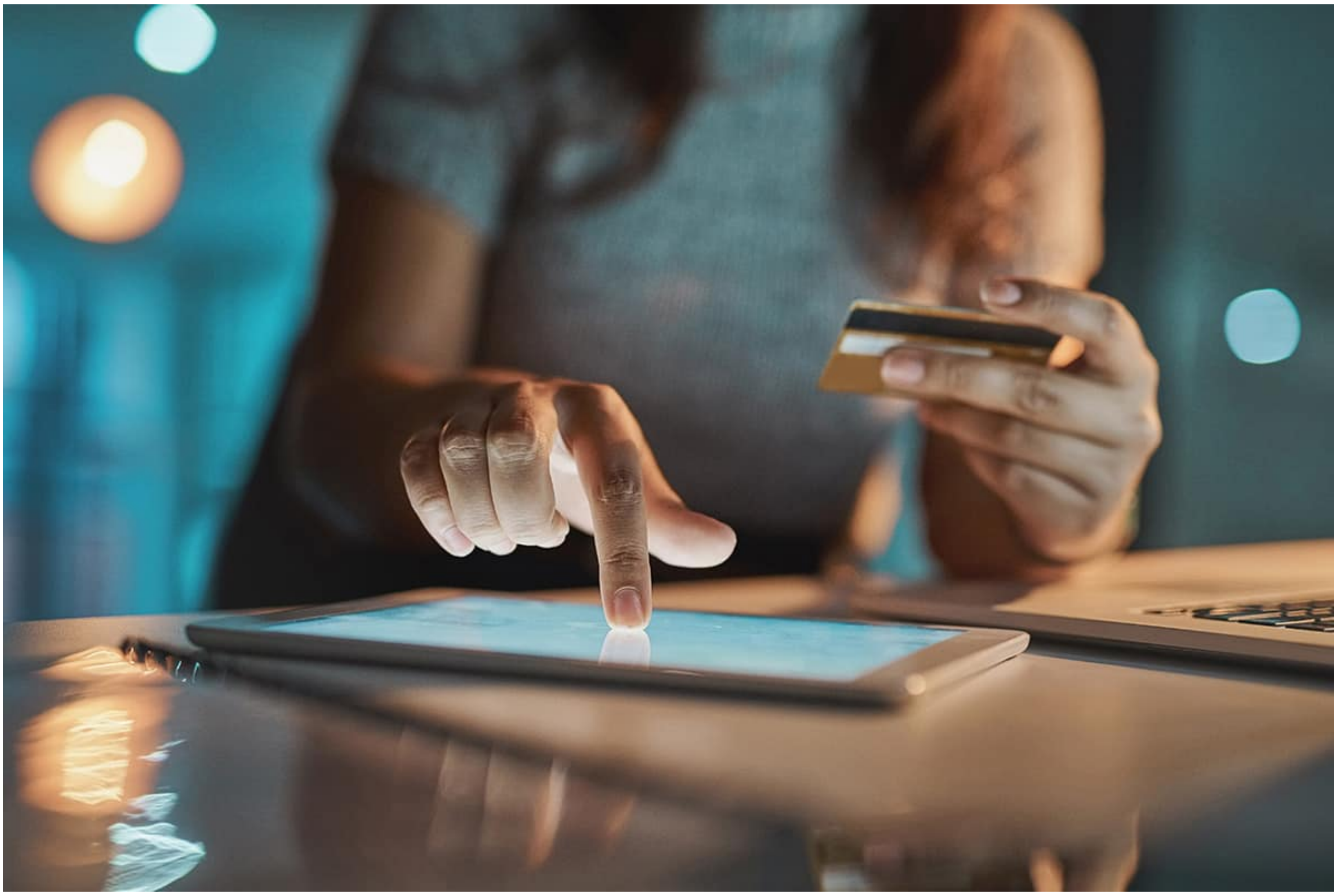
physicsworld

CRYPTOGRAPHY | RESEARCH UPDATE

Quantum-secure online shopping comes a step closer

23 Jan 2024



(Courtesy: iStock/Jay-Yuno)

Online shopping boomed during the pandemic, but it remains vulnerable to scams involving both buyers and sellers. Quantum communication could, in principle, add another layer of security, but verifying a transaction securely, rather than simply communicating it, requires a “signature” consisting of thousands of quantum bits (qubits) for a single bit of message.

