Fernuniversität Hagen

Fakultät für Mathematik und Informatik

Quantenkryptografie

Seminar 01909 IT-Sicherheit

Roland Szypula
Matrikelnummer: 9774629

Betreuung:
PD Dr.-Ing. habil. Mario Kubek

1. März 2020

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Kapitel 1

Einleitung

Über *Quantencomputer* wird in den Medien oft berichtet. Man sagt sie würden sich von klassischen Computern deutlich unterscheiden. Und Ohnehin seien sie viel leistungsfähiger. In dieser Ausarbeitung werden wir den grundlegenden Prinzipien dieser *Quanten* folgen und uns anschauen, ob diese neue Rechnerarchitektur Vorteile hat. Ganz besonders werden wir uns im Rahmen der Quantentheorie dem Schlüsselaustauschverfahren zuwenden, da dies ein grundlegendes Element für die Quantenkryptografie ist. Hat man diese eingängig verstanden, so versteht man gleichzeitig den gegenwärtigen Stand der Forschung und der konkreten Umsetzung. Wir werden uns im Anschluss fragen welche Implikationen das Rechnen mit Quanten für uns hat und ob die klassischen Verfahren, die wir heute benutzen, noch so sicher sind wie oft geglaubt wird. Wir werden auch an zwei Punkten die kommerzielle Welt streifen und sehen an welcher Stelle bereits erste Produkte auf dem Markt kommen. Aufgrund der Kürze dieser Arbeit ist natürlich die Darstellung eines vollständiges Bildes in beliebiger Tiefe nicht möglich. Das Ziel ist vielmehr einen Einblick in die Technologie zu vermitteln und zum weiteren Lesen anzuregen.

Kapitel 2

Grundlegende Prinzipien

2.1 Was ist Kryptografie?

Kryptografie ist ein zusammengesetztes Wort aus den lateinischen Begriffen für „verstecken“ und „schreiben“ [12, S. 11]. Es geht ganz prinzipiell darum Informationen vor dem Mitlesen Dritter zu schützen. Dabei ist nicht nur die Information, welche eine Nachricht enthält, schützenswert, sondern auch die Übermittlung der Nachricht selbst.

2.2 Was ist ein Quantum bzw. Quantenkryptografie?

Die klassische Physik kennt zwei prinzipiell unterschiedliche Modelle zur Erklärung der Wirklichkeit: Die Teilchen (auch Massenpunkte genannt) und die Wellen. In der makroskopischen Welt ließ sich durch diese Einteilung die Welt sehr gut erklären. Experimantalphysiker zeigten jedoch durch den oft zitierten *Doppelspaltversuch*, dass das Licht scheinbar gleichzeitig Charakteristika von Teilchen und Wellen aufweist. Dieser sog. Teilchen-Welle-Dualismus war aber durch die Erkenntnisse der klassischen Physik nicht mehr zu erklären. Das bedeutete, dass die physikalischen Gesetze der Makroskopie nicht für die Welt der kleinsten Elemente gilt.

Bei der Betrachtung von sog. *schwarzen Körpern* versagten die bisher bekannten makroskopischen Gesetze abermals. Die Erklärung dieses zunächst unverstandenen Phänomens führte Max Planck zu der revolutionären Theorie, dass die Menge an Energie einer

Lichtwelle nicht kontinuierlich, sondern diskret d. h. unteilbar ist. Allein diese Annahme genügte, um gänzlich mit der klassischen Physik zu brechen. Planck zeigte, dass Energie nicht in beliebigen Mengen, sondern nur *quantisiert* d. h. mit einer bestimmten Mindestmenge ausgetauscht werden kann. Die Entdeckung dieser Naturkonstante der absoluten Mindestmenge an Energie wird seitdem das *Plancksche Wirkungsquantum h* genannt. Ein Quantum ist also die kleinste mögliche Menge an Energie.

Die Quantenkryptografie ist diejenige Disziplin, die sich nun diese neuen - nach dem alten klassischen Bild der Physik unmöglichen - Eigenheiten der Quantenphysik zu nutze macht, um daraus Anwendungen zu generieren, die Informationen für Dritte verschlüsseln bzw. unlesbar machen. Diese speziellen Eigenschaften sind der Grund weshalb Quantencomputer *anders* rechnen.

2.3 Auf welchen Prinzipien beruht das Rechnen mit Hilfe von Quanten?

Ein klassischer Rechner arbeitet mit den Zuständen 1 und 0. Ein Zustand wird durch ein *Bit* repräsentiert. Bewegen wir uns im Raum der Quantenphysik, führen wir hierzu analog den Begriff des *Qubit* ein. Dieser repräsentiert fortan einen Zustand innerhalb eines Quantencomputers. Um präzise zu sein: Ein Quantenrechner rechnet nicht direkt mit Quanten als solchen, sondern bedient sich der speziellen Eigenschaften der Quantenphysik, um Ergebnisse zu errechnen.

Grundlegend haben Quantenzustände mehrere herausragende neue Eigenschaften. Für die Zwecke der Quantenkryptografie sind vorrangig die Eigenschaften der **Superposition** und die der **Unschärferelation** wichtig. Bei neueren Entwicklungen ist ergänzend auch der Begriff der **Verschränkung** von Bedeutung.

