Funktionsweise und Sicherheit von Netzwerken zum Quantenschlüsselaustausch

Sicherheit von IT-Systemen

Jan Zimmer

Sommersemester 2021

Inhaltsverzeichnis

1. Einleitung

Eine der wichtigsten Funktionen kryptographischer Protokolle besteht in der Vereinbarung gemeinsamer Sitzungsschlüssel zwischen Kommunikationspartnern (Carle 2003, 4).

Ein solcher Schlüssel stellt eine geheime Information in Form eines Kennworts oder, wie bei kontemporären, computergestützten, symmetrischen und asymmetrischen Verfahren üblich, einer Bitfolge dar und dient als Parameter für kryptographische Algorithmen zur Ver- und Entschlüsselung von Texten oder Nachrichten.

Um das Problem der Verteilung von Schlüsseln zu lösen, existieren verschiedene Schlüsselaustauschprotokolle, darunter auch der 1976 von Whitfield Diffie und Martin Hellman entwickelte gleichnamige Schlüsselaustausch, der in vielen Protokollen wie TLS, IPsec und SSH Anwendung findet (Lake 2021).

Eine besondere Form des Schlüsselaustausches, der auf den Prinzipien der Quantenmechanik beruht und den Aufbau spezieller Netzwerke erfordert, ist der Quantenschlüsselaustausch (engl.: Quantum key distribution), im Folgenden auch als QKD abgekürzt.

Diese Arbeit soll die Funktion von Netzen zum Quantenschlüsselaustausch, insbesondere anhand des BB84-Protokolls, erläutern und einen Überblick über ihre besonderen, sicherheitstechnischen Vor- und Nachteile verschaffen.

2. Grundlagen des Quantenschlüsselaustausch

2.1 Grundlagen und geschichtliche Hintergründe

Durch die Bezeichnung „Quantenschlüsselaustausch“ bzw. „distribution“ kann der Eindruck entstehen, dass lediglich bereits vorhandene Informationen an die Kommunikationspartner eines solchen QKD-Netzwerks weitergeleitet werden. Tatsächlich dient aber das Protokoll selbst zur Generierung eines zufälligen Schlüssels.
Es werden außerdem ausschließlich Schlüssel übertragen; Quantenschlüsselaustausch dient nicht zur Übertragung von Nachrichten.

Die Anfänge dieser Technologie finden sich bereits in einem 1983 von Stephen Wiesner veröffentlichten Paper mit dem Titel „Conjugate coding“, in dem er die Verwendung von konjugierten Quantenzuständen zur Codierung vorschlägt (Wiesner 1983).

Wiesner leistet darin einige der bedeutendsten Beiträge zur Quanteninformationstheorie und beschreibt darin unter anderem unfälschbare „Quanten-Banknoten“ (Satell 2016) und „Quanten-Multiplexing“.

Ein Konzept für das erste quanten-basierte QKD-Protokoll, genannt BB84, wurde 1984 von Charles Bennett und Gilles Brassard entwickelt und dient seitdem als Grundlage für entsprechende Forschungen (Cyril Branciard 2005).

QKD-Protokolle nutzen zur Kodierung ihrer Informationen sogenannte Quantenbits (auch Qubits), im Gegensatz zu den Bits der klassischen Informationstheorie.
Das Qubit ist ein Zwei-Zustands-System der Quantenmechanik und die grundlegende Einheit der Quanteninformation.
In der Regel dient ein Photon als ein solches System. Im Fall von BB84 werden einzelne Photonen angenommen. Protokolle wie das 1991 von Artur Ekert erdachte E91 nutzen allerdings auch Photonen-Paare.

Die Eigenschaft des Photons, die dabei zur Kodierung genutzt wird, ist seine Polarität. Photonen können vom Sender in eine bestimmte Polarität gebracht und vom Empfänger gemessen werden.
Zur Übertragung der polarisierten Photonen kann ein optisches Medium wie etwa ein Lichtwellenleiter aber auch freier Raum dienen.

2.2 Anwendungsfälle

Durch die Nutzung von Qubits als Informationsträger ergeben sich für die Nutzer eines solchen Netzwerks einige einzigartige Vorteile.

Während asymmetrische Kryptosysteme und Public-Key-Verfahren sich auf die Rechenintensität der Umkehrung von Einwegfunktionen stützen, sind die Folgenlosigkeit (Perfect Forward Secrecy) und informationstheoretische Sicherheit von QKD-Verfahren beweisbar (Peter W. Shor 2000).

