MAX-PLANCK-INSTITUT
FÜR QUANTENOPTIK

Garching, 2. Oktober 2012

Presse-Information

Fälschungssichere Quantenkreditkarten in Sicht.

Wissenschaftler am Max-Planck-Institut für Quantenoptik, der Harvard Universität und dem California Institute of Technology entwickeln eine Methode, fehlertolerante und gleichzeitig fälschungssichere „Quanten-Gutscheine“ herzustellen.

Presse- und Öffentlichkeitsarbeit
Dr. Olivia Meyer-Streng

Tel.: 089 / 32 905-213
E-Mail: olivia.meyer-streng@mpq.mpg.de

Wer immer seine Hotelrechnung mit einer Kreditkarte bezahlt hat, kennt auch die damit verbundenen Gefahren: die Preisgabe von Karten- und Kontonummer, der Bankleitzahl und ähnlichem, könnte es einem Betrüger ermöglichen, die Karte zu duplizieren, alles auf dem Konto verfügbare Geld abzuräumen und so den Karteninhaber zu ruinieren. Auf der anderen Seite stellt die Natur, wie der Physiker Stephen Wiesner bereits 1983 zeigte, Mittel bereit, dieser Gefahr vorzubeugen: nach den Regeln der Quantenphysik ist es prinzipiell nicht möglich, Quanteninformation exakt zu kopieren. Warum also sollte sich dieses Potential nicht für die sichere Beglaubigung von „Quantengeld“ nützen lassen? Die Schwierigkeit dabei liegt in der Empfindlichkeit der Träger der Quanteninformation. Während die auf eine Kreditkarte oder Banknote gedruckten Ziffern nicht so schnell beim täglichen Gebrauch beschädigt werden, werden ihre quantenmechanischen Gegenstücke schnell durch Rauschen, Dekohärenz oder fehlerhafte Bedienung beeinträchtigt. Die Anforderungen an die Echtheitsüberprüfung müssen daher herabgesetzt werden. Physiker am Max-Planck-Institut für Quantenoptik (MPQ), der Harvard-Universität (Cambridge, USA) und dem California Institute of Technology (Pasadena, USA) haben nun Prüfungsprotokolle so gestaltet, dass sie Fehler in gewissem Umfang tolerieren und gleichzeitig hohe Sicherheit gewährleisten (Proceedings of the National Academy of Science (PNAS), 18. September 2012).

Auf der einen Seite bieten die Eigenschaften von Quanteninformation den idealen Schutz vor jeder Art von Fälschung. Auf der anderen Seite sind ihre Träger, z. B. einzelne Atomkerne, so empfindlich, dass es praktisch unmöglich ist, unter Alltagsbedingungen Quanteninformation absolut fehlerfrei abzuspeichern. Forscher unter der Leitung von Professor Ignacio Cirac, Direktor am MPQ und Leiter der Abteilung Theorie, und Prof. Mikhail Lukin (Harvard Universität) arbeiten derzeit daran, sowohl die Qualität der Speicherbausteine zu verbessern als auch Protokolle zu entwickeln, welche die in der realen Welt unvermeidlich auftretenden Mängel tolerieren. Dementsprechend muss auch der Beglaubigungsprozess für diese Protokolle ein gewisses Maß an Unvollkommenheit der zu prüfenden Quantenbits in Kauf nehmen. Diese Aufweichung der Anforderungen für den Echtheitsnachweis erhöht jedoch die Chance für einen Betrüger, den Gutschein zu fälschen. Die Wissenschaftler führen deswegen eine Toleranzschwelle ein, die ein bestimmtes Maß an Ungenauigkeit zulassen und dennoch höchste Sicherheit garantieren soll. Wie Dr. Fernando Pastawski, der dieses Thema im Rahmen seiner Doktorarbeit behandelte, herausfand, beinhalten zwei Arten von Protokollen eine derartige Toleranzschwelle. Bei dem ersten Protokoll muss die Quanteninformation physikalisch an den Beglaubiger zurückgegeben werden, der ihre Gültigkeit direkt bestätigt. Im Gegensatz dazu

Hans-Kopfermann-Str. 1
D-85748 Garching

Tel.: 089 / 32 905-0
Fax: 089 / 32 905-200

stellt das zweite Protokoll einen indirekten Echtheitsnachweis dar. Hier kommuniziert der Prüfer mit dem Besitzer des Gutscheins, der seinerseits lokal die auf den Quantenbits gespeicherte Information misst.

In beiden Ansätzen stellt die Bank die Gutscheine aus und sendet sie an die Besitzer. Die „Identität“ des Gutscheins wird dabei z. B. in die Polarisationszustände von Photonen kodiert, die über eine optische Glasfaser verschickt werden können, oder auf die Spins von Atomkernen in einem Festkörperspeicher, der dem Halter überbracht wird. Eine vollständige klassische Beschreibung der Quantenzustände besitzt jedoch nur die Bank.

