Das Problem des Schlüsselaustausches in der Kryptographie

Vergleich zweier Verfahren

Vorwissenschaftliche Arbeit verfasst von

Mirijam Marschner

8B 2019/20

Betreuerin

Mag. Dr. Sonja Salzger

Bundesgymnasium 8

1080 Wien

13.2.2020

Abstract

Kryptographie. Ohne diese Wissenschaft könnten wir weder E-Mails sicher verschicken noch im Internet einkaufen. Die Sicherheit von Verschlüsselungsalgorithmen entscheidet über den Ausgang von Kriegen und den wirtschaftlichen Erfolg von großen Unternehmen. Da neueste Erkenntnisse aber meistens zum Schutz der Systeme geheim gehalten werden, wird selten über dieses Thema gesprochen.

Ziel dieser Arbeit ist es, die Anforderungen für ein sicheres Verschlüsselungssystem im Zeitalter des Internets zu illustrieren und verschiedene Beispiele für solche kryptographischen Systeme vorzustellen. Im Besonderen wird dabei auf die Problematik des Schlüsselaustausches eingegangen. Dazu werden zwei verschiedene Verfahren, das Open-Key-Verfahren und das System des Quantenschlüsselaustausches, genauer erklärt, die dieses Problem umgehen und ohne im Vorhinein ausgetauschte Informationen funktionieren. Außerdem wird versucht herauszufinden, welches dieser Systeme sich in Zukunft durchsetzen wird.

Diese Arbeit stützt sich größtenteils auf Artikel aus Fachzeitschriften, welche neue Erkenntnisse in der Kryptographie präsentieren und Literatur über diese Forschungsergebnisse. Die Abschnitte über die neuesten Entwicklungen in der Quantenkryptographie beziehen sich auf ein schriftliches Interview mit einem Wissenschaftler, der in diesem Bereich arbeitet.

Der letzte Teil der Arbeit befasst sich mit der Frage, welches der beiden vorgestellten Systeme praktischer in der Anwendung ist. Die Antwort lässt spannende Spekulationen zu, da sich die beiden Systeme wahrscheinlich in naher Zukunft ablösen oder in verschiedenen Bereichen Anwendung finden werden.

Inhaltsverzeichnis

Abstract 2

1. Einleitung 5

2. Klassische Kryptographie 6

2.1. Definition 6

2.2. Anfänge der Kryptographie 6

2.3. Grundbegriffe 7

2.4. Algorithmen als Funktionen 9

3. Public Key Verfahren 11

3.1. Einwegfunktionen 12

3.1.1. Echte Einwegfunktionen 12

3.1.2. Einwegfunktionen mit Trapdoor 12

3.2. Das RSA-Verfahren 12

3.3. Signaturen 14

3.4. Angriffsmöglichkeiten 15

3.5. Hybridverfahren 16

3.6. Pretty Good Privacy 17

4. Quantenschlüsselaustausch 18

4.1. Physikalische Voraussetzungen 19

4.2. Entstehung 20

4.3 Protokolle 20

4.3.1 BB84 20

4.3.2. BBM92 22

4.4. Übertragung 23

4.4.1. Freiraum 24

4.4.2. Glasfaserkabel 25

4.5. Fehlerrate 25

4.6. Attack Strategies 26
4.6.1. Man in the Middle 26
4.6.2. Intercept-resend 26
4.6.3 Photon-Number-Splitting 28
4.6.4. Denial of Service 28

5. Vergleich der beiden Verfahren 29
5.1. Public Key Verfahren in der Praxis 29
5.1.1. WhatsApp 29
5.1.2. E-Mail 30
5.1.3 Banktransaktionen 30
5.2. QKD-Systeme in der Praxis 30
5.3. Schwachstellen der Systeme 32
5.4. Zukunft 32

6. Fazit 34

Literaturverzeichnis 36

Abbildungsverzeichnis 37

Interview 38

Selbstständigkeitserklärung 40

1. Einleitung

Kryptographie, die Wissenschaft der Verschlüsselung von Nachrichten, ist heute kaum noch aus unserem Leben wegzudenken. Schon seit der Antike versuchen Länder, sichere Strategien zur Verschlüsselung zu entwickeln. Heute verwenden wir Codes für ganz alltägliche Tätigkeiten, zum Beispiel für Einkäufe im Internet. Spätestens seit der Erfindung des Internets ist es deshalb von großer Bedeutung, dass viele Menschen miteinander sicher kommunizieren können. Auch politische Diskussionen beschäftigen sich häufig mit dem Thema Privatsphäre. Deshalb halte ich Kryptographie auch für ein gesellschaftlich relevantes Thema.

Ich habe vor einigen Jahren ein Buch über die historische Entwicklung der Kryptographie von Simon Singh gelesen. Dabei ist mir aufgefallen, wie schwierig es ist, konkrete Informationen über moderne Kryptosysteme zu finden. Als ich mich mehr mit diesem Thema beschäftigte, stellte ich fest, dass der Schlüsselaustausch eines der Hauptproblem in der modernen Kryptographie ist. Für die meisten Systeme ist es nötig, im Vorhinein Informationen auszutauschen, wodurch ein Sicherheitsrisiko entsteht. Ich beschäftige mich in meiner Arbeit mit zwei Systemen, die eine sichere Kommunikation ohne Schlüsselaustausch ermöglichen sollen. Das Open-Key-Verfahren stützt sich auf Einwegfunktionen mit Hintertür, während das QKD-Verfahren Nachrichten mit polarisierten Photonen verschlüsselt. Ich habe diese beiden Systeme gewählt, da sie sehr unterschiedliche Lösungsansätze für dasselbe Problem sind und zu den wenigen Verschlüsselungssystemen zählen, über die viele Details bekannt sind.

Im ersten Teil der Arbeit werden Grundbegriffe der Verschlüsselungstechnologie erläutert. In den darauffolgenden zwei Kapiteln werden die beiden Verfahren genauer behandelt. Der letzte Teil der Arbeit versucht zu erklären, welches der beiden vorgestellten Systeme sich in Zukunft durchsetzen wird.

Ziel der Arbeit ist es, die Anforderungen für ein modernes kryptographisches System zu illustrieren. Außerdem werden beide Systeme verglichen, um so zu zeigen, welches mehr Sicherheit bietet. Um diese Fragen zu beantworten, habe ich nicht nur die Vor- und Nachteile beider Systeme aufgrund von Beschreibungen in Fachzeitschriften und Literatur verglichen, sondern dazu auch einen Experten befragt, der in dem Bereich der Quantenkryptographie forscht.

2. Klassische Kryptographie

2.1. Definition

Die Kryptographie beschäftigt sich mit der Verschlüsselung und geheimen Weitergabe von Nachrichten. Es wird nicht versucht, die Existenz einer Nachricht zu verschleiern, sondern diese so zu verändern, dass sie nur von Eingeweihten entziffert werden kann. Damit unterscheidet sich die Kryptographie deutlich von der Steganografie, die sich mit dem Verstecken von Nachrichten befasst. Das Wort Kryptographie leitet sich von dem griechischen Wort *kryptos* ab, welches verborgen bedeutet. Nachrichten werden mit zwei grundsätzlichen Verfahren verschlüsselt: Transposition, andere Anordnung der Buchstaben und Substitution, Ersetzung der Buchstaben durch andere Zeichen.[1]

2.2. Anfänge der Kryptographie

Kryptographie ist eine sehr alte Wissenschaft, da es im Laufe der Geschichte oft notwendig war, vertrauliche Nachrichten sicher zu übermitteln. Vor allem während Kriegen ist es wichtig, dass Botschaften nur von bestimmten Personen gelesen werden können, weshalb die Geschichte der Kryptographie eng mit der Weltgeschichte verbunden ist. Die ersten bekannten Geheimschriften stammen aus dem alten Ägypten und sind vermutlich 1900 v. Chr. entstanden.[2] Dabei handelt es sich um sonst unbekannte Hieroglyphen, die statt den üblichen verwendet wurden und so nur für bestimmte Menschen lesbar waren. Die Spartaner verwendeten im 5. Jahrhundert Skytale, um die Buchstaben einer Nachricht in eine andere Reihenfolge zu bringen. Für dieses Transpositionsverfahren wurde ein Lederband um einen Holzstab gewickelt und die Nachricht senkrecht darauf geschrieben. Nur ein Empfänger, der einen Holzstab mit exakt dem selben Durchmesser besaß, konnte die Nachricht entschlüsseln.[3]

Eine der bekanntesten antiken Geheimschriften geht auf Julius Cäsar zurück. Laut seinem Biograph Suetonius benutze Cäsar eine einfache Substitutionschiffre, um private Nachrichten zu verschlüsseln.[4]

---

[1] vgl. Singh, Simon: Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet. - München: dtv Verlagsgesellschaft mbH&Co. KG, 2001. S.22f

[2] vgl. Steward, Ian: Unglaubliche Zahlen. Reinbek bei Hamburg: Rowohlt Taschenbuch Verlag. 2016. S.358

[3] vgl. Singh, 2001, S. 23

[4] vgl. Steward, 2016, S.358

„(…)wenn etwas ziemlich Geheimes zu überbringen war, schrieb er es chiffriert, das heißt, indem er die Reihenfolge der Buchstaben so anordnete, dass kein Wort entziffert werden konnte. Wenn jemand das entziffern und den Sinn erkennen wollte, muss er den vierten Buchstaben des Alphabets austauschen, das heißt D für A, und auch so mit den Übrigen verfahren." [5]

2.3. Grundbegriffe

Obwohl die Cäsar-Chiffre ein sehr unsicheres Verfahren ist, das ohne technische Hilfsmittel entschlüsselt werden kann, lassen sich daran die Grundbegriffe eines kryptographischen Verfahrens erklären. Der unverschlüsselte Text, der Klartext, wird auf eine bestimmte Weise abgeändert, sodass er danach nicht mehr lesbar ist. Dieses Verfahren wird als Verschlüsselungsalgorithmus bezeichnet. Danach wird die verschlüsselte Nachricht, der Geheimtext, versendet. Der Empfänger kann das Verfahren wieder rückgängig machen, indem er den Entschlüsselungsalgorithmus anwendet und so aus dem Geheimtext wieder den Klartext gewinnt. Bei der Cäsar-Verschlüsselung ist die Verschiebung des Alphabets um eine bestimmte Anzahl an Stellen der Verschlüsselungsalgorithmus, der Entschlüsselungsalgorithmus ist die Verschiebung in die Gegenrichtung. So wird der Buchstabe D zum Beispiel als A verschlüsselt und als D wieder entschlüsselt.[6]

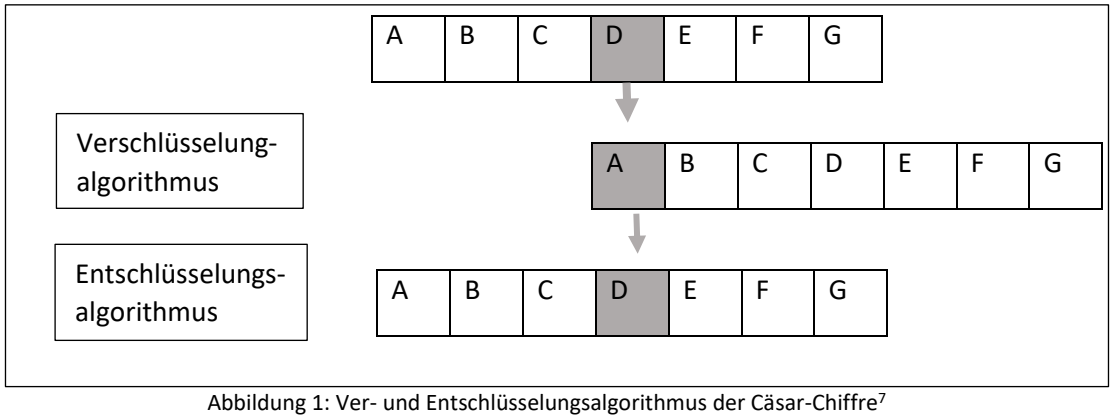

Abbildung 1: Ver- und Entschlüsselungsalgorithmus der Cäsar-Chiffre[7]

