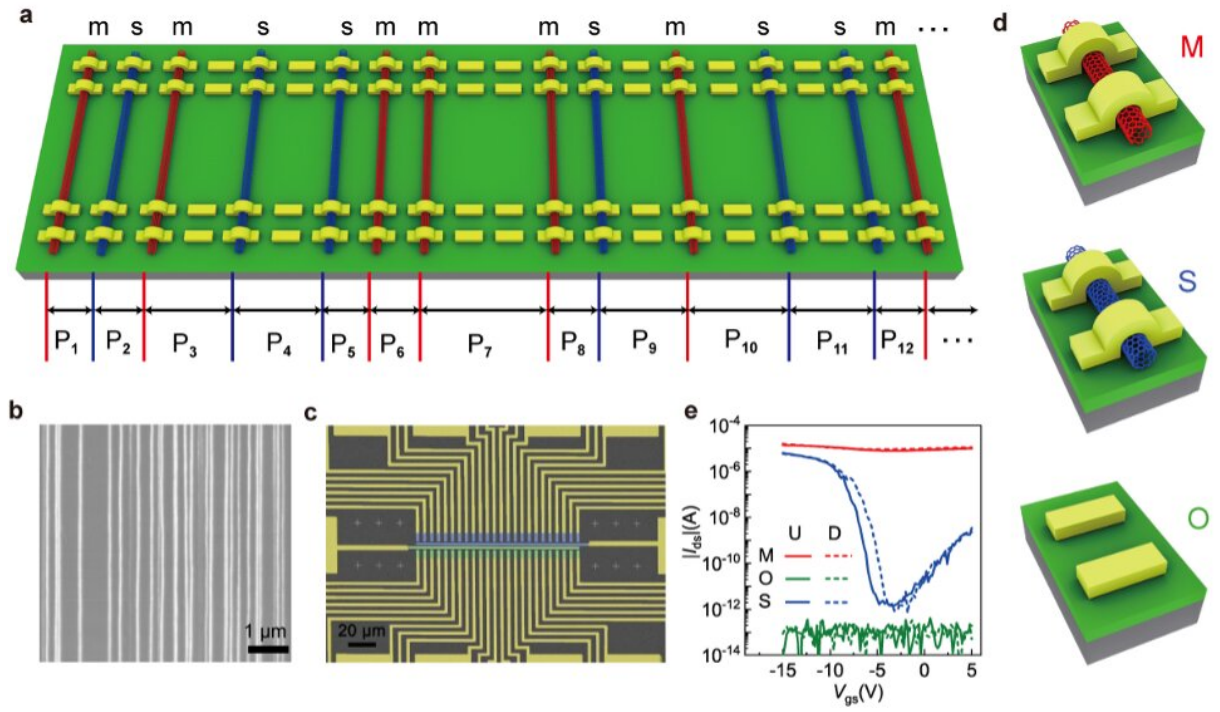
Twin physically unclonable functions (PUFs) based on carbon nanotube arrays to enhance the security of communications

July 28 2022, by Ingrid Fadelli



Twin physically unclonable functions based on aligned 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, SEM image of aligned CNT array. d, False-colored SEM image showing a group of 24 pairs of twin PUF devices. e, Transfer characteristics measured from the three pairs of devices in (d). Credit: Zhong et al.

As the amount of data stored in devices and shared over the internet continuously increases, computer scientists worldwide are trying to devise new approaches to secure communications and protect sensitive information. Some of the most well-established and valuable approaches are cryptographic techniques, which essentially encrypt (i.e., transform) data and texts exchanged between two or more parties, so that only senders and receivers can view it in its original form.

Physical unclonable functions (PUFs), devices that exploit "random imperfections" unavoidably introduced during the manufacturing of devices to give physical entities unique "fingerprints" (i.e., trust anchors). In recent years, these devices have proved to be particularly valuable for creating cryptographic keys, which are instantly erased as soon as they are used.

Researchers at Peking University and Jihua Laboratory have recently introduced a new system to generate cryptographic primitives, consisting of two identical PUFs based on aligned carbon nanotube (CNT) arrays. This system, introduced in a paper published in *Nature Electronics*, could help to secure communications more reliably, overcoming some of the vulnerabilities of previously proposed PUF devices.

