Sicherheitsaspekte der Authentifizierungsphase in der Quantenkryptographie

Thomas Messmer

Matrikelnummer 280053
thmessme@htwg-konstanz.de

Abstract: Dieser Artikel beschreibt im wesentlichen die Sicherheitsaspekte des Authentifizierungsverfahrens in der Quantenkryptographie und dessen sicherheitskritischen Bereiche. Genauer geht es darum wie viel Informationen aus einer generierten Schlüssel-Sequenz erhalten werden können. Hört ein Lauscher einen Teil des Schlüssels ab, besitzt er Teilwissen über den verwendeten Schlüssel, dies stellt jedoch noch keine allzu große Gefahr dar. Betrachtet man jedoch das gesamte Authentifizierungsprotokoll und den Fakt, dass der Lauscher nicht nur lauschen sondern auch aktiv Nachrichten verändern kann, dann kann dieses zusätzliche Teilwissen über den Schlüssel eine Gefahr darstellen. Die Sicherheitslücke entsteht durch das verwendete Authentifizierungsverfahren. Dieses ist "'robust"' falls Nachrichten von einen Lauscher verändert werden, der über keinerlei Teilwissen über den Schlüssel verfügt. Es wird jedoch "'unrobust"' sobald Teilwissen über den Schlüssel zur Verfügung steht. Im Verlauf dieses Artikels das Authentifizierungsverfahren, ein möglicher Angriff, sowie eine einfache Lösung beschrieben die diese Schwachstelle schließt.

Key words: Authentication, quantum cryptography (QC), quantum key distribution, quantum key growing (QKG)

ACM classification: D.4.6, E.3

1 Einleitung

Diese Ausarbeitung entstand im Rahmen einer Seminararbeit an der HTWG Konstanz. Es bestand die Aufgabe den Artikel "'Security Aspects of the Authentication Used in Quantum Cryptography"' von Jörgen Cederlöf und Jan-Åke Larsson bzw. dessen Inhalt zu untersuchen und zu beschreiben. Alle getroffenen Aussagen, beziehen sich auf diesen Artikel, sollte dies nicht der Fall sein wird dies ausdrücklich erwähnt. Zu Beginn werden einige Erklärungen zur Kryptographie allgemein, sowie zu den in der Quantenkryptographie verwendeten Quantenzuständen beschrieben. Darauf folgend werden die Inhalte des originalen Artikels aufgezeigt. Um die Quantenkryptographie erklären zu können wird an dieser Stelle zuerst auf die wesentlichen kryptographischen Merkmale eingegangen, die auch in der Quantenkryptographie Verwendung finden. Es hat sich in der Computer-basierten Kryptographie etabliert einen Plaintext (Reintext) mit einem gegebenen Schlüssel "'exclusiv zu verodern (XOR)"'. Dies hat den Vorteil, dass der Ciphertext (entspricht verschlüsseltem Plaintext) mit dem gleichen Schlüssel und der selben XOR-Operation entschlüsselt werden kann. Nutzt man einen echt zufälligen Schlüssel k der mindestens genau so lang ist wie die zu verschlüsselnde Nachricht m ($|m| \leq |k|$), dann spricht man hierbei von einem "'One-Time-Pad"' (deutsch: Einmalblock). Dieses Verfahren ist für einen echt zufälligen Schlüssel k beweisbar sicher. Abbildung 1 beschreibt eine solche schematische Darstellung eines "'One-Time-Pad"'.

Plain	10000101 11000111 ...	0x 85 C7 ...
	XOR	
Key	10111000 10100011 ...	0x B8 A3 ...
	=	
Chiffer	00111101 01100100 ...	0x 3D 64 ...

Figure 1: One-Time-Pad

Jedoch ergibt sich daraus das Problem, dass der Schlüssel für sehr lange Nachrichten sehr lange sein muss und schwer zwischen den jeweiligen Parteien, auf sicherem Weg, geteilt werden kann. Die "'Quantenkryptographie"' (englisch: Quantum Cryptography (QC)) bzw. spezifis-

cher ausgedrückt, das "'Quanten basierte Schlüssel Wachstum (englisch: Quantum Key Growing (QKG))"' nutzt spezielle Eigenschaften der Quantenmechanik um einen solchen zufälligen Schlüssel für zwei Endpunkte zu generieren. Im Jahre 1984 wurden das QKG das erste Mal in [BB84] vorgeschlagen. Seit dieser Zeit wurden diverse Erweiterung in diesem Gebiet vorgestellt siehe [Eke91, BBB+92, GRTZ02]. Der genaue Aufbau von QKG-Systemen ist in diversen Literaturen zu finden. Eine gute Erklärung findet sich in [GRTZ02]. In dieser Ausarbeitung werden somit nur grundlegend die einzelnen Phasen des QKG-Prozesses beschrieben und vermehrt auf den Authentifizierungsphase und dessen sicherheitskritischen Stellen eingegangen. Im Gegensatz zu den herkömmlichen kryptographischen Systemen, basiert die Quantenkryptographie nicht auf der Komplexität von Computer-Algorithmen siehe [RSA78], sondern auf Naturgesetze siehe [Bel64, Cla74, WZ82].

Die Autoren Cederlöf und Larsson nutzen als übliche Terminologie die Namen Alice für den Sender, Bob für den Empfänger und Eve als Synonym für den Lauscher. Dies wird auch weiterhin beibehalten werden. Damit ein QKG-System funktionieren kann, muss es zwischen Alice und Bob einen Quantenkanal geben auf dem Quantenzustände übertragen werden können. Diese Zustände können auf verschiedenen Arten realisiert werden. Eines der heute am Häufigsten angewandten Verfahren nutzt die Polarisation von Photonen (BB84 Protokoll). Der Kanal kann zum Beispiel mittels einer Glasfaser-Leitung realisiert werden, auf der einzelne mit einem Polarisationsfilter polarisierte Photonen zwischen Alice und Bob übertragen werden. Diese Photonen beinhalten die kleinst mögliche Informationseinheit, nämlich ihre Polarisation, ähnlich den Bits in der Informatik. Diese Zustände werden daher Qubits (Quanten Bits) genannt.

In einem perfekten Kanal würden alle Qubits die von Alice versendet werden von Bob empfangen werden. Diese Annahme erweist sich bei einem echten Kanal jedoch als Trugschluss. Auf einem echten Kanal können sehr viele Qubits verloren gehen oder gar durch äußere Einflüsse verändert werden. Solange die Fehlerrate diese Übertragung jedoch unter einer gewissen Höchstgrenze bleibt, produziert das System weiterhin brauchbare Informationen die zur sicheren Schlüsselerzeugung genutzt werden können. Einige genauere Informationen finden sich in [GRTZ02] bzw. in [May96, MY98, Lüt99, SP00, NPW+00, GBS00]. Abbildung 2 zeigt schematisch einen praktischen Aufbau eines Quantenkanals.

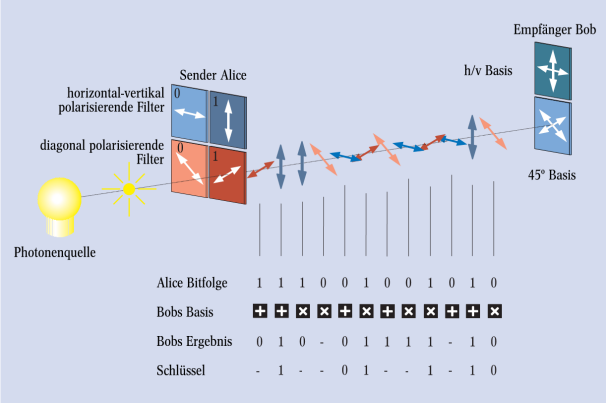


Figure 2: Praktische Umsetzung eines Quantenkanals - Quelle: W. Tittel et al., Physikalische Blätter 55 (1999) Nr. 6, S.3

Da der Quantenkanal jedoch nur zur Schlüsselerzeugung genutzt werden kann, benötigen Alice und Bob noch einen weiteren Kanal über den nach wie vor die klassisch verschlüsselten oder signierten Daten übertragen werden. Dieser Kanal kann über das öffentliche Internet hergestellt werden. Da dieser öffentliche Kanal jedoch sehr leicht abgehört werden kann, benötigen Alice und Bob authentifizierte Nachrichten die es ihnen erlauben die Echtheit der Nachrichten zu prüfen und Modifikations-Versuche von Eve zu erkennen. Der eigentliche Sinn dieses QKG-Systems besteht darin, mittels des Quantenkanals und einem zuvor auf sicherem Wege festgelegten kleinen initialen Schlüssel, weitere Schlüsselstücke zu generieren. Diese Schlüsselstücke werden nach und nach in vielen einzelnen QKG-Runden generiert und wachsen pro Runde immer stärker. Sie können somit in einer weiteren Runde für die Schlüsselerzeugung und für die Authentifizierung oder Verschlüsselung von Nachrichten genutzt werden. Im Normalfall wird der erste initiale Schlüssel zur Authentifizierung von zwei Nachrichten verwendet. Eine von Alice zu Bob und umgekehrt. Damit ist jeder Nutzer bzw. der verwendete initiale Schlüssel bei dem jeweils anderen authentifiziert. Der Prozess der Schlüsselerzeugung erfolgt in mehreren Teilphasen die in folgender Auflistung aufgezeigt sind.