Ein weiterer wichtiger Begriff in der Kryptographie ist der sogenannte Schlüssel. Er bezeichnet die Information, die Sender und Empfänger einer Nachricht benötigen, um diese zu verschlüsseln beziehungsweise zu entschlüsseln. Anders als der Algorithmus, das System, welches zur Verschlüsselung angewandt wird, darf der Schlüssel nie an die Öffentlichkeit geraten. Im Fall der Cäsar-Verschlüsselung ist der Schlüssel die genaue

[5] Divus Julius: De Vita Caesarum (Suet. Jul. 56.6 ff) [Übersetzung der Verfasserin]
[6] vgl. Steward, 2016, S.360
[7] Eigene Darstellung [Anmerkung der Verfasserin]

Anzahl an Buchstaben, um die das Alphabet verschoben wird. Diese Zahl kann und sollte für verschiedene Nachrichten geändert werden, das Verfahren bleibt aber das Gleiche. Der holländischen Linguist Auguste Kerckhoff von Nieuwenhof schreibt in seinem Buch „La Cryptograohie Militaire“, dass die Sicherheit eines Kryptosystems nicht von der Geheimhaltung des Algorithmus, sondern nur von der des Schlüssels abhängen darf.[8]

Ein sicherer Schlüssel zeichnet sich unter anderem dadurch aus, dass er möglichst groß ist, das heißt, dass es viele verschiedene Möglichkeiten für ihn gibt und er so schwer erraten werden kann. Der Schlüssel der Cäsar-Chiffre ist zum Beispiel sehr klein, da es nur 25 Möglichkeiten gibt, das Alphabet zu verschieben. Durch Ausprobieren kann ein unbefugter Zuhörer leicht den richtigen Schlüssel finden.[9]

Um sich Kryptosysteme besser vorstellen zu können, werden den beteiligten Personen oft Namen gegeben. Alice möchte Bob eine Nachricht schicken, ohne dass Eve sie lesen kann. Alice und Bob kennen beide den Schlüssel. Eve, die nach dem englischen eavesdropping benannt ist, kennt diese Information nicht und versucht trotzdem, möglichst viele Informationen über die Nachricht zu erhalten.[10]

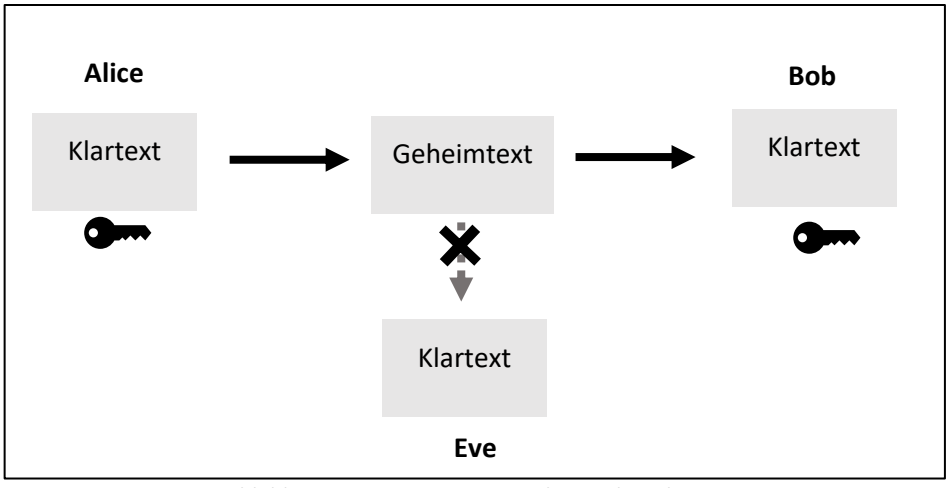

Abbildung 2: Kryptosystem mit Alice, Bob und Eve[11]

[8] vgl. Singh, 2001, S.27
[9] vgl. Devlin, Keith: Sternstunden der modernen Mathematik. -Basel: Birkhäuser Verlag. 1990, S.34
[10] vgl. Wolfgang Tittel, Jürgen Brendel, Nicolas Gisin, Grégoire Ribordy, Hugo Zbinden: Quantenkryptographie. In: Physikalische Blätter, Nr. 55/6, 1999, S.25-30, -Weinheim: WILEY-VCH Verlag GmbH & Co. KGaA. S.26
[11] Eigene Darstellung [Anmerkung der Verfasserin]

2.4. Algorithmen als Funktionen

Damit Computer mit Algorithmen arbeiten können, werden diese heute meistens als Funktionen dargestellt. Der Verschlüsselungsalgorithmus „verschiebe das Alphabet um zwei Stellen“ wird also durch folgende Funktion beschrieben:

$$f(n)=n+2 \pmod{26}$$

Für n wird der Klartext, also die unverschlüsselte Nachricht, eingesetzt. (mod 26) steht für Modulus und bedeutet, dass nach der Zahl 25 wieder bei 0 angefangen werden soll. Dieses Element aus der modularen Arithmetik stellt sicher, dass zum Beispiel ein Z als B verschlüsselt wird.[12]

Da Computer aber mit Bits, also Folgen aus 0 und 1, arbeiten, werden Verschlüsselungen meistens im ASCII-Code gerechnet. Dieser ordnet jedem Buchstaben eine Binärzahl zu.

2.5. Sicherheit von Algorithmen

Die Kryptoanalyse versucht, den Sinn einer Nachricht ohne dazugehörigen Schlüssel zu entziffern. Damit eine Verschlüsselung nicht entziffert werden kann, ist neben einem großen Schlüssel auch ein Verfahren nötig, welches keine Regelmäßigkeiten im Geheimtext erkenne lässt. In einem Text, der mit dem Cäsar-Verfahren verschlüsselt ist, lässt sich zum Beispiel immer noch gut erkennen, welcher Buchstabe am häufigsten vorkommt. Dieser Buchstabe entspricht in der deutschen Sprache meistens dem E. Bei einem ausreichend langen Text kann so der gesamte Schlüssel mithilfe einer Häufigkeitstabelle der Zeichen ermittelt werden. Eine Art, dieses Problem zu umgehen, sind polyalphabetische Schlüssel. Da nicht jeder Buchstabe auf dieselbe Art verschlüsselt wird, sind auch keine Regelmäßigkeiten im Geheimtext zu erkennen.[13] Die sicherste polyalphabetische Chiffre wäre eine, deren Schlüssel genauso lange ist wie die Nachricht selbst. Zum Beispiel würde zu jedem Buchstaben im ASCII-Code ein weiterer im Modulus 1 addiert werden. So können sicher keine Regelmäßigkeiten erkannt werden, außerdem ist der Schlüssel sehr groß. Der einzige Nachteil dieser Verschlüsselungsmethode, one-time-pad genannt, ist, dass der lange Schlüssel

[12] vgl. Steward, 2016, S.361f
[13] vgl. Singh, 2001, S.65ff

ausgetauscht werden muss, wobei er abgefangen werden könnte.[14] Diese Methode ist deshalb nur für sehr brisante, seltene Kommunikationen zu benutzen. Der heiße Draht zwischen dem amerikanischen und russischen Präsidenten wird zum Beispiel durch ein one-time-pad gesichert.[15]

2.6. Kryptographie und Internet

Mit der Erfindung des Computers und der Entwicklung des Internets veränderte sich die Kryptographie drastisch. Zum Einen gab es jetzt leistungsfähige Maschinen, die komplizierte Algorithmen durchführen und eine große Menge an Schlüsseln in kurzer Zeit ausprobieren konnten. Außerdem wurde die Verschlüsselung von Nachrichten zu einem Thema, das viele Menschen betraf. Nicht nur Nachrichten über Truppenpositionen oder geheime Gespräche zwischen Präsidenten sollten verschlüsselt werden, sondern auch die privaten Konversationen der Internetbenutzer. Anders als bei früheren Kryptosystemen müssen sich Bob und Alice nicht persönlich kennen, außerdem ist es für Eve einfacher geworden, eine Nachricht abzufangen. Eine weitere Herausforderung ist, dass plötzlich Millionen Menschen spontan sicher miteinander kommunizieren wollen, nicht nur einzelne Personen.[16] Dadurch wären bei nur 500 Internetbenutzern, die alle miteinander kommunizieren wollen, $\binom{n}{2} = \frac{n\,(\mathrm{n}-1)}{2}$, also 124750 Schlüsselpaare nötig.[17]

Das größte Problem ist aber die sichere Schlüsselübergabe. Obwohl die Kommunikation spontan passiert und sich Alice und Bob nicht persönlich kennen, müssen sie zuvor einen Schlüssel ausgetauscht haben. Dies kann nicht über das Internet passieren, da er dafür wieder verschlüsselt sein müsste.[18] Deshalb werden in den nächsten Kapiteln zwei Verfahren vorgestellt, die dieses Problem umgehen. Für die erste Methode müssen keine Schlüssel im Vorhinein ausgetauscht werden, die zweite generiert mithilfe von polarisiertem Licht einen Schlüssel, der nicht abgefangen werden kann.

---

[14] vgl. Wolfgang Tittel, 1999, S.26
[15] vgl. Singh, 2001, S. 156
[16] vgl. Singh, 2001, S.308
[17] vgl. Hannesschläger, Thomas. Einführung in Die Public-Key Kryptographie [!] Mittels RSA Und Knapsack-Methoden. (Dipl. Arb.) -Salzburg: Universität Salzburg. 2002. S.37
[18] vgl. Singh, 2001, S. 305

3. Public Key Verfahren

Das Grundkonzept für Public Key Verfahren wurde 1975 von Whitfield Diffie und Martin Hellman entwickelt. Sie wollten das Problem des Schlüsselaustausches umgehen, indem sie verschiedene Schlüssel für die Verschlüsselung und Entschlüsselung benutzten. So war kein Schlüsselaustausch und das damit verbundene Sicherheitsrisiko nötig.[19] Das Prinzip wird am Besten durch folgendes Beispiel erläutert: Bob möchte Alice eine Nachricht senden. Dazu bekommt er von Alice ein Vorhängeschloss, mit welchem er die Kiste, in der seine Nachricht liegt, verschließt. Bob kann das Schloss selbst nicht mehr öffnen, da Alice ihm nie den Schlüssel dazu gegeben hat, mit dem sie selbst die Kiste aufsperren und die Nachricht lesen kann. Eve hatte keine Möglichkeit, den Schlüssel abzufangen, da Alice ihn nie versendet hat. Das Schloss wird als Public Key bezeichnet, jeder, auch Eve, darf ihn sehen. Der Schlüssel aber, Private Key genannt, wird von Alice geheim gehalten und mit niemandem geteilt.[20]

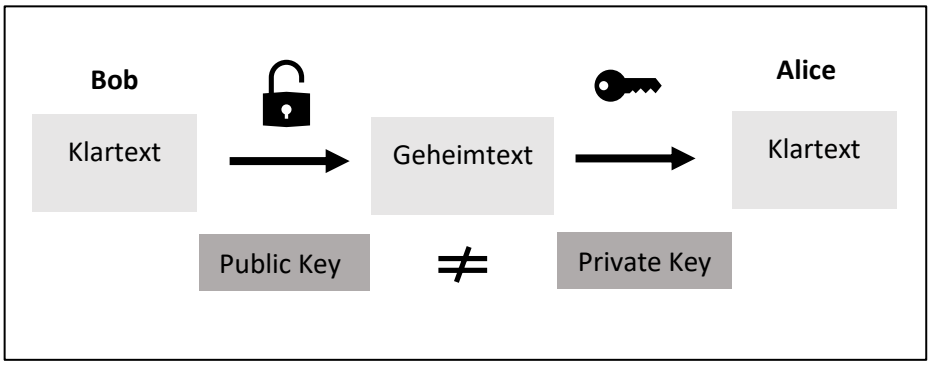

Abbildung 3: Grundprinzip Public Key Verfahren[21]

Diffie und Hellman fanden aber keine mathematische Funktion, mit der sie ihr Prinzip in die Praxis umsetzen konnten und veröffentlichten ihre Idee ohne ein konkretes Verfahren.

