07.06.2017

Seminar IT-Sicherheit

Sommersemester 2017

Quanten-Kryptographie

Céline Nöldemann
Master IT-Sicherheit
its102553@fh-wedel.de

Betreuer:
Prof. Dr. Gerd Beuster
gb@fh-wedel.de

Inhaltsverzeichnis

1 Einführung **1**

2 Die „Klassische" Kryptographie **2**
2.1 Verschlüsselungsverfahren 2
2.2 One Time Pad 2
2.3 Schlüsselproblem 3

3 Quantenkryptographie **5**
3.1 Schlüsselaustausch 5
3.1.1 Physikalische Komponenten 5
3.1.2 Das BB84-Protokoll 6
3.1.3 Probleme 7
3.2 Sicherheit 8

4 Vergleich **9**

5 Ausblick **10**
5.1 Europas Zukunft 10
5.2 Übertragung per Satellit 10
5.3 Tiefgefrorene Leitungen 10
5.4 Quantenkryptographie im Smartphone 11

6 Fazit **12**

1 Einführung

Schon zu Zeiten des Römischen Reiches, fing Julius Caesar an, geheime Nachrichten zu verschlüsseln. Die nach ihm benannte Caesar-Chiffre scheint heutzutage primitiv zu sein und stellt so gut wie gar keine Sicherheit, war damals allerdings ein sehr effektives Mittel um zu verhindern, dass Informationen in die falschen Hände geraten. Dies war der Beginn der klassischen Kryptographie, wie wir sie kennen.

In der heutigen Kryptographie werden in der Regel keine simplen Verschiebechiffren verwendet, da sie viel zu leicht zu brechen sind. Die Verfahren sind von deutlich komplexerer Natur, mit komplizierten Berechnungen für den Schlüssel und rundenbasierter Chiffrierung der Nachricht. Ein wirklich sicheres Verfahren zeichnet aus, dass selbst nach der Veröffentlichung des Algorithmus, es immer noch nicht möglich ist, ihn zu brechen. Umso wichtiger wird es dann, dass der Schlüssel geheim und vollkommen zufällig ist, damit niemand Unbefugtes die Nachricht entschlüsseln kann. Über die Jahre gab es schon viele Versuche, dies zu ermöglichen. Eines der jüngsten Entwicklungen ist hierbei die Quantenkryptographie, die viele für das Verschlüsselungsverfahren der Zukunft halten.

2 Die „Klassische” Kryptographie

2.1 Verschlüsselungsverfahren

Wie in der Einleitung bereits erwähnt, liegen die ersten verschlüsselten Nachrichten schon fast 2000 Jahre zurück. In der Zwischenzeit hat sich vieles im Bereich der Kryptographie verändert. Es wird ständig danach gestrebt, noch sicherere Algorithmen zu entwickeln, damit Privates auch wirklich privat bleibt, gerade jetzt wo sich die Kommunikation vieler Menschen zunehmend ins Internet verlagert. Mittlerweile gibt es eine Vielzahl der verschiedensten Verschlüsselungsverfahren. In der Regel werden diese in **symmetrisch** und **asymmetrisch** unterteilt.

Symmetrische Verfahren zeichnet aus, dass derselbe Schlüssel für sowohl Ver- als auch Entschlüsselung verwendet wird. Hierbei ist es besonders wichtig, dass der Schlüssel geheim bleibt. Die Schwierigkeit darin besteht, dass sich Sender und Empfänger auf einen gemeinsamen Schlüssel verständigen müssen, ohne dabei von einem Angreifer abgehört zu werden. Ein Beispiel ist das One Time Pad, welches später (Abschnitt 2.2) genauer erläutert wird.

