PQC versus QKD

Eine Gegenüberstellung

Autoren: Felix Trunk, Martin Seidel, Sascha Schweiger

Inhalt

Einführung

Insbesondere mit der zunehmend voranschreitenden Entwicklung von Quantencomputern stellt sich die Frage, ob bisher verwendete kryptografische Verfahren zur Sicherung von Computernetzen und vertrauenswürdigen Daten ausreichend sind. Der Grund hierfür ist, dass es für Quantencomputer spezielle Quantenalgorithmen gibt, die klassisch schwierig zu lösende Probleme deutlich einfacher lösen können.

Der bekannteste von diesen neuen Algorithmen ist der *Shor Algorithmus*, der eine drastische Beschleunigung für die Berechnung der Primfaktorzerlegung einer natürlichen Zahl bedeuten würde. Weitere kryptografisch relevante Quantenalgorithmen sind ein zweiter Quantenalgorithmus von Shor der eine vergleichbar drastische Beschleunigung für die Berechnung des diskreten Logarithmus bedeuten würde und der *Grover Algorithmus* der eine starke Beschleunigung für die Durchsuchung unsortierter Datenbanken verspricht [1], [2].

Dies ist ein Problem da gegenwärtige asymmetrische Kryptosysteme wie beispielsweise RSA, der *Diffie-Hellmann Schlüsselaustausch* (DH) oder auch der *Digital Signature Algorithm* (DSA) auf der Schwierigkeit der Berechnung einer Primfaktorzerlegung beziehungsweise des diskreten Logarithmus basieren. So würde beispielsweise laut ITU-T X.1811 nach aktuellem Wissenstand ein Quantencomputer mit knapp über sieben Millionen physischer *QuBits* benötigt werden um mit etwas mehr als einer halben Billion Gatteroperationen in weniger als 10 Stunden eine RSA1024 Verschlüsselung zu brechen. Auch die Sicherheit der symmetrischen AES Verschlüsselung wird durch den *Grover Algorithmus* gefährdet.

Es muss jedoch angemerkt werden, dass aktuell eine solche Quantenhardware noch in ungewisser Ferne liegt. Zum Vergleich, der 2019 von *Google* vorgeführte Quantencomputer besaß nur 53 Qubits [3]. Da aber beachtliche Fortschritte in diesem Feld erzielt werden und die (vollständige) Migration zu sicheren Verfahren in jedem Fall eine lange Zeit in Anspruch nehmen wird, ist es dringend notwendig sich früh genug mit diesem Thema zu beschäftigen.

Asymmetrische kryptographische Verfahren wie RSA, DH und DSA sind weit verbreitet. Würden sie unsicher werden, dann würden auch viele Protokolle, Produkte und Sicherheitsarchitekturen betroffen sein [4]:

Key Exchange: Zur sicheren Kommunikation über einen unsicheren (öffentlichen) Kanal können zwei Personen einen öffentlichen Schlüssel austauschen, um damit einen geheimen Schlüssel zu vereinbaren. Dies wird in wichtigen Verschlüsselungsprotokollen wie SSL/TLS, SSH und IKE/IPsec verwendet.

VPN: Gesicherte Kommunikation über unsichere IP-Netze kann mit IPsec realisiert werden. Zur Schlüsselerzeugung wird das IKE Protokoll verwendet.

SSL/TLS: Dieses Verschlüsselungsprotokoll ist insbesondere durch seine Verwendung im HTTPS Kommunikationsprotokoll bekannt.

PKI-Infrastrukturen: In diesen Strukturen stellen sog. *Certificate Authorities* (CA) Zertifikate aus, anhand derer ein öffentlicher Schlüssel eindeutig einer Person oder Institution zugeordnet werden kann.

Software-Validierung: Softwareupdates enthalten zusätzlich eine digitale Signatur, um die Authentizität der Software prüfen zu können.

S/MIME: Zur Absicherung von E-Mails und deren Anhang, werden bei S/MIME ebenfalls Zertifikate verwendet, die von einer CA ausgestellt werden.

Dieses Dokument beschäftigt sich deswegen mit Ansätzen, die Verschlüsselung und digitale Signaturen trotz Quantencomputer, sogenannte *Post-Quantum* oder *Quantum-Safe* Sicherheit, gewährleisten können beziehungsweise gut erforscht sind und als resistent gegenüber Angriffen durch bekannte Quantenalgorithmen gelten. Zum einen gibt es den Ansatz der ***Post Quantum Cryptography***, wo anstelle der unsicheren bisherigen Verschlüsselungs- und Signaturverfahren auf neue quantensichere Ansätze für asymmetrische Kryptosysteme gesetzt wird. Zum anderen gibt es aber auch den Ansatz der ***Quantum Key Distribution*** bei der neue Hardware die Eigenschaften der Quantenmechanik zur sicheren Verschlüsselung verwendet.

PQC

Definition

Bei **PQC** (kurz für ***Post Quantum Cryptography***) handelt es sich um neue asymmetrische kryptographische Verfahren, die sicher gegen Angriffe von Quantencomputern sein sollen. Diese Algorithmen werden entwickelt, um die langfristige Sicherheit von digitalen Signaturen und Verschlüsselungen zu gewährleisten.

Auch wenn aktuelle kryptographische Verfahren bei ausreichender Schlüssellänge zurzeit sicher sind, besteht die Gefahr das verschlüsselte Kommunikation abgefangen und gespeichert wird bis eine Entschlüsselung möglich ist. Diese Gefahr ist bei digitalen Signaturen weniger akut, da sie oft eine beschränkte Gültigkeitsdauer besitzen [5].

Nach aktuellem Wissenstand sind symmetrische Verschlüsselungsverfahren wie AES und Hashfunktionen weniger anfällig gegenüber Quantencomputern und können durch Erhöhung der Schlüssellänge gegen neue Quantenalgorithmen wie dem Grover abgesichert werden. Im Gegensatz dazu basieren die für Verschlüsselung und Signaturen verwendeten asymmetrischen Verfahren auf Komplexitätsannahmen die durch Shors Algorithmen nicht mehr gelten. PQC untersucht deshalb neue Ansätze um asymmetrische Verschlüsselung und Signaturen zu ermöglichen [5].

Varianten / Algorithmen

Folgend werden die fünf Arten von Algorithmus Familien beschrieben, die zur Realisierung asymmetrischer PQC-Systeme untersucht werden [5] [6]:

Hashbasierte Signaturen

Bei hashbasierten Signaturen werden Systeme betrachtet, deren Sicherheit auf der gut untersuchten Schwierigkeit der Berechenbarkeit von symmetrischen Hashfunktionen basiert. Oft verwenden diese Verfahren Hash-Bäumen, ein spezielles Verfahren, dass es ermöglicht, mehreren Einmal-Signaturen einen gemeinsamen Verifikationsschlüssel zuzuweisen. Solche Systeme sind daher zustandsbehaftet, d.h. der Erzeuger der Signatur muss seinen Signaturschlüssel nach jedem Vorgang aktualisieren und bereits bei dem Erstellen der Schlüssel wird die maximale Anzahl an Signaturen festgelegt. Zu diesen Verfahren zählen die bereits standardisierten *eXtended Merkle Signature Scheme* (**XMSS**) und *Leighton Micali System* (**LMS**). Es sind auch zustandslose Signatursysteme basierend auf Hashfunktionen möglich, allerdings werden dann mehr Rechenzeit zur Erstellung der Signaturen und längere Signaturen benötigt. Ein Beispiel für ein zustandsloses Signatursystem ist **SPHINCS** [7].

Codebasierte Kryptographie

Es ist auch möglich Verschlüsselungen zu realisieren basierend auf der Annahme, dass bestimmte mathematische Probleme der Codierungstheorie angewandt auf *Error Correcting Codes* schwer zu lösen sind. Der bekannteste Vertreter ist das **McEliece** Kryptosystem, das bereits seit mehr als 40 Jahren untersucht wird und auf sogenannten *Goppa Codes* basiert. Zusätzlich zu der langjährigen Sicherheitsanalyse weist es sehr effiziente Ver- und Entschlüsselung auf. Allerdings sind die öffentlichen Schlüssel extrem groß. Das darauf basierende **Niederreiter** Kryptosystem kann die Größe der öffentlichen Schlüssel auf ca. 1 MB reduzieren, allerdings sind die verwendeten besser strukturierten Codes wie *QC-*

MDPC noch nicht so tief analysiert worden. In einem Bericht zur 22. DFN-Sicherheitskonferenz wurde demonstriert, dass der DH Algorithmus im IKE Protokoll durch das Niederreiter-Verfahren ersetzt werden kann [8].

