Quantenkryptografie – Hacker haben ausgedient!

written by Julia Weinzettl - www.taskfarm.com

Dr. Rupert Ursin,
Gruppenleiter am Institut für Quantenoptik und Quanteninformation
der Österreichische Akademie der Wissenschaften,
Founder Quantum Technology Laboratories GmbH

Nichteinmal ein Quantencomputer wird es schaffen die Quantenverschlüsselung zu hacken. Warum? Weil es bei Quantencryptographie nicht um den Wettlauf der Computerkapazitäten geht. Die Verschlüsselung erfolgt mittels Naturgesetz. Daher wird aber mit Ankunft des Quantencomputers, der in sekundenschnelle alle Verschlüsselungen auch rückwirkend dechiffrieren kann, der Ruf nach einer tatsächlich unhackbaren Lösung laut. Die Forschungsergebnisse dazu kommen aus Österreich. Der nächste Schritt ist die wirtschaftliche Umsetzung. Dr. Rupert Ursin, Gruppenleiter Institut für Quantenoptik und Quanteninformation und Founder Quantum Technology Laboratoires im Interview.
Im Sinne des Taskfarm Konzepts wurde Dr. Rupert Ursin von Helmut Blocher, Geschäftsführer Succus Gmbh, auf das Interview eingeladen. Er spricht am 15./ 16. Oktober 2020 am Austrian Innovation Forum in Wien.

Wie funktioniert Quantenverschlüsselung?

Dr. Rupert Ursin: Quantenverschlüsselung ist die Kunst eine Nachricht von A nach B zu übertragen, ohne dass ein Dritter sie abhören kann. Sie basiert auf dem sogenannten No-Cloning-Theorem. Das bedeutet, man kann sie nicht, wie eine klassische

Nachricht, beliebig oft kopieren und auch nicht klonen. Jeder Versuch das zu tun führt dazu, dass der Abhörer ganz unweigerlich auffliegt. Das ist in der klassischen Kommunikation intrinsisch nicht der Fall.

Wieso fliegt der Abhörer auf?

Dr. Rupert Ursin: Quantenzustände sind Zustände, die ein einzelnes Teilchen trägt. Wenn eine Messung an dem Teilchen vorgenommen wird, ändert sich dadurch der Zustand unweigerlich.

Wenn ich beispielsweise ein Thermometer in einen See halte, messe ich die Temperatur. Weil das Thermometer im Vergleich zum See so klein ist, ist die Auswirkung vernachlässigbar. Wäre das Thermometer aber so groß wie der See, würde das Thermometer den See durch die Messung verändern. Genauso verhält es sich in der Quantenphysik. Das bedeutet, der Messapparat den der Abhörer hat, wird unweigerlich diesen Quantenschlüssel ändern. Das ist feststellbar. In der Kommunikation zwischen zwei Personen verursacht der Abhörer einen Fehler und diese Fehler kann man messen. Das ist bei einer klassischen Verschlüsselung nicht möglich. Man kann bei der Verwendung eines USB-Sticks nicht wissen, ob jemand den Schlüssel kontaminiert hat oder nicht. Ein Quantenzustand ist sehr empfindlich, man muss ihn in der Superposition halten.

Wie bei Schrödingers Katze…

Dr. Rupert Ursin: Genau. Die Kunst ist, diesen labilen Überlagerungszustand zwischen tot und lebendig zu halten. Diese Empfindlichkeit wirft die Schwierigkeit auf, einen Speicher, der tatsächlich nicht misst sondern nur speichert, für den Schlüssel zu konstruieren. Um einen sicheren Schlüssel zu generieren ist diese Empfindlichkeit aber unschlagbar. Sie ermöglicht etwas, das die klassische Technologie niemals ermöglicht, nämlich absolut ‚unhackbare' Kommunikation, verschlüsselt durch ein Naturgesetz.

Wie unterscheidet sich die Quantenverschlüsselung von der bisherigen RSA – Verschlüsselung?

Dr. Rupert Ursin: Das RSA Verfahren wird derzeit fast bei allen gängigen Verschlüsselungen verwendet. Es wurde in den späten 70er Jahren nach den drei Erfindern benannt und ist eine sogenannte asymmetrische Verschlüsselung. Diese Verschlüsselung basierte auf einem mathematischen Verfahren, für das es gar keinen Sicherheitsbeweis gibt. Das bedeutet, man weiß nur aus Erfahrung, dass es schwierig abzuhören ist. Wir wissen weder, ob das nicht bereits jemand kann – Stichwort Geheimdienste – oder ob vielleicht jemand morgen herausfindet, wie man RSA entschlüsselt.

Das ist wenigen Leuten klar, aber es ist tatsächlich ein großes Problem.

