ARTICLES
https://doi.org/10.1038/s41928-022-00787-x

nature electronics

Twin physically unclonable functions based on aligned carbon nanotube arrays

Donglai Zhong[1], Jingxia Liu[1,4], Mengmeng Xiao[1,2], Yunong Xie[1], Huiwen Shi[1], Lijun Liu[1], Chenyi Zhao[1], Li Ding[1], Lian-Mao Peng[1,2] ✉ and Zhiyong Zhang[1,2,3] ✉

Physically unclonable functions (PUFs) are a promising technology for generating cryptographic primitives using random imperfections in a physical entity. However, the keys inside PUFs are still vulnerable as they must be written into non-volatile memories and shared with participants that do not hold the PUF before secure communication. Here we show that pairs of identical PUFs (twin PUFs) can be fabricated together on an aligned carbon nanotube array and used for secure communication without key pre-extraction and storage. Two rows of field-effect transistors are fabricated perpendicular to the carbon nanotube growth direction, randomly producing three types of transistor channel—based on metallic nanotubes, semiconducting nanotubes and no nanotubes—that can be used to extract ternary bits for use as a shared key. The twin PUFs exhibit high uniformity, uniqueness, randomness and reliability, as well as a consistency of approximately 95%. We show that separated twin PUFs can provide secure communication with a bit error rate of one bit per trillion via a fault-tolerant design.

Classical cryptography uses cryptographic algorithms and keys to authenticate electronic devices and encrypt or decrypt information[1]. The most popular asymmetric algorithm for secure communication is Rivest–Shamir–Adleman encryption[2,3], which is predicated on the difficulty for a classical computer for factoring a very large number. This task has, however, been mathematically shown to be accomplishable in polynomial time using a quantum computer[4]. Another strategy is symmetric encryption where all the communication participants possess the same secret keys for encryption or decryption, and secret keys are stored in non-volatile memory, such as erasable programmable read-only memory or static random-access memory. However, the stored keys are vulnerable to physical and side-channel attacks, such as by observing the consumed power or emitted radiation[5,6] and thus can be accessible to an attacker. Quantum key distribution can exhibit higher security than classical methods by exploiting quantum theory[7,8]—specifically, the feature of quantum systems to be intrinsically disturbed by the process of measuring them—but this technology requires expensive and unproven equipment[9,10].

Physically unclonable functions (PUFs), also known as physical one-way functions[11], are hardware-based security primitives that allow secret keys to be extracted on demand from a reliable and random physical system instead of being stored in non-volatile memory[12–14]. Random physical imperfections and small-scale variations caused by the fabrication process can be used by PUFs to generate the keys, and these imperfections cannot be predicted or cloned even by the original manufacturer[15,16]. A single PUF can be considered to be a unique and unclonable black-box challenge–response system[12]. The first PUFs were based on the unique speckle pattern generated by a laser beam going through a scattering medium at a select angle and point of incidence[11]. However, PUFs based on electrical properties are preferred to those based on optical ones due to their simple connection to key-readout circuits.

Conventional silicon PUFs[17–19], such as delay- 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 PUFs based on nanomaterials, including molybdenum disulfide (MoS_2), graphene and carbon nanotubes (CNTs) in memristor structures, have been shown to be more reliable than silicon PUFs[20–29]. In particular, reliable physically unclonable cryptographic primitives using solution-derived CNTs, which were randomly self-assembled into hafnium oxide trenches with different yields via the trench dimensions, have been shown to exhibit high immunity to electronic and environmental noise (such as supply voltage and temperature variations)[25,26].

Unclonability ensures the safety of PUF-generated keys from being predicted or copied. If a PUF is used for secure communication, then the generated keys must be written into non-volatile memory and shared with other participants that do not hold the PUF[30–32], which makes the keys vulnerable. An alternative would be to develop a way to initially make two identical PUFs in a single fabrication run that can then be separated and placed in two places, with the extracted keys being used to encrypt and decrypt communications. There is also a need to develop PUF technology that is compatible with CNT-based electronics. Due to developments in solution-derived CNT materials[33], there has been recent progress in CNT-based complementary metal–oxide–semiconductor field-effect transistors (FETs) and integrated circuits (ICs)[33–37]. Wafer-scale fabrication of complementary metal–oxide–semiconductor CNT FETs on an eight-inch wafer[36,37], high-speed transistors and ring oscillators with oscillation frequency up to 8 GHz[33,34], and large-scale digital ICs including a 16-bit microcontroller unit containing 14,000 transistors[37] have been demonstrated on high-purity semiconducting CNT films. Due to low-temperature fabrication, CNT PUFs could also be heterogeneously integrated with silicon or other semiconductor-based ICs as an encryption module, as previously shown with the monolithic integration of silicon ICs and CNT FETs[38,39].

In this Article, we show that pairs of identical PUFs (twin PUFs) can be fabricated using chemical vapour deposition (CVD)-grown aligned CNT arrays and used for secure communication without

[1]Key Laboratory for the Physics and Chemistry of Nanodevices and Center for Carbon-based Electronics, Department of Electronics, Peking University, Beijing, China. [2]Jihua Laboratory, Foshan, China. [3]Frontiers Science Center for Nano-optoelectronics, Peking University, Beijing, China. [4]Deceased: Jingxia Liu. ✉e-mail: lmpeng@pku.edu.cn; zyzhang@pku.edu.cn

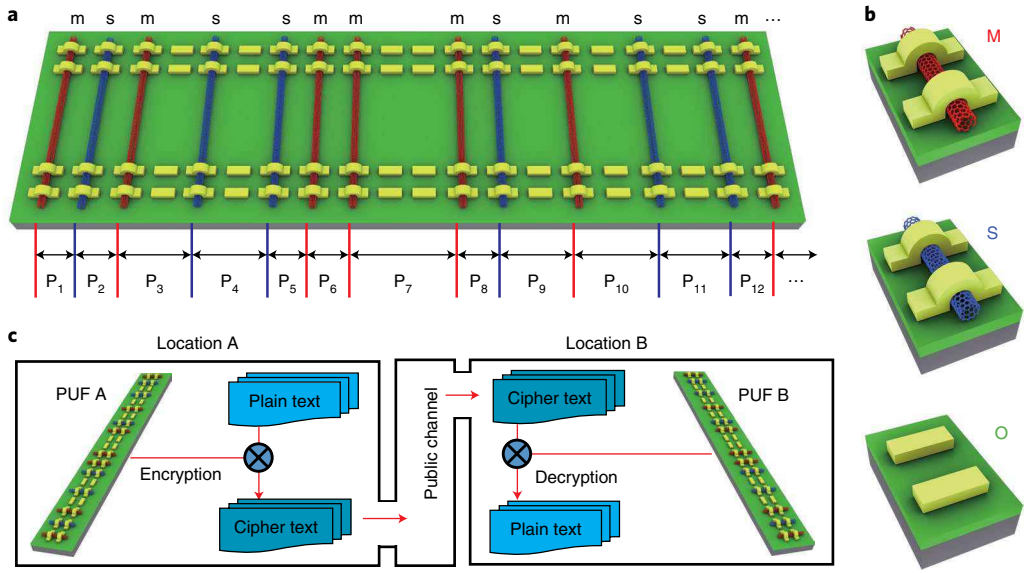

Fig. 1 | Twin PUFs based on aligned CNT arrays and usage in secure communication. a, Schematic of twin PUFs based on CVD-grown CNT arrays. The letters 'm' and 's' represent a metallic or semiconducting CNT, whereas letter 'P' represents interspacing between two adjacent CNTs. **b**, Schematic of three distinct types of device according to their conduction type. Letter 'O' represents a device with an open channel, and 'S' and 'M' represent device channels with a 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.