2.3.1 Superposition

Die Eigenschaft der Superposition bedeutet verkürzt, dass zwei Zustände, wie beispielsweise 1 und 0, sich überlagern können: das heißt gleichzeitig in einem Qubit existieren

können. Dies erscheint in unserer bisherigen klassischen Weltanschauung paradox, doch wir werden später noch sehen wie dies zu interpretieren ist.

2.3.2 Verschränkung

Die Eigenschaft der Verschränkung bedeutet verkürzt, dass zwei Teilchen miteinander in Korrelation stehen. Das heißt, dass zwei zusammenhängende Teilchen sich exakt gleich verhalten, obwohl sie an unterschiedlichen Orten sind.

2.3.3 Unschärferelation

Während ein klassischer Computer im Binärsystem exakt mit zwei Zuständen rechnet - nämlich an oder aus: d. h. den Bits 1 und 0 - ist ein Quantencomputer Kraft der Superposition in der Lage mit einem Qubit mit einem Zustand zu rechnen, der gleichzeitig 1 **und** 0 ist. Erst durch eine Messung des Zustands wird das Qubit den ablesbaren Zustand 1 oder 0 annehmen. Man schreibt diese Zustände den sog. *Spins* zu. Dies kann man sich als eine Drehrichtung - einen Drehimpuls - des Teilchens vorstellen.

Bei der Messung des Zustands eines Teilchens tritt eine Besonderheit in den Quantenphysik zu Tage: Werner Heisenberg zeigte, dass der Ort eines Teilchens und der Impuls eines Teilchens nicht gleichzeitig gemessen werden können. Je präziser der Ort eines Teilchens bestimmt wird, desto ungenauer wird sein Impuls - und umgekehrt [5, S. 264]. Diese Gesetzmäßigkeit wird *Heisenbergsche Unschärferelation* genannt. Solange der Zustand eines Qubits nicht gemessen wird, bleibt er *unbestimmt (unscharf).*

Kapitel 3

Quantencomputing und dessen Potentiale

3.1 Welche technischen Realisierungsformen von Quantencomputern gibt es?

Quantencomputer müssen in der Lage sein Qubits zur Verfügung zu stellen, Rechenoperationen auf diesen auszuführen und die Ergebnisse abzulesen. Die Tabelle 3.1 gibt einen Überblick über die im Jahre 2011 aktuellen Eigenschaften der unterschiedlichen Lösungssysteme [3, S. 343]. Die Leistungsfähigkeit wird anhand dreier Faktoren bemessen:

1. **Dekohärenzzeit**: Dies ist die stabile Zeit in welcher ein Quantenzustand nicht durch Wechselwirkungen mit anderen Teilchen verändert wird. Je besser die Systemisolierung desto länger dauert der stabile Zustand an.
2. **Operationszeit**: Dies ist die effektive Zeit in welcher das System zu Berechnungen in der Lage ist.
3. **Anzahl der Operationen**: Aus Dekohärenzzeit und Operationszeit ergibt sich die Anzahl der möglichen Berechnungen. Nach Einschätzung von Brands sind Systeme mit weniger als $10^6 - 10^8$ Operationen nicht leistungsfähig genug, sodass nur die mit einem Stern versehenen Systeme für die realistische Nutzung übrig bleiben [3, S. 343].

System	Dekohärenzzeit	Operationszeit	Operationen
Kernspin*	$10^{-2} - 10^{8}$	$10^{-3} - 10^{-6}$	$10^{5} - 10^{14}$
Elektronenspin	10^{-3}	10^{-7}	10^{4}
Ionenfalle*	10^{-1}	10^{-14}	10^{13}
Elektronen-Au*	10^{-8}	10^{-14}	10^{6}
Elektronen-GaAs	10^{-10}	10^{-13}	10^{3}
Quantenpunkt	10^{-6}	10^{-9}	10^{3}
Optische Kavität*	10^{-5}	10^{-14}	10^{9}
Mikrowellenkavität	10^{0}	10^{-4}	10^{4}
Cooper-Paare	$> 10^{-3}$	unbekannt	unbekannt 10^{5}

Tabelle 3.1: Technologien für die Umsetzung von Quantencomputern

3.2 Wie leistungsfähig sind Quantencomputer?

Die Eigenschaft der Superposition - also dass ein Qubit gleichzeitig zwei Zustände repräsentieren kann - führt vereinfacht ausgedrückt dazu, dass eine einzige Berechnungsoperation stets auf beide Zustände gleichzeitig angewendet wird. Wenn wir nun Operationen auf eine Kaskade aus Qubit-Registern anwenden, dann führt dies dazu, dass bei jedem Kaskadenschritt eine Operation auf alle dem System möglichen Qubit-Zustände ausgeführt wird. Pro zusätzlicher Qubit-Ebene nimmt also die Leistungsfähigkeit des Quantencomputers **exponentiell** zu (siehe Abb. 3.1). Verglichen mit den heutigen klassischen Computern, welche Operationen nur linear abarbeiten können, ist die Fähigkeit Operationen **parallel** ausführen zu können, die große Stärke der Quantencomputer. Wie wir in Kapitel 4 sehen werden, führt dies zu einem beträchtlichen Risiko für die Sicherheit von aktuellen kryptografischen Verfahren.

