Seminar Quanten-Computing und Quanten-Informationstheorie

Sommersemester 2003 Nielaba

Quantenkryptografie

Moritz Bubek

4. Juni 2003

Motivation

- Kryptografie wird seit der Antike für militärische Zwecke genutzt
- Auch diplomatische Abkommen sollen nicht bekannt werden
- In der Wirtschaft sollen Verfahren, Rezepturen, usw nicht an die Konkurenz gelangen
- EC-Karten Daten werden verschlüsselt übertragen

Kryptografische Verfahren

- Alle verwendeten Verfahren ersetzen die Zeichen eines Textes durch das Verfahren gegebene andere.
- Das einfachste Verfahren ist eine Zuordnungtabelle, die jedem Zeichen des Zeichensatzes (z.B. von A bis Z) jeweils ein anderes zuordnet.
- Beim Ceasar-Code wird jedes Zeichen um eine Zahl n weiter gedreht
- Diese Verfahren sind sehr einfach zu knacken, da jedes Zeichen immer durch das selbe Zeichen ersetzt wird. Mit statistischer Analyse der Sprache kann der Schlüssel geknackt werden.

Vigenere - Chiffre

- Ein Schlüssel, der periodisch an den Text addiert wird, verbessert das Verfahren.
- gleiche Zeichen werden nicht automatisch zu den selben verschlüsselten.

Orginaltext	Q	U	A	N	T	E	N
Schlüssel (+)	K	E	Y	K	E	Y	K
Verschlüsselter Text	B	Z	Z	Y	Y	D	Y
			↓ öffentlicher Kanal ↓				
Empfangener Text	B	Z	Z	Y	Y	D	Y
Schlüssel (-)	K	E	Y	K	E	Y	K
Entschlüsselter Text	Q	U	A	N	T	E	N

- Aber auch dieses Verfahren ist immer noch durch statistische Verfahren knackbar

One Time Pad

- Das Verfahren wird erst sicher, wenn der Schlüssel die selbe Länge wie der zu verschlüsselnde Text hat und auch keine Regelmäsigkeiten mehr vorweist, er also eine völlig zufällige Kombination ist.
- Diesen Schlüssel nennt man Vernam Chiffre oder auch One-Time-Pad (OTP).
- Er darf nur einmal verwendet werden, um die Sicherheit zu garantieren.
- Das OTP die einzige informationtheoretisch sichere Verschlüsselungsvefahren, d.h es kann nur durch eine Brute-Force-Attacke geknackt werden.

Orginaltext	Q	U	A	N	T	E	N
Schlüssel (+)	G	U	R	H	W	A	F
Verschlüsselter Text	X	P	S	V	Q	F	T
		↓ öffentlicher Kanal ↓					
Empfangener Text	X	P	S	V	Q	F	T
Schlüssel (-)	G	U	R	H	W	A	F
Entschlüsselter Text	Q	U	A	N	T	E	N

Problem: Schlüsselübertragung

- Alle diese Verfahren müssen zuerst die Schlüssel (die Tabelle, die Zahl, das Schlüsselwort) über einen unsicheren Kanal zum Empfänger übertragen
- Dabei kann dieser so wie ursprünglich die Nachricht abgefangen und abgehört werden.
- Zur Lösung dieses Problems kann man auf asymetrische Verfahren zurückgreifen, bei dem der Absender und der Empfänger verschiedene Schlüssel haben.
- Eines dieser Verfahren ist RSA, dessen Sicherheit auf der Faktorisierung großer Primzahlprodukte basiert. Für einen Quantencomputer stellt dies bei entsprechender Realisation des Shor-Algorithmus kaum ein Problem dar.
- Die Lösung des Problems der Schlüsselübertragung ist aber ebenfalls die Quantenmechanik.

Das Non-Cloning-Theorem

Ist es möglich einen unbekannten Quantenzustands zu kopieren ?

Eine Quantenmaschiene mit einem Eingang A und einem Ausgang B. A ist in einem unbekannten, aber reinem Zustand $|\psi\rangle$. Dieser Zustand soll auf den Ausgang B, welcher sich am Anfang im Zustand $|s\rangle$ befindet, kopiert werden.

Der Anfangszustand des Kopierers ist

$$|\psi\rangle \otimes |s\rangle$$

Durch eine unitäre Entwicklung U wird der Kopiervorgang durchgeführt

$$|\psi\rangle \otimes |s\rangle \xrightarrow{U} U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle$$

Wendet man dieses Kopieren auf zwei unabhängige Zustände $|\psi\rangle$ und $|\varphi\rangle$ an, erhält man

$$U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle = |\psi\psi\rangle$$
$$U(|\varphi\rangle \otimes |s\rangle) = |\varphi\rangle \otimes |\varphi\rangle = |\varphi\varphi\rangle$$

Der Zustand $|\xi\rangle$ setzt sich aus den Zuständen $|\psi\rangle$ und $|\varphi\rangle$ zusammen

$$|\xi\rangle = \frac{1}{\sqrt{2}}(|\psi\rangle + |\varphi\rangle)$$

Da U Qubits klont, muß gelten

$$U(|\xi s\rangle) = |\xi\xi\rangle = \frac{1}{2}\left(|\psi\rangle + |\varphi\rangle\right) \otimes \left(|\psi\rangle + |\varphi\rangle\right) = \frac{1}{2}\left(|\psi\psi\rangle + |\psi\varphi\rangle + |\varphi\psi\rangle + |\varphi\varphi\rangle\right)$$

Wegen der Linearität von U gilt aber auch

$$U(|\xi s\rangle) = \frac{1}{\sqrt{2}}\left(