Grenzen der Kryptographie

2. Eingangs wurde erwähnt, dass in unserer technisierten Welt sichere Datenübertragung auch für Privatpersonen immer wichtiger wird. Das macht den Einsatz von kryptographischen Methoden sinnvoll. Allerdings sind einige einschränkende Bemerkungen am Platz. Die Kryptographie analysiert das Problem der sicheren Datenübertragung auf der Ebene eines mathematischen Modells. In der Praxis gibt es bei der Umsetzung der theoretisch guten Verfahren mindestens zwei Probleme:

1. Eine Nachricht ist vor der Verschlüsselung und nach der Entschlüsselung unsicher und höchstens so geheim wie der Schlüssel.

2. Die Sicherheit hängt von der technischen Umsetzung jeder einzelnen Komponente ab.

So haben wir gesehen, dass die Sicherheit der One-Time Pads von der Geheimhaltung der Schlüssel abhängt, die in der mathematischen Analyse wie selbstverständlich vorausgesetzt wird. Und Situationen wie die folgende ereignen sich täglich an Bankautomaten oder Rechnerkonsolen: Jemand möchte eine Geheimzahl übermitteln, um so Zugriff auf sein Konto zu erhalten. Die Übermittlung über ein ausgeklügeltes Kryptographiesystem nutzt nichts, wenn ihm bei der Eingabe der Zahl jemand auf die Finger sieht oder eine Kamera seine Aktion aufzeichnet. Zudem sind Alice und Bob in der Praxis oft komplexe Institutionen, zum Beispiel Nachrichtendienste oder Firmen, so dass die *interne Geheimhaltung* zum Problem werden kann.

Diese Anmerkung ist wichtig, um den Nutzen eines Kryptographiesystems realistisch einschätzen zu können. Ein falsch eingesetztes Sicherheitssystem erhöht die Gefahr, wichtige Daten preiszugeben. So wird niemand gesunden Verstandes wichtige Bankdaten in irgendein Internetformular eintragen, außer ihm wurde glaubhaft versichert, die Kommunikation verliefe über eine sichere Leitung. Wie glaubhaft diese Sicherheitsversprechen sind, ist nicht immer klar.

7.2 Quantenverschlüsselung: das BB84-Protokoll

Im Jahr 1984 haben Charles Bennett von IBM und Gilles Brassard von der Universität Montreal ein Quantenkryptographieverfahren veröffentlicht, das heute unter dem Namen BB84 bekannt ist. Fünf Jahre später wurde es das erste Mal experimentell umgesetzt, wobei die Quantenbits als polarisierte Photonen (siehe Abschnitt 9.3) realisiert wurden. In diesem Abschnitt stellen wir das BB84-Protokoll auf eine Weise dar, die unabhängig von der Umsetzung ist. Wir nehmen dazu an, dass zwischen Alice und Bob ein perfekter, störungsfreier Quantenkanal existiert. Da Kanäle in der Praxis nie störungsfrei sind, betrachten wir am Ende des Abschnittes die Auswirkung von Rauschen auf das geschilderte Verfahren.

Die Aufgabe lautet, Alice und Bob mit einer Folge von *zufälligen* und geheimen Bits auszustatten. Diese können dann als One-Time Pads zur sicheren klassischen Verschlüsselung genutzt werden.

Wir beginnen mit der Erzeugung eines einzelnen Bits und setzen danach das eigentliche Schlüsselübertragungsprotokoll aus einer Folge solcher Schritte zusammen. Die Biterzeugung beginnt mit einer Aktion von Alice.

A. Alice verschickt ein Quantenbit

Verwendet wird ein Quantenbit $|x\rangle$.

1. Erzeuge ein zufälliges klassisches Bit a;
   Versetze das Quantenbit in den Zustand $|x\rangle \leftarrow |a\rangle$
2. Erzeuge ein zweites klassisches Zufallsbit a':
   Ist $a' = 1$, wende die Hadamard-Transformation an: $|x\rangle \leftarrow H|x\rangle$
3. Schicke $|x\rangle$ an Bob.

Wir bezeichnen im folgenden

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = H|0\rangle \text{ mit } |+\rangle$$

und

$$\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = H|1\rangle \text{ mit } |-\rangle.$$

In welchem Zustand befindet sich das Bit $|x\rangle$ nach Schritt 3? Mit Wahrscheinlichkeit von jeweils $1/4$ in einem der Zustände

$$|0\rangle, |1\rangle, |+\rangle, |-\rangle.$$

Das Quantenbit $|x\rangle$ wurde gemäß folgender Tabelle aus den Zufallsbits erzeugt:

	$a' = 0$	$a' = 1$
$a = 0$	$\|0\rangle$	$\|+\rangle$
$a = 1$	$\|1\rangle$	$\|-\rangle$

Verwendete Basen

Das Zufallsbit a soll an Bob übermittelt werden. Das Zufallsbit a' bestimmt, in welcher Basis a dargestellt wird. Mit B bezeichnen wir ab jetzt die Standardbasis $|0\rangle, |1\rangle$, mit B' die Hadamardbasis $|+\rangle, |-\rangle$. Alice' zweiter Münzwurf entscheidet also, welche Basis für die Übertragung gewählt wird.

Nun hat Bob das Quantenbit $|x\rangle$ erhalten. Wie kann er etwas über das Bit a herausfinden? Er muss es messen. Da er nicht weiß, bezüglich welcher Basis es kodiert wurde, überlässt er diese Entscheidung dem Zufall.

