Quantenkryptographie

A. Dirks, B. Lenk

16.12.2005

Inhaltsverzeichnis

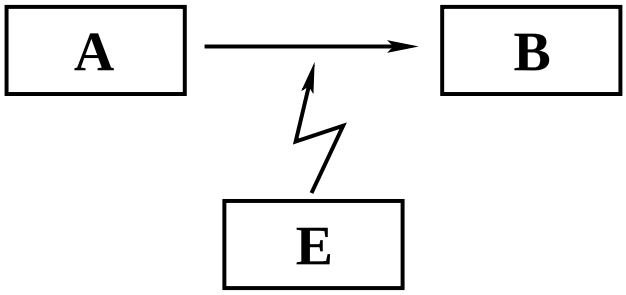

Abbildung 1: Allgemeine kryptographische Kommunikationssituation. Alice möchte Bob eine Nachricht übermitteln, die von Eve gelesen bzw. manipuliert werden könnte und somit in zweierlei Hinsicht einer Störung ausgesetzt ist.

1 Einführung

Die Quantenkryptographie beschäftigt sich mit der sicheren Übertragung von Informationen unter Nutzung der Gesetzmäßigkeiten der Quantenmechanik. Im Gegensatz zur klassischen Kryptographie bietet sie sichere Kommunikation, ohne dass zuvor die Kommunikationspartner eine mit der zu übermittelnden Nachricht von der Größe her vergleichbare gemeinsame Informationsbasis haben müssen.
Hier soll der Gegensatz zur klassischen Kryptographie herausgestellt, Funktionsweise am Beispiel des *BB84*-Protokolls verdeutlicht, selbige durch Angabe anderer Protokollmechanismen vertieft und aktuelle Entwicklungen in diesem Feld erläutert werden.

2 Grundlagen, *BB84* und Eavesdropping

2.1 Motivation

Als Ausgangsproblem dient die in Abbildung 1 skizzierte Situation. In der Kryptographie untersucht man dabei Möglichkeiten zur sicheren Übertragung von Informationen. Das einzig im Sinne von verschwindender Shannon-Information von Eve als sicher bekannte Verfahren der klassischen Informationstheorie ist das one-time-pad. Alle anderen heute gängigen Verschlüsselungsmethoden wie beispielsweise RSA basieren auf „Komplexitätsfallen“. So fällt die Faktorisierung von Primzahlen unter die Klasse NP-vollständiger Probleme, die mit deterministischen Rechnerarchitekturen – wie zur Sicherheit der Algorithmen vermutet wird – eine exponentielle Laufzeit besitzen. Untersucht man dieses Problem jedoch mit prinzipiell mögli-

chen nichtdeterministischen[1] Architekturen, etwa Quantencomputern, so ist eine Berechnung in Polynomialzeit möglich.[2] Auch Probleme mit erwiesenermaßen deterministisch exponentieller Laufzeit können teilweise mit Quantencomputern recht schnell gelöst werden.
Von dieser Warte aus betrachtet liefern Komplexitätsbetrachtungen also nur relative Sicherheit. Die Alternative des absolut sicheren one-time-pads ist jedoch in den meisten Fällen unpraktikabel, da der Schlüsselaustausch für kryptographische Sicherheit mit nonkryptographischen Methoden durchgeführt werden muss – aus Sicht der klassischen Informationstheorie: Die Schlüssellänge muss mindestens der Nachrichtenlänge entsprechen, um die zur (De-)Kodierung notwendigen bitweisen `XOR`-Verknüpfungen[3] durchführen zu können.

Idee der Quantenkryptographie

Die Quantenkryptographie setzt an genau diesem Punkt an. Sendet Alice anstatt eines klassischen Signals einen Quantenzustand $|\psi\rangle$ an Bob, so wird eine von Eve durchgeführte Messung einer Observablen $\mathcal{L}$ den Zustand $|\psi\rangle$ im Allgemeinen manipulieren, wenn $|\psi\rangle$ nicht gerade ein Eigenzustand von $\mathcal{L}$ ist. Durch geschickte Präparation der Umstände wird die Eve vermittelte Information nun minimal, da Alice zufällig Zustände auswählen kann, die mit $\mathcal{L}$ verträglich sind oder auch nicht. Insbesondere ist dabei die durch Eve verursachte Störung für Bob und Alice auszumachen, die über einen authentifizierten öffentlichen klassischen Informationskanal verfügen, über den sie Abgleiche vornehmen können, der aber von allen gelesen werden kann.
Eve kann prinzipiell keine Messungen durchführen, ohne entdeckt zu werden, denn sie kann $|\psi\rangle$ auch nicht kopieren, um an der Kopie Messungen durchzuführen, wie man leicht zeigt (*no-cloning theorem*):
Sei $\mathcal{H}_{\mathrm{QCM}}$ der Hilbertraum der „Quanten-Kopiermaschine“ (QCM) von Eve und $|b\rangle$ der Zustand, der mit $|\psi\rangle$ überschrieben werden soll, sowie $|0\rangle \in \mathcal{H}_{\mathrm{QCM}}$ der Ausgangszustand der QCM. Idealerweise sollte die QCM eine Zuordnung

$$|\psi, b, 0\rangle \mapsto |\psi, \psi, f_\psi\rangle\,,$$

durchführen (f_ψ : Endzustand der QCM), soll das aber auch für ein linear unabhängiges $|\phi\rangle$ funktionieren, so folgt bis auf Normierung

$$|\psi + \phi, b, 0\rangle = |\psi, b, 0\rangle + |\phi, b, 0\rangle \mapsto |\psi, \psi, f_\psi\rangle + |\phi, \phi, f_\phi\rangle \neq |\psi + \phi, \psi + \phi, f\rangle$$

für egal welches $f \in \mathcal{H}_{\mathrm{QCM}}$, da nach Ausschreiben des rechten Termes die in ψ und ϕ gemischten Terme nicht eliminiert werden können.