Warum?

Dr. Rupert Ursin: Ob oder wann RSA entschlüsselt wurde oder wird, ist unklar. Was aber ganz sicher eintreten wird, ist, dass es einen Quantencomputer geben wird.

Bisher galt die Verschlüsselung von Nachrichten schon als sicher, wenn man dafür 28 Bits verwendete. Wenn Nachrichten mit 64 Bit verschlüsselt werden, ist das in gängiger Betrachtung eine wirklich sichere Verschlüsselung. Denn das bedeutet, dass ein klassischer Computer, nach derzeitigen mathematischen Methoden, die in wissenschaftlichen Publikationen öffentlich zugänglich sind, länger rechnet als das Universum alt ist (ca. 13,7 Milliarden Jahre)*.

Ein **Quantencomputer**, nach dem heutigen Stand (und das sind erst 20 Jahre Forschung), braucht **weniger als eine Sekunde**, um diese Nachricht zu entschlüsseln.

Das ist ein tatsächliches und wahrhaftiges großes Problem und stürzt ganze Volkswirtschaften ins Verderben, denn Volkswirtschaften sind auf die Übertragung von Geheimnissen

angewiesen. Das fängt bei der Authentifizierung beim Einstieg ins Online-Banking an und betrifft unzählige Branchen, wie die Energieversorgung, Fluglinien, Atomkraftwerke, den Betrieb von Autonomous Cars, etc…

Können wir Quantenkryptografie heute schon wirtschaftlich anwenden? Es war früher ja viel zu teuer.

Dr. Rupert Ursin: Es ist auch heute noch zu teuer, aber es wird ein Umdenken stattfinden. Grundsätzlich muss man wissen, die RSA-Verschlüsselung, die wir heute verwenden um unsere Bankgeschäfte zu erledigen, ist eine Software Security. Diese Verschlüsselung wird von der CPU im Handy, dem Laptop zu Hause oder dem Server der Bank, die man verwendet, erstellt. Man verwendet also vorhandene Ressourcen und ein mathematisches Verfahren zur Verschlüsselung.
Bei Quantenkryptografie ist das anders. Man benötigt physische Sicherheit – also Geräte, und das ist intrinsisch teurer.

Die Marktteilnehmer, die wir kennen, waren in den letzten 20 Jahren der Meinung, dass sich Quantenryptografie nicht durchsetzen wird, weil sie Geld kostet. Mittelweile sehen sie aber, dass sie ein echtes wirtschaftliches Problem haben, und zwar schon heute. Warum? Jedes Geheimnis, das eine Bank heute abspeichert, kann ein Quantencomputer – wenn er in 10 Jahren existiert – auch rückwirkend lösen. Ein quantenkryptografisch übertragenes Verschlüsselungssystem kann ein Quantencomputer aber auch in hundert Jahren nicht lösen.

Das ist der große Unterschied beispielsweise auch zu Quantensensoren, denn sie können nichts besser messen als klassische Sensoren, nur schneller. Auch ein Quantencomputer, kann auch nichts intrinsisch besser als ein klassischer Computer. Er kann es nur sehr, sehr viel schneller. Aber im Prinzip kann man die Ergebnisse auch mit einem Abakus zu Hause im Kinderzimmer ausrechnen. Es dauert nur viel, viel länger.

Die Quantenkryptografie funktioniert aber anders.

Dr. Rupert Ursin: Genau, denn die Quantenkryptografie basiert auf einem Naturgesetz und dieses Naturgesetz erlaubt etwas, das die klassische Technologie einfach nicht erlaubt. Und zwar lässt es den Abhörer unweigerlich auffliegen.

Welche Jobs wird es in Zukunft geben werden, die heute noch keinen Namen haben?

Dr. Rupert Ursin: Quanteningenieur ist ein Berufsstand, den wir in Zukunft brauchen werden. Wir brauchen eine Mischung aus einem Physiker, einem Mathematiker, einem Ingenieur und einem Optiker. Personen, die diese Technologien beherrschen und sehr viel mehr können als nur Quantencomputer und Kommunikationssysteme bauen, die Anwendungsgebiete umfassen auch bildgebende Verfahren, die z. B. in der Medizin immer wichtiger werden.
Daher rufe ich auch immer die Universitäten auf, Lehrgänge zu installieren, die für diese zukünftigen Jobs Studenten ausbilden. Wir haben eine hervorragende Forschungslandschaft, aber um die Früchte dieser wissenschaftlichen Erkenntnisse auch hier im Land zu behalten, benötigen wir die richtigen Leute.

Was hält Dich nachts wach?