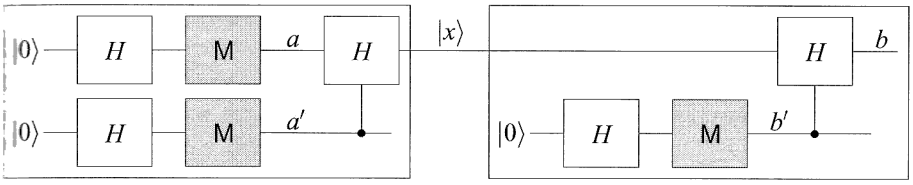

Abbildung 7.2: Schaltkreis für die Schritte A. und B.: Der Quantenkanal zwischen Alice und Bob ist der unsichere Teil.

B. Bob misst Alice' Quantenbit

$|x\rangle$ ist das von Alice in Schritt A erzeugte und verschickte Quantenbit.

1. Erzeuge ein zufälliges Bit b':
   Ist $b' = 0$, miss $|x\rangle$ bezüglich $B = \{|0\rangle, |1\rangle\}$,
   ist $b' = 1$, miss $|x\rangle$ bezüglich $B' = \{|+\rangle, |-\rangle\}$.

2. Teile Alice über einen klassischen Kanal mit, bezüglich welcher Basis gemessen wurde.

Das Ergebnis der Messung ergibt ein Bit b. Dieses ist 0, falls $|x\rangle$ vor der Messung im Zustand $|0\rangle$ war und in B gemessen wurde, oder im Zustand $|+\rangle$ war und in B' gemessen wurde. Entsprechend ist es 1 im Falle der Kombinationen $|1\rangle$ und B bzw. $|-\rangle$ und B'. Die Schritte A. und B. lassen sich wie in dem Schaltkreis in Abbildung 7.2 ausführen.

Aufgabe 7.1: Zeigen Sie: Ist $b' = a'$, so ist auch $b = a$.

Aufgabe 7.1 zeigt: Haben Alice und Bob die gleiche Basis gewählt, sind sie im Besitz desselben zufälligen Bits. Im anderen Fall hat Bob nichts über Alice' Bit erfahren. Hat Alice etwa $|+\rangle$ verschickt und misst Bob in der Basis B, erhält er die beiden möglichen Ergebnisse mit jeweils derselben Wahrscheinlichkeit.

Aufgabe 7.2: Zeigen Sie: Ist $b' \neq a'$, so sind die Ergebnisse $b = a$ und $b \neq a$ gleich wahrscheinlich.

Verwenden Alice und Bob verschiedene Basen, ist das Ergebnis von Bobs Messung nach Aufgabe 7.2 ein Zufallsbit, das unabhängig von dem Wert von Alice' Bit a ist. Darum teilt Bob in Schritt B.2 Alice die gewählte Basis mit. Entscheidend ist nun: Im weiteren verwenden Alice und Bob die Bits

a und b nur dann für den Schlüssel, wenn sie die gleiche Basis verwendet haben.

C. Alice und Bob entscheiden, ob das Zufallsbit verwendbar ist

1. Alice teilt Bob mit, ob sie die gleiche Basis verwendet haben. Falls nicht, nutzen sie das Ergebnis nicht.

In etwa der Hälfte der Fälle benutzt Bob die gleiche Basis wie Alice. Tauschen die beiden auf diese Weise eine Reihe Bits aus, können sie erwarten, dass dies für die Hälfte zutrifft.

Die folgende Tabelle fasst das Vorgehen zusammen. Der Eintrag Z steht für ein Zufallsbit: mit Wahrscheinlichkeit von jeweils $1/2$ ist dessen Wert 0 oder 1. Im Fall $a' \neq b'$ ist b – das Ergebnis von Bobs Messung – ein solches Zufallsbit und a beziehungsweise b werden nicht als Schlüssel verwendet. Statt von *Schlüsselverteilung* spricht man deshalb besser von *Schlüsselerzeugung*. Es ist nämlich nicht so, dass der Schlüssel schon zu Beginn feststeht und nur verschickt wird: er entsteht erst im Verlauf des Kommunikationsprozesses, da Bobs Wahl von b' die Gestalt des Schlüssels mitbestimmt.

a	0	0	1	1	0	0	1	1
a'	0	1	0	1	0	1	0	1
$\|x\rangle$	$\|0\rangle$	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$
b'	0	0	0	0	1	1	1	1
b	0	Z	1	Z	Z	0	Z	1
Schlüssel	0		1			0		1

Eves Zug

Nach den Schritten A bis C – eventuell müssen diese mehrfach ausgeführt werden – besitzen Alice und Bob ein gemeinsames Zufallsbit. Nun kommen wir zu dem interessanten Punkt des Verfahrens, zu Eve. Das Ziel ist ja gerade, dass diese nichts über den Schlüssel, sprich das Bit a erfährt. Eve steht damit natürlich stellvertretend für alle unbefugten Personen.

Gemäß dem Kerkhoffsschen Prinzip gehen wir davon aus, dass Eve das Prozedere genau kennt. Sie hat vollen Zugriff auf den Quantenkanal, und auch den klassischen Kanal kann sie belauschen, auf dem sich Alice und Bob über die verwendete Basis austauschen. Dadurch erfährt sie die Bits a' und b'; aber erst *nachdem* Bob gemessen hat. Kann Eve mit diesem Wissen das Bit a bestimmen?