Asymmetrische Verfahren haben dieses Problem nicht. Die Nachrichten werden mit einem öffentlichen Schlüssel (Public Key) generiert und können nur von dem dazugehörigen privaten Schlüssel (Private Key) entschlüsselt werden. Dieses sogenannte Schlüsselpaar wird abhängig voneinander berechnet und gilt nur füreinander. Dabei ist der Public Key für jeden zugänglich, wobei der Private Key nur in den Händen des Empfängers bleibt. Bei einer Antwort wird dann der Public Key des jeweils anderen verwendet. Ein anschauliches Beispiel in der realen Welt wäre hierbei der Briefkasten. Jeder ist in der Lage eine Nachricht in den Briefkasten zu werden, da er öffentlich zugänglich ist und jeder weiß, wo er steht. Allerdings kann nur der Besitzer des Briefkastens, also der Empfänger mit dem richtigen Schlüssel, diesen öffnen und die Nachrichten lesen.

2.2 One Time Pad

Das One Time Pad gilt als perfektes Verschlüsselungsverfahren, sofern bestimmte Regeln eingehalten werden [SHA49]. Perfekt bedeutet hierbei, dass es unmöglich zu knacken ist. Der Plaintext (= die Nachricht) wird mittels XOR mit dem Schlüssel verknüpft. Die Länge des Schlüssels muss dabei der des Plaintextes entsprechen. Das Ergebnis der Berechnung ist der Ciphertext und kann mit demselben Schlüssel wieder lesbar gemacht werden.

Beispiel:

$$\begin{array}{ll} 10011101 & \text{(Plaintext)} \\ 11001111 & \text{(Schlüssel)} \\ \hline 01010010 & \text{(Ciphertext)} \end{array}$$

Nur mit dem Ciphertext ist es weder möglich die ursprüngliche Nachricht, noch den Schlüssel zu rekonstruieren. Auf den ersten Blick also ein vollkommen sicheres Verfahren. Allerdings hat das One Time Pad eine ganz gravierende Schwäche: wie der Name bereits erwarten lässt, kann man einen Schlüssel nur ein einziges Mal verwenden. Wird dies nicht eingehalten und man verschlüsselt mehrere Nachrichten mit ein und demselben Schlüssel, gibt man einem Angreifer die Möglichkeit, den Plaintext zu erraten, ohne den Schlüssel zu kennen. Diese Schwachstelle ist auf die Natur des XORs zurück zu führen. Verknüpft man zwei vollkommen identische Zahlen miteinander, so ist das Ergebnis 0 und somit für den Rest der Berechnung trivial, da die Null das neutrale Element des XORs ist. Auf das One Time Pad übertragen, ergibt sich dabei folgende Rechnung:

$$\begin{aligned} C1 \oplus C2 &= (P1 \oplus K) \oplus (P2 \oplus K) \\ &= P1 \oplus K \oplus K \oplus P2 \\ &= P1 \oplus 0 \oplus P2 \\ &= P1 \oplus P2 \end{aligned}$$

Hierbei stehen C1,C2 für die jeweiligen Cipher-, P1,P2 für die Plaintext und K für den Schlüssel.
Nun bedarf es nur noch Geduld und einem Angreifer ist es möglich, die ursprünglichen Nachrichten wieder herzustellen. Je mehr Nachrichten mit dem gleichen Schlüssel verschlüsselt worden sind, desto einfach ist am Ende das Knacken. Es ist also von erheblicher Wichtigkeit, dass für jede Nachricht, ein neuer Schlüssel erzeugt werden muss. Ein neuer Schlüssel, der vorher zwischen Sender und Empfänger ausgetauscht werden muss. Dies ist ein immenser Aufwand und nicht praktikabel, auch weil sich durch jeden Austausch die Gefahr erhöht, von einem Angreifer belauscht zu werden.

