Theoretisches Seminar -Quantum Computing
Quantenkryptographie

Jim Kallarackal (255 409)
Jim.Kallarackal@rwth-aachen.de

16. Juni 2005

Zusammenfassung

Die Motivation Nachrichten zu verschlüsseln ist wohl ebenso alt, wie die menschliche Gesellschaft selbst. Die Anstrengungen verschlüsselte Nachrichten zu entschlüsseln waren dann zwingend: „Man nimmt die unerklärte dunkle Sache wichtiger als die erklärte helle."(Nietzsche, Menschliches Allzumenschliches, S.277, Z. 532)

Kryptographische Verfahren werden seit Jahrhunderten benutzt und entwickelt. Diese Arbeit beginnt zunächst mit einer Einführung in Klassische Kryptographieverfahren und wird im zweiten Teil auf die Bedeutung der Quantentheorie eingehen, welche die Schwächen der klassischen Kryptographieverfahren eliminieren kann.

1 Klassische Kryptographie

Kryptologie ist die Wissenschaft vom Entwurf, der Anwendung und der Analyse von kryptographischen Systemen. Die Kryptographie beschäftigt sich mit der Verschlüsselung und entschlüsselung von Nachrichten, während man unter Kryptoanalyse die Analyse der Sicherheit von Verschlüsselungsverfahren versteht.

Das Verschlüsseln ist der Vorgang, in dem ein Klartext durch ein Verschlüsselungsverfahren in eine unlesbare Zeichenfolge umgewandelt wird. Der Algorithmus verwendet dabei einen oder mehrere Paramter (Schlüssel), mit diesen ist es möglich den Verschlüsselungsvorgang rückgängig zu machen.

In der klassischen kryptographie unterscheidet man grob zwei Systeme

- Symmetrische Kryptogrpahieverfahren

- Asymmetrische Kryptographieverfahren

In der Kryptographie ist es üblich folgende Namen einzuführen (siehe Abbildung 1)

Alice: Sender der Nachricht

Bob: Empfänger der Nachricht

Eve: Potenzieller Feind, der die Nachricht abhören versucht

Eine sichere Kommunikation soll zwischen Alice und Bob stattfinden. Der Name Eve ist der englischen Sprache angelehnt (eavesdropper = Lauscher).

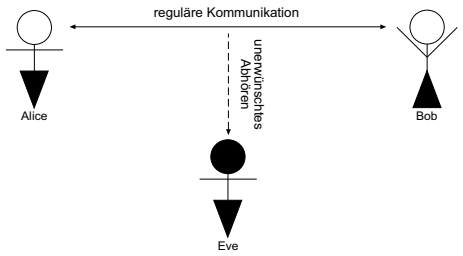


Abbildung 1: Protagonisten der Kommunikation

1.1 Symmetrische Kryptographieverfahren

Symmetrische Kryptographieverfahren sind wesentlich älter und benötigen nur einen Schlüssel zum verschlüsseln und entschlüsseln der Nachricht. Dieser Schlüssel muss also geheim sein. Ein sehr bekanntes und einfaches symmetrsiches Verfahren ist die Cäsar-Verschlüsselung, wobei das Alphabet um k Stellen nach rechts verschoben wird. So wird aus

$$\text{THEORIE} \xrightarrow{+3} \text{WKHRULH}$$

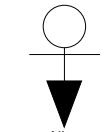
In diesem Fall ist der geheime Schlüssel $k = +3$, ist dieser bekannt, so kann die Verschlüsselung einfach rückgängig gemacht werden.

Die Cäsar-Verschlüsselung wurde etwa 50 vor Christus angewandt und ist leicht zu entschlüsseln. Aus statistischen Analysen weiss man, dass der Buchstabe ‚e' der häufigste in der deutschen Sprache ist. Also ist es naheliegend den häufigsten Buchstaben in der verschlüsselten Nachricht (hier ‚H') mit ‚E' zu identifizieren. In der Tat erhält man so den Schlüssel $k = +3$.