[1] Nichtdeterminismus im Sinne von Feynmanschen Pfadintegralen.
[2] NP bezeichnet ein „Nichtdeterministisches Polynomialzeitproblem“.
[3] Auch zu verstehen als Additionen im Körper $\mathbb{F}_2$ bzw. Vektorraum $\mathbb{F}_2^N$.

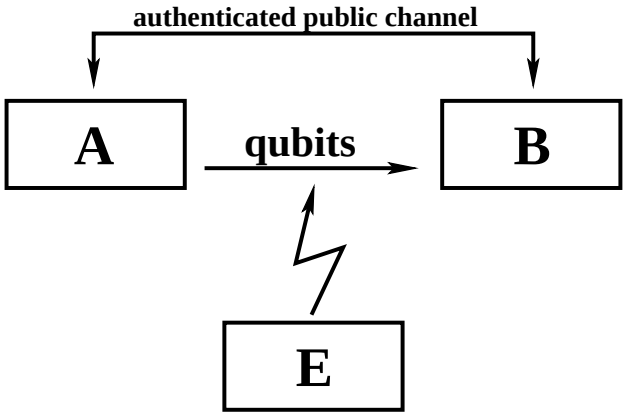

Abbildung 2: Grundschema der Quantenkryptographie.

Die beschriebene fundamentale Anordnung zur Quantenkryptographie (QC) ist in Abbildung 2 dargestellt. Wie bereits erläutert, ist die QC keine vollwertige Kryptographie im eigentlichen Sinne, sondern beschäftigt sich – zumindest aktuell – lediglich mit einem sicheren Schlüsselaustausch, auf den ein klassisches one-time-pad aufsetzen kann.

2.2 QC am Beispiel von *BB84*

BB84 ist das erste vorgeschlagene Protokoll zur Quantenkryptographie und wurde von Bennett und Brassard im Jahre 1984 entwickelt.

Initialisierung und Kodierungskonventionen

Folgende Voraussetzungen bzw. Annahmen liegen dem Protokoll zu Grunde:

- Beliebiges *Zweizustandssystem* mit Hilbertraum $\mathcal{H} \Rightarrow \dim \mathcal{H} = 2$, zu betrachtende Qubits $|\psi_i\rangle \in \mathcal{H}$, Basen $\mathfrak{A}$ und $\mathfrak{B}$ von $\mathcal{H}$;
- *Maximale Konjugation* von $\mathfrak{A}$ und $\mathfrak{B}$: $\forall(|\phi\rangle, |\psi\rangle) \in \mathfrak{A} \times \mathfrak{B} : |\langle\phi|\psi\rangle|^2 = \frac{1}{2}$. Diese Bedingung liefert maximale Unbestimmtheit bei Messung eines Basisvektors mit der nicht zugehörigen Basis;
- Ohne Einschränkung *Spinraum* mit Basen $\mathfrak{A} := \{|\uparrow\rangle, |\downarrow\rangle\}$ und $\mathfrak{B} := \{|\rightarrow\rangle, |\leftarrow\rangle\}$.

Zur Codierung der Basisvektoren. Man ordnet je einem Vektor pro Basis einen Wert 0 oder 1 zu, z.B.:

$$\underbrace{|\uparrow\rangle \mapsto 1, \quad |\downarrow\rangle \mapsto 0,}_{\mathfrak{A}} \qquad \underbrace{|\rightarrow\rangle \mapsto 1, \quad |\leftarrow\rangle \mapsto 0.}_{\mathfrak{B}}$$

Austausch des *„sifted keys“*

Der „sifted key“ ist die erste Vorstufe des resultierenden Schlüssels. Er wird mit den folgenden Schritten generiert:

- Alice schickt *gleichverteilt-zufällige* Sequenz $|\psi_i\rangle \in K_{\mathrm{A}i} \subset \mathfrak{A} \cup \mathfrak{B}$ von Qubits an Bob und merkt sich die verwendete Basissequenz $K_{\mathrm{A}i}$.
- Bob misst $|\psi_i\rangle$ mit ebengleich *zufälliger* Basis $K_{\mathrm{B}i} \in \{\mathfrak{A}, \mathfrak{B}\}$ und merkt sich das resultierende Messergebnis, eine Folge von Einsen und Nullen und die verwendete Basissequenz $K_{\mathrm{B}i}$.
- Korrelation der Basissequenzen K_{A} und K_{B} über öffentl. Kanal, z.B.:

$K_{\mathrm{A}i}$	$\mathfrak{A}$	$\mathfrak{B}$	$\mathfrak{B}$	$\mathfrak{A}$	$\mathfrak{B}$	$\mathfrak{A}$	$\mathfrak{A}$
$K_{\mathrm{B}i}$	$\mathfrak{A}$	$\mathfrak{A}$	$\mathfrak{B}$	$\mathfrak{B}$	$\mathfrak{B}$	$\mathfrak{A}$	$\mathfrak{B}$
	✓	✗	✓	✗	✓	✓	✗

  Dabei bedeutet „✓“ ein Beibehalten der zugehörigen Bits in beiden Schlüsseln (Alice & Bob), „✗“ ein Löschen.

