

*Neues aus der Welt der Wissenschaft*[ORF ON Science](#) · [News](#) · [Medizin und Gesundheit](#) · [Leben](#)

Patentbewilligung für abhörsichere Kommunikation

Quantenkryptographie als Mittel zu abhörsicherer Kommunikation könnte bald Wirklichkeit werden: Das Europäische Patentamt gab grünes Licht für ein Patent der Austrian Research Centers (ARC).

Kombination klassischer und neuer Verschlüsselung

"Ring of Trust" nennt sich das laut ARC neuartige Konzept für die sichere Kommunikation zwischen örtlich beliebig weit entfernten Partnern. Ermöglicht wird das durch die Kombination klassischer Verschlüsselungsmethoden mit Quantenkryptographie.

Für das eingereichte Patent wurde durch das Europäische Patentamt dieser Tage ein so genannter "positiver vorläufiger internationaler Prüfungsbericht" erstellt.

Datenleitungen oder Satelliten verwendet

"Ring of Trust" ermögliche durch die Einbindung von Schlüsselverteilungs- Zentralen ("Points of Trust") den Nachrichtenverkehr sowohl zwischen Partnern innerhalb einer Stadt als auch in verschiedenen Ländern - über Datenleitungen oder Satelliten, so die ARC in einer Aussendung.

Das Ergebnis sei eine gesicherte Kommunikation mit einem skalierbarer Sicherheitsgrad und gleichzeitig einer effizienten Übertragung über beliebig weite Distanzen unter Einbindung der bestehenden Kommunikationsstrukturen.

Datenaustausch z.B. via E-Mail

Die Schlüsselzentralen "Points of Trust" kommunizieren untereinander über geschützte Datenleitungen.


Das Konzept ermögliche es, dass Clients aus verschiedenen Ländern untereinander beispielsweise über E-Mail Daten austauschen, und zwar über Distanzen, die alleine durch Quantenkryptographie nicht überbrückbar wären.

→ [Quantum Cryptography](#)

→ [ARC](#)

→ [science.ORF.at-Archiv zum Thema](#)

[starburst1](#) | 08.02, 23:36

der hat eiskalt meine Idee patentiert. Denn dass das ganze System an den Knotenpunkten Schwächen aufweist, darauf habe ich schon beim ersten ORF-Artikel zu diesem Thema hingewiesen. Wenn man die Knotenpunkte nun zu Teilen des "Rings of Trust" erklärt, dann definiert man das Sicherheitsproblem natürlich weg... 

[starburst1](#) | 08.02, 23:38

zugegeben: Der "Ring of Trust" bzw. das Erklären der Knotenpunkt zu Sicherheitszentren war nicht meine Idee, ist aber eine logische Schlussfolgerung. Und wahrscheinlich wurde das Patent schon vor dem ersten ORF-Bericht eingereicht... das würde ich zumindest mal annehmen...

[starburst1](#) | 08.02, 23:50

Ein Beispiel-Link - ich bin mir aber sicher, dass ich das gleiche auch früher schon geschrieben habe - ich kann mich erinnern, dass ich das hier nicht neu erdacht, sondern nur nochmals niedergeschrieben habe:

<http://science.orf.at/science/news/112098>

[starburst1](#) | 09.02, 00:05

noch ein Link - aber ich bin mir sicher, dass ich das schon früher geschrieben habe:

<http://science.orf.at/science/news/110019>

[starburst1](#) | 09.02, 00:14

disclaimer

vielleicht sollte ich zur Sicherheit noch anbringen, dass sich meine Einwände jeweils auf die Sicherheit an den Knotenpunkten bzw. Endpunkten bezogen haben - nicht auf die Quantenkryptographie an sich. Dh. ich behaupte NICHT, dass die Idee zur Quantenkryptographie von mir stammen sollte, sondern nur der Einwand des Sicherheitsrisikos an den Knotenpunkten. Dieser Einwand kam regelmäßig von mir zu den diesbezüglichen ORF-Artikeln, da dieses Problem meines Wissens dort bislang nicht erwähnt wurde (bis gestern).

[starburst1](#) | 09.02, 00:26


mein Einwand deckt einen ganz anderen Bereich ab

Das Patent geht ja noch in eine ganz andere Richtung, wie ich erst beim zweiten Lesen des Artikels gesehen habe: Es geht ja primär gar nicht darum, dass die Nachrichten nur auf Quantenstrecken vom Sender über Knotenpunkte zum Empfänger (und retour) übermittelt werden, sondern Sender und Empfänger kommunizieren über herkömmliche Leitungen miteinander und "nur" die Schlüssel werden zwischen den "Points of Trust" ausgetauscht. Vielleicht sogar mehrfach während der Übertragung größerer Datenmengen. (Und Sender und Empfänger kommunizieren mit den "Points of Trust"). Das hat mit meinem oben beschriebenen Einwand zur Sicherheit über die Knotenpunkte hinweg natürlich herzlich wenig zu tun.

[sensortimecom](#) | 08.02, 11:41

Beam me up, Scotty...
Jetzt bin ich bloß neugierig, WER die erste
Patentanmeldung auf die Teleportation von Entitäten
einbringt..

Zeilinger sicher nicht;-)))

E. B. 

Die ORF.at-Foren sind allgemein zugängliche, offene und demokratische Diskursplattformen. Bitte bleiben Sie sachlich und bemühen Sie sich um eine faire und freundliche Diskussionsatmosphäre. Die Redaktion übernimmt keinerlei Verantwortung für den Inhalt der Beiträge, behält sich aber das Recht vor, krass unsachliche, rechtswidrige oder moralisch bedenkliche Beiträge sowie Beiträge, die dem Ansehen des Mediums schaden, zu löschen und nötigenfalls User aus der Debatte auszuschließen.

Sie als Verfasser haften für sämtliche von Ihnen veröffentlichte Beiträge selbst und können dafür auch gerichtlich zur Verantwortung gezogen werden. Beachten Sie daher bitte, dass auch die freie Meinungsäußerung im Internet den Schranken des geltenden Rechts, insbesondere des Strafgesetzbuches (Üble Nachrede, Ehrenbeleidigung etc.) und des Verbotsgesetzes, unterliegt. Die Redaktion behält sich vor, strafrechtlich relevante Tatbestände gegebenenfalls den zuständigen Behörden zur Kenntnis zu bringen.

Die Registrierungsbedingungen sind zu akzeptieren und einzuhalten, ebenso Chatiquette und Netiquette!

[Übersicht: Alle ORF-Angebote auf einen Blick](#)