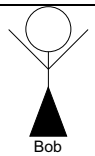
Die Cäsar-Verschlüsselung wird in diesem Zusammenhang oft erwähnt, weil sie auf sehr einfache Weise das Prinzip symmetrischer Verfahren verdeutlicht und zudem offenbart, dass solche einfachen Schlüssel aus Sicht der Kryptoanalyse nicht sicher sind. Ein sicheres Verfahren ist das von Gilbert Vernam (AT&T 1926) vorgeschlagene „One-time pad". Dieses Verfahren erfolgt in drei Schritten

1. Alice und Bob einigen sich auf einen geheimen Schlüssel k, der im Idealfall dieselbe Länge hat wie die zu übertragende Nachricht
2. Alice kodiert ihre Nachricht mit dem Schlüssel k durch eine XOR- Verknüpfung
3. Bob empfängt die Nachricht und kann sie mit dem Schlüssel k und einer weiteren XOR-Verknüpfung entschlüsseln

Das Folgende Beispiel verdeutlicht den Vorgang



Schlüssel	k = 6	0110
Nachricht	x = 5	0101
kodiert	c = x XOR k	0011
c = 3		



Schlüssel	k = 6	0110
Verschlüsselt	c = 3	0011
dekodiert	x = c XOR k	0101
x = 5		

Hat der Schlüssel k dieselbe Länge, wie die Nachricht x, so kann man die Sicherheit dieses Verfahrens beweisen.

Symmetrische Verfahren sind nur dann sicher, wenn es gelingt einen geheimen Schlüssel zu vereinbaren. Zudem kann dieser Schlüssel nur einmal benutzt werden, da zwei Nachrichten, die mit demselben Schlüssel kodiert wurden, durch statistische Analysen (z.B. durch bestimmte Eigenarten der Sprache) Rückschlüsse auf den Inhalt oder den Schlüssel erlauben. Aus diesem Grund heisst das oben genannte Verfarhren auch „One-time pad“.

1.2 Asymmetrische Kryptographieverfaren

Asymmetrische Verfahren wurden erst 1976 von Whitfield Diffie und Martin Hellman in Stanford vorgeschlagen. Der britische Geheimdienst behauptet, dass solche Verfahren bereits 1973 bekannt waren, jedoch aufgrund der großen Bedeutung nicht veröffentlicht wurden.

Asymmetrische Verfahren benötigen einen geheimen Schlüssel zum entschlüsseln und einen öffentlichen zum verschlüsseln der Nachrichten. Aus diesem Grund heissen diese Systeme auch „public-key cryptosystems“. Nur der Empfänger besitzt den geheimen Schlüssel, so dass nur er die verschlüsselten Nachrichten entschlüsseln kann.

Grundlegend für die Funktionweise eines solchen Systems, sind sog. „One- way“-Funktionen (Einwegfunktionen) $f(x)$, bei denen es leicht ist den Funktionswert $f(x) = y$ zu berechnen, aber die Bestimmung des Argumentes zu einem gegeben Funktionswert y sehr schwierig ist (mehrere Jahrzehnte andauert!).

Der bekannteste „public-key“-Algorithmus ist der von Ronald Rivest, Adi Shamir, Leonard Adleman (MIT 1978) entwickelte und nach ihnen benannte Algorithmus RSA.

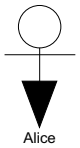
1. Einweg-Funktion: $f(q,p) = q \cdot p =: n, \quad q,p$ sind Primzahlen
   $f(13,19) = 247$

2. $A(p,q) = (p-1) \cdot (q-1)$
   $A(13,19) = 216$

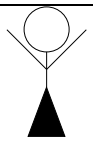
3. Wähle ein $e < n$ mit $\mathrm{ggT}(e,A) = 1, \quad \Rightarrow e$ ist ungerade
   $e = 5$

4. bestimme d derart, dass $e \cdot d = 1 \bmod A$ und $d < A$ (d.h. d ist das inverse Element zu e in der Modulo-Gruppe: $d = e^{-1}$)
   $d = 173$, denn $5 \cdot 173 = 865 = 4 \cdot A + 1 = 1 \bmod A$