1. *Raw key generation:* Erzeugung einer Qubitsequenz zwischen Alice und Bob mittels des Quantenkanals. Diese Sequenz ist jedoch

nur an einigen Stellen für Alice und Bob identisch. Dies liegt an dem verwendeten Protokoll, den Eigenschaften des Kanals und daran ob Eve gerade den Kanal abhört oder nicht.

2. *Stifing:* Bob und Alice teilen sich gegenseitig mit auf welcher Basis jeweils erzeugt bzw. gemessen wurde und verwerfen diejenigen Qubits bei denen sie unterschiedliche Basen verwendet haben.

3. *Error correction, or key reconciliation [BS94]:* In dieser Phase werden einzelne Bits, die nach dem "'Stifing"' also dem Abgleich der Basen übrig bleiben herausgezogen und von Alice und Bob verglichen. Die Fehlerrate dieser Bits gibt Aufschluss darüber ob zuviele Fehler entstanden sind, z.B. dadurch das Eve den Kanal abgehört hat. Diese Bits werden im weiteren Verlauf nicht mehr für die Authentifizierung bzw. Nachrichtenverschlüsselung benutzt.

4. *Privacy Amplification [BBR86, BBR88, BBCM95]:* Wenn das Rauschen bzw. die Fehlerrate kleiner einer zuvor festgelegten Grenze ist, können Alice und Bob dennoch nicht sicher sein das Eve nicht doch einen Teil des Schlüssels abgehört hat. In diesem Schritt wird das Wissen von Eve über den Schlüssel beliebig weit reduziert. Dazu werden mehrere Qubits der übrig gebliebenen Schlüsselsequenz zu einem Qubit zusammengefasst.

5. *Authentication [WC79, WC81, Sti91]:* Der letzte Schritt ist die eigentliche Authentifizierung einer Nachricht zwischen Alice und Bob. Dazu erzeugt Alice mithilfe eines Teils des erzeugten Schlüssels einen Tag (Tag entspricht einem speziellen für die Nachricht generierten, kryptographischen Hashwert) für ihre Nachricht und sendet beides über einen klassischen Kanal an Bob. Bob erzeugt wiederum aus ihrer Nachricht und dem Schlüssel ein Tag, vergleicht beide und authentifiziert dadurch die Nachricht auf ihre Echtheit. Im Anschluss wird der verwendete Teil des Schlüssel verworfen. Wenn die zwei Tags jedoch ungleich sind, kann davon ausgegangen werden das Eve eventuell den Kanal abgehört hat und die QKG-Runde sollte daraufhin abgebrochen werden.

Die einzelnen Authentifizierungsverfahren können durchaus unterschiedlich aufgebaut sein, die grundlegenden Schritte sind jedoch mit den zuvor beschriebenen identisch. Eves Lausch- bzw. Modifikationsversuche können auf zwei Arten detektiert werden. Zum Einen durch eine hohe Fehlerrate auf dem Quantenkanal, zum Anderen durch eine fehlerhafte Authentifizierung auf dem klassischen Kanal. Wenn die Authentifizierung über den Klassischen Kanal nicht durchgeführt wird, kann dieses System immer durch eine "'Man-In-The-Middle"'-Attacke angegriffen werden. Eve gibt sich dabei für Alice als Bob aus und für Bob als Alice. Sobald Eve den Schlüssel einer Runde erfolgreich gebrochen hat, kann sie auch jede weitere Runde erfolgreich brechen. Im weiteren Verlauf wird beschrieben, dass eine geeignete Wahl der Nachricht sich auf die Wahrscheinlichkeit den Schlüssel erfolgreich zu brechen auswirken kann. Zuerst sollen aber in Kapitel 2 einige grundlegenden Arbeiten im Bereich der Quantenkryptographie aufgezeigt werden.

2 Verwandte Arbeiten

Im Jahre 1984 wurde von Charles H. Bennett und Gilles Bassard, in ihrer Arbeit "'Quantum cryptography: Public key distribution and coin tossing"', die ersten Ansätze zum QKG bzw. ein funktionsfähiges Quantenkryptographie-Protokoll namens "'BB84-Protokoll"' veröffentlicht. Das dieses Verfahren zur Schlüsselgenerierung beweisbar sicher ist, lässt sich massgeblich auf ein Gedankenexperiment von Einstein, Podolsky und Rosen zurückführen, welches später das Einstein-Podolsky-Rosen Paradoxon genannt wurde. Dieses Gedankenexperiment ist zum Beispiel in [Bel64] näher beschrieben. William Wootters und Wojciech Zurek veröffentlichten im Jahre 1982 das No-Cloning-Theorem. Dieses Theorem beschreibt den Fakt, dass es unmöglich ist einen quantenmechanischen Zustand exakt zu kopieren. Somit können auch keine polarisierten Photonen kopiert werden ohne dabei ihren Zustand zu verändern. Ben-Or, Horodecki, Leung, Mayers und Oppenheim beschreiben ihn ihrem Werk "'The universal composable security of quantum key distribution"' potentielle Sicherheitslücken des QKG und schließen diese Lücke durch die Verwendung eines universell zusammensetzbaren Theorems, welches für die Konfiguration der Quanten bzw. des Quantenkanals genutzt werden kann.

3 Authentifizierungsphase

Die Authentifikationsphase in einem QKG-System beruht auf der Wegman-Carter Authentifizierung. Diese stellt das Äquivalent zur Vernam Verschlüsselung bzw. dem "'One-Time-Pad"' in der Kryptographie dar. Zusätzliche Informationen über das "'One-Time-Pad"' befinden sich in [Sch93]. In der Wegman-Carter Authentifizierung sind alle erzeugten Tag-Kombinationen gleich wahrscheinlich solange auch alle Schlüssel-Kombinationen gleich wahrscheinlich sind. Da ein erzeugter Tag kürzer ist als die dazugehörige Nachricht, ist es wahrscheinlicher einen korrekten Tag zu schätzen als die komplette entschlüsselte Nachricht. Da man den Tag bei der Wegman-Carter Authentifizierung aber immer entsprechend lang hält, ist auch diese Wahrscheinlichkeit sehr gering. Im Gegensatz zu der Vernam-Verschlüsselung bei der die Schlüssellänge linear (sogar proportional) mit der Nachrichtenlänge wächst, wächst der Schlüssel bei der Wegman-Carter Authentifizierung logarithmisch mit der Nachrichtenlänge. Dies ist ein wichtiges Merkmal dieses Verfahrens, da somit nur genügend QKG-Runden durchgeführt werden müssen um Schlüssel mit ausreichender Länge zu erhalten.

Eine wesentliche Eigenschaft dieser Wegman-Carter Authentifizierung beschreiben die darin verwendeten universellen Hash-Funktionen. Dabei stellt $\mathcal{H}$ eine Teilmenge von Hash-Funktionen dar, die eine Nachricht aus der Teilmenge der möglichen Nachrichten $\mathcal{M}$ auf einen Tag aus der Teilmenge der möglichen Tags $\mathcal{T}$ abbildet. Die folgenden zwei Definitionen sind aus [Sti91] entnommen worden.

1. Die Anzahl an Hashfunktionen in $\mathcal{H}$ die eine willkürliche Nachricht $m_1 \in \mathcal{M}$ in einen willkürlichen Tag $t_1 \in \mathcal{T}$ abbilden ist genau $|\mathcal{H}|/|\mathcal{T}|$. Dabei beschreibt der Schrägstrich die Kardinalität also die Anzahl der Elemente pro Teilmenge.

2. Der Anteil derer Funktionen die zudem eine willkürliche Nachricht $m_2 \neq m_1$ in $\mathcal{M}$ in einen willkürlichen Tag $t_2 \in \mathcal{T}$ abbilden, wobei $t_1 = t_2$ ist, ist nicht größer als ϵ.