Multivariate Kryptographie

Mit multivariater Kryptographie werden Kryptosysteme bezeichnet, die auf der Schwierigkeit der Lösung multivariater Polynom-Gleichungssysteme über endlichen Körpern basieren. Viele dieser Systeme sind Signatursysteme, die sehr effizient sind und kurze Signaturen aber sehr lange Schlüssel verwenden. Bekannte Beispiele für diese Art von Algorithmen sind **GeMSS** und **Rainbow**.

Gitterbasierte Kryptographie

Diese kryptographischen Systeme basieren auf der Schwierigkeit von mathematischen Problemen in Gittern. Aufgrund ihrer hohen Effizienz in kryptographischen Anwendungen werden sie sehr intensiv untersucht. Verfahren zum Schlüsselaustausch sind beispielsweise **NewHope**, **FrodoKEM** und **CRYSTALS-Kyber**. Zu den gitterbasierten Signatursystemen zählen **FALCON** und **CRYSTALS-Dilithium**. Das gitterbasierte Verfahren CRYSTALS-Kyber muss besonders hervorgehoben werden, da es bereits vielfältig angewandt wird. So unterstützt *Google Chrome* seit Ende 2023 (Version 116) für TLS das X2551Kyber768 Schlüsselaustauschverfahren, das einen PQC Schlüssel mittels einer Kombination aus (*Elliptic Curve*) ECDH und CRYSTALS-Kyber generiert [9]. Analog wird auch im Messenger *Signal* seit Ende 2023 das PQXDH Protokoll verwendet [10] und *Apple* gab Anfang 2024 bekannt, künftig das PQ3 Protokoll für seinen Messenger *iMessage* zu verwenden [11]. Bei beiden Protokollen handelt es sich um hybride Schlüsselaustauschverfahren basierend auf ECDH und CRYSTALS-Kyber.

Isogenbasierte Kryptographie

Diese Art von Algorithmen werden auch als supersinguläre isogenbasierte Algorithmen bezeichnet. Als kryptografisches Prinzip wird dabei eine bekannte Isogenie (d.h. eine Abbildung mit speziellen Eigenschaften) zwischen zwei supersingulären elliptischen Kurven ausgenutzt. Für Angreifer besteht die Schwierigkeit darin, diese Isogenie zwischen den beiden Kurven zu finden. Ein Beispiel ist der sogenannte *Supersingular Isogeny DH Key Exchange* (**SIKE**) Algorithmus [12].

Standardisierungen und Empfehlungen

NIST

Bereits 2016 startete das *National Institute for Standards and Technology* (NIST) einen mehrstufigen Auswahlprozess, der das Ziel hat geeignete PQC-Algorithmen für Digitale Signaturen und Schlüsselaustausch zu finden und zu standardisieren [13]. Die erste PQC-Standardisierungskonferenz zur Vorstellung potentieller Kandidaten fand 2018 statt. Im Rahmen dieser Konferenz wurden noch über 50 Algorithmen vorgestellt. Im Jahr 2022 fand die vierte PQC-Standardisierungskonferenz statt. Besonders hervorzuheben ist die Vorstellung eines Seitenkanalangriffes auf die FACLON Signatur. Anschließend wurden folgende Algorithmen ausgewählt, die den Kriterien der Ausschreibung des NIST genügen [14]:

Tabelle 1: NIST PQC Kandidaten 2022.

Klassifikation	Name des Algorithmus	Kategorie /Verfahren
Public-Key Verschlüsselung	CRYSTALS-Kyber[1]	gitterbasiert
Digitale Signatur	CRYSTALS-Dilithium	gitterbasiert
	FALCON	gitterbasiert
	SPHINCS$^+$	hashbasiert

Eine fünfte PQC-Standardisierungskonferenz wird am 10.-12. April 2024 stattfinden [15]. Eine komplette Übersicher aller PQC-Algorithmen, die bisher am NIST Auswahlverfahren teilgenommen haben, ist auf [16] abrufbar.

Neben der Auswahl geeigneter PQC-Algorithmen durch Ausschreibungen kümmert sich das NIST auch aktiv um die Standardisierung der ausgewählten Algorithmen. Zusammen mit dem *U.S. Department of Commerce* werden *Federal Information Processing Standards* (FIPS) veröffentlicht. Aktuell befinden sich drei PQC-Verfahren im Standardisierungsprozess: CRYSTALS-Dilithium, CRYSTALS-Kyber und SPHINCS$^+$ [17]. Außerdem wurde bereits im Oktober 2020 die Standardisierung der zustandsbehafteten hashbasierten Signaturverfahren LMS und XMSS abgeschlossen. Tabelle 2: Übersicht FIPS Veröffentlichungen gibt eine Übersicht über FIPS Veröffentlichungen mit PQC-Bezug:

Tabelle 2: Übersicht FIPS Veröffentlichungen.

Spezifikation	Basis Algorithmus	Titel
FIPS-203	CRYSTALS-Dilithium	Module-Lattice-Based Key-Encapsulation Mechanism (**ML-KEM**) Standard
FIPS-204	CRYSTALS-Kyber	Module-Lattice-Based Digital Signature (**ML-DSA**) Standard
FIPS-205	SPHINCS$^+$	Stateless Hash-Based Digital Signature (**SLH-DSA**) Standard
SP 800-208	LMS	Recommendation for Stateful Hash-Based Signature Schemes -> Erweiterung von FIPS-186 (Digital Signature Standard)
	XMSS	

ETSI

Das *European Telecommunications Standards Institute* (ETSI) ist eine europäische Normungsorganisation, die weltweite Standards im Bereich Informations- und Kommunikationstechnologien schafft. Für den Bereich PQC hat ETSI die *Quantum Safe Cryptography* (QSC) Working Group gegründet [18], die u.a. Empfehlungen und Beurteilungen für PQC-Protokolle und Leitlinien für die Umsetzung solcher Protokolle herausgibt. Im Jahr 2020 veröffentlichte die QSC-Group das Strategiepapier ETSI TR 103 619, das

[1] **Anmerkung zu CRYSTALS-Kyber**: Schwedische Wissenschaftler konnten 2023 zeigen, dass dieser Algorithmus eine Schwachstelle im Hinblick auf die kryptografische Sicherheit aufweist. Mithilfe von Machine Learning gelang es einen Seitenkanalangriff zu realisieren [54]. Dieser Angriff wird vermutlich auf der fünften PQC Standardisierungskonferenz vorgestellt werden.

Empfehlungen und Strategien enthält, die die Umstellung auf PQC sichere Systeme erleichtern sollen. Außerdem liegt ein Whitepaper *Quantum Safe Cryptography and Security* [4] vor, dass sich u.a. mit potentiellen Upgrades von Zertifikaten wie X.509, TLS, IKE auseinandersetzt.

BSI

Das *Bundesamt für Sicherheit in der Informationstechnik* (BSI) beschäftigt sich auch mit PQC und analysiert potentielle Gefahren die durch zukünftige Quantencomputer entstehen. In der Rubrik Entwicklungsstand Quantencomputer [19] informiert das BSI über den Stand der Technik und über Technologien, die in Quantencomputern vermutlich eingesetzt werden.

Um Organisationen wie Unternehmen oder öffentliche Institutionen bestmöglich auf zukünftige Bedrohungen durch Quantencomputer vorzubereiten, veröffentlicht das BSI regelmäßig Leitlinien, Handlungsempfehlungen und technische Richtlinien, die Themen wie die quantensichere Gestaltung von Kryptografie, die Migration zur PQC und als bisher sicher eingestufte PQC Algorithmen enthalten. Zudem führt das BSI auch Marktumfragen zum Thema Kryptographie und Quantencomputing durch, um damit das Bewusstsein für dieses Thema bei Unternehmen zu erhöhen. Aktualisierte Links zu den beschriebenen Themen und Umfragen veröffentlicht das BSI unter der Rubrik Quantentechnologien und quantensichere Kryptographie [20].

Für die Schüsseleinigung empfiehlt das BSI das codebasierte Verfahren Classic McEliece und das gitterbasierte Verfahren FrodoKEM [5].

Neben dem reinen Informieren zum Thema PQC kümmert sich das BSI auch aktiv um die Implementierung quantensicherer Algorithmen. Zu diesem Zweck kooperiert das BSI zusammen mit der Firma *Rhode & Schwarz Cybersecurity GmbH*. Ziel dieser Kooperation ist die Schaffung einer neuen Version (3.0) der freien Kryptographie-Bibliothek *Botan*, die neben herkömmlichen auch PQC-Algorithmen enthalten soll [21].