> *„As such, a public key cryptosystem is a multiple access cipher. A private conversation can there- fore be held between any two individuals regardless of whether they have ever communicated before. Each one sends messages to the other enciphered in the receiver' s public enciphering key and deciphers the messages he receives using his own secret deciphering key. We propose some techniques for developing public key cryptosystems, but the problem is still largely open."*[22]

[19] vgl. Devlin, 1990, S. 37f.

[20] vgl. Hannesschläger, 2002, S. 38

[21] Eigene Darstellung [Anmerkung der Verfasserin]

[22] Diffie, Whitfield; Hellman, Martin: New directions in Cryptography. In: IEEE Transactions on Information Theory, 22,6, 1976, S.644-654.- Piscataway: IEEE Information Theory Society. S. 644

3.1. Einwegfunktionen

Ein Verfahren, das in eine Richtung einfach durchzuführen, aber schwer rückgängig zu machen ist, bezeichnet man in der Mathematik als Einwegfunktion, wobei zwischen echten Einwegfunktionen und Einwegfunktionen mit Trapdoor unterschieden wird.

3.1.1. Echte Einwegfunktionen

Eine Funktion f wird als echte Einwegfunktion bezeichnet, wenn es ein leicht durchführbares Verfahren zur Bestimmung von f(x) gibt, aber keines zur Berechnung des x-Wertes aus einem beliebigen Funktionswert f(x).

Ein einfaches Beispiel für eine derartige Verschlüsselung wäre ein Verschlüsselungsalgorithmus, der auf einem Telefonbuch basiert. Jeder Buchstabe wird einzeln verschlüsselt, in dem eine beliebige Telefonnummer einer Person mit diesem Anfangsbuchstaben angegeben wird. So ist eine Nachricht in wenigen Minuten verschlüsselt, zur Entschlüsselung müsste man aber das gesamte Telefonbuch nach den übermittelten Nummern durchsuchen, was ohne Computer oder ähnliche Hilfsmittel fast unmöglich ist.[23]

3.1.2. Einwegfunktionen mit Trapdoor

Eine Funktion f wird als Einwegfunktion mit Falltüre (=Trapdoor) bezeichnet, wenn es ein leicht durchführbares Verfahren zu Bestimmung von f(x) gibt und es effizient möglich ist, den x-Wert zu einem beliebigen Funktionswert zu berechnen, wobei dazu eine zusätzliche Information benötigt wird.

Nach so einer Funktion suchten Diffie und Hellemann. Alice kann problemlos f(x) als Geheimtext berechnen, wobei es für Eve unmöglich ist, die Funktion umzukehren und den Klartext x zu erfahren. Bob aber, der die zusätzliche Information besitzt, kann diese Einwegfunktion mit Falltüre einfach rückgängig machen und x ermitteln.[24]

3.2. Das RSA-Verfahren

Das erste praktisch anwendbare Public-Key-Verfahren wurde nicht von Diffie und Hellemann, sondern von drei Forschern des MIT-Labors für Computerwissenschaften

[23] vgl. Hannesschläger, 2002, S. 41f.
[24] vgl. Singh, 2001, S.328

in Amerika entwickelt.[25] Leonard Adelman, Ron Rivest und Adi Shamir suchten nach einer Funktion, wie sie im Artikel „New directions in Cryptography“ beschrieben wurde, und erfanden so das RSA-Verfahren, das nach seinen drei Erfindern benannt ist. Im folgenden Abschnitt wird das Verschlüsseln und Entschlüsseln einer Nachricht mithilfe dieses Verfahrens beschrieben.[26]

Bob möchte Alice eine Nachricht senden. Dazu wählt Alice zwei beliebige, sehr große Primzahlen p und q aus. Mit diesen berechnet sie N, das Produkt von p und q. Außerdem wählt Alice eine Zahl e, die teilerfremd mit (p-1)(q-1) ist. Sie übermittelt Bob die Zahlen N und e, den öffentlichen Schlüssel. Diese beiden Zahlen darf jede andere Person, auch Eve, sehen, deshalb kann Alice sie über einen ungesicherten Kanal verschicken oder im Internet veröffentlichen. Mithilfe der Formel ed=1 (mod(p-1)(q-1)) kann sie mit dem Euklidischen Algorithmus die Zahl d, ihren privaten Schlüssel, ermitteln. Diese Zahl d wird nur zum Entschlüsseln der Nachricht benötigt, Alice hält sie deshalb geheim.[27]

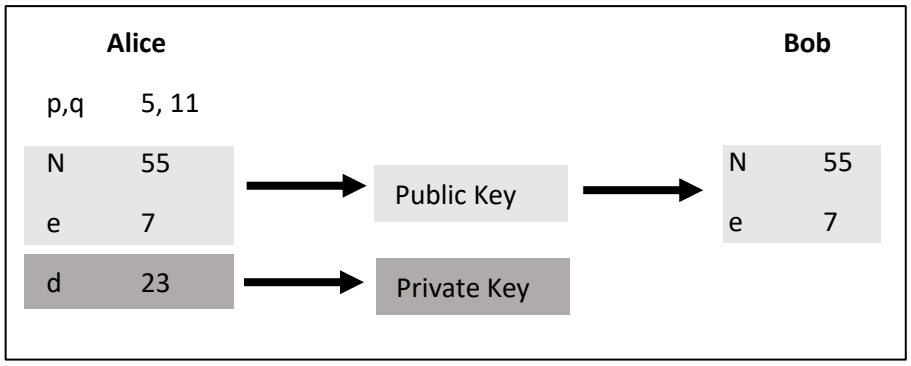

Abbildung 4: Erstellung von Private und Public Key[28]

Bob verschlüsselt seinen in Zahlen umgewandelten Klartext m mit dem Verschlüsselungsalgorithmus

$$c=m^e \pmod n$$

zum Geheimtext c. Da diese Rechenoperation nicht effizient rückgängig gemacht werden kann, spricht man von einer Einwegfunktion.

[25] vgl. Bourseau, Frank; Fox, Dirk; Thiel, Christoph : Vorzüge und Grenzen des RSA-Verfahrens. In: Datenschutz und Datensicherheit, 26, 2002, S. 84-89. – Wiesbaden: Springer Fachmedien. S. 84
[26] vgl. Singh, 2001, S. 329ff
[27] vgl. Gahleitner, Angelika Maria. Das RSA-Verfahren Im Schulunterricht : Didaktische Aufbereitung Der Mathematischen Grundlagen. (Dipl. Arb.) -Linz: Universität Linz. 2003. S.53ff
[28] Eigene Darstellung [Anmerkung der Verfasserin]

Eve kann von c nicht auf m schließen. Alice aber, die über die Zahl d, den privaten Schlüssel, verfügt, kann mit dem Entschlüsselungsalgorithmus

$$c^d \bmod n = m$$

den Klartext m berechnen.[29]

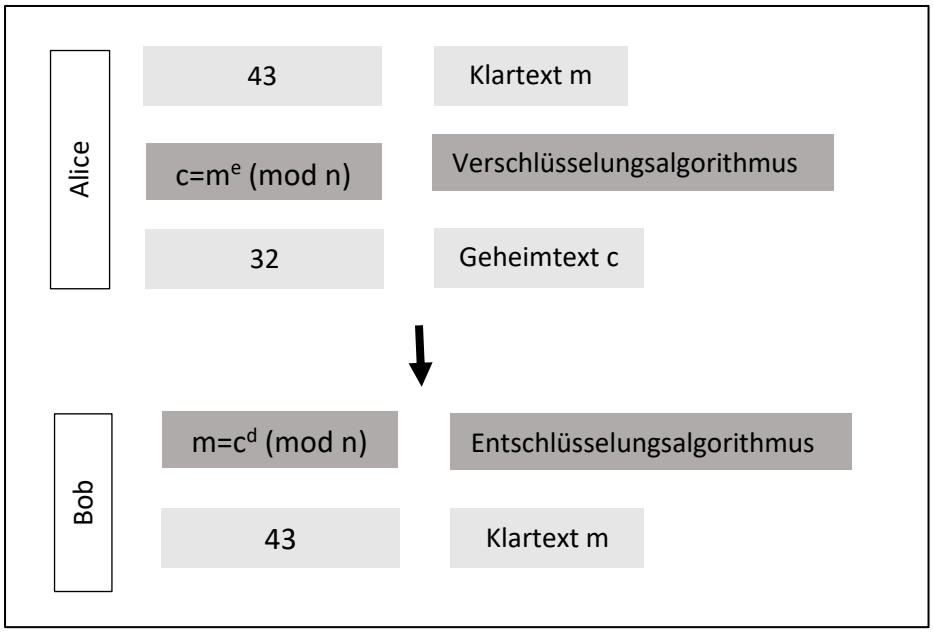

Abbildung 5: Verschlüsselung und Entschlüsselung mithilfe RSA[30]

Da zur Verschlüsselung und Entschlüsselung verschiedene Algorithmen verwendet wurden, nennt man Public-Key-Verfahren auch asymmetrische Verfahren. Nur Alice kann die Nachricht entschlüsseln, da nur sie über den privaten Schlüssel verfügt. Auch Bob kennt diesen nicht, er kann die Nachricht nur verschlüsseln, nicht entschlüsseln, weshalb kein Schlüsselaustausch notwendig ist.

