Fraud-proof credit cards possible with quantum physics

December 15 2014

A team of researchers from the Netherlands has harnessed the power of quantum mechanics to create a fraud-proof method for authenticating a physical 'key' that is virtually impossible to thwart. Credit: The Optical Society (OSA) and MESA+ Institute for Nanotechnology, Complex Photonic Systems Department of the University of Twente

Credit card fraud and identify theft are serious problems for consumers

and industries. Though corporations and individuals work to improve safeguards, it has become increasingly difficult to protect financial data and personal information from criminal activity. Fortunately, new insights into quantum physics may soon offer a solution.

As reported in The Optical Society's (OSA) new high-impact journal *Optica*, a team of researchers from the Netherlands has harnessed the power of quantum mechanics to create a fraud-proof method for authenticating a physical "key" that is virtually impossible to thwart.

This innovative security measure, known as Quantum-Secure Authentication, can confirm the identity of any person or object, including debit and credit cards, even if essential information (like the complete structure of the card) has been stolen. It uses the unique quantum properties of light to create a secure question-and-answer (Q&A) exchange that cannot be "spoofed" or copied.

The "Question-and-Answer" Security Game

Traditional magnetic-stripe-only cards are relatively simple to use but also simple to copy. Recently, banks have begun issuing so-called "smart cards" that include a microprocessor chip to authenticate, identify and enhance security. But regardless of how complex the code or how many layers of security, the problem remains that an attacker who obtains the information stored inside the card can copy or emulate it.

The new approach outlined in this paper avoids this risk entirely by using the peculiar quantum properties of photons that allow them to be in multiple locations at the same time to convey the authentication questions and answers. Though difficult to reconcile with our everyday experiences, this strange property of light can create a fraud-proof Q&A exchange, like those used to authorize credit card transactions.

"Single photons of light have very special properties that seem to defy normal behavior," said Pepijn Pinkse, a researcher from the University of Twente and lead author on the paper. "When properly harnessed, they can encode information in such a way that prevents attackers from determining what the information is."

The process works by transmitting a small, specific number of photons onto a specially prepared surface on a credit card and then observing the tell-tale pattern they make. Since—in the quantum world—a single photon can exist in multiple locations, it becomes possible to create a complex pattern with a few photons, or even just one.

Due to the quantum properties of light, any attempt by a hacker to observe the Q&A exchange would, as physicists say, collapse the quantum nature of the light and destroy the information being transmitted. This makes Quantum-Secure Authentication unbreakable regardless of any future developments in technology.

Making Cards Quantum Secure

To provide security in the real world, a [credit card](#)—for example—would be equipped with a paper-thin section of white paint containing millions of nanoparticles. Using a laser, individual photons of light are projected into the paint where they bounce around the nanoparticles like metal balls in a pinball machine until they escape back to the surface, creating the pattern used to authenticate the card.

If "normal" light is projected onto the area, an attacker could measure the entering pattern and return the correct response pattern. A bank would therefore not be able to see a difference between the real card and the counterfeit signal projected by the attacker.

However, if a bank sends a pattern of single "quantum" photons into the

paint, the reflected pattern would appear to have more information - or points of light - than the number of photons projected. An attacker attempting to intercept the "question" would destroy the quantum properties of the light and capture only a fraction of the information needed to authenticate the transaction.

"It would be like dropping 10 bowling balls onto the ground and creating 200 separate impacts," said Pinkse. "It's impossible to know precisely what information was sent (what pattern was created on the floor) just by collecting the 10 bowling balls. If you tried to observe them falling, it would disrupt the entire system."

Quantum, But Not Difficult

According to Pinkse, this unique way of providing security is suitable for protecting government buildings, bank cards, credit cards, identification cards, and even cars. "The best thing about our method is that secrets aren't necessary. So they can't be filched either," he said.

Quantum-Secure Authentication could be employed in numerous situations relatively easily, since it uses simple and cheap technology—such as lasers and projectors—that is already available.