Messen und weiterschicken

Nach dem No-Cloning-Theorem (Abschnitt 3.4) kann Eve das Quantenbit $|x\rangle$ nicht kopieren, denn dessen vier mögliche Zustände sind nicht orthogonal. Damit bietet sich folgender Angriff an: Sie misst das Quantenbit und schickt es dann an Bob weiter – oder erzeugt gemäß dem Messergebnis ein neues Quantenbit, das sie Bob übermittelt, als käme es von Alice.

1. Eve wählt ein Bit e'.

2. Ist $e' = 0$, misst sie bezüglich B, sonst bezüglich B'.

Die Erzeugung von e' lassen wir offen. Hier könnte irgendeine raffinierte Strategie oder auch ein Zufallsverfahren zum Zuge kommen. Eve kann dabei ausschließlich ihr erlauschtes Wissen verwenden; das Bit e' ist darum *unabhängig* von den Bits, die Alice und Bob erzeugen. Natürlich könnte Eve auch in anderen Basen als B und B' messen. Man kann sich jedoch überlegen, dass daraus kein Vorteil entsteht: so lässt sich das Grundproblem nicht umgehen, dass die möglichen Zustände des zu belauschenden Bits nicht orthogonal sind. Im nächsten Abschnitt diskutieren wir allgemeinere Lauschstrategien, die diesen Fall einschließen.

Wüsste Eve, bezüglich welcher Basis Alice das Zufallsbit kodiert hat, könnte sie erfolgreich und unbemerkt lauschen. Denn eine Messung in der korrekten Basis beeinflusst den Zustand nicht. Da dies nicht der Fall ist, wird sie – wie Bob – in der Hälfte der Fälle die falsche Basis wählen, egal nach welcher Strategie sie e' wählt.

Beispiel 7.1: Wir nehmen an, dass

$$|x\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

ist, das heißt $a = 0, a' = 1$.

1. Wählt Eve $e' = 1$ und misst in der Basis $B' = \{|+\rangle, |-\rangle\}$, ist das Ergebnis $|+\rangle$. Sie folgert $a = 0$ und das Quantenbit $|x\rangle$ wurde nicht verändert.
2. Anderenfalls – $e' = 0$ – misst Eve in der Basis $B = \{|0\rangle, |1\rangle\}$. Das Ergebnis ist mit jeweils gleicher Wahrscheinlichkeit $|0\rangle$ oder $|1\rangle$, und sie hat nichts über das Bit a erfahren. Mehr noch: Bit $|x\rangle$ wurde verändert. Es ist in gerade den Zustand übergegangen, den Eve beobachtet hat. ◇

Bei wiederholtem Lauschen, kann Eve auf diese Weise dennoch einiges über den ausgetauschten Schlüssel herausbekommen. Alice und Bob verwenden ein Bit nur im Fall $a' = b'$. Da e' von der Wahl der Zufallsbits von Alice und Bob unabhängig ist, hat e' mit Wahrscheinlichkeit $1/2$ den gleichen Wert, und Eve erfährt aus dem Basenaustausch in Schritt C, ob das der Fall ist. Anderenfalls ist ihr Messergebnis ein wertloses Zufallsbit, aber immerhin: sie

erfährt die Hälfte des Schlüssels. Wir folgern: die Schritte A bis C allein sind unsicher!

Aber die Bits, die Eve in der falschen Basis gemessen hat, sind verändert. Das können Alice und Bob ausnutzen, um einen Test auf unbefugten Zugriff auszuführen. Dazu müssen sie ein bereits korrekt übertragenes Bit opfern.

D. Alice und Bob opfern ein Bit, um Eve zu entlarven

Alice und Bob haben ein übertragenes Bit $|x\rangle$ bezüglich derselben Basis gemessen: Es gilt $a' = b'$ und deshalb erwarten sie $a = b$.

1. Alice und Bob tauschen a und b über den klassischen Kanal aus.
2. Stimmen die Ergebnisse nicht überein, brechen sie die Schlüsselerzeugung ab und verwenden die bereits übertragenen Schlüssel nicht.
3. Stimmen die Ergebnisse überein, fahren Sie mit der Schlüsselübertragung fort, verwenden aber das ausgetauschte Bit nicht.

Wie groß ist die Wahrscheinlichkeit, Eves Lauschversuch aufzudecken? Voraussetzung von Teil D ist $a' = b'$. Hat Eve die Basis korrekt geraten – $a' = b' = e'$ – stimmen die Bits a und b überein und Eve wird nicht entlarvt. Hat Eve falsch geraten, projiziert die Messung das ausgetauschte Bit $|x\rangle$ in die falsche Basis. Damit ist Bobs Messung ein Zufallsbit – wie in dem Fall, in dem er selbst die falsche Basis wählt – und mit Wahrscheinlichkeit $1/2$ gilt $a \neq b$. Insgesamt wird Eve in diesem Schritt also mit Wahrscheinlichkeit $1/4$ entdeckt.

Aufgabe 7.3: Rechnen Sie nach: falls Eve bezüglich der falschen Basis gemessen hat, gilt mit Wahrscheinlichkeit $1/2$, dass $a \neq b$.

Die folgende Tabelle zeigt, wie Bits zur Enttarnung Eves verwendet werden. Im Falle 'Z' wird Eves Zugriff mit Wahrscheinlichkeit $1/2$ aufgedeckt.

a	0	0	1	1	0	0	1	1
a'	0	1	0	1	0	1	0	1
b'	0	1	0	1	0	1	0	1
e'	0	0	0	0	1	1	1	1
b	0	Z	1	Z	Z	0	Z	1

Wir fassen Eves Situation zusammen. Da Alice das Bit a' zufällig wählt, gibt es für Eve keine gute Strategie, in der richtigen Basis zu messen. In der Hälfte der Fälle wählt sie die falsche und erhält ein Zufallsbit. Das ist aus Eves Sicht nicht schlimm, da sie so immerhin die Hälfte des Schlüssels zuverlässig erlauscht. Schlimm für Eve und gut für Alice und Bob ist: Eves Lauschangriff wird dann in der Hälfte der Fälle aufgedeckt. Alice und Bob brechen in diesem Fall die Schlüsselerzeugung ab.

