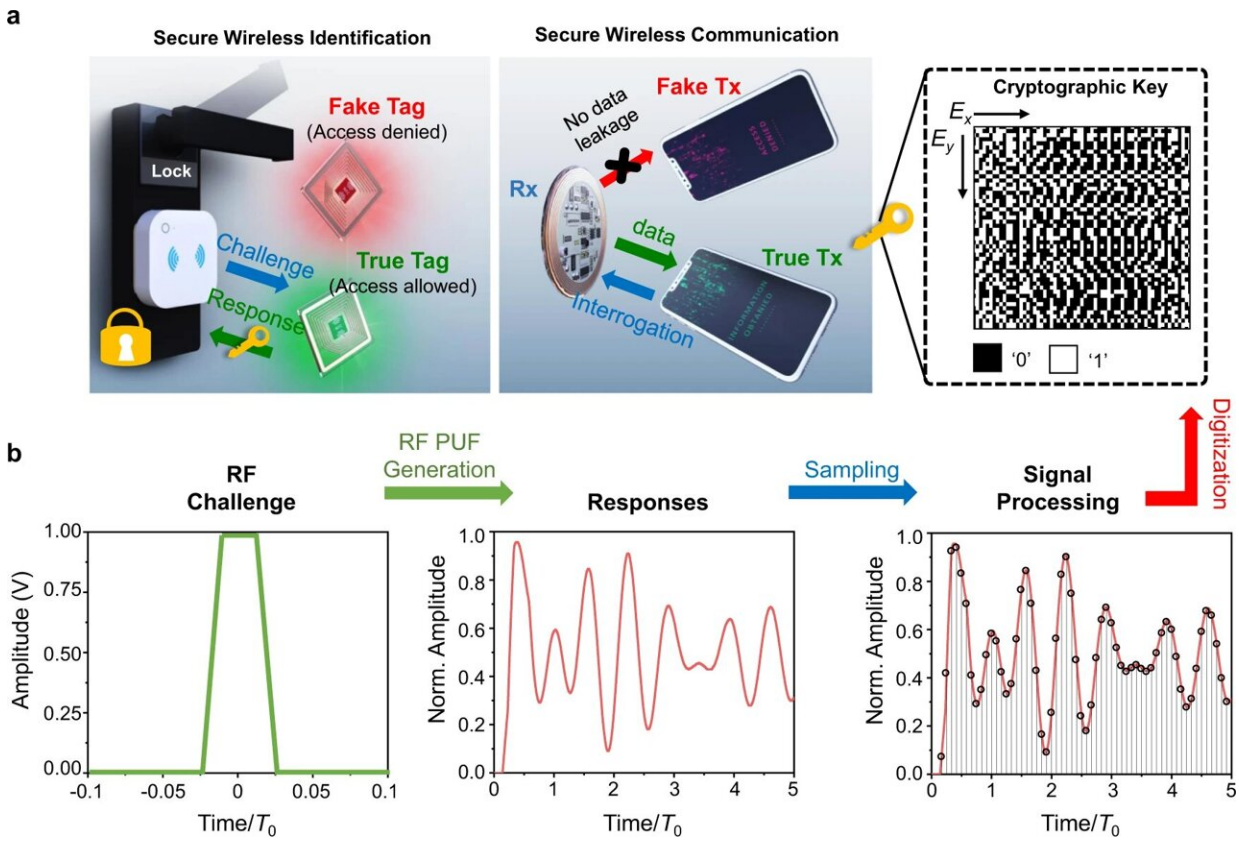
Using quantum physics to secure wireless devices

April 26 2023



Physically unclonable function (PUF) based cryptographic keys generated by the PT-symmetric electronic system. **a** Illustration of the PUF-enabled secure radio-frequency (RF) authentication and communication. **b** Generation of the challenge-response pair (CRP) and the cryptographic key in the proposed PUF system. Our experiments utilize the pulse excitation shown in the left panel of b, and the response, represented by the transient voltage signal measured across the reader's capacitor, and its discretized form are shown in the middle and right panels of b, respectively. After proper sampling and processing, the analog

response is converted to a digital key composed of a bitstring. Credit: *Nature Communications* (2023). DOI: 10.1038/s41467-023-36508-x

From access cards and key fobs to Bluetooth speakers, the security of communication between wireless devices is critical to maintaining privacy and preventing theft. Unfortunately, these tools are not foolproof and information on how to hack, clone and bypass these systems is becoming easier to find.

That's why computer engineers at the University of Illinois Chicago have been investigating ways to create more secure devices. In a new paper, UIC scientists report a method inspired by quantum physics to improve wireless device identification and protect device-to-device communication. It uses a truly random and unique digital fingerprint to create a hardware encryption system that is virtually unbreakable.

The scientists, led by Pai-Yen Chen, used a theory from quantum physics in math-based experiments to identify a "divergent exceptional point."

Quantum physics describes systems for which precise measurement is difficult or impossible; a quantum state describes a parameter space or range of possible measurements. Within these states, there exist exceptional points where the uncertainty of the system is at its maximum. These points are promising for cryptography—the more uncertain the system, the more secure.

Chen and colleagues figured out a mathematical approach to identify these exceptional points in a radio frequency identification system—the technology used by key cards, fobs and other devices that unlock or communicate with nearby sensors. In traditional RFID systems,

encrypted keys are stored inside memory chips, which are limited in size and vulnerable to attack.

Chen's group created new RFID lock-and-tag devices that utilize the exceptional point algorithm to create a secure signal. Since every piece of hardware is slightly different due to small variations during the fabrication process, each RFID device produces its own unique digital fingerprint in light of the maximized uncertainty at the exceptional point.

Like each individual's voice—which is heard via analog sound waves—their key cryptography structure makes the signal from each device unique, Chen said.

After thousands of simulations, they could not find two identical digital fingerprints, passing National Institute of Standards and Technology randomness tests and machine learning-based attacks.

"Many scientists have thought that the exceptional point theory would be impossible to apply reliably in the real world, but we were able to leverage such a property to implement a novel system," said Chen, associate professor of electrical and computer engineering at the UIC College of Engineering. "In this paper, we proposed a new circuit with a divergent exceptional point to significantly improve the uniqueness, randomness and robustness of an electromagnetic physically unclonable function."

"This lightweight and robust analog PUF structure may lead to a variety of unforeseen securities and anti-counterfeiting applications in radio-frequency fingerprinting and wireless communications," the authors write.

Chen said that the technology is also low cost and highly versatile, which

is why it could be particularly helpful for products, such as key cards and near-field communication devices, that are mass-produced and more vulnerable to hacks.

"We simply used the standard printed circuit board fabrication process, suitable for low-cost and mass production. The improved security lies in carefully designing the radio frequency circuit to operate around the exceptional point, which we demonstrated with a wireless identification system," Chen said.

"Spectral sensitivity near exceptional points as a resource for hardware encryption" is published in *Nature Communications*.

More information: Minye Yang et al, Spectral sensitivity near exceptional points as a resource for hardware encryption, *Nature Communications* (2023). DOI: 10.1038/s41467-023-36508-x

Provided by University of Illinois at Chicago