3.3 Wie lässt sich Kryptografie basierend auf Quantencomputing umsetzen?

Die Kryptografie bezeichnet Methoden, um Informationen für Dritte unlesbar zu machen. Dies wird einerseits dadurch erreicht, dass die Information selbst verschlüsselt wird und andererseits dadurch, dass die Übertragung dieser Information - sei sie verschlüsselt oder nicht - möglichst sicher oder gar unabhörbar geschieht. Die Übertragungsart einer Information spielt eine wichtige Rolle, um den Schutz der zu übertragenden Inhalte

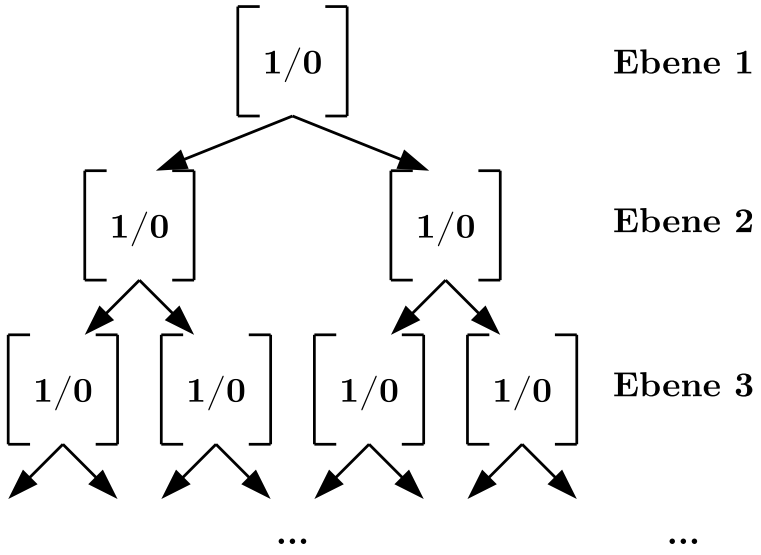

Abbildung 3.1: Exponentielle Leistung durch Qubit-Kaskaden

zu gewährleisten. Gelingt es (a) zwei Kommunikationspartnern einen Einmalschlüssel (*Vernam-Chiffre*) mit absoluter Sicherheit zu übertragen und (b) sind diese Schlüsselwerte absolut zufällig, so erhält man eine perfekte Geheimhaltung (Schmeh, 2016, S. 52).

3.3.1 Die absolut vertrauliche Übertragung eines Schlüssels

Der **Quantenschlüsselaustausch** (englisch: *QKD - Quantum Key Distribution*) ist ein Verfahren mit dessen Hilfe der Sender dem Empfänger über einen sog. *Quantenkanal* (d. h. einem Übertragungsweg über den man beispielsweise quantisierte Photonen übertragen kann) Informationen zum Schlüssel übermitteln kann. Das Ziel ist es einen Schlüssel auszutauschen, um mit dessen Hilfe eine Nachricht verschlüsseln zu können. Dritte sollen diesen Schlüssel nicht abhören können. Hierfür gibt es bereits ein Verfahren namens *Quantum Key Distribution BB84*, welches 1984 von C. H. Bennet und G. Brassard entwickelt wurde.

Wätjen [16, S. 153ff.] skizziert das Verfahren folgendermaßen: Das Licht auf Senderseite wird zunächst in vier mögliche Richtungen polarisiert

- vertikal (0 Grad bzw. |)

- horizontal (90 Grad bzw. —)
- linksdiagonal (45 Grad bzw. \ )
- rechtsdiagonal (135 Grad bzw. /)

und eine zufällige Sequenz hierüber über den Quantenkanal an den Empfänger gesendet (Abb. 3.2 links). Der Photonen-Strahl wird beim Empfänger an einem doppelbrechenden Kristall wieder in zwei Teile geteilt: einen Strahl der horizontalen Photonen mit 0 Grad und einen Strahl mit den vertikalen Photonen mit 90 Grad (Abb. 3.2 mittig). Der Empfänger misst dann die ankommenden zwei Photonenstrahlen mit zwei Polarisationsdetektoren (Abb. 3.2 rechts).

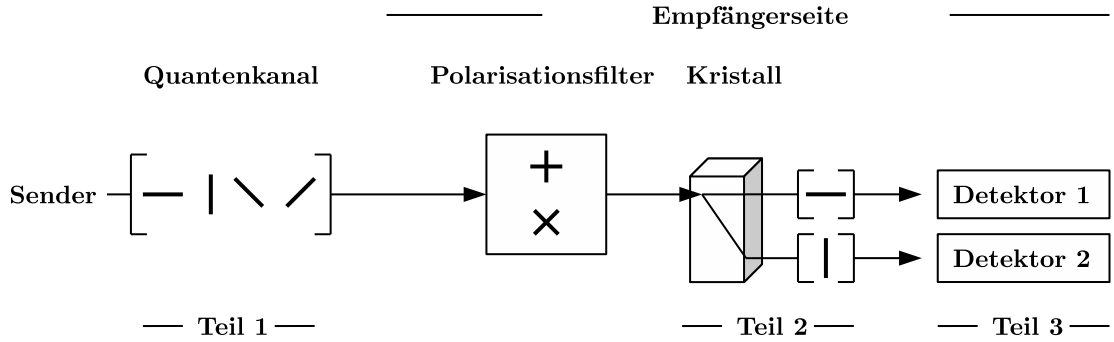

Abbildung 3.2: Prinzipieller Aufbau des BB84-Verfahrens

Betrachten wir zuerst den einfachen Fall, um uns mit dem Aufbau vertraut zu machen: Würde der Sender abwechselnd nur vertikal oder horizontal polarisiertes Licht versenden, dann würden die beiden Detektoren des Empfängers abwechselnd ein Photon registrieren. Dabei würden bei einem strikten Wechsel zwischen vertikal und horizontal auch genau die Hälfte der Photonen auf Detektor 1 und die andere Hälfte auf Detektor 2 treffen.