Die Situation des Lauschers

Nun ist es an der Zeit, das Protokoll als Ganzes zu diskutieren.

Das BB84-Protokoll zur Schlüsselerzeugung

Benötigt werden ein Quantenkanal und ein klassischer Kanal.

Falls das Protokoll nicht wegen Lauschverdachts abgebrochen werden muss, ergibt sich der Schlüssel aus Alice' Bits $a_1,\ldots,a_m$ und Bobs Bits $b_1,\ldots,b_m$, die in den Schritten 4 und 5 nicht verworfen werden.

1. Alice erzeugt Zufallsbits $a_1,\ldots,a_m$ und $a'_1,\ldots,a'_m$.
2. Alice erledigt für $i=1,\ldots,m$:
   - kodiere a_i als $|0\rangle$ beziehungsweise $|1\rangle$ falls $a'_i=0$
   - kodiere a_i als $|+\rangle$ oder $|-\rangle$ falls $a'_i=1$
   - schicke das entstandene Quantenbit an Bob.
3. Bob erzeugt Zufallsbits $b'_1,\ldots,b'_m$.
   Das i-te Quantenbit von Alice misst er
   - in der Basis $B=\{|0\rangle,|1\rangle\}$ falls $b'_i=0$
   - in der Basis $B'=\{|+\rangle,|-\rangle\}$ falls $b'_i=1$

   und speichert das Ergebnis als b_i.
4. Alice und Bob vergleichen für $i=1,\ldots,m$ die Bits a'_i und b'_i über einen klassischen Kanal.
   Ist $a'_i\neq b'_i$ werden a_i beziehungsweise b_i nicht verwendet.
5. Alice und Bob tauschen k der nicht gelöschten Bits a_i, b_i aus und ermitteln die Fehlerrate, definiert als *Anzahl der sich unterscheidenden Bits geteilt durch k*.
   Ist die Fehlerrate zu hoch, verwenden sie die erzeugten Bits nicht, da Verdacht auf einen Angriffe seitens Eve besteht.

Den letzten Schritt sollten wir noch eingehender betrachten. Wir haben bereits gesehen, dass Eves oben beschriebene Lauschstrategie für jedes der k geopferten Bits mit Wahrscheinlichkeit $1/4$ einen Fehler verursacht. Zu

Beginn dieses Abschnitts haben wir einen perfekten Quantenkanal vorausgesetzt. Somit hat ein unbelauschter Ablauf die Fehlerrate 0. Belauscht Eve jedes Bit, bleibt sie nur mit Wahrscheinlichkeit $(3/4)^k$ unerkannt. Die Wahrscheinlichkeit, einen Lauschangriff zu entdecken, wächst exponentiell in der Zahl der dafür geopferten Bits; das Restrisiko, dass Eve mit dem Schlüssel unbemerkt entwischt, wird bei geeignet groß gewähltem k so klein, dass es praktisch irrelevant ist. Zumal wir ihr bereits optimale Voraussetzungen zugestanden haben. Aus Zweckpessimismus ignorieren wir, dass Eves Zugriff auf die Kanäle in realen Fällen meist weniger absolut sein wird. Wir folgern: *Das BB84-Protokoll erlaubt sichere Schlüsselverteilung*. Aber nur unter den Voraussetzungen, von denen unsere bisherige Analyse ausging:

1. Eve verwendet die oben beschriebene Lauschstrategie.

2. Der Quantenkanal ist perfekt.

Kryptographie über verrauschte Kanäle

Punkt 1 werden wir im nächsten Abschnitt diskutieren. Punkt 2 ist deshalb wichtig, weil in der Praxis keine perfekten Quantenkanäle zur Verfügung stehen. Bei einem realen Kanal hat unser Protokoll daher auch unbelauscht eine Fehlerrate größer 0. Belauscht Eve jedes Bit, ist die erwartete Fehlerrate $1/4$. Heutige Übertragungsmethoden lassen unbelauscht deutlich niedrigere Fehlerraten zu, so dass die Fälle *belauscht* und *nicht belauscht* trotz Rauschens unterschieden werden können.

Allerdings bietet sich dann für Eve die folgende Strategie an: Sie misst nur wenige Bits. Auf diese Weise erhält sie nur einen geringen Teil des Schlüssels, die Auswirkungen ihrer Lauschtätigkeit könnten – geschickt kalkuliert – in dem allgemeinen Rauschen unentdeckt bleiben. Diesem Problem begegnet man mit dem Einsatz fehlerkorrigierender Codes und dem folgenden Verfahren.

Verstärkung der Sicherheit

Privacy amplification

Eine Methode namens *privacy amplification* erlaubt es, aus einem nur teilweise geheimen Schlüssel einen kürzeren, sehr geheimen Schlüssel zu erzeugen; und zwar mittels öffentlicher Diskussion.