Der Wert von ϵ beschreibt dabei eine Kompromissgröße zwischen der Größe der Teilmenge $\mathcal{H}$ und der Wahrscheinlichkeit den korrekten Tag zu schätzen. Die Untergrenze von $\epsilon = 1/|\mathcal{T}|$ wird erreicht, wenn man eine recht große Familie von Hashfunktionen verwendet. Wegman und Carter haben in [WC79] einige Beispiele aufgeführt die diesen Sachverhalt näher beschreiben. Diese Familien sind jedoch zu groß um sie in dem QKG zu verwenden. Wegman und Carter zeigen aber, dass nur durch eine Verdopplung der Wahrscheinlichkeit um einen Tag korrekt zu schätzen, eine wesentlich kleinere $2/|\mathcal{T}|$-ASU_2 Familie genutzt werden kann. Diese kleineren Familien können in dem QKG verwendet werden. Es existieren eine Vielzahl solcher Familien. Welche man verwendet spielt keine wesentliche Rolle. In der weiteren Betrachtung wird die Familie die auch im original Beispiel aus [WC81] verwendet wurde genutzt.
In folgendem Abschnitt soll die Authentifizierungsphase näher erläutert werden. Alice und Bob tauschen einen Schlüssel k untereinander aus, der gerade groß genug ist, um eine Hashfunktion $h_k \in \mathcal{H}$ wobei $0 \leq k < |\mathcal{H}|$ ist auswählen zu können. Alice möchte das Bob die Nachricht $m_A \in \mathcal{M}$ erhält und sendet einerseits m_A andererseits $t_A = h_k(m_A)$ an Bob. Dieser verifiziert das $t_A = h_k(m_A)$ ist und akzeptiert daraufhin diese Nachricht. Im Anschluss wird der Schlüssel k verworfen. Die dritte Person in dieser fiktiven Runde ist wiederum Eve. Diese hat Zugriff auf den Kommunikationskanal zwischen Alice und Bob und möchte, dass Bob eine von ihr gefälschte Nachricht $m_E \in \mathcal{M}$ annimmt. Sie kennt den Schlüssel k nicht, daher ist für sie der Schlüssel im kompletten Bereich zwischen $0 \leq k < |\mathcal{H}|$ gleichartig.

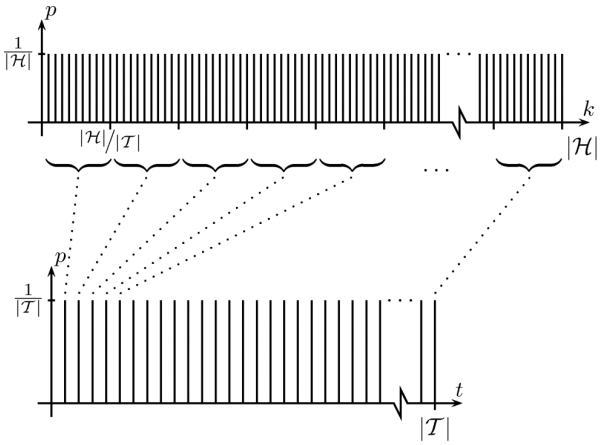


Figure 3: Darstellung wie mehrere Teilmengen von Schlüssel bzw. Hashfunktionen auf einzelne Tags abgebildet werden.

Definition 1 besagt, dass sobald K gleichartig in seinem kompletten Bereich ist, so ist dies auch T_E.

Daher entspricht Eves Tag $T_E = h_k(m_E)$. Abbildung 3 zeigt diesen Sachverhalt. Eve kann nun den korrekten Tag für ihre Nachricht schätzen, jedoch nur mit einer Wahrscheinlichkeit von

$$P(T_E = t) = 1/|\mathcal{T}| \quad (1)$$

.

Eine weitere Möglichkeit ist, dass Eve wartet bis Alice an Bob eine Nachricht sendet. Eve fängt diese Nachricht und den entsprechenden Tag ab und stellt sicher, dass Bob diese Nachricht nicht erreicht (Man-In-The-Middle). Da sie nun einerseits m_A und andererseits $t_A = h_K(m_A)$ kennt, kann sie mit genügend Rechenleistung die nicht passenden Schlüssel aussortieren und hat nur noch $1/|\mathcal{T}|$ der ursprünglichen Schlüssel übrig um davon den Richtigen zu schätzen, siehe dazu Abbildung 4.

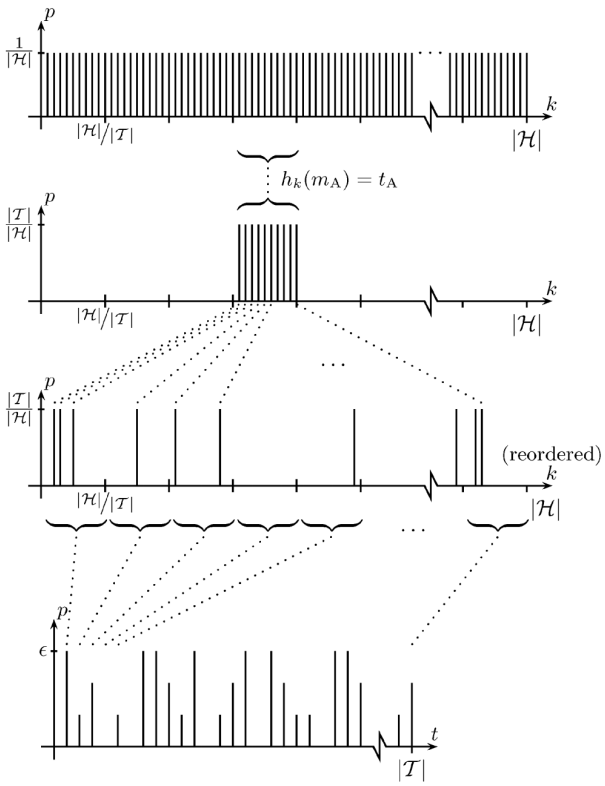


Figure 4: In der Wegman-Carter Authentifizierung entspricht ein Nachrichten-Tag Paar einer bestimmten Teilmenge von Schlüsseln, welche die gegebene Nachricht auf den entsprechenden Tag abbilden. Eine weitere Nachricht entspricht einer weiteren Teilmenge, die die Anzahl an restlichen Schlüsseln weiter erhöht, sodass alle Tags eine Wahrscheinlichkeit kleiner oder gleich ϵ besitzen.

Definition 1 besagt weiterhin, dass Eve auch mit diesem Wissen den korrekten Tag T_E für ihre Nachricht $m_E \neq m_A$ nur mit einer Wahrscheinlichkeit von

$$P(T_E = t | h_K(m_A) = t_A) \leq \epsilon \quad (2)$$

schätzen kann.

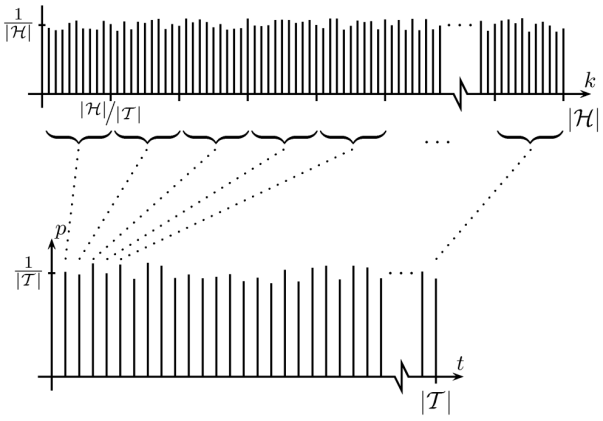
Der Parameter ϵ beschreibt eine Obergrenze der Wahrscheinlichkeit für Eve ohne Informationen über den Schlüssel eine korrekte Schätzung über den Schlüssel zu treffen, einen Tag ihrer Nachricht zu erstellen, welchen Bob dann als echtes Nachricht-Tag Paar erkennt. Die Sicherheit dieser Wegman-Carter Authentifizierung wird in den folgenden Zeilen näher betrachtet. Die Wahrscheinlichkeit, dass Eve den korrekten Tag für ihre Nachricht m_E schätzt, hängt nicht von Alice gesendeter Nachricht m_A ab, solange diese beiden Nachrichten nicht gleich sind. Die Wahrscheinlichkeit ist immer kleiner als ϵ. Dies kann in anderen Worten folgendermaßen beschrieben werden: Es gibt keine Nachrichten-Tag Paare von Alice die kritischer bzw. schwächer sind als Andere. Auch wenn Eve die Nachricht m_A (ungleich m_E) selbst auswählen kann und den entsprechenden Tag für diese Nachricht besitzt, erhält sie keine weiteren, nützlichen Informationen die ihr helfen einen entsprechenden Tag für ihre Nachricht zu finden. Dieser Fakt scheint momentan noch unnütz wird jedoch im späteren Verlauf noch wichtig werden.