Jetzt wird es spannend: Was würde passieren, wenn wir ein links- oder rechtsdiagonales Photon versenden? Dieses Photon, welches eben gerade noch *unbestimmt* war, würde nach den Gesetzen der Quantenphysik auf den Kristall treffen und zur Einnahme eines *bestimmten* Zustands gezwungen werden. Das bedeutet konkret, dass das eintreffende diagonale Photon mit der quantenphysikalischen Wahrscheinlichkeit von genau 50% umpolarisiert würde: entweder zu einem vertikal oder einem horizontal polarisierten Photon.

Weil dieses außergewöhnliche Verhalten für die kryptografische Anwendung der Schlüs-

selübertragung gleich noch sehr wichtig sein wird, machen wir uns dies nochmals an einem konkreten Beispiel bewusst. Angenommen der Sender schickt über den Quantenkanal jeweils 10 Photonen aller vier Polarisationsmöglichkeiten (|, —, \ , und /). Am Kristall treffen die ersten 10 vertikalen Photonen auf und werden am Detektor 2 registriert (Detektor 2 = 10 Photonen). Die nächsten 10 horizontalen Photonen werden am Detektor 1 registriert (Detektor 1 = 10 Photonen). Kommen nun die nächsten 10 linksdiagonalen Photonen am Kristall an, so werden 50% dieser Photonen zu vertikalen Photonen (Detektor 2 = 15) und die anderen 50% zu horizontalen Photonen (Detektor 1 = 15) umpolarisiert. Wir erkennen, dass aufgrund der Wahrscheinlichkeit von exakt 50% die Detektoren 1 und 2 immer die gleiche Anzahl von Photonen registrieren werden.

Nun da wir das Prinzip der Quanten-Wahrscheinlichkeit eingängig beleuchtet haben, schreiten wir voran und lassen Sender und Empfänger eine Beispielsequenz übermitteln. Dabei setzen wir einfach fest, dass bestimmte Polarisationen als bestimmte Bit interpretiert werden:

Polarisation	vertikal (|)	horizontal (—)	linksdiagonal (\)	rechtsdiagonal (/)
Entsprechung	Bit 1	Bit 0	Bit 0	Bit 1

Tabelle 3.2: Zuordnung von Polarisation zu Bits

Auf der Empfängerseite bauen wir jedoch nun zusätzlich einen Polarisationsfilter ein, welcher in der ersten Einstellung nur horizontale/vertikale Photonen und in der zweiten Einstellung nur diagonale Photonen durchlässt. Für jedes ankommende Photon wird nun die Einstellung des Polarisationsfilters abwechselnd geändert. Wir nennen diese beiden Einstellungen Basis-+ und Basis-× . Natürlich kann man an dieser Stelle ebenfalls den Quantenzufall für die beiden Einstellungen bemühen, da dies statistisch ebenfalls zu einer gleichen Wahrscheinlichkeit von jeweils 50% für die beiden Einstellungen führt.

Wir lassen nun die beiden Kommunikationspartner die in Tabelle 3.3 benannte Sequenz durchlaufen. Der Anschaulichkeit halber verwenden wir dabei alle möglichen Permutationen hintereinander. Wichtig ist die Tatsache, dass in der Tabelle auch die Fälle aufgeführt sind, bei denen die Polarisationsbasen von Sender und Empfänger nicht zusammenpassen, sodass der Quantenzufall entscheidet, wie das Photon umpolarisiert wird. Diese Fälle sind in Tabelle 3.3 jeweils mit a und b gekennzeichnet. Weiterhin ergänzen wir Tabelle 3.3 mit den jeweiligen Bit-Entsprechungen des Senders.

Der Empfänger ist jetzt im Besitz einer Sequenz zu der er Aussagen kann welche Basis

Fälle	1	2a	2b	3	4a	4b	5	6a	6b	7	8a	8b
Gesendetes Bit	1	1	1	0	0	0	0	0	0	1	1	1
Gesendete Polarisation	/	/	/	\	\	\	—	—	—	|	|	|
Basis des Empfängers	×	+	+	×	+	+	+	×	×	+	×	×
Gemessene Polarisation	/	—	|	\	—	|	—	/	\	|	/	\

Tabelle 3.3: Sequenz und gemessene Polarisation des Empfängers

er benutzt hat und welche Polarisation er gemessen hat. Wir sehen, dass die gemessene Polarisation nicht immer der tatsächlich verwendeten auf der Senderseite entspricht.

Darauf aufbauend teilt der Empfänger dem Sender mit welche Basis er für die Sequenz der Photonen gewählt hat (Tab. 3.4).

Fälle	1	2a	2b	3	4a	4b	5	6a	6b	7	8a	8b
Basis des Empfängers	×	+	+	×	+	+	+	×	×	+	×	×

Tabelle 3.4: Mitteilung der Basen an den Sender

Im nächsten Schritt retourniert der Sender die Information, welche Basis die richtige war. Der Sender weiß nämlich welches Bit bzw. welche Polarisation er versendet hat und weiß daher automatisch auch mit welcher Basis es hätte dekodiert werden sollen (Tab. 3.5).