Wir stellen uns vor, Alice und Bob haben zwei Schlüsselbits b_1 und b_2 ausgetauscht. Eve hat eines davon erfahren. Darum beschließen Alice und Bob, aus den zwei Schlüsselbits ein einzelnes neues zu erzeugen:

$$b_3 = b_1 \oplus b_2.$$

Angenommen, Eve weiß, dass $b_1 = 0$ gilt. Über b_2 weiß sie hingegen nichts: aus ihrer Sicht sind die Fälle $b_2 = 0$ und $b_2 = 1$ gleichwahrscheinlich. Dann weiß sie über b_3 ebenso wenig! Ihre Kenntnis von b_1 verrät nichts über b_3, da b_1 mit dem unbekannten, aus Eves Sicht zufälligen Bit b_1 überschrieben ist; wie bei der Verschlüsselung mittels One-Time Pads.

Genauso ist die Summe $b_1 \oplus b_2 \oplus \ldots \oplus b_k$ ein ihr unbekanntes Zufallsbit, wenn sie *eines* der k Bits nicht kennt. Um aus einer Folge von m Zufallsbits n neue zu erzeugen ($n < m$), wählt man zufällig n Teilmengen der Bits aus. Die Summe der Bits jeweils einer Teilmenge ergeben ein neues Zufallsbit. In [15] ist dieses Verfahren analysiert worden und hat sich als effizient erwiesen, insbesondere in Verbindung mit fehlerkorrigierenden Codes. Die Fehlerrate des BB84-Protokolls gibt einen deutlichen Hinweis darauf, wieviele Bits Eve kennen kann. Verkürzen Alice und Bob mittels *privacy amplification* den Schlüssel um diese Zahl, kennt Eve mit großer Wahrscheinlichkeit nur noch sehr wenige Bits.

Zusammenfassung

Was bringt die Quantenkryptographie Neues? Unberechtigte Versuche, auf die übermittelten Daten zuzugreifen, werden aufgedeckt. Ein Lauschangriff auf ein einzelnes Bit wird zwar nur mit einer bestimmten Wahrscheinlichkeit bemerkt. Wird jedoch ein längerer Schlüssel übertragen ist es praktisch nicht möglich, relevante Informationen über diesen zu erlangen, ohne entdeckt zu werden. Verlassen wir zur Erläuterung kurz das Gebiet der Kryptographie: Ein Einbruch in ein hochmodernes Sicherheitssystem, zum Beispiel in den Safe einer Zentralbank, kann theoretisch unbemerkt bleiben. Nach den Gesetzen der klassischen Physik spricht nichts dagegen, dass Eve das System in exakt dem gleichen Zustand zurücklässt, in dem sich dieses vor dem Eindringen befand. Dagegen folgt aus den Gesetzen der Quantenmechanik, dass ihre Messungen am Quantenkanal deutliche Spuren hinterlassen, möchte sie Wesentliches über den ausgetauschten Schlüssel erfahren.

Die Möglichkeit, Lauschangriffe aufzudecken, ist der wesentliche Beitrag der Quantenmechanik. Dazu gibt es im klassischen Fall kein Pendant. Durch das beschriebene Verfahren werden die sicheren, aber durch das Problem der Schlüsselverteilung unhandlichen, One-Time Pads praktikabel.

7.3 Lauschstrategien

Im letzten Abschnitt wurde das BB84-Protokoll eingeführt. Um zu analysieren, wie sicher das Verfahren ist, müssen wir die möglichen Angriffe von Eve untersuchen. Wir sind bisher davon ausgegangen, dass Eve das übermittelte Quantenbit misst und weiterschickt. Diese Strategie liegt nah, da sich Quantenbits nicht kopieren lassen. Ein Vorteil dieser Lauschstrategie ist, dass Eve kein Quantenbit speichern muss: das wäre mit beträchtlichem Aufwand verbunden und ist zurzeit nur für kurze Zeitspannen möglich. Allerdings sind auch Angriffe interessant, die bisher nur theoretisch möglich sind. So können Alice und Bob nicht wissen, ob Eves technische Fähigkeiten nicht viel weiter fortgeschritten sind, als sie glauben.

Im letzten Abschnitt haben wir gesehen: Wenn Eve die übermittelten Bits misst, werden diese Eingriffe mit hoher Wahrscheinlichkeit entdeckt. Darum untersuchen wir einen anderen Ansatz. Wir setzen voraus, dass Eve im Besitz einer Reihe von Quantenbits $|e_1\rangle, |e_2\rangle, \ldots$ ist. Sie wendet unitäre Transformationen auf den Kanal und diese Quantenbits an und versucht so viel Information über das gesendete Bit wie möglich auf ihre Bits zu

übertragen. Das andere wesentliche Ziel ist natürlich weiterhin, unentdeckt zu bleiben.

Die Sicherheit des BB84-Protokolls – angereichert um die Verwendung von fehlerkorrigierenden Codes und *privacy amplification* – allgemein zu untersuchen, ist eine Aufgabe, die jenseits der in diesem Buch vermittelten Methoden liegt. Doch bereits im letzten Abschnitt haben wir erfahren: Wenn Eve die gesendeten Quantenbits misst und weiterschickt, kann sie die Sicherheit des Protokolls nicht gefährden. Dieser Abschnitt soll ein Gefühl dafür vermitteln, dass auch allgemeinere Angriffe entweder bemerkt werden oder nur sehr wenig über den Schlüssel in Erfahrung bringen.

Wir beginnen mit einem einfachen Beispiel.