2.2.1 Abhörsicherheit und Abhördetektion

Da das Messen von Quantenzuständen diese generell verändert, ist es Sender und Empfänger möglich, eventuelle Abhörversuche durch Dritte zu detektieren und festzustellen,

welche Menge an Informationen abgefangen wurde, wenn sie ihre eigenen Messergebnisse vergleichen (Brassard 1984). Diese besondere Eigenschaft von Quantensystemen ist auch unter dem Begriff des „Messproblems“ (engl.: Measurement problem) bekannt.
Wird ein solcher Eingriff festgestellt, kann die Kommunikation abgebrochen werden und ein neuer Versuch zur Schlüsselgenerierung gestartet werden.

2.2.2 QKD in Verbindung mit One-Time-Pad

Eine sinnvolle Anwendung von QKD ist die Verwendung in Kombination mit dem One-Time-Pad (OTP) oder Einmalverschlüsselungsverfahren.

OTP bietet bei bestimmungsgemäßer Verwendung eine nachweislich perfekte Sicherheit (Nokia Bell Labs 1949). Voraussetzung dafür sind:

- Der Schlüssel muss zufällig sein.
- Die Länge des Schlüssels muss größer/gleich der Länge der zu chiffrierenden Nachricht sein.
- Der Schlüssel darf weder ganz noch in Teilen wiederverwendet werden.
- Der Schlüssel muss geheim sein.

Mit QKD können leicht (bestehendes Netzwerk vorausgesetzt) zufällige Schlüssel variabler Länge generiert werden, sodass sich eine Verwendung von OTP auch bei längeren Nachrichten anbietet (Alain Aspect 2017).

2.3 Quantenmechanische Grundlagen von QKD Netzwerken

QKD-Protokolle wie BB84 und E91 machen sich die quantenmechanischen Eigenschaften von Elementarteilchen zu nutze. Namentlich spielen das Superpositionsprinzip, das No-Cloning-Theorem und die Quantenverschränkung bei diesen Verfahren eine Rolle.

2.3.1 Superpositions- und Unschärfeprinzip

Das Superpositionsprinzip der Quantenmechanik besagt, dass zwei oder mehr Quantenzustände (ähnlich wie Wellen in der klassischen Physik) sich „überlagern“ können und dann einen weiteren validen Quantenzustand bilden.

Im Gegensatz zum Bit, dass entweder 0 oder 1 ist, kann sich Qubit deshalb auch in einer Superposition beider Zustände befinden. Die Wahrscheinlichkeit, bei einem gegebenen Qubit einen Zustand zu messen, der logisch zu 0 oder 1 codiert, ist deshalb in der Regel weder P=0.0 noch P=1.0.

Der Polarisierungszustand von Photonen kann in Form von drei Basen beschrieben werden, die jeweils zwei mögliche, zueinander orthogonale Zustände und eine Superposition aus beiden Zuständen erlauben.

- Lineare Basis (horizontal/vertikal bzw. 90°/0°)
- Zirkulare Basis (links/rechts)
- Elliptische Basis (135°/45°)

Soll die Polarität eines Photons gemessen werden, um daraus ein Bit zu „extrahieren“, muss eine der drei Basen (und damit ein entsprechend polarisierter optischer Filter) für den Messvorgang gewählt werden.

In der Praxis werden zum Erzeugen und Messen von bestimmten Polarisierungen Prismen in Kombination mit Lasern verwendet.

Entsprechende Filter gibt es als natürliches Vorkommen in Form von doppelt-brechenden Kristallen (z.B. Kalzit). Aus solchen Materialien können Wollaston-Prismen hergestellt werden, die den gewünschten Filtereffekt herbeiführen (American Meteorological Society 2012).

Zeitgenössische Implementierungen verwenden für diesen Zweck synthetisch hergestellte Strahlteiler (Alain Aspect 2017).

2.3.2 No-Cloning-Theorem

Das No-Cloning-Theorem bildet die Grundlage der Quantenkryptograpie. Es besagt, dass es unmöglich ist, eine absolut identische, unabhängige Kopie eines beliebigen unbekannten Quantenzustands zu erschaffen.
Eine Informationsübertragung kodiert in Qubits kann nicht abgehört werden, ohne die ursprüngliche Information zu verändern, da ein Abhören zwangläufig ein Kopieren der übertragenen Qubits erfordert (Brassard 1984).

2.3.3 Quantenverschränkung

Zur Implementierung des E91-Protokolls müssen verschränkte Paare von Photonen erzeugt werden. Von Quantenverschränkung ist die Rede, wenn der Quantenzustand eines Teilchens nicht unabhängig vom Quantenzustand eines oder mehrerer anderer Teilchen beschrieben werden kann, das System als ganzes aber trotzdem einen wohldefinierten Zustand hat. Räumliche Distanz zwischen verschränkten Teilchen spielt dabei keine Rolle.

Das Phänomen Quantenverschränkung und seine scheinbare Unvereinbarkeit mit dem Lokalitätsprinzip der klassischen Physik ist auch unter dem von Einstein geprägten Begriff der „spukhaften Fernwirkung“ bekannt.