3.3. Signaturen

Ein mögliches Angriffsverfahren auf ein Public-Key-System ist die sogenannte Man-in-the-middle-Methode. Dabei gibt sich Eve entweder als Alice oder als Bob aus, um mit dem anderen zu kommunizieren und so vertrauliche Daten zu erhalten.[31] Deshalb benutzen diese Kryptosysteme digitale Signaturen, um die Authentizität der Gesprächsteilnehmer zu gewährleisten. Wenn Alice eine Nachricht verschickt, sendet

[29] vgl. Steward, 2016, 123f
[30] Eigene Darstellung [Anmerkung der Verfasserin]
[31] vgl. Schrenk, 2007, S.21

sie auch eine Folge an Zahlen, die nur sie erzeugen kann. Bob kann überprüfen, ob sie die Zahlenfolge selbst erstellt hat, diese selbst aber nicht erzeugen.[32]

Im Falle der RSA-Verschlüsselung werden dazu Verschlüsselungs- und Entschlüsselungsalgorithmus vertauscht. Bob kreiert seine Signatur s, indem er einen Text m mit dem Entschlüsselungsalgorithmus verschlüsselt.

$$s= m^d \pmod n$$

Er verschickt diese Signatur s an Alice, die sie mit dem Verschlüsselungsalgorithmus entschlüsselt.

$$m= s^e \pmod n$$

Bob hat auch die unverschlüsselte Botschaft m übermittelt, deshalb kann Alice jetzt ihr Ergebnis damit vergleichen. Da nur Bob den privaten Schlüssel d kennt, konnte nur er diese Nachricht erstellen.[33]

3.4. Angriffsmöglichkeiten

Weil es sich bei den Algorithmen um Einwegfunktionen handelt, ist es nicht möglich, aus dem Geheimtext direkt den Klartext zu gewinnen. Die einzige Möglichkeit, Public-Key-Verfahren unerlaubterweise zu entschlüsseln, ist, den privaten Schlüssel zu rekonstruieren. Im Fall des RSA-Verfahrens muss d berechnet werden. Dazu werden außer dem öffentlichen Schlüssel p und q gebraucht, die berechnet werden können, indem N in seine Primfaktoren zerlegt wird, da N=pq.[34]

Je größer die Zahlen p und q, desto länger und aufwändiger ist die Primfaktorzerlegung, deshalb werden in der Praxis p und q so gewählt, dass ihr Produkt pq größer als 10^{200} ist. Einer der schnellsten bekannten Algorithmen zur Faktorisierung einer Zahl wurde von Richard Schröppel entwickelt und benötigt ungefähr

$$(\ln(n))^{\sqrt{\frac{\ln(n)}{\ln(\ln(n))}}}$$

[32] vgl. Schauer, Stefan: Attack Strategies in Quantum Cryptography. (Dipl.-Arb.) -Klagenfurt: Alpen-Adria-Universität, 2007, S.13
[33] vgl. Hannesschläger, 2002, S. 56
[34] Bourseau, 2002, S.85

einzelne Rechenoperationen. Bei einer Zahl $N>10^{200}$ ergibt das ungefähr $1{,}2 \times 10^{23}$ Operationen. Ein Prozessor, der in der Lage ist, 10^6 Operationen in der Sekunde durchzuführen, braucht dafür ungefähr 4 000 000 000 Jahre.[35]

Das RSA-Verfahren wurde zum ersten Mal in der Zeitschrift „Scientific American" in einer Kolumne namens „Mathematische Spiele" veröffentlicht. Der Autor Martin Gardner forderte die Leserschaft dazu auf, einen 129-stelligen Wert von N in seine Primfaktoren zu zerlegen.

> *„To prove the point, the RSA team provided Gardner with a 128-digit coded message e, computed using a specified 129-digit n, which was the product of mysterious top-secret, 64-digit and 65-digit primes p and q, respectively. They also indicated that s = 9007." [36]*

17 Jahre später, am 26.4.1994, verkündete eine Gruppe von 600 Freiwilligen aus Australien, England, Amerika, Venezuela und Frankreich, die ihre Firmen- und Großrechner zu einem Netzwerk zusammengeschlossen hatten, dass sie p und q berechnet hätten. Da heutige RSA-Verfahren aber mit deutlich größeren Zahlen arbeiten, ist die Faktorisierung deutlich aufwändiger geworden.[37]

Es gibt jedoch Sonderfälle, in denen die Faktorisierung von N deutlich einfacher ist, zum Beispiel wenn die für p und q gewählten Werte nahe aneinander liegen. In diesem Fall liegen sie nämlich in der Größenordnung von $\sqrt{n}$, weshalb sie mit der Methode von Fermat bestimmt werden können. Deshalb sollten sich p und q immer um einige Ziffern in ihrer Länge unterscheiden. Trotzdem darf keine der zwei Zahlen so niedrig sein, dass sie aus Primzahlentafeln entnommen werden können.[38]

3.5. Hybridverfahren

Ein großer Nachteil der Public-Key-Verfahren ist, dass sie in der Praxis deutlich langsamer als symmetrische Verschlüsselungsmethoden sind. Deshalb werden meist sogenannte Hybridverfahren benutzt, welche die Vorteile beider Methoden vereinen.[39] Das erste derartige Verfahren wurde von Phil Zimmermann entwickelt. Er

[35] vgl. Hannesschläger, 2002, S.54
[36] Gardner, Martin: A new kind of cipher that would take millions of years to break. In: Scientific American 237.8, 1977, S.120-124. -New York City: Nature Publishing Group. S. 120
[37] vgl. Singh, 2001, S.337
[38] vgl. Hannesschläger, 2002, 54
[39] Gahleitner, 2003, S. 62

verschlüsselte eine Nachricht mithilfe von IDEA, einem symmetrischen Verschlüsselungsalgorithmus. Damit diese entschlüsselt werden kann, muss der Schlüssel übermittelt werden. Dazu wird dieser mit RSA verschlüsselt, weshalb Alice ihn ohne vorher ausgetauschte Informationen empfangen kann. Public-Key-Verfahren werden also meistens nicht zur Verschlüsselung von Nachrichten benutzt, sondern um Schlüssel für andere Verfahren sicher zu versenden.[40]

3.6. Pretty Good Privacy

Obwohl mit RSA ein Verschlüsselungsverfahren entwickelt wurde, das sichere Kommunikation zwischen vielen Menschen im Internet möglich macht, wurde es zuerst nur von Regierungen, großen Unternehmen und dem Militär eingesetzt, da nur diese ausreichend leistungsfähige Computer besaßen. Phil Zimmermann, der das erste Hybridverfahren entwickelte, wollte diese neue Technologie für alle Menschen zugänglich machen und sein Programm Pretty Good Privacy (PGP), eine Kombination von RSA und dem symmetrischen Verfahren IDEA, veröffentlichen. Aus Angst vor einem Verbot der Software, die es nicht nur Eve, sondern auch dem amerikanischen Staat unmöglich machen würde, Konversationen mitzulesen, veröffentlichte er das Programm 1991 gratis im Internet, anstatt es zu verkaufen. 1993 wurde Zimmermann vom FBI wegen illegalem Rüstungsexport angeklagt, da das Programm auch in anderen Ländern installiert wurde und Verschlüsselungssoftwares in Amerika als Rüstungsgüter, die nur mit Genehmigung des Außenministers exportiert werden dürfen, gezählt werden. Das Verfahren gegen Zimmermann wurde drei Jahre später eingestellt, trotzdem hatte der Fall eine große Debatte zur Folge, ob eine öffentlich zugängliche Verschlüsselungssoftware das Recht auf Privatsphäre sichert oder Verbrechern erlaubt, ohne Wissen des Staates zu kommunizieren.[41]

[40] vgl. Singh, 2001, S. 359f
[41] vgl. Singh, 2001, S. 353ff

4. Quantenschlüsselaustausch

Wie im vorherigen Kapitel beschrieben wurde, beruht die Sicherheit von Public-Key-Verfahren ausschließlich darauf, dass es mit den heutigen Methoden nicht möglich ist, große Zahlen in kurzer Zeit in ihre Primfaktoren zu zerlegen. Mit der Entwicklung von neuen, leistungsfähigeren Computern könnte das in naher Zukunft aber möglich sein. Derzeit setzen viele Kryptoanalytiker ihre Hoffnung auf Quantencomputer. Diese Maschinen benutzen kleinste Teilchen, um Daten zu speichern und zu verarbeiten. Dabei handelt es sich zum Beispiel um Photonen, die in eine bestimmte Richtung polarisiert sind. Aufgrund des Phänomens der Superposition, das im folgenden Abschnitt noch genauer erläutert wird, können diese Teilchen mehrere Zustände gleichzeitig annehmen und so verschiedene Zahlen darstellen. Während ein herkömmlicher Computer, der mit Bits, also einer Folge aus 0 und 1 arbeitet, immer eine Zahl nach der anderen testen muss, um die Primfaktoren einer Zahl zu ermitteln, kann ein Quantencomputer mehrere Rechenoperationen gleichzeitig ausführen, eine Primzahlenzerlegung in einem Bruchteil der Zeit durchführen und so die RSA-Chiffre knacken.[42]

Es scheint also, als würde das Aufkommen von Quantencomputern einen großen Vorteil für die Kryptoanalyse bedeuten. Jedoch kommt aus dem Bereich der Quantenmechanik auch ein System für die Verschlüsselung, die sogenannte Quantum Key Distribution, kurz QKD. Wie der Name schon sagt, ermöglicht dieses Verfahren, einen Schlüssel aus zufälligen Bitfolgen zu generieren und diesen so zu verteilen, dass Unbeteiligte diesen nicht unbemerkt abfangen können.[43] Dafür wird eine Eigenschaft der Quantenmechanik benutzt, laut der die Beobachtung eines Teilchens zwangsläufig dessen Zustand verändert. Probiert Eve also, den Schlüssel heimlich mitzulesen, verändert sie diesen unbewusst, was Bob und Alice auffällt. Wird der Schlüssel nach der Übertragung als sicher eingestuft, kann Bob ihn dazu benutzen, seine Botschaft mithilfe eines herkömmlichen Chiffrierverfahrens, zum Beispiel als One-Time-Pad, zu

[42] vgl. Singh, 2001, S.395ff

[43] vgl. Schrenk, Bernhard: Polarisationsnachregelung über Lange Glasfaserstrecken Für Quantenkryptographie. (Dipl.-Arb.) -Wien: Technische Universität, 2007, S.7

verschlüsseln.[44] QKD-Systeme sind also aufgrund gewisser physikalischer Gesetze beinahe immun gegen Hacking-Angriffe.

4.1. Physikalische Voraussetzungen

Um die verschiedenen Kryptosysteme, die unter dem Begriff QKD zusammengefasst werden, verstehen zu können, muss man mit einigen quantenphysikalischen Phänomenen vertraut sein. Quantenphysik beschreibt generell das Verhalten von Teilchen auf einer sehr kleinen Ebene.

Licht wird in der modernen Physik sowohl als Welle als auch als Teilchen betrachtet. Es gibt Experimente, in denen bei Licht eindeutige Wellenphänomene wie zum Beispiel Interferenz oder Beugung beobachtet werden können. Andere Phänomene, wie zum Beispiel der Photoelektrische Effekt können nur erklärt werden, wenn man davon ausgeht, dass Licht aus einzelnen Teilchen, sogenannten Photonen, besteht.[45] Bei QKD-Systemen wird meistens von der Teilchentheorie des Lichtes ausgegangen, für die Übertragung von der Wellentheorie.