5. Der öffentliche Schlüssel ist $(e, n) = (5, 247)$, der geheime Schlüssel ist $(d, n) = (173, 247)$



Nachricht	x = 12
Schlüssel	$(e, n) = (5, 247)$
kodiert	$c = x^e \bmod n$
$c = 12^5 \bmod 247$	$= 103$



Verschlüsselt	c = 103
Schlüssel	$(d, n) = (173, 247)$
dekodiert	$x = c^d \bmod n$
$x = 103^{173} \bmod 247$	$= 12$

Beachte, dass die verschlüsselte Nachricht $c = x^e$ ist, so dass man aus c die Nachricht x bekommt, indem man $x = c^{\frac{1}{e}}$ bestimmt. $d = e^{-1}$ ist jedoch nur dem Empfänger bekannt. d lässt sich aus n durch Faktorisieren bestimmen!

Der RSA Algorithmus nutzt die Komplexität des Faktorisierens natürlicher Zahlen. Obwohl bislang noch nicht bewiesen wurde, dass das Faktorisieren nicht effizient gelöst werden kann, gilt dies im Rahmen klassischer Rechenmethoden als wahrscheinlich! Ein Algorithmus gilt als 'effizient', wenn die Rechenzeit im schlimsten Fall polynomiell beschränkt ist. Bislang sind nur solche Algorithmen für das Faktorisieren natürlicher Zahlen bekannt, dessen Rechenzeit exponentiell beschränkt sind. Abbildung 2 veranschaulicht die Bedeutung des Faktorisierens in der Kryptographie

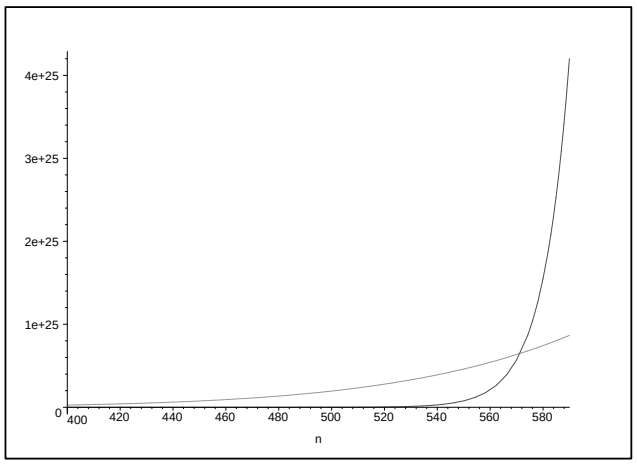


Abbildung 2: $f(n) = \exp(0.1 \cdot n), \qquad g(n) = n^9$

Qualitative Überlegungen zeigen, dass das Universum etwa aus 10^{78} Atomen besteht, die obige Exponentialfunktion ergibt für $n = 2048$

$$f(2048) = 8.8 \cdot 10^{88}$$

Eine Schlüssellänge von $n = 2048$ ist problemlos handhabbar. Analytisch exakte Verfahren, die heute Bekannt sind, benötigen zur Bestimmung von Primfaktoren exponentielle Rechenzeit, so dass RSA als sicher gilt.

Da symmetrische Verfahren schneller Ver- und Entschlüsseln, werden asymmetrische Verfahren benutzt, um den Geheimen Schlüssel zu übertragen. Die weitere Kommunikation erfolgt dann über symmetrische Kryptographieverfahren.

1.3 Komplexitätsklassen

In der theoretischen Informatik teilt man Probleme in Komplexitätsklassen ein. Diese basieren auf die ursprüngliche Definition von Rechenmaschienen, die von Turing 1993 eingeführt wurden.

Die Klasse P Probleme, für die es eine deterministische Turingmaschiene gibt, dessen Rechenzeit im schlimmsten Fall polynomiell beschränkt ist.

Die Klasse NP Probleme, für die es eine nicht-deterministische Turingmaschiene gibt, dessen Rechenzeit im Schlimsten Fall polynomiell beschränkt ist.