Quantenverschränkung von Photonen kann durch die Verwendung entsprechender optischer Dämpfungsglieder gezielt herbeigeführt werden.

3. QKD Protokolle

Im Allgemeinen kann zwischen zwei Kategorien von QKD-Protokollen unterschieden werden, je nachdem welches Prinzip der Quantenmechanik sie sich zu Nutzen machen:

- Vorbereiten-und-Messen (engl.: Prepare-and-Measure)
- Verschränkungs-basiert (engl.: Entanglement-based)

Beide Ansätze können außerdem diskrete oder kontinuierliche Variablen verwenden. Praktische Implementierungen von QKD arbeiten allerdings meist mit diskreten Variablen.

Continous variable quantum key distribution (CV-QKD) ist aufgrund der Kompatibilität mit existierender Telekommunikationsinfrastruktur allerdings eine vielversprechende Technologie, an deren Ausarbeitung bereits gearbeitet wird (Fabian Laudenbach 2017).

3.1 Typischer Ablauf

Ungeachtet des Verfahrens lässt sich der Ablauf eines Quantenschlüsselaustausch allerdings in einigen Schritten verallgemeinern:

- Erzeugung und Übertragung von Qubits
- Messvorgang
- Schlüsselabgleich (engl.: reconciliation)
- Privacy Amplification

Gemäß Konvention werden im folgenden Beispiel der Sender als „Alice“, der Empfänger als „Bob“ und der unberechtigte Mithörer als „Eve“ bezeichnet.

3.2 BB84-Protokoll mit Beispielübertragung

3.2.1 Erzeugung und Übertragung der Qubits

Bevor mit der Übertragung begonnen wird, benötigen Alice und Bob zunächst einen klassischen, authentifizierten Kommunikationskanal zusätzlich zu ihrem Quantenkanal, z.B. über das Internet.

Anschließend einigt sich Alice zusammen mit Bob auf zwei für das Protokoll zu verwendende Basen (linear, zirkular oder elliptisch). Sie bestimmt außerdem eine zufällig ausgewählte Bitfolge, die als Grundlage für den später erzeugten Schlüssel dienen wird.
Jeweils zwei zueinander nicht-orthogonale, konjugierte Zustände aus beiden Basen codieren zu 0 und 1.
Entscheidet sich Alice also für die Basen „linear“ und „elliptisch“, so kann sie festlegen, dass 90° und 135° „0“ und, dass 0° und 45° „1“ codieren.

Beginnend mit dem ersten Bit übersetzt Alice jetzt die gewählte Bitfolge in entsprechend polarisierte Photonen, wobei sie bei jedem Polarisierungsvorgang zufällig eine Basis wählt (P=0.5).
Beim Codieren einer 0 mit der zufällig gewählten Basis „elliptisch“, muss Alice also ein Photon mit einer Polarität von 135° erzeugen.

Dieser Vorgang wird solange wiederholt, bis Alice die gesamte in Form von Photonen bzw. Qubits codierte Bitfolge über den Quantenkanal an Bob gesendet hat. Alice zeichnet dabei

für jedes verschickte Photon den Zeitstempel, die Polarität und die gewählte Basis auf. Diese Aufzeichnung wird sie später mit Bobs vergleichen, um den Schlüsselabgleich durchzuführen.

3.2.2 Messvorgang

Beim Empfangen eines Photons wählt Bob ebenfalls zufällig eine Basis für seinen Filter aus.

Entscheidet er sich für die gleiche Basis, wie die, die Alice beim Erzeugen ihres Qubits verwendet hat, so wird er die Polarität des Photons korrekt messen können.

Wählt Bob allerdings eine sich unterscheidende Basis, so wird er sich mit P=0.5 entweder eine 0 oder 1 notieren. Obwohl er eine andere Basis zum Messen gewählt hat, als Alice zum Erzeugen, wird Bob zufällig einen der zwei Zustände als Ergebnis erhalten, die zu seiner Basis passen. Nachdem er eine solche Messung durchgeführt hat, ändert sich der Polarität des Photons gemäß der gewählten Basis und jede Information über den vorherigen Zustand geht unwiderruflich verloren (Brassard 1984).
Solche „falsch“ gemessenen Bits werden im nächsten Schritt, dem Abgleich, wieder verworfen.
Das Unschärfeprinzip der Quantenmechanik besagt dabei, dass es keine einzige mögliche Messung gibt, die mit Sicherheit alle vier möglichen Zustände unterscheiden kann.

Auch Bob zeichnet für jede Messung den entsprechenden Zeitstempel, die Polarität und die gewählte Basis auf.

3.2.3 Schlüsselabgleich

Für den Schlüsselabgleich (engl.: reconciliation) wird erneut der authentifizierte Kommunikationskanal verwendet.

