Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Sicherheit von QKD aus Sicht des BSI

Dr. Tobias Hemmert, Referat Vorgaben an und Entwicklung von Kryptoverfahren, BSI

OMNISECURE 2022, Berlin, 23.06.2022

Kryptografie ist im Umbruch

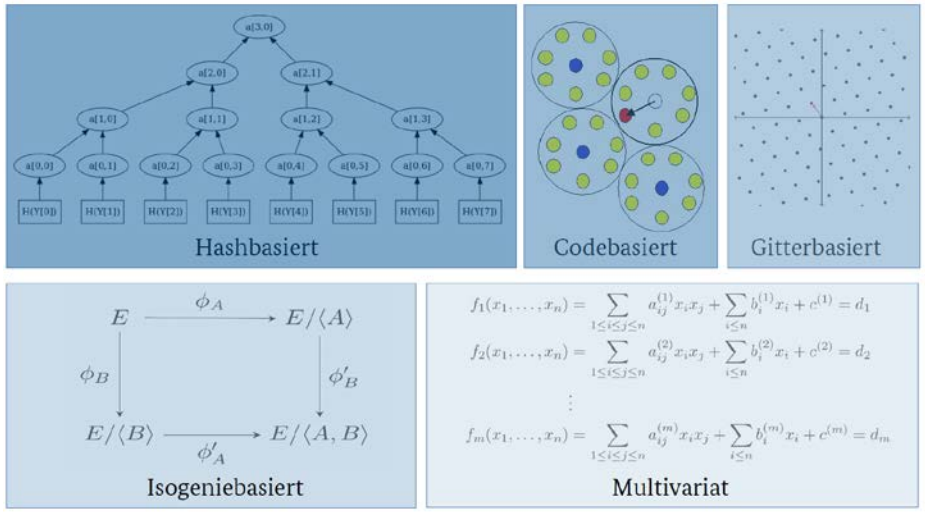
Ankündigung der NSA zu Migration zu quantensicheren Verfahren (2016)

Heute eingesetzte Public-Key-Kryptografie ist durch die fortschreitende Entwicklung von Quantencomputern bedroht.

Arbeitshypothese des BSI für den Hochsicherheitsbereich:

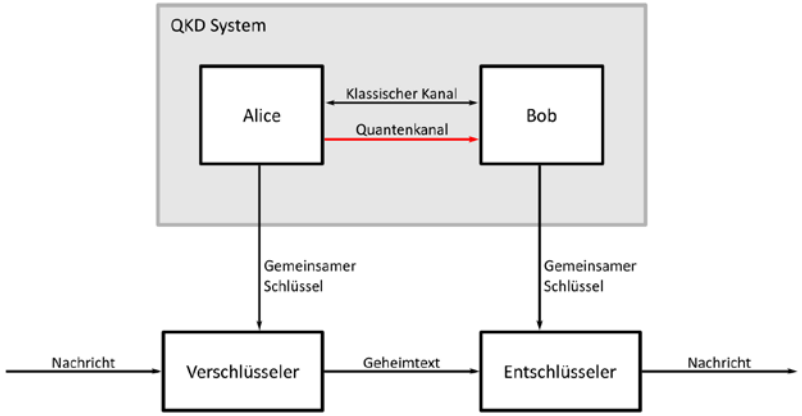
Mit signifikanter Wahrscheinlichkeit gibt es Anfang der 2030er Jahre einen kryptografisch relevanten Quantencomputer.

Quantensichere Kryptografie



Post-Quanten-Kryptografie

Theoretische Sicherheit basiert auf angenommener Schwierigkeit bestimmter mathematischer Probleme.



Quantum Key Distribution

Theoretische Sicherheit basiert auf quantenmechanischen Prinzipien.

Einschränkungen von QKD

- Spezialisierte Hardware wird benötigt.
- Beschränkte Reichweite, daher ist Ende-zu-Ende-Sicherheit schwierig umzusetzen.
- Vorverteilte Schlüssel werden benötigt.

→ **QKD ist nur für spezielle Anwendungsszenarien geeignet.**

Internationale Aktivitäten zu QKD

EuroQCI Declaration of Cooperation

- Chinesische QKD-Verbindung Shanghai ↔ Peking (in Betrieb seit 2017)
- EuroQCI – Quantenkommunikationsinfrastruktur für Europa (im Aufbau)
- Deutsche Forschungs- und Entwicklungsprojekte

Notwendige Schritte zu sicherer QKD

- Sicherheitsbeweise für praktisch relevante QKD-Protokolle
- Erarbeitung weiterer Standards (z. B. für QKD-Protokolle)
- Weitere Untersuchung der Implementierungssicherheit
- Evaluierungsmethodologie und Zertifizierung von Produkten

Fazit

Weitere Informationen: www.bsi.bund.de/PQ-Migration

Post-Quanten-Kryptografie ist die primäre Lösung für quantensichere Kryptografie.

QKD kann künftig für einige Anwendungsfälle eine Ergänzung zu Post-Quanten-Kryptografie darstellen.

Dazu sind aber noch einige Arbeiten zu Sicherheitsfragen erforderlich.