NP vollständig Dies sind Probleme aus NP, die bzgl. polynomieller Reduzierbarkeit größer sind als alle anderen Probleme aus NP

Beim Übergang zu Registermaschienen (PC) ändern sich die Klassen nicht, d.h. ein Problem, welches für eine Turingmaschiene in der Klasse P, NP oder NP-vollst. liegt, ist auch beim Übergang zu einem heutigen PC in derselben Klasse. Nichtdeterministische Turingmaschienen entsprechen klassichen Computern mit endlich vielen Prozessoren.

Die polynomielle Reduzierbarkeit definiert eine Ordnung auf der Menge aller Probleme. Ich möchte mich an dieser Stelle darauf beschränken eine intuitive Definition anzugeben. Genaueres findet man in [2] oder [3]

Def. 1 (polynomielle Reduzierbarkeit) *Es gilt $L_1 \leq L_2$ falls es ein Polynom $p(n)$ gibt, so dass L_1 in Rechenzeit $p(n) + t(n)$ lösbar ist, wobei $t(n)$ die Rechenzeit von L_2 ist.*

Dies bedeutet, dass L_1 in P ist, falls L_2 in P ist. Aber $L_1 \leq L_2$ bedeutet nicht, dass L_1 in kürzerer Rechenzeit entscheidbar ist als L_2.

Es war von großer Bedeutung als Cook (1971) bewies, dass das Erfüllbarkeitsproblem SAT NP-vollständig ist (siehe [2]).

Def. 2 (SAT) *Für natürliche Zahlen n und m seien m Klauseln über n Variablen gegeben. Eine Klausel ist die Disjunktion von einigen Literalen x_i bzw. $\bar{x_j}$ mit $i, j \in \{1, \ldots, n\}$. Es soll entschieden werden, ob es eine Belegung $a = (a_1, \ldots, a_n) \in \{0, 1\}^n$ der Variablen $x_1, \ldots, x_n$ gibt, so dass alle Klauseln erfüllt sind, d.h. den boolschen Wert 1 ergeben.*

Schon der Spzialfall, in dem Klauseln genau drei Literale enthalten, genannt 3- SAT, ist NP-vollständig.

Für das Faktorisieren natürlicher Zahlen gelang es nicht zu zeigen, dass es NP-vollständig ist! Der RSA-Algorithmus wird heute in vielen kritischen Bereichen (Zahlungsverkehr, Online-Banking) verwendet, so dass eine theoretische Grundlage für die Sicherheit dieser Systeme wünschenswert ist.

2 Quantenkryptographie

Wie bereits im ersten Teil erwähnt werden asymmetrische (klassische) Kryptographieverfahren verwendet um einen geheimen Schlüssel für symmetrische Verfahren zu vereinbaren, so dass die Sicherheit symmetrischer Verfahren auf die der asymmetrischen Verfahren reduziert wird. Die Quantentheorie ermöglicht den sicheren Austausch eines Schlüssels, falls es gelingt einzelne Quanten zu separieren und zu übertragen.

Das erste Protokoll zur Quantenkryptographie wurde 1984 von Charles H. Bennet (IBM, New York) und Gilles Brassard (University of Montreal) in einer Konferenz in Indien vorgeschlagen. Das Protokoll trägt daher den Namen BB84. Als Träger der Information dienen Quantenzustände, diese können beliebe zwei-Zustands-Quantensysteme sein. Im Folgenden werden Photonen und ihre Polarisationszustände betrachtet.

Bekanntlich erzeugen die Eigenvektoren eines hermiteschen, linearen Operators den zugrundeliegenden Hilbertraum. Zwei nicht-kommutierende Operatoren liefern demnach zwei unterschiedliche Erzeugendensysteme desselben Hilbertraumes. Für die Polarisationszustände von Photonen können ebenfalls verschiedene Basen angegeben werden. Das BB84-Protokoll operiert auf vier Quantenzustände, dabei kennzeichnen die Zustände $|V\rangle$ und $|H\rangle$ vertikal bzw. horizontal polarisierte Photonen, die in einer rechtwinkligen Basis präpariert werden, während die Zustände $|R\rangle$ und $|L\rangle$ in einer dazu gedrehten Basis präpariert werden. Es gilt

$$|R\rangle = \frac{1}{\sqrt{2}} \left(|V\rangle + |H\rangle\right)$$

$$|L\rangle = \frac{1}{\sqrt{2}} \left(|V\rangle - |H\rangle\right)$$

Die Zustände $|V\rangle$ und $|R\rangle$ werden mit dem Bitwert 1 identifiziert, während die Zustände $|H\rangle$ und $|L\rangle$ den Bitwert 0 kennzeichnen.

