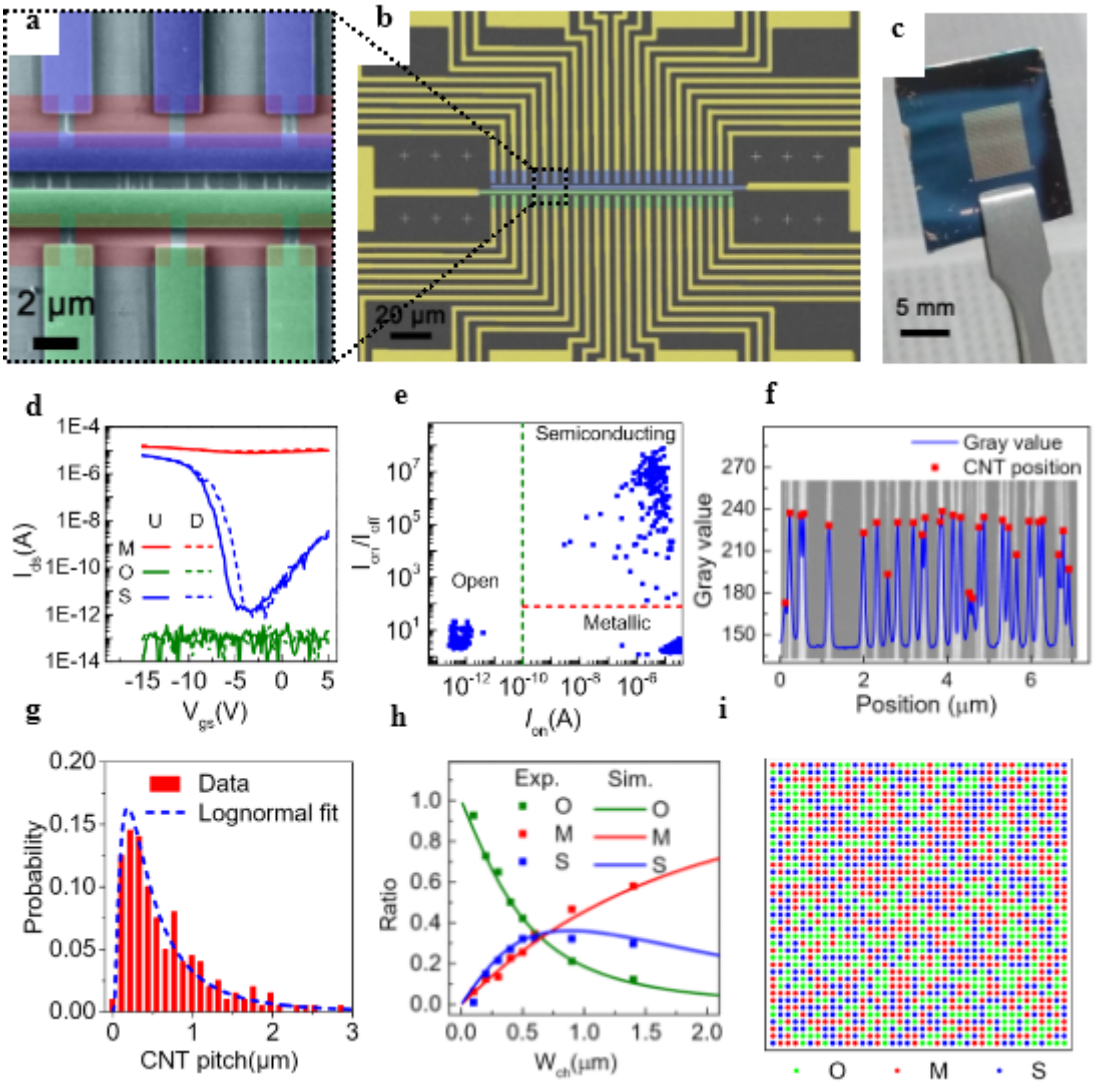

Figure 2

Structure and performance of CNT twin PUFs and PUF-generated ternary bits. a, Enlarged SEM image showing three pairs of twin PUF devices. The scale bar represents 2 μm. b, False-coloured SEM image showing a group of 24 pairs of twin PUF devices. The scale bar represents 20 μm. c, Optical image showing a twin PUF matrix. The scale bar represents 5 mm. d, Transfer characteristics measured from the three pairs of devices in (a). The solid and dashed curves represent the devices from the upper and lower rows of devices, respectively. e, Classification of 500 devices using the on-state current (0.1nA) and current on/off ratio (100) as the boundaries. f, Extraction of CNT pitch from SEM images of CNT arrays. g, Distribution of CNT pitch and lognormal fit of the data. h, Ratios of three types of devices versus channel width of PUF devices. The squares and lines represent experimental and simulation data, respectively. i, CNT PUF-generated ternary keys including 1600 bits. The green, red and blue circles represent open (0,0), semiconducting (1,0) and metallic (1,1) bits or devices, respectively.