"Classical cryptography uses cryptographic algorithms and keys to encrypt or decrypt information, and the most popular strategies are Rivest, Shamir, and Adleman (RSA) encryption," Zhiyong Zhang, one of the researchers who carried out the study, told TechXplore. "In an asymmetric algorithm, the public key can be accessed by anyone, but the public key cracking requires factoring a very large number, which is extremely difficult for a classical computer. This task has, however, been shown mathematically to be accomplishable in polynomial time using a quantum computer."

One of the most employed cryptographic strategies today is symmetric encryption, which shares the same "secret keys" for encryption and decryption with all users participating in a specific conversation. These strategies generally store secret keys in a non-volatile memory, which is vulnerable to physical and side-channel cyber-attacks.

In recent years, researchers have thus been exploring alternative cryptographic approaches, including quantum key distribution (QKD). QKD methods exploit concepts rooted in quantum theory to protect communications. Specifically, they leverage the intrinsic disturbances affecting quantum systems while they are being measured.

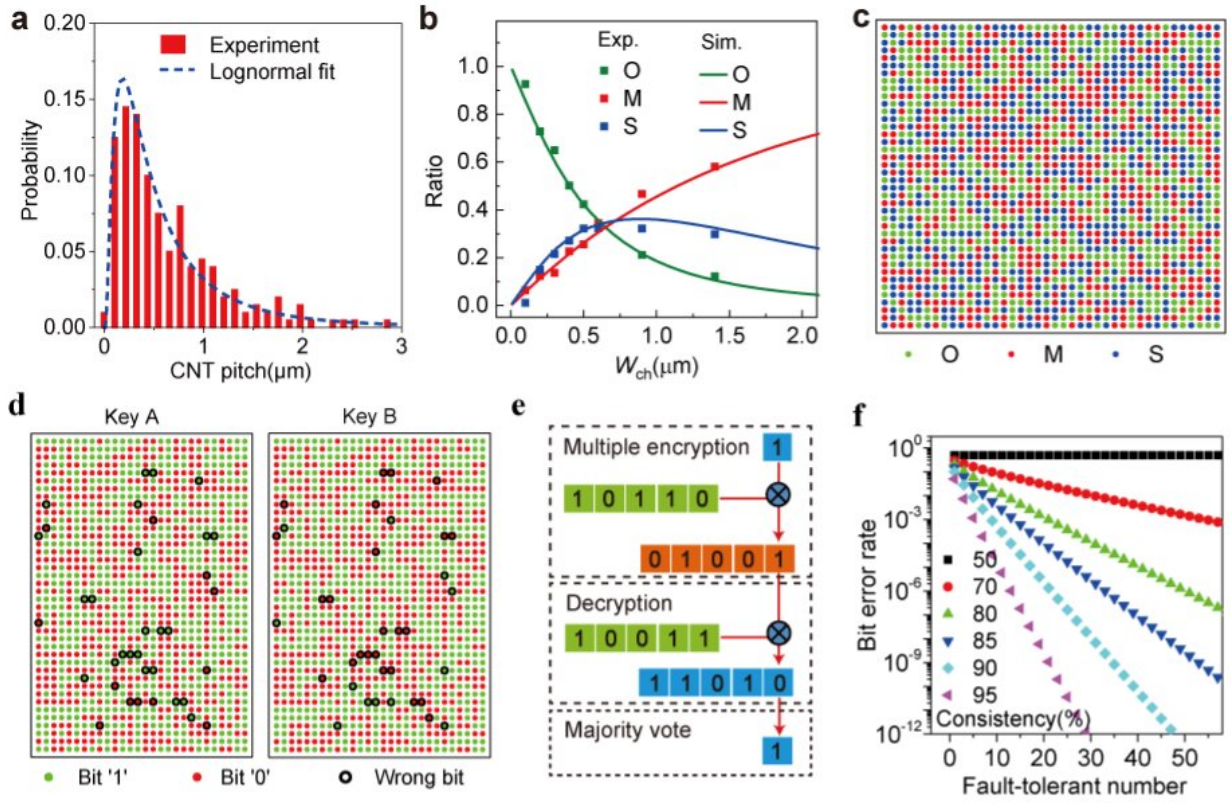
QKD has been found to be particularly effective at detecting a third party's attempts to gain access to the secret key protecting communications. While some QKD strategies have attained remarkable results, they typically require sophisticated and highly expensive hardware.