key pre-extraction and storage (Fig. 1). Aligned CNT arrays should have random characteristics, such as chirality and position, perpendicular to the CNT growth direction and identical characteristics along the growth direction. Back-gated FETs fabricated on arrays perpendicular to the growth direction show three channel types with distinct electrical properties—channels containing some metallic CNTs, purely semiconducting CNTs and no CNTs at all ('open channel')—from which ternary bits can be extracted and used as secure keys. Through simulation and optimization of purity and device dimensions, the ternary bits are tuned to have maximum randomness. Two rows fabricated in parallel on the same CNT array produce twin PUFs with a consistency of approximately 95%, compared with approximately 35% for two independent PUFs. We illustrate the potential of twin PUFs for secure communication using twin binary keys (2 × 1,120 bits) generated by the devices. Through a fault-tolerant design, where multiple key bits are used to encrypt one plain text bit, the bit error rate (BER) of the encryption and decryption process can be reduced, potentially down to one bit per trillion.

Fabrication of twin PUFs on aligned CNT array

Well-aligned CNT arrays were grown via CVD on ST-cut quartz substrates using iron nanoparticles as the catalyst (Supplementary Fig. 1). Deposited via electron-beam evaporation (EBE), the iron nanoparticles in the catalyst stripes were randomly positioned and had different sizes owing to the statistical nature of the EBE process. In addition, nucleation through the vapour–liquid–solid processes is also stochastic; therefore, CNT arrays were randomly distributed perpendicular to the growth direction defined by the crystal orientation in terms of both chirality and position (Supplementary Figs. 2 and 3), which is highly unwanted for high-performance electronics applications[40–42]. 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, that is, O channel with very low current and a 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 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 is not predictable or clonable; therefore, in principle, one row of FETs meets the requirements of PUFs. Induced by the quartz lattice–CNT interaction[43], CNT arrays grew along the [2, −1, −1, 0] crystal orientation for several hundred micrometres[44], 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; therefore, two identical PUFs can be fabricated together.

To fabricate FETs, CNT arrays were transferred using polymethyl methacrylate (PMMA) as a medium to the target Si/SiO_2 substrate before device fabrication[45], and the substrate served as the global back gate to measure the transfer characteristics. Palladium (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 (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 the FETs were connected to peripheral on-chip pads (Fig. 2b and Supplementary Fig. 4). According to the patterned catalyst stripes with 0.25 mm distance and pad settings, the test units were batch fabricated in the form of a matrix with 0.50 mm distance (Fig. 2c and Supplementary Fig. 4).

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, whereas the FETs with CNTs in the channel showed I_{on} far above 1 µA. Among the conducting FETs, the FETs with only semiconducting CNTs showed an on/off ratio of up to 6 decades, whereas 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 FET pairs with the same order from the two rows of FETs showed transfer characteristics that almost coincide, indicating that they were identical. Here 500 FETs on

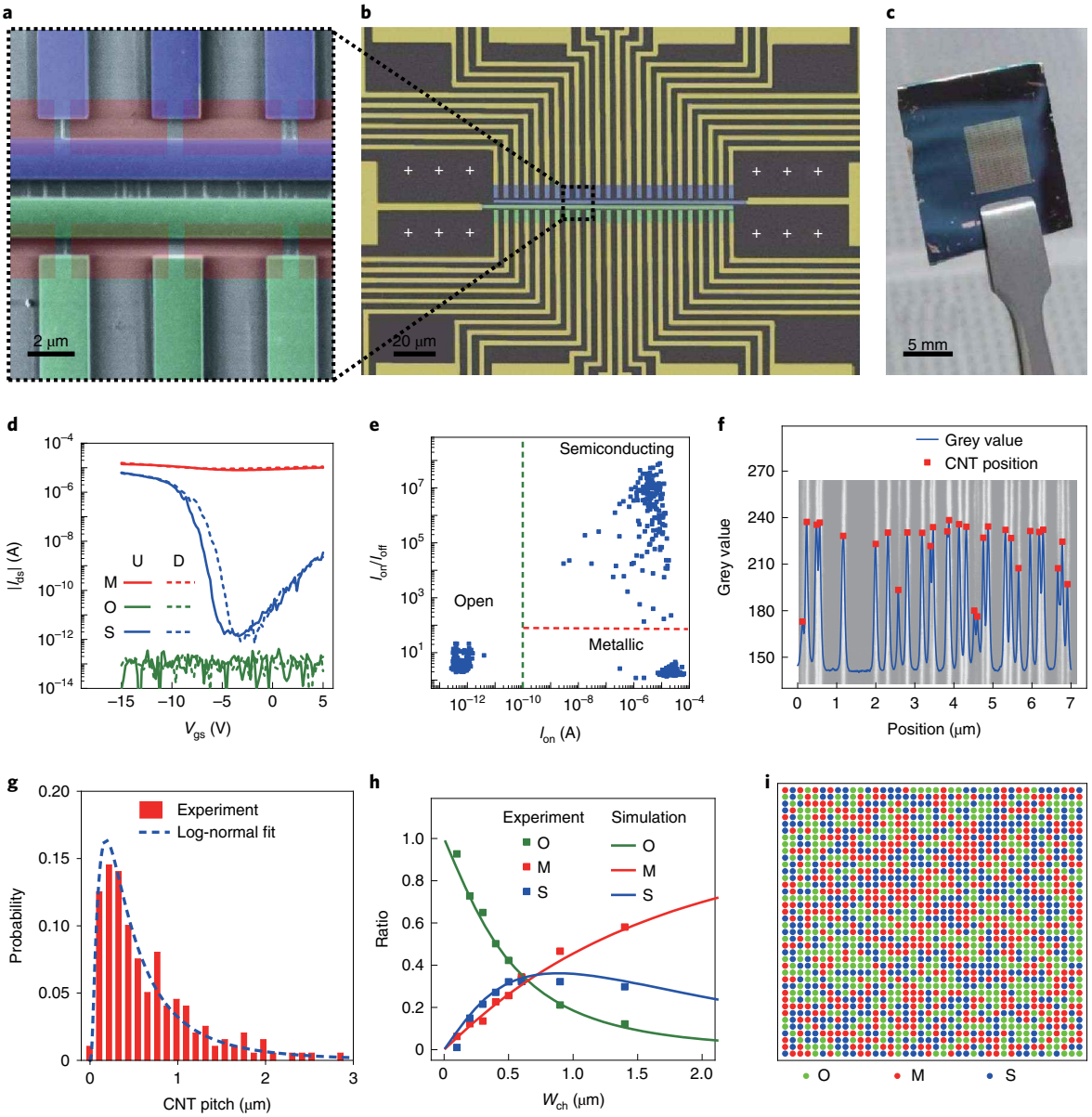

Fig. 2 | Structure and performance of CNT twin PUFs and PUF-generated ternary bits. a, Enlarged SEM image showing three pairs of twin PUF devices. Scale bar, 2 μm. The red box represents the CNT etching area, and the channel width can be adjusted by changing the size of the etching area. **b**, False-coloured SEM image showing a group of 24 pairs of twin PUF devices. Scale bar, 20 μm. **c**, Optical image showing a twin PUF matrix. Scale bar, 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 (0.1 nA) and current on/off ratio (100) as the boundaries. **f**, Extraction of CP from the SEM images of CNT arrays. **g**, Distribution of CP and log-normal fit of the data. **h**, Ratios of the three types of device versus the channel width of PUF devices. The squares and lines represent experimental and simulation data, respectively. **i**, CNT-PUF-generated ternary keys including 1,600 bits. The green, red and blue circles represent open (0,0), semiconducting (1,0) and metallic (1,1) bits or devices, respectively.