2.3 Schlüsselproblem

Bei einer symmetrischen Verschlüsselung müssen sich Sender und Empfänger im Vorwege auf einen Schlüssel einigen. Da die Algorithmen öffentlich bekannt sind, muss der Schlüssel bestimmte Eigenschaften erfüllen, damit die Verschlüsselung auch wirklich sicher ist:

- **Zufällig:** Der Schlüssel muss (pseudo-)zufällig und darf nicht vorhersehbar sein
- **Geheim:** Nur der Sender und der Empfänger dürfen den Schlüssel kennen
- **Einzigartig:** In einigen Fällen (z.B. One Time Pad) darf der Schlüssel nur ein einziges Mal verwendet werden

Aus diesem Grund wurden asymmetrische Verfahren entwickelt, bei denen ein Schlüsselaustausch nicht länger notwendig ist und die Geheimhaltung einfacher macht. Vor einigen Jahren kam ein weiteres abhörsicheres Verfahren hinzu, was mithilfe der Quantenmechanik, all diese Eigenschaften für einen Schlüssel erfüllen kann.

3 Quantenkryptographie

Bei der Quantenkryptographie geht es nicht darum, mithilfe der Quantenmechanik die Nachrichten selbst sicher auszutauschen, wie viele bei dem Namen erwarten würden. Ziel der Quantenkryptographie ist es, einen *zufälligen* Schlüssel *sicher* zwischen Sender und Empfänger auszutauschen. Aus diesem Grund wird es auch *Quantenschlüsselaustausch(system)* genannt.

Die erste (zunächst theoretische) Veröffentlichung zu dem Thema erschien Dezember 1984 von Charles H. Bennett und Gilles Brassard [BB84]. Ihr *Quantum Key Distribution Protocol* wurde schließlich nach ihnen und dem Veröffentlichungsjahr benannt: BB84-Protokoll.

3.1 Schlüsselaustausch

In dem folgenden Szenario soll ein Schlüssel zwischen Alice und Bob ausgetauscht werden. Ein Angreifer Eve versucht dabei, den geheimen Schlüssel abzufangen, ohne dass Alice und Bob es bemerken.

3.1.1 Physikalische Komponenten

- Einzelphotonenquelle
- Sichere Leitung[1]
- Öffentliche Leitung (z.B. Internet)
- Polarisationsfilter
- Polarisationsdreher
- Detektor
- (Quantenzufallsgenerator)

[1] Es ist in Ordnung, wenn die Leitung belauscht werden kann, solange Manipulation ausgeschlosssen ist

3.1.2 Das BB84-Protokoll

Bei der Schlüsselerzeugung werden einzelne Teilchen (in den meisten Fällen Photonen) über eine sichere Leitung von Alice zu Bob gesendet. Anhand ihrer Polarisation werden sie am Detektor von Bob als 0 oder 1 interpretiert. Die Polarisation beschreibt die Ausrichtung eines Photons. Ein Photon kann auf vier verschiedene Weisen polarisiert sein: senkrecht(0°), waagerecht(90°) oder diagonal(45° bzw. 135°). Die Polarisation kann durch ein hinter der Quelle geschalteten Polarisationsdreher eingestellt werden. Bei einer manuellen Durchführung, muss Alice selbst die Einstellungen vornehmen. Es empfiehlt sich allerdings für eine absolute Zufallspolarisation einen Quantenzufallsgenerator zu verwenden.