Dr. Rupert Ursin: Ich finde, wir können und sollen es uns nicht noch einmal leisten das Informationszeitalter zu übersehen, wie wir es damals mit dem Mailüfterl (entwickelt von dem Österreicher Prof. Zemanek), übersehen haben. Hier ist die Wertschöpfung dann eben im Silicon Valley passiert. Jetzt müssen wir versuchen, das im Donauvalley hinzukriegen.

Die Quantenforschung hat sich seit den 70er Jahren hier in Österreich entwickelt. Damals gab es Pioniere wie Peter Zoller und Anton Zeilinger in einem Feld, das niemanden interessierte. Es war ein österreichisches Unikum.
In den letzten 30 Jahren wurde ausgesprochen viel Geld von Forschungstöpfen aus öffentlicher Hand in Quantenforschung

investiert. Das heißt, man hat in Hochrisikoforschung investiert. Risiko in dem Sinn, dass man nicht wusste, welche Ergebnisse es geben wird und ob die Erkenntnisse aus der Quantenforschung jemals in eine anwendbare Technologie gießbar sind, weil sie so empfindlich sind. Das Risiko und die Kosten haben also keine Investoren, sondern die österreichische Gesellschaft als Ganzes getragen.
Jetzt sind wir so weit, dass wir in die wirtschaftliche Anwendung gehen können, daher ist es wichtig, dass die Wertschöpfung, die aus diesen Forschungsergebnissen entsteht, auch wieder hier in Österreich passiert.

Und das schaut gerade nicht gut aus. Das muss man ganz offen sagen. Wir Europäer haben derzeit keine industrielle Kompetenz, wenn es um Quantentechnologie geht. Die Kompetenz liegt zurzeit ausschließlich in China und in den USA. Wir versuchen hier als kleine Firma, qtl.at, dem entgegenzuwirken, aber wir sind tatsächlich die einzigen in der Europäischen Union. Es gibt in Österreich ein paar andere Unternehmen, die sich um andere Technologien in der Quantenforschung bemühen. Aber es ist beschämend wenig dafür, wie viel Risiko der Steuerzahler auf sich genommen hat. Das ist für mich eine persönliche Geschichte. Hier möchte ich einfach das Gegenteil beweisen.

–

Good to know: Was ist ein Quantensprung tatsächlich?

Dr. Rupert Ursin: *Wir verwenden das Wort Quantensprung nicht, denn ein Quantensprung per Definition ist das Kleinste, was man sich vorstellen kann und ist außerdem völlig zufällig. Wenn ein Politiker daher verkündet, er würde z.B. das Pensionsssystem reformieren und das wäre ein Quantensprung, dann ist das oft genau das: ein unendlich kleiner Schritt und völlig zufällig.*

–

[iqoqi – vienna]

[qtl.at]

About:

Dr. Rupert Ursin ist Gruppenleiter am Institut für Quantenoptik und Quanteninformation der Österreichische Akademie der Wissenschaften. Sein Forschungsschwerpunkt ist die Entwicklung von Quantenkommunikations- und Quanteninformationsverarbeitungstechnologien, vor allem für Freiraumübertragung bis hin zu Satelliten, aber auch für faserbasierte Systeme. Ziele seiner Arbeit reichen von kurzfristigen Ingenieurlösungen für die sichere Schlüsselaufteilung (Quantenkryptographie) bis hin zu spekulativer Forschung (Entkohärenz verschränkter Zustände in Gravitationsfeldern). Experimente zur Quantenkommunikation und Teleportation mit verschränkten Photonenpaaren gehören zu seinen Interessen, mit dem langfristigen Ziel eines zukünftigen globalen Quantennetzes. Er ist experimentell in zahlreichen internationalen Kooperationen in Deutschland, Italien, Spanien, USA sowie in Japan tätig. Bisher wurden einige seiner Publikationen als jährliche Highlights des britischen PhysikWebs und anderer ausgewählt. Im Jahr 2008 erhielt er den Award für das Telecommunications Advancement Research Fellowship (Nationales Institut für Informations- und Kommunikationstechnologie NICT, Tokio, Japan) und 2010 den Christian-Doppler-Preis. Er hat mehr als 60 Beiträge in wissenschaftlichen Fachzeitschriften wie Science und Natur veröffentlicht und auf mehr als 100 renommierten internationalen Konferenzen eingeladene Vorträge über seine wissenschaftlichen Ergebnisse gehalten. Weiter ist er Gastprofessor an der Universität für Wissenschaft und Technologie (USTC) in Shanghai, China.

—

** Ich könnte natürlich 13,7 Milliarden Computer kaufen, dann kann ich die Nachricht schon in einem Jahr entschlüsseln – das ist aber vermutlich wirtschaftlich nicht*

sinnvoll.