Es resultiert der „sifted key“. Alice's und Bob's Version dieses Schlüssels sind i.a. *ungleich* aufgrund der Intervention von Eve bzw. aufgrund von Leitungsrauschen (z.B. nicht perfekte Messinstrumente).

Einfaches Eavesdropping

Unter dem Begriff des *Eavesdropping* fasst man Formen unerwünschter Einflussnahme seitens Eves zusammen. Naive Versuche der Beeinflussung scheitern: Eve kann weder ein Qubit messen und dann nichts weiterleiten (Bob benachrichtigt Alice über öffentlichen Kanal), noch kann Eve sich ein Qubit kopieren (*no-cloning theorem*).
Es existiert dennoch in diesem Punkt des Protokolls eine einfache Strategie:

Intercept-resend-Strategie. Eve fängt ein Qubit auf, misst es in einer Basis aus $\{\mathfrak{A}, \mathfrak{B}\}$ und leitet einen entsprechend dem Messergebnis präparierten Zustand an Bob weiter. Eve erhält dabei 50 % der Information und generiert eine Qubitfehlerrate QBER von 25 % im Qubitstrom zwischen Alice und Bob.

Privacy Amplification

Unter dem für sich sprechenden Begriff *privacy amplification* versteht man die Vorgänge, die vom sifted zum secret key führen, bzw. enger auch vom gleich erklärten raw key zum secret key. Es soll am Beispiel des einfachen dekohärenten (s.u.) Eavesdroppings von Eve (*intercept-resend*) die Vorgehensweise zur P.A. erläutert werden. Dies geht hier mit klassischer Informationstheorie. Bezeichnen α, β und ε die Variablensätze von Alice, Bob und Eve, so findet man als hinreichende Bedingung an die geteilte Information $S(\alpha, \beta \| \varepsilon)$ von Alice und Bob unter Ausschluss von Eve für die „*key distillation*“ von sifted zu secret key:

$$S(\alpha, \beta \| \varepsilon) \geq \max\{I(\alpha, \beta) - I(\alpha, \varepsilon), I(\alpha, \beta) - I(\beta, \varepsilon)\}. \tag{1}$$

Das Protokoll setzt wie folgt fort:

- *Abschätzung der QBER*: Alice und Bob gleichen *zufällige* Untermenge S des sifted-keys K_{sifted} ab. Dies führt zu einer beliebig genauen Abschätzung von $P(\alpha, \beta)$. Anschließend setzen beide $K_{\text{sifted}} := K_{\text{sifted}} \setminus S$, um die veröffentlichte Information zu löschen. Daraus lässt sich ablesen, ob P.A. möglich ist oder nicht (QBER bis zu 11 % zulässig (s.u.)).

- *Fehlerkorrektur*. Es geschieht mittels klassischer Verfahren Fehlerkorrektur mit Hilfe des öffentlichen Kanals. Z.B. teilt Alice Bob den `XOR`-Wert zweier Bits mit, und wenn dieser mit Bob's übereinstimmt, so löschen beide nur eines der Bits, sonst beide. Alice und Bob haben nun den gleichen Schlüssel, den *raw key*, über den Eve noch Information besitzt.

- *Privacy Amplification*. Dies kann auch klassisch geschehen. Alice wählt zwei Bits und ersetzt diese mit dem `XOR`-Wert, teilt Bob die Bitnummern mit, Bob verfährt ebenso. $\rightsquigarrow$ Eve's Information wird minimiert. $\rightsquigarrow$ *secret key*.

An diesem Punkt terminiert *BB84*, da Alice und Bob nun einen Geheimschlüssel teilen.

2.3 Allgemeines Eavesdropping in *BB84*

Eve kann wesentlich ausgefeiltere Methoden als die *intercept-resend* Strategie verwenden. Man unterscheidet zwischen *dekohärentem* und *kohärentem* Eavesdropping.

Dekohärentes Eavesdropping

Dekohärentes Eavesdropping vermisst alle passierenden Qubits $|\psi_i\rangle$ einzeln. Dies kann im Prinzip schon beim Protokollstand von Abschnitt 2.2 geschehen, da aus weiteren Informationen kein messtechnisches Nutzen gezogen werden kann.

