Positionspapier
Empfehlungen zur quantensicheren Kryptographie

Quantencomputer werden (bei ausreichender Leistungsfähigkeit) in naher Zukunft einige der mathematischen Probleme hinter der aktuellen Kryptographie effizient lösen können und damit einen Großteil der digitalen Kommunikation unsicher machen. Betroffen ist in einem hohen Maße die „asymmetrische“ Kryptographie, die über die letzten 30 Jahre ein unverzichtbares Sicherheitselement in der digitalen Kommunikation und damit in den modernen Geschäftsmodellen darstellt. Die Bedrohung ist bereits heute relevant, da verschlüsselte Kommunikation erfasst, gespeichert und später entschlüsselt werden kann („Harvest-now-decrypt-later”), sobald ein ausreichend leistungsfähiger Quantencomputer vorhanden ist.

Die jüngsten Fortschritte im Quantencomputing haben bei Regierungen und Standardisierungsgremien einen verstärkten Handlungsdruck ausgelöst. Auch die EU-Kommission empfiehlt [1] eine baldige **Migration der digitalen Infrastrukturen auf die quantensichere Kryptographie** (Post-Quanten-Kryptographie (PQC)) und damit hin zu auf klassischen Berechnungen basierenden Verfahren, die nicht anfällig für Quantenangriffe sind. Diese Algorithmen sind in einem vom US National Institute of Standards and Technology (NIST) moderierten Prozess aus einer Anzahl von internationalen Einreichungen ausgewählt worden. IBM Research hat einen wichtigen Beitrag zu diesem Prozess geleistet: **Drei Algorithmen stehen seit 2024 bereits als Standards zur Verfügung – Co-Autoren dieser Algorithmen sind Forscher aus dem IBM-Forschungslabor in der Schweiz.**

Das Deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) analysiert seit Jahren den Einsatz von quantensicheren Algorithmen und hat 2024 gemeinsam mit Partnern aus 17 weiteren EU-Mitgliedsstaaten einen Report [2] veröffentlicht, in dem die Industrie, KRITIS-Betreiber und die öffentliche Verwaltung aufgefordert werden, zur quantensicheren Kryptographie überzugehen. Diese Umstellung betrifft die gesamten digitalen Ökosysteme und wird als komplex betrachtet, daher sollten die Planungs- und Priorisierungsaktivitäten umgehend eingeleitet werden.

Prioritäten für die quantensichere Kryptographie in Deutschland

Wir empfehlen der Bundesregierung, in Zusammenarbeit mit dem BSI und in Übereinstimmung mit den Empfehlungen der EU-Kommission die folgenden Schritte einzuleiten:

[1] https://digital-strategy.ec.europa.eu/de/policies/european-quantum-communication-infrastructure-euroqci
[2] https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2024/241127_PQC-Joint-Statement.html

- Laufende Bereitstellung von Informationen und detaillierten Leitlinien zu PQC für Organisationen und Industrieverbände;
- Regelungen zu erlassen, um Konsistenz und Interoperabilität zu unterstützen;
- Einsatz einer Fachgruppe für „Quanten-Sicherheit“, bestehend aus Vertretern von Behörden, Cybersicherheitsexperten und der Privatwirtschaft;
- Förderung des Austausches von Erkenntnissen und Erfahrungen mit anderen EU-Mitgliedsstaaten und zwischen den Industrien;
- Beschleunigung der Zertifizierung von industrierelevanten Technologieprodukten.

Die Industrie, KRITIS-Betreiber und die öffentliche Verwaltung sollten mit Hochdruck ihre Migration zu einer quantensicheren Kryptographie planen. Konkret sollten sie:

- die Quantensicherheit auf die Management Agenda setzen;
- dringende Maßnahmen gegen „Harvest-now-decrypt-Later“-Angriffe umsetzen;
- Verantwortliche benennen und bevollmächtigen, entsprechende Aktivitäten voranzutreiben;
- den (Quanten-)Technologiefortschritt verfolgen und Pläne bei Bedarf anpassen;
- wichtige Erkenntnisse und Empfehlungen organisationsübergreifend teilen.

Prioritäten für die politische Flankierung durch die Bundes- und Landesregierungen

Wir unterstützen die Vorhaben zu PQC im Handlungskonzept Quantencomputing der Bundesregierung – insbesondere die Migration zur quantensicheren-Kryptographie in Deutschland voranzutreiben und Forschungsprojekte zu quantensicherer Kryptographie zu fördern.

Die EU-Kommission, das BSI und sein französisches Pendant ANSSI empfehlen den Einsatz von quantensicheren Algorithmen in einem hybriden Modus – entweder mit klassischen kryptografischen Verfahren oder per Quantum Key Distribution (QKD). QKD, die Datensicherheit durch quantenmechanische Prinzipien gewährleistet, wird von mehreren Unternehmen und Institutionen geprüft. In experimentellen Kontexten gibt es großes Interesse an QKD; so soll beispielsweise das EuroQCI-Projekt im Auftrag der EU-Kommission kritische Kommunikationsinfrastruktur schützen, indem bestehende Kommunikationskanäle mit quantenbasierten

Systemen erweitert werden[1]. Für einen weiträumigeren Einsatz von QKD sind jedoch noch viele Hürden wie Skalierbarkeit und Effizienzfragen zu überwinden.

Diese Hürden haben dazu geführt, dass **internationale Behörden und Institutionen von einer großflächigen produktiven Verwendung von QKD abraten**. Sowohl die US-amerikanische NSA[3] als auch europäische Institutionen (wie BSI und ANSSI)[4] sind zum Schluss gekommen, dass QKD wegen technologischer Einschränkungen nur in sehr speziellen Anwendungen eingesetzt werden kann und derzeit nicht eigenständig einsatzreif sei. Stattdessen wird empfohlen, **bei der notwendigen Migration zu quantensicheren Verfahren die Priorität auf die PQC zu legen**.

Kontakt

Government & Regulatory Affairs IBM DACH

Martin Wegele, Director, martin.wegele@ibm.com, +49 173 5769369

Svenja Frerichs, Senior Manager, svenja.frerichs@ibm.com, +49 172 7655429

[3] https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

[4] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Quantum_Positionspapier.pdf?__blob=publicationFile&v=4