Das BB84-Protokoll besteht im wesentlichen aus vier Schritten

1. Alice wählt zufällig eine der zwei Basen und präpariert den Wert 1 oder 0
2. Bob empfängt das Teilchen und ermittelt den Eigenwert, wobei er wegen seiner Unkenntnis über die Basis eine beliebige wählt
3. Sind hinreichend viele Teilchen auf diese Weise übertragen, so offenbart Bob seine jeweilige Wahl der Basen
4. Alice teilt mit, welche Teilchen mit Bob's Wahl der Basis korrespondieren. Dabei kommunizieren Alice und Bob über einen authentischen[1] aber nicht notwendig abhörsicheren Kanal.

[1] Ein authentischer Kanal gewährleistet, dass die Nachricht unverfälscht übertragen wird, d.h. die Nachricht kann nicht modifiziert werden

Beachte, dass im Schritt vier die Eigenwerte nicht übermittelt werden! Der Schlüssel am Ende des dritten Schrittes heisst 'raw key', der bereinigte Schlüssel am Ende von Schritt vier heisst 'sifted key'.

Die untenstehende Tabelle verdeutlicht den Vorgang:

Alice										
Basis	$\oplus$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\otimes$	$\otimes$	$\oplus$	$\oplus$
Zusatnd	$\|H\rangle$	$\|R\rangle$	$\|V\rangle$	$\|H\rangle$	$\|L\rangle$	$\|L\rangle$	$\|R\rangle$	$\|H\rangle$	$\|H\rangle$	$\|V\rangle$
Bitwert	0	1	1	0	0	0	1	0	0	1
Bob										
Basis	$\otimes$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$
Zusatnd	$\|R\rangle$	$\|R\rangle$	$\|R\rangle$	$\|H\rangle$	$\|H\rangle$	$\|L\rangle$	$\|V\rangle$	$\|L\rangle$	$\|L\rangle$	$\|V\rangle$
Bitwert	1	1	1	0	1	0	1	0	0	1
Schlüssel										
Bitwert		1		0		0		0		1

Im Durchschnitt entspricht die Länge des bereinigten Schlüssels der Hälfte der Sequenz von Alice bzw. Bob (bei idealen Bedingungen).

Wie auch bei klassischen Verfahren muss man nun die Auswirkungen des Abhörens beatrachten, allerdings unterliegt das Abhören einigen quantentheoretischen Grenzen:

Unschärfe Eigenwerte (also die physikalischen Messwerte) zu zwei nicht-kommutierenden Operatoren können nicht beliebig genau bestimmt werden. Die Unschärfe ist eine direkte Konsequenz der quantenmechanischen Postulate.

No-Cloning Ein Quantenzustand kann nicht kopiert werden. Gäbe es einen Operator, der einen Zustand kopiert, so darf er nicht den Ausgangszustand verändern. Also muss er unitär und insbesondere linear sein. Angenommen es gäbe einen solchen unitären Operator U, dann gilt:

$$|\psi, \psi\rangle = \widehat{U}|\psi, \varphi\rangle$$

Auf der rechten Seite bezeichnet ψ das zu kopierende Teilchen, während φ ein zweites Teilchen kennzeichnet, welches initial in einem beliebigen Zustand sei. Nach der Anwendung des Operators $\widehat{U}$ soll das zu kopierende Teilchen unverändert sein, während das zweite Teilchen nun im selben Zustand sei wie das erste.