Alice und Bob vergleichen nun ihre gewählten Basen. Stimmen die Basen überein, so stimmen auch die zugehörigen Bits überein und können für den gemeinsamen Schlüssel verwendet werden. Alle anderen Bits (im Schnitt 1/2 der Gesamtmenge) können verworfen werden.

Die folgenden Tabellen zeigen einen beispielhaften Ausschnitt eines BB84-Schlüsselaustausch. Alices Anteil ist rot hinterlegt, Bobs Anteil grün. Eine lineare Basis wird durch „+“ gekennzeichnet, eine elliptische durch „x“.

Tabelle 1 - Codierung

Basis	0	1
Elliptisch (x)	135°	45°
Linear (+)	90°	0°

Tabelle 2 - Schlüsselaustausch

Bitfolge von Alice	0	0	1	0	1	0	1
Basis von Alice	x	+	+	+	x	+	x
Polarität des Photons	135°	90°	0°	90°	45°	90°	45°
Basis von Bob	x	x	+	x	x	+	x
Gemessene Polarität	135°	45°	0°	135°	45°	90°	45°
Gemessene Bitfolge	0	1	1	0	1	0	1
Schlüssel	**0**		**1**		**1**	**0**	**1**

Um herauszufinden, ob sie durch Eve belauscht wurden, opfern Alice und Bob eine zuvor vereinbarte Teilzeichenfolge ihres Bit-Schlüssels und vergleichen diesen über den authentifizierten Kanal.

In dem Fall, dass Eve den Quantenkanal abgehört hat, ist mit einer Fehlerrate von 0.5*0.5=0.25 zu rechnen, da Eve in der Hälfte aller Fälle die falsche Basis zum Belauschen wählt und Bob beim Messen eines belauschten Qubits mit der *korrekten* Basis nur mit P=0.5 den richtigen Zustand misst.

Die Wahrscheinlichkeit, dass Bob und Alice einen solchen Lauschangriff durch Eve bemerken, wenn sie *n* Bit ihres Schlüssels zum Vergleichen opfern, beträgt also *P=1-(3/4)^n*.

Um einen Lauschangriff, der die gesamte Übertragung abgehört hat, mit P=0.9999999899 zu entdecken, müssen Alice und Bob also einen Vergleich von 64 Bit einplanen.

Der folgende Schlüsselaustausch zeigt die Folgen eines Abfangens einzelner Qubits durch Eve:

Bitfolge von Alice	0	0	1	0	1	0	1
Basis von Alice	x	+	+	+	x	+	x
Polarität des Photons	135°	90°	0°	90°	45°	90°	45°
Basis von Eve	x	x	+	x	+	+	+
Von Eve gemessen & weitergeleitet	135°	45°	0°	45°	90°	90°	0°
Basis von Bob	x	x	+	x	x	+	x
Gemessene Polarität	135°	45°	0°	45°	135°	90°	45°
Gemessene Bitfolge	0	1	1	1	0	0	1
Schlüssel	**0**		**1**		**1**	**0**	**1**
Fehler vorhanden	**nein**		**nein**		**ja**	**nein**	**nein**

Bits 1,3 und 6 wurden von Eve erfolgreich abgehört, ohne Spuren zu hinterlassen, da seine und Alices Basen übereinstimmen.
Bit 5 wurde von Eve mit der falschen Basis gemessen und zeigt, wie sich der eingeführte Fehler auf Bobs Messung fortpflanzt.
Bit 7 wurde von Eve mit der falschen Basis gemessen und demonstriert, dass ein einzelner Messfehler nicht zwangsläufig beim Vergleich sichtbar wird.

Bei einem Vergleich der letzten 3 Bit würden Alice und Bob allerdings den Fehler im 5. Bit finden. Er stellt ein Indiz für Eves Angriff auf ihre Kommunikation dar, da Alice und Bob die gleichen Basen gewählt haben.

Sollte Eve nur jedes 2. Qubit abhören, so veringert sich die zu erwartende Fehlerrate um den Faktor 0.5. Dadurch können Alice und Bob anhand der gemessenen Fehlerrate abschätzen, wie viele Informationen Eve über ihren Schlüssel in Erfahrung bringen konnte.

Fehler können allerdings nicht nur durch Lauschangriffe, sondern auch durch störende Umgebungsfaktoren wie falsch kalibrierte Sender und Empfänger oder fehlerhafte Leitungen hervorgerufen werden. Da es unmöglich ist, sicher zwischen Fehlerursachen zu unterscheiden, wird in der Praxis eine Fehlerschwelle von *n* Bits festgelegt, bis zu deren Erreichen die Schlüsselgenerierung nicht abgebrochen wird.
Dabei wird *n* so gewählt, dass die geringe Menge an Teilinformationen, über die ein Dritter möglicherweise verfügt, im nächsten Schritt eliminiert werden kann.

