Quantum mechanics could make money, credit cards, and tickets immune to fraud

October 3 2012, by Lisa Zyga

Currency is based on the assumption that it is impossible to duplicate bank notes and other objects that embody money. The uncertainty principle of quantum mechanics, attributed to Werner Heisenberg, may provide the ultimate key to making counterfeiting fundamentally impossible. Pastawski, et. al., show that this may even be possible if the storage of quantum states is imperfect. Credit: Fernando Pastawski.

(Phys.org)—Theoretically, the laws of quantum mechanics – particularly the "no-cloning theorem" – guarantee that any attempt at counterfeiting a credit card, bill, coin, token, etc., will fail if the object is embedded with quantum information. However, this security holds only under perfect conditions, whereas in real life quantum information is subject to noise,

decoherence, and operational imperfections, all of which provide loopholes that dishonest users might exploit. Since it's impossible to completely eliminate these imperfections, in a new study physicists have developed protocols that can tolerate some noise and still remain secure.

The scientists, from the Max Planck Institute for Quantum Optics in Garching, Germany; Harvard University in Cambridge, Massachusetts; and the California Institute of Technology in Pasadena, have published their study on noise-tolerant quantum protocols in a recent issue of *PNAS*.

"Our main contribution is to prove that the physical requirements for realizing unforgeable quantum tokens are significantly less demanding than previously thought," lead author Fernando Pastawski of the Max Planck Institute for Quantum Optics told *Phys.org*. "Only initialization storage and measurement of single qubits can suffice."

In a paper published in 1983, physicist Stephen Wiesner introduced the concept of "quantum money," or money that is immune to counterfeiting, by taking advantage of quantum properties. A quantum bank note is encoded with qubits, and not even the owner of this money can extract a complete description of the qubits' quantum states. Any measurements the owner makes only reveal part of this information, so that it is impossible to fully reconstruct the original quantum state. In other words, the money cannot be copied exactly.

If someone were to try to forge a quantum bank note, they would, in theory, almost always be caught by an authentication protocol based on classical communication. However, to tolerate the inherent noise in real situations, the verification process must allow for a small fraction of qubit failures; these relaxed standards give a dishonest person a chance of passing the authentication protocol with imperfectly forged quantum notes.

To address this shortcoming, the physicists in the current study have developed a new class of verification protocols that are tolerant to errors associated with encoding, storing, and decoding quantum bits. In one protocol, they focus on the relative fidelity levels of a counterfeit quantum ticket (qticket) and the tolerance fidelity of the verification process. They explain that a successful forgery attempt must contain a number of perfectly cloned qubits that is higher than the number required by the verification protocol. If the verification protocol requires a correct qubit number that is higher than that achievable for optimal qubit cloning, then the forgery is unlikely to succeed.

"Security is based on quantifying what the best possible counterfeiter can do when restricted only by the laws of quantum mechanics," Pastawski said. "Fraudulent tokens are excluded by setting verification requirements even higher. However, these verification requirements still leave room for honest participants who are subject to a mild amount of noise. Simply speaking, we can guarantee through quantum mechanics that, on average, no more than 83% of the secret digits may be duplicated correctly by a counterfeiter (this is where most of the theory work goes) and we assume that actual conditions allow honest participants to recover 95% of the digits correctly. If a verifier demands 90% of the digits to be returned as expected and the number of digits used is large, it will be almost impossible to have fraudulent tokens get by or to reject authentic ones."

In a second protocol, the researchers demonstrated a specific realization of an approach in which a quantum token's validity can be verified remotely by the token holder answering a set of questions by measuring the quantum states. Under these circumstances, remotely means that the verifier does not need to use quantum communication with the holder and does not need to be handed back the original token. The verification may take place by only having classical communication among verifier and holder. Although the token holder should be able to answer any

single question correctly, quantum laws dictate that there is only an exponentially small probability that the holder can correctly answer any two questions. By employing this protocol within a particular framework, the researchers showed that a dishonest user is exponentially unlikely to be authenticated by two independent verifiers, while an honest user would be verified.

Although the proof for the security of these protocols is complex, the researchers note that it may be possible to experimentally realize the protocols using current technology. Nevertheless, reaching parameter regimes that are actually useful is still far away. Qubit memory times need to be improved to the order of days and the number of controlled qubits scaled up to the hundreds of thousands. On the other hand, certain applications may not require long memory times, and these protocols may be realized using photon polarizations. Possible systems that could demonstrate the protocols include trapped ions, superconducting devices, and solid-state spins.

These protocols could have a variety of fraud prevention applications. For instance, the protocols could ensure that a credit card encoded with qubits cannot be split into two valid subparts; in other words, a credit card number could not be stolen and successfully used apart from the physical credit card.

The protocols could also prevent dishonest users from copying tickets for concerts or sporting events and then attempting to use the tickets at separate gates. Similarly, voter fraud could theoretically be eliminated if every voter was issued one quantum token that was impossible to duplicate. However, preventing voter fraud has other complications, such as ensuring anonymity, that make this issue more complex.

"The protocols in our paper are less demanding but also have fewer features than quantum money proposals," Pastawski said. "One simple

application that I like to think about is to have a privately transferable insurance. Of course, the insurance company does not want to have many copies of the same policy circulating, since each copy increases the chance of the policy being redeemed. This can be prevented by having the policy be embodied by a quantum token. The reason for thinking about the insurance policy scenario is that, on average, a policy is NOT redeemed and hence the insurance company would have no way to realize if copies are circulating. A transferable license of a given computer program constitutes a similar scenario. Usually no one controls such license, but if it does get controlled, only the legitimate holder would be able to pass such a control."

Pastawski added that these applications will take many years to be realized.

"Even the simplified implementation demands of our protocols defy current technology," he said. "The protocol itself could in principle be demonstrated now by using qubits consisting of single photon polarizations or single nuclear spins. However, in order to reach the time scales necessary for relevant applications, good qubit memories are needed that can hold quantum information for longer times and, more importantly, using a technology that is practical for the application at hand. I have collaborated in a project to extend the lifetime of such memories to one second, which was a record for single qubits at room temperature. Clearly, one second is not enough and apart from being a room-temperature implementation, the conditions cannot be claimed to be practical for applications. I think it will likely take more than 10 years in order for the necessary technologies to become practically available. However, I do hope to see this happen within my lifetime."

More information: Fernando Pastawski, et al. "Unforgeable noise-tolerant quantum tokens." *PNAS Early Edition*. DOI;10.1073/pnas.1203552109