Fälle	1	2a	2b	3	4a	4b	5	6a	6b	7	8a	8b
Korrekte Senderbasis	×	×	×	×	×	×	+	+	+	+	+	+
Basis des Empfängers	×	+	+	×	+	+	+	×	×	+	×	×
Basis korrekt?	j	n	n	j	n	n	j	n	n	j	n	n

Tabelle 3.5: Vergleich der Basen auf Seite des Senders

Mit der Information welche Basis für welches detektierte Photon die richtige war, weiß der Empfänger nun, welche Polarisationen korrekt übertragen wurden und verwirft diejenigen Fälle in denen die Basis nicht gleich war (Tab. 3.6).

Dieses Beispiel ist aufgrund des Zwecks zur Veranschaulichung und der deshalb verwendeten Permutation kein gutes Beispiel, um die Zufälligkeit der **nachfolgenden** Bits erkennen zu lassen: Dafür ist es schlicht zu kurz. Der Schlüssel wäre hier nämlich nur 1001. Wenn man dieses Prinzip jedoch für längere Schlüssel anwendet, dann ist das

Fälle	1	2a	2b	3	4a	4b	5	6a	6b	7	8a	8b
Gesendetes Bit	1	1	1	0	0	0	0	0	0	1	1	1
Gesendete Polarisation	/	/	/	\	\	\	—	—	—	|	|	|
Basis des Empfängers	×	+	+	×	+	+	+	×	×	+	×	×
Gemessene Polarisation	/	—	|	\	—	|	—	/	\	|	/	\
Basis korrekt?	j	n	n	j	n	n	j	n	n	j	n	n
Korrektes Bit	1			0			0			1		

Tabelle 3.6: Gesamte Sequenztabelle mit korrekt interpretierten Bits des Empfängers

Ergebnis aber am Ende eine quantenzufällige Folge aus Bits mit einer Wahrscheinlichkeitsverteilung von genau 50% für das Bit 1 und 50% für das Bit 0. Dies lässt sich bereits gut an der kurzen Schlüsselfolge 1001 erkennen: Zu jeweils exakt 50% tauchen hier nämlich die Bits 1 und 0 auf.

Wir merken uns gedanklich, dass es uns mit dem obigen Verfahren gelungen ist einen Schlüssel mit Hilfe eines Quantenkanals zu übertragen. Weiterhin erkennen wir, dass die Anzahl der Bits 1 und 0 immer gleich ist, d. h. die Wahrscheinlichkeit für diese Bits jeweils **immer** 50% beträgt.

Man mag sich jetzt zu Recht fragen: Was hat dieses Verfahren mit Sicherheit zu tun? Auf die Frage der Abhörsicherheit kommen wir gleich zu sprechen.

In den Unterkapiteln *Unschärferelation* und *Superposition* haben wir gesehen, dass die Messing des Ortes eines Quantums unweigerlich dafür sorgt, dass der Implus nicht mehr genau gemessen werden kann und vice versa. Beim Lauf des Photons durch den Kristall zwingen wir also das sich noch in Superposition befindliche Photon sich „zu entscheiden“ und mit dem Zufall von exakt 50% einen bestimmten Zustand anzunehmen. Wir interpretieren diesen Zustand mit der Detektions-Apparatur dann als 1 oder 0. Das Photon wird also für uns erst genau in dem Moment sichtbar, in welchem wir es mit dem Detektor messen.

Wir stellen uns weiter vor, dass eine dritte Person während der Übertragung ein Photon abgreift, da sie wissen möchte, welchen Impuls unser Photon trägt, um damit den Schlüssel abzugreifen, den wir ja unbedingt zu schützen versuchen. Des Weiteren stellen wir uns vor, dass dieser Wert von der dritten Person notiert wird und unverändert weitergesendet wird. Was würde geschehen?

Die Messung durch die dritte Person würde das Photon dazu zwingen einen Zustand einzunehmen, damit es überhaupt lesbar und interpretierbar wird. Bei diesem zwischengeschalteten Detektor wären das Verhalten und die Wahrscheinlichkeit genau wie beim originären Empfänger: jeweils 50% für die Werte 1 und 0. Das Abfangen des Photons würde allerdings dazu führen, dass der Empfänger gar keine Information - also kein Photon - mehr erhält. Das bedeutet, dass die dritte Person ein Photon mit eben jener abgelesen Information weiterschicken muss. Wir nehmen daher Mal an dieser Wert würde zum eigentlichen Empfänger weitergeschickt. Die Photonen müssten nun also jetzt derart weitergeschickt werden, dass sich der Wert des Photons nicht mehr verändert, sonst sind die notierten Informationen der dritten Person nutzlos. Das bedeutet, dass der intermittierende Dritte nun Photonen weitersendet, bei denen er sicher ist, dass das gewünschte Ergebnis von 1 oder 0 eintritt. Die Photonen wurden ja bereits „ausgelesen“ und können daher beim Empfänger nicht mehr zufällig die Polarisation ändern.