Licht, das von einer Quelle wie zum Beispiel einer Glühbirne oder der Sonne gesendet wird, kommt in vielen unterschiedlichen Wellenlängen und Schwingungsrichtungen vor. Auf die Teilchentheorie übertragen bedeutet das, dass die Photonen derselben Lichtquelle in unterschiedliche Richtungen schwingen. Mithilfe eines Polarisationsfilters werden nur die Photonen durchgelassen, die in dieselbe Richtung schwingen. Dieses Prinzip wird zum Beispiel von Sonnenbrillen oder Kameras genutzt.[46]

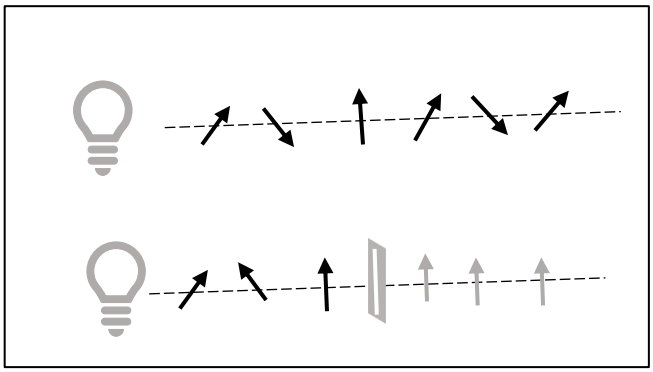

Abbildung 6: Polarisation einzelner Photonen[47]

[44] vgl. Wolfgang Tittel, 1999, S.26
[45] vgl. Hawking, Stephen; Mlodinow, Leonard: The Grand Design. -London: Transworld Publishers. S.73ff
[46] vgl. Singh, 2001, S.401f
[47] Eigene Darstellung [Anmerkung der Verfasserin]

Polarisationsfilter können auch als Detektoren benutzt werden, die herausfinden, in welche Richtung das Licht zuvor polarisiert wurde. Dabei ist es aber nur möglich, zwischen zwei Zuständen zu unterscheiden.

Photonen können auch durch andere Eigenschaften wie zum Beispiel dem Spin beschrieben werden. Der Spin ist der Drehimpuls eines Teilchens und beträgt ein Vielfaches des Planckschen Wirkungsquantums. Genau wie die Masse ist der Spin eine unveränderliche Eigenschaft eines Teilchens.[48]

4.2. Entstehung

Die erste Person, die auf den Gedanken kam, Quantenzustände von Photonen zu nutzen, um geheime Informationen zu speichern, war der amerikanische Physiker Stephen Wiesner. Er entwickelte als Gedankenexperiment eine Methode, Dollar-Scheine fälschungssicher zu machen, indem er sie mit verschieden polarisierten Photonen bestückte. Ein Fälscher müsste die Polarisation jedes Teilchens einzeln messen, was nur gelingen würde, wenn er die richtigen Polarisationsfilter benutzte. Andernfalls würde der Zustand wie oben beschrieben verändert und ein zufälliges Ergebnis zurückgeliefert. Dieses Quantengeld wäre in der Realität aber zu teuer, außerdem ist es nicht möglich, einzelne Photonen über einen langen Zeitraum festzuhalten. Wiesner teilte diese Idee aber mit einem befreundeten Forscher, Charles Bennett. Gemeinsam mit weiteren Physikern entwickelte dieser als Forscher des IBM die ersten QKD-Protokolle.[49]

4.3 Protokolle

Es gibt verschiedene Varianten, sogenannte Protokolle, ein QKD-System aufzubauen. Einige davon werden im folgenden Abschnitt genauer beschrieben.

4.3.1 BB84

Es wird wieder von dem typischen Problem der Kryptographie ausgegangen: Bob möchte Alice eine Nachricht schicken, ohne dass Eve mitlesen kann.[50] Dazu sendet Alice präparierte Photonen aus. Sie hat vier verschiedene Polarisationsfilter, die sie

[48] Vgl Al-Khalili, Jim: Quantum. A guide to the perplexed. -London: W&N, 2012. S.153ff
[49] vgl. Singh, 2001, S.403ff
[50] vgl. Wolfgang Tittel, 1999, S. 26

zufällig nacheinander benutzt.[51] Folglich entstehen Photonen, die zufällig horizontal (H), vertikal (V), -45° oder +45° polarisiert sind. Diese vier Quantenzustände werden in klassische Bits umgewandelt, wobei immer zwei Zustände 0 beziehungsweise 1 zugeordnet werden. Vertikal und -45° polarisierte Photonen entsprechen 1, horizontal und +45° 0 in digitalen Bits. Ein Bit entspricht so mit zwei Quantenzuständen, zwei verschiedenen quantum bits (qubits). Alice notiert sich, in welche Richtung sie die Photonen polarisiert hat. Diese manipulierten Photonen, welche einer zufälligen Abfolge von 0 und 1 entsprechen, verschickt sie jetzt an Bob.[52]

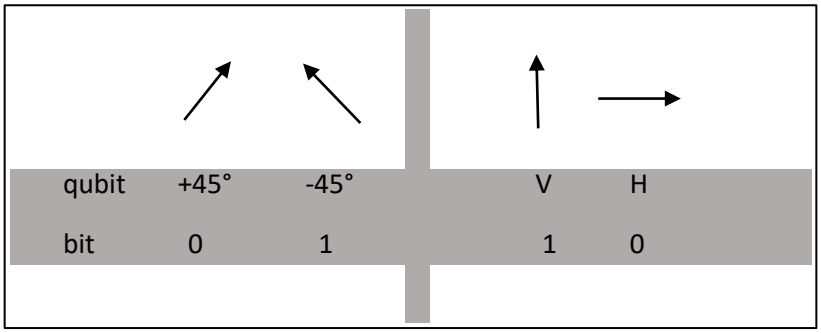

Abbildung 7: Zusammenhang zwischen qubits und bits[53]

Bob hat zwei Detektoren, mit denen er die Polarisation der ankommenden Photonen messen kann. Der erste unterscheidet zwischen horizontalen und vertikalen Photonen, der zweite zwischen -45° und +45°. Ein Photon kann immer nur mit einem der Filter gleichzeitig gemessen werden. Probiert Bob aber, ein Photon, das vertikal polarisiert ist, mit dem zweiten Detektor zu messen, bekommt er auch ein Ergebnis: das Photon muss sich „entscheiden“, ob es sich H oder V verhält und passiert so den Detektor. Bob bekommt folglich einen Zustand übermittelt, der nicht mit Alice Aufzeichnungen übereinstimmt.[54]

Nach der Übertragung der Photonen haben Bob und Alice eine Reihe von Messungen, die in Bits umgewandelt werden, die in den Fällen übereinstimmen, in denen Bob durch Zufall die richtige Messbasis gewählt hat. Nach den Gesetzen der Wahrscheinlichkeit passiert das bei einer großen Anzahl an Versuchen bei 50% der gemessenen Photonen. Die übrige Hälfte der Photonen wurde mit dem falschen Filter

[51] vgl. Schrenk, 2007, S.8f
[52] vgl. Hipp, 2016, S.23
[53] Eigene Darstellung [Anmerkung der Verfasserin]
[54] vgl. Wolfgang Tittel, 1999, S. 27

untersucht und hat sich so spontan für einen Zustand entschieden. Deshalb hat sich Bob auch bei 50% der falsch gemessenen Photonen das richtige Ergebnis notiert.[55]

Bob und Alice tauschen jetzt über einen öffentlichen Kanal aus, wann sie welche Basis benutzt haben. Nur jene Ergebnisse, bei denen beide dieselbe benutzt haben, sind weiterhin relevant und werden als Distilled Key bezeichnet. Aufgrund technischer Fehler oder einem Spion, Eve, der einzelne Photonen manipuliert, können aber immer noch Unterschiede vorhanden sein.[56]

Im nächsten Schritt wird ein Teil des Schlüssels zwischen Bob und Alice ausgetauscht. Je nachdem wie viele Messergebnisse übereinstimmen, wird eine Fehlerrate ermittelt. Liegt diese über einem bestimmten Wert, ist es sehr wahrscheinlich, dass ein Spion in das System eingreift, daher wird die gesamte Bit-Folge verworfen.[57] Danach folgen verschiedene weitere Schritte, in denen die Schlüssel weiter überprüft und dabei verkürzt werden. Folglich ist die Folge an 0 und 1 am Ende des Verfahrens deutlich kleiner als zu Beginn.

Die so entstandene Bit-Folge kann zum Beispiel für die Verschlüsselung als One-Time-Pad benutzt werden.[58]

4.3.2. BBM92

Dieses Verfahren basiert auf einem Gedankenexperiment von Einstein, Podolsky und Rosen über die Natur von verschränkten Teilchen oder EPR-Pärchen, wie sie nach den drei Physikern benannt wurden. Dabei handelt es sich um kleine Teilchen, zum Beispiel Photonen, deren Quantenzustände durch ihre Entstehung untrennbar miteinander verbunden sind.[59] Zum Beispiel entsteht aufgrund des Erhaltungssatzes aus einem Teilchen mit dem Spin 0 zwei Teilchen mit genau entgegengesetztem Spin, ½ und – ½ . Der genaue Spin des einzelnen Teilchens ist unbekannt, sobald wir aber einen der beiden kennen, können wir auf den Zustand des anderen schließen.[60] Einstein, Podolsky und Rosen wollten beweisen, dass diese Informationen schon im Vorhinein

[55] vgl. Hipp, 2016, S.24
[56] vgl. Schrenk, 2007, S.9
[57] vgl. Singh, 2001, S.416
[58] vgl. Hipp, Florian Peter: Novel Schemes for QKD.(Dipl.-Arb.) -Wien: Technische Universität, 2016
[59] Al-Khalili, 2012, S.91ff
[60] Zarda, Patrick: Quantenkryptographie.(Dipl.-Arb.)-Innsbruck: Universität Innsbruck, 1999. S. 26

ausgetauscht wurden, damit kein Informationsaustausch zwischen den Teilchen im Moment der Messung geschehen muss, was womöglich mit Überlichtgeschwindigkeit passieren müsste, wodurch Einsteins Relativitätstheorie verletzt werden würde. Im Jahr 1964 schlug Bell ein Experiment vor, um diesen Disput zu lösen. Es stellte sich heraus, dass Einstein Unrecht hatte und Informationen zwischen den Teilchen ausgetauscht werden können.[61] Dieser Versuchsaufbau wurde 1991 von A. Ekert als kryptographisches System vorgeschlagen.

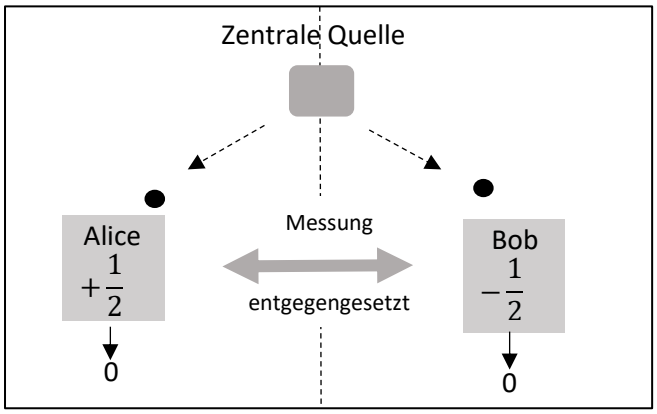

Abbildung 8: Schematischer Versuchsaufbau BBM92[62]

Eine zentrale Quelle erzeugt verschränkte EPR-Pärchen und schickt je eines der Teilchen an Alice und Bob, die zufällig aus drei verschiedenen Detektoren auswählen. Misst Alice einen Spin von ½, muss Bob aufgrund der Verschränkung – ½ messen. Wie beim BB84-Protokoll tauschen sich beide über einen öffentlichen Kanal über die benutzten Detektoren aus und streichen alle Messergebnisse, bei denen sie unterschiedliche benutzt haben. Diese Einträge können aber mit Hilfe der Bell-Ungleichung dazu benutzt werden, mögliche Spione ausfindig zu machen und die Sicherheit des Verfahrens so weiter zu erhöhen. Die übrigen Messergebnisse werden wie beim BB84-Protokoll weiter verkürzt und gesiebt, bis ein sicherer Schlüssel entsteht.[63]

4.4. Übertragung

Wie in den vorherigen Abschnitten erklärt wurde, existieren schon verschiedene QKD-Protokolle, die in der Theorie oder in Labors funktionieren. Eine der größten

[61] Wolfgang Tittel, 1999, S. 28
[62] Eigene Darstellung [Anmerkung der Verfasserin]
[63] vgl. Zarda, 1999, S. 26

Schwierigkeiten, die es zu bewältigen gilt, um diese Technologien auch im Alltag einsetzbar zu machen, ist die Übertragung der präparierten Photonen, ohne dabei Informationen zu verlieren.