BMBF

Das *Bundesministerium für Bildung und Forschung* (BMBF) hat bereits verschiedene Forschungsprojekte gegründet, die die Nutzbarkeit bzw. den Einfluss von Quantentechnologie auf unterschiedliche Branchen untersucht [22]. Zu diesen Projekten gehören:

- *Aquorypt*: behandelt eingebettete Systeme in der Industrie und Chipkarten-basierte Sicherheitsanwendungen
- *PQC4MED*: beschäftigt sich mit Anwendungen aus dem Bereich Medizintechnik
- *QuantumRISC*: behandelt die besonderen Anforderungen die sich durch die limitierten Ressourcen von eingebetteten Systemen ergeben
- *FLOQI* (Full Lifecycle Post Quantum PKI): zielt auf die Entwicklung einer Quantencomputer-resistenten PKI
- *KBLS*: will die freie Kryptographie-Bibliothek *Botan* um PQC-Verfahren erweitern

CACR

Analog zum NIST startete auch die *Chinese Association for Cryptologic Research* (CACR) in den Jahren 2018 und 2019 eine Ausschreibung für PQC-Algorithmen. Es wurden jedoch nur Vorschläge von chinesischen Entwicklern akzeptiert. Leider sind die insgesamt 36 eingereichten Algorithmen bisher nur in chinesischer

Sprache verfügbar. Dennoch sollten die weitere Entwicklung dieser PQC-Vorschläge verfolgt werden, da CACR eine weitere Ausschreibung auf internationaler Ebene starten könnte und China seine Vorschläge zu PQC auch an internationale Standards angleichen wird [23].

NCSC

Das britische *National Cyber Security Center* (NCSC) veröffentlicht regelmäßig Artikel zur PQC-Migration und Vorbereitung auf diese neue Technologie. Das NCSC entwickelt im Gegensatz zum CACR und NIST keine eigenen Algorithmen für eine spätere Standardisierung. Bisher wurden zwei Whitepapers zur PQC-Migration [24] und Vorbereitung auf PQC [25] auf der NCSC Website veröffentlicht. Aus diesen Whitepapers geht hervor, dass auch das NCSC die in Tabelle 2 aufgeführten Spezifikationen bzw. Algorithmen empfiehlt. Folgende Punkte sollten jedoch dabei berücksichtigt werden:

- Die Algorithmen der Kategorien ML-KEM (CRYSTALS-Kyber) und ML-DSA (CRYSTALS-Dilithium) haben vielseitige Anwendungsgebiete. Insbesondere empfiehlt das NCSC die Verwendung von ML-KEM-768 und ML-DSA-65, da sie sich durch ein hohes Maß an Sicherheit und Effizienz auszeichnen.
- Die hashbasierten Signaturen SPHINCS$^+$, LMS und XMSS unterscheiden sich von ML-DSA und FALCON dahingehend, dass sie von unterschiedlichen (kryptografischen) Annahmen ausgehen. SPHINCS$^+$, LMS und XMSS sind im Gegensatz zu ML-DSA deutlich langsamer und haben lange Signaturen und sind somit nicht für den allgemeinen Einsatz bestimmt. Sie eignen sich daher für Anwendungsgebiete in denen digitale Signaturen gelegentlich verwendet werden wie z.B. bei Software- und Firmwareupdates, wo Geschwindigkeit bzw. Performance weniger eine Rolle spielen.
- Bei der Verwendung vom XMSS und LMS ist besonders darauf zu achten, dass eine Signatur nur einmal verwendet wird. Daher sollten diese beiden Algorithmen nur in solchen Fällen verwendet werden, wo die Überwachung des Status eines Schlüssels garantiert ist.

Marktausblick

Bei der Umsetzung von PQC-Algorithmen kommt vor allem Software zum Einsatz. Dies hat zur Folge, dass auf teure Hardware weitestgehend verzichtet werden kann und die PQC Integration deutlich kostengünstiger ist. Außerdem lässt sich die PQC-Technologie dadurch in bereits existierende Netzwerke unabhängig von der Hardware wesentlich einfacher integrieren.

Nachteilig ist, dass es trotz jahrelanger Entwicklung und Testen dieser Algorithmen keine 100% Garantie auf die kryptographische Sicherheit gibt. Im Jahre 2023 konnten schwedische Wissenschaftler einen Seitenkanalangriff auf einen vom NIST sicher eingestuften PQC-Algorithmus demonstrieren, siehe oben in der Anmerkung zu CRYSTALS-Kyber.

Migration

Schon jetzt sollten Unternehmen und Behörden ein Bewusstsein für die zukünftige Bedrohung durch Quantencomputern auf gängige kryptografische Verfahren entwickeln. Werden heute sensible verschlüsselte Daten abgefangen, die mit klassischen Computern derzeit nicht entschlüsselt werden können, so sind sie (möglicherweise) in Zukunft nicht mehr sicher. Aus diesem Grund besteht schon jetzt ein Handlungsbedarf kritische Infrastrukturen und Daten gegenüber Quantencomputern abzusichern.

Obwohl eine Standardisierung von PQC-Algorithmen derzeit noch nicht abgeschlossen ist, gibt es bereits (Handlungs-) Empfehlungen für eine Migration hin zu Quantencomputer resistenten Verfahren.

CISA/NSA/NIST

Im August 2023 haben die amerikanische *Cybersecurity and Infrastructure Security Agency* (CISA) in Kooperation mit der NSA und dem NIST Handlungsempfehlungen für Unternehmen und Behörden zum Umstieg auf PQC herausgegeben [26]. Darin wird empfohlen, dass innerhalb einer Organisation ein Management Team zu etablieren ist, dass sich um die Planung und Vorbereitung für eine PQC Migration kümmert. Ein weiteres sog. *Quantum-Readiness* Team soll verwendete kryptografische Systeme in der Organisation identifizieren, die anfällig gegenüber Angriffen von Quantencomputer sind. Nach der Identifizierung kritischer Infrastrukturen (Inventar), kann eine Priorisierung –abhängig vom jeweiligen Risiko- bei der PQC-Migration erfolgen. Als weitere Maßnahme sollen Organisationen Kontakt mit Herstellern bzw. Zulieferern aufnehmen, um zu evaluieren, inwiefern sie ihre Produkte (Software, Hardware) gegenüber der (zukünftigen) Bedrohung absichern wollen bzw. welche Roadmaps und Maßnahmen sie bezgl. der PQC-Migration ergreifen.

BSI

Das BSI hat bereits einige Maßnahmen veröffentlicht [5] [27], um einen einfacheren Umstieg auf PQC-Technologie zu ermöglichen:

- **Kryptoagilität**: Kryptoagilität ist ein Designkriterium für derzeitige und zukünftige kryptografischen Protokolle und Anwendungen. Diese sollen nach Möglichkeit so konzipiert sein, dass ein Kryptographie-Verfahren, was sich im Nachhinein als unsicher erweist, einfach durch ein anderes ohne großen Aufwand oder gar Neuimplementierung ersetzt werden kann.
- **Hashbasierte Signaturverfahren**: Für Firmwareupdates sollen nach Möglichkeit zustandsbehaftete Signaturverfahren eingesetzt werden. Grund dafür ist, dass diese PQC-Verfahren nur eine geringe zur Verfügung stehende Anzahl an Signaturen liefern und sich daher z.B. für Firmware-Updates eignen.
- **Schlüssellänge für symmetrische Verfahren**: Wie bereits erwähnt sind symmetrische -im Unterschied zu asymmetrischen- kryptographische Verfahren resistenter gegen Quantencomputer. Jedoch sollte die Schüssellänge auf 256 Bit erhöht werden, um die Gefährdung durch den Grover Algorithmus zu reduzieren.
- **Kurzfristige Schutzmaßnahmen**: Symmetrische Schüssel werden meist über PQC anfällige asymmetrische Verfahren verteilt. Daher können vorverteilte symmetrische Langzeitschüssel einen Schutz vor Angriffen gewährleisten. Jedoch bleibt das Problem der Verteilung dieser Schlüssel bestehen.
- **Hybride Lösungen**: Da die Entwicklung und Standardisierung quantenresistenter Verfahren noch nicht abgeschlossen ist und sich mögliche Schwächen erst in der Implementierung oder durch Seitenkanal-Angriffe zeigen, empfiehlt das BSI solche Algorithmen nicht isoliert, sondern nur in Kombination mit klassischen Verfahren einzusetzen.

Anpassung kryptografischer Protokolle

Verschiedene Sicherheitsprotokolle wie z.B. IKE oder TLS müssen angepasst werden, da in diesen vulnerable asymmetrische Verfahren zum Einsatz kommen. Mögliche Anpassungen an PQC sollen anhand von TLS, IKE und X.509 Zertifikaten näher erläutert werden [4] [5]:

IKE

Das IKEv2 Protokoll sieht zur Generierung des gemeinsamen Sitzungsschlüssels nur den (EC)DH Algorithmus vor, der anfällig für Attacken durch Quantencomputer ist. Demgegenüber bietet IKEv1 für den Prozess der Authentisierung und Generierung des gemeinsamen Schüssels die Möglichkeit, einen *Pre-Shared Key* mitzuverwenden. In IKEv2 können solche Schlüssel lediglich für die Authentisierung verwendet werden. Es existiert allerdings RFC 8784 der es wieder möglich macht *Pre-Shared Keys* auch für die Schlüsselerzeugung zu verwenden. Die Verwendung von (hybriden) PQC-Verfahren benötigt allerdings eine größere Änderung des Standards.

