PHYS.ORG

Quantum physicists design unconditionally secure system for digital payments

July 4 2023

Artistic image of digital payments secured by quantum technology. Credit: Christine Schiansky

Have you ever been compelled to enter sensitive payment data on the website of an unknown merchant? Would you be willing to consign your credit card data or passwords to untrustworthy hands? Scientists from the University of Vienna have now designed an unconditionally secure system for shopping in such settings, combining modern cryptographic techniques with the fundamental properties of quantum light. The demonstration of such "quantum-digital payments" in a realistic environment has been published in *Nature Communications*.

Digital payments have replaced physical banknotes in many aspects of our daily lives. Similar to banknotes, they should be easy to use, unique, tamper-resistant and untraceable, but additionally withstand digital attackers and data breaches.

In today's payment ecosystem, customers' sensitive data is substituted by sequences of random numbers, and the uniqueness of each transaction is secured by a classical cryptographic method or code. However, adversaries and merchants with powerful computational resources can crack these codes and recover the customers' private data, and for example, make payments in their name.

A research team led by Prof. Philip Walther from the University of Vienna has shown how the quantum properties of light particles or photons can ensure unconditional security for digital payments.

In an experiment the researchers have demonstrated that each transaction cannot be duplicated or diverted by malicious parties, and that the user's sensitive data stays private. "I am really impressed how the quantum properties of light can be used for protecting new applications such as digital payments that are relevant in our every day's life," says Tobias Guggemos.

For enabling absolute secure digital payments, the scientists replaced classical cryptographic techniques with a quantum protocol exploiting single photons. During the course of a classical digital payment transaction the client shares a classical code—called cryptogram—with his payment provider (e.g. a bank or credit card company).

This cryptogram is then passed on between customer, merchant and payment provider. In the demonstrated quantum protocol this cryptogram is generated by having the payment provider sending particularly prepared single photons to the client.

For the payment procedure, the client measures these photons whereby the measurement settings depend on the transaction parameters. Since quantum states of light cannot be copied, the transaction can only be executed once. This, together with the fact that any deviation of the intended payment alters the measurement outcomes, which are verified by the payment provider, makes this digital payment unconditionally secure.

The researchers successfully implemented quantum-digital payments over an urban optical fiber link of 641m, connecting two university buildings in down-town Vienna. Digital payments currently operate within a few seconds.

"At present, our protocol takes a few minutes of quantum communication to complete a transaction. This is to guarantee security in the presence of noise and losses," says Peter Schiansky, first author of the paper. "However, these time limitations are only of technological nature," adds Matthieu Bozzio, who is convinced that "we will witness that quantum-digital payments reach practical performance in the very near future."

More information: Peter Schiansky et al, Demonstration of quantum-digital payments, *Nature Communications* (2023). DOI: 10.1038/s41467-023-39519-w

Provided by University of Vienna

Citation: Quantum physicists design unconditionally secure system for digital payments (2023, July 4) retrieved 28 April 2024 from https://phys.org/news/2023-07-quantum-physicists-unconditionally-digital-payments.html