Zur Idee der Quantenkryptographie

Beatrix C. Hiesmayr[1]

Unterlagen zum Workshop "Quantenkryptographie und Quantencomputer"
im Rahmen der 58. Fortbildungswoche Physik/Chemie
Institut für Theoretische Physik der Universität Wien, 25. 2. 2004

1 Zur Idee der Quantenkryptographie

Kryptographie ist eine beeindruckende Art der Kommunikation und wurde nachweislich schon 400 Jahre vor Christi Geburt verwendet. Im Jahre 1949 veröffentlichte C. Shannon den ersten Artikel zu diesem Thema und damit wurde Kryptographie ein Teil der Mathematik und der Informationstheorie. Kurz zusammengefasst könnte man es so definieren, Kryptographie ist ein mathematisches System zum Transformieren von Informationen, so dass die übertragene Information für einen Dritten unverständlich und dadurch sinnlos ist. Allerdings ist der Prozess, der nötig ist, um die Information zu verschlüsseln, immer ein physikalischer Vorgang. D.h. man kann die mathematische Struktur von den zugrunde liegenden physikalischen Gesetzen beim Verschlüsselungsprozess nicht trennen. D. Deutsch war einer der ersten, der bemerkte, dass die Quantenphysik, die wie keine andere Theorie unserer Alltagserfahrung so stark widerspricht, unsere Möglichkeiten des Verschlüsselungsprozesses nicht nur erweitert, sondern dass erstmals eine absolut abhörsichere Kommunikation möglich sein wird, wie es mit klassischer Kryptographie nie möglich sein kann.
Gewöhnlicherweise erfolgt die Entschlüsselung einer Nachricht zwischen zwei verschiedenen Personen, die wir im Folgenden Alice und Bob nennen werden, über einen gemeinsamen sicheren Schlüssel (secret key). Solange man den key nicht besitzt, ist es unmöglich oder mit sehr viel Aufwand verbunden die Nachricht zu entschlüsseln. Im Prinzip ist es immer möglich, dass ein Dritter, der im Folgenden Eve genannt wird, bei der Schlüsselvergabe/-erzeugung unbemerkt an diesen herankommt. Alice und Bob können nie sicher sein, dass ihr Schlüssel nicht kopiert wurde. Dieses große Schlupfloch (loophole) der klassischen Kryptographie kann durch die Erzeugung des Schlüssels über Quantensysteme umgangen werden.
In diesem Workshop werden wir zwei einfache, aber effektive Protokolle kennenlernen, um einen secret key zu erzeugen, die uns einerseits die gewaltigen Vorzüge gegenüber der klassischen Erzeugung eines secret keys aufzeigen werden, andererseits wird der Vergleich beider Protokolle uns über das grundlegende Prinzip und die

[1]hiesmayr@ap.univie.ac.at

Sicherheit dieser aufklären. Damit sollten wir uns das Basiswissen der neuen Technologie, der Quantenkryptographie, erarbeitet haben, die schon in naher Zukunft eingesetzt werden wird.

2 Das BB84 Protokoll

Für dieses Protokoll, das C. H. Bennett und G. Brassard 1984 entwickelten, muss Alice einzelne Photonen zu Bob schicken. Sie präpariert diese ganz zufällig in vier möglichen Polarisationszuständen $|0°\rangle, |45°\rangle, |90°\rangle, |135°\rangle$. Bob analysiert die zu ihm gesendeten Photonen mit einem Zwei-Kanal-Analysator, welchen er zufällig zwischen 0° und 45° Basis variiert und daher das Photon entweder im oberen Detektor " + " —das Photon ist im Zustand $|0°\rangle$ oder $|45°\rangle$, je nach eingestellter Basis— oder im unteren Detektor " − " —das Photon ist im Zustand $|90°\rangle$ oder $|135°\rangle$— detektiert. Nachdem eine gewisse Anzahl an Photonen an Bob gesendet wurden, diskutieren Alice und Bob ganz öffentlich darüber, welche Photonen Bob auch wirklich erreicht haben. Bob klärt Alice auch darüber auf, welche Messbasis er jeweils verwendet hat, 0° oder 45°. Alice dagegen, gibt Bob darüber Bescheid, wann beide die gleiche Basis verwendet haben. In diesem Fall sind die Messresultate im Idealfall identisch und können zur Produktion des Keys verwendet werden. Dabei ordnen Alice und Bob dem " + " Resultat eine "1" zu und dem " − " Resultat eine "0" zu. Das ergibt im idealen Fall für beide einen identischen Key (sifted key), eine Abfolge von "1"en und "0"en (siehe auch Tabelle 1).

Qubits	1	2	3	4	5	6	...
Alice's Basis	45°	0°	45°	45°	0°	0°	...
Alice's Zustand	+	−	−	−	−	+	...
Bob's Basis	45°	0°	0°	45°	0°	45°	...
Bob's Messung	+	−		−		−	...
Sifted Key	1	0		0			...