TLS

Wie auch bei IKE wird bei TLS ein asymmetrisches Verfahren wie RSA oder ECDH für den Schüsselaustausch verwendet, wodurch TLS vulnerabel ist. 2018 untersuchte *Google* inwieweit sich die vom NIST vorgestellte PQC-Verfahren zum Schlüsselaustausch in TLS 1.3 integrieren lassen [28]. Die beiden wichtigsten Ergebnisse dieser zweistufigen Studie waren: PQC-Algorithmen, die auf unstrukturierten Gittern basieren, führen zu einer großen zusätzlichen Verzögerung beim TLS Handshake und sind daher für die Integration in das TLS Protokoll ungeeignet. Kryptografische Verfahren, die strukturierte Gitter oder supersinguläre Isogenien nutzen, eignen sich für den Einsatz in TLS, wobei erstere deutlich schneller sind und daher zu geringeren Verzögerungen führen. Während das Hinzufügen eines (hybriden) PQC-Schlüsselaustauschverfahrens grundsätzlich nur eine kleine Änderung des Standards darstellt, ist es problematisch dass bei vielen PQC-Verfahren die verwendeten öffentlichen Schlüssel sehr groß sind. Das limitiert stark die möglichen PQC-Algorithmen da seit TLS 1.3 die öffentlichen Schlüssel im initialen TLS Handshake enthalten sind.

X.509 Zertifikate

Die X.509 Zertifikatstruktur kann unkompliziert um neue Signaturverfahren erweitert werden. Allerdings werden diese Zertifikate in sehr verschiedenen Protokollen verwendet, die gegebenenfalls Probleme mit sehr langen Signaturen haben können. Für hybride Signaturverfahren liegen bereits erste IETF Entwürfe wie z.B. draft-ounsworth-pq-composite-sigs-12 vor.

QKD

Definition

QKD (kurz für ***Quantum Key Distribution***) beschreibt eine Gruppe von Verfahren, die es ermöglichen, geheime gemeinsame Zufallszahlen basierend auf quantenmechanischen Prinzipien zu erzeugen. Während im klassischen Fall Verschlüsselungen auf (oft unbewiesener) mathematischer Komplexität basieren, ermöglicht die QKD im Prinzip absolute Sicherheit, da die Verschlüsselung auf grundlegenden physikalischen Gesetzen basiert. QKD bietet sich insbesondere als Ersatz für bisher verwendete asymmetrische Verschlüsslungsverfahren an.

Als Teil der zweiten Quantenrevolution befindet sich QKD am Übergang zwischen Forschung und Anwendung und erste kommerzielle Systeme sind bereits erhältlich. Zeitgleich werden neue Verfahren entwickelt und es ist nicht klar welche Protokolle sich etablieren werden.

Allen Ansätzen ist gemein, dass es aktuell starke Limitierungen bezüglich Reichweite und Übertragungsraten gibt. Außerdem werden parallel zu der bestehenden Hardware neue Komponenten benötigt um sogenannte Quantenkanäle zu schaffen. Die nachfolgenden Abschnitte basieren soweit nicht anders spezifiziert auf [29].

Hintergrund

In den Quantenkanälen findet der Informationstransport mittels sogenannter QuBits statt. Analog zu den klassischen Bits die in verschiedenen Formen vorliegen, z.B. als Lichtpuls in einer Glasfaser oder als Magnet in einer Festplatte, können auch QuBits verschieden realisiert werden. Für den Informationstransport werden fast ausschließlich Photonen, also ‚Lichtteilchen', verwendet. Eine binäre Information kann dabei beispielsweise in der Lichtpolarisation, also der Schwingungsrichtung des Lichtfeldes, kodiert werden. In der nachfolgenden Beschreibung wird davon ausgegangen, dass ein Photon mit einer vertikalen oder diagonalen Polarisation (Zustand |↕> oder |↗>) einer **0** entspricht und eine horizontale oder antidiagonale Polarisation (Zustand |↔> oder |↖>) einer **1** entspricht.

Quantenobjekte haben eine Reihe besonderer Eigenschaften. So gibt es keine Möglichkeit Zustände zu kopieren und Messungen (zer)stören den originalen Zustand. Für die davor beschriebenen Polarisationszustände kann daher entweder bestimmt werden, ob das Photon vertikal/horizontal polarisiert ist (im Folgenden bezeichnet als Messung in der +-Basis) oder anti-/diagonal (Messung in der x-Basis), da nach der Messung das Photon nicht mehr im ursprünglichen Zustand vorliegt. Beispielsweise ausgehend von einem |↕> Zustand, würde eine Messung in der +-Basis eine vertikale Polarisation ergeben und den Zustand danach in |↕> überführen. Würde allerdings in der x-Basis gemessen werden, so würde mit jeweils 50 % Wahrscheinlichkeit anti-/diagonale Polarisation gemessen werden und der Zustand danach die gemessene Polarisation annehmen. Die ursprüngliche Information über die vertikale Polarisation wäre verloren.

Eine weitere faszinierende Eigenschaft von Quantenobjekten ist, dass sie verschränkt sein können. Sind beispielsweise zwei Photonen verschränkt, so befinden sie sich in einem gemeinsamen Zustand und Messungen an einem der beiden Photonen bestimmen die möglichen Messergebnisse an dem anderen, egal wie weit die beiden Photonen voneinander entfernt sind.

Allerdings sind Quantenzustände sehr empfindlich und werden durch Interaktionen mit der Umwelt bei der Propagation durch Glasfasern spätestens nach einigen hundert Kilometern zerstört. Auch die

Erzeugung und Detektion einzelner Photonen ist technisch sehr anspruchsvoll und benötigt spezialisierte Hardware.

Verfahren und Protokolle

BB84 Protokoll

Bei dem BB84 Protokoll handelt es sich um eine der ersten Überlegungen zu QKD. Der Sender Alice bereitet die Polarisation von Photonen entsprechend zufälliger Bits bei zufälliger Basiswahl vor und sendet diese dann an den Empfänger Bob. Dieser misst in einer zufälligen Basis und erhält somit teilweise Alices Bits als auch zufällige Werte. Im nächsten Schritt verwenden Alice und Bob einen klassischen Kommunikationskanal und verständigen sich öffentlich darüber, in welchen Fällen sie zufälligerweise die gleiche Basis verwendet haben und somit jetzt die gleichen Zufallszahlen haben sollten. Tabelle 3 zeigt das zugrundeliegende Prinzip im idealen Fall. Abschließend kann ein Teil der gemeinsamen Zufallszahlen öffentlich verglichen werden um die Fehlerrate festzustellen, da jeder Versuch einer dritten Person Eve auf die Quantenkommunikation zuzugreifen unweigerlich Fehler verursachen würde. Wird die Fehlerrate als klein genug erachtet können klassische Fehlerkorrekturalgorithmen sicherstellen, dass Alice und Bob aus den restlichen gemeinsamen Zufallszahlen den gleichen Schlüssel erhalten. 2013 wurde demonstriert, das mit dem BB84 Protokoll über 50 km Glasfaser Übertragungsraten von mindestens 1 Mbps realisiert werden können [30]. 2017 wurde von einer chinesischen Forschungsgruppe ein Schlüsselaustausch mit einem Satelliten realisiert [31] und 2018 wurde über mehr als 400 km Glasfaser erfolgreich ein Schlüssel generiert [32].

Tabelle 3: Prinzip von BB84.

Alice Bits	0	1	0	0	1	1	1	1	0
Alice Basis	+	+	x	+	x	x	X	+	+
Gesendetes Photon	|↕>	|↔>	|↗>	|↕>	|↖>	|↖>	|↖>	|↔>	|↕ >
Bobs Basis	+	x	x	+	x	+	+	+	x
Bobs Bits	0	?	0	0	1	?	?	1	?
Gemeinsamer Schlüssel	**0**		**0**	**0**	**1**			**1**	

E91 Protokoll

Bei dem E91 Protokoll werden verschränkte Photonenpaare von einer zentralen Quelle erzeugt und an die Teilnehmer verteilt. Alice und Bob messen jeweils in einer zufälligen Basis. Anschließend wird öffentlich über einen klassischen Kanal geklärt, ob die gleiche Basis verwendet wurde oder nicht. Im Fall von unterschiedlichen Basen werden die erhaltenen Messwerte verwendet um eine Korrelationsfunktion zu berechnen, die Aufschluss darüber gibt, ob sich der Quantenkanal und die Messgeräte wie erwartet verhalten. Falls das zutrifft, werden die Messwerte bei gleicher Basiswahl zu einem gemeinsamen Schlüssel verarbeitet.