Breidbartbasis. Eve muss nicht unbedingt mit Hilfe der Basen $\mathfrak{A}$ und $\mathfrak{B}$ messen, sondern kann sich auch einer Zwischenbasis $\mathfrak{C}$ bedienen, etwa

$$\begin{aligned} |0_{\mathfrak{C}}\rangle &= \frac{\sqrt{2}}{2}\left(|0_{\mathfrak{A}}\rangle + |0_{\mathfrak{B}}\rangle\right), \\ |1_{\mathfrak{C}}\rangle &= \frac{\sqrt{2}}{2}\left(|1_{\mathfrak{A}}\rangle + |1_{\mathfrak{B}}\rangle\right). \end{aligned}$$

Dies ist die *Breidbartbasis*. Es stellt sich aber heraus, dass dies auch eine QBER von 25 % liefert bei einem Information von aber nur ungefähr 39.9 %. Dieser Ansatz ist also ungünstiger als *intercept-resend*.

Symmetrischer Angriff. Eve verschränkt das Qubit $|\vec{m}\rangle$ mit einem Quantensystem des Hilbertraums $\mathcal{H}_{\text{Eve}}$ mittels unitärer Transformationen im Produktraum

$$\mathcal{H} \cong \mathbb{C}^2 \otimes \mathcal{H}_{\text{Eve}}.$$

Bezeichnet man die Anfangszustände als $|0\rangle \in \mathcal{H}_{\text{Eve}}$, $|\vec{m}\rangle \in \mathbb{C}^2$ und die unitäre Transformation als U, so muss man den verschränkten Zustand von Bob's Qubit quantenstatistisch mit der Dichtematrix

$$\begin{aligned} \rho_{\text{Bob}}(\vec{m}) &= \text{tr}_{\mathcal{H}_{\text{Eve}}} U\,|\vec{m},0\rangle\,\langle\vec{m},0|\,U^\dagger \\ &= (\mathbb{1}_{\mathbb{C}^2} + \eta\vec{m}\vec{\sigma})/2 \end{aligned}$$

beschreiben, wobei $\eta \in [0,1]$ eine Art „Schrumpfungsfaktor“ ist. Die Gleichung wird in [1] allgemein hergeleitet. Die Tatsache der Existenz einer Dichtematrix, die Bob's Qubit beschreibt, lässt dieses im Inneren der es visualisierenden Bloch-Kugel liegen. Dies ist durch den Faktor η gegeben. Die Transformation ist dabei symmetrisch insofern, als dass eine Kontraktion mit der Kugelmitte als Zentrum durchgeführt wird. Im Schnitt der Blochkugel

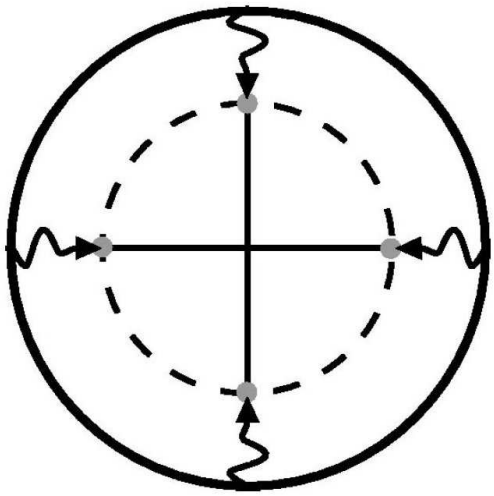

Abbildung 3: Symmetrischer Angriff. Das Qubit gelangt durch symmetrische Kontraktion ins Innere der Bloch-Kugel.

durch die Basisebene, die die polar bzw. äquatorial angeordneten Vektoren der Basen $\mathfrak{A}$ und $\mathfrak{B}$ definieren, ist dieser Vorgang in Abbildung 3 dargestellt. Man kann zeigen, dass dekohärentes Eavesdropping bis zu einer QBER von 15 % behandelt werden kann mit den vorgestellten einfachen Methoden. Abbildung 4 stellt die Gegebenheiten des dekohärenten Eavesdroppings zusammen.

Kohärentes Eavesdropping

Beim kohärenten Eavesdropping passiert folgendes:

- Eve verschränkt jedes Qubit $|\psi_i\rangle$ in einem Hilbertraum $\mathbb{C}^2 \otimes \mathcal{H}_{\mathrm{Eve},i}$ mit einem Zustand $|\phi_i\rangle \in \mathcal{H}_{\mathrm{Eve},i}$.
- Sie belässt i.a. den Produktraum $\bigotimes_i \mathcal{H}_{\mathrm{Eve},i}$ dann in seinem Zustand bis der gesamte *BB84*-Mechanismus von Alice und Bob durchlaufen wurde.
- Eve führt die Kryptoanalyse durch Messungen im Produktraum durch.

Kohärentes Eavesdropping lässt sich dementsprechend nur quanteninformationstheoretisch analysieren. Es lässt sich zeigen, dass hier QBERs von bis zu 11 % akzeptabel sind, um dem Produktraum jegliche nutzbare Information zu entziehen.