CNT arrays were readily classified into these three types (O, S and M devices) according to their extracted on-state current I_{on} and current on/off ratio, by defining O-type FETs as the ones with I_{on} below 0.1 nA, S-type FETs with I_{on} above 0.1 nA and an on/off ratio greater than 100, and M-type FETs with I_{on} above 0.1 nA and an on/off ratio of less than 100 (Fig. 2e and Supplementary Fig. 5).

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 array density and FET channel width W_{ch}. As shown in Fig. 2f, we extracted CNT positions from scanning electron microscopy (SEM) images of CNT arrays and then calculated the tube-to-tube spacing (CNT pitch (CP)). Through statistical distribution fitting, the CPs were found to meet the log-normal distribution, which was verified by other CNT samples that we grew with different densities and those published by other groups[41,46] (Fig. 2g and Supplementary Fig. 6). According to the simulation with a CP of 1.0 ± 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}, whereas the ratio of S-type FET first increases and then decreases (Supplementary Fig. 4). The non-monotonic change in the ratio of S-type FETs results from the fact that the possibility of metallic CNTs appearing in the S-type channel rapidly increases

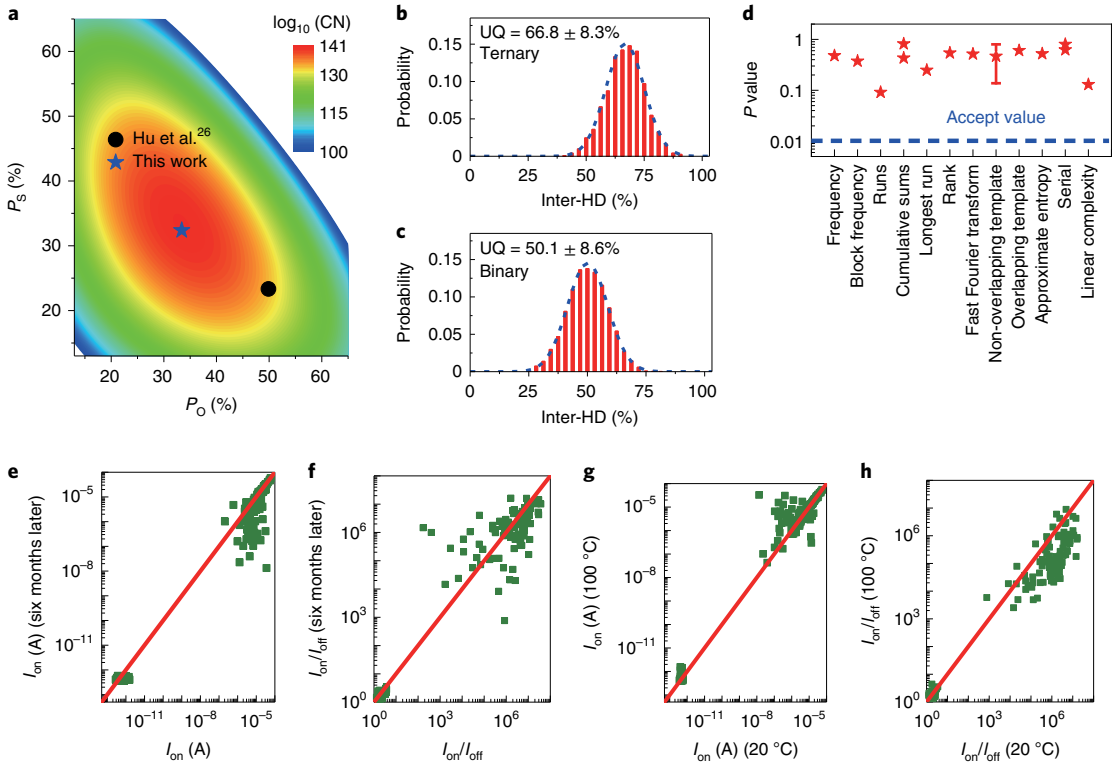

Fig. 3 | Characteristics of CNT-PUF-generated secret keys. a, CN map as a function of ratios of O- and S-type FETs. **b**,**c**, Distribution of normalized inter-HD of binary keys,UQ represents uniqueness. (**b**) and ternary keys (**c**). The key size is set to be 64 bits. **d**, NIST statistical randomness test suite of binary keys transformed from ternary keys. The error bar is the standard deviation of P-values of the non-overlapping template test. **e**,**f**, Long-term stability of CNT PUFs. **g**,**h**, High-temperature stability of CNT PUFs. The green squares represent experimental data, and the red lines represent perfect performance with no electrical property changes after six months or at a temperature of 100 °C.

when W_{ch} exceeds 1 μm, which effectively turns the S-type FET into an M-type FET (Supplementary Fig. 7).

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 a 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, respectively; 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 (Supplementary Fig. 8), and the other is to increase the deviation in the CP to increase mixed FETs (Supplementary Fig. 9). The MSR can be adjusted by many factors, including catalyst, carbon source, atmosphere and electromagnetic field[47,48], whereas CP is mainly determined by the distribution of iron nanoparticles. Through the co-optimization of CP and MSR, MD is reduced down to 10^{-4} (Supplementary Fig. 10). Finally, CNT arrays with a CP of 0.65 ± 0.58 μm and MSR of approximately 0.4 (Supplementary Fig. 11) were selected to demonstrate CNT twin PUFs with ideal ternary bits, and the experimental result is in good agreement with the simulation (Fig. 2h). A total of 1,600 FETs with 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[49,50]; when applied to cryptography applications, randomness and unpredictability are also indispensable[46]. The optimized ternary bit distribution showed that the three types of FET have occurrence probabilities of 33.25%, 32.25% and 34.50% and are uniformly distributed in different regions (Supplementary Fig. 12). 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 and Methods)[26]. Additionally, a delayed ternary PUF circuit based on CNT FETs was also designed to exhibit high randomness and the CN is calculated to be 1.81×10^{140} from the simulation[29]. Although the CN of the same quantity of PUF units is close to our result, the unit of the PUF also contains more than 50 transistors; therefore, the key density will be much lower than our transistor-based PUFs. 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; Supplementary Fig. 13). Besides that, the entropy of our ternary PUF was up to 1.58, higher than those PUFs based on other technologies[23,25–27] (Supplementary Table 1).