Weitere Verfahren

Neben den eben vorgestellten Protokollen gibt es eine Vielzahl weiterer Verfahren und auch andere diskrete Quanteneigenschaften neben der Polarisation die verwendet werden können. Ausgehend davon, ob verschränkte Zustände verwendet werden (z.B. E91 Protokoll) oder unverschränkte Zustände

entsprechend präpariert und dann gemessen werden (z.B. BB84 Protokoll), spricht man von ***Entanglement-based*** **(EB)** und ***Prepare-and-Measure*** **(PM)** Protokollen.

Da Implementierungen von QKD möglicherweise Schwachstellen schaffen, die in Seitenkanalangriffen ausgenutzt werden könnten, gibt es auch den Ansatz Protokolle zu entwickeln, die während der Schlüsselerzeugung das korrekte Verhalten der verwendeten Geräte sicherstellen. Da diese Protokolle sozusagen von den verwendeten Geräten unabhängig sind, werden sie als ***Device Independent*** **(DI)** bezeichnet. Ähnlich wie bei dem E91 Protokoll werden dafür verschränkte Zustände verwendet und Korrelationsfunktionen berechnet. Die erhöhte Sicherheit bringt allerdings einen technischen Mehraufwand mit sich, der sich in geringeren Reichweiten und Schlüsselraten widerspiegelt.

Eine ähnliche Strategie verfolgen auch Protokolle, bei denen Alice und Bob nur Quantenteilchen senden, während die Messungen öffentlich an einem zentralen Relay stattfinden. Da bei diesen Verfahren die Sicherheit unabhängig von der tatsächlichen Implementierung der Messung ist, werden sie als ***Measurement-Device-Independent*** **(MDI)** bezeichnet.

Eine vielversprechende Realisierung von PM MDI QKD stellt das ***Twin-Field*** **Verfahren** dar. Alice und Bob senden speziell präparierte schwache Laserpulse zu einer zentralen Relay Station. Dort findet Interferenz und anschließend eine Messung statt, deren Ergebnis bekanntgegeben wird. Indem Alice und Bob gewisse Eigenschaften der von ihnen verwendeten Laserpulse bekanntgeben, können sie einen geheimen Schlüssel erhalten. Dieses Verfahren ähnelt klassischen Netzwerkstrukturen und ermöglicht erhöhte Reichweiten und Übertragungsraten, so wurde beispielsweise 2022 in China die Übertragung eines geheimen Schlüssels über 833 km Glasfaser demonstriert [33].

Es ist auch möglich, kontinuierliche statt diskreter Quantenzustände wie die zuvor beschriebene Polarisation zu verwenden. Man spricht in diesem Fall von ***Continuous Variable*** **(CV)** QKD anstelle von ***Discrete Variable*** **(DV)** QKD. Anstelle einzelner Photonen können dann spezielle Laserpulse verwendet werden. Häufig werden kohärente Zustände von Alice mittels Gaußscher Modulation präpariert und von Bob mittels einer homodynen Messung ausgelesen. Ein öffentlicher Vergleich eines Teils der Daten ermöglicht eine Fehlerabschätzung und falls der ermittelte Fehler klein genug ist, findet eine Fehlerkorrektur mit Diskretisierung statt. Ein Vorteil der CV Verfahren ist, dass sie technisch näher an etablierten Verfahren sind und theoretisch leistungsstärker wie die DV Verfahren sind. Allerdings besitzen sie aktuell eine geringere Reichweite. Erst 2020 wurde eine Übertragung über 200 km Glasfaser mit mehr als 5 bps realisiert [34].

Bei allen Verfahren lassen sich Schlüssel nur über wenige hundert Kilometer erzeugen. Da klassische Repeater die Quanteninformationen zerstören, lassen sich höhere Reichweiten aktuell nur über *Trusted Nodes* realisieren. Die aktuelle Forschung untersucht aber auch sogenannte *Quantenrepeater*, die es ermöglichen könnten Quantenzustände mittels Verschränkung über weite Distanzen zu transportieren.

Risiken und Angriffe

Die davor vorgestellten QKD Protokolle wären bei perfekter Implementierung beweisbar absolut sicher. Allerdings ist es möglich, dass die technische Realisierung Schwachstellen erzeugt, die Seitenkanalangriffe ermöglichen. Die jeweiligen Angriffsvektoren unterscheiden sich hierbei von Protokoll zu Protokoll und insbesondere die (M)DI Protokolle weisen weniger Angriffspunkte auf.

Ein wichtiger Angriffsvektor bei PM QKD sind ***Photon-Number-Splitting*** Angriffe. Da Ein-Photonen-Quellen technisch aufwendig sind werden stattdessen normalerweise stark abgeschwächte Laserpulse verwendet, die allerdings häufig mehr als ein Photon enthalten. Das ermöglicht aber, dass einige Photonen unbemerkt abgezweigt und gemessen werden können und somit Teile des Schlüssels ausgespäht werden, ohne dass eine Erhöhung der Fehlerrate auftritt.

Eine mögliche Gegenmaßnahme stellt die Methode der ***Decoy States*** dar. Indem gelegentlich ein Laserpuls mit einer anderen Intensität gesendet wird, ist es möglich während des *Postprocessings* einen solchen Angriff wahrzunehmen und die Schlüsselrate entsprechend anzupassen.

Weitere Angriffsstrategien und mögliche Gegenmaßnahmen werden im ETSI Whitepaper *Implementation Security of Quantum Cryptography* [35] oder in mehr Detail in der Veröffentlichung des BSI *Implementation Attacks against QKD Systems* [36] diskutiert.

Wichtig hervorzuheben ist außerdem, dass bei allen Protokollen die klassische Kommunikation authentifiziert sein muss, da sonst ein ***Man-in-the-Middle*** Angriff durchgeführt werden könnte. Bei einem solchen Angriff gibt sich der Angreifer gegenüber Alice als Bob aus und umgekehrt und erhält dadurch Zugriff auf die gesamte Kommunikation, da die Verschlüsselung nur jeweils zwischen Alice beziehungsweise Bob und dem Angreifer besteht. Um dies zu verhindern können beispielsweise digitale Signaturen zur Authentifizierung eingesetzt werden: Wenn Alice ihre verschlüsselten Nachrichten signiert kann Bob mit ihrem öffentlichem Verifikationsschlüssel sicherstellen, dass die Nachricht auch wirklich von Alice kommt. Bisherige Verfahren basieren allerdings üblicherweise auf Ansätzen die nicht *quantum-safe* sind.

Wie in [37] beschrieben kann auch mit *Pre-Shared Secrets* und klassischen *Message Authentication Codes* wie z.B. dem *Wegman-Carter* Verfahren gearbeitet werden. Hierbei dient ein bereits vor der Kommunikation ausgetauschtes Geheimnis zwischen Alice und Bob um für jede Nachricht eine Prüfsumme zu bestimmen, die die Authentizität der Nachrichten sicherstellt. Obwohl durch diesen Ansatz ein so hohes Sicherheitslevel erreicht werden kann, dass während der gesamten Kommunikation die symmetrische Verschlüsselung das schwächste Glied des Gesamtsystems darstellt, ist der logistische Aufwand der mit *Pre-Shared Secrets* einhergeht sehr nachteilig. Allerdings ist es auch möglich initial PQC-Signaturen zu verwenden die analog zu bisherigen Verfahren funktionieren. Wird die Signatur vor und während der Kommunikation nicht gebrochen, so ermöglicht dieser Ansatz ebenfalls, dass zumindest nach der Kommunikation die symmetrische Verschlüsselung das schwächste Glied des Gesamtsystems darstellt.

Standardisierungen und Empfehlungen

Da QKD im Bereich der Informationssicherheit eingesetzt wird, existieren starke Bemühungen im Hinblick von Standardisierungen trotz des recht jungen Alters der Technologie. Insbesondere das ETSI und die Internationale Fernmeldeunion (ITU) haben bereits Empfehlungen und Standards veröffentlicht.

Eine recht aktuelle und detaillierte Übersicht über bereits erfolgte und noch laufende oder mögliche Standardisierungsbemühungen ist in ITU-T FG QIT4N D2.5 und ITU-T Y.Sup74 zu finden. Nachfolgend wird eine Übersicht über die verschiedenen Richtungen der Standardisierungsbemühungen gegeben:

Architektur, Management und Machine Learning

Die aktuell verfügbare QKD Hardware ist limitiert auf relativ kurzreichweitige *Point-to-Point* Verbindungen. Durch Verwendung eines Schlüsselverwaltungssystems mit *Trusted Nodes* lässt sich der Schlüsseltransport

zwischen beliebig weit entfernten Teilnehmern eines QKD Netzes realisieren. Ein großer Teil der Standardisierungsbemühungen bezieht sich auf dieses Schlüsselverwaltungssystem.