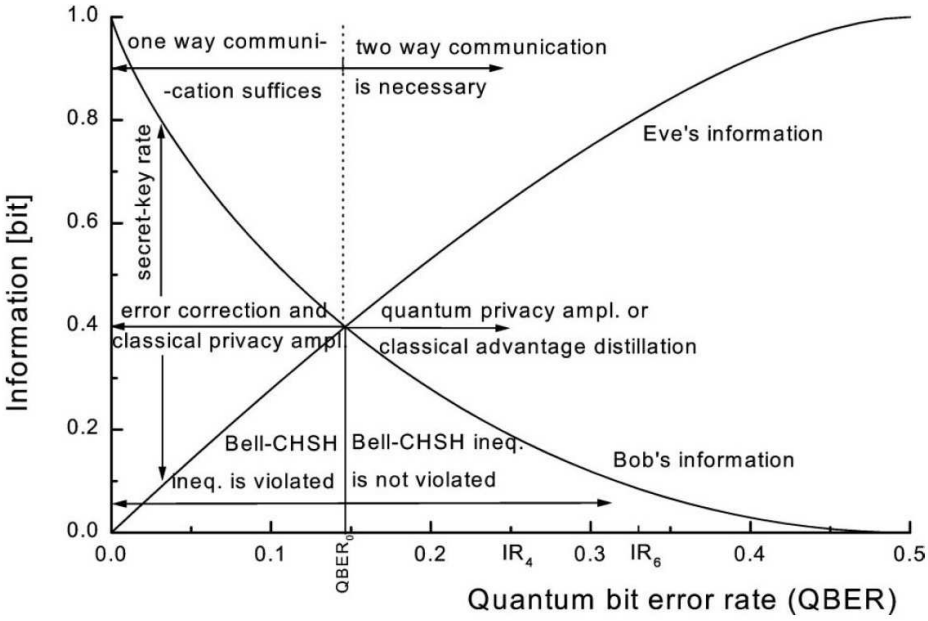

Abbildung 4: Dekohärentes Eavesdropping. Links des Schnittpunktes der Information von Bob und Eve befindet sich der mit den hier behandelten Verfahren zu bewältigende QBER-Bereich. Die rechte Seite kann in einigen Fällen mit komplizierteren Verfahren angegangen werden. Im Übrigen besteht ein interessanter Zusammenhang mit der Bellschen Ungleichung, auf den hier aber nicht weiter eingegangen wird. Eine allgemeine Behandlung des Zusammenhanges des Bell-Theorems und QC konnte zudem laut [2] noch nicht erreicht werden. Interessant ist in diesem Kontext auch, dass die QC nicht notwendigerweise – bzw. in *BB84* gar nicht – Gebrauch von Nichtlokalität macht.

Natürlich ist kohärentes Eavesdropping extrem schwierig zu realisieren, aber für den Sicherheitsbeweis muss man von einer perfekt ausgestatteten Eve ausgehen. Weitere Informationen zu diesem Thema liefert der Artikel [2].

3 EPR-Protokoll, Anwendung und Ausblick

Kurze Zusammenfassung *BB84*

Im ersten Teil des Vortrages wurde das quantenkryptographische Protokoll *BB84* ausführlich behandelt. In Kürze zusammengefasst gilt: Alice erzeugt zufällig mit einer aus zwei möglichen Basen Qubits der Werte 0 oder 1. Bob misst nun auch mit zufälliger Basis den Wert. Dann vergleichen sie die Basen und haben eine Fehlerrate von 25 %. In der letzten Phase erfolgt dann die *Schlüsseldestillierung* mittels *Fehlerkorrektur* und *Vertraulichkeitsverstärkung* (privacy amplification). Am Ende haben sie einen geheimen Zufallsschlüssel erzeugt.
Für die Quantenkryptographie gilt ganz allgemein, dass immer nur ein sicherer Schlüssel erzeugt wird. Der anschließende Datenaustausch findet über einen klassischen Kanal statt, wobei die Daten mit dem geheimen Schlüssel kodiert werden. Dieser Zusammenhang ist in Abbildung 2 verdeutlicht.
Im Folgenden Abschnitt werden wir kurz auf einige weitere Protokolle ausser *BB84* eingehen.

3.1 andere Protokolle

Two State Protocol, auch *B92*

Bei diesem Protokoll werden nur 2 statt 4 nicht-orthogonale Quantenzustände verwendet. Dadurch erhöht sich die Effizienz gegenüber *BB84*, jedoch werden Lauschangriffe von Eve leichter: In der Praxis könnte Eve gut zwischen den beiden Zuständen unterscheiden, wenn sie geringe Verluste auf Seiten der Signalstärke akzeptiert (falls Alice und Bob keine einzelnen Photonen zur Übertragung der Signale verwenden; '*photon number splitting attack*'). Da bisher keine perfekten Einzelphotonenquellen existieren, ist dieses Protokoll theoretisch sicher, aber praktisch nicht von Nutzen.

Six State Protocol

Hier verwendet Alice 6 anstatt 4 nicht-orthogonale Quantenzustände, codiert ihre Qubits also in einer von drei Basen. Dann ergibt sich eine Fehlerrate des *raw key* von 33 % gegenüber 25 % bei *BB84*. Das heisst also, dieses Protokoll

hat eine deutlich geringere Effizienz im Vergleich zu *BB84*, allerdings ist Sicherheit auch deutlich erhöht; Eve kann einfach viel weniger Informationen erlangen. Dadurch wird gegebenenfalls die geringere Effizienz gerechtfertigt.

