

Pressemitteilung

Universität Wien

Alexandra Frey

04.07.2023

<http://idw-online.de/de/news817189>

Forschungs- / Wissenstransfer, Forschungsergebnisse
Informationstechnik, Physik / Astronomie
überregional



Quantenphysik schützt digitale Zahlungen

Jede*r von uns war schon gezwungen, sensible Zahlungsdaten auf der Website eines unbekannten Händlers einzugeben oder Kreditkartendaten sowie Passwörter in unbekannte Hände zu geben. Wissenschaftler*innen der Universität Wien haben nun ein bedingungslos sicheres System für solche Einkäufe entwickelt, das moderne kryptographische Techniken mit den grundlegenden Eigenschaften des Quantenlichts kombiniert. Die Demonstration solcher "quanten-digitaler Zahlungen" in einer realistischen Umgebung wurde soeben in Nature Communications veröffentlicht.

Digitale Zahlungen haben physische Banknoten in vielen Bereichen unseres täglichen Lebens ersetzt. Ähnlich wie Banknoten sollten sie einfach zu verwenden, einzigartig, fälschungssicher und nicht rückverfolgbar sein, aber auch digitalen Angriffen und Datenverletzungen standhalten. Im heutigen Zahlungssystem werden die sensiblen Daten der Kund*innen durch Zufallszahlenfolgen ersetzt und die Einzigartigkeit jeder Transaktion wird durch eine klassische kryptografische Methode oder einen Code gesichert. Allerdings können Angreifer*innen und Händler*innen, die über sehr leistungsstarke Computer verfügen, diese Codes knacken und die privaten Daten der Kund*innen entschlüsseln, um dann beispielsweise in deren Namen zu bezahlen.

Ein Forscher*innenteam unter der Leitung von Philip Walther von der Universität Wien hat gezeigt, wie die Quanteneigenschaften von Lichtteilchen oder Photonen bedingungslose Sicherheit für digitale Zahlungen gewährleisten können. In einem Experiment haben die Forscher*innen gezeigt, dass keine Transaktion dupliziert oder von böswilligen Dritten abgezweigt werden kann und dass die sensiblen Daten der Nutzer*innen privat bleiben. "Ich bin wirklich beeindruckt, wie die Quanteneigenschaften des Lichts für den Schutz neuer Anwendungen wie digitaler Zahlungen genutzt werden können, die in unserem täglichen Leben von Bedeutung sind", sagt Tobias Guggemos von der Fakultät für Physik.

Um absolut sichere digitale Zahlungen zu ermöglichen, ersetzen die Wissenschaftler*innen die klassischen kryptografischen Techniken durch ein Quantenprotokoll, das einzelne Photonen nutzt. Bei einer klassischen digitalen Zahlungstransaktion teilen Kund*innen dem Zahlungsdienstleister (z. B. einer Bank oder einem Kreditkartenunternehmen) einen klassischen Code – das so genannte Kryptogramm – mit. Dieses Kryptogramm wird dann zwischen Kund*in, Händler*in und Zahlungsdienstleister weitergegeben. In dem im Experiment gezeigten Quantenprotokoll wird dieses Kryptogramm mit Quantentechnologie erzeugt, indem der Zahlungsdienstleister speziell präparierte Einzelphotonen an Kund*innen sendet. Für den Bezahlvorgang misst der*die Kund*in diese Photonen, wobei die Messeinstellungen von den Transaktionsparametern abhängig sind. Da Quantenzustände des Lichts nicht kopiert werden können, kann die Transaktion nur einmal durchgeführt werden. Dies und die Tatsache, dass jede Abweichung von der beabsichtigten Zahlung die vom Zahlungsdienstleister überprüften, Messergebnisse verändert, macht diese digitale Zahlung bedingungslos sicher.

Die Forscher*innen haben erfolgreich quantendigitale Zahlungen über eine 641 m lange städtische Glasfaserverbindung zwischen zwei Universitätsgebäuden in der Wiener Innenstadt realisiert. Digitale Zahlungen funktionieren derzeit innerhalb weniger Sekunden. "Derzeit benötigt unser Protokoll einige Minuten an Quantenkommunikation, um eine

Transaktion abzuschließen. Damit soll die Sicherheit bei Rauschen und Verlusten gewährleistet werden", sagt Peter Schiansky, Erstautor der Publikation. "Diese zeitlichen Beschränkungen sind jedoch nur technologischer Natur", fügt Matthieu Bozzio hinzu, der davon überzeugt ist, dass "wir erleben werden, dass quantendigitale Zahlungen in sehr naher Zukunft eine praktische Leistungsfähigkeit erreichen".

wissenschaftliche Ansprechpartner:

Univ.-Prof. Dipl.-Ing. Dr. Philip Walther
Fakultät für Physik, Universität Wien
1090 Wien, Boltzmannngasse 5
T +43-1-4277-72560
M +43-664-8175859
philip.walther@univie.ac.at
<https://walther.univie.ac.at/>

Originalpublikation:

P. Schiansky, J. Kalb, E. Sztecsny, M.-C. Roehsner, T. Guggemos, A. Trenti, M. Bozzio, P. Walther, "Demonstration of quantum-digital payments"
Nature Communications 14, 3849 (2023)
DOI: 10.1038/s41467-023-39519-w
<https://doi.org/10.1038/s41467-023-39519-w>

URL zur Pressemitteilung: https://medienportal.univie.ac.at/media/aktuelle-pressemeldungen/detailansicht/artikel/quantenphysik-schuetzt-digitale-zahlungen/?mtm_campaign=presse&mtm_kwd=idw



Künstlerische Darstellung der durch Quantentechnologie gesicherten digitalen Zahlung
C: Peter Schiansky

D