Für quantenmechanische Zustände gilt (axiomatisch) das Superpositionsprinzip, so dass der Zustand $|\psi\rangle$ in einer Basis entwickelt werden kann. Die Basisvektoren seien $|V\rangle$ und $|H\rangle$ mit $|\psi\rangle = a \cdot |V\rangle + b \cdot |H\rangle$ folgt

$$|\psi, \psi\rangle = a^2 \cdot |V, V\rangle + b^2 \cdot |H, H\rangle + ab \cdot (|V, H\rangle + |H, V\rangle)$$

während

$$\begin{aligned} \widehat{U} \cdot |\psi, \varphi\rangle &= \widehat{U} \cdot (a \cdot |V\rangle + b \cdot |H\rangle) * |\varphi\rangle \\ &= a \cdot |V, V\rangle + b \cdot |H, H\rangle \end{aligned}$$

Insgesamt also

$$a^2 \cdot |V, V\rangle + b^2 \cdot |H, H\rangle + ab \cdot (|V, H\rangle + |H, V\rangle) \stackrel{!}{=} a \cdot |V, V\rangle + b \cdot |H, H\rangle$$

$$\Rightarrow ab = 0, \qquad a, b \in \{0, 1\}$$

Einen unitären ‚Kopieroperator'kann in der Quantenmechanik also nur dann geben, wenn die Entwicklungskoeffizienten ausschließlich die Werte $\{0, 1\}$ annehmen und das Produkt $a \cdot b$ verschwindet. Dies ist der klassische Grenzfall!

Einen ‚Kopieroperator'kann es also in der Quantentheorie nicht geben (Diese Aussage gilt auch für kontinuierliche Basen, davon überzeuge man sich in den Grundlagen der Quantenmechanik).

2.1 Strategien des Abhörens

Da es nicht möglich ist, einen Quantenzustand zu kopieren, besteht die einzige Möglichkeit für Eve an der Kommunikation teilzuhaben darin, die Photonen in einer beliebigen Basis zu Messen und anschließend ein neues Photon mit dem gemessenen Eigenwert zu präparieren und an Bob weiterzugeben. Dabei gilt

$$\|\langle V||R\rangle\|^2 = \|\langle V| \cdot \frac{(|v\rangle + |H\rangle)}{\sqrt{2}} = \|^2 = \frac{1}{2}$$

Entsprechendes gilt dann auch für $\langle L| \, |H\rangle$ usw.

Das Abhören von Quanteninformation führt zwingend zu Fehlern in der Übertragung, die von Alice und Bob durch weitere Verfahren festgestellt werden können. Die untenstehende Tabelle verdeutlicht diesen Sachverhalt anhand eines Beispiels

Alice										
Basis	$\oplus$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\otimes$	$\otimes$	$\oplus$	$\oplus$
Zusatnd	$\|H\rangle$	$\|R\rangle$	$\|V\rangle$	$\|H\rangle$	$\|L\rangle$	$\|L\rangle$	$\|R\rangle$	$\|H\rangle$	$\|H\rangle$	$\|V\rangle$
Bitwert	0	1	1	0	0	0	1	0	0	1
Eve										
Basis	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\otimes$	$\oplus$	$\oplus$	$\otimes$
Zusatnd	$\|H\rangle$	$\|R\rangle$	$\|V\rangle$	$\|R\rangle$	$\|L\rangle$	$\|H\rangle$	$\|R\rangle$	$\|V\rangle$	$\|H\rangle$	$\|L\rangle$
Bitwert	0	1	1	1	0	1	1	1	1	0
Bob										
Basis	$\otimes$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$
Zusatnd	$\|R\rangle$	$\|R\rangle$	$\|L\rangle$	$\|H\rangle$	$\|H\rangle$	$\|L\rangle$	$\|V\rangle$	$\|L\rangle$	$\|L\rangle$	$\|V\rangle$
Bitwert	1	1	0	1	1	0	1	1	0	1
Schlüssel										
Alice		1		**0**		0		**0**		1
Bob		1		**1**		0		**1**		1