4.4.1. Freiraum

Im Zuge des ersten praktischen QKD-Experimentes, welches 1989 von Forschern des IBM durchgeführt wurde, verschickte man polarisierte Photonen über 30 cm Luftweg.[64] Auch bei späteren Experimenten wurde oft auf Freiraumübertragung gesetzt, da die Atmosphäre im Vergleich zu Glasfaserkabeln nicht doppelbrechend wirkt und daher den Polarisationszustand eines Photons nicht verändern kann.[65]

Für Freiraumübertragungen werden Wellenlängen zwischen 770 und 860nm benutzt, wodurch Übertragungsrate und Effizienz der Detektoren begünstigt werden. Damit man bestehende Systeme verwenden kann, werden auch Signale mit einer Wellenlänge von bis zu 1550nm versendet, wobei jedoch Detektoren zur Messung der Polarisation nicht mehr effizient funktionieren.

Ein weiteres Problem ist, dass zwischen Sender und Empfänger freie Sichtverbindung bestehen muss. Um dies zu gewährleisten, wird bei klassischen Systemen der Lichtstrahl dazu künstlich ausgeweitet, damit ein Teil des Lichtes in jedem Fall beim Empfänger ankommt. Bei QKD-Systemen würden dazu aber zu viele einzelne Photonen verloren gehen, was die Übertragung sehr langsam und nicht mehr funktionstüchtig machen würde.

Außerdem sind Freiraumsysteme stark abhängig von äußeren Umständen wie Luftdruck, Temperatur und Luftfeuchtigkeit, da sich der Lichtstrahl je nach Wetterlage anders ausbreitet. Auch geographische Lage und unterschiedliche Tages- und Nachtzeiten spielen eine Rolle, ebenso mechanische Erschütterungen, wie sie im städtischen Raum oft vorkommen.

Bei der Übertragung mithilfe eines Satelliten, wie es zum Beispiel beim BBM92-Protokoll angedacht wäre, sind diese Komplikationen weniger relevant, da diese nur

[64] vgl. Wolfgang Tittel, 1999, S. 28
[65] vgl. Schrenk, 2007, S. 18

innerhalb der Atmosphäre auftreten und der Lichtstrahl sich dadurch die größte Zeit unbeeinflusst fortbewegen kann.[66]

4.4.2. Glasfaserkabel

Bei einer Wellenlänge von 800nm können zwar billige und gute Detektoren benutzt werden, aber die Dämpfungsrate ist ziemlich hoch, weshalb die Anwendung nur auf kurze Distanzen sinnvoll ist.[67] Bei höheren Wellenlängen müssen zwar andere, ungenauere Detektoren benutzt werden, trotzdem sind mit dieser Methode längere Übertragungen in bereits existierenden Netzwerken möglich, wie schon bei mehreren Experimenten gezeigt wurde.[68]

> *„Wir verschickten (…) polarisierte Photonen über eine Strecke von 23 km unterhalb des Genfer Sees, wozu wir uns des Telekommunikations-Fasernetzes der Swisscom bedienten.“*[69]

Auch bei diesen Wellenlängen wird die Strecke von der Dämpfung des Glasfaserkabels begrenzt. Aufgrund verschiedener physikalischer Phänomene erreichen nicht alle Photonen den Empfänger, ein Effekt, der mit zunehmender Strecke größer wird. Um diesem entgegenzuwirken, werden bei klassischen Systemen Zwischenverstärker integriert. Diese sind bei Quantensystemen aber nicht anwendbar, da laut dem No-Cloning-Theorem ein einzelnes Photon nicht nachgebildet und so nicht verstärkt werden kann, weshalb Quantenzustände wie die genaue Polarisation eines Teilchens verloren gehen würden. Außerdem sind auch Glasfaserkabel stark von äußerlichen Umständen wie Temperaturschwankungen abhängig.[70]

4.5. Fehlerrate

Die sogenannte Quantenbit-Fehlerrate beschreibt die fehlerhaft übertragenen qubits im Vergleich zur Gesamtzahl und ist eine Kennzahl der Effizienz eines QKD-Systems. Eine fehlerhafte Übertragung kann zum Beispiel dadurch hervorgerufen werden, dass sich der Polarisationszustand eines Photons während der Übertragung verändert. Dies kommt aufgrund der Doppelbrechung optischer Fasern jedoch selten vor. Eine weitere Fehlerquelle wird „Rauschen der Detektoren“ genannt. Wenn ein Photon nicht

[66] vgl. Schrenk, 2007, S.18ff
[67] vgl. Wolfgang Tittel, 1999, S. 29
[68] vgl. Schrenk, 2007, S.15
[69] Wolfgang Tittel, 1999, S. 29
[70] vgl. Schrenk, 2007, S. 16

ankommt, ist es möglich, dass ein beliebiger Detektor in dem Moment anspringt, in dem es theoretisch angekommen wäre. Auch Ungenauigkeiten bei der Polarisierung können dazu führen, dass Bob Photonen anders misst, als Alice sie versendet hat. All diese Fehlerquellen führen dazu, dass die Messergebnisse von Versender und Empfänger nicht übereinstimmen, ohne dass Photonen abgefangen wurden. Deshalb ist es wichtig, die Quantenbit-Fehlerrate möglichst gering zu halten, um Abhörversuche von technischen Fehlern unterscheiden zu können.[71]

4.6. Attack Strategies

Der größte Vorteil der vorgestellten QKD-Systeme ist, dass ihre Sicherheit ausschließlich auf physikalischen Gesetzen beruht. Unabhängig davon, wie viel Zeit ein Spion zu Verfügung hat und wie ausgereift seine technischen Hilfsmittel sind, wird es ihm auch in Zukunft nicht möglich sein, unbemerkt an Informationen über den Schlüssel zu gelangen. Trotzdem gibt es einige Methoden, die Eve benutzen kann, um die Polarisation der Photonen zu erfahren. Diese funktionieren aber ausschließlich durch technische Fehler im Versuchsaufbau, die aus heutiger Sicht nicht zu beheben sind.

4.6.1. Man in the Middle

Diese Methode ist zwar keine direkte Abhörstrategie, erlaubt Eve aber trotzdem, Nachrichten mitzulesen. Sie gibt sich in der Konversation abwechselnd als Alice oder Bob aus, und erfährt so Inhalte, die die beiden geheim halten wollten. Um diesen Angriff zu vermeiden, beinhaltet jedes QKD-System eine sogenannte Signatur, mit der die Authentizität des Seders und Empfängers gewährleistet wird. Meist ist diese ein Stück des Schlüssels der vorherigen Übertragung, der nicht zur Verschlüsselung eingesetzt wurde und mit dem Bob sich Alice gegenüber ausweist. Sie kann sich jetzt sicher sein, wieder mit derselben Person zu kommunizieren.[72]

4.6.2. Intercept-resend

Bei dieser Methode misst Eve jedes Photon, das von Alice gesendet wird. Genau wie Bob hat sie zwei verschiedene Detektoren, von denen sie einen auswählt, da es nicht

[71] vgl. Wolfgang Tittel, 1999, S.28
[72] vgl. Schrenk, 2007, S. 21

möglich ist, beide gleichzeitig zu benutzen. Benutzt Eve den falschen, verfälscht sie damit nicht nur möglicherweise ihr Messergebnis, sondern ändert auch, wie oben beschrieben, die Polarisation des Photons. Folglich erhält Bob ein Signal, bei dem 50% der Teilchen durch Eve verändert wurden.[73] Diese Veränderung wirkt sich so auf die Fehlerrate aus, da sich Bobs Ergebnisse stark von Alice Aufzeichnungen unterscheiden. Alice und Bob bemerken Eve mit der Wahrscheinlichkeit

$$P = 1 - (\frac{1}{2})^n,$$

wobei n die Anzahl der gemessenen Photonen ist. Die Wahrscheinlichkeit, dass Eve einen falschen Detektor benutzt, steigt mit jedem gemessenen Photon.[74]

Eve könnte dieses Problem umgehen, indem sie das Photon zuerst kopiert, eines der Photonen misst und das zweite an Bob weiterschickt. Sie könnte das erste Photon auch ein zweites Mal duplizieren und so beide Filter anwenden, um mit Sicherheit ein korrektes Ergebnis zu erhalten. Laut des No-Cloning-Theorems kann aber der allgemeine Quantenzustand eines Teilchens nicht kopiert werden.[75] Dies wurde zum ersten Mal 1982 von den Physikern Wootters und Zurek bewiesen. In einem wissenschaftlichen Artikel setzten sie sich mit den Möglichkeiten, die durch geklonte Teilchen entstehen würden, auseinander und kamen aber zu dem Schluss, dass dies physikalisch unmöglich sei.

> *„If [the cloning of photons] were [possible], the amplifying process could be used to ascertain the exact state of a quantum system: in the case of a photon, one could determine its polarization by first producing a beam of identically polarized copies and then measuring the Stokes parameters. We show here that the linearity of quantum mechanics forbids such replication and that this conclusion holds for all quantum systems."*[76]

Da sich dieses Gesetzt auch in Zukunft nicht ändern wird, ist es Eve unmöglich, ein Photon zu kopieren, weshalb sie mit der oben genannten Wahrscheinlichkeit von Bob und Alice bemerkt wird.

[73] vgl. Hipp, 2016, S.14
[74] vgl. Schauer, 2007, S.60
[75] vgl. Zarda, 1999, S.29
[76] Wootters, William; Zurek, Wojciech: A single quantum cannot be cloned. In: Nature, Nr. 299, 1982, S.802–803. -Berlin: Springer Nature Publishing AG. S. 802

4.6.3 Photon-Number-Splitting

Obwohl bei allen QKD-Systemen von einzelnen Photonen, die alle zufällig und unterschiedlich polarisiert werden, ausgegangen wird, können diese derzeit noch nicht technisch erzeugt werden. Deshalb werden sogenannte abgeschwächte Pulse benutzt, die im Idealfall aus einem Photon, oft aber auch aus null, zwei oder mehreren bestehen.[77] Eve könnte deshalb bei Signalen, die aus mehreren Photonen bestehen, eines unbemerkt entfernen und messen, ohne dass Bob es bemerkt. Jene Signale, die aus einzelnen Photonen bestehen, unterdrückt Eve einfach.[78]

Diese Angriffsmethode ist nicht nur technisch aufwendig und fehlerhaft, kann aber auch durch sogenannte Decoy-States unmöglich gemacht werden. Dabei handelt es sich um Signale, die gezielt mehr als ein Photon enthalten und an denen so gemessen werden kann, ob Teilchen am Weg verloren gehen.