3.2.4 Privacy Amplification

Durch Privacy Amplification (PA) können Alice und Bob ihr Wissen über die Fehlerrate nutzen, um das Risiko eines teilweise abgehörten Schlüssels praktisch auf null zu reduzieren.

Dazu dient die restliche Bitfolge als Input eine zufällig ausgewählten, universellen Hashfunktion, welche den finalen Schlüssel auf eine bestimmte Länge kürzt.
Wie stark die Hashfunktion den Schlüssel dabei reduziert, kann anhand der errechneten Fehlerrate, die als Maß für Eves Teilinformationen über den Schlüssel dient, festgelegt werden.

Aufgrund der Länge der generierten Schlüssel, und damit der Länge des Inputs, ist es sinnvoll, QKD-optimierte PA-Algorithmen, zum Beispiel auf Basis schneller Fourier-Transformationen, zu verwenden (Tang 2019).

3.3 Alternative Protokolle

Neben BB84 existieren noch weitere Protokolle, die einen Quantenschlüsselaustausch beschreiben. Einige der wichtigsten sollen an dieser Stelle kurz Erwähnung finden:

Decoy State BB84 ist ein Abkömmling des BB84-Protokolls, der entwickelt wurde, um Angriffe durch Photonen-Trennung (engl.: Photon number splitting) abzuwehren. Dazu versendet Alice ihre Photonen mit unterschiedlicher Intensität, die später mit Bobs Ergebnissen verglichen werden (Hwang 2003).

SARG04 wurde für die Verwendung mit stark gedämpften Pulslasern entwickelt und verwendet eine alternative Codierung (Valerio Scarani 2004).

E91 verwendet im Gegensatz zu den zuvor genannten Protokollen verschränkte Photonen-Paare zur Übertragung (Ekert 1991).

4. Praktische Implementierungen von QKD-Netzwerken

Eine der ersten nicht-experimentellen Implementierungen eines QKD-Netzwerks war das Quantum Network der „Defense Advanced Research Projects Agency“ (DARPA), einer Behörde des US-amerikanischen Verteidigungsministeriums.

Seine Entwicklung begann 2002 durch BBN Technologies. 2004 war das Netz einsatzbereit und verband über bis dahin ungenutzte Glasfaserkabel unter der Metropolregion Boston-Cambridge-Quincy die Campus der Boston und Harvard University (Elliott 2005).

Das Netzwerk nutzte 5MHz Decoy State BB84 mit ständiger Verfügbarkeit und unterstützte zum Zeitpunkt seiner Abschaltung 2007 bis zu 10 Knotenpunkte.

2004 begannen auch die Vorarbeiten für das von der Europäischen Union geförderte Projekt „Secure Communiaction based on Quantum Cryptography“ (SECOQC).

Das Netzwerk wurde 2008 offiziell gestartet und verbindet sechs „Trusted Private Networks“ in Wien und Umgebung über einen Quantum Backbone bestehend aus 200 Kilometer handelsüblicher Glasfaserleitung (Pease 2008).

Kurz davor wurde im Rahmen der 2007 Schweizer Parlamentswahlen eine von der Firma ID Quantique entwickelte Verbindung zum Quantenschlüsselaustausch genutzt, um Daten aus einem der dezentralen Wahlbüros für den Versand nach Bern zu verschlüsseln (Ziegler 2007).

Eine Vorreiterrolle in der praktischen Umsetzung von QKD kommt China zu. Dort wurde unter der Leitung von Jian-Wei Pan von der Heifei University of Technology mit Partnern aus der Industrie und akademischen Welt ein landesweites Netzwerk aufgebaut, das 4 Quantennetzwerke in Metropolen im Osten und Westen Chinas miteinander verbindet. Das Netzwerk umfasst 2000 Kilometer lange Glasfaserverbindungen zwischen Shanghai, Hefei, Jinan und Beijing, sowie eine 2600 Kilometer Satelliten-Verbindung über den ersten quantenkryptografie-fähigen Satelliten „Micius“ (Johnston 2021).

Die bisher entwickelten, kommerziell erhältlichen QKD-Systeme richten sich zumeist an Regierungen oder Unternehmen mit sehr hohen Sicherheitsanforderungen. Dort werden sie in der Regel als Alternative zur Schlüsselübertragung durch Kuriere genutzt.

Ihr Hauptvorteil liegt gegenüber Kurieren besteht in der Möglichkeit, ein Abfangen der Schlüsselinformationen messen und erkennen zu können.
Den hohen Anschaffungskosten eines QKD-Netzes stehen geringere Betriebskosten und höhere Zuverlässigkeit als einem sicheren Kurierdienst gegenüber.