For today’s noisy, imperfect quantum systems, that’s a very high bar, but researchers at China’s Nanjing University, Renmin University and the Beijing National Laboratory for Condensed Matter Physics found a way of lowering it. By using a mathematical technique called one-time universal hashing that generates shorter secure “keys”, the researchers substantially reduced the number of qubits required to verify an e-commerce transaction. They also considered different realistic source flaws based on a scheme that is independent of the measurement devices used, thereby avoiding the need for perfect signals to distribute the information.

From QKD to QDS

Quantum communication rests on the principle that anyone who tries to intercept a message encoded in quantum states will inevitably interfere with these states in a way that is easily detected. This principle is already used in quantum key distribution (QKD), but on its own, QKD cannot guarantee e-commerce security because it only provides a secure communication channel. It does not enforce other important e-commerce objectives such as integrity, authenticity or nonrepudiation (repudiation is where one party rejects the contract).

One possible way of fulfilling these other objectives involves a more complex method known as quantum digital security (QDS). This method uses the secure transmission of quantum states in QKD and the mathematics of information theory to generate unique keys for signing a contract and paying.

Ultra-secure protocol

The researchers' QDS protocol involves three parties: a merchant, a client and a third party (TP). It begins with the merchant preparing two sequences of coherent quantum states, while the client and the TP prepare one sequence of coherent states each. The merchant and client then send a state via a secure quantum channel to an intermediary, who performs an interference measurement and shares the outcome with them. The same process occurs between the merchant and the TP. These parallel processes enable the merchant to generate two keys that they use to create a signature for the contract via one-time universal hashing.

Once this occurs, the merchant sends the contract and the signature to the client. If the client agrees with the contract, they use their quantum state to generate a key in a similar way as the merchant and send this key to the TP. Similarly, the TP generates a key from their quantum state after receiving the contract and signature. Both the client and the TP can verify the signature by calculating the hash function and comparing their result to the signature. Payment can be made from the client to the TP if both verify the signature. If either of them cannot verify the signature, the contract is automatically aborted.

Quantum retailer

The researchers experimentally verified this protocol using optical fibres as quantum channels and a pulsed laser modulated in both phase and intensity to produce the quantum states for key generation. To eliminate the need for perfect devices, they characterized the source flaws of this system and combined the key generation process with a method called four-phase measurement device–independent QKD. This method uses the phase of the optical pulses at the intermediate interference measurement to obtain a secure key even if the intermediary that performs the measurement cannot be trusted.

To test the system's functionality, the team used it to sign a file containing 428 kB of data, which is approximately the size of an Amazon Web Services customer agreement. They were able to perform this signature 0.82 times per second, and the system worked even with the equivalent 100 km distance between the client and the merchant.

Team member Hua-Lei Yin, a quantum communications expert at Renmin, says the work shows it is possible to use non-repudiation features to perform e-commerce as efficiently and practically as private communications. The next step will be to demonstrate the technique in practical scenarios using real metropolitan quantum networks. "We hope to collaborate with more research groups to further develop quantum technology (including high-precision phase locking and phase tracking techniques) to improve the corresponding rates and transmission distances", he tells *Physics World*.

Qin Wang, an IT and networking expert at the Nanjing University of Posts and Telecommunications who was not involved in the research, says the quantum e-commerce scheme based on QDS offers enhanced security and practicality compared to corresponding classical schemes. The team's biggest achievement, she says, is to extend QDS to a useful scenario within e-commerce, thereby demonstrating its potential applications in daily life. She is, however, critical of Sagnac-type optical setup used in the experimental demonstration, which she says could be vulnerable to "Trojan horse" type hacks.

The research is published in *Science Advances*.

Martijn Boerkamp is a science writer based in the Netherlands

OUR MISSION

Physics World represents a key part of IOP Publishing's mission to communicate world-class research and innovation to the widest possible audience. The website forms part of the ***Physics World* portfolio**, a collection of online, digital and print information services for the global scientific community.