Diese Tatsache, dass sich die Polarisation bei einem abgefangenen Photon nicht mehr ein zweites Mal zufällig ändern kann, hat eine weitreichende Implikation zur Folge: Der Intermittierende erhält mit seiner Ablesung zu 50% das korrekte Ergebnis. Er selbst hat keine Kenntnis davon, welche Basis der Sender verwendet hat, also bleibt ihm der Zufall übrig eine der beiden Basen anzusetzen - genauso wie es beim Empfänger der Fall wäre. Möchte der Intermittierende nun ein Photon weiterschicken, so hat er sich nun bereits für eine Basis entschieden. Da auch der Empfänger die verwendeten Basen des Senders nicht kennt, wählt auch er diese mit Zufall. Dies führt unweigerlich dazu, dass der Sender bemerken wird, dass der Empfänger zwar die richtigen Basen verwendet hat, aber dass trotzdem beim Empfänger die falsche Polarisation gemessen wurde. Das Ablesen einer falschen (anderen) Polarisation kann nur geschehen, wenn ein gänzlich neues Photon durch einen Intermittierenden auf den Weg gebracht wird. Beispiel: Der Sender verschickt ein horizontales Photon mit der Basis-+. Der Mithörer hat durch Zufall die Basis-× angesetzt und misst deshalb ein diagonales Photon. Da der Mithörer selbst ein diagonales Photon gemessen hat, schickt er ein solches weiter an den ursprünglichen Empfänger. Dieser hat seinerseits durch Zufall die richtige Basis wie der Sender (+), erhält aber ein ankommendes diagonales Photon, welches sich wiederum mit der Wahrscheinlichkeit von 50% zu einem vertikalen verwandelt. Der Sender weiß natürlich, dass bei der gleichen Basis ein horizontales Photon auch zur gleichen horizontalen Detektion führen muss. An diesem Punkt ist nun auch die vorherige Frage nach der Sicherheitseigenschaft beantwortet: Der Sender ist nun in der Lage den Empfänger zu warnen, dass der Schlüsselaustausch gestört wurde, sodass ein neuer Versuch unternommen werden kann. Zu dieser Zeit ist die sicher zu übertragende Nachricht weiterhin geschützt, da sie

noch nicht übertragen wurde. Sender und Empfänger befanden sich lediglich in der Stufe des sicheren Schlüsselaustausches.

3.3.2 Fortgeschrittene Schlüsselverteilung

E91. Das Protokoll *BB84* nutzt einen einzelnen Photonengenerator, um die Photonen zu erzeugen, welche anschließend polarisiert an den Empfänger gesendet werden. Anstelle dieses einzelnen Photonengenerators kann man auch eine Apperatur einsetzen, die *verschränkte* Photonen erzeugt. Diese prinzipiell auf den Mechanismen von *BB84* beruhende Methode wurde 1991 von Artur Ekert veröffentlicht und wird *E91* genannt. Im Kern unterscheidet sie sich dadurch, dass von einer sendenden Stelle (z. B. einem Satelliten) *verschränkte* Photonen gleichzeitig an zwei Empfänger versendet werden. Bei diesem Verfahren wird also nicht erst wie bei *BB84* das Photon erst erzeugt, das Bit kodiert und dann übertragen, sondern das Photon erhält erst durch die Messung bei den Empfängern seinen Wert. Folglich kann das Bit durch einen Dritten nicht abgehört werden, da es nie übertragen wurde. Das Photon erhält seinen Wert erst in dem Moment, an dem es gemessen wird. Sobald ein Photon durch einen Dritten gemessen wird, ändert sich auch der Zustand der anderen Photonen bei den Empfängern.

B92. Das Protokoll *BB84* wurde 1992 von Bennett weiterentwickelt. Diese Weiterentwicklung wird *B92* genannt und verwendet gegenüber dem alten Protokoll nur noch zwei Polarisationszustände anstatt vier: beispielsweise nur horizontale und rechtsdiagonale Photonen. Das grundlegende Prinzip ist gleich dem des *BB84*.

3.4 Auswirkung der Quantentechnologie auf klassische Krypto-Verfahren

Die bisherigen klassischen **asymmetrischen** Verfahren wie RSA basieren auf der Schwierigkeit der Primfaktorzerlegung oder der Berechnung diskreter Logarithmen. Mit Hilfe des *Shor-Algorithmus* [13] sind diese Systeme in polynomieller Laufzeit entschlüsselbar. Große Teile der heutigen technischen Sicher- und Privatheit basieren auf asymmetrischen Verfahren. Dies ist der Grund weshalb aktuell stark nach Nachfolgern geforscht wird.

Die bisherigen klassischen **symmetrischen** Verfahren wie AES gelten bis dato als sicher, da bislang auch das bekannteste Lösungsverfahren wie der Grover-Algorithmus (eigentlich ein Such-Algorithmus für Datenbanken) die Güte des Schlüssels nur um die Hälfte reduzieren würde. Diesem Umstand kann man einfach durch einen längeren Schlüssel entgegenwirken.

Kapitel 4

Aktueller Stand

4.1 Welche Krypto-Anwendungen existieren bereits?

QKD. Die in Kapitel 3 vorgestellten Verfahren zum *Quantenschüsselaustausch* werden an einer Vielzahl von Forschungseinrichtungen weiterentwickelt. Einige davon befinden sich bereits in kommerzieller Nutzung und werden durch Firmen vertrieben wie beispielsweise:

- Speqtral (https://speqtral.space)
- ID Quantique (https://idquantique.com)
- KETS Quantum (https://kets-quantum.com)
- Quantum Xchange (https://quantumxc.com)

4.2 Wie weit ist die Quanten-Technologie fortgeschritten?

Zum einen ist es interessant auf welchen Gebieten aktuell geforscht wird und zum anderen ist die Realisierung mancher dieser Forschungsergebnisse direkt von der Leistungsfähigkeit der Quanten-Computer abhängig.