5. Angriffsvektoren und Schutzmaßnahmen

Es existieren eine Reihe möglicher Angriffsstrategien, die nicht auf der oben beschriebenen „Abfangen-und-Weiterleiten“ Taktik basieren, darunter traditionelle Techniken wie Man-in-the-Middle (MITM) und Denial-of-Service (DoS), aber auch QKD-spezifische Seitenkanalangriffe wie Photonen-Trennung (engl.: Photon splitting) und Detektorblendung oder Analyse von Reflektionen.

5.1 Photonen-Trennung

Zur Implementierung von Protokollen wie BB84, die bei der Übertragung von einzelnen Photonen ausgehen, werden in der Praxis meist stark gedämpfte Pulslaser verwendet. Ein einzelner Puls enthält im Schnitt weniger als ein Photon. Die Verteilung der Photonen folgt der Poisson-Verteilung. In den meisten Fällen wird kein Puls ausgesandt (da keine Photonen ausgehen), in einigen Fällen wird ein Puls mit einem einzigen Photon ausgesandt und in den restlichen Fällen enthält ein Puls zwei oder mehr Photonen.

Eve kann in einem solchen Fall die überschüssigen Protonen abfangen und in einem Speicher für Quanteninformation (Wang 2019) lagern. Sobald Alice und Bob über den klassischen Kommunikationskanal ihren Schlüsselabgleich beginnen, kann Eve die korrekten Basen in Erfahrung bringen und die abgefangen Photonen nachträglich messen, um Teilinformationen über den Schlüssel zu erlangen.

Eine mögliche Abhilfe ist die Verwendung des SARG04-Protokolls, welches resistenter gegen Photonen-Trennungs-Angriffe ist oder der Einsatz von Decoy states.

Die Verwendung einer „echten“ Quelle einzelner Photonen (engl.: Quantum dot source) bietet immunität gegen derartige Angriffe (P. M. Intallura 2007).

5.2 Man-in-the-Middle

Sollten Alice und Bob auf Authentifizierung bei der Nutzung ihres Quantenkanals verzichten, machen sie sich anfällig für einen MITM-Angriff, bei dem Eve sich gegenüber Alice als Bob und gegenüber Bob als Alice ausgibt. Eve generiert so zwei Schlüssel (jeweils einen für seine Kommunikation mit Bob und Alice) und kann sich bei einem zukünftigem Austausch verschlüsselter Nachrichten zwischenschalten.

5.3 Denial-of-Service

Da die Übertragung von Photonen einen Lichtwellenleiter oder Sichtkontakt zwischen Sender und Detektor voraussetzt, kann das entsprechende Medium durchtrennt oder Blockiert werden.

Versuchte Lauschangriffe führen bei ihrer Detektierung ebenfalls dazu, dass die Verbindung für Alice und Bob unbrauchbar wird.

Abhilfe schafft die Erstellung redundanter Verbindung im QKD-Netzwerk, auf die im Falle von Störungen ausgewichen werden kann.

5.4 Trojanisches Pferd

Ein Trojanisches-Pferd-Angriff, ursprünglisch auch unter der Bezeichnung „large pulse attack“ bekannt, ist effektiv gegen Protokolle wie SARG04, bei denen die von Bob gewählten

Basen aufgrund ihrer Relevanz für die Codierung geheim gehalten werden müssen (Artem Vakhitov 2001).

Dabei bestrahlt Eve Bobs Detektor mit einem hellen Pulslaser. Eine Analyse der Reflektion kann dann Informationen über die von Bob gewählte Messbasis preisgeben.

Diese Form von Angriff wurde in Tests bereits erfolgreich gegen das komnerziell erhältliche QKD-System Clavis2 eingesetzt (Sajeed 2017).

Im Falle von BB84 ist Bobs Messbasis allein keine für Eve interessante Information. Ein Trojanisches Pferd kann aber möglicherweise mit anderen Angriffsarten kombiniert werden, um das Kryptosystem zu brechen (Sajeed 2017).

5.5 Detektorblendung

Eine weitere Form von Angriff, der auf Schwachstellen in der Konstruktion des Detektors abzielt, besteht darin, diesen durch kontinuierliches Bestrahlen mit einem Laser zu blenden. Dieses Bestrahlen macht den Detektor zum Messen von Quantenzuständen unbrauchbar – er fungiert aber weiterhin als klassischer Detektor, der Bob einen Bitwert anzeigt (Lydersen 2010).

Eve kann damit den Quantenaspekt von Bobs Detektor aushebeln und seine gemessenen Bitwerte über einen Laser fernsteuern. Jedes mal, wenn Eve eines von Alices Photonen misst und den Wert „1“ erhält, kann er Bobs Empfänger bestrahlen. Dieser misst dann ebenfalls den Bitwert „1“. Eve kann so Informationen über den Schlüssel erlangen und trotzdem unentdeckt bleiben.