Table 1: Das Schema für das BB84 Protokoll.

Sobald Alice und Bob den Key erzeugt haben, können sie zum Beispiel über das einfache, aber effektive Verschlüsselungsschema von Vernam (1926) kommunizieren (siehe Tabelle 2). Dabei muss der Key völlig zufällig erzeugt worden sein und mindestens die Länge der Nachricht haben. Wenn jedes Bit des Keys nur einmal verwendet wird, dann ist es nicht möglich über irgendwelche statistischen oder numerischen Methoden die Nachricht zu dechiffrieren.

Alice:	
Nachricht	01001101
Key	11010101
Verschlüsselte Nachricht	10011000
Bob:	
Verschlüsselte Nachricht	10011000
Key	11010101
Entschlüsselte Nachricht	01001101

Table 2: Hier ist die einfache Funktionsweise eines Key demonstriert. Dabei wird jedes Bit der Nachricht bitweise durch eine Exklusive-Oder Transformation (XOR) verschlüsselt ($00 \rightarrow 0, 01 \rightarrow 1, 10 \rightarrow 1, 11 \rightarrow 0$). Wobei die verschlüsselten Nachrichten durchwegs über einen offenen Kanal an Alice geschickt werden können.

Fragen, Aufgaben, Anregungen:

- Wie groß sind die Wahrscheinlichkeiten für alle Messresultate von Bob, wenn Alice ihr Photon im Zustand $|45°\rangle$ präpariert?
- Wieviele Daten werden verworfen, bzw. können für die Erzeugung des Keys verwendet werden?
- Wie könnte eine Attacke von der "bösen" Eve ausschauen? Könnte sie das von Alice gesendete Photon einfach kopieren und das Original oder die Kopie an Bob weitersenden?

  Hinweis: *Non-cloning theorem*
  Ein Kopierer sollte den Zustand $|0\rangle$ wohl in $|0\rangle|0\rangle$ übergehen lassen und ebenso für $|1\rangle$. Was bedeutet das jedoch für eine Superposition $|0\rangle + |1\rangle$, ergibt das das gewünschte Resultat?
- Welche anderen möglichen Attacken stehen Eve zur Verfügung? Und wie erkennen Bob und Alice eine mögliche Attacke?
- Argumentiere, warum das quantenmechanische Prinzip, dass jede Messung einen Quantenzustand stört, die absolute Sicherheit der Quantenkryptographie möglich macht.

3 Ekert's Protokoll

Ein sehr beeindruckende Art der Erzeugung eines Schlüssels mit Hilfe eines Quantensystems wurde von A. Ekert[2] 1991 vorgeschlagen. Dabei teilen sich Alice und Bob verschränkte Photonenpaare. Der Zustand der Photon–Paare kann in folgender Weise beschrieben werden

$$|\psi^-\rangle \;=\; \frac{1}{\sqrt{2}}\Big\{|H\rangle_A \otimes |V\rangle_B - |V\rangle_A \otimes |H\rangle_B\Big\}\,, \tag{1}$$

wobei sich der erste Ket auf das Photon, das Alice zur Verfügung hat, und sich der zweite Ket auf das Photon, das Bob zur Verfügung hat, bezieht. Findet Alice ein horizontal polarisiertes Photon, $|H\rangle$, dann findet Bob immer, wenn er in der gleichen Basis misst, ein vertikal polarisiertes Photon, $|V\rangle$. Dieser Zustand, da er total antisymmetrisch ist, nimmt die gleiche formale Struktur für jede beliebige Basis ein, so kann der Zustand in der 45° Basis folgenderweise angeschrieben werden

$$|\psi^-\rangle \;=\; \frac{1}{\sqrt{2}}\Big\{|+45^\circ\rangle_A \otimes |-45^\circ\rangle_B - |-45^\circ\rangle_A \otimes |+45^\circ\rangle_B\Big\}\,, \tag{2}$$

wie einfach über die Beziehung zwischen der 0° Basis (H, V) zur 45° Basis $(+45^\circ, -45^\circ)$ nachgerechnet werden kann (siehe Handout "Einführung"). Der Zustand zeigt wieder die oben beschriebene starke EPR-Korrelation (Einstein, Podolsky, Rosen): Findet Alice den Zustand $|-45^\circ\rangle$, dann falls Bob in der gleichen Basis misst, findet er sein Photon im Zustand $|+45^\circ\rangle$.
Für das Ekert Protokoll wählen Alice und Bob jeweils für ihr Photon zufällig zwischen mindestens drei verschiedenen Richtungen. Dabei werden gleich gewählte Richtungen wieder verwendet, um den Key zu erzeugen, da hierbei Bob immer das Gegenteil von Alice misst. Einer der Zwei braucht also nur den Schlüssel zu invertieren, so dass beide den identischen Schlüssel besitzen. Die restlichen Messresultate werden jedoch nicht, wie beim vorigen Protokoll, verworfen, sondern zum Testen der Sicherheit (security) benützt. Dies erfolgt über den Test einer Bell Ungleichung (siehe Anhang 4).