Im Durchschnitt wird Eve in der Hälfte aller Messungen die richtige Basis wählen (also in Übereinstimmung mit Alice) und so den korrekten Zustand reproduzieren. In der anderen Hälfte aller Photonen, die Eve in der falschen Basis präpariert, wird der ideale quantenmechanische Zufallscharakter dazu führen, dass Bob den richtigen Eigenwert erhält. Insgesamt führt das konsequente Abhören zu einer Fehlerrate von 25% in dem bereinigten Schlüssel von Alice und Bob. Die nächsten Abschnitte behandeln Prozeduren, die es Alice und Bob erlauben, die Fehlerrate ihres Schlüssels festzustellen und den Informationsgehalt von Eve auf ein Minimum zu reduzieren.

2.2 Fehlerrate und Fehlerkorrektur

Fehlerrate Alice und Bob vergleichen eine Teilmenge ihres bereinigten Schlüssels und vergleichen die entsprechenden Bitwerte. Aus den Fehlerhaften Bits in dieser Teilmenge schließen sie auf die Fehlerrate des bereinigten Schlüssels.

Fehlerkorrektur Alice wählt beliebige zwei Bits des Schlüssels und teilt Bob das Resultat der XOR Verknüpfung sowie die Indices der Zustände mit. Erhält Bob denselben Wert, so behalten sie jeweils das erste Bit, ansonsten ignorieren sie beide Bits. Durch diese Prozedur kann die Fehlerrate des Schlüssels auf Kosten der Schlüssellänge minimiert werdeen

Erhöhung der Sicherheit Alice wählt beliebige zwei Bits und teilt Bob ihre Wahl der Indices mit. Beide ersetzen die Bits mit dem Resultat der XOR Verknüpfung. Wenn Eve vollständige Information über eines dieser Bits hat und keine Information über das Zweite, so hat sie am Ende dieser Prozedur keine Information über das XOR-Resultat. Selbst wenn Eve partielle Information über beide Bits, so hat sie am Ende dieser Prozedur aufgrund der gauß'schen Fehlerfortpflanzung weniger Information über das XOR-Resultat.

Diese Prozedur minimiert Eve's Wissen über den bereinigten Schlüssel und heisst deshalb ‚Privacy amplification'.

Die obige Überlegung legt einen Grenzwert für die Güte der Übertragung fest

- Es sei p die Wahrscheinlichkeit dafür, dass aufgrund technischer Imperfektionen z.B. aus $|V\rangle$ der Zustand $|H\rangle$ wird.
- Das obige Verfahren zur Fehlerkorrektur basiert darauf, dass nicht zwei Bits gleichzeitig falsch sind. Ferner weiss man, dass das konsequente Abhören der ‚Quantenleitung' zu einem Fehler von max. 25% in dem bereinigten Schlüssel führt. Dieser Umstand muss klar von technischen Imperfektionen zu unterscheiden sein!

  Die Fehlerkorrektur ist nur dann sinvoll, wenn die Wahrscheinlichkeit dafür, dass zwei beliebige Zustände gleichzeit falsch sind geringer als 25% ist: $\Rightarrow p^2 = \frac{1}{4} \Rightarrow p = \frac{1}{2}$. Um also das Abhören von technischen Unvollkommenheiten zu unterscheiden, müssen mindestens 50% aller Photonen fehlerfrei übertragen werden.

2.3 Alternative Protokolle

Es gibt verschieden Variantionen des BB84-Protokolls, zwei Protokolle, die sich fundamental unterscheiden sind

2.3.1 2-State protokoll

Das Prinzip der Quantenkryptographie bedarf lediglich zwei Zustände (anstatt vier wie in BB84). Diese zwei Zustände dürfen allerdings nicht orthogonal sein (beispielsweise könnte man die Zustände $|R\rangle$ und $|H\rangle$ nutzen), dies wurde von Charles H. Bennet 1992 betont.

Obwohl dies die praktische Realisierung nicht erleichtert, mach es deutlich, dass das BB84-Protokoll lediglich auf die fundamentale quantenmechanische Eigenschaft beruht, dass Eigenwerte zu nicht-kommutierenden Operatoren nicht gleichzeit beliebig genau bestimmt werden können.