Figure 3

Characteristics of CNT PUF-generated secret keys. a, Combination number (CN) map as a function of ratios of O- and S-type FETs. b-c, Distribution of normalized inter-HDs of binary keys (b) and ternary keys (c). The key size is set to be 64 bits. d, NIST statistical randomness test suite of binary keys transformed from ternary keys. e-f, Long-term stability of CNT PUFs. g-h, High-temperature stability of CNT PUFs. Green squares represent experimental data, and red lines represent perfect performance with no electrical property changes after six months or at a temperature of 100 °C.

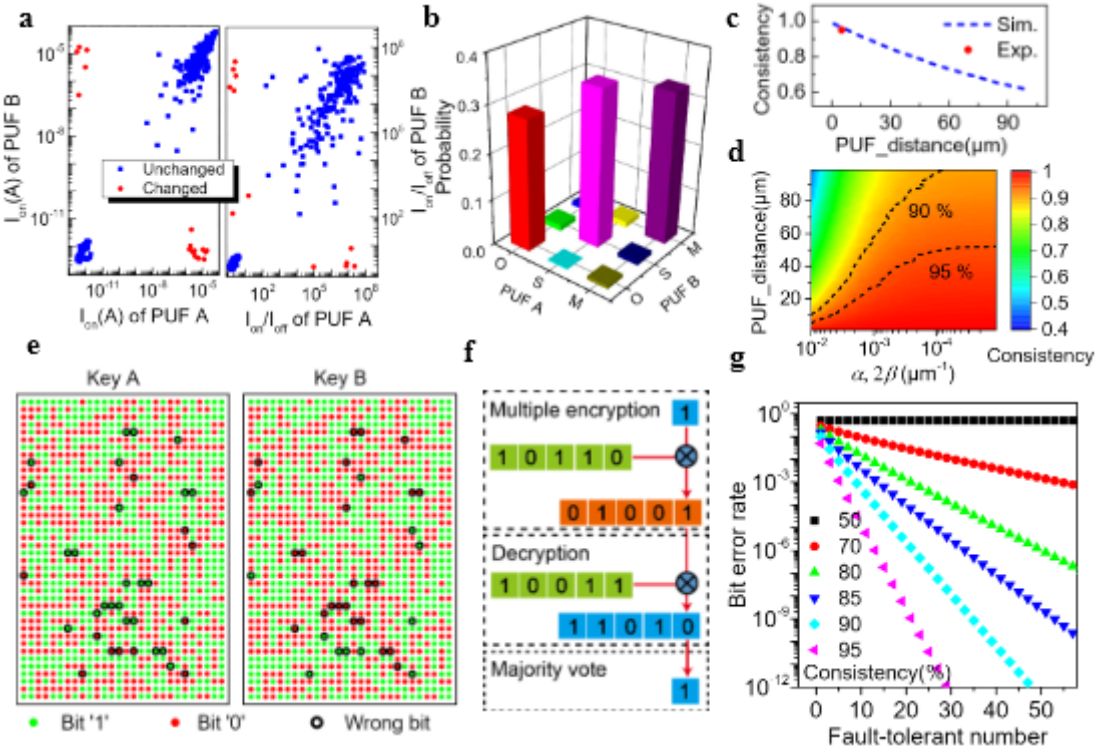

Figure 4

Consistency of CNT twin PUFs, and their application in secure communication. a-c, Comparison of twin PUFs (A and B): (a) on-state current, current on/off ratio, and (b) electrical type, i.e. O-, S- or M-type. c, Simulation of the consistency versus PUF distance, with α=300-1 μm-1 and β= 600-1 μm-1. d, Improvement in the consistency through optimization; the misalignment and angular deviation are set to 0.03°. e, Twin binary bit maps generated from twin PUFs using double-binary bits. The solid green and solid red circles represent bit ‘1’ and bit ‘0’, respectively. The hollow black circles represent in-consistent or “wrong” bits. f, Schematic of secure communication using a fault-tolerant design. g, BER versus fault-tolerant number with different consistencies.

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- DLZhongCNTTwinPUFsSI20210710.docx