Beispiel 7.2: Eve erinnert sich daran, dass man mit einem CNOT-Gatter Quantenbits miteinander verschränken kann. Wäre das nicht die Lösung? Sie verschränkt ein Quantenbit in ihrem Besitz mit dem gesendeten. Dann wartet sie ab, bis Alice und Bob ihre Basen vergleichen. Sie belauscht diesen Schritt und verwendet die gewonnene Information, wenn sie ihr eigenes Quantenbit misst: sie nutzt es für die Wahl einer Messbasis.

1. Wir nehmen an, Alice sendet $|x\rangle = |1\rangle$. Eve führt die Operation CNOT auf diesem Bit und einem vorbereiteten Quantenbit $|e\rangle$ im Zustand $|0\rangle$ aus. Das Ergebnis: Die Bits sind im Zustand

$$|x\rangle|e\rangle = |1\rangle|1\rangle.$$

Eve wartet Bobs Messung ab und belauscht, welche Basis er verwendet hat. Misst Bob in der richtigen – in B also – tut sie es ihm gleich und erfährt das Schlüsselbit $a = b = 1$. Misst Bob in der anderen Basis, verwenden Alice und Bob das Bit nicht, und Eve ignoriert es ebenso.

BB84 deckt Verschränkung auf

2. Sendet Alice hingegen $|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, überführt das CNOT-Gatter die Bits in den Zustand

$$|x\rangle|e\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle).$$

2.1 Bob misst in der Basis B. Er beobachtet $|0\rangle$ oder $|1\rangle$ mit gleicher Wahrscheinlichkeit. Eve misst ihr Bit und erhält dasselbe Ergebnis wie Bob. Das ist schließlich der Grund, ihr Quantenbit mit dem gesendeten zu verschränken. Allerdings wird dieses Bit nicht verwendet, da Bobs Basis nicht mit der von Alice übereinstimmt.

2.2 Das nächste übermittelte Bit ist ebenfalls im Zustand $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, diesmal misst Bob in der richtigen Basis B' – und das BB84-Protokoll enttarnt Eve in der Hälfte der Fälle!

Das zeigt folgende Rechnung: Ein Bit in der Basis B' zu messen, entspricht einer Anwendung der Hadamard-Transformation mit anschlie-

ßender Messung in B. Bob misst das erste Bit des verschränkten Paares $|x\rangle|e\rangle$.

$$\begin{aligned} H(|x\rangle)|e\rangle &= \frac{1}{\sqrt{2}}\Big((H|0\rangle)|0\rangle - (H|1\rangle)|1\rangle\Big) \\ &= 1/2(|00\rangle - |01\rangle + |10\rangle + |11\rangle) \end{aligned}$$

Das Ergebnis stimmt in der Hälfte der Fälle nicht mit Alice' Bit überein, obwohl die gleichen Basen verwendet wurden.

In diesem Fall hat die Anwendung des CNOT-Gatters die gleiche Auswirkung auf Bobs Ergebnis wie eine Messung in der falschen Basis B.

Es gibt ein Analogon zu CNOT, dessen Einfluss in der Basis B aufgedeckt wird und in der Basis B' unbemerkt bleibt. Die Situation ist die gleiche wie beim direkten Messen: da die möglichen Zustände des Quantenbits $|x\rangle$ nicht orthogonal sind, wird die Verschränkung mit Eves Bits bei Bobs Messung in einem Viertel der Fälle aufgedeckt. ◇

Ohne es formal bewiesen zu haben, hat uns Beispiel 7.2 folgendes einsehen lassen: Verschränkt Eve eines ihrer Quantenbits mit $|x\rangle$, dem über den Quantenkanal versendeten Bit, wird das Ergebnis von Bobs Messung genauso beeinflusst, als würde Eve das Bit $|x\rangle$ messen. Damit haben wir einen weiteren speziellen Angriff untersucht. Nun wollen wir uns der Aufgabe nähern, mögliche Angriffe von Eve allgemein zu beschreiben.

Angriffe ohne Verschränkung

Wir verallgemeinern nun Eves Möglichkeiten. Die folgende Angriffsart schöpft sie zwar noch nicht ganz aus, ist dafür jedoch sehr einfach zu analysieren.

Eve möchte unterscheiden, ob das von Alice an Bob gesendete Quantenbit $|x\rangle$ im Zustand $|0\rangle$ oder im Zustand $H|0\rangle = |+\rangle$ ist. Dazu wendet sie eine unitäre Zwei-Bit-Transformation U auf den Kanal (das heißt, auf $|x\rangle$) und ihr Bit an, insgesamt also auf $|x\rangle|e\rangle$. Den Anfangszustand von $|e\rangle$ nennen wir $|\phi_a\rangle$. Anschließend misst Eve $|e\rangle$ in irgendeiner Weise.

1. Eve will absolut unbemerkt bleiben und fordert, dass die Transformation U das Bit $|x\rangle$ unverändert lassen soll. Dann gibt es zwei von der Wahl von U abhängige Einheitsvektoren $|\phi_0\rangle$, $|\phi_+\rangle$, so dass

$$|0\rangle|\phi_a\rangle \xrightarrow{U} |0\rangle|\phi_0\rangle \text{ und } |+\rangle|\phi_a\rangle \xrightarrow{U} |+\rangle|\phi_+\rangle.$$