Wenn Eve versucht das System zu brechen und dieses Vorgehen wird erfasst, wird die QKG Runde abgebrochen. Ein weiterer Schwachpunkt liegt an der Fehleranfälligkeit der Authentifizierung. Durch Rauschen des Übertragungskanals können Fehler entstehen, die auch ohne das Zutun von Eve auftreten können. Somit kann Eve immer mal wieder versuchen den Kanal abzuhören, bzw. zu modifizieren ohne das dies merklich auffällt. Sie darf dies natürlich nicht zu häufig versuchen, da ansonsten die Fehlerrate für diesen Kanal überschritten wird. Der Parameter ϵ sollte so gewählt werden, dass auch wenn Eve diese Modifikationen durchführt, das System solange bestehen bleiben kann wie Alice und Bob dieses benötigen. Für die in [WC81] beschriebene $2/|T| - ASU_2$ Familie ergibt sich durch Auswahl eines 32-Bit Tags eine Wahrscheinlichkeit von 2^{-31} den korrekten Tag auszuwählen, in Anbetracht das niemals zuvor ein Nachrichten-Tag Paar betrachtet wurde. Somit benötigt Eve im Mittel $2^{31} \approx 2.1 * 10^9$ Versuche.

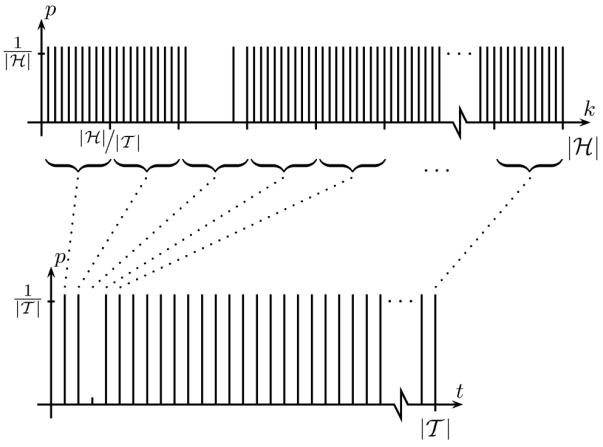
Geht man davon aus, dass ein von Eve erzeugter Fehlversuch alle 10 Sekunden durchgeführt werden kann, ohne das dies von Alice bzw. Bob bemerkt wird, dann dauert das Finden des gültigen Tags im Mittel 680 Jahre. Lange genug für die meisten Anwendungen.

4 Partielles Teilwissen über den Schlüssel

Im vorangegangenen Kapitel wurde davon ausgegangen, dass Eve keinerlei Informationen über den Schlüssel K hat. Für sie war dieser Schlüssel nichts anderes als eine Zufallszahl. Dies stellt jedoch eine für das QKG unrealistische Annahme dar! Um die Sicherheit zu erhöhen kann eine sogenannte "'Privacy Amplification"' durchgeführt werden. Dadurch werden Eves Information weiter verringert. Solange der gesamte "'Pre-Shared-Key (Schlüsselsequenz nach dem Stifing)"' genutzt wird, müssen Alice und Bob der Authentifizierung unter Verwendung dieses Schlüssels vertrauen, auch wenn dieser nicht vollkommen sicher ist.



(a)



(b)

Figure 5: Eves Teilwissen über den Schlüssel führt zu einer uneinheitlichen Wahrscheinlichkeitsverteilung für die Schlüssel k demnach auch für die Tags t. Bild a) zeigt eine uneinheitliche Verteilung der Schlüssel k, somit ist auch t uneinheitlich verteilt. Bild b) zeigt eine asymetrische Verteilung falls Eve Schlüssel entfernen kann.

Wenn Eve in vorangegangenen Runden des QKG Vorwissen über den Schlüssel sammeln konnte, jedoch kein Nachrichten-Tag Paar (wie in Abbildung 5 gezeigt) ausgelesen hat, dann kann die obere Grenze für die Wahrscheinlichkeit einen korrekten Tag zu schätzen als die Summe der $|\mathcal{H}|/|\mathcal{T}|$ wahrscheinlichsten Schlüssel, angegeben werden. Diese Grenze ist als minimale Entropie definiert:

$$H_\infty(K) = \min_k -log_2 P(K = k) \tag{3}$$

.

Die Wahrscheinlichkeit für einen gegebenen Wert einen korrekten Tag zu schätzen wird nun maximal, wenn die Wahrscheinlichkeiten von $P(K = k)$ genau gleich sind. Dies ist genau dann der Fall, wenn Eve ihr gesammeltes Wissen dazu ausnutzt, Schlüssel die nicht sein können aus der Teilmenge der möglichen Schlüssel zu entfernen.

$$\mathcal{H}_E = \mathcal{H} \backslash \{h_1, \ldots, h_n\} \tag{4}$$

. Aus ihrer Sicht befindet sich der echte Schlüssel nun in $|\mathcal{H}_E| = r|\mathcal{H}|$ die alle die Wahrscheinlichkeit $H_\infty(K) = log_2 r|\mathcal{H}|$ besitzen. Fügen man diese Erkenntnisse zusammen, kann folgenden Formulierung getroffen werden:

$$P(T_E = t) \leq \sum_1^{|\mathcal{H}|/|\mathcal{T}|} \frac{1}{r|\mathcal{H}|} = \frac{1}{r|\mathcal{T}|} \tag{5}$$

.

Die Wahrscheinlichkeit den korrekten Tag zu erraten erhöht sich genau dann, wenn der Parameter r kleiner 1 ist. WeißEve nichts über den Schlüssel, dann beschreibt ihre minimal Entropie der vermutlichen Schlüssel genau die Wahrscheinlichkeit $1/|\mathcal{T}|$. Hat Eve jedoch ein wenig Information über den Schlüssel und greift ein Nachrichten-Tag Paar $m_A + t_A$ von Alice ab, erhöht sich ihr Wissen über den Schlüssel. Das Nachrichten-Tag Paar identifiziert eine Teilmenge von Schlüssel bzw. Hashfunktionen der Größe $|\mathcal{H}|/|\mathcal{T}|$ aus welchen der Schlüssel ausgewählt werden musste.

$$\mathcal{H}_{t_A} = \{h \in \mathcal{H} : h(m_A) = t_A\}. \quad (6)$$

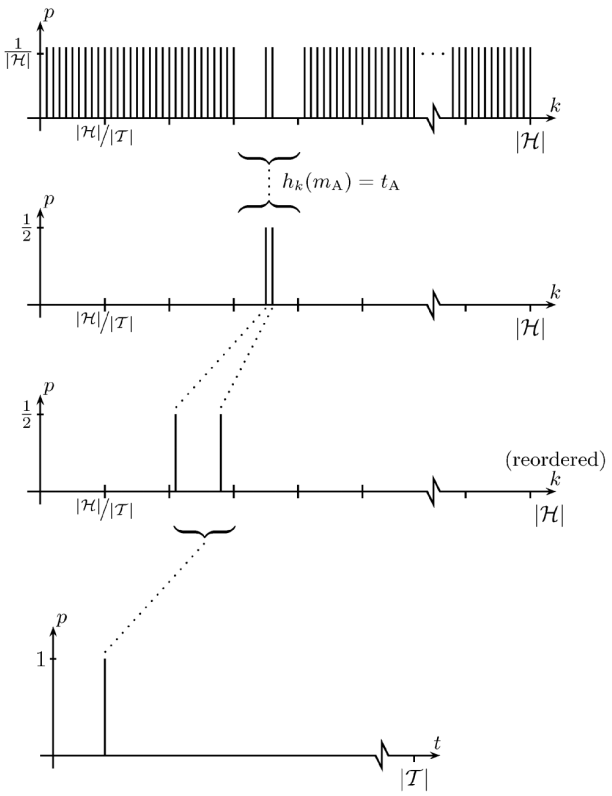


Figure 6: Eve kann durch ihre Teilwissen Schlüssel aussortieren die nicht verwendet wurden. Es kann passieren das Eve so viele Schlüssel aus den Teilmengen entfernen kann, dass nur noch wenige übrig bleiben, die ihre Nachricht auf nur noch einen Tag abbilden.