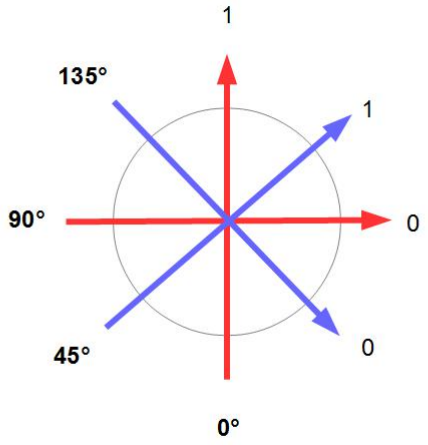

Abbildung 3.1: Polarisationsdreher mit Bit-Besetzungen

Auf Bobs Seite steht vor dem Detektor geschaltet ein Polarisationsfilter. Dieser kann wie der Polarisationsdreher auf zwei verschiedene Basen eingestellt werden: + (waagerecht, senkrecht) und × (diagonal). Bob entscheidet ebenfalls rein zufällig nach jedem Photon wie der Filter eingestellt werden soll. Sowohl Bob als auch Alice notieren sich nach jedem Photon die Einstellung der Filter/Dreher hatte und welche Polarisation das Photon hatte. Erst nachdem das letzte Teilchen übermittel worden ist, setzten sich Alice und Bob über eine öffentliche Leitung in Verbindung und teilen dem jeweils anderen mit, welche Basis sie bei welchem Photon verwendet haben. Die gemessene oder gesendete Polarisierung der Photonen bleibt dabei jedoch geheim. Nun werden alle Messergebnisse gestrichen, bei denen eine unterschiedliche Basis verwendet worden ist, da diese ungenau sind. Die Bits die übrig

bleiben, bilden den geheimen Schlüssel, der nun zum Enkodieren der Nachricht von Alice verwendet werden kann. Die übertragung der Nachricht findet ebenfalls über den öffentlichen Kanal statt. Da Bob den gleichen Schlüssel hat wie Alice, kann er ihn verwenden um die Nachricht zu dekodieren.

Gesendetes Bit	1	0	1	0	0	0	1	0
Alice Basis	+	x	+	+	x	+	x	x
Bobs Basis	x	+	+	+	x	x	+	x
Schlüssel	-	-	1	0	0	-	-	0

Abbildung 3.2: Schlüsselerzeugung mit dem BB84-Protokoll

3.1.3 Probleme

Obwohl im vorherigen Teil behauptet wurde, dass Bob den gleichen Schlüssel besitzt wie Alice, muss dies nicht immer zwingend der Fall sein. Bei den Ergebnissen können immer Messfehler unterlaufen, die ein Rauschen bei dem dekodierten Text erzeugen. Solange die Anzahl der Fehler klein ist, gibt es allerdings keinen Grund zur Sorge. Sobald sich die Fehler allerdings häufen, könnte dies ein Anzeichen dafür sein, dass sich ein Angreifer in die Leitung gehängt hat.

Eine weitere potenziell problematische Eigenschaft dieses Protokolls ist der Zufall. Dies erscheint im ersten Moment paradox, da es ja genau diese Zufälligkeit ist, die wir brauchen für unseren Schlüssel, doch nicht nur die Sequenz des Schlüssels ist dadurch zufällig, sondern auch seine Länge. Die von Alice eingegebene Sequenz von Bits sollte lange genug sein, dass der resultierende Schwund von Bits durch unterschiedliche Basen den generierten Schlüssel nicht allzu kurz macht. Doch wenn der Zufall es so wollte, dann können auch von 1024 Bits nur vier übrig bleiben. Unwahrscheinlich, aber dennoch möglich. Da der Schlüssel mindestens so lang sein muss, wie der zu verschlüsselnde Text, ist es ziemlich willkürlich, ob der generierte Schlüssel tatsächlich verwendet werden kann. Im schlimmsten Fall muss er dann verworfen, und ein neuer Schlüssel generiert werden oder durch weitere Anwendungen die fehlenden Bits ergänzt werden.

Bei bereits existierenden Experimenten mit diesem Verfahren, wurde die Reichweite getestet. Dabei wurde festgestellt, dass mit zunehmender Entfernung, sich die Fehlerrate deutlich erhöht. Dies hat mit den Störfaktoren zu tun, mit denen das Photon zu kämpfen hat, da es sich nicht in einem Vakuum bewegt. Es ist durchaus möglich, dass sich die Polarisation des Photons auf dem Weg von Alice zu Bob verändert. Die momentan maximale Entfernung für einen erfolgreichen Schlüsselaustausch beträgt 144km von Teneriffa bis La Palma de Mallorca aus dem Jahr 2007 [WdPh].