Die Leistung eines Quantencomputers hängt maßgeblich von der Anzahl der Qubits ab, die für Operationen zur Verfügung stehen. Wenn wir uns in der aktuellen digitalen

Nachrichtenwelt umsehen, dann finden wir einige markante Punkte und Prognosen:

01.11.2012. Dem Unternehmen D-Wave Systems ist es gelungen in Kooperation mit anderen Herstellern eine Berechnung mit Hilfe von 84 Qubit durchzuführen [2].

09.01.2018. Auf der Elektronikmesse *CES 2018* stellt der Chip-Hersteller Intel eine experimentelle Version eines Chips mit 49 Qubit vor [6].

05.03.2018. Google experimentiert gemäß einem eigenen Blog-Artikel an einem Quantencomputer mit 9 Qubit und arbeitet an der Fehlerrate, um 72 Qubit zu ermöglichen [8].

10.01.2019 Gemäß einem Artikel der Zeitung *Die Zeit* [9] bietet IBM einen ersten kommerziell nutzbaren Quantencomputer mit 20 Qubit an.

22.01.2019. In einer wissenschaftlichen Publikation über die Erweiterung einer von D-Wave genutzten Architektur [4] ist ein System vermerkt, welches mit einer Anzahl von 2048 Qubit operieren können soll. Die Herstellerwebsite [15] wiederholt diese Leistungsfähigkeit.

29.12.2019. Der französische Ingenieur Yann Allain berichtet [1] auf dem *Chaos Communication Congress* über sein Projekt unter Ausnutzung der Technologie einer Ionen-Falle einen eigenen Quantencomputer in der Garage zu bauen. Im Rahmen seines Vortrags verweist er auf eine ähnliche Grundarchitektur seines Quanten-Computers mit der Architektur, deren experimentelle Bauteile aus 2017 im Quanten-Museum der Universität von Sussex ausgestellt werden.

Wenn man sich vor Augen führt, dass der erste Intel Prozessor 4004 [7] im Jahre 1971 gerade einmal 2300 Transistoren besaß und ungefähr 10 Jahre später im Jahre 1982 ein Intel 80286 [10] mit bereits 134.000 Transistoren im Rechenwerk operierte, dann ist davon auszugehen, dass die Zahl der nutzbaren Qubit in Quantenrechnern zu Anfang keine großen Sprünge macht, da sich vieles im Bereich der Experimente abspielt. Es ist jedoch zu erwarten, dass die fortschreitende Beherrschung dieser neuen Technologien dazu führen wird, dass nach der Experimentierphase der Schritt der Skalierung folgen wird und damit - wie in der Entwicklungsphase der klassischen Prozessoren - die Leistungsfähigkeit der Quantencomputer signifikant steigt.

Geheimdienste wie die NSA sind spätestens seit 2014 aus naheliegenden Gründen der Informationsgewinnung an der Entschlüsselung von klassischen asymmetrischen Verfahren interessiert [11]. Es ist aufgrund der finanziellen Mittel der Geheimdienste stark davon auszugehen, dass in den jeweils eigenen Forschungseinrichtungen der Geheimdienste bereits Prototypen existieren, die über eine enorme Anzahl nutzbarer Qubit verfügen. Dies scheint realistisch, wenn man bedenkt, dass experimentelle Bauteile aus 2017 mittlerweile sogar schon in einem Museum ausgestellt werden.

4.3 Post-Quanten-Kryptografie

Aufgrund der Schwäche von asymmetrischen Kryptosystemen wird gegenwärtig nach sicheren Nachfolgeverfahren gesucht, welche resistent gegenüber den Fähigkeiten von Quantencomputern sind. Diese Klasse von Verfahren wird unter dem Begriff *Post-Quanten-Kryptografie* zusammengefasst.

Eine Publikation zu den Vorlesungen des *College of Saint Benedict/Saint John's University* [17] prognostiziert einen Bedarf von mindestens 10.000 Qubit, um RSA mit 2048 Bit mit Hilfe des Shor-Algorithmus zu entschlüsseln. Sollte diese Annahme zutreffend sein, so wäre die heutige Nutzung von RSA nicht mehr hinreichend sicher, da man davon ausgehen muss, dass der technologische Fortschritt der Geheimdienste einige Jahre beträgt.

Die zuvor beschriebene rasante Entwicklung von Quantencomputern hat wahrscheinlich dazu geführt, dass das amerikanische *National Institute of Standards and Technology (NIST)* Ende 2016 einen Prozess initiiert hat, um quantenresistente Public-Key Algorithmen zu finden, zu evaluieren und zu standardisieren [14]. Am 30. Januar 2019 wurden dort die folgenden potentiellen PKI-Algorithmen genannt:

- BIKE
- Classic McEliece
- CRYSTALS-KYBER
- FrodoKEM
- HQC
- LAC

- LEDAcrypt (merger of LEDAkem and LEDApkc)
- NewHope
- NTRU (merger of NTRUEncrypt and NTRU-HRSS-KEM)
- NTRU Prime
- NTS-KEM
- ROLLO (merger of LAKE, LOCKER and Ouroboros-R)
- Round5 (merger of HILA5 and Round2)
- RQC
- SABER
- SIKE
- Three Bears

An der Länge dieser Aufzählung erkennt man bereits, dass die Betätigung in diesem Forschungsgebiet sehr rege ist. Aktuell sieht die Zeitplanung des NIST vor, dass eine weitere dritte Runde 2020/2021 stattfindet und erste konkrete Entwürfe für zukünftige Standards im Zeitraum 2022/2024 erstellt werden.

