

Seminar Quantum Computation

Quantum Key Generation

Oliver Huras
ohuras@informatik.tu-cottbus.de

09.01.2004

Inhalt:

1. Mehrparteien-Schlüssel-Erzeugung (-Verteilung)
(Multiparty key generation)
2. Verschränkungs-basierte QKG-Protokolle
(Entanglement-based QKG protocols)
3. Bedingungslose Sicherheit der QKG
(Unconditional security of QKG)
4. Experimentelle Quanten-Kryptographie
(Experimental quantum cryptography)

Mehrparteien-Schlüssel-Erzeugung (-Verteilung)

Es gibt viele Anwendungen, wo verschiedene Kommunikationspartner einen geheimen Schlüssel benötigen. Dabei ist es wichtig, den Fall genauer zu beleuchten, wo eine Partei als nicht vertrauenswürdig angesehen werden kann. Folgende Ausführungen betrachten dieses.

Alice, Bob und Charles wollen einen gemeinsamen geheimen Schlüssel generieren (verteilen). Alice weiß, dass sie einem der beiden anderen nicht vertrauen kann, d.h. es gibt einen Lauscher. Sie hat allerdings keine Erkenntnis darüber, wer es ist. Zusätzlich ist ihr bekannt, wenn die beiden zusammenarbeiten, kann der ehrliche Kommunikationspartner den Lauscher dazu bringen, sich anständig zu benehmen.

Alice, Bob und Charles teilen 3 Teilchen und messen diese hinsichtlich einer zufällig gewählten Basis (entweder der Standardbasis oder der dualen Basis oder der zirkulären Basis). Dann werden die Ergebnisse der Messungen veröffentlicht. Wichtig hierbei ist, dass zuerst Bob und Charles ihre Basen für die Messung zu Alice schicken. Dann sendet Alice ihre zu den anderen beiden. Das verhindert, dass weder Bob noch Charles (derjenige, der nicht vertrauenswürdig ist) seine Wahl der Basen zurückhält bis er herausbekommen hat, welche Basen von Alice und dem anderen gewählt wurden.

Verschrankungs-basierte QKG-Protokolle

Im Jahre 1991 entdeckte A. Ekert einen neuen Typ von QKG-Protokollen, welche nicht auf Heisenbergs Unschärferelation basieren, sondern auf der Vollständigkeit der Quanten-Mechanik. Das bedeutet, ein Lauscher wird als „Einschub eines Elements der physikalischen Realität in die Messung“ [1] angesehen.

Allgemeiner Entwurf eines verschrankungs-basierten QKG-Protokolls:

1. Vorbereitungsphase

Alice wählt 3 Vektoren $\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3$ in H_2 .

Bob wählt 3 Vektoren $\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3$ in H_2 .

⇒ Wahl sollte so ausfallen, dass mindestens 1 Vektor bei beiden gleich ist

Welche Vektoren stehen zur Verfügung?

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$|0'\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}, |1'\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}$$

$$|0''\rangle = \begin{pmatrix} 1 \\ \frac{1}{\sqrt{2}} \\ i \\ \frac{1}{\sqrt{2}} \end{pmatrix}, |1''\rangle = \begin{pmatrix} 1 \\ \frac{1}{\sqrt{2}} \\ -i \\ -\frac{1}{\sqrt{2}} \end{pmatrix}$$

2. Schlüsselgenerierungsphase

Eine Quelle produziert eine Sequenz von maximal verschränkten Zuständen (oder maximal verschränkte Photonenpaare) und sendet den einen Teil jedes Paares zu Alice und den anderen zu Bob.

Beide messen ihre Teilchen hinsichtlich eines ihrer zufällig gewählten Vektoren und machen diese Sequenz von Vektoren öffentlich. Der gemeinsame Schlüssel ergibt sich aus der Sequenz der Resultate der Messung, die bei Alice und Bob mit dem gleichen Vektor gemessen wurden.

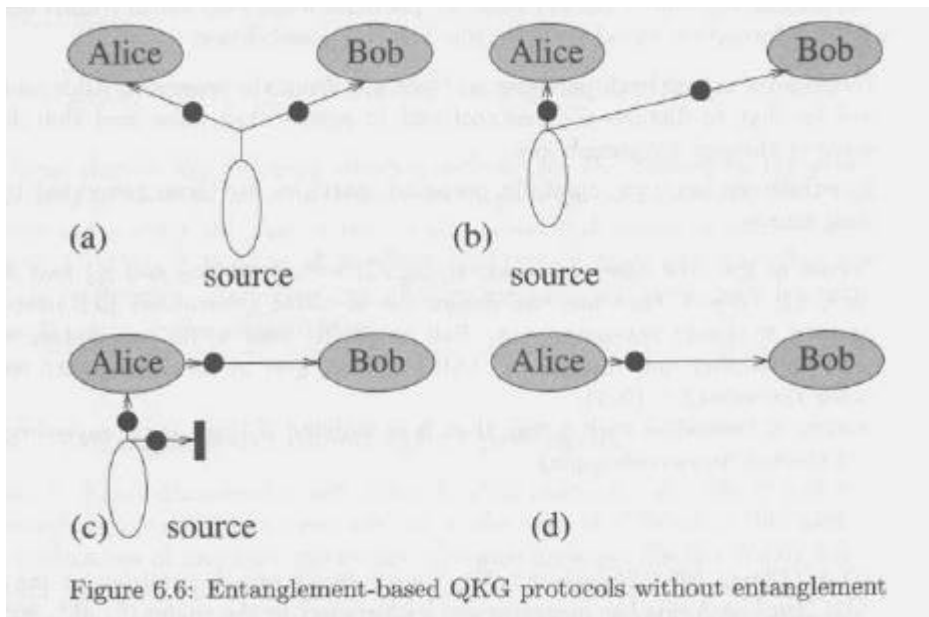
3. Test auf Lauscher

Eve hat keine Möglichkeit, Informationen von den Teilchen über den Schlüssel zu erhalten, während diese in Bewegung sind (von der Quelle zu Alice und/oder Bob), weil es keine verschlüsselte Information gibt. Sie hat also nur 2 Möglichkeiten:

- (a) Sie misst die Teilchen auf dem Weg von der Quelle zu Alice und Bob, um sie damit zu zerstören. Als Folge hätten die beiden keine gemeinsamen Schlüssel.
- (b) Sie ersetzt den Quellstrom durch ihren eigenen Teilchenstrom. Dieser muss aber gut vorbereitet sein.