Einstein-Podolsky-Rosen Protokoll

Dieses Protokoll wurde 1991 von Artur Ekert entwickelt, deswegen wird es teilweise auch als das *Ekert Protokoll* bezeichnet. Es benutzt verschränkte Zustände für die Schlüsselverteilung und ist daher von besonderem praktischen und historischen Interesse.
Entscheidender Unterschied zu *BB84* ist, dass Alice und Bob jeweils ein Qubit von einem zentralen Sender empfangen. Diese beiden Qubits sind verschränkt in einem der vier Zustände von *BB84* und Alice und Bob messen zufällig und unabhängig voneinander in einer der beiden Basen. Danach gibt es zwei Möglichkeiten zum Vergleich der Ergebnisse:

- Entweder verkündet der Sender öffentlich die Basen, in denen er die Qubits codiert hat und Alice und Bob behalten jeweils die Qubits, die sie in der richtigen Basis gemessen haben
- oder Alice und Bob vergleichen über einen klassischen Kanal (Telefon), ob sie in der gleichen Basis gemessen haben und behalten in diesem Fall das perfekt korrelierte Ergebnis.

Wenn der zentrale Sender vertrauenswürdig ist, erhalten sie analog zu *BB84* einen geheimen, gemeinsamen (und vorläufigen) Schlüssel ('*raw key*'), den sie mit den üblichen Methoden verbessern können zum '*sifted key*'.

Besonderheiten des EPR Protokolls

Falls Alice und Bob 3 anstatt 2 Basen benutzen, sinkt zwar die Wahrscheinlichkeit dafür, dass sie die gleiche Basis benutzen reduziert sich von 1/2 auf 2/9, allerdings sammeln sie gleichzeitig genug Daten, um die *Bell'sche Ungleichung* zu testen. Somit können sie überprüfen, ob der Sender tatsächlich 2 verschränkte Photonen, bzw. Qubits, ausgesendet. hat.
Ist dies nicht der Fall (*Bell's Ungleichung* also nicht verletzt), müssen sie im schlimmsten Fall davon ausgehen, dass ein Spion den Zustand geändert und dadurch die Verschränkung der Photonen zerstört hat.
Zwar ist die genaue Verbindung zwischen Sicherheit des *EPR Protokolls* und *Bell'scher Ungleichung* noch nicht vollständig bekannt und erklärt, allerdings ergeben sich doch faszinierende Zusammenhänge.
Genau hier liegt auch die Besonderheit dieses Protokolls: Die ursprünglich

philosophische Debatte um *EPR* wandelte sich mit der *Bell'schen Ungleichung* in eine Debatte der theoretischen Physik und nach den ersten experimentellen Untersuchungen der Jahre 1972 [4], 1976 [5] und 1982 [6] ist sie nun seit Artur Ekert Teil der angewandten Physik.

weitere

Zu den oben genannten Protokollen kommen noch solche, die auf kontinuierlichen Variablen beruhen. Dafür existieren diverse Möglichkeiten, beispielsweise die Benutzung kohärenter Zustände. In [2] finden sich dazu ausführliche Beschreibungen.

3.2 Technische Anwendung und experimenteller Status

Bisher sind wir davon ausgegangen, dass die Qubits zur Datenübertragung Photonen sind. Das ist die in Zukunft wahrscheinlichste Anwendung der *QC*, daher werden wir bei dieser Voraussetzung bleiben.

Der erste sichere Austausch eines Quantenschlüssels fand 1991 im Labor des IBM Forschungszentrums in Yorktown Heights statt. Benutzt wurden schwache Laserpulse, die eine Strecke von 32 cm überquerten. Schlüsselrate waren einige hundert Bits pro Sekunde. Gleichzeitig wurden mehrere Abhörattacken simuliert und gezeigt, das auch Fehler und Rauschen innerhalb gewisser Grenzen die Sicherheit nicht notwenigerweise verringern.

Seither wurden viele Techniken und Varianten entwickelt, mit denen *QC* betrieben werden kann. Eine grundlegende Unterscheidung ist bezüglich der benutzten Wellenlänge möglich: entweder 800 nm, wofür effiziente Photonendetektoren kommerziell verfügbar sind, oder 1300 bzw 1550 nm.

- In der aktuellen Telekommunikation werden Glasfasern verwendet, die sich einzig für Lichtwellenlängen um 1300 oder 1550 nm eignen. Will man *QC* über diese Fasern betreiben, muss man vorher neue, effiziente Detektoren entwickeln, die nicht auf Siliciumhalbleitern basieren. Das ist kosten- und zeitaufwändig und stellt ein großes Problem dar.

- Bei Wellenlängen um 800 nm kann man zwar auf kostengünstige Laserdioden und Detektoren zurückgreifen, aber nicht die gängigen Glasfasern benutzen. Die Entwicklung von neuen Glasfasern wäre zwar ein Ausweg, aber die müsste man dann ja überall verlegen, etc. Deswegen betreibt man also *QC* mit Licht um 800 nm immer bei direktem Sichtkontakt, d.h. durch die Luft.

Später werden wir die *Free Space QC* in einem gesonderten Abschnitt kurz vorstellen.