3.2 Sicherheit

Natürlich ist dieses Verfahren trotz aller Versprechungen und Vorkehrungen nicht hundertprozentig abhörsicher. Ein Angreifer Eve könnte sich an die Leitung hängen und den Photonenstrom ebenfalls messen. Eve müsste sich in diesem Moment aber ebenfalls für eine Basis entscheiden. Da sie aber nicht weiß, mit welcher Basis Alice das Photon abgeschickt hat, bekommt sie in 50% der Fälle ein zufälliges Ergebnis. Da es nicht möglich ist, ein Photon zu messen, ohne es dabei zu zerstören, muss Eve nun ebenfalls ein Photon in Richtung Bob senden, damit ihr Eingreifen nicht auffällt. Auch diesmal muss sie sich für eine Polarisation entscheiden. Die Wahrscheinlichkeit, dass sie diesmal richtig liegt, liegt bei 25%.
Um sicherzugehen, dass eine Leitung wirklich frei von Angreifern ist, müssen Alice und Bob zu Beginn der Übertragung, einmal ihre gesendeten und empfangenen Bits vergleichen. Beträgt die Fehlerrate mehr als 25%, ist die Leitung sehr wahrscheinlich unsicher und darf nicht zum Schlüsselaustausch verwendet werden.[2]

[2] Dies war nur eine kleine Einführung in das Thema Sicherheit und Angriffe. Eine tiefgründigere Erläuterung finden Sie in der Ausarbeitung von Sebastian Krumm: *Angriffe auf Quanten-Kryptographie*

4 Vergleich

Tabelle 4.1: Vergleich Klassische Kryptographie und Quantenkryptographie

Klassische Kryptographie	**Quantenkryptographie**
Belauschen der Schlüsselübetragung wird meist nicht bemerkt	Belauschen der Schlüsselübetragung wird (in den meisten Fällen) bemerkt und die Übetragung wird unterbrochen
Bitsequenz nicht immer zufällig	Bitsequenz rein zufällig (wenn Quantenzufallsgenerator verwendet)
Länge des Schlüssels kann kontrolliert werden	Länge kann nicht kontrolliert werden
Übertragungsweite nicht beschränkt	Reichweite beschränkt auf 100-200km (Über Luft)
Keine zusätzliche Hardware notwendig	Physikalische Komponenten erforderlich
In der Regel ist Schlüssel ohne Übertragungsfehler	Schlüssel relativ anfällig für Übetragungsfehler

5 Ausblick

5.1 Europas Zukunft

Einige zweifeln nicht daran, dass die Zukunft der Verschlüsselung bei der Quantenkryptographie liegt. Vielleicht wird es sogar die letzte verbleibende Methode sein, um vertraulich Daten über das Netz zu versenden. Sogar die Europäische Union hat im Jahr 2016 ein Quantenmanifest veröffentlicht, in dem sie vorhaben, die Zukunft der Technologie in Richtung Quanten zu lenken. Neben Quantencomputern ist auch das sogenannte „Quanten-Internet" ein Ziel, das bis 2035 erreicht werden soll. Die EU möchte "Vorreiter der zweiten Quanten-Revolution"werden [EU16].

5.2 Übertragung per Satellit

Da die Übertragen über die Luft auf zu große Entfernungen eine zu große Fehlerrate mit sich bringt, haben Forscher die Überlegung, den Schlüssel per Satelliten zu übetragen. Das Vakuum im Weltall stellt keine Störfaktoren dar, nur der Weg von der Bodenstation zum Satelliten und zurück muss so noch überwunden werden. Problematisch dabei ist allerdings, dass sich Satelliten ständig in Bewegung befinden[WdPh].

5.3 Tiefgefrorene Leitungen

Im März 2017 haben Forscher die scheinbare Lösung für das Problem der störanfaälligen Photonen gefunden: Sie haben die Leitung auf wenige Grad über dem Gefrierpunkt heruntergekühlt. Dies hat die Fehleranfälligkeit drastisch reduziert. Doch trotz dieses Erfolges, denken sie nicht, dass dieser Ansatz eine Zukunft hat. Das Problem dabei sind die erheblichen Kosten, die ein dermaßiges Kühlen mit sich bringt. Sie setzen dabei eher auf neue Glasfaserkabel für eine bessere Datenübertragung [Xiang].