Uniqueness measures the ability of a PUF to be different from other PUFs and is generally characterized by the inter-Hamming distance (HD)[31]. 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, 1,600-bit ternary keys were converted into 3,200-bit binary keys by successively extracting two types of bit to form three groups of binary keys and then connecting them (Supplementary Fig. 14). The normalized inter-HD of the divided 50 64-bit binary keys was centred at 50.1% with a standard

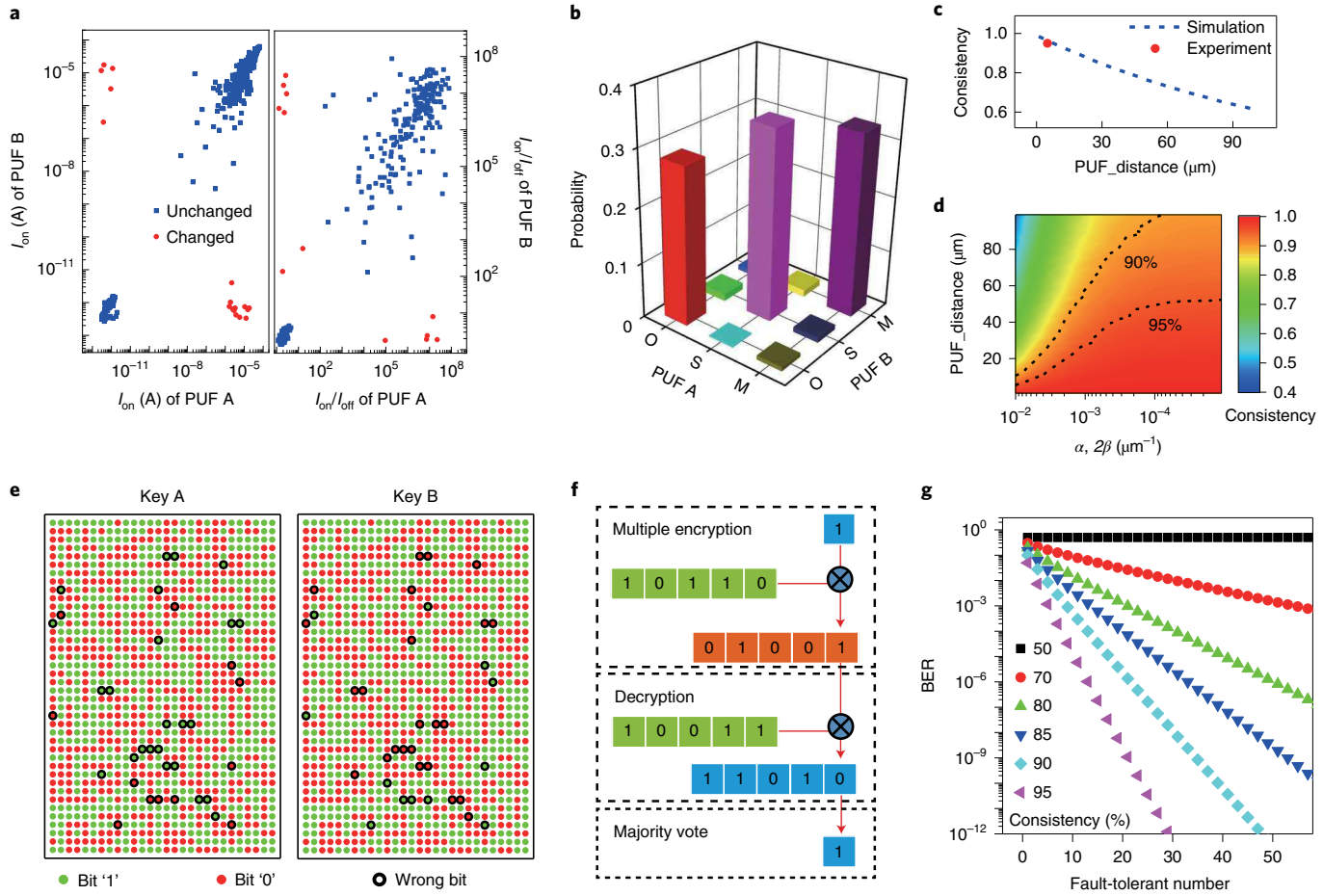

Fig. 4 | Consistency of CNT twin PUFs and their application in secure communication. a,**b**, Comparison of twin PUFs (A and B): on-state current, current on/off ratio (**a**) and electrical type, that is, O, S or M type (**b**). **c**, Simulation of the consistency versus PUF distance, with $\alpha = 300\,\mu m^{-1}$ and $\beta = 600\,\mu m^{-1}$. **d**, Improvement in 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 inconsistent or 'wrong' bits. **f**, Schematic of secure communication using a fault-tolerant design. **g**, BER versus fault-tolerant number with different consistencies.

deviation of 8.6% (Fig. 3c), and the mean was close to the ideal value (1/2). For different-sized 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 (Supplementary Fig. 14). To assess the randomness and unpredictability of CNT PUFs, 3,200-bit binary keys were subjected to the National Institute of Standards and Technology (NIST) statistical randomness test suite[51]. For the 1% significance level, all the p values were larger than 0.01, and most of them were even larger than 0.1; therefore, it is accepted that highly random keys were generated through CNT PUFs. CNT PUFs can be considered as strong PUFs and exhibit true unclonability[13], since they can support a very large number of challenge–response pairs benefitting from the small size of the PUF cell and wafer-scale growth of CNT arrays.

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 Fig. 3e,f, the extracted I_{on} values and on/off ratios of these FETs follow the ideal 1:1 guideline, and there was no change among the O-, M- and S-type FETs. To demonstrate the temperature stability, we compared the electrical properties of 240 FETs at room temperature and at 100 °C. As shown in Fig. 3g,h, the extracted I_{on} values of these FETs basically followed the ideal 1:1 guideline, whereas 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 (Supplementary Fig. 16). The electrical property changes of CNT FETs arise from the temperature-dependent carrier concentration and mobility, and then increase the BER. However, the digitalized classification of CNT FETs into three types does not require exactly the same properties of twin PUFs; therefore, it would be tolerant to considerable temperature variations. Besides that, we can store twin PUFs in the same temperature or use some fault-tolerant cryptography to reduce the BER. Since no FETs changed their types in our experiment, the intra-HD was close to the ideal value (zero). The high reliability of CNT PUFs comes from at least three aspects: the intrinsic stability of CNT randomness[52], stable or reliable contacts between electrodes and CNTs[53], and large noise margin between the three types of FET, 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[30–32]. 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 communication are used to encrypt the plain text and decrypt the cipher text (Fig. 1c). In principle, more than two PUFs can be fabricated to enable 'multiple-birth' PUFs (Supplementary Fig. 17), especially on long CNT arrays. The 'multiple-birth' PUFs can have an advantage over twin PUFs as multiple users participate in the secure communication, where one user can send the cipher text to all the others holding 'multiple-birth' PUFs. However, if more than two PUFs were fabricated, there is a risk of leaking one copy from the manufacturer. To put an end to this risk, we can control the number of fabricated PUFs by controlling the mean length of the CNT arrays on the wafer or using separate PUF design, fabrication and packaging.