Angenommen, dass die Menge der möglichen Schlüssel eher $\mathcal{H}_E$ als $\mathcal{H}$ ist, dann ist die gesamte Menge der möglichen Schlüssel nicht $\mathcal{H}_{t_A}$ sondern $\mathcal{H}_{t_A} \cap \mathcal{H}_E$. Im besten Fall befindet sich nur ein Schlüssel in der Teilmenge und Eve weißdirekt welcher Schlüssel verwendet wurde. Aber auch wenn sich mehrere Schlüssel in dieser Teilmenge befinden, kann Eve den korrekten Schlüssel herausfinden wie in Bild 6 gezeigt. Wird diese Aussage noch etwas verfeinert,

$$|\mathcal{H}_{t_A} \cap \mathcal{H}_E| \leq \epsilon|\mathcal{H}|/|\mathcal{T}| \quad (7)$$

dann können Nachrichten existieren für die gilt:

$$\forall h_1, h_2 \in \mathcal{H}_{t_A} \cap \mathcal{H}_E, h_1(m) = h_2(m). \quad (8)$$

Für diese Nachricht werden für alle restlichen Schlüsseln ein identischer Tag erstellt. Die maximale Anzahl dieser Nachrichten $\epsilon|\mathcal{H}|/|\mathcal{T}|$ ist in der zweiten Anforderung von Definition 1. beschrieben. Die Anzahl der Nachrichten mit dieser Eigenschaft steigt, wenn $|\mathcal{H}_{t_A} \cap \mathcal{H}_E|$ kleiner wird als $\epsilon|\mathcal{H}|/|\mathcal{T}|$. Wenn eine dieser Nachrichten mit m_E übereinstimmt, kann Eve die Authentifizierung brechen. Sie weiß zwar nicht alles über den Schlüssel k, jedoch genug um für ihr Nachricht den richtigen Tag $t_E = h_k(m_E)$ zu erstellen. Falls Eves Nachricht nicht mit einer dieser schwachen Nachrichten übereinstimmt, kann sie ihre Nachricht auf bestimmte Arten modifizieren bis sie übereinstimmt. Der schlechteste Fall ist dann gegeben sobald Eve ihre Nachricht komplett selbst wählen und den entsprechenden Tag t_E generieren kann. Die funktioniert jedoch nur solange die Bedingung 7 gilt. An diesem Punkt wird davon ausgegangen das Eve in der Lage ist genau dies zu tun. Weitere Anmerkungen finden sich in Kapitel 7. Diese Annahme impliziert jedoch den Fakt, dass auch wenn $|\mathcal{H}_{t_A} \cap \mathcal{H}_E| > \epsilon|\mathcal{H}|/|\mathcal{T}|$ Eve nach wie vor ihre Nachricht m_E so wählen kann, dass $\epsilon|\mathcal{H}|/|\mathcal{T}|$ Schlüssel in $\mathcal{H}_{t_A} \cap \mathcal{H}_E$ den korrekten Tag für ihre Nachricht erzeugen. Die Wahrscheinlichkeit, mit diesen zwei Informationen den korrekten Tag zu erstellen, beträgt:

$$P(T_E = t|K \in \mathcal{H}_{t_A} \cap \mathcal{H}_E) \leq \frac{\epsilon|\mathcal{H}|/|\mathcal{T}|}{\mathcal{H}_{t_A} \cap \mathcal{H}_E}. \quad (9)$$

Die Wahrscheinlichkeit dafür, dass Eve den vor dem erfolgreichen Lesen des Tag t_A ihren Tag t_E korrekt schätzt liegt bei:

$$P(T_E = t|K \in \mathcal{H}_E)$$

$$= \sum_{r=1}^{|\mathcal{T}|} P(K \in \mathcal{H}_r \cap \mathcal{H}_E) \times P(T_E = t|K \in \mathcal{H}_r \cap \mathcal{H}_E)$$

$$\leq \sum_{r=1}^{|\mathcal{T}|} \frac{|\mathcal{H}_r \cap \mathcal{H}_E|}{r|\mathcal{H}|} \times \frac{\epsilon|\mathcal{H}|/|\mathcal{T}|}{\mathcal{H}_r \cap \mathcal{H}_E} = \frac{\epsilon}{r} \quad (10)$$

.

Da Bedingung 5 besagt, dass die Wahrscheinlichkeit nur schwach steigt wenn der Faktor r nahe 1 ist, kann das System als sicher betrachtet werden.

Wenn Eve sowohl die Nachricht wie auch den entsprechenden Tag ausgelesen bekommt, muss

sie entscheiden ob sie diese mit ihrer eigenen Nachricht ersetzt. Um dies abschätzen zu können, sollte die angegebene Grenze aus Formel 9 benutzt werden. Die rechte Seite der Formel wird nahe 1 wenn bestenfalls $\epsilon|\mathcal{H}|/|\mathcal{T}|$ Schlüssel in $|\mathcal{H}_{t_A} \cap \mathcal{H}_E|$ übrig sind. Ist dies der Fall hat Eve genügend Informationen zur Hand um zu entscheiden ob sie den Angriff durchführen kann oder nicht, schon bevor sie das Nachrichten-Tag Paar ersetzt hat. Sie kann nun immer entscheiden ob das Nachrichten-Tag Paar erfolgreich ersetzt werden kann oder nicht. Sie stellt mit diesem Vorgehen sicher, dass sie nicht erkannt wird.

Der gesamte Ablauf des Lauschvorgangs wird in folgenden Zeilen zusammengefasst beschrieben.
Eve hört den Quantenkanal in einer Art und Weise ab, dass sie sicher sein kann nicht zu viele Störungen zu verursachen, was ihre Anwesenheit durch eine zu hohe Fehlerrate deutlich machen würde. Das Ziel von Eve ist in diesem Falle nicht die abgehörten Informationen dazu zu nutzen die Nachrichten zu entschlüsseln, sondern sie möchte damit eigenen Nachrichten einen korrekten Tag geben können. Sie fängt jede von Alice gesendete Nachricht ab und nutzt diese weiteren Informationen dazu, den gültigen Tag für ihre gefälschte Nachricht zu bestimmen. Dieser Vorhaben wird aber nur unter folgenden Bedingungen erfolgreich sein. Wenn,

1. die Nachricht m_A die von Alice gesendet wurde so aufgebaut ist, dass gerade in mindestens einer Teilmenge (wie in Bild 4 gezeigt) weniger als $\epsilon|\mathcal{H}|/|\mathcal{T}|$ Schlüssel sind.

2. der Schlüssel den Eve willkürlich auswählt, sich in einer solchen Teilmenge befindet.

Da Eve herausfinden kann wann ihr Angriff erfolgreich sein wird, z.B. wenn die übrig gebliebenen Schlüssel, ihre Nachricht alle auf den selben Tag abbilden. Ist dies der Fall, dann wird sie das Nachrichten-Tag Paar von Alice nur dann ersetzen wenn sie dies herausgefunden hat. Solange sich Eve passiv verhält muss sie ohnehin nicht befürchten entdeckt zu werden. Dieser Angriff kann im Gegensatz zu der zuvor beschrieben, spärlichen Strategie in jeder Runde erneut durchgeführt werden. Eves Wahrscheinlichkeit ist dann durch Formel 9 beschrieben.

5 Sicherheitsaspekte

In diesem Abschnitt soll das Ausmaß der Bedrohung, welche von Eve ausgeht, genauer betrachtet werden. Es wird davon ausgegangen, dass sie mit wenig Information über den Schlüssel ein korrektes Nachrichten-Tag Paar erstellen kann. Anfangs wird davon ausgegangen das Eve, mit ihrem anfänglichen Wissen über den Schlüssel nichts weiter machen kann als willkürlich Schlüssel, aus ihrer Liste der möglichen Schlüssel, zu löschen. Die Nachrichten-Tag Paare die Eve abfängt, entsprechen dem Ziehen von $|\mathcal{H}|/|\mathcal{T}|$ Schlüsseln aus einer Menge $\mathcal{H}$ ohne Zurücklegen. Der echt Schlüssel wird immer in den gezogenen Schlüsseln vorhanden sein und sich zudem in der Menge der restlichen möglichen Schlüssel befinden. Während die anderen $|\mathcal{H}|/|\mathcal{T}| - 1$ Schlüssel aus der Menge $|\mathcal{H}| - 1$ gezogen werden, wobei $r|\mathcal{H}| - 1$ möglich sind. Als Beispiel sei die Teilmenge H_E genannt. Die Anzahl der möglichen gezogenen Schlüssel X, beschreibt eine Zufallsvariable. Entfernt man den echten Schlüssel, dann beschreibt die neue Zufallsvariable $X - 1$ eine hypergeometrische Verteilung.

$$(X-1) \in Hyp\left(|\mathcal{H}| - 1, \frac{|\mathcal{H}|}{|\mathcal{T}|} - 1, \frac{r|\mathcal{H}| - 1}{|\mathcal{H}| - 1}\right) \quad (11)$$

.