5.6 Stimulierte Emission

Es existieren theoretische Überlegungen zu einem Angriff, wonach Eve mittels eines optischen Verstärkers quantenmechanische Kopien (inklusive ihrer Polarität) von Alices Photonen erzeugen könnte.

Eine optischer Verstärker funktioniert nach dem Prinzip der stimulierten Emission. Trifft ein Photon mit der richtigen Energie auf ein angeregtes Atom und erlaubt diesem in einen Zustand niedrigerer Energie zu wechseln, so strahlt das Atom ein zweites Photon ab, das unter anderem die gleiche Polarität wie das einfallende Photon aufweist.

Mit der gleichen Wahrscheinlichkeit, mit der eine solche stimulierte Emission eintritt, kommt es allerdings auch zu einer *spontanen* Emission, die in einem Photon resultiert, das vollkommen unabhängig vom einfallend Photon ist und eine zufällige Polarität besitzt (Wootters 1982).

6. Fazit und Zukunftsausblick

Netzwerke zum Quantenschlüsselaustausch bieten durch die Möglichkeit, Abhörversuche in Form einer Fehlerrate sichtbar zu machen, einen in der Kryptographie einzigartigen Vorteil.

Durch die vielerorts bereits vorhandene Infrastruktur an Lichtwellenleitern, vor allem in Ballungsgebieten, wäre eine breite Annahme der Technologie theoretisch möglich.

In der Praxis stehen der Implementierung von QKD-Netzwerken allerdings zahlreiche Hindernisse im Weg. Die benötigte Ausrüstung zum Aufbau von Knotenpunkten ist kostspielig und reagiert sensibel auf Störungen.

Die Tatsache, das fast alle Ansätze zum Quantenschlüsselaustausch bereits einen authentifizierten Kommunikationskanal - in der Regel über das Internet - erfordern, setzt bereits einen Austausch von symmetrischen Schlüsseln voraus. Auch gibt es derzeit keinen Grund zur Annahme, dass bereits existierende, etablierte Schlüsselaustauschprotokolle (wie etwa der Diffie-Hellman-Schlüsselaustausch) keine hinreichende Sicherheit bieten.

Der US-amerikanische Experte für Kryptographie und Computersicherheit, Bruce Schneier, ging sogar so weit, Quantenkryptographie als „sinnlos“ zu bezeichnen (Schneier 2008).

Wie die Arbeit von Vadim Makarov, Leiter des Moskauer Quantum Hacking Lab, zeigt, weist die nötige Hardware zur Umsetzung von QKD-Netzwerken derzeit noch viel Angriffsfläche für Seitenkanalangriffe auf (Quantum Hacking Lab 2020).

Auch der derzeitige Mangel an Standardisierung steht einer weiteren Verbreitung der Technologie im Wege.

Bis die Technik hinter QKD weiter ausgereift ist, oder die Bedrohung der heutigen kryptografischen Algorithmen und Protokolle durch Quantencomputer zunimmt, ist also damit zu rechnen, dass Quantenschlüsselaustausch ein Nischendasein fristen wird.

7. Glossar

Kryptographisches Protokoll
Sicherheitsbezogene Kommunikationsregeln, die eine oder mehrere Funktionen wie Schlüsselerzeugung, Schlüsselverteilung, Authentifizierung und/oder Verschlüsselung erfüllen

Kryptographischer Schlüssel
Geheime Information, die als Parameter für die zur Verschlüsselung von Nachrichten eingesetzten Algorithmen dient. Kommte eine symmetrische Verschlüsselung zum Einsatz, dient sie auch gleichzeitig zum Entschlüsseln.

Sitzungsschlüssel
Kurzlebiger symmetrischer Schlüssel für die Dauer einer Sitzung

Quantenschlüsselaustausch
Vorgang zur Generierung und Verteilung kryptographischer (Sitzungs-)Schlüssel, bei dem Quantensysteme als Informationsträger dienen

Qubit
Zwei-Zustands-Quanten-System, grundlegende Einheit der Quanteninformation

Photon
Elementarteilchen, das als Energieträger der elektromagnetischen Strahlung fungiert und eine messbare Polarität besitzt

Perfect Forward Secrecy
Fähigkeit eines Schlüsselaustauschprotokolls, einen nicht rekunstruierbaren Sitzungsschlüssel zu erzeugen

(Mess-)Basis
Polarität des optischen Filters der, zusammen mit einem Laser, zum Erzeugen und danach auch zum Messen von Qubits (Photonen) eingesetzt wird

Privacy Amplification
Reduzieren eines Schlüssels auf eine bestimmte Länge mittels Hashfunktionen

Emission
Spontane oder stimulierte Abgabe eines Photons durch ein Atom in einem höheren Energiezustand

7.1 Abkürzungen und Akronyme

QKD Quantum key distribution

CV Continuous variable

PA Privacy amplification

MITM Man-in-the-Middle

DoS Denial-of-Service

8. Quellen

Alain Aspect, Michel Brune, École Polytechnique. 2017. *coursera.org.* November 8. Accessed April 15, 2021. https://www.coursera.org/learn/quantum-optics-single-photon/.