5.4 Quantenkryptographie im Smartphone

Zum aktuellen Zeitpunkt benötigt man noch große Apparaturen, um einen Schlüssel auszutauschen. Die Übertragung mit einer physikalischen Leitung ist umständlich, das Versenden über die Luft auf größere Distanzen fehleranfällig. Und trotzdem erhofft man sich für die Zukunft, diese Technologie so zu minimieren, dass sie sogar in ein Smartphone passt. Verschlüsselung sicher und schnell für jedermann[WdPh].

6 Fazit

Mit den ersten Quantencomputern werden heute anerkannte Verfahren wie RSA nicht länger sicher sein. Die Quantenkryptographie bietet dabei eine Möglichkeit, auch weiterhin vertraulich Nachrichten auszutauschen.

Die Technologie scheint noch nicht ganz ausgereift zu sein. Obwohl das Verfahren in der Theorie komplett abhörsicher ist, sind die Sender- und Empfängerschnittstellen dies noch nicht und müssen dringend geschützt werden. Eine flexible End-zu-End-Übertragung ist durch die begrenzte Reichweite per Luft auch noch nicht möglich. Es muss ein Weg gefunden werden, die Fehlerrate zu minimieren.

Erfolgreiche Experimente sind bereits durchgeführt worden. Die Quantenkryptograhie existiert bereits in der realen Welt und wird sogar schon von einigen Banken verwendet[WdPh]. Es ist also nicht völlig abwegig, dass eines Tages jegliche Kommunikation mithilfe dieses Verfahrens verschlüsselt wird. Und Anbetracht der rapiden Entwicklung in den letzten Jahren, könnte das Ziel 2035 der EU eine realistische Vorstellung sein.

Literaturverzeichnis

[BB84] Charles H. Bennett, Gilles Brassard. *Quantum cryptography: Public key distribution and coin tossing.*Proceedings of IEEE International Conference on Computers, Systems & Signal Processing; 1984

[Bras] Gilles Brassard. *Brief History of Quantum Cryptography: A personal Perspective.* Université de Montréal; Oktober 2005, `https://arxiv.org/pdf/quant-ph/0604072.pdf`

[EU16] Quantum Manifesto. Quantum Information Processing and Communication in Europe, 2016 `http://qurope.eu/system/files/u7/93056_Quantum%20Manifesto_WEB.pdf` (Zugriff: 04.06.2017)

[Gol] Golem.de: Die leeren Versprechen der Quantenkryptographie, `https://www.golem.de/news/verschluesselung-die-leeren-\versprechen-der-quantenkryptographie-1605-120767.html`(Zugriff: 03.05.2017)

[Gol2] Golem.de: Flugzeug sendet Quantenschlüssel an Bodenstation, `https://www.golem.de/news/kryptographie-flugzeug-sendet-\quantenschluessel-an-bodenstation-1304-98478.html`(Zugriff: 04.06.2017)

[QLab] QuantumLab. Quantenkryptographie, `http://www.didaktik.physik.uni-erlangen.de/quantumlab/`(Zugriff:27.05.2017)

[SHA49] C. E. Shannon. *Communication Theory of Secrecy Systems.* Bell System Technical Journal, Vol.28, S.656-715; 1949

[WdPh] Welt der Physik: Quatenkryptographie – ein Schlüssel im Licht: `http://www.weltderphysik.de/gebiet/technik/quanten-technik/quantenkryptografie/` (Zugriff: 20.05.2017)

[Xiang] Ze-Liang Xiang, Mengzhen Zhang, Liang Jiang, Peter Rabl. *Intracity Quantum Communication via Thermal Microwave Networks.* American Physical Society, Vol.7 Issue 1; March 2017, `https://doi.org/10.1103/PhysRevX.7.011035`