To study the consistency of keys, we measured the I–V curves of 2 × 560 FETs in twin PUFs. Figure 4a shows a comparison of I_{on} extracted from two sets of PUF pairs, in which 2 × 543 FETs were the same in terms of conducting or non-conducting types, whereas 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% (Supplementary Fig. 18). The small number of inconsistent FETs in twin PUFs was mainly caused by imperfection during CNT growth, including chirality transition, existence of broken tubes between catalyst stripes and misalignment (Supplementary Fig. 19). 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

$$P|_{l\geq L} = (1-\beta L)\mathrm{e}^{-\alpha L}, \quad (1)$$

where l is the tube length and α and β are the probabilities of growth stopping and chirality transition per unit distance, respectively (Supplementary Information). The misalignment is characterized by the angle between the CNTs in the array, which is measured to have a standard deviation of 0.09° (Supplementary Fig. 20). The inconsistency can also be caused by the fabrication process, including FET failure and angular deviation (0.05°) between the FET channel direction and CNT growth direction (Supplementary Fig. 21). 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 the twin PUFs should be larger than approximately 20 µm, considering that the cut size is approximately 10 µm using plasma dicing[54]. The larger the distance between the twin PUFs, the smaller is the damage caused by dicing but larger is the inconsistency. Two approaches are helpful to mitigate this contradiction: reducing the substrate thickness to reduce the dicing size and improving the growth of aligned CNT arrays. It is well known that this inconsistency mainly arises from the imperfect CNT growth caused by an unclean substrate, lattice mismatch, unstable growth temperature and unstable growth atmosphere, which is hard to minimize in a university-level lab, but can be greatly reduced by fabrication in an industry-level factory. According to the simulated results, the consistency of twin PUFs decreases to a barely acceptable value of 85% when the PUF distance is 30 µm (Fig. 4c). Through the optimization of 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 × 1,120 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 greatly reduced 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 '10011011011111000111011000010' by performing an XOR operation with key A. After transferring from location A to B through a public channel, the cipher text is decrypted into the binary code '10101001110111110100111011110' by performing an XOR operation with key B, which is translated into the word 'Twin' to complete the secure communication. However, due to the non-perfect consistency of twin PUFs, the encryption and decryption process could introduce wrong bits, which is generally measured using the BER. To reduce the 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 one plain text bit is generated 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

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

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.

Conclusions

We have reported twin PUFs made using well-aligned CNT arrays. The properties of the CNT arrays are random and impossible to predict or clone perpendicular to the CNT growth direction and are identical along the parallel direction. Rows of back-gated FETs fabricated perpendicular to the CNT growth direction create FETs with three types of channel and distinct electrical properties, which can be used to extract ternary bits. Through simulation and optimization of the purity and device dimensions, the randomness of the ternary keys was maximized. The PUFs exhibited high uniformity, uniqueness, randomness, unpredictability and reliability over six months and at a high temperature of 100 °C. Two parallel rows of FETs on the CNT arrays can be used to create twin PUFs, which showed a consistency of approximately 95%; two independent PUFs show a consistency of approximately 35%. The twin PUFs were used to demonstrate secure communication, and the BER could be decreased to one bit per trillion through a fault-tolerant design. Our twin PUFs offer a convenient, low-cost and reliable technology that can serve as alternative high-security hardware primitive to typical PUFs. The technology could also be easily integrated with other CNT-based electronic devices and circuits.

Methods

CNT growth and transfer. Well-aligned CNT arrays were grown on quartz substrates. ST-cut (Hoffman) quartz wafers were annealed at 900 °C for 9 h to improve the crystallinity. Standard ultraviolet photolithography was performed to pattern catalyst stripes with a width of 5 µm and spacing of 250 µm. The catalyst stripes were patterned perpendicular to [2, −1, −1, 0] of the quartz surface. An iron film with a thickness of approximately 0.1 nm was deposited as a catalyst layer using an electron-beam evaporator followed by a lift-off process. CNT growth was performed in a horizontal CVD furnace. The prepared substrate with the patterned catalyst was annealed at 800 °C for 1 h in air to oxidize the catalysts and remove the remaining polymer residue from the photolithography process. After cooling to room temperature, the furnace was again heated to 800 °C in 30 min under the protection of Ar (500 s.c.c.m.) before CNT growth. In a typical CVD growth process of CNTs, H_2/Ar (50/50 s.c.c.m.) was used to reduce the catalyst for 10 min at 800 °C. Subsequently, an Ar flow of ~50 s.c.c.m. through an ethanol bubbler and a hydrogen flow of ~50 s.c.c.m. were introduced into the CVD furnace for 23 min for CNT growth. The system was then cooled to room temperature in an Ar atmosphere to finish the growth process.

PMMA films were used as the medium to transfer the CNT arrays from a quartz substrate onto the target Si/SiO_2 structure. The substrate with CNT arrays was covered with a photoresist film by spin coating and then dried at room temperature. An open-box tape was attached to the photoresist film for avoiding fracture, and then the substrate was immersed in a hydrofluoric acid buffer. After being automatically released from the substrate, the photoresist film with CNTs was taken out and immersed into deionized water for removing the remains of the hydrofluoric acid buffer. Then, a drop of water was dropped onto the target substrate and the photoresist film was put on the water drop. After the water drop dried and the photoresist film was firmly attached, the new substrate with the photoresist film and CNTs was immersed into acetone, *N*-methyl-2-pyrrolidone and alcohol for 20 min each and then dried using high-purity nitrogen to finish the CNT film transfer process.

Fabrication and measurement of twin PUFs. CNT FETs in twin PUFs were fabricated with a back-gate structure. Pd/Au stack metal films of about 20/60 nm were first deposited via EBE on the CNT arrays to achieve an ohmic contact to CNTs. Unwanted CNTs were etched by reactive ion etching to form independent channels. Ti/Au stack metal films of about 20/100 nm were deposited as connected wires and testing pads. The as-fabricated CNT FETs were measured using a probe station (Cascade Summit 1100) and a semiconductor analyser (Keithley 4200).

Extraction of CP and fitting. The extraction of CP includes three steps: (1) read the grey values perpendicular to the CNT growth direction in the SEM image of CNT arrays; (2) locate the CNT positions by finding the local maximum values; (3) calculate the CPs by subtraction between the adjacent CNT positions. We used normal distribution, logistic distribution and log-normal distribution to fit the experiment data, and found that log-normal distribution yields the best fitting. Supplementary Fig. 6 shows the results of four samples with different CNT densities, where Supplementary Fig. 6c,d are extracted from the literature. Variable X is log-normally distributed if $Y=\ln(X)$ is normally distributed, and the probability density function and cumulative distribution function of log-normal distribution are given by

$$p(x) = \frac{1}{x\sigma\sqrt{2\pi}} e^{-\frac{(\ln(x-\mu))^2}{2\sigma^2}},\ x > 0, \tag{3}$$

$$F(X \le x) = \frac{1}{2}\mathrm{erfc}\left(-\frac{\ln(x-\mu)}{\sigma\sqrt{2}}\right), \tag{4}$$

respectively, where σ and μ are parameters, x is a random variable and erfc is the complementary error function. Specifically, the arithmetic mean and standard deviation of a log-normally distributed variable X are given by

$$E(X) = e^{\mu+\frac{\sigma^2}{2}}, \tag{5}$$

$$\mathrm{SD}(X) = e^{\mu+\frac{\sigma^2}{2}}\sqrt{e^{\sigma^2}-1}, \tag{6}$$

respectively, where E and SD are the arithmetic mean and standard deviation, respectively. Conversely, the parameters μ and σ can be obtained from the arithmetic mean and standard deviation and are given by

$$\mu = \ln\left(\frac{E^2}{\sqrt{\mathrm{SD}^2+E^2}}\right), \tag{7}$$

$$\sigma = \sqrt{\ln\left(1+\frac{\mathrm{SD}^2}{E^2}\right)}, \tag{8}$$

respectively.