American Meteorological Society. 2012. *Glossarey of Meteorology.* Januar 26. Accessed April 15, 2021. https://glossary.ametsoc.org/wiki/Wollaston_prism.

Artem Vakhitov, Vadim Makarov et. al. 2001. "Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography." *Journal of Modern Optics.*

Brassard, Charles H. Bennett und Gilles. 1984. "Quantum cryptography: Public key distribution and coin tossing." *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* 8.

Carle, Prof. Dr.-Ing. Georg. 2003. *ccs-labs.org.* Accessed April 15, 2021. https://web.archive.org/web/20190627222426/http://www.ccs-labs.org/~dressler/teaching/netzsicherheit-ws0304/07_CryptoProtocols_2on1.pdf.

Cyril Branciard, Nicolas Gisin, Barbara Kraus, Valerio Scarani. 2005. "Security of two quantum cryptography protocols using the same four qubit states." *Physical Review A.*

Ekert, Artur K. 1991. "Quantum cryptography based on Bell's theorem." *Physical Review Letters.*

Elliott, Chip. 2005. "The Darpa Quantum Network." *researchgate.net.* Januar. Accessed April 16, 2021. https://www.researchgate.net/publication/2194325_The_DARPA_Quantum_Network.

Fabian Laudenbach, Christoph Pacher, Chi-Hang Fred Fung et al. 2017. "Continuous-Variable Quantum Key Distribution with Gaussian Modulation -- The Theory of Practical Implementations." *Advanced Quantum Technologies* 2.

Hwang, Won-Young. 2003. "Quantum Key Distribution with High Loss: Toward Global Secure Communication." *Physical Review Letters.*

Johnston, Hamish. 2021. *physicsworld.com.* Januar 07. Accessed April 16, 2021. https://physicsworld.com/a/quantum-cryptography-network-spans-4600-km-in-china/.

Lake, Josh. 2021. *What is the Diffie–Hellman key exchange and how does it work?* März 23. Accessed April 15, 2021. https://www.comparitech.com/blog/information-security/diffie-hellman-key-exchange/.

Lydersen, L., Wiechers, C., Wittmann, C. et al. 2010. "Hacking commercial quantum cryptography systems by tailored bright illumination." *Nature Photon* 686–689.

Nokia Bell Labs. 1949. "Communication theory of secrecy systems." *The Bell System Technical Journal* 656-715.

P. M. Intallura, M. B. Ward et. al. 2007. "Quantum key distribution using a triggered quantum dot source emitting near 1.3µm." *Applied Physics Letters.*

Pease, Roland. 2008. *news.bbc.co.uk.* Oktober 9. Accessed April 16, 2021. http://news.bbc.co.uk/2/hi/science/nature/7661311.stm.

Peter W. Shor, John Preskill. 2000. "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol." *Physical Review Letters* 441.

Quantum Hacking Lab. 2020. *vad1.com.* März 15. Accessed April 16, 2021. http://www.vad1.com/lab/publications.html.

Sajeed, S., Minshull, C., Jain, N. et al. 2017. "Invisible Trojan-horse attack." *Scientific Reports.*

Satell, Greg. 2016. *forbes.com.* Juli 10. Accessed April 15, 2021. https://www.forbes.com/sites/gregsatell/2016/07/10/the-very-strange-and-fascinating-ideas-behind-ibms-quantum-computer/.

Schneier, Bruce. 2008. *schneier.com.* Oktober 16. Accessed April 16, 2021. https://www.schneier.com/essays/archives/2008/10/quantum_cryptography.html.

Tang, BY., Liu, B., Zhai, YP. et al. 2019. "High-speed and Large-scale Privacy Amplification Scheme for Quantum Key Distribution." *Scientific Reports* 9.

Valerio Scarani, Antonio Acín, Grégoire Ribordy und Nicolas Gisin. 2004. "Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations." *Physical Review Letters.*

Wang, Y., Li, J., Zhang, S. et al. 2019. "Efficient quantum memory for single-photon polarization qubits." *Nature Photonics* 346–351.

Wiesner, Stephen. 1983. "Conjugate coding." *Sigact News* 1.

Wootters, W., Zurek, W. 1982. "A single quantum cannot be cloned." *Nature* 802–803.

Ziegler, Elke. 2007. *orf.at.* Oktober 16. Accessed April 16, 2021. https://sciencev1.orf.at/science/news/149797.html.