ITU-T Y.3800/3801/3802 definieren ein Schichtenmodell aus Quantenebene, Schlüsselaustauschebene, Kontrollebene, Managementebene und Anwendungsebene. Abbildung 1 dient der Veranschaulichung der Funktionalitäten der verschiedenen Ebenen und deren Beziehungen untereinander:

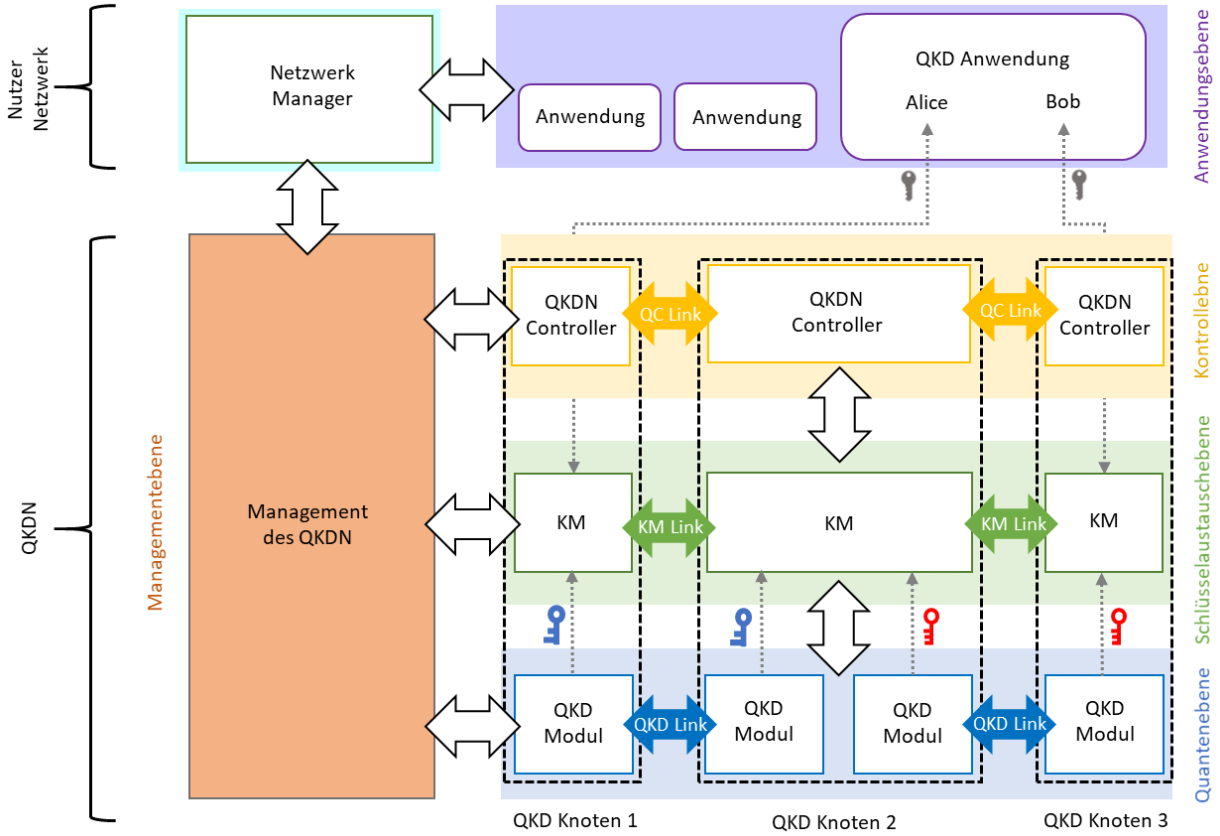

Abbildung 1: Realisierung einer QKD Anwendung mittels eines QKD Netzes (QKDN) mit 3 Nodes und dezentraler Kontrollebene.

In der Quantenebene findet zwischen benachbarten Knoten des QKD Netzes die Erzeugung gemeinsamer Schlüssel statt. Hierbei kommunizieren die QKD Module über QKD *Links* und erhalten nach dem *Postprocessing* jeweils gemeinsame geheime Zufallszahlen. Diese werden an die Schlüsselaustauschebene (engl. *Key Management* (KM)) weitergeben. Neben der Verwaltung der Schlüssel in den Knoten realisiert diese Ebene den Schlüsselaustausch über das gesamte Netzwerk mithilfe der KM *Links* und kommuniziert außerdem mit den Anwendungen in der Anwendungsebene. Die Kontrollebene koordiniert die über alle Knoten verteilte Schlüsselaustauschebene und kann sowohl durch einen zentralen QKDN Controller als auch durch dezentralisierte QKDN Controller in allen Knoten realisiert werden. Die Managementebene verwaltet das gesamte Netzwerk.

Empfehlungen für die Schlüsselaustauschebene sind in ITU-T Y.3803 zu finden. Allgemeine Empfehlungen für die Kontroll- und Managementebene werden in ITU-T Y.3804 gegeben, während *Quality of Service* in ITU-T Y.3806/3807/3811 behandelt wird. Außerdem beschäftigt sich ITU-T Y.3805 mit *Software-Defined Networking* wofür in ETSI GS QKD 015/018 Schnittstellen festgelegt werden.

Inwieweit *Machine Learning* eingesetzt werden kann, wird in ITU-T Y.3812/3814/3816/Sup70 untersucht, insbesondere im Hinblick auf Kontrolle und Management.

ITU-T Y.3808 und ITU-T X.1715 befassen sich mit Überlegungen zur Integration von QKD Netzen mit *Secure Storage Networks*.

Interoperabilität

Da es viele verschiedene QKD Protokolle mit jeweils sehr spezifischen Hardware Anforderungen gibt, konzentrierten sich bisherige Standardisierungsbemühungen hauptsächlich auf die Schichten oberhalb der Quantenebene. Allerdings beschäftigt sich der bald veröffentlichte ETSI GR QKD 019 u.a. mit den Schnittstellen der authentifizierten klassischen Kommunikation in der Quantenebene. Die QKD Module an den Knoten sind somit nicht wirklich interoperabel.

Es besteht jedoch Potential für eine Interoperabilität mit dem bestehenden klassischen Datenverkehr in den Glasfasern wie in ETSI GS QKD 012 und insbesondere ITU-T FG QIT4N D2.4 beschrieben ist. *Wavelength-Division Multiplexing* mit klassischem Datenverkehr ist grundsätzlich möglich, allerdings sind klassische Signale mehrere Größenordnungen stärker und müssen deshalb abgeschwächt werden um Störungen zu reduzieren. Hierbei ist CV QKD weniger empfindlich. Klassische Repeater zerstören die Quanteninformation und dürfen deshalb nicht in dem Kanal enthalten sein oder müssen umgangen werden und selbst in *Multicore Fibers* gibt es Einschränkungen für die verwendeten Wellenlängen der angrenzenden Kanäle. Insbesondere für lange Reichweiten bieten sich jedoch separate Kanäle an, da jegliche Störungen die Reichweite und Datenrate reduzieren und spezialisierte Hardware wie beispielsweise *Hollow Core Fibers* vorteilhaft sein kann.

Die Interoperabilität zwischen verschiedenen Schlüsselverwaltungssystemen wird ausführlich in ITU-T Y.3810/3813/3817/3818 behandelt. Außerdem wird das bald erscheinende ETSI GS QKD 020 eine Schnittstelle dafür definieren.

Für die Weitergabe der Schlüssel an Anwendungen liegen Empfehlungen in ITU-T Q.4160 vor und es werden häufig die Schnittstellen definiert in ETSI GS QKD 004/014 verwendet. Daneben gibt es aber auch proprietäre Ansätze wie das CISCO SKIP (*Secure Key Import Protocol*) für die Schlüsselweitergabe an CISCO Geräte.

Sicherheitszertifizierungen

Bezüglich einer Sicherheitszertifizierung nach ISO/IEC 15408 "Common Criteria" für QKD Geräte gibt es aktuell eine Definition eines Schutzprofils nach ETSI GS QKD 016 für PM QKD basierte Geräte und einen alternativen Ansatz in ISO/IEC 23837 wo grundlegende funktionale Sicherheitsanforderungen für QKD Systeme definiert und untersucht werden.

Jenseits davon beschäftigt sich ITU-T Y.3815 mit der Widerstandsfähigkeit von QKD Netzen und es liegen Sicherheitsempfehlungen in ITU-T X.1710/1712/1714 für die Schlüsselaustauschebene vor. ETSI GS QKD 005/008 und die bald veröffentlichten ETSI GS QKD 010/013 beschäftigen sich mit der Implementierungssicherheit beziehungsweise der Charakterisierung der QKD Module und kritischer Komponenten.

