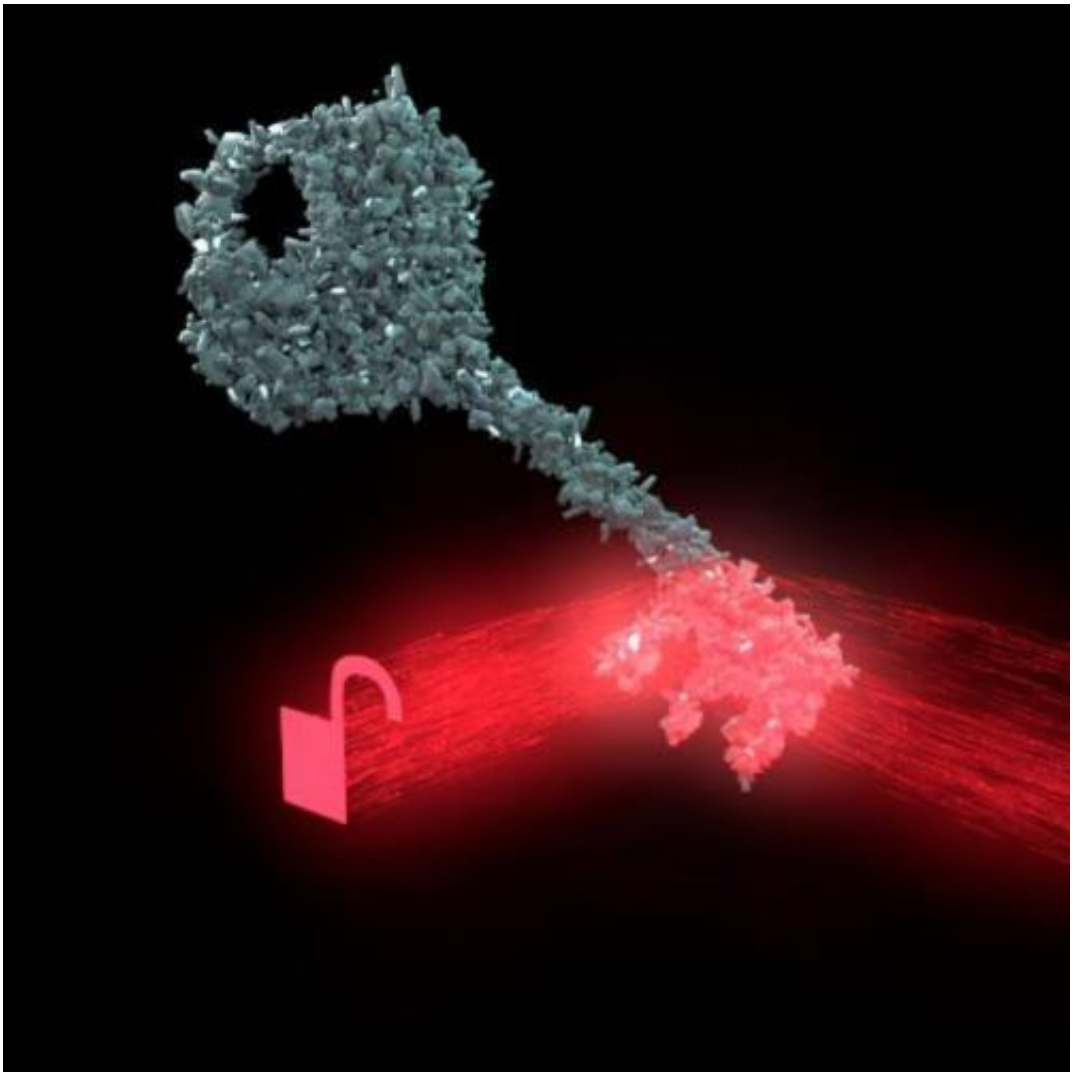
Quantum physics can fight fraud by making card verification unspoofable

February 5 2015, by Boris Škorić



Harnessing the quantum property of light takes security to the next level. Credit: Boris Skoric, Author provided

Decades of data security research have brought us highly reliable, standardized tools for common tasks such as digital signatures and encryption. But hackers are constantly working to crack data security innovations. Current credit/debit card technologies put personal money at risk because they're vulnerable to fraud.