Wenn die Vektoren $\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3$ und $\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3$ gut gewählt wurden, kann mittels der sogenannten *Bell inequality* ein Lauschen erkannt werden.

Verschränkungs-Protokolle sind nicht sehr verschieden von BB84- und B92-Protokollen. Bennett, Brassard und Mermin haben 1992 gezeigt, dass eine vereinfachte Version eines Verschränkungs-Protokolls äquivalent gegenüber BB84 ist. Hierbei wird zufällig 0° oder 90° für die Messung gewählt. Zusätzlich wurde durch Barnett und Phoenix 1995 gezeigt, dass ein Protokoll mit nur einem Teilchen (Partikel) einen äquivalenten Sicherheits-Level wie ein Verschränkungs-Protokoll hat.



entnommen: [2]

- Figure 6.6 (a) Die Quelle liegt weder in der Umgebung von Bob, noch von Alice. Er sendet ein Photon pro Paar zu Alice und das andere zu Bob. Beide Kommunikationspartner messen ihren Strom.
- 6.6 (b) Die Quelle liegt in der Umgebung von Alice.
- 6.6 (c) Das zweite Teilchen an Bob wird nicht von der Quelle geschickt. Alice macht nach ihrer Messung eine Kopie des dem Teilchen entsprechenden Zustands, das an Bob geschickt wird.
- 6.6 (d) Tatsächlich benötigt Alice gar keine verschränkten Teilchen. Sie wählt zufällig einen der 6 möglichen Zustände, in dem Bobs Original-Teilchen sein könnte und schickt das Teilchen in diesem Zustand zu Bob.

Bedingungslose Sicherheit der QKG

Man betrachtet hierbei 2 Sicherheitskriterien:

Privat-Kriterium (**privacy criterion**) und Sicherheit-gegen-Einmischungs-Kriterium (**security against tampering criterion**).

Letzteres bedeutet, der Angreifer kann Alice und Bob nicht glauben machen, dass sie einen sicheren Schlüssel haben, wenn er unsicher ist. Um zu entscheiden, ob ein Schlüssel sicher ist oder nicht, führen Alice und Bob einen Test durch.

Ersteres bedeutet, der Angreifer erhält nur unbedeutende Informationen über den Schlüssel. Die Grundidee hierbei ist, wie immer Eves Attacke aussieht, die Information i , die Eve erhält, führt entweder dazu, dass der Test fehlschlägt oder i wertlos ist.

Verschiedene andere Sicherheitskriterien wurden untersucht. Jedoch sind die beiden erwähnten stark genug, allen bekannten Attacken-Typen stand zu halten.

Weiterhin wurde gezeigt, dass das Protokoll BB84 sicher und geschützt ist gegen alle Angriffe, die ein Lauscher quanten-mechanisch anwenden kann. Das bedeutet **bedingungslose Sicherheit**. Die Sicherheit bleibt auch bei mangelhaften Übertragungskanälen und Detektoren bestehen; wichtig ist aber eine fehlerlose Teilchen-Quelle.

Experimentelle Quanten-Kryptographie

Die erste experimentelle Übertragung von Quanten-Bits über Photonen wurde 1989 verwirklicht. Realisiert wurde es in einer 32 cm langen Röhre. Marand und Townsend berichteten 1995 von einer Übertragung über 30 km in optischen Fasern (nur in einem Raum). Im gleichen Jahr gelang Muller, Zbinden und Gisin eine Übermittlung mittels optischer Kabel unter dem Genfer See über eine Entfernung von 22,7 km.

Welches Übertragungsmedium ist günstig? Photonen scheinen das beste Medium zu sein, um QuBits zu übertragen. Sie sind relativ leicht herzustellen und mit bestimmten Wellenlängen können sie sicher über bereits bestehende optische Fasern gesendet werden. Photonen mit einer Wellenlänge von $1,3\mu\text{m}$ sind gut geeignet, um QKG in lokalen Netzen zu verwirklichen, da sie sich bis zu 10 km in optischen Fasern bewegen können, bis die Hälfte der Photonen absorbiert wird.

Auch für QKG-Protokolle wurde eine in der Praxis sinnvoll einsetzbare Technik entwickelt (Bennett, 1992). Hierbei wird ein Mach-Zehnder-Interferometer benutzt.

Um dem Fortschritt von experimenteller zu praktischer Quanten-Kryptographie keinen Abbruch zu leisten, sind Forschungen in den beiden Gebieten **Zuverlässigkeit** und **Übertragungsrates** unumgänglich. Die Wettbewerbsfähigkeit der Quanten-Kryptographie als eine sichere Datenübertragung kann aber nur dann gewährleistet sein, wenn sie auch in Mehrbenutzer-Quanten-Netzwerken funktioniert.

Literaturverzeichnis

- [1] Ekert, A. K.: *Quantum cryptography based on Bell's theorem*, Physical Review Letters, vol. 67, pp 661-663, 1991.
- [2] Gruska J.: *Quantum Computation*, McGraw-Hill Publishing Company, 1999.