Anmerkung: Die hypergeometrische Verteilung beschreibt die Wahrscheinlichkeit, bei N gegebenen Elementen, von denen M die gewünschte Eigenschaft besitzen, beim Herausgreifen von n Probestücken genau k Treffer zu erzielen. In anderen Worten, die Wahrscheinlichkeit dafür, dass in $nVersuchen X = kErfolge$ stattgefunden haben.

Umformuliert bedeutet dies:

$$P(X=i) = \frac{\binom{r|\mathcal{H}| - 1}{i-1}\binom{|\mathcal{H}| - r|\mathcal{H}|}{|\mathcal{H}|/|\mathcal{T}| - i}}{\binom{|\mathcal{H}| - 1}{|\mathcal{H}|/|\mathcal{T}| - 1}} \quad (12)$$

.

Der ausschlaggebende Fall ist derer, bei dem die Anzahl der gezogenen Schlüssel kleiner ist als $\epsilon|\mathcal{H}|/|\mathcal{T}|$ oder präziser ausgedrückt:

$$P\left(X \leq \epsilon\frac{|\mathcal{H}|}{|\mathcal{T}|}\right) = \sum_{i=1}^{\epsilon|\mathcal{H}|/|\mathcal{T}|} \frac{\binom{r|\mathcal{H}|-1}{i-1}\binom{|\mathcal{H}|-r|\mathcal{H}|}{|\mathcal{H}|/|\mathcal{T}|-i}}{\binom{|\mathcal{H}|-1}{|\mathcal{H}|/|\mathcal{T}|-1}} \tag{13}$$

Die Annahme über diese Wahrscheinlichkeitsverteilung ist schwer zu bewerten, kann jedoch mit der Chebyshev Ungleichung abgeschätzt werden.

$$P(|X-\mu| \geq c\sigma) \leq 1/c^2 \tag{14}$$

Diese Chebyshev Ungleichung beschreibt die Wahrscheinlichkeitsverteilung jedoch ziemlich "'ungenau"'. Es kann aber für diese Formel eine generelle Gültigkeit veranschlagt werden, die für die weitere Betrachtung ausreichend ist. Daraus folgt die folgende Formulierung.

$$P\left(X \leq \epsilon\frac{|\mathcal{H}|}{|\mathcal{T}|}\right) = P\left(\mu - X \geq \mu - \epsilon\frac{|\mathcal{H}|}{|\mathcal{T}|}\right)$$

$$\leq P\left(|X-\mu| \geq \mu - \epsilon\frac{|\mathcal{H}|}{|\mathcal{T}|}\right)$$

$$= P\left(|X-\mu| \geq \frac{\mu - \epsilon\frac{|\mathcal{H}|}{|\mathcal{T}|}}{\sigma}\sigma\right)$$

$$\leq \frac{\sigma^2}{\left(\mu - \epsilon\frac{|\mathcal{H}|}{|\mathcal{T}|}\right)^2} \tag{15}$$

Der Mittelwert beträgt in diesem Fall

$$\mu = \left(\frac{|\mathcal{H}|}{|\mathcal{T}|} - 1\right)\frac{r|\mathcal{H}|-1}{|\mathcal{H}|-1} + 1 \tag{16}$$

und die Standardabweichung

$$\sigma = \sqrt{\left(\frac{|\mathcal{H}|}{|\mathcal{T}|} - 1\right)\frac{r|\mathcal{H}|-1}{|\mathcal{H}|-1}\left(1 - \frac{r|\mathcal{H}|-1}{|\mathcal{H}|-1}\right)\frac{|\mathcal{H}|-|\mathcal{H}|/|\mathcal{T}|}{|\mathcal{H}|-2}} \tag{17}$$

.

Dies vereinfacht die asymtotische Ordnung erheblich.

$$r|\mathcal{H}| \gg r|\mathcal{H}|/|\mathcal{T}| \gg 1 \tag{18}$$

.

In dieser vereinfachten Ordnung ist der Mittelwert und die Standardabweichung folgendermaßen definiert:

$$\mu = r\frac{|\mathcal{H}|}{|\mathcal{T}|} \; und \; \sigma = \sqrt{r(1-r)}\frac{|\mathcal{H}|}{|\mathcal{T}|} \tag{19}$$

Dies hat nun die folgende Wahrscheinlichkeitsverteilung zur Folge

$$P\left(X \leq \epsilon\frac{|\mathcal{H}|}{|\mathcal{T}|}\right) \leq \frac{r(1-r)\frac{|\mathcal{H}|}{|\mathcal{T}|}}{\left(r\frac{|\mathcal{H}|}{|\mathcal{T}|} - \epsilon\frac{|\mathcal{H}|}{|\mathcal{T}|}\right)^2} = \frac{r(1-r)|\mathcal{T}|}{(r-\epsilon)^2|\mathcal{H}|} \tag{20}$$

.

Sobald $r \gg \epsilon$ lässt sich diese Gleichung folgendermaßen vereinfachen.

$$P\left(X \leq \epsilon\frac{|\mathcal{H}|}{|\mathcal{T}|}\right) \leq \frac{1-r}{r}\frac{|\mathcal{T}|}{|\mathcal{H}|} \tag{21}$$

In der Praxis ist die rechte Konstante der Gleichung ziemlich klein.

Die $2/|\mathcal{T}| - ASU_2$ Hashfamilie aus [WC81] hat die Größe

$$|\mathcal{H}| = |\mathcal{T}|^{4\log\log|\mathcal{M}|} \tag{22}$$

.

Wählt man beispielsweise eine 100kBit Nachricht und einem 32-Bit breiten Tag, erhält man eine Größe der Hash-Menge von

$$|\mathcal{H}| \approx 2^{32\times4\times17} = 2^{2176} \tag{23}$$

. Diese Rechnung zeigt, dass ein ungefähr 2kBit großer Schlüssel verwendet wird.

Geht man davon aus, dass Eve jedes achte Bit der Schlüsselsequenz als Vorwissen zur Verfügung hat ($r \approx 0.917$), dann beträgt die Wahrscheinlichkeit den Tag in einer Runde zu finden, $3,5 \times 10^{-647}$. Wenn sie 1000 Runden pro Sekunde durchführen kann, dann benötigt sie im Schnitt 10^{635} Jahre um den Tag zu finden. Es ist ersichtlich, dass dieses

Vorgehen viel länger dauert als wenn sie nur jeweils alle 10 Sekunden einen Schlüssel erraten würde. Auch wenn Eve durch ihre Technik Wissen über den Schlüssel erlangen konnte, so hat dies keine merkliche Steigerung der Wahrscheinlichkeit einen korrekten Tag zu schätzen zur Folge. Eve hat jedoch noch einen zusätzlichen Plan, der ihr helfen kann diese Informationen besser zu nutzen. Dieser Plan soll in dem folgenden Abschnitt 6 näher betrachtet werden.

6 Möglicher Angriff

Eves größte Hürde bei dieser Technik stellt die Chebyshev Ungleichung dar. Um dies mit anderen Worten auszudrücken: Der "'Zentrale Grenzwertsatz"' stellt in diesem Zusammenhang sicher, dass nahezu alle Teilmengen mit großer Wahrscheinlichkeit eine Anzahl an Schlüssel enthalten, die sehr nahe bei $r|\mathcal{H}|/|\mathcal{T}| \gg \epsilon|\mathcal{H}|/|\mathcal{T}|$ liegen. Eves Möglichkeit den Schlüssel zu brechen steigt drastisch an, wenn die restlichen Schlüssel nur in zwei Teilmengen aufgeteilt werden können. Darin befinden sich einerseits $\epsilon|\mathcal{H}|/|\mathcal{T}|$, andererseits $|\mathcal{H}|/|\mathcal{T}|$ viele Schlüssel. Tritt dieser Fall auf, dann hat das Argument der Chebyshev Ungleichung kein Gewicht mehr. Ist der korrekte Schlüssel in einer solchen Teilmenge, in der $\epsilon|\mathcal{H}|/|\mathcal{T}|$ Schlüssel sind, dann hat Eve die Möglichkeit durch die zuvor beschriebene Freiheit, Nachrichten-Tag Paare selbst zu erstellen, den entsprechenden richtigen Tag für ihre Nachricht herauszufinden.