Physical security – which deals with anti-counterfeiting and the authentication of actual objects – is part of the problem too. The good guys and bad guys are locked in a never-ending arms race: one side develops objects and structures that are difficult to copy; the other side tries to copy them, and often succeeds.

But we think our new invention has the potential to leave the hackers behind. This innovative security measure uses the quantum properties of light to achieve fraud-proof authentication of objects.

PUFs: fighting with open visors

The arms race is fought in secret; revealing your technology helps the enemy. Consequently, nobody knows how secure a technology really is.

Remarkably, a recent development called Physical Unclonable Functions (PUFs) has made it possible to be completely open. A PUF is a piece of material that can be probed in many ways and that produces a complex response that depends very precisely on the challenge and the PUF's internal structure.

The best known examples are Optical PUFs. The PUF is a piece of material – such as white paint with millions of nanoparticles – that will strongly scatter any light beamed at it. The light bounces around inside the paint, creating a unique pattern that can be used for authentication. Optical PUFs could be used on any object, but would be especially useful on credit/debit cards.

Imagine presenting your card to an ATM. The ATM fires a laser beam at the white paint on the card. The beam has an intricate, unpredictable "shape" (angle, focus, pixel pattern) randomly generated by the ATM, which serves as the challenge. Inside the PUF, the light scatters many times, causing lots of interference.The exiting light is the response – a complex pattern of dark and bright spots known as speckle that the ATM can record with a camera. The ATM has access to the PUF enrollment database and thus knows the properties of your card's PUF when you insert it. The ATM computes what the reflected speckle pattern should look like. If the resemblance is close enough, the ATM considers the card authentic.

Speckle is sensitive to tiny changes in the challenge and the PUF's structure. Due to the complexity of speckle physics, PUFs are practically unclonable.

The process for manufacturing PUFs does not have to be kept secret, precisely because of the unclonability: even if you know the manufacturing process, the uncontrollable randomness in the process still prevents you from cloning PUFs. One could organize open competitions and establish solid standards for physical security akin to those in cryptography.

Digital emulation still a problem

Shady dealings at the ATM? Optical PUFs to the rescue! Chris Goldberg, CC BY-NC

It's conceivable a PUF could be cloned exactly, or physically emulated precisely, although it would be very, very difficult. With Optical PUFs the good guys are firmly on the winning side in the arms race.

A bigger risk for the authentication protocol is digital emulation. A digital emulation attack on a particular PUF would consist of three steps:

- First, a hacker measures the challenge. In the ATM example, this is the laser beam.
- Second, the hacker obtains the response to this challenge. This can be done either by looking it up in a previously compiled table, or by running emulation software. (Remember, the attacker knows everything about each PUF because this is public knowledge.)
- Third, the hacker sends out laser light with what he's determined the correct "response" speckle pattern to be.

We are interested in "remote" authentication, where the verifier has no

direct control over the PUF, and the attacker knows everything about the PUF. This scenario typically requires the verifier to put in the field heavily defended hardware devices (like ATMs), whose task is to read PUFs without being spoofed. But this opens a second type of arms race, namely designing secure electronics versus hardware hacking and spoofing. In this kind of game the "good guys" often find themselves on the losing side.