Schlusswort. An dieser Stelle sind unsere Ausflüge in die Quantenwelt zu Ende. Mit diesem Überblick an Grundkenntnissen vermag sich der interessierte Leser gern weiter an der Literaturliste versuchen, um ein tieferes Verständnis für einzelne Teilbereiche zu erlangen. Es scheint mir bei der Durchsicht der vorhanden Literatur als wäre die Quantenmechanik zwar um 1950 korrekt postuliert und seitdem verstanden worden. Zwar sind viele Forschergruppen auf verschiedenen Arbeitsgebieten tätig - wie jede schnelle Recherche im Internet zeigt - aber wirklich viele Neuerungen und Anwendungen sind bislang unter dem Strich nicht in Erscheinung getreten. Hier ist sicherlich noch Platz für die eine oder andere Entdeckung!

Literaturverzeichnis

[1] Allain, Yann: *Build you own Quantum Computer @ Home - 99Hacker Style !* https://media.ccc.de/v/36c3-10808-build_you_own_quantum_computer_home_-_99_of_discount_-_hacker_style. Version: 2019, Abruf: 28.02.2020

[2] Bian, Zhengbing ; Chudak, Fabian ; Macready, William G. ; Clark, Lane ; Gaitan, Frank: Experimental determination of Ramsey numbers. In: *Phys. Rev. Lett. vol.* 111 (2013), 130505. http://dx.doi.org/10.1103/PhysRevLett.111.130505. – DOI 10.1103/PhysRevLett.111.130505

[3] Brands, Gilbert: *Einführung in die Quanteninformatik*. Springer Berlin Heidelberg, 2011. http://dx.doi.org/10.1007/978-3-642-20647-4. http://dx.doi.org/10.1007/978-3-642-20647-4. – ISBN 9783642206474

[4] Dattani, Nike ; Szalay, Szilard ; Chancellor, Nick: Pegasus: The second connectivity graph for large-scale quantum annealing hardware. (2019), 01. https://arxiv.org/pdf/1901.07636.pdf

[5] Homeister, Matthias: *Quantum Computing verstehen: Grundlagen - Anwendungen - Perspektiven*. Springer Fachmedien Wiesbaden, 2015 (Computational Intelligence). https://books.google.de/books?id=MgVcCgAAQBAJ. – ISBN 9783658104559

[6] Hsu, Jeremy: CES 2018: Intel's 49-qubit chip shoots for quantum supremacy. In: *IEEE Spectrum Tech Talk* (2018). https://spectrum.ieee.org/tech-talk/computing/hardware/intels-49qubit-chip-aims-for-quantum-supremacy

[7] Intel: *The Story of the Intel 4004: Intel's First Microprocessor - Its invention, in-*

troduction, and lasting influence. https://www.intel.com/content/www/us/en/history/museum-story-of-intel-4004.html. Version: 2020, Abruf: 20.02.2020

[8] Kelly, Julian: *A Preview of Bristlecone, Google's New Quantum Processor*. https://ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html. Version: 2018, Abruf: 10.02.2020

[9] Lindinger, Manfred: *Der Quantencomputer verlässt das Labor*. https://www.faz.net/aktuell/wissen/computer-mathematik/ibm-praesentiert-den-ersten-kommerziellen-quantencomputer-15980196.html. Version: 2019, Abruf: 14.02.2020

[10] Oppelt, Dirk: *The Intel 80286 Processor*. http://www.cpu-collection.de/?l0=co&l1=Intel&l2=80286. Version: 2020, Abruf: 28.02.2020

[11] Rich, Steven ; Gellman, Barton: NSA seeks to build quantum computer that could crack most types of encryption. In: *The Washington Post* 2 (2014)

[12] Schmeh, Klaus: *Kryptografie: Verfahren, Protokolle, Infrastrukturen*. dpunkt.verlag, 2016 (iX Edition). https://books.google.de/books?id=MJ10DAAAQBAJ. – ISBN 9783864919084

[13] Shor, Peter W.: Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. In: *SIAM J.Sci.Statist.Comput.* 26 (1997), 1484. http://dx.doi.org/10.1137/S0097539795293172. – DOI 10.1137/S0097539795293172

[14] Standards, National I. ; Technology: *Post-Quantum Cryptography*. https://csrc.nist.gov/projects/post-quantum-cryptography. Version: 2017, Abruf: 27.02.2020

[15] Systems, D-Wave: *The D-Wave 2000Q System*. https://www.dwavesys.com/d-wave-two-system. Version: 2020, Abruf: 28.02.2020

[16] Wätjen, Dietmar: *Kryptographie: Grundlagen, Algorithmen, Protokolle*. 2. Auf-

lage. Springer Fachmedien Wiesbaden, 2018 https://books.google.de/books?id=7xhgDwAAQBAJ. – ISBN 9783658224745

[17] Ziegler, Lynn: *Online security, cryptography, and quantum computing.* ttps://digitalcommons.csbsju.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1118&context=forum_lectures. Version: 2015, Abruf: 28.02.2020