Faint Laser Pulses

Hauptsächlich wird *QC* heute mit schwachen Laserpulsen betrieben. Schwach bedeutet in diesem Fall, dass die mittlere Photonanzahl μ pro Puls sehr klein gemacht wird. Dies ist sehr gut möglich mit der Technologie, d.h. Halbleiterlaser und entsprechend kalibrierte Dämpfer, die schon heute zur kommerziellen Verfügung steht. Damit hat man eine sehr einfache Möglichkeit, *Einzelphotonen Fock Zustände* durch kohärente Zustände zu approximieren (herzustellen).
Die Wahrscheinlichkeit, n Photonen in einem dieser kohärenten Zustände zu finden, ist dann Poisson verteilt:

$$P(n, \mu) = \frac{\mu^n}{n!} e - \mu$$

Die Wahrscheinlichkeit $P(n > 1, \mu)$ für $n > 1$ kann mittels Verkleinerung von μ dann sehr klein gemacht werden und schon hat man sein Ziel erreicht: Mit hoher Wahrscheinlichkeit befindet sich in einem nicht-leeren Puls genau ein Photon.
Das Problem, das sich ergibt, ist dann aber, dass mit kleiner werdendem μ mehr und mehr Pulse leer sind. Ansich könnte man dies sehr gut mit hoch modulierten Lasern im GHz-Bereich kompensieren, das eigentliche Hinderniss stellen dann aber die *dark counts* der Detektoren dar. Ist ein gemessenes Photon tatsächlich angekommen, oder hatte der Detektor einen *dark count*? Vor allem für steigende Modulationsraten des Lasers erhöht sich die Anzahl der *dark counts*.
Ausweg in diesem Fall bietet ein Kompromiss zwischen möglichst kleinem μ und möglichst hoher Modulationsrate. Es stellt sich also heraus, dass ein optimales μ existiert, abhängig vom benutzten Kanal (Leitungsverluste), Laser und Detektor.
Dieser Bereich der angewandten *QC* ist Objekt intensiver Forschung, zur Zeit sind bereits die ersten Module zum alltäglichen Einsatz von *QC* kommerziell erhältlich. Derzeit liegt ihre Größe ungefähr bei der eines Schuhkartons.

verschränkte Photonenpaare (*EPR*)

Aufbauten, die verschränkte Photonenpaare verwenden, sind weitaus komplexer als solche, die mit schwachen Laserpulsen arbeiten. Ihr Vorteil liegt allerdings darin, dass die Messung eines Photons die Anwesenheit des anderen erzwingt. Dadurch lassen sich leere Pulse sofort erkennen, falls der

Detektor nur ein Photon misst. Das Problem der *dark counts* (s.o.) macht also viel weniger Schwierigkeiten, wenn man nur davon ausgeht, dass immer beide Photonen gemessen werden.
An dieser Stelle ist zu wenig Platz, um in die genauen Details zu gehen, aber prinzipiell gibt es zwei Möglichkeiten für die Realisation des *EPR Protokolls*: Polarisationsverschränkung und Energie-Zeit-Verschränkung. Ausführliche Beschreibungen finden sich dazu in [2].

Quantenrepeater

Mit Glasfasern hat man das Problem der Übertragung über große Entfernungen hinweg. Zwar haben Verluste entlang der Leitung keinen Einfluß auf die Sicherheit, allerdings reduzieren sie die Anzahl der übertragenen Photonen. Ab einer Verlustrate von 11 % kann dann trotz Fehlerkorrektur kein korrekter, geheimer Schlüssel mehr erzeugt werden.
Das Problem liegt in der Kombination von Leitungsverlusten und Detektorrauschen. Die Verluste allein sind kein Problem mit perfekten Detektoren, aber irgendwann sinkt die Signalstärke so stark, dass das Signal praktisch nicht mehr vom realen Detektorrauschen zu unterscheiden ist. Die heutige Machbarkeitsgrenze liegt noch unter 100 Kilometern.
Das *No-Cloning Theorem* verbietet natürlich eine einfache Verstärkung des Signals irgendwo im Leiter. Aber auch ohne die quantenmechanischen Gesetze zu verletzen lässt sich eine höhere Reichweite erzielen: Basierend auf *verschränkten Zuständen* und der *Quantenteleportation* funktioniert der *Quantenrepeater*.
Ausgangspunkt ist die Erzeugung eines verschränkten Photonenpaares, im Folgenden 'A' und 'B'. Diese beiden Photonen werden nun an die verschiedenen Enden der Leitung gesendet und dort gespeichert. Die Enden der Leitung sind in diesem Fall ein bestimmter Detektor in der Leitung, genannt *entanglement swapper*, und Bob. Ein irgendwie codiertes Qubit wird nun von Alice in Richtung Bob gesendet und trifft vorher auf den *entanglement swapper*. An dem Qubit wird eine Messung durchgeführt derart, dass dessen Zustand auf das dort gespeicherte, verschränkte Photon, z.B. 'A', übertragen (*entanglement swapping*)wird. Dabei werden keine Informationen über den gemessenen Zustand bekannt. Die Wellenfunktion von 'A' kollabiert also in den Zustand des Qubits, wodurch effektiv das Qubit durch die Leitung teleportiert wird, denn 'B' wird wegen der Verschränkung genauso kollabieren.
Diese Darstellung eines *Quantenrepeaters* ist stark vereinfacht, lässt sich theoretisch allerdings auf eine beliebig große Anzahl n von Knoten verallgemeinern.
Es ist noch eine Menge Entwicklungsarbeit notwendig, bevor dieses Konzept

breitflchige Anwendung finden kann - eine offensichtliche Schwierigkeit ist die Speicherung von Photonen - aber wenn einmal die nötige Technologie zur Verfügung steht, wird das bedeuten, dass *QC* nicht mehr auf relativ geringe Distanzen beschränkt ist. Hintereinander gereiht werden die *Quantenrepeater* nahezu verlustfreie Verbindungen über beliebige Strecken ermöglichen.