Mit der Wahl dieser Vektoren ist die unitäre Transformation bereits exakt bestimmt; da U linear ist, folgen mit einer einfachen Rechnung die Bilder von zum Beispiel $|1\rangle|\phi_a\rangle$ und $|-\rangle|\phi_a\rangle$. Welchen der beiden möglichen Folgezustände $|\phi_0\rangle$ und $|\phi_+\rangle$ Eves Bit angenommen hat, ist die einzige Information, die sie bei dem Lauschversuch gewonnen hat. Aus dieser allein muss

entschieden werden, welchen Zustand $|x\rangle$ hat. Da unitäre Transformationen winkelerhaltend sind, gilt[1]

$$\langle 0|+\rangle\langle \phi_a|\phi_a\rangle = \langle 0|+\rangle\langle \phi_0|\phi_+\rangle.$$

Da $|0\rangle$ und $|+\rangle$ nicht orthogonal sind, können wir durch $\langle 0|+\rangle$ teilen; es folgt

$$\langle \phi_0|\phi_+\rangle = 1.$$

Das heißt (siehe Aufgabe A.8 im Anhang):

$$|\phi_0\rangle = |\phi_+\rangle.$$

Mit der $|x\rangle$ unverändert lassenden Transformation U kann Eve nicht entscheiden, ob $|x\rangle$ den Wert $|0\rangle$ oder $|+\rangle$ hat. Daraus folgt: Wenn Eve in dieser Methode das Risiko entdeckt zu werden, ganz ausschließen will, erfährt sie nichts über $|x\rangle$.

2. Eve beschließt, eine gewisse Störung in Kauf zu nehmen. Sie verwendet eine unitäre Transformation U', die Bit $|x\rangle$ verändert, wenn auch nach Möglichkeit nicht zu sehr. Ist dieses im Zustand $|0\rangle$, so ist das Ergebnis $|\tilde{0}\rangle$, aus dem Zustand $|+\rangle$ wird $|\tilde{+}\rangle$.

$$|0\rangle|\phi_a\rangle \xrightarrow{U'} |\tilde{0}\rangle|\phi_0\rangle \text{ und } |+\rangle|\phi_a\rangle \xrightarrow{U'} |\tilde{+}\rangle|\phi_+\rangle.$$

Es folgt

$$\langle 0|+\rangle = \langle \tilde{0}|\tilde{+}\rangle\langle \phi_0|\phi_+\rangle.$$

Die Zustände $|\phi_0\rangle$ und $|\phi_+\rangle$ lassen sich umso besser unterscheiden, desto kleiner $\langle \phi_0|\phi_+\rangle$ ist. Also müsste Eve die Transformation U' entsprechend wählen. Von dieser Wahl unabhängig ist jedoch das Skalarprodukt $\langle 0|+\rangle = 1/\sqrt{2}$. Dadurch wird $\langle \tilde{0}|\tilde{+}\rangle$ in gleichem Maße größer, wie $\langle \phi_0|\phi_+\rangle$ kleiner wird. Der Wert $\langle \tilde{0}|\tilde{+}\rangle$ ist ein Maß für die Störung des bei Bob ankommenden Bits. Das heißt:

Umso mehr Information Eve erhält, desto stärker wird $|x\rangle$ verändert.

Eves Zielkonflikt

Unsere Argumentation ähnelt der in den Abschnitten 3.4 und 3.6. Allerdings schöpft Eve mit der beschriebenen Strategie ihre Möglichkeiten wie erwähnt nicht aus. Deutlich wird ihr Zielkonflikt zwischen *viel Information* erhalten und *unbemerkt* bleiben. Diesen kann sie mit keiner Strategie wie eben beschrieben der eben beschriebenen Art umgehen. Wenn Eve unbemerkt bleiben will, kann sie nur wenig über das übermittelte Quantenbit $|x\rangle$ in Erfahrung bringen. Wenn sie über dieses viel erfährt, wird sie aller Wahrscheinlichkeit nach ertappt.

[1] Die linke Seite der Gleichung besteht aus dem Skalarprodukt der beiden Ausgangszustände $|0\rangle|\phi_a\rangle$ und $|+\rangle|\phi_a\rangle$, die rechte aus dem der beiden Bilder unter der Transformation U, siehe auch Seite 2.7

Eine Lauschstrategie mit verschränkten Bits

Wir können diesen Ansatz noch verallgemeinern, indem wir Eve erlauben, ihr Bit mit dem versendeten zu verschränken. Einen speziellen Fall dieser Idee haben wir bereits im Beispiel 7.2 kennen gelernt. Eve verwendet ein Quantenregister $|E\rangle$ im Anfangszustand $|\phi_a\rangle$ und wendet eine unitäre Transformation V auf $|x\rangle|E\rangle$ an. Dadurch hat sie die Möglichkeit ihr Quantenregister mit dem übermittelten Bit zu verschränken. Mit der Messung ihres Quantenregisters kann sie warten, bis Alice und Bob die verwendeten Basen öffentlich ausgetauscht haben. Die Nachfolgezustände von Eves Transformation V haben die Form

$$|0\rangle|\phi_a\rangle \xrightarrow{V} |0\rangle|\phi_{00}\rangle + |1\rangle|\phi_{01}\rangle$$

und

$$|1\rangle|\phi_a\rangle \xrightarrow{V} |0\rangle|\phi_{10}\rangle + |1\rangle|\phi_{11}\rangle.$$

Eves Anteile $|\phi_{00}\rangle, |\phi_{01}\rangle$ etc. sind in diesen Formeln keine normalisierten Zustände: Gilt beispielsweise

$$|0\rangle|\phi_a\rangle \xrightarrow{V} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle),$$

so wäre $|\phi_{00}\rangle = 1/\sqrt{2} \cdot |0\rangle$ und $|\phi_{01}\rangle = 1/\sqrt{2} \cdot |1\rangle$. Aus der Forderung, dass Eves Zugriff so unauffällig wie möglich sein soll, folgt sofort dass $\langle\phi_{01}|\phi_{01}\rangle$ und $\langle\phi_{10}|\phi_{10}\rangle$ so klein wie möglich zu sein haben.