4.6.4. Denial of Service

Die einfachste Methode, sicheren Austausch zwischen Alice und Bob zu verhindern, ist die Störung der Übertragung der Signale, indem das Glasfaserkabel durchtrennt wird beziehungsweise die Signale im freien Raum blockiert oder mit anderer Strahlung überlagert werden. Eve erfährt so zwar nicht den Inhalt der Nachricht, macht aber jegliche Kommunikation über das System unmöglich und zwingt die beiden so, einen anderen, unsicheren Kanal zu benutzen. Diese Angriffsmethode mag zwar logisch klingen, ist aber nicht gefährlich, wenn man von einem weltumspannenden Netzwerk ausgeht, bei dem nicht nur einer, sondern viele Übertragungswege zu Verfügung stehen.[79]

[77] vgl. Zarda, 1999, S. 28
[78] vgl. Schauer, 2007, S. 61
[79] vgl. Schrenk, 2007, S.22

5. Vergleich der beiden Verfahren

Obwohl beide Verfahren sehr unterschiedlich sind, da eines auf mathematischen und das andere auf physikalischen Prinzipien beruht, kann man vergleichen, wie sehr sie in der Praxis anwendbar sind.

5.1. Public Key Verfahren in der Praxis

Seit PGP veröffentlicht wurde, sind Public-Key-Verfahren zur üblichsten Verschlüsselungsmethode geworden. Heute sind alle vertraulichen Kommunikationen und Daten mithilfe eines asymmetrischen Verschlüsselungsverfahren geschützt. Im folgenden Abschnitt werden einige Anwendungsbereiche vorgestellt.

5.1.1. WhatsApp

Da er in der Vergangenheit oft von Datenschützern kritisiert wurde, verwendet der Messaging-Dienst seit 2014 eine Ende-Zu-Ende-Verschlüsselung. Das Public-Key-Verfahren namens Signal-Protokoll von Open Whisper Systems soll garantieren, dass die versendeten Nachrichten von niemanden, auch nicht vom Betreiber selbst, gelesen werden können. Da die Verschlüsselung ausschließlich zwischen den beiden Gesprächspartnern mithilfe von Private und Public Key erfolgt, kennt auch der Hersteller der App den privaten Schlüssel nicht und kann keine Nachrichten lesen. Trotzdem ist WhatsApp noch immer heftiger Kritik ausgesetzt, da diese Verschlüsselung nicht verhindert, dass die App die Identität der Gesprächspartner speichert und für ihre Zwecke benutzt. Außerdem hatte der Sicherheitsforscher Tobias Boelter 2016 eine Schwachstelle im System entdeckt: Ist das Senden einer Nachricht nicht möglich, wird diese später automatisch erneut versendet, auch wenn sich der Public Key des Empfängers geändert hat. Dadurch wird ein Man-in-the-Middle-Angriff ermöglicht, indem sich eine unbeteiligte Person als Empfänger der Nachricht ausgibt. Des Weiteren ist das System nur sicher, wenn Versender und Empfänger ihre Sicherheitsnummern austauschen, um ihre Identität zu gewährleisten, was aber von den wenigsten Benutzern der App gemacht wird. [80]

[80] Himmelein, Gerald : Krypto-Experte. Keine Backdoor in WhatsApp. 14.01.2017. https://www.heise.de/newsticker/meldung/Krypto-Experte-Keine-Backdoor-in-WhatsApp-3596359.html. [Zugriff: 13.8.2019]

5.1.2. E-Mail

Obwohl PGP ursprünglich für das sichere Versenden von E-Mails entwickelt wurde, wird es heute von den wenigsten Anbietern standardmäßig verwendet. Es gibt viele weiterentwickelte Versionen der ursprünglichen PGP-Software, die mit E-Mail-Programmen kompatibel sind, jedoch sind diese meist umständlich oder langsam. Große E-Mail-Dienste wie Gmail weigern sich, die Verschlüsselung direkt in ihre Produkte einzubauen, da diese zu umständlich seien, dem Betreiber aber auch die Möglichkeit nehmen würden, selbst den Inhalt der Nachrichten zu lesen und zum Beispiel für Werbezwecke zu verwenden. Trotzdem hat Google 2017 das Programm E2Email als Open-Source-Projekt veröffentlicht, dass mit Gmail kompatibel ist und Nachrichten Ende-zu-Ende verschlüsselt.[81]

5.1.3 Banktransaktionen

Auch die meisten Banken benutzen RSA und ähnliche Systeme, um sichere Banktransaktionen zu gewährleisten. Dabei wird das Public-Key-Verfahren nicht dazu benützt, Nachrichten zu verschlüsseln, sondern um mithilfe digitaler Signaturen die Identität der Nutzer zu überprüfen. 2008 wurde EBICS-Verfahren in vielen Banken und Kreditinstituten eingeführt, die die Sicherheit der Transaktionen beim E-Banking gewährleisten und vereinheitlichen soll. Ohne Open-Key-Verfahren wären Online-Banking und damit auch der Online-Handel in der heutigen Form nicht möglich.[82]

5.2. QKD-Systeme in der Praxis

Obwohl im Bereich der Quantenkryptographie heute noch viel geforscht und weiterentwickelt wird, gibt es bereits einige kommerzielle QKD-Systeme, zum Beispiel von der Firma ID-quantique, die unter anderem in Banken oder bei Wahlen benutzt werden.[83]

---

[81] Scherschel, Fabian A. : E2Email. Google veröffentlicht PGP für GMail als Open-Source-Projekt. 28.02.2017. https://www.heise.de/security/meldung/E2EMail-Google-veroeffentlicht-PGP-fuer-GMail-als-Open-Source-Projekt-3638073.html. [Zugriff: 13.8.2019]

[82] Leupold; de Lorenzo; Hopfgartner: Online Banking. 13.3.2011. http://www.cosy.sbg.ac.at/~held/teaching/wiss_arbeiten/slides_10-11/Online-Banking.pdf [Zugriff: 13.8.2019]

[83] vgl. Marschner, Mirijam: Interview mit Sebastian Etcheverry. -Wien: E-Mail. 17.7.2019. S.1

Um QKD-Technologien der Öffentlichkeit zugänglich zu machen, sucht das Projekt CiViQ Wege, Quantenschlüsselaustausch billig und effizient in bestehende Systeme einzubauen.

> *„The goal of the CiViQ project is to open a radically novel avenue towards flexible and cost-effective integration of quantum communication technologies, and in particular Continuous-Variable QKD, into emerging optical telecommunication networks."*[84]

Das Projekt ist Teil des „Quantum Flagship", einem Forschungsprojekt, welches von der EU gefördert wird.

Laut Sebastián Etcheverry, einem schwedischen Physiker des CiViQ-Projektes, wäre es technisch gesehen heute möglich, Online-Shopping oder E-Mail-Konversationen durch abhörsichere Quantenkanäle zu betreiben. Da diese Systeme nicht nur teure Glasfaserlinks benötigen, weshalb sie schwer zu optimieren sind, sondern auch nur zwischen zwei Personen funktionieren, sind sie nicht für den privaten Markt oder das Internet bestimmt. Das möchte CiViQ ändern, indem es probiert QKD in bestehende Netzwerke und Infrastrukturen zu integrieren. Dazu wird ein QKD-Protokoll namens „Continuous variables" benutzt, das viele Ähnlichkeiten mit klassischer Kommunikation hat und deshalb einfach integrierbar ist. Die Vereinbarkeit mit bestehenden Systemen sei nämlich eine der größten Herausforderungen für QKD.[85]

> *"The biggest challenge is to develop QKD that can work in real networks scenarios and coexist with classical communication, without affecting the performance of the network. Also, it is important demonstrate the use of QKD in real applications."*

Die Entwicklung von satellitengestützten QKD-Systemen ist laut dem Physiker einer der größten Fortschritte in diesem Gebiet in den vergangenen Jahren.

> *"The realization of satellite-to-ground quantum key distribution was one of the major achievements of the last years. Also, the demonstration of QKD networks in several cities of the world has been really important to understand the feasibility of the technology."* [86]

[84] Pruneri, Valerio: CiViQ - Continuous Variable Quantum Communications. https://qt.eu/understand/projects/civiq-continuous-variable-quantum-communications/ [Zugriff: 13.8.2019]

[85] vgl. Marschner, 2019, S.1

[86] Marschner, 2019, S.1

5.3. Schwachstellen der Systeme

RSA und andere Public Key Verfahren sind technisch gesehen so lange sicher, solange es nicht möglich ist, n in kurzer Zeit in seine Faktoren zu zerlegen. Obwohl das heute noch nicht möglich ist, können Kryptoanalytiker trotzdem wichtige Informationen aus verschlüsselten Nachrichten erhalten. Beispielsweise verbirgt RSA nicht die Identität der Benutzer, deshalb ist leicht nachvollziehbar, wer mit wem kommuniziert. Außerdem ist es möglich, mithilfe eines Trojaners oder einem ähnlichen Computervirus, die unverschlüsselte Botschaft abzuspeichern und über einen anderen Kanal zu versenden.[87] All diese Schwachstellen treten nicht ausschließlich bei Public Key Verfahren auf und haben nichts mit dem eigentlichen Algorithmus zu tun, trotzdem können sie die Sicherheit des Verfahrens deutlich verkleinern.

QKD-Verfahren sind in der Theorie nicht nur mit heutigen technischen Mitteln abhörsicher, sondern werden das aufgrund physikalischer Prinzipien auch in Zukunft sein. Der größte Nachteil dieser Systeme in der Praxis ist, dass sie oft nicht mit bestehenden Netzen kompatibel sind. Auch durch andere Faktoren sind QKD-Systeme so teuer in der Anschaffung, dass sie heute nur von großen Firmen oder Banken innerhalb eines abgegrenzten Systems benutzt werden.[88]

5.4. Zukunft

Es ist wahrscheinlich, dass Public Key Verfahren, wie sie heute benutzt werden, in Zukunft kaum noch Sicherheit bieten. Zwar ist es mathematisch nicht möglich, die Einwegfunktion ohne Zusatzinformation rückgängig zu machen, trotzdem wird es mit Hilfe von leistungsfähigen Computern möglich sein, den private key zu ermitteln und so die Nachricht zu entschlüsseln.[89] Deshalb wird ein alternatives System, zum Beispiel QKD, Public Key Verfahren ersetzen.

Etcheverry glaubt aber nicht, dass dies in naher Zukunft geschehen wird. Zuerst werde es laut ihm eine Übergangsphase geben, in der QKD für kritische Daten benutzt werden wird, während private Kommunikationen über verbesserte mathematische Algorithmen verschlüsselt werden, die auch von Hochleistungsrechnern oder

[87] vgl. Singh, 2001, S. 385f
[88] vgl. Marschner, 2019, S.1
[89] vgl. Singh, 2001, S.387

Quantencomputern nicht entschlüsselt werden können.[90] Obwohl noch keine Quantencomputer existieren, die tatsächlich Chiffren wie RSA knacken können, schrieb die amerikanische NIST einen Wettbewerb aus, um die perfekte Post-Quantum-Chiffre zu finden.[91] Dieser Wettbewerb ist bis heute leider erfolglos geblieben, trotzdem ist Etcheverry optimistisch, dass so ein Verfahren gefunden werden wird.