Abbildung: Illustration einer „Quanten-Banknote“ (IN QUANTUM PHYSICS WE TRUST)
© Hintergrund: vektorportal.com, Kollage: F. Pastwaski

In dem als „Quanten-Ticket“ bezeichneten Ansatz muss der Besitzer den Gutschein für die Zertifizierung wieder an die Bank oder einen anderen anerkannten Prüfer zurückgeben. Die von den Prüfern zugelassene Toleranzschwelle ist groß genug, um den bei der Kodierung, Speicherung und Entschlüsselung der einzelnen Quantenbits unvermeidlichen Fehlern gerecht zu werden. Als Rückmeldung erhält der Besitzer von der Bank allein die Information, ob der Schein akzeptiert wurde oder nicht. Der Gutschein selbst ist aufgebraucht und steht ihm nicht mehr zur Verfügung. Sowohl die Wahrscheinlichkeit, dass ein ehrenhafter Besitzer zurück gewiesen wird, als auch die Wahrscheinlichkeit dafür, dass ein Duplikat akzeptiert wird, sind vernachlässigbar klein.

Der zweite Ansatz beschreibt das „Quanten-Ticket mit klassischer Zertifizierung“. Es kann vorkommen, dass ein Gutschein nicht physikalisch eingelöst werden kann. Hier muss der Besitzer die Echtheit des Gutscheins aus der Ferne nachweisen – indem er bestimmte Testfragen beantwortet. Die Forschungsgruppe hat dafür ein Schema entwickelt, bei dem die Quanteninformation in Blocks von je zwei Quantenbits organisiert ist. Eine solche Testfrage, die selbst keine Information preisgibt, verlangt von dem Besitzer, für die Messung eines jeden Blocks eine spezifische Basis zu verwenden. Damit ist der Ehremann in der Lage, die richtige Antwort zu geben. Da durch die Messung die im Quanten-Gutschein gespeicherte Information zerstört wird, ist ausgeschlossen, dass ein unehrlicher Betrüger durch die Beantwortung weiterer, komplementärer Fragen zum Zuge kommen könnte. Wie bei dem vorherigen Ansatz ist durch die Höhe der Toleranzschwelle festgelegt, wie viele richtige Antworten für den Echtheitsnachweis des Gutscheins notwendig sind. Aufgrund der blockweisen Struktur der Information nehmen die Betrugsmöglichkeiten exponentiell mit der Zahl der Speicherbausteine ab, während der Gutschein des wahren Besitzers mit höchster Wahrscheinlichkeit akzeptiert wird.

Mit beiden Protokollen kann eine realistische Toleranzschwelle erzielt werden. „Aus der Theorie folgt, dass ein Nachahmer maximal 83% der geheimen Ziffern korrekt wiedergeben könnte. Wir können aber annehmen, dass der echte Besitzer unter realistischen Bedingungen etwa 95% der Ziffern richtig benennen kann. Wenn der Beglaubiger die Schwelle also bei 90% korrekten Inhalts setzt, dann ist es fast unmöglich, dass gefälschte Gutscheine angenommen oder echte zurück gewiesen werden“, erklärt Dr. Pastawski.

Beide Protokolle können im Prinzip schon mit heute zur Verfügung stehenden Techniken umgesetzt werden. So könnte die Quanteninformation z.B. in die Polarisation einzelner Photonen gespeichert werden, oder in die Spinzustände einzelner Atomkerne. „Um allerdings die Zeitskalen zu erreichen, die für wichtige Anwendungen notwendig sind, benötigen wir besonders gute Speicherbausteine. Wir haben vor kurzem Speicherzeiten von rund einer Sekunde für einzelne Quantenbits bei Zimmertemperatur erreicht. Das ist bereits ein großer Schritt, allerdings nicht groß genug“, schränkt Fernando Pastawski ein. Der hier vorgestellte Gutschein könnte als Vorlage dienen, um „Quantengeld“ zu konstruieren, das von Hand zu Hand geht, oder auch Quantenkreditkarten, die fälschungssicher sind und betrügerische Abhebungen unmöglich machen. „Ich denke schon, dass solche Anwendungen noch zu meinen Lebzeiten kommerziell werden“, meint der Wissenschaftler. „Aber dafür muss die Technologie der Speicherbausteine erst noch eine gewisse Reife erlangen.“ *O. Meyer-Streng*

Originalveröffentlichung:
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

Kontakt:

Prof. Dr. Ignacio Cirac
Honorarprofessor für Physik, TU München,
Direktor am Max-Planck-Institut für Quantenoptik
Hans-Kopfermann-Straße 1, 85748 Garching
Tel.: +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-Institut für Quantenoptik
Hans-Kopfermann-Straße 1, 85748 Garching
Tel.: +49 - 89 / 32905 639
Fax: +49 - 89 / 32905 336
E-Mail: fernando.pastawski@mpq.mpg.de