Randomness of CNT arrays. The randomness of CNT PUFs comes from the randomness of CNT arrays themselves including position and chirality. As shown in Supplementary Fig. 2, CPs are randomly distributed and the adjacent pitch differences follow a normal distribution, which means there is little influence of one pitch on adjacent pitches. As shown in Supplementary Fig. 3, from the atomic force microscopy image of the CNT arrays, we extracted the diameters along with tubes, and the diameters are also randomly distributed perpendicular to the CNT growth direction.

Simulation of PUFs on CNT arrays. CNT arrays are simulated using three parameters: the mean of the CP, the standard deviation of the CP and the MSR. Through equations (7) and (8), parameters μ and σ can be obtained to generate a set of data (CP), and to generate the CNT positions by accumulating CPs. The generated CNTs are semiconducting with a probability of $1/(1+\mathrm{MSR})$, and the others are metallic. The FETs are simulated with different channel widths (W_{ch}) and a spacing of 5 µm. Supplementary Fig. 7 shows the illustration of a simulated CNT array and FETs, given the following parameters: CP = 2.0 ± 1.5 µm, MSR = 1:2 and W_{ch} values of 0.5, 1.0 and 2.0 µm.

According to the electrical properties, CNT FETs can be classified into three types: O type (without CNTs in the channel), S type (only semiconducting CNTs in the channel) and M type (at least one metallic CNT in the channel). We simulated 3×10^5 FETs for every W_{ch} value, changing from 0 to 4.0 µm with a step of 0.1 µm (CP = 1.0 ± 0.5 µm and MSR = 1/2), and calculated the relation of the probabilities of three FET types with W_{ch} values (Supplementary Fig. 7a). With W_{ch} increasing, the ratios of O-, S- and M-type FETs decreases monotonously, first increases and then decreases, and increases monotonously, respectively. The non-monotonic change in the ratio of S-type FETs comes from the rapid increase in FETs having mixed semiconducting and metallic CNTs in the channel when W_{ch} exceeds 1 µm (Supplementary Fig. 7b).

Optimization of ternary keys. O-, S- and M-type FETs should be tuned to have an equal probability of 1/3 to realize an ideal ternary key. This optimization requires the ratio–W_{ch} curves of three FET types have the same intersections, which can be simplified to another task that the longitudinal coordinate of the intersection of two of the curves is equal to 1/3. We selected O- and M-type FETs to study it, because their ratios change monotonously.

As shown in Supplementary Fig. 8, we simulated the ratio–W_{ch} curves with different metallic CNT ratios (MR, CP = 1.0 ± 0.5 µm). With the MR increasing from 0.3 to 0.6, the ratio of M-type FETs increases, whereas the ratio of O-type FETs remains constant. When the MR is about 0.48, the longitudinal coordinate of the intersection of two of the curves is closest to 1/3. As shown in Supplementary Fig. 9, we simulated the ratio–W_{ch} curves with different standard deviations (MR = 1/3 and the mean of the CP is 1 µm). With the standard deviation of CNT pitches increasing from 0.1 to 0.9, the ratio of M-type FETs decreases slightly, whereas the ratio of O-type FETs increases substantially. When the MR is increasing, the longitudinal coordinate of the intersection of two of the curves is closer to 1/3.

To study the influence of both standard deviation and MR on the optimized target, we define MD as a sum of the square difference between the ratios of O-, S- and M-type FETs and the ideal value (1/3) for a given CP and MR. The MD is given by

$$\mathrm{MD} = \min\left\{\left(R_\mathrm{O}-\frac{1}{3}\right)^2+\left(R_\mathrm{S}-\frac{1}{3}\right)^2+\left(R_\mathrm{M}-\frac{1}{3}\right)^2\right\}, \tag{9}$$

where R_O, R_S and R_M represent the ratios of O-, S- and M-type FETs, respectively, and are functions of W_{ch}. We used the coefficient of variation to replace the standard deviations to perform the simulation so that it is more universal. We simulated MD with the coefficient of variation from 0.4 to 1.0 and MR from 0.2 to 0.7 (Supplementary Fig. 10). Through the co-optimization of CP and MR, MD can be reduced to be smaller than 10^{-4}, and our work yielded MD of close to 10^{-4}.

Extraction of metallic ratio of CNT arrays. The most common way based on the electrical measurement to extract the MR or semiconducting ratio (SR) is to calculate the on/off ratio (OR) from the transfer characteristic curves of FETs with a wide channel on the CNT array. The MR and SR values are given by

$$\mathrm{MR} = \frac{1}{\mathrm{OR}}, \tag{10}$$

$$\mathrm{SR} = \frac{\mathrm{OR}-1}{\mathrm{OR}}, \tag{11}$$

respectively. We used this method to extract MR of the CNT arrays used in PUFs to be 38% (Supplementary Fig. 11a). This method is based on a hypothesis that the on-state current of a semiconducting tube is equal to that of a metallic CNT; however, this hypothesis is not accurate, since metallic CNTs have large on-state currents.

We designed another method to more accurately extract the MR/SR of CNT arrays in which many small FETs are used. The channel needs to be narrow enough to make sure that the number of CNTs in the channel is not larger than one; then, R_M/R_S will be equal to MSR. MR and SR are given by

$$\mathrm{MR} = \frac{R_\mathrm{M}}{R_\mathrm{M}+R_\mathrm{S}}, \tag{12}$$

$$\mathrm{SR} = \frac{R_\mathrm{S}}{R_\mathrm{M}+R_\mathrm{S}}, \tag{13}$$

respectively. According to the simulation shown in Supplementary Fig. 8, the ratio of the mixed M/S FETs is close to zero when W_{ch} is smaller than about 500 nm. As shown in Supplementary Fig. 11b, we calculate $R_M/(R_S+R_M)$, and used these data with W_{ch} ranging from 100 to 500 nm to fit the MR of about 43%.

Calculation of possible CN. The possible CNs of ternary keys and binary keys are given by

$$\mathrm{CN}_3 = C_n^c C_c^m = \frac{n!}{c!(n-c)!}\frac{c!}{s!(c-s)!} = \frac{n!}{o!s!m!}, \quad (14)$$

$$\mathrm{CN}_2 = C_n^c = \frac{n!}{c!(n-c)!} = \frac{n!}{c!o!}, \quad (15)$$

respectively, where n, c, s, m and o represent the number of all the FETs, connected FETs, S-type FETs, M-type FETs and O-type FETs, respectively. We calculated CN_3 by changing s and m and keeping n constant; we found that CN_3 reaches the maximum value when $m = s = \frac{n}{3}$. Fabricating a 300-bit ternary key, our PUF gives (s, m) of (103, 97), making CN_3 reach 3.44×10^{140}, whereas the PUF from the literature gives (s, m) of (69, 80), making CN_3 reach 2.90×10^{132}. As shown in Supplementary Fig. 14, we also compared the maximum CN of ternary keys and binary keys with the same key size, and ternary keys have a much larger CN.