Free Space QC

Die Atmosphäre transmittiert Photonen der Wellenlänge 800 bis 850 nm sehr gut. Ausserdem sind effiziente und rauscharme Si-Avalanchedioden zur Einzelphotondetektion sowie Laserdioden in diesem Wellenlängenbereich sehr kostengünstig. Für jede Polarisationsrichtung kann man dann einfach verschieden ausgerichtete Dioden benutzen. Insgesamt sind dies alles Vorteile, die den Schlüsselaustausch bei bestehender Sichtverbindung mittels Teleskopen und optischem Richtfunk wettbewerbsfähig machen.
Ein erfolgreiches Experiment wurde zwischen Zugspitze und der westlichen Karwendelspitze in den Alpen durchgeführt. Die Entfernung betrug 23 km und die Übertragungsrate lag bei etwa 1000 bit/s. Weltweit arbeiten diverse Gruppen am quantenmechanischen Schlüsselaustausch durch die Luft, daher gibt es eine Vielzahl von Experimenten, die unter verschiedenen Bedingung erfolgreich durchgeführt wurden. Die bisher möglichen Pulsraten liegen mit hochintegrierter Elektronik sogar schon bei 125 MHz.
Technologisch hat man das Problem, die Lichtpulse trotz Luftturbulenzen richtig und punktgenau zu fokussieren, dies kann man allerdings durch die Benutzung adaptiver Optiken kompensieren, d.h. durch eine Rückkopplung wird das Signal, das Alice sendet, ständig neu ausgerichtet.
Die Wichtigkeit der *Free Space QC* sollte man nicht unterschätzen. Zwar ist das heutige Anwendungsgebiet beschränkt auf Distanzen einiger 10 km, aber auf lange Sicht ergibt sich eine realistische Möglichkeit, in die Reichweite von erdnahen Satelliten (500 - 1000 km) vorzudringen. Dann kann mit zwei verschiedenen Bodenstationen (nennen wir sie Alice und Bob) jeweils ein Einzelschlüssel ausgetauscht werden. Aus diesen Schlüsseln lässt sich ein geheimer Schlüssel zwischen Alice und Bob ermitteln, wodurch praktisch alle Entfernungsschranken entfallen. Solange also keine *Quantenrepeater* zur Überwindung mehrerer Dutzend Kilometer mit Glasfasersystemen zur Verfügung stehen, bieten *Free Space Systeme* eine echte Alternative.
Eine weitere Besonderheit der *Free Space QC* ist, dass nicht nur Alice und Bob den Schlüssel kennen, sondern auch der Betreiber des Satelliten. Dieser Punkt könnte sich als weiterer Antrieb herausstellen, denn jede Regierung kontrolliert gerne die Kommunikation, was nicht mehr möglich ist, wenn *QC* einmal über Glasfaser betrieben wird.

3.3 Ausblick

Ganz generell steht nicht die Frage im Raum, ob die QC kommerzielle Anwendung findet, sondern wann. Das Problem, dass heutige Kryptographie auf der Multiplikation von Primzahlen beruht, besteht in der QC nicht. Wenn übermorgen ein Algorithmus zur Primfaktorzerlegung vom Himmel fällt, ergäben sich einige ziemlich große Probleme für Banken, Geheimdienste und alle privaten Anwender.
Zwar kann man sich nicht darauf verlassen, dass die Sicherheit der QC allein auf den Prinzipien der Quantenmechanik beruht (vgl. perfekte Einphotonenquelle $\leftrightarrow$ technische Machbarkeit), aber durch hinreichend sorgfältige technische Umsetzung ist möglich, dass bald jedermann sichere Kommunikation mit den Mitteln der Physik betreibt.

Literatur

[1] Fuchs, C. A., N. Gisin, R.B. Griffiths, C.-S. Niu, and A. Peres: 'Optimal eavesdropping in quantum cryptography. I: Information bound and optimal strategy', Phys. Rev. A 56, 1163-1172 (1997)

[2] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden: 'Quantum cryptography', Rev. Mod. Phys. 74, 145 (2002)

[3] D. Bruß, H. Weinfurter: 'Geheime Botschaften aus Licht', Physik Journal Nr. 11, 57 (2005)

[4] S.J. Freedmann, J.F. Clauser: 'Experimental test of local hidden variable theories', Phys. Rev. Lett. 28, 938 (1972)

[5] E.S Fry, R.C. Thompson: 'Experimental test of local hidden variable theories', Phys. Rev. Lett. 37, 465 (1976)

[6] A. Aspect, J. Dalibard, G. Roger: 'Experimental test of Bell's inequalities using timevarying analyzers', Phys. Rev. Lett. 49, 1804 (1982)

[7] `http://www.wikipedia.org`