2.3.2 EPR-Protokoll

Das EPR-Protokoll ist technisch schwieriger zu realisieren als BB84, beinhaltet jedoch wesentliche theoretische Aspekte, welche die Sicherheit des bereinigten Schlüssels auf einen Test der Bellschen Ungleichungen zurückführt.

Im Gegensatz zum BB84-Protokoll braucht man nun zwei-teilchen Zustände. Dies werde dadurch realisiert, dass eine Quelle, die sich zwischen Alice und Bob befindet, Paare von verschränkten Zuständen der Form

$$|\psi\rangle = \frac{1}{\sqrt{2}} \cdot (|V, H\rangle + |H, V\rangle)$$

produziert, wobei eines der Teilchen zu Alice und das Andere zu Bob propagiert. O.B.d.A. nehmen wir an, dass Alice das erste Teilchen und Bob das zweite Teilchen erhält (siehe Abbildung 3).

Eine Messung (in einer beliebigen Basis) führt nun dazu, dass die Verschränktheit vernichtet wird. Alice und Bob führen nun neben der Basen $\bigoplus$ und $\bigotimes$ eine weitere relativ zu $\bigoplus$ gedrehte Basis ein. Die verschränkten Zustände werden von der Quelle in einer der drei Basen präpariert. Zwar ist nun die Wahrscheinlichkeit, dass Alice und Bob dieselbe Basis zum Messen ihrer Teilchen wählen geringer, allerdings können nun die unkorrellierten Messungen dazu benutzt werden, die Bellsche Ungleichung zu testen. Wird diese nicht verletzt, so deutet dies auf technische Mängel oder auf einen potenziellen Feind hin.

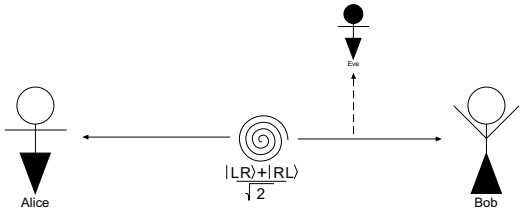


Abbildung 3: EPR-Protokoll

2.4 Technische Realisation

Quantenkryptographie wurde schon sehr kurz nach der Veröffentlichung des BB84-Protokolls realisiert

1989-1992 Brassard (1989), Bennet, Bessette (1992)
Übertragung durch Luft mit polarisierten Photonen: 32cm

1995 Müller, Breguet, Gisin, Zbinden (1993-1996)
Übertragung durch Glasfaser mit polarisierten Photonen: 22,8 km

1999 Forschungsgruppe in Los Alamos, Übertragung durch Glasfaser mit phasenkodierten Photonen: 48km

Die oben angeführten Experimente sind keine vollständige Liste.

Der Umstand, dass Quantenkryptographiesysteme sogar käuflich erwerblich sind, mag überzeugender erscheinen als die obigen experimentellen Daten

http://www.idquantique.com

http://www.magiqtech.com

Literatur

[1] Quantum cryptography, Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, Hugo Zbinden, University of Geneva/Switzerland, Reviews of Modern Physics, July 8 2004

[2] Theoretische Informatik -eine algorithmenorientierte Einführung, Ingo Weegener, 2.Aufl, Leipzig:Teubner, 1999

[3] Der Turing Omnibus, A.K. Dewdney, Springer 1995

[4] Lecture notes on quantum computation, Section VI: Quantum cryptography and some uses of entanglement, N.David Mermin, Cornell University 2004

[5] Quantenkryptographie, Wolfgang Tittel, Jürgen Brendel, Nicolas Gisin, Grégoire Ribordy, Hugo Zbinden, Physikalische Blätter 55 (1999) Nr. 6, WILEY-VCH Verlag

[6] Description of physical reality, A.Einstein, B.Podolsky, N.Rosen, Institute for advanced study, Princeton, New Jersey, 03.1935

[7] Calssical and quantum information, A.Galindo, M.A. Martin Delgado, section B, Rev. Mod. Phys., Vol 74, No. 2, 04.2002