Später aber, so Etcheverry, werden QKD-Systeme *„the core of cryptography"* werden, da sie die einzigen Systeme sind *„where the security does not depend on the computational capability of an adversary"*.[92]

[90] vgl. Marschner, 2019, S.1f

[91] vgl. Ducklin, Paul : Serious Security: Post-Quantum Cryptography (and why we're getting it). 7.2.2019. https://nakedsecurity.sophos.com/2019/02/07/serious-security-post-quantum-cryptography-and why-we-are-getting-it/ [Zugriff: 13.8.2019]

[92] vgl. Marschner, 2019, S.2

6. Fazit

Der Schlüsselaustausch ist eines der Hauptprobleme in der modernen Kryptographie. Es gibt zwei Lösungsansätze für dieses Problem, einen physikalischen und einen mathematischen. Da diese beiden Systeme so unterschiedlich sind, war es kaum möglich, sie direkt miteinander zu vergleichen. Jedoch sind bei beiden Verfahren deutlich Vor- und Nachteile zu erkennen.

Public-Key-Verfahren wie das RSA-Verfahren basieren auf Einwegfunktionen. Da für Entschlüsselung und Verschlüsselung andere Informationen benötigt werden, ist kein Schlüsselaustausch nötig. Außerdem handelt es sich um ein mathematisches Verfahren, welches, anders als QKD-Systeme, mit bestehenden Computern und Netzwerken kompatibel ist. Jedoch wird es durch immer schnellere und leistungsfähigere Maschinen in naher Zukunft möglich sein, diese Funktionen ohne die geheimen Zusatzinformationen rückgängig zu machen. Deshalb glauben die meisten Wissenschaftler, dass Systeme wie das RSA-Verfahren bald keine Sicherheit mehr bieten werden.

QKD-Verfahren funktionieren aufgrund fundamentaler physikalischer Gesetze. Deshalb wird es auch in Zukunft nicht möglich sein, sie unautorisiert zu entschlüsseln. Obwohl es schon Bereiche gibt, in denen QKD-Systeme eingesetzt werden, ist die technische Umsetzung noch nicht perfekt. Deshalb ist es möglich, gewisse Informationen abzufangen. Ein weiterer Nachteil ist, dass diese Systeme teuer in der Anschaffung sind, da sie eigene Netzwerke benötigen.

Es ist nicht möglich, genau zu sagen, welches der Systeme besser ist. Heute werden fast ausschließlich Public-Key-Verfahren eingesetzt, da diese praktisch anzuwenden sind. Die meisten Wissenschaftler wie Etcheverry halten es für wahrscheinlich, dass QKD-Verfahren in Zukunft Programme wie RSA ablösen werden.

Eine Frage, die in der Arbeit nur am Rande thematisiert wurde, ist, ob ein perfektes kryptographisches System ein Gewinn oder ein Nachteil für die Gesellschaft wäre. Bei der Veröffentlichung von PGP wurde zum Beispiel kritisiert, dass dieses System nicht nur private Konversationen schützt, sondern auch von Kriminellen verwendet werden könnte.

Abschließend stelle ich fest, dass in der modernen Kryptographie verschiedene Möglichkeiten genutzt werden, um das Problem des Schlüsselaustausches zu umgehen. Trotzdem gibt es heute kein perfektes kryptographisches System, obwohl viele Wissenschaftler hoffen, dass das QKD-Verfahren einmal ausnahmslose Sicherheit bieten könnte.

Literaturverzeichnis

Literatur

Al-Khalili, Jim: Quantum. A guide to the perplexed.
-London: W&N, 2012.

Bourseau, Frank; Fox, Dirk; Thiel, Christoph: Vorzüge und Grenzen des RSA-Verfahrens. In: Datenschutz und Datensicherheit, 26, 2002, S. 84-89.
-Wiesbaden: Springer Fachmedien.

Devlin, Keith: Sternstunden der modernen Mathematik.
-Basel: Birkhäuser Verlag. 1990.

Diffie, Whitfield; Hellman, Martin: New directions in Cryptography. In: IEEE Transactions on Information Theory, 22,6, 1976, S.644-654.
- Piscataway: IEEE Information Theory Society.

Divus Julius: De Vita Caesarum [Übersetzung der Verfasserin]

Gahleitner, Angelika Maria. Das RSA-Verfahren Im Schulunterricht: Didaktische Aufbereitung Der Mathematischen Grundlagen. (Dipl. Arb.)
-Linz: Universität Linz. 2003.

Gardner, Martin: A new kind of cipher that would take millions of years to break. In: Scientific American 237.8, 1977, S.120-124.
-New York City: Nature Publishing Group.

Hannesschläger, Thomas. Einführung in Die Public-Key Kryptographie [!] Mittels RSA und Knapsack-Methoden. (Dipl. Arb.)
-Salzburg: Universität Salzburg. 2002.

Hawking, Stephen; Mlodinow, Leonard: The Grand Design.
-London: Transworld Publishers. 2010.

Hipp, Florian Peter: Novel Schemes for QKD. (Dipl.-Arb.)
-Wien: Technische Universität, 2016.

Marschner, Mirijam: Interview mit Sebastian Etcheverry.
-Wien: E-Mail. 17.7.2019.

Schauer, Stefan: Attack Strategies in Quantum Cryptography. (Dipl.-Arb.)
-Klagenfurt: Alpen-Adria-Universität, 2007.

Schrenk, Bernhard: Polarisationsnachregelung über Lange Glasfaserstrecken Für Quantenkryptographie. (Dipl.-Arb.)
-Wien: Technische Universität, 2007.

Singh, Simon: Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet.
- München: dtv Verlagsgesellschaft mbH&Co. KG, 2001.

Steward, Ian: Unglaubliche Zahlen.
-Reinbek bei Hamburg: Rowohlt Taschenbuch Verlag. 2016.

Wolfgang Tittel, Jürgen Brendel, Nicolas Gisin, Grégoire Ribordy, Hugo Zbinden: Quantenkryptographie. In: Physikalische Blätter, Nr. 55/6, 1999, S.25-30, -Weinheim: WILEY-VCH Verlag GmbH & Co. KGaA.

Wootters, William; Zurek, Wojciech: A single quantum cannot be cloned. In: Nature, Nr. 299, 1982, S.802–803.
-Berlin: Springer Nature Publishing AG.

Zarda, Patrick: Quantenkryptographie.(Dipl.-Arb.)
-Innsbruck: Universität Innsbruck, 1999.

Internetquellen

Ducklin, Paul: Serious Security: Post-Quantum Cryptography (and why we're getting it). 7.2.2019. https://nakedsecurity.sophos.com/2019/02/07/serious-security-post-quantum-cryptography-and-why-we-are-getting-it/
[Zugriff: 13.8.2019]

Himmelein, Gerald: Krypto-Experte. Keine Backdoor in WhatsApp. 14.01.2017. https://www.heise.de/newsticker/meldung/Krypto-Experte-Keine-Backdoor-in-WhatsApp-3596359.html.
[Zugriff: 13.8.2019]

Leupold; de Lorenzo; Hopfgartner: Online Banking. 13.3.2011. http://www.cosy.sbg.ac.at/~held/teaching/wiss_arbeiten/slides_10-11/Online-Banking.pdf
[Zugriff: 13.8.2019]

Pruneri, Valerio: CiViQ - Continuous Variable Quantum Communications. https://qt.eu/understand/projects/civiq-continuous-variable-quantum-communications/
[Zugriff: 13.8.2019]

Scherschel, Fabian A.: E2Email. Google veröffentlicht PGP für GMail als Open-Source-Projekt. 28.02.2017. https://www.heise.de/security/meldung/E2EMail-Google-veroeffentlicht-PGP-fuer-GMail-als-Open-Source-Projekt-3638073.html.
[Zugriff: 13.8.2019]

Abbildungsverzeichnis

Abbildung 1(S.5): Eigene Darstellung [Anmerkung der Verfasserin]

Abbildung 2 (S.6): Eigene Darstellung [Anmerkung der Verfasserin]

Abbildung 3 (S.9): Eigene Darstellung [Anmerkung der Verfasserin]

Abbildung 4 (S.11): Eigene Darstellung [Anmerkung der Verfasserin]

Abbildung 5 (S.12): Eigene Darstellung [Anmerkung der Verfasserin]

Abbildung 6 (S.17): Eigene Darstellung [Anmerkung der Verfasserin]

Abbildung 7 (S.19): Eigene Darstellung [Anmerkung der Verfasserin]

Abbildung 8 (S.21): Eigene Darstellung [Anmerkung der Verfasserin]

Interview

Written interview via mail with Sebastian Etcheverry, currently working on the CiViQ-project

You are currently working on a project called CiViQ, which is part of the quantum flagship. What exactly is the aim of this project?

The secure of current cryptography is based on mathematical algorithm that are expected to become vulnerable with coming development in computational capabilities (i.e with a quantum computer). Quantum key distribution (QKD) is a technology that allows two or more parties to exchange a secret key, whose security is based on the laws of quantum physical. The aim of the CiViQ project is to integrate QKD into current network infrastructure, allowing for the wide-scale deployment of the technology. To this end, we are using a type of QKD called Continuous variable QKD that has many similarities with classical coherent communication, and it can be implemented with mature telecom components. CiViQ includes the development of QKD systems that are less expensive, more flexible, and capable of being easily integrated into real network.

What would you say is the biggest challenge in trying to include QKD-technologies in commercial systems?

There are commercial QKD systems, from instance ID-quantique realised many years ago their first QKLD system. However, these systems are point-to-point and need dedicated fiber links to operate, which have limited the deployment of the technology. The biggest challenge is to develop QKD that can work in real networks scenarios and coexist with classical communication, without affecting the performance of the network. Also, it is important demonstrate the use of QKD in real applications. That's with the CIVIQ projects involves the participation of telecom companies that define relevant use-cases.

Where are QKD-systems already being used today?

QKD has been used by banks and political elections, however the use of QKD in real applications is very limited today and few commercial systems are available. From a more scientific perspective, there have been implementations of multi-party QKD,

long-distance, as well as satellite-ground QKD. CiViQ aims at developing QKD to be widely used by providing network integration and scalability.

Will QKD some day replace all other cryptographic technologies? Or will it only be used for certain purposes?

I believe that depends on the maturity level and performance that QKD achieves, as well as the other technologies that could provide high security. It is known that classical cryptography will be vulnerable when sufficiently large quantum computer become available. However, there are people working on developing cryptographic algorithm (classical) that quantum computers could not efficiently break (post-quantum cryptography). I think that in the near future, QKD will be used for application where security in critical, whereas improved mathematical algorithm will be used for the other cases. Nevertheless, since QKD is the only technology where the security does not depend on the computational capability of an adversary, I would expect that at some point QKD will become the core of cryptography.

What, from your point of view, were the major achievements in the field of quantum communication in the last decade?

The realization of satellite-to-ground quantum key distribution was one of the major achievements of the last years. Also, the demonstration of QKD networks in several cities of the world has been really important to understand the feasibility of the technology. I would say that also the experimental implementation of technologies such as measurement devices independent QKD and continuous-variable QKD has been really important to define the roadmap for QKD deployment.

When will I be able to make private bank transitions through quantum networks? Write private mails? Do online shopping?

The technology is available today, however it is very expensive and needs dedicated communication channels. The aim of CiViQ is to overcome these limitations and bring QKD to the society.

Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich diese Vorwissenschaftliche Arbeit eigenständig angefertigt und nur die im Literaturverzeichnis angeführten Quellen und Hilfsmittel benutzt habe.

_____ _____

Ort, Datum Unterschrift der Schülerin

Zustimmung zur Aufstellung in der Schulbibliothek

Ich gebe mein Einverständnis, dass ein Exemplar meiner Vorwissenschaftlichen Arbeit in der Schulbibliothek aufgestellt wird.

_____ _____

Ort, Datum Unterschrift der Schülerin