[2]Hier wird zwar Ekert's Protokoll verwendet, jedoch zum Testen der Sicherheit wird nicht die CHSH-inequality, sondern eine einfachere Version einer Bell Ungleichung verwendet, die Wigner Ungleichung. Diese wurde ebenfalls dem Experiment der Zeilinger Gruppe zugrunde gelegt.

Fragen, Aufgaben, Anregungen:

- Einstein argumentierte, dass die Quantentheorie nicht komplett sein kann; es müssen verborgene Parameter existieren. Ekert's Protokoll testet die Sicherheit der Leitung über eine Bell Ungleichung, also ob verborgene Parameter existieren. Warum ist die Verletzung der Bell Ungleichung ein Test für die Sicherheit?

- Die "beam splitter" Attacke beruht auf der Tatsache, dass es keine idealen Ein-Photon Quellen gibt. Und dadurch kann nicht ausgeschlossen werden, dass zwei Photonen gleichzeitig erzeugt werden und dieses zweite Photon durch einen "beam splitter" von Eve abgezweigt werden kann. Inwieweit wurde diese Attacke bei dem Experiment der Zeilingergruppe umgangen?

4 Anhang

- **Was ist eine Bell Ungleichung?**

  Nehmen wir an, dass Alice zwischen den zwei Achsen, a und b ($a, ...$ gibt den Winkel zu einer beliebig davor definierten Achse an und beschreibt damit die gewählte Basis), mit den möglichen Messergebnissen $+1$ und -1 wählen kann. Bob hingegen wählt zwischen den zwei Achsen, b und c, aus. Wenn die Werte für die verschiedenen Achsen vorbestimmt sind, dann erhält man für die Wahrscheinlichkeit, dass Alice bei der Achseneinstellung a ein Ereignis im oberen Detektor $+1$ findet und Bob bei der Achseneinstellung b ebenfalls im oberen Detektor ein Photon findet, die Summe der folgenden Häufigkeiten (siehe Tabelle 3)

$$p_{++}(a,b) = \frac{N_6 + N_7}{\sum_i N_i} \ . \tag{3}$$

  Analog dazu berechnen sich die Wahrscheinlichkeiten

$$\begin{aligned} p_{++}(a,c) &= \frac{N_2 + N_6}{\sum_i N_i} \ , \\ p_{++}(b,c) &= \frac{N_2 + N_4}{\sum_i N_i} \ . \end{aligned} \tag{4}$$

  Da alle N's positiv sind gilt klarerweise die folgende Ungleichung

$$N_2 + N_6 \ \leq \ N_2 + N_4 + N_6 + N_7 \ , \tag{5}$$

  woraus mit Gl.(3) und Gl.(4) die Wigner Ungleichung folgt

$$p_{++}(a,c) \ \leq \ p_{++}(b,c) + p_{++}(a,b) \ . \tag{6}$$

Table 3: Acht unabhängige Ergebnisse mit der entsprechenden Häufigkeit N_i.

Häufigkeit	Alice	Bob
	(a, b, c)	(a, b, c)
N_1	$(+, +, +)$	$(-, -, -)$
N_2	$(+, +, -)$	$(-, -, +)$
N_3	$(-, +, +)$	$(+, -, -)$
N_4	$(-, +, -)$	$(+, -, +)$
N_5	$(+, -, +)$	$(-, +, -)$
N_6	$(+, -, -)$	$(-, +, +)$
N_7	$(-, -, +)$	$(+, +, -)$
N_8	$(-, -, -)$	$(+, +, +)$

D.h. alle Theorien, die auf lokal realistischen Argumenten beruhen, müssen die obige Bell Ungleichung erfüllen.

- **Welches Ergebnis liefert die Quantenmechanik?**

  Die quantenmechanische Wahrscheinlichkeit für die Achsenwahl α von Alice und für die Achsenwahl β für Bob ist gegeben durch

$$P_{++}^{QM}(\alpha, \beta) = \frac{1}{2}\sin^2(\alpha - \beta) \tag{7}$$

  und damit berechnet sich die Wigner Ungleichung mit $\alpha = -30°, \beta = 0°$ and $\gamma = 30°$ zu

$$\underbrace{p_{++}^{QM}(-30°, 30°)}_{\frac{3}{8}} \leq \underbrace{p_{++}^{QM}(0°, 30°)}_{\frac{1}{8}} + \underbrace{p_{++}^{QM}(-30°, 0°)}_{\frac{1}{8}} . \tag{8}$$

  Und dies ist offensichtlich ein Widerspruch!

Links und Literatur

zu diesem Workshop finden Sie im Web unter

http://www.ap.univie.ac.at/users/fe/Quantentheorie/Fortbildungswoche2004/