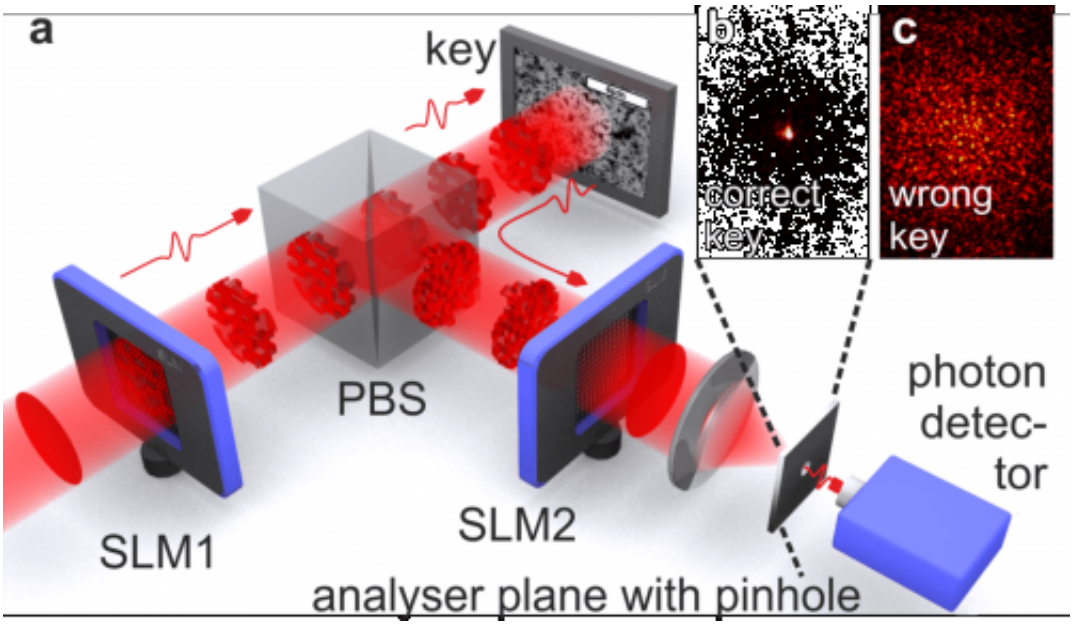
Solution: Quantum Readout

A few years ago, I realized that using quantum physics in the PUF readout would completely eliminate the threat of digital emulation.

The challenge has to be an unpredictable quantum state – that is, a single photon – which then interacts with the PUF and returns as a modified quantum state. Instead of a "classical" speckle pattern as above, the verifier is looking for a lone photon in a particular complicated quantum state.

Due to the laws of quantum physics, an attacker cannot accurately determine what the challenge is. If the hacker tries to watch the photon, he collapses the quantum state – any attempt at measurement destroys most of the information. And the No Cloning Theorem says that it's impossible to create an identical copy of a quantum state.

The attacker is out of luck. Not knowing the challenge, he doesn't know where to look in his lookup table for a response. The verifier, on the other side, knows exactly which response is expected (in contrast to the attacker, he does know the challenge) and is able to determine if the returning photon is in the right state.



Quantum-Secure Authentication uses two spatial light monitors and a particle beam splitter so that only the true unique key's response would make it through the pinhole to the photon detector. Credit: Boris Škorić, Author provided

Though the security of the Quantum Readout concept has been rigorously proven, it was not immediately clear how to realize Quantum Readout in practice.

Manipulation of light

The funny thing about a photon is that it is both particle and wave. Since it is a particle you have to detect it as a single chunk of energy. And being a wave, it spreads out and interferes with itself, forming a speckle pattern response. Quantum light is like a complicated-looking ghost. But how do you verify a single-photon speckle pattern?

In 2012, researchers at Twente University realized they held the answer in their hands. The magic ingredient is a Spatial Light Modulator (SLM),

a programmable device that re-shapes the speckle pattern. In their experiments, they programmed an SLM such that the correct response from an Optical PUF gets concentrated and passes through a pinhole, where a photon detector notices the presence of the photon. An incorrect response, however, is transformed to a random speckle pattern that does not pass through the pinhole.

The method was dubbed Quantum-Secure Authentication (QSA).

Quantum, but not difficult

QSA does not require any secrets, so no money has to be spent on protecting them. QSA can be implemented with relatively simple technology that is already available. The PUF can be as simple as a layer of paint.It turns out that the challenge does not have to be a single photon; a weak laser pulse suffices, as long as the number of photons in the pulse is small enough. Laser diodes, as found in CD players, are widely available and cheap. SLMs are already present in modern projectors. A sensitive photodiode or image sensor can serve as the photon detector.

With all these advantages, QSA has the potential to massively improve the security of cards and other physical credentials.

Source: The Conversation