Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Quanten-Nomenklatur

Die wichtigsten Begriffe im Kontext quantensicherer Kryptographie

Stand: 09. Juni 2023

Einleitung

Im Kontext der Nutzung von Quantentechnologien in der Kryptographie hat sich eine Vielzahl von Fachbegriffen etabliert. Nicht einheitlich verwendete Terminologie kann zu Missverständnissen führen. In der folgenden Tabelle werden häufig verwendete Fachbegriffe erläutert. Hierbei sind in den ersten beiden Spalten die vom BSI favorisierten Begriffe – jeweils auf Deutsch und auf Englisch – aufgelistet. In der dritten Spalte werden Synonyme genannt, die vom BSI nicht verwendet werden, um eine einheitliche Nutzung der Fachbegriffe sicherzustellen.

Für eine detaillierte englischsprachige Übersicht zur Terminologie im Bereich der Post-Quanten-Kryptographie wird auf den IETF-Draft "Terminology for Post-Quantum Traditional Hybrid Schemes" verwiesen.

Quanten-Nomenklatur

Deutscher Begriff (vom BSI favorisiert)	Englischer Begriff (vom BSI favorisiert)	Synonyme (vom BSI nicht verwendet)	Definition	Anmerkungen
Quantensicherheit	Quantum safety	Quantenresistenz, Quantencomputerresistenz Quantum resistance	Algorithmen, Verfahren oder Systeme werden als quantensicher bezeichnet, wenn deren Sicherheitsanforderungen auch gegenüber einem Angreifer erfüllt sind, welcher Zugang zu einem leistungsstarken Quantencomputer hat.	In seltenen Fällen taucht in der englischsprachigen Literatur auch der Begriff „Quantum security“ auf, was als weiteres Synonym zu „Quantum safety“ aufgefasst werden kann.
Quantensichere Kryptografie	Quantum safe cryptography	Quantenresistente/quantencomputerresistente Kryptografie Quantumresistant cryptography	Kryptografische Verfahren, von denen angenommen wird, dass sie weder mit Hilfe eines leistungsstarken Quantencomputers noch mit Hilfe eines klassischen Computers zu brechen sind. Dabei unterscheidet man zwischen Post-Quanten-Kryptografie und Quantenkryptografie.	Gelegentlich werden auch die irreführenden Terminologien "Post-Quanten-Sicherheit" oder „Post-Quanten-Resistenz“ verwendet.
Post-Quanten-Kryptografie (PQK)	Post-quantum cryptography (PQC)		Quantensichere, asymmetrische kryptografische Verfahren, die auf klassischen Computern implementiert werden können. Die Sicherheit dieser Verfahren basiert auf der Schwierigkeit mathematischer Probleme, von denen derzeit angenommen wird, dass sie auch mit leistungsstarken Quantencomputern nicht effizient lösbar sind.	

Deutscher Begriff (vom BSI favorisiert)	Englischer Begriff (vom BSI favorisiert)	Synonyme (vom BSI nicht verwendet)	Definition	Anmerkungen
Quantenkryptografie	Quantum cryptography		Verfahren, die quantenmechanische Effekte ausnutzen, um kryptografische Aufgaben zu erfüllen. Für die Implementierung wird im Unterschied zur Post-Quanten-Kryptografie in der Regel spezialisierte Hardware (beispielsweise Einzelphotonendetektoren) benötigt.	
Quantum Key Distribution (QKD)	Quantum Key Distribution (QKD)	Quantenbasierte Schlüsseleinigung	Protokolle, die quantenmechanische Effekte zur sicheren Schlüsseleinigung ausnutzen. QKD ist ein Teilbereich der Quantenkryptografie.	
Klassisches (asymmetrisches) Verfahren / klassischer (asymmetrischer) Algorithmus (im Kontext der Post-Quanten-Kryptografie)	Classical (asymmetric) scheme / algorithm Auch: Traditional (asymmetric) scheme / algorithm		Derzeit verwendete asymmetrische Verfahren oder Algorithmen, die mit Hilfe eines leistungsstarken Quantencomputers gebrochen werden können.	
Schüsseltransportverfahren, Key Encapsulation Mechanism (KEM)	Key Encapsulation Mechanism (KEM)		Bei einem Schlüsseltransportverfahren erzeugt eine der beiden Parteien einen symmetrischen Schlüssel und sendet diesen asymmetrisch verschlüsselt an die andere Partei.	
Schlüsselableitungsfunktion Auch: Key Derivation Function (KDF)	Key Derivation Function (KDF)		Eine Funktion, die aus geheimen Eingabewerten, beispielsweise einem Hauptschlüssel, einem Passwort oder einer Passphrase, einen oder mehrere andere kryptografische Schlüssel erzeugt.	
Key Combiner	Key Combiner		Eine Funktion, die aus mehreren geheimen Eingabewerten einen oder mehrere kryptografische Schlüssel erzeugt.	Manchmal werden in der Literatur "Key Combiner" auch als "KEM Combiner" bezeichnet.

Deutscher Begriff (vom BSI favorisiert)	Englischer Begriff (vom BSI favorisiert)	Synonyme (vom BSI nicht verwendet)	Definition	Anmerkungen
Hybrides Verfahren (im Kontext der Post-Quanten-Kryptografie)	Hybrid scheme (in the context of post-quantum cryptography)		Ein kryptografisches Verfahren, dessen geheimer Schlüssel auf der Kombination • eines geheimen Schlüssels aus einem Post-Quanten-Verfahren mit • einem geheimen Schlüssel aus einem klassischen Verfahren beruht. Alternativ kann entweder der Schlüssel aus dem Post-Quanten-Verfahren oder der Schlüssel aus dem klassischen Verfahren ersetzt werden durch einen vorverteilten symmetrischen Schlüssel.	Es ist wichtig, dass durch das kryptografische Verfahren die Sicherheit des kombinierten Schlüssels gewährleistet ist, solange mindestens das Post-Quanten-Verfahren oder das klassische Verfahren nicht gebrochen wurden.
Kryptoagilität	Cryptographic agility		Kryptoagilität bietet die Möglichkeit, kryptografische Verfahren, Protokolle oder Implementierungen sicher auszutauschen.	