Marktanalyse

QKD stellt eine neue Technologie mit viel Potential da. Aktuell gibt es in dem Feld sehr viele neue Start-Ups, die oft Ausgründungen aus Forschungsinstituten sind. Allerdings gibt es auch bereits Unternehmen die mehrere Jahre Erfahrung haben und auch einige große internationale Unternehmen sind in dem Feld aktiv. Oft kommt es auch zu sehr enger Zusammenarbeit mit den Telekommunikationsunternehmen. Einen lehrreichen Einblick stellt das GÉANT Infoshare vom 21.06.2023 [38] da, worauf dieser Abschnitt soweit nicht anders angegeben basiert.

Tabelle 4 zeigt eine Auswahl an aktuell verfügbaren kommerziellen QKD Systemen. Bereits 2009 betrug der Preis für ein QKD Gerätepaar von *ID Quantique* nur noch knapp über 80.000 $ [39]. Forschung und Entwicklungen im Feld der integrierten Optik, dem optischen Äquivalent von integrierten Schaltkreisen, versprechen allerdings erhebliche Vergünstigungen.

Tabelle 4: Ausgewählte kommerzielle QKD Systeme.

Hersteller	**Produkt (Jahr)**	**Maximale Reichweite**	**Schlüsselrate**	**QKD Protokoll**
Standards	**Abmessungen**	**Frequenzband**	**Anmerkungen**	
Toshiba	Multiplexed QKD System MU (2020 [40])	30 dB -> 90 km	300 kbps @ 10 dB	Decoy BB84
ETSI 014	19‘‘, 3U	O		
Toshiba	Long-Distance QKD System LD (2020 [40])	30 dB -> 150 km	300 kbps @ 10 dB	Decoy BB84
ETSI 014	19‘‘, 3U	C		
LuxQuanta	NOVA LQ (2023 [41])	8 dB -> 40 km		CV QKD
ETSI 004+014	19‘‘	C	100% EU	
QTI	Quell-X (2022 [42])	30 dB	2 kbps @ 14 dB	Decoy BB84
ETSI 014+015, CISCO SKIP	19‘‘, 2U	C, O	100% EU	
ID Quantique	Clavis XG (2022 [43])	30 dB -> 150 km	1 kbps @ 24 dB [44]	Decoy BB84
ETSI 014+018	19‘‘, 1U	O	100% EU	
ID Quantique	Cerberis XG (2021 [45])	18 dB -> 90 km	2 kbps @ 12 dB [46]	PM QKD
ETSI 014+018	19‘‘, 1U	O	100% EU	
ThinkQuantum	QuKy (2022 [47])	33 dB -> 165 km	18 kbps @ 13 dB	Decoy BB84
ETSI 004+014, CISCO SKIP	19‘‘, 2U	C, O	100% EU	

Migration

Verschlüsselungen basierend auf QKD sind in verschiedenen Schichten möglich. QKD wird dabei für den initialen Schlüsselaustausch verwendet. Eine aktuelle Übersicht über die Kompatibilität zu bisherigen Verschlüsselungsprotokollen ist in ITU-T XSTR-HYB-QKD zu finden. Wie bei PQC befindet sich die

standardisierte Integration in die bisher verwendeten Protokolle noch am Anfang aber es sind bereits funktionierende Lösungen verfügbar.

Ein Beispiel für Schicht 1 Verschlüsselung mit QKD über die ETSI 014 Schnittstelle sind die *Apollo TM400ENB – 400G Multiservice Encryption Muxponder* von *Ribbon* [38]. Die Kompatibilität zwischen MACsec in Schicht 2 und ETSI 014 wurde von *Juniper* in einem Whitepaper [48] untersucht und ein konkretes Protokoll wird in [49] vorgeschlagen. In Schicht 3 verwendet IPsec mit IKEv2 aktuell kein *post-quantum* Protokoll, allerdings ermöglicht RFC 8784 für IKEv2 die zusätzliche Verwendung eines *Pre-Shared Keys* der zum Beispiel aus QKD kommen kann. Dieser Ansatz wurde bereits kommerziell von *CISCO* unter Zuhilfenahme der CISCO SKIP Schnittstelle implementiert [38]. Ein analoger Ansatz von *Juniper* basiert auf ETSI 014 und wird in [50] beschrieben. Auch TLS 1.3 in Schicht 5 bietet Möglichkeiten für *Pre-Shared Keys* die aus QKD kommen können, wie im Detail in [51] untersucht wurde.

Fazit

Quantensichere Kryptographie stellt ein wichtiges Thema mit akutem Handlungsbedarf da. Sowohl PQC als auch QKD sind in der Lage, die Sicherheit von Kryptosystemen gegenüber den voranschreitenden Entwicklungen in der klassischen Algorithmik und Computertechnik, als auch deren Quantenäquivalente zu erhöhen. Außerdem liegen Ansätze und kommerzielle Lösungen bezüglich einer Migration vor.

Gegenüberstellung

Da PQC und QKD stark unterschiedliche Ansätze verfolgen, haben sie jeweils sehr eigene Stärken und Schwächen. Tabelle 5 stellt die wichtigsten Eckpunkte gegenüber.

Tabelle 5: Gegenüberstellung PQC und QKD.

Eigenschaft	**PQC**	**QKD**
Sicherheit	Sicherheitsbeweise für zugrunde liegende Mathematik Gegenstand aktueller Forschung, Sicherheitszertifizierungen größtenteils ausstehend	Sicherheitsbeweise für zugrunde liegende Physik erbracht aber Möglichkeiten für Seitenkanalangriffe, in absehbarer Zeit *Trusted Nodes* nötig, authentifizierte klassische Kanäle nötig, Sicherheitszertifizierungen ausstehend
Umsetzung	Vor allem softwarebasiert	Spezielle Hardware erforderlich
Kosten	Niedrige Kosten, da softwarebasiert	Hohe Kosten wegen spezieller Hardware
Übertragungsmedien	Glasfaser, Kupferleitungen, RF-Übertragung	Nur optische Übertragungsmedien oder *free space*
Reichweite	-	begrenzt (maximal einige hundert km)
Schlüsselrate	z.T. hoher Rechenaufwand	begrenzt

Empfehlungen gegen QKD

Im Zuge der Gegenüberstellung muss das aktuelle Positionspapier *Position Paper on Quantum Key Distribution* aus der Zusammenarbeit des BSI und seinen Schwesterbehörden aus Frankreich, Schweden und den Niederlanden erwähnt werden [52]. Dort wird startend bei den Problemen von QKD aus Tabelle 5 herausgearbeitet, dass für die meisten Anwendungen PQC gegenüber QKD zu empfehlen wäre. Außerdem wird betont, dass selbst für mögliche Anwendungen in speziellen Nischenmärkten die fehlenden Sicherheitszertifizierungen ein großes Problem darstellen.

Auch die NSA spricht sich derzeit für die Verwendung von PQC anstatt von QKD aus [53].

Im Anblick dessen, dass es sich bei beiden Ansätzen um vergleichsweise junge Technologien handelt, zu denen regelmäßig neue Erkenntnisse erbracht werden, bleibt es abzusehen, wie diese Empfehlungen

altern. Insbesondere die voranschreitenden Sicherheitszertifizierungsprozesse zu QKD und den PQC Verfahren sollten aufmerksam verfolgt werden.

Literaturverzeichnis

[1] Wikipedia, "Shor's algorithm," 29 01 2024. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Shor%27s_algorithm&oldid=1200508621. [Accessed 08 02 2024].

[2] Wikipedia, "Grover's algorithm," 02 02 2024. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Grover%27s_algorithm&oldid=1202313743. [Accessed 08 02 2024].

[3] F. Arute et al., "Quantum supremacy using a programmable superconducting processor," *Nature,* 23 10 2019.

[4] ETSI, "White Paper: Quantum Safe Cryptography and Security," 06 2015. [Online]. Available: https://www.etsi.org/technologies/quantum-safe-cryptography. [Accessed 22 02 2024].

[5] BSI, "Quantum-safe cryptography – fundamentals, current developments and recommendations," 18 05 2022. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.html?nn=916626. [Accessed 22 02 2024].

[6] T. Pöppelman, J. Haid and P. Schmitz, "Die Zukunft der Kryptographie im Zeitalter der Quanten," Security Insider, 26 09 2017. [Online]. Available: https://www.security-insider.de/die-zukunft-der-kryptographie-im-zeitalter-der-quanten-a-645548/. [Accessed 09 02 2024].

[7] D. J. Bernstein et al., "SPHINCS: Practical Stateless Hash-Based Signatures," *Advances in Cryptology,* 2015.

[8] E. Zimmer, "Post-Quantum Kryptographie für IPsec," 2015. [Online]. Available: https://svs.informatik.uni-hamburg.de/publications/2015/2015-02-24-Zimmer-DFN-PQC-fuer-IPsec.pdf. [Accessed 22 02 2024].

[9] The Hackers News, "Enhancing TLS Security: Google Adds Quantum-Resistant Encryption in Chrome 116," 11 08 2023. [Online]. Available: https://thehackernews.com/2023/08/enhancing-tls-security-google-adds.html. [Accessed 23 02 2024].

