MAX-PLANCK-INSTITUTE
OF QUANTUM OPTICS

Garching, 2 October 2012

Press Release

Unforgeable quantum credit cards in sight.

A team of physicists at Max-Planck-Institute of Quantum Optics, Harvard University, and California Institute of Technology develops a scheme for noise tolerant and yet safely encrypted quantum tokens.

Whoever has paid a hotel bill by credit card knows about the pending danger: given away the numbers of the card, the bank account and so on, an adversary might be able to forge a duplicate, take all the money from the account and ruin the person. On the other hand, as first acknowledged by Stephen Wiesner in 1983, nature provides ways to prevent forging: it is, for example, impossible to clone quantum information which is stored on a qubit. So why not use these features for the safe verification of quantum money? While the digits printed on a credit card are quite robust to the usual wear and tear of normal use in a wallet, its quantum information counterparts are generally quite challenged by noise, decoherence and operational imperfections. Therefore it is necessary to lower the requirements on the authentication process. A team of physicists at Max-Planck-Institute of Quantum Optics (Garching), Harvard University (Cambridge, USA), and California Institute of Technology (Pasadena, USA) has demonstrated that such protocols can be made tolerant to noise while ensuring rigorous security at the same time (Proceedings of the National Academy of Science (PNAS), 18 September, 2012).

On the one hand, the properties of quantum information make it ideal for preventing any kind of forgery. On the other hand, everyday life conditions make it virtually impossible to perfectly store quantum bits of information due to the fragility of their physical carriers which could be individual nuclei. Researchers under the direction of Prof. Ignacio Cirac, director at MPQ and head of the Theory Division, and Prof. Mikhail Lukin (Harvard University) have focused on both improving storage quality and providing protocols which accommodate for such real-world imperfections. In order to do so, the verification process for such protocols must condone a certain amount of quantum bit failures. Relaxing the requirements for verification enhances the ability for a dishonest user to forge a quantum token. This interplay is addressed by the scientists by setting a tolerance threshold which admits a certain amount of noise while guaranteeing high security against fraudulent copies. As Dr. Fernando Pastawski (MPQ), who has worked on this topic in his doctoral thesis, was able to demonstrate, such thresholds are found for two kinds of “quantum token” protocols. In the first protocol, quantum information must be physically transferred back to the verifier who can then asses its validity directly. In contrast, the second protocol involves indirect verification by having the verifier communicate with the holder who locally measures constituent qubit memories.

In both approaches, the bank issues a token and sends it to the holder. The “identity” of the token can be encoded on photons transmitted via an optical fibre or on nuclear spins in a solid memory transferred to the holder. However, only the bank stores a full classical description of these quantum states.

**Press &
Public Relations**
Dr. Olivia Meyer-Streng

Phone:
+49 - 89 / 32 905-213
E-mail: olivia.meyer-streng@mpq.mpg.de

Hans-Kopfermann-Str. 1
D-85748 Garching

Phone:+49 - 89 / 32 905-0
Fax:+49 - 89 / 32 905-200

In the approach denoted by “quantum ticket”, the holder has to return the token to the bank or another trusted verifier for validation. The verifier is willing to tolerate a certain fraction of errors which should be enough to accommodate the imperfections associated with encoding, storage and decoding of individual quantum bits. The only information returned to the holder is whether the ticket has been accepted or rejected. Thus it is “consumed” and no longer available to the holder. The scientists show that through such an approach, both the likelihood of rejecting the token from an honest user and that of accepting a counterfeit can be made negligible.

Figure: Illustration of a quantum bill (IN QUANTUM PHYSICS WE TRUST)
© background by vektorportal.com, collage by F. Pastwaski

The second approach is the “classical verification quantum ticket”. In some cases it may be impossible that the quantum tickets are given back to the bank physically. Here the holder has to validate his quantum token remotely – by answering challenge questions. The group considers a scheme where the quantum information is organized in blocks of qubit pairs. A non-revealing challenge question consists of requesting the holder to use a specific measurement basis for each block. By doing so, the holder is capable of providing a correct answer, but the token is consumed. This excludes the possibility for a dishonest user to cheat by answering complementary questions. As before, the given tolerance threshold determines the number of correct answers that is necessary for the verification of the token. The block structure used for the tokens allows exponentially suppressing the undesired capability of a dishonest holder to answer two complementary questions while assuring a true holder’s token will be authenticated with a very high probability.

For both protocols a realistic noise tolerance can be achieved. “We can deduce from theory that on average no more than 83% of the secret digits may be duplicated correctly by a counterfeiter. Under realistic conditions, we can assume that an honest participant should be able to recover 95% of the digits. If now the verifier sets the tolerance level to 90%, it will be almost impossible to accept fraudulent tokens or to reject an authentic holder,” Dr. Pastawski explains.

The protocols could in principle be demonstrated by using single qubits, e.g. single photons which carry the information in their polarization state, or single nuclei where the quantum information is encoded in their spin state. “However, in order to reach the time scales necessary for relevant applications, good qubit memories are needed. We have recently achieved

storage times of one second for single qubits at room temperature, which is a big step, but not yet sufficient," Fernando Pastawski concedes. The quantum token presented here could serve as a primitive to construct quantum money – that can change hands several times – or even quantum credit cards that are unforgeable and hence immune to fraudulent charges. "I expect to live to see such applications become commercially available. However quantum memory technology still needs to mature for such protocols to become viable," the scientist adds. *F. Pastawski/O. Meyer-Streng*

Original publication:
Fernando Pastawski, Norman Y. Yao, Liang Jiang, Mikhail D. Lukin, and J. Ignacio Cirac
"Unforgeable noise-tolerant quantum tokens"
Proceedings of the National Academy of Science (PNAS), 18 September, 2012

Contact:

Prof. Dr. Ignacio Cirac
Honorary Professor, Technische Universität München
Max-Planck-Institute of Quantum Optics
Hans-Kopfermann-Straße 1
85748 Garching
Phone: +49 - 89 / 32905 705 / 736
Fax: +49 - 89 / 32905 336
E-mail: ignacio.cirac@mpq.mpg.de
www.mpq.mpg.de/cirac

Dr. Fernando Pastwawski
Max-Planck-Institute of Quantum Optics
Hans-Kopfermann-Straße 1
Phone: +49 - 89 / 32905 639
Fax: +49 - 89 / 32905 336
E-mail: fernando.pastawski@mpq.mpg.de