"To achieve a low-cost and hardware-based secure communication, we introduced a new technology, twin physically unclonable functions (PUFs)," Zhang said. "The basic idea behind 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."

Due to their unique design, PUF devices are unclonable and unpredictable. This makes them incredibly effective at generating safe secret keys for encryption.

Nonetheless, when PUFs are used to secure communications, the keys they produce need to be written on non-volatile memories and shared with other conversation participants that do not own a PUF device. These stored keys will thus be vulnerable to attacks.

The key objective of the recent work by Zhang and his colleagues was to overcome this limitation of PUF devices for securing communications. To do this, instead of cloning an existing PUF, they tried to create two identical (twin) PUFs.



Performance of CNT twin PUFs and demonstration of secure communication. a, Distribution of CNT pitch and lognormal fit of the data. b, Ratios of three types of devices versus channel width of PUF devices. The squares and lines represent experimental and simulation data, respectively. c, 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. d, 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. e, Schematic of secure communication using a fault-tolerant design. f, BER versus fault-tolerant number with different consistencies. Credit: Zhong et al.

"We fabricated twin physically unclonable functions (PUFs) based on aligned CNT arrays," Zhang explained. "Firstly, we grew aligned CNT arrays on quartz substrate. On one hand, induced by the quartz lattice-CNT interaction, CNT arrays grew along the [2 -1 -1 0] crystal orientation for several hundred microns, which ensured that the properties of CNT arrays were identical parallel to the growth direction. On another hand, CNT arrays have random characteristics, such as chirality and position, perpendicular to the CNT growth direction."

To create their device, Zhang and his colleagues fabricated two rows of field-effect transistors (FETs) on CNT arrays. They used transistors with three channel types with different electrical properties, namely channels containing some metallic CNTs (M), purely semiconducting CNTs (S) and no CNTs at all (O).

"Since the location and type of CNTs in the channel are determined by the stochastic nucleation and random catalyst distribution, FETs were fabricated on the CNT arrays," Zhang said. "Meanwhile, 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 (twin PUFs) can be fabricated together."

Zhang and his colleagues initially devised a model that would allow them to study the relationship between PUFs and both CNT arrays and device dimensions. This model allowed them to optimize the randomness and entropy of their PUFs.

"We found that the CNT pitches (CPs) meet the lognormal distribution, which was verified by other CNT samples we grew with different densities and those published by other groups," Zhang said.

Using simulations and the model they created as a reference, the researchers optimized their design and created CNT arrays with a CNT pitch of 0.65±0.58 μm and a metallic/semiconducting CNT ratio of approximately 0.4. They then used these arrays to create a prototype of their PUFs with ideal ternary bits.

"We fabricated a total of 1600 FETs with a channel width of 600 nm, to generate a 40×40 ternary bit map, in which 532, 516, and 552 O-, S- and M-bits were counted, respectively," Zhang said. "Our PUFs also exhibited high randomness, uniformity, uniqueness, unpredictability, and reliability."

In their experiments, the researchers successfully used their twin PUFs to attain fault-tolerant cryptography. Due to imperfections associated with the growth of the CNTs, including chirality transitions, the existence of broken tubes between catalyst stripes and misalignment, the team's twin PUFs initially showed a non-perfect consistency. This means that the encryption and decryption process could introduce wrong bits, which resulted in a high Bit Error Rate (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 generate one plain text bit through a majority vote," Zhang said. "The BER was exponentially reduced, with a fault-tolerant number for consistency greater than 80%. In 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."

In the future, the twin PUFs devices created by this team of researchers could help to secure communications more reliably on a large-scale. In their next studies, Zhang and his colleagues would like to improve their devices further, for instance by optimizing the materials used in their

recent work.

"We plan to improve the cleanness of the quartz substrate and the airflow stability during CNT growth, which can reduce the occurrence of broken tubes and the chirality change," Zhang added. "In this paper we used a global bottom gate, but we now also plan to change it to top-gate structure for small operation voltage and easy integration with other circuits. Finally, while so far we used a probe station to test our PUF unit one by one, the next step will be to integrate our twin PUFs with peripheral circuits, which can automatically realize the encryption of information."

More information: Donglai Zhong et al, Twin physically unclonable functions based on aligned carbon nanotube arrays, *Nature Electronics* (2022). DOI: 10.1038/s41928-022-00787-x