Inter-HD and intra-HD. The uniqueness and reliability of a PUF are characterized by inter-HD and intra-HD, respectively, and the means of normalized inter-HD and intra-HD are given by

$$\mu_{N\_\mathrm{inter\_HD}} = \frac{2}{KN(N-1)}\sum_{i=1}^{N-1}\sum_{j=i+1}^{N}\mathrm{HD}(S_i, S_j), \quad (16)$$

$$\mu_{N\_\mathrm{intra\_HD}} = \frac{1}{KN}\sum_{i=1}^{N}\mathrm{HD}(S_i, S_i'), \quad (17)$$

respectively, where S_i and S_j are the ith and jth key extracted from the CNT PUFs, respectively, S_i' is the ith key extracted from the CNT PUFs at a different time or different environment (where K is the size of one key) and N is the total number of keys. For an ideal multivariate key with M choices in one bit, the expectation of inter-HD is equal to $\frac{MK}{M+1}$; therefore, the mean of normalized inter-HD is given by

$$\mu_{N\_\mathrm{inter\_HD}} = \frac{M}{M+1}. \quad (18)$$

The means of normalized inter-HD of ideal ternary keys and binary keys are 2/3 and 1/2, respectively, according to equation (18).

Entropy calculation. In information theory, given a discrete random variable X, with possible outcomes $x_1, x_2, \ldots, x_n$, which occur with probability $P(x_1), P(x_2), \ldots, P(x_n)$, the entropy of X is defined as

$$E = -\sum_{i=1}^{n} P(x_i)\log_2\left[P(x_i)\right], \quad (19)$$

For our ternary PUFs, $P_\mathrm{O} = 33.25\%$, $P_\mathrm{S} = 32.25\%$ and $P_\mathrm{M} = 34.50\%$; therefore, the entropy is calculated as 1.58.

Simulation of consistency of twin PUFs. The inconsistent FETs in twin PUFs can be caused by imperfect CNT growth, which includes the existence of broken tubes, chiral change and array misalignment. First, we consider the existence of broken tubes, and assume a tube has a constant and uniform probability to stop growing in every unit distance. The probability of a tube with length larger than L is given by

$$P|_{l\geq L} = (1-\alpha L_0)^{L/L_0}, \quad (20)$$

where l is the length of the tube, α is the probability of stopping growing in every unit distance and L_0 is a very short length and can be divisible by L. When L_0 is close to zero, the limitation of equation (20) is given by

$$P|_{l\geq L} = \mathrm{e}^{-\alpha L}. \quad (21)$$

According to equation (18), the average length of the CNT array is given by

$$L_m = \int_0^{+\infty} \mathrm{e}^{-\alpha L}\alpha L\mathrm{d}L = \frac{1}{\alpha}. \quad (22)$$

According to the literature, the average length is about 300 μm (ref. [37]); then, α is equal to 3.33 mm^{-1}. However, α can be reduced by optimizing the growth condition including proper C:H ratio, steady growth environment, cleaner substrate and so on.

Then, we consider the chiral transition between metallic tubes and semiconducting tubes, and assume a tube has a constant and uniform probability to change its chirality in every unit distance. The probability of a tube at a distance L having a different chirality with its original chirality is given by

$$P = \sum_i C_{L/L_0}^{2i-1}(\beta L_0)^{2i-1}(1-\beta L_0)^{L/L_0+1-2i}, \quad (23)$$

where β is the probability of a chiral transition in every unit distance and L_0 is a very short length and can be divisible by L. Because of the need of extra energy to overcome the barrier, the chiral transition is difficult; hence, we only consider a single chiral transition. Then, equation (20) is simplified as

$$P = \beta L. \quad (24)$$

Overall, the probability of a tube at a distance L having the same electrical properties with its original ones is given by

$$P = (1-\beta L)\mathrm{e}^{-\alpha L}. \quad (25)$$

The misalignment comes from the defect and dislocation of the quartz substrate, containment on the substrate and unsteady growth atmosphere. We use angles between the CNTs to measure the misalignment degree (Supplementary Fig. 20) and the normalized angle has a small standard deviation of 0.09°.

This inconsistency can also be caused by the fabrication process, including FET failure and angular deviation between the FET channel direction and CNT growth direction. In a mature device fabrication process, the probability of FET failure can be reduced to a very low value, and we assume it causes a 1% decrease in our simulation. In our twin PUFs, the angle between the FET channel direction and CNT growth direction is smaller than 0.05°.

Overall, we simulated the consistency versus distance of the twin PUFs (Fig. 4c). The consistency can be largely increased by optimizing the growth of the CNT arrays and device fabrication process (Fig. 4d and Supplementary Fig. 21) and thus increase the allowable distance of twin PUFs.

Data availability

The data that support the findings of this study are available from the corresponding authors upon reasonable request.

Received: 10 July 2021; Accepted: 24 May 2022;
Published online: 4 July 2022

References

1. Goldreich, O. *Foundations of Cryptography: Basic Tools* (Cambridge Univ. Press, 2001).
2. Rivest, R., Shamir, A. & Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **21**, 120–126 (1978).
3. Thorsteinson, P. & Ganesh, G. G. A. *NET Security and Cryptography* (Prentice Hall Professional, 2004).
4. Shor, P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.* **26**, 1484–1509 (1997).
5. Sadeghi, A. R. & Naccache, D. *Towards Hardware-Intrinsic Security: Foundations and Practice* (Springer, 2010).
6. Kömmerling, O. & Kuhn, M. G. Design principles for tamper-resistant smartcard processors. *Smartcard* **99**, 9–20 (1999).
7. Shor, P. W. & Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **85**, 441–444 (2000).
8. Scarani, V. et al. The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301–1350 (2009).
9. Beveratos, A. et al. Single photon quantum cryptography. *Phys. Rev. Lett.* **89**, 187901 (2002).
10. Aspelmeyer, M., Jennewein, T., Pfennigbauer, M., Leeb, W. R. & Zeilinger, A. Long-distance quantum communication with entangled photons using satellites. *IEEE J. Sel. Topics Quantum Electron.* **9**, 1541–1551 (2003).
11. Pappu, R., Recht, B., Taylor, J. & Gershenfeld, N. Physical one-way functions. *Science* **297**, 2026–2030 (2002).
12. Herder, C., Yu, M.-D., Koushanfar, F. & Devadas, S. Physical unclonable functions and applications: a tutorial. *Proc. IEEE* **102**, 1126–1141 (2014).
13. Roel, M. *Physically Unclonable Functions: Constructions, Properties and Applications*. PhD thesis, Univ. KU Leuven (2012).
14. Kang, H., Hori, Y., Katashita, T., Hagiwara, M. & Iwamura, K. Cryptographic key generation from PUF data using efficient fuzzy extractors. In *16th International Conference on Advanced Communication Technology* 23–26 (IEEE, 2014).
15. Maes, R., Van Herrewege, A. & Verbauwhede, I. PUFKY: a fully functional PUF-based cryptographic key generator. In *International Workshop on Cryptographic Hardware and Embedded Systems* 302–319 (Springer, 2012).
16. Rührmair, U. & Holcomb, D. E. PUFs at a glance. In *2014 Design, Automation & Test in Europe Conference & Exhibition (DATE)* 1–6 (IEEE, 2014).
17. Gassend, B., Clarke, D., van Dijk, M. & Devadas, S. Silicon physical random functions. In *Proc. 9th ACM Conference on Computer and Communications Security* (ed. Atluri, V.) 148–160 (ACM Press, 2002).
18. Bolotnyy, L. & Robins, G. Physically unclonable function-based security and privacy in RFID systems. In *Fifth Annual IEEE International Conference on Pervasive Computing and Communications (PerCom'07)* 211–220 (IEEE, 2007).