Das gleiche gilt, wenn Alice das Bit in der Hadamardbasis kodiert hat. Wir setzen an:

$$|+\rangle|\phi_a\rangle \xrightarrow{V} |+\rangle|\phi_{++}\rangle + |-\rangle|\phi_{+-}\rangle$$

und

$$|-\rangle|\phi_a\rangle \xrightarrow{V} |+\rangle|\phi_{-+}\rangle + |-\rangle|\phi_{--}\rangle,$$

wobei $|\phi_{++}\rangle, |\phi_{+-}\rangle, \ldots$ vier weitere nichtnormalisierte Zustände sind. Wenden wir die Linearität von V an, können wir diese als Linearkombination von $|\phi_{00}\rangle$ und $|\phi_{10}\rangle$ darstellen. Damit lässt sich der Wunsch $\langle\phi_{+-}|\phi_{+-}\rangle$ und $\langle\phi_{-+}|\phi_{-+}\rangle$ klein zu halten, als weitere Bedingung an $|\phi_{00}\rangle, |\phi_{10}\rangle$ etc. formulieren.

Auf der anderen Seite will Alice natürlich möglichst viel über das gesendete Bit herausfinden. In einer Reihe von Veröffentlichungen ist dieser Ansatz intensiv untersucht worden (eine Übersicht findet der Leser in [19]). Eve hat demnach denselben Zielkonflikt, den wir bei den Angriffen ohne Verschränkung beobachtet haben. In dem Maß, in dem Eve Informationen über den Schlüssel gewinnt, verändert sie die übermittelten Bits. Werden Fehlerkorrektur und privacy amplification verwendet, bietet das BB84-Protokoll gegen derartige Angriffe hinreichende Sicherheit. Ist die Anzahl der ausgetauschten Bits hinreichend groß, ist die Anzahl der für den Erhalt der Sicherheit aufzuwendenden Bits tolerierbar.

Die allgemeinste mögliche Lauschsituation würde nur voraussetzen, dass Eve mit den ausgetauschten Quantenbits in Kontakt tritt und dass die Gesetze der Quantenmechanik gelten. Die bisher beschriebenen Angriffe sind

noch nicht so generell modelliert. Sie werden als *inkohärente* oder *unzusammenhängende* Angriffe bezeichnet, da Eve die von Alice an Bob geschickten Quantenbits nacheinander, jedes für sich analysiert. Man kann nun noch allgemeinere Szenarien erdenken, in denen Eve die ausgetauschten Quantenbits als ein System auffassen kann und Messungen vornehmen darf, die allgemeiner als die in diesem Buch präsentierten sind (siehe zum Beispiel [74]). Nach unseren bisherigen Überlegungen dürfen wir zu Recht vermuten, dass daraus kein Vorteil entsteht.

Man-in-the-middle attack

Einen Angriff gibt es, dem das BB84-Protokoll zunächst schutzlos ausgeliefert ist. Vielleicht ist der eine oder andere Leser selbst auf die Idee gekommen: Wenn Eve sich Alice gegenüber als Bob ausgibt und alle seine Schritte simuliert, wenn Eve außerdem in gleicher Weise Bob gegenüber Alice' Rolle im BB84-Protokoll übernimmt, kann sie natürlich nicht entdeckt werden. Allerdings benötigt Eve dazu eine vollkommene Kontrolle des Geschehens. Und glücklicherweise gibt es klassische Verfahren, die vor einem solchen *man-in-the-middle attack* schützen: das sind sogenannte *Authentisierungsverfahren*. Ein Stichwort in diesem Zusammenhang lautet *digitale Unterschrift*.

7.4 Quantenverschlüsselung mit Verschränkung

Die bisher beschriebene BB84-Verschlüsselung beruht darauf, dass Quantenzustände mit nicht-orthogonalen Zuständen verändert werden, möchte man etwas über sie herausfinden. 1991 hat Artur Ekert von der Universität Oxford ein Verfahren vorgeschlagen, das verschränkte Quantenbits nutzt. Diese nur zweieinhalb Seiten lange Publikation [42] zählt mittlerweile zu den meist zitierten Veröffentlichungen zur Kryptographie.

Vorüberlegung

Wir erinnern uns an das Gedankenexperiment aus Abschnitt 2.11. Alice erzeugt ein Paar verschränkter Quantenbits

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Eines davon schickt sie Bob. Messen beide ihre Hälften des verschränkten Paares, erhalten sie dasselbe Ergebnis. Mit Wahrscheinlichkeit $1/2$ ist dieses 0, mit der gleichen Wahrscheinlichkeit 1. Nach der Messung besitzen beide das gleiche, zufällig erzeugte Bit, ohne dass dieses im gewohnten Sinn ausgetauscht werden musste. Zum Zeitpunkt der Übertragung stand das Ergebnis der Messungen allerdings noch nicht fest. Das Zufallsbit ist in diesem Sinne nie übertragen worden und konnte also nicht belauscht werden.

Damit scheinen verschränkte Bits für die Erzeugung von Schlüsseln gut geeignet zu sein. Nach den Erfahrungen, die wir in den vorhergehenden Abschnitten mit Eves Raffinesse gemacht haben, erscheint uns das jedoch als zu einfach. Bitte denken Sie vor dem Weiterlesen eine Weile über die folgende Aufgabe nach: