

Buch: Alternativen zur Quantenkryptographie

Datum 13.10.2026
Subjekt FH St. Pölten
Kontakt

FH-Prof. Univ.-Doz. Dipl.-Ing. Dr. Ernst Piller

 Hochschul-Dozent Department Informatik und Security M: +43/676/847 228 636 ernst.piller@ustp.at

Dipl.-Ing. Hubert Schölnast

 BSc

Junior Researcher Institut für IT Sicherheitsforschung Department Informatik und Security hubert.schoelnast@ustp.at

Mag. Mark Hammer

 Fachverantwortlicher Presse

- T: +43/2742/313 228 269 mark.hammer@ustp.at

Ein neues Fachbuch vergleicht physikalische Verfahren der Datenverschlüsselung: Quantenkryptografie ist oftmals nicht die beste Wahl.

Die Sicherheit von Daten gewinnt in einer zunehmend digitalisierten und vernetzten Welt kontinuierlich an Bedeutung. Ob Forschungsdaten, medizinische Informationen oder strategisch wichtige Unternehmens- und Staatsdaten: Der Schutz sensibler Informationen ist eine zentrale Voraussetzung für moderne Kommunikation und digitale Prozesse. Quantenkryptographie (Quantum Key Distribution – QKD) ist eine oft genannte Technik zum Verschlüsseln von Daten, in die große Hoffnung für die Zukunft gesteckt und über die viel berichtet wird. Doch ein neu erschienenes Buch auf Basis einer wissenschaftlichen Studie zweier Forscher der USTP – University of Applied Sciences St. Pölten beleuchtet erstmals verschiedene physikalische Verfahren der Datenverschlüsselung in einem gemeinsamen Vergleich und zeigt: Die oft genannte Quantenkryptografie ist in vielen Anwendungsfällen nicht die sinnvollste oder wirtschaftlichste Lösung.

Mit dem Buch „Data Encryption at the Intersection of Mathematics and Physics – Comparing Physical Methods of Cryptography“ haben Ernst Piller und Hubert Schölnast vom Institut für IT-Sicherheitsforschung der USTP einen umfassenden und technologieutralen Überblick über physikalische Verfahren der Kryptografie vorgelegt. Das Werk ist bei Springer Nature erschienen und erstmals werden fünf unterschiedliche Technologien der physikalischen Kryptografie wissenschaftlich fundiert, praxisnah und leicht verständlich gegenübergestellt.

Im Mittelpunkt des Buches steht die Frage, welche Technologie für welchen Einsatzzweck geeignet ist und welche Kosten, Annahmen und Risiken damit verbunden sind.

Rechenleistung als Achillessehne der Quantenkryptografie

Die heute weit verbreiteten kryptografischen Verfahren beruhen auf mathematischen Problemen, die von Angreifer*innen gelöst werden müssen, um die Daten zu entschlüsseln. Dies ist mit aktuellen Rechenleistungen nicht möglich, könnte sich in Zukunft jedoch ändern. Zudem könnten Angreifer*innen neue, bisher unveröffentlichte Verfahren zum Knacken der mathematischen Probleme kennen.

Physikalische Verfahren verfolgen einen anderen Ansatz: Sie nutzen Eigenschaften der Physik, um kryptografische Schlüssel zu erzeugen und zu verteilen. Das Buch vergleicht technologieneutral, leicht verständlich und wissenschaftlich fundiert fünf verschiedene Technologien der physikalischen Kryptografie. Analysiert haben Piller und Schölnast unter anderem die Quantenkryptografie, die funksignalbasierte Schlüsselverteilung sowie die Memory Key Distribution. Bewertet werden Kriterien wie Schlüsselraten, Reichweiten, Robustheit, Implementierungsaufwand und Kosten.

„Viele Diskussionen über Quantenkryptografie konzentrieren sich auf die theoretische Sicherheit. In der Praxis müssen jedoch auch Kosten, Wartungsaufwand, Skalierbarkeit und konkrete Einsatzszenarien berücksichtigt werden. Unser Buch schafft hier erstmals eine wissenschaftlich fundierte und technologieneutrale Vergleichsbasis“, erklärt Buchautor Ernst Piller.

Technische Herausforderungen und hohe Kosten

Die Analysen zeigen, dass Quantenkryptografie mit technischen Herausforderungen und hohen Kosten verbunden ist. Zudem sind Angriffe über Umwege, sogenannte Seitenkanalangriffe, möglich. Denn laut Ernst Piller nutzen Angreifer*innen immer das schwächste Glied in der Sicherheitskette: „Das ist so, wie wenn man ein tolles Schloss ans Fahrrad hängt, aber die Kette dünn und schwach ist. Die Hoffnungen in die Quantenkryptographie sind groß, gerne wird auch der Bezug zu Einstein und Heisenberg zitiert. Die Quantenkryptografie ist jedoch in der Praxis leider wenig tauglich.“

Gleichzeitig existieren alternative Verfahren, die in vielen Anwendungsfeldern vergleichbare Sicherheitsniveaus zu deutlich geringeren Kosten ermöglichen. Besonders die Memory Key Distribution weist laut den Autoren das Potenzial auf, große Mengen an Schlüsselmaterial sicher zu übertragen und damit den Einsatz eines Verfahrens zu ermöglichen, das beweisbar als zu 100 Prozent sicher gilt. Gemeint sind damit Transport und Speicherung kryptografischer Schlüssel mithilfe sicherer Medien wie Chipkarten oder spezieller tragbarer Speichergeräte.

Das Buch richtet sich an Entscheidungsträger*innen aus Wirtschaft, Verwaltung und Politik, die Sicherheitslösungen bewerten und auswählen müssen. „Anstatt eine Technologie als überlegen darzustellen, liefert es eine fundierte Entscheidungsgrundlage für die Auswahl geeigneter kryptografischer Verfahren“, so Piller.

Buch „ Data Encryption at the Intersection of Mathematics and Physics - Comparing Physical Methods of Cryptography

Das Buch „ Data Encryption at the Intersection of Mathematics and Physics - Comparing Physical Methods of Cryptography“ ist im Verlag Springer Nature erschienen und auch kostenlos in einer Open-Access-Variante verfügbar. Es stellt das Ergebnis des Projektes Kryptovergleich dar, das vom Bundesministerium für Finanzen (BMF) im Sicherheitsforschungs-Förderprogramm KIRAS/K-Pass der österreichischen Forschungsförderungsgesellschaft FFG gefördert wurde. Das Buch sowie zusätzliche Informationen, die einen Anhang zum Buch darstellen, werden vom Institut auf der Website [cryptography.study](https://www.ustp.at/Plone/de/stories/news/buch-alternativen-zur-quantenkryptographie) angeboten.

Link zum Buch bei Springer

Forschungsprojekt Kryptovergleich

<https://www.ustp.at/Plone/de/stories/news/buch-alternativen-zur-quantenkryptographie>