19. Guajardo, J., Kumar, S. S., Schrijen, G.-J. & Tuyls, P. FPGA intrinsic PUFs and their use for IP protection. In Cryptographic Hardware and Embedded Systems—CHES 2007 (eds. Paillier, P. & Verbauwhede, I.) 63–80 (Springer, 2007).
20. Rahman, F., Shakya, B., Xu, X. L., Forte, D. & Tehranipoor, M. Security beyond CMOS: fundamentals, applications, and roadmap. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* **25**, 3420–3433 (2017).
21. Waser, R., Dittmann, R., Staikov, G. & Szot, K. Redox-based resistive switching memories—nanoionic mechanisms, prospects, and challenges. *Adv. Mater.* **21**, 2632–2663 (2009).
22. Chen, A. Comprehensive assessment of RRAM-based PUF for hardware security applications. *In Proc. 2015 IEEE International Electron Devices Meeting (IEDM)* 10.7.1–10.7.4 (IEEE, 2015).
23. 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).
24. 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).
25. Hu, Z. Y. & Han, S.-J. Creating security primitive by nanoscale nanipulation of carbon nanotubes. In *2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)* 29–34 (IEEE, 2017).
26. Hu, Z. et al. Physically unclonable cryptographic primitives using self-assembled carbon nanotubes. *Nat. Nanotech.* **11**, 559–565 (2016).
27. Dodda, A. et al. Graphene-based physically unclonable functions that are reconfigurable and resilient to machine learning attacks. *Nat. Electron.* **4**, 364–374 (2021).
28. 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).
29. He, Z. et al. Design of delayed ternary PUF circuit based on CNFET. In *2018 24th Asia-Pacific Conference on Communications (APCC)* 503–507 (IEEE, 2018).
30. 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).
31. Delavar, M., Mirzakuchaki, S., Ameri, M. H. & Mohajeri, J. PUF based solutions for secure communications in advanced metering infrastructure AMI. *Int. J. Commun. Syst.* **67**, 74–88 (2017).
32. Chatterjee, U., Chakraborty, R. S. & Mukhopadhyay, D. A PUF-based secure communication protocol for IoT. *ACM Trans. Embedded Comput. Syst.* **16**, 67 (2017).
33. Liu, L. et al. Aligned, high-density semiconducting carbon nanotube arrays for high-performance electronics. *Science* **368**, 850–856 (2020).
34. Shi, H. et al. Radiofrequency transistors based on aligned carbon nanotube arrays. *Nat. Electron.* **4**, 405–415 (2021).
35. Zhao, C. et al. Strengthened complementary metal–oxide–semiconductor logic for small-band-gap semiconductor-based high-performance and low-power application. *ACS Nano* **14**, 15267–15275 (2020).
36. Bishop, M. D. et al. Fabrication of carbon nanotube field-effect transistors in commercial silicon manufacturing facilities. *Nat. Electron.* **3**, 492–501 (2020).
37. Hills, G. et al. Modern microprocessor built from complementary carbon nanotube transistors. *Nature* **572**, 595–602 (2019).
38. Shulaker, M. M. et al. Three-dimensional integration of nanotechnologies for computing and data storage on a single chip. *Nature* **547**, 74–78 (2017).
39. 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).
40. Kang, S. J. et al. High-performance electronics using dense, perfectly aligned arrays of single-walled carbon nanotubes. *Nat. Nanotechnol.* **2**, 230–236 (2007).
41. Zhang, J., Patil, N., Hazeghi, A. & Mitra, S. Carbon nanotube circuits in the presence of carbon nanotube density variations. In *Proc. 46th Annual Design Automation Conference* 71–76 (ACM, 2009).
42. Franklin, A. D. The road to carbon nanotube transistors. *Nature* **498**, 443–444 (2013).
43. Xiao, J. L. et al. Alignment controlled growth of single-walled carbon nanotubes on quartz substrates. *Nano Lett.* **9**, 4311–4319 (2009).
44. 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).
45. 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 International Electron Devices Meeting (IEDM)* 5.6.1–5.6.4 (IEEE, 2017).
46. Xie, X. et al. Microwave purification of large-area horizontally aligned arrays of single-walled carbon nanotubes. *Nat. Commun.* **5**, 5332 (2014).
47. 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).
48. Wang, J. T. et al. Growing highly pure semiconducting carbon nanotubes by electrotwisting the helicity. *Nat. Catal.* **1**, 326–331 (2018).
49. 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).
50. 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).
51. Rukhin, A. et al. *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*. Report No. 800-22 (NIST, 2001).
52. Dresselhaus, G., Dresselhaus, M. S. & Saito, R. *Physical Properties of Carbon Nanotubes* (Imperial College Press, 1998).
53. Xie, Y. et al. Highly temperature-stable carbon nanotube transistors and gigahertz integrated circuits for cryogenic electronics. *Adv. Electron. Mater.* **7**, 2100202 (2021).
54. Westermana, R. J. et al. Plasma dicing: current state & future trends. *ECS Trans.* **69**, 3–14 (2015).

Acknowledgements

This work was supported by the National Key Research & Development Program (grant no. 2021YFA1202904); the Beijing Municipal Science and Technology Commission (grant no. Z191100007019001-3); the Basic and Applied Basic Research Major Programme of Guangdong Province, China (grant no. 2021B0301030003); and Jihua Laboratory (project no. X210141TL210).

Author contributions

Z.Z. and L.-M.P. proposed and supervised the project. D.Z., Z.Z. and L.-M.P. conceived the idea of twin PUFs and designed the experiment. D.Z. fabricated the devices. D.Z., J.L., Y.X., H.S. and C.Z. performed the electrical measurements. D.Z. performed the modelling and simulations. M.X. grew and characterized the 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 co-wrote the manuscript. All the authors discussed the results and commented on the manuscript.

Competing interests

The authors declare no competing interests.

Additional information

Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s41928-022-00787-x.

Correspondence and requests for materials should be addressed to Lian-Mao Peng or Zhiyong Zhang.

Peer review information *Nature Electronics* thanks Miguel Garcia-Bosque, Jin-Woo Han and Satish Kumar for their contribution to the peer review of this work.