[10] ehrenkret, "Quantum Resistance and the Signal Protocol," Signal, 19 09 2023. [Online]. Available: https://signal.org/blog/pqxdh/. [Accessed 23 02 2024].

[11] Apple, "iMessage with PQ3: The new state of the art in quantum-secure messaging at scale," 21 02 2024. [Online]. Available: https://security.apple.com/blog/imessage-pq3/. [Accessed 23 02 2024].

[12] D. Jao et al., "Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies," *Lecture Notes in Computer Science,* 2011.

[13] NIST, "Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms," 20 12 2016. [Online]. Available: https://csrc.nist.gov/news/2016/public-key-post-quantum-cryptographic-algorithms. [Accessed 09 02 2024].

[14] NIST, "Selected Algorithms 2022," [Online]. Available: https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022. [Accessed 09 02 2024].

[15] NIST, "Fifth PQC Standardization Conference," 30 08 2023. [Online]. Available: https://csrc.nist.gov/Events/2024/fifth-pqc-standardization-conference. [Accessed 09 02 2024].

[16] Fraunfofer AISEC, "qpdb," [Online]. Available: https://www.pqdb.info/. [Accessed 09 02 2024].

[17] NIST, "Post-Quantum Cryptography Standardization," 03 01 2017. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization. [Accessed 09 02 2024].

[18] ETSI, "Quantum-Safe Cryptography," ETSI, [Online]. Available: https://www.etsi.org/technologies/quantum-safe-cryptography. [Accessed 09 02 2024].

[19] BSI, "Entwicklungsstand Quantencomputer," [Online]. Available: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Quantentechnologien-und-Post-Quanten-Kryptografie/Entwicklungsstand-Quantencomputer/entwicklungsstand-quantencomputer_node.html. [Accessed 09 02 2024].

[20] BSI, "Quantentechnologien und quantensichere Kryptografie," [Online]. Available: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Quantentechnologien-und-Post-Quanten-Kryptografie/quantentechnologien-und-quantensichere-kryptografie_node.html. [Accessed 09 02 2024].

[21] BSI, "BSI-Projekt: Entwicklung einer sicheren Kryptobibliothek," [Online]. Available: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kryptografie/Kryptobibliothek-Botan/kryptobibliothek-botan_node.html. [Accessed 09 02 2024].

[22] BMBF, "Post-Quanten-Kryptografie," [Online]. Available: https://www.forschung-it-sicherheit-kommunikationssysteme.de/foerderung/bekanntmachungen/pqk. [Accessed 09 02 2024].

[23] QApp, "CACR post-quantum competition," 2022. [Online]. Available: https://en.qapp.tech/help/cacr. [Accessed 09 02 2024].

[24] H. John, "Migrating to post-quantum cryptography," NCSC, 03 11 2023. [Online]. Available: https://www.ncsc.gov.uk/blog-post/migrating-to-post-quantum-cryptography-pqc. [Accessed 09 02 2024].

[25] NCSC, "Next steps in preparing for post-quantum cryptography," 03 11 2023. [Online]. Available: https://www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography. [Accessed 03 11 2024].

[26] CISA, NIST, NSA, "QUANTUM-READINESS: MIGRATION TO POST-QUANTUM CRYPTOGRAPHY," https://www.cisa.gov/sites/default/files/2023-08/Quantum%20Readiness_Final_CLEAR_508c%20%283%29.pdf, 2023.

[27] BSI, "Migration zu Post-Quanten-Kryptografie," https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Post-Quanten-Kryptografie.pdf?__blob=publicationFile&v=1, 2020.

[28] A. Langley and M. Braithwhite, "Post-quantum confidentiality for TLS," Imperialviolet, 11 04 2018. [Online]. Available: https://www.imperialviolet.org/2018/04/11/pqconftls.html. [Accessed 09 02 2024].

[29] S. Pirandola et al., "Advances in quantum cryptography," *Adv. Opt. Photon,* 2020.

[30] M. Lucamarini et al., "Efficient decoy-state quantum key distribution with quantified security," *Opt. Express,* 2023.

[31] J. G. Ren et al., "Ground-to-satellite quantum teleportation," *Nature,* 09 08 2017.

[32] A. Boaron et al., "Secure Quantum Key Distribution over 421 km of Optical Fiber," *Phys. Rev. Lett.,* 11 2018.

[33] S. Wang et al., "Twin-field quantum key distribution over 830-km fibre," *Nat. Photon,* 2022.

[34] Y. Zhang et al., "Long-Distance Continuous-Variable Quantum Key Distribution over 202.81 km of Fiber," *Phys. Rev. Lett.,* 06 2020.

[35] ETSI, "Whitepaper: Implementation Security of Quantum Cryptography," [Online]. Available: https://www.etsi.org/technologies/quantum-safe-cryptography. [Accessed 08 02 2024].

[36] BSI, "Implementation Attacks against QKD Systems," 21 12 2023. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/QKD-Systems/QKD-Systems.html. [Accessed 08 02 2024].

[37] M. Mosca et al., "Quantum Key Distribution in the Classical Authenticated Key Exchange Framework," *arXiv,* 2012.

[38] "GÉANT Infoshare: QKD and Quantum Solutions 21 June 2023," 21 06 2023. [Online]. Available: https://www.youtube.com/watch?v=bjWvw3rmFQs. [Accessed 09 02 2024].

[39] D. Graham-Rowe, "Quantum Cryptography for the Masses," MIT Technology Review, 28 08 2009. [Online]. Available: https://www.technologyreview.com/2009/08/28/210221/quantum-cryptography-for-the-masses/. [Accessed 08 02 2024].

[40] Toshiba, "Toshiba launches Quantum Key Distribution (QKD) System Business," 19 10 2020. [Online]. Available: https://www.global.toshiba/ww/news/corporate/2020/10/pr1901.html. [Accessed 08 02 2024].

[41] J. Dargan, "LuxQuanta Launches its First CV-QKD System, NOVA LQ™," The QUANTUM Insider, 02 05 2023. [Online]. Available: https://thequantuminsider.com/2023/03/02/luxquanta-launches-its-first-cv-qkd-system-nova-lq/. [Accessed 08 02 2024].

[42] EasyEngineeringMag, "INTERVIEW WITH QTI," Easy Engineering, [Online]. Available: https://easyengineering.eu/interview-with-qti/. [Accessed 08 02 2024].

[43] IDQ, "ID Quantique expands the XG Series with the launch of the Clavis XG," 10 05 2022. [Online]. Available: https://www.idquantique.com/id-quantique-expands-the-xg-series-with-the-launch-of-the-clavis-xg/. [Accessed 08 02 2024].

[44] IDQ, "Clavis XG QKD System," [Online]. Available: https://www.idquantique.com/quantum-safe-security/products/clavis-xg-qkd-system/. [Accessed 08 02 2024].

[45] IDQ, "ID Quantique unveils its 4th generation of Quantum Key Distribution (QKD): the Cerberis XG, the ultimate in quantum-safe security," 17 05 2021. [Online]. Available: https://www.idquantique.com/id-quantique-unveils-its-4th-generation-of-quantum-key-distribution-qkd-the-cerberis-xg-the-ultimate-in-quantum-safe-security/. [Accessed 08 02 2024].

[46] IDQ, "Cerberis XG QKD System," [Online]. Available: https://www.idquantique.com/quantum-safe-security/products/cerberis-xg-qkd-system/. [Accessed 08 02 2024].

[47] ThinkQuantum, "History," [Online]. Available: https://www.thinkquantum.com/projects/. [Accessed 08 02 2024].

[48] JUNIPER, "Integrating Quantum-Safe Security with existing encryption solutions," 2022. [Online]. Available: https://www.idquantique.com/quantum-safe-security/integrated-solutions/. [Accessed 09 02 2024].

[49] J. Cho et al., "Using QKD in MACsec for secure Ethernet networks," *IET Quant. Comm.,* 2021.

[50] JUNIPER, "DAY ONE: QUANTUM-SAFE IPSEC VPNS," 2023. [Online]. Available: https://www.juniper.net/documentation/jnbooks/us/en/day-one-books. [Accessed 09 02 2024].

[51] C. Garcia et al., "Quantum-resistant Transport Layer Security," *Computer Communications,* 2024.

[52] ANSSI, BSI, NLNCSA and Swedish Armed Forces, "Position Paper on Quantum Key Distribution," 26 01 2024. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Quantum_Positionspapier.html. [Accessed 08 02 2024].

[53] NSA, "Quantum Key Distribution (QKD) and Quantum Cryptography (QC)," [Online]. Available: https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/. [Accessed 08 02 2024].

[54] E. Dubrova et al., "Breaking a Fifth-Order Masked Implementation of CRYSTALS-Kyber by Copy-Paste," in *ASIA CCS '23: ACM ASIA Conference on Computer and Communications Security*, 2022.