Es existieren mehrere Möglichkeiten wie Eve diese Teilmengen an ihre Bedürfnisse anpassen kann. Die Einfachste ist das einfache Abändern der ursprünglichen Nachricht. Die Nachricht die von Alice an Bob gesendet wird, enthält einige Informationen über den Quantenkanal. Eve kann diese Informationen auslesen und verändern. Dies bedeutet, dass Eve in einem kleinen Rahmen Einfluss auf den Inhalt der gesendeten Nachricht hat. Daraus folgt, dass Eve in der Lage ist die Teilmengen der Schlüssel zu verändern. Die Veränderungen, die Eve auf dem Quantenkanal durchführt, unterscheiden sich von denen die auftreten, wenn sie Informationen von dem Kanal ausliest. Diese dürfen nicht durch den Abgleichungsprozess des BB84 Protokolls entdeckt werden. Es dürfen somit keine zusätzlichen Störungen auf dem Kanal auftreten.

Das hier vorgestellte Vorgehen beschreibt eine andere Art um nützliche Informationen vom System zu erlangen. Es wird nicht versucht zusätzliche Informationen über den Schlüssel zu erlangen, sondern den Nutzen der Information die sie aus vorangegangenen Runden gesammelt hat, zu erhöhen. Wenn davon ausgegangen wird das Eve dies so gut es nur irgend möglich ist macht, dann können die Teilmengen entweder $\epsilon|\mathcal{H}|/|\mathcal{T}|$ oder $\epsilon|\mathcal{H}|/|\mathcal{T}|$ Schlüssel enthalten. Ist dies genau so der Fall, dann entspricht die Wahrscheinlichkeit für einen Erfolg genau der Wahrscheinlichkeit, dass sich der korrekte Schlüssel in der Teilmengen mit der Schlüsselanzahl von $\epsilon|\mathcal{H}|/|\mathcal{T}|$ befindet.
Die Anzahl dieser entstandenen Teilmengen beträgt dann

$$n = \frac{\text{\# eliminated keys}}{\text{\# eliminated keys in a "'good"' subset}}$$

$$= \frac{(1-r)|\mathcal{H}|}{(1-\epsilon)|\mathcal{H}|/|\mathcal{T}|} \tag{24}$$

und die Wahrscheinlichkeit, dass der Schlüssel sich in solch einer Teilmenge befindet liegt bei

$$P\left(X \leq \epsilon\frac{|\mathcal{H}|}{|\mathcal{T}|}\right) = \frac{\text{\# possible keys in "'good"' subsets}}{\text{\# possible keys}}$$

$$= \frac{n\epsilon|\mathcal{H}|/|\mathcal{T}|}{r|\mathcal{H}|} = \frac{1-r}{r}\frac{\epsilon}{1-\epsilon} \tag{25}$$

.

Die Änderung der Wahrscheinlichkeitsverteilung von Gleichung 21 nach 25 bedeutet einen enormen Anstieg der Wahrscheinlichkeit. In der $2/|\mathcal{T}| - ASU_2$ Hashfamilie ist der Unterschied zwischen $|\mathcal{T}|/|\mathcal{H}|$ und $\epsilon/(1-\epsilon)$ enorm. Dies zeigt sich wenn mithilfe der Formel 22 folgende neue Formulierung gewählt wird

$$\frac{|\mathcal{T}|}{|\mathcal{H}|} = \frac{1}{|\mathcal{T}|^{4\log\log|\mathcal{M}|-1}} \ll \frac{2}{|\mathcal{T}|} = \epsilon < \frac{\epsilon}{1-\epsilon} \tag{26}$$

.

Dieser Sachverhalt soll nochmals anhand eines Beispiels verdeutlicht werden. Es wurde eine $2/|\mathcal{T}| - ASU_2$ Hashfamilie, ein 32-Bit breiter Tag und 1/8-Bit Initiales Wissen über den Schlüssel veranschlagt. Dies entspricht einem r von ungefähr $0,9170$. Die Wahrscheinlichkeit für ein erfolgreiches Schätzen des Schlüssels liegt dann bei $4,2 * 10^{-11}$. Wenn nun wiederum davon ausgegangen wird, dass man 1000 Runden pro

Sekunde durchführen kann, dann benötigt Eve im Schnitt 9 Monate um das System zu brechen ohne zwischenzeitlich detektiert zu werden. Ein Vergleich diese Zeit und der zuvor berechneten Zeit, um das System zu brechen zeigt auf, dass dieses Verfahren ein erhebliches Sicherheitsproblem darstellt. Auch dann wenn Eve nicht in der Lage ist die idealen Teilmengen zu finden. Der wesentliche theoretische Aspekt dieses Angriffs liegt darin, dass die Wegman-Carter Authentifizierung kryptographisch unsicher ist, sobald man einen Teil des Schlüssels oder Teilwissen über diesen Schlüssel besitzt. Besitzt man einen 100% sicheren Schlüssel, dann ist auch diese Authentifizierung sicher.
Die Wahrscheinlichkeit dafür, dass Eve den korrekten Tag schätzt hängt in dieser Betrachtung stark davon ab, welche Nachricht m_A von Alice gesendet wird. Nicht nur dann wenn die Nachrichten $m_A \; und \; m_E$ gleich sind, sondern auch wenn diese verschieden voneinander sind. Es steht somit fest, dass es in der Tat mehr und weniger sichere Nachrichten-Tag Paare gibt, die von Alice versendet werden können. Während der QKG-Runden kann Eve die Nachricht m_A von Alice, mithilfe des Quantenkanals, modifizieren und erhält zudem den Tag für diese Nachricht. Dadurch verbessert sich die Möglichkeit für sie den korrekten Tag t_E für ihre Nachricht m_E zu bestimmen. Es ist klar, das ein einfaches Senden der Nachricht und des entsprechenden Tag, auch wenn Eve wenigstens etwas Wissen über den Schlüssel besitzt, langfristig dennoch nicht funktioniert, da ein stupides durchprobieren sehr schnell erkannt wird. Das bisschen Information, welches Eve über den empfangenen Tag t_A von Alice erhält, kann mit dem Wissen das Eve zuvor schon gesammelt hat, aber ausreichend sein, damit sie sich sicher sein kann, ob der Angriff funktionieren wird oder nicht.

7 Vorbeugende Maßnahmen

Damit dieses System trotzdem von Eve geschützt werden kann, müssen geeignete Maßnahmen getroffen werden. Dazu stehen mehrere Möglichkeiten zur Verfügung. Einerseits kann die Größenordnung von $|\mathcal{T}$ verändern werden, wodurch sich auch der Parameter ϵ ändert und ein längeren Tag entsteht. Andereseits kann der Parameter r verändert werden, indem eine höhere Geheimhaltung (Privacy Amplification) genutzt wird. Das Ziel besteht darin die Wahrscheinlichkeit, die in Formel 25 beschrieben ist, zu verkleinern um zum Beispiel die "'Time-To-Life"'-Zeit des Systems so anzupassen, dass sie ihren Wünschen weiterhin genügt. Wenn dies gemacht wird, werden für die Authentifizierung mehr Schlüsselbits benötigt und/oder es müssen mehr Schlüsselbits während der "'Privaty Amplification"' benutzt werden.
Daraus ist ersichtlich, dass die Rate mit der die echten Schlüsselbits erzeugt werden sinkt. Dies ist aber in den heutigen Systemen nicht tragbar. Um diesen Effekt zu minimieren, muss eine sehr eindringliche Analyse des gesamten Systems bzw. des verwendeten Protokolls durchgeführt werden.
Der einfachere und effizientere Weg eine generellen Korrektur für diese Art von Lücke zu bekommen liegt darin, die zweite Information, also den Tag von Alice, mit einer Verzögerung Eve zukommen zu lassen. Dann kann Eve nicht mehr sicherstellen ob sie das System nun wirklich brechen kann oder nicht und muss es einfach irgendwann versuchen. Der sinnvollste Weg liegt darin, Eve zu zwingen ihre oder Alice Nachricht an Bob weiterzuleiten bevor sie den Tag von Alice abfangen kann. Eine mögliche Lösung kann durch die Verwendung eines synchronen Taktes realisiert werden. Die Nachrichten werden zu vorbestimmten Zeiten gesendet. Zwischen den Nachrichten wird eine Pause-Zeit eingehalten die länger ist als die Genauigkeit des Taktes. In aktuellen QKG Systemen spielen diese synchronisierten Takte auch in anderen sicherheitsrelevanten Gebieten Verwendung. Probleme die dabei entstehen können, werden in 11 beschrieben. Eine weitere Lösung für dieses Problem, dass laut den Autoren auch eine bessere Lösung ist, benötigt zur Erhöhung der Sicherheit keine Takte sondern basiert auf der Verwendung einer zusätzlichen Zufallszahl. Dies soll in folgenden Zeilen näher betrachtet werden.

1. Alice sendet ihre Nachricht m_A, daraufhin empfängt Bob eine Nachricht m

2. Bob wählt nun eine Zufallsvariable s_B" die sich in einer Menge befindet, die mindestens die Größe der Teilmenge von Hashfunktionen $0 \leq s_B < |\mathcal{T}|$ entspricht. Alice empfängt daraufhin eine Zufallsvariable s

3. Alice berechnet nun aus ihrer Nachricht und der empfangenen Zufallszahl $m_A + s$ ihren Tag $t_A = h_k(m_A + s)$. Bob empfängt daraufhin den Tag t und überprüft die Echtheit

indem er diesen Tag t mit $h_k(m + s_B)$ vergleicht.

Die Länge dieser Zufallsvariable sollte genau so lang sein wie die des Tags, damit beide genau gleich schwer zu erraten sind. Dies hat natürlich zur Folge, dass die gesamte Nachrichtenlänge wächst. Dies ist aber nahezu vernachlässigbar, da die original Nachricht viel länger ist als der Tag und der Schlüssel logarithmisch zur Nachrichtenlänge wächst. Wenn sich Eve in dieser Situation befindet, muss sie auch ohne zu wissen ob ihr Angriff erfolgreich sein wird, diesen einfach durchführen. Entscheidet sich sich dafür, dann kann sie dies auf zwei verschiedene Arten tun.

1. Sie sendet ihre Nachricht m_E direkt an Bob und die Zufallszahl s_B oder aber eine gefälschte s_E an Alice.
2. Sie zögert das Senden ihrer Nachricht an Bob hinaus und sendet eine gefälschte Zufallszahl s_E an Alice. Dies erlaubt ihr die Nachricht anzupassen bevor sie diese an Bob sendet.

Es sei angemerkt, dass Eve in beiden Fällen die Nachricht und/oder die Zufallsvariable aktiv auf dem klassischen Übertragungskanal verändern muss, bevor sie den Tag von Alice bekommt. Dieser Tag gibt Eve die zusätzliche Information ob ihr Angriff erfolgreich sein wird oder nicht. In dieser Situation beschreibt die Formel 10 die geeignete Grenze. Durch diesen Aspekt wurde die Sicherheit wiederhergestellt. Dieses Verfahren beschreibt somit einen generell gültigen Ansatz um die Sicherheit merklich zu erhöhen ohne aufwändige Analysen des kompletten Quantenkryptographie-Systems durchzuführen.

8 Zusammenfassung

An dieser Stelle sollen nochmals die erzielten Erkenntnisse zusammengefasst werden. Auch wenn die Wegman-Carter Authentifizierung sicher scheint, falls Eve nur Teilwissen über den Schlüssel erhalten konnte (siehe [MOML$^+$05]), muss man noch eine weitere Eigenschaft des QKG berücksichtigen. Eve kann nämlich aktiv Nachrichten die gesendet werden sollen verändern. Das Teilwissen über den Schlüssel und die Möglichkeit Nachrichten zu verändern, erhöhen Eves Wahrscheinlichkeit das System zu brechen. Die Lösung ist recht einfach, man zwingt Eve ihren Angriffsversuch durchzuführen bevor sie sicher sein kann das er erfolgreich sein wird. Dies wird erreicht indem Alice solange wartet um ihren Authentifizierungs-Tag zu senden, bis entweder Bob die Nachricht empfangen hat, oder Eve versucht hat das System zu brechen. Ein praktisches QKG-System macht es Eve sehr schwierig diese behandelte theoretischen Ansätze in der Praxis durchzuführen, da

1. Eves Freiheiten die Nachrichten beliebig zu verändern sehr stark beschränkt sind und
2. eine QKG-Runde normalerweise durch mehrere Dialoge zwischen den jeweiligen Parteien und einen anschließenden Senden des Authentifizierungs-Tags aufgebaut ist.

Diese Eigenschaften des QKG-Systems reichen aus damit es, je nach Systemkonfiguration, als sicher gelten kann. Der Lösungsvorschlag dieses Artikels sollte dennoch in Zukunft angewandt werden, da er mit sehr geringen Kosten realisiert werden kann und für jedes QKG-System die Sicherheit erhöht. Gerade bei Systemen die einen sehr rauschanfälligen Quantenkanal besitzen sollte dieses Verfahren angewandt werden.
Zum Schluss möchte ich noch meinen persönlichen Eindruck über diesen Artikel abgeben. Die Autoren gingen bei ihrer Betrachtung davon aus, dass der Quantenkanal sehr störanfällig implementiert ist. Deswegen kann Eve recht viele Informationen über den Schlüssel erlangen ohne entdeckt zu werden. Dies stellt jedoch keine vollkommen gerechtfertigte Annahme dar, da heutige Quantenkanäle von vornherein besser implementiert werden. Jedoch stellt diese Betrachtungsweise ein "'Worst-Case"'-Szenario dar und ist daher für fast alle Quantenkryptographiesysteme gültig. Daher vertrete ich die Meinung der Autoren, in allen zukünftigen Systemen die hier vorgestellten Lösungsansätze, zur Schließung der Sicherheitslücke, umzusetzen.

References

[BB84] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *Proc. IEEE Int. Conf. Comput. Syst. Signal Process.*, pages 175–179, Bangalore, India, 1984.

[BBB+92] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin. Experimental quantum cryptography. *J. Cryptol*, vol. 5:3–28, 1992.

[BBCM95] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer. Generalized privacy amplification. *IEEE Trans. Inf. Theory*, vol. 41:1915–1923, 1995.

[BBR86] C. H. Bennett, G. Brassard, and J.-M. Robert. *How to reduce your enemy's information*, volume vol. 218. Springer-Verlag, Berlin, advances in cryptology-proceedings of crypto'85, ser. lecture notes in computer science edition, 1986.

[BBR88] C. H. Bennett, G. Brassard, and J.-M. Robert. Privacy amplification by public discussion. *SIAM J. Comput.*, vol. 17:210–229, 1988.

[Bel64] J. S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, vol. 1:195–200, 1964.

[BS94] G. Brassard and L. Salvail. *Secret key reconciliation by public discussion*, volume vol. 765. Springer-Verlag, Berlin, advances in cryptology: eurocrypt'93, ser. lecture notes in computer science edition, 1994.

[Cla74] J. F. Clauser. Experimental distinction between the quantum and classical field-theoretic predictions for the photoelectric effect. *Phys. Rev. D, Part. Fields*, vol. 9:853–860, 1974.

[Eke91] A. K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, vol. 67:661–663, 1991.

[GBS00] T. Mor G. Brassard, N. Lütkenhaus and B. C. Sanders. Limitations on practical quantum cryptography. *Phys. Rev. Lett.*, vol. 85:1330–1333, 2000.

[GRTZ02] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. Quantum cryptography. *Rev. Mod. Phys.*, vol. 74:145–195, 2002.

[Lüt99] N. Lütkenhaus. Estimates for practical quantum cryptography. *Phys. Rev. A, Gen. Phys.*, vol. 59:3301–3319, 1999.

[May96] D. Mayers. *Quantum key distribution and string oblivious transfer in noisy channels*. Springer-Verlag, Berlin, in advances in cryptology-proceedings of crypto'96, ser. lecture notes in computer science edition, 1996.

[MOML+05] M.Ben-Or, M.Horodecki, D.W. Leung, D.Mayers, and J.Oppenheim. *The universal composable security of quantum key distribution*, volume vol. 3378. Springer-Verlag, 2005.

[MY98] D. Mayers and A. Yao. Quantum cryptography with imperfect apparatus. *in Proc. 39th Annu. Symp. Found. Comput. Sci.*, pages 503–509, 1998. Los Alamitos.

[NPW+00] D. S. Naik, C. G. Peterson, A. G. White, A. J. Berglund, and P. G. Kwiat. Entangled state quantum cryptography: Eavesdropping on the Ekert protocol. *Phys. Rev. Lett.*, vol. 84:4733–4736, 2000.

[RSA78] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, vol. 21:120–126, 1978.

[Sch93] B. Schneier. *Applied Cryptography*. New York: Wiley, 1993.

[SP00] P. W. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.*, vol. 85:441–444, 2000.

[Sti91] D. R. Stinson. *Universal hashing and authentication codes*, volume vol. 576. Springer-Verlag, Berlin, advances in cryptology-proceedings of crypto'91, ser. lecture notes in computer science edition, 1991.

[WC79] M. N. Wegman and J. L. Carter. Universal classes of hash functions. *J. Comput. Syst. Sci.*, vol. 18:143–154, 1979.

[WC81] M. N. Wegman and J. L. Carter. New hash functions and their use in authentication and set equality. *J. Comput. Syst. Sci.*, vol. 22:265–279, 1981.

[WZ82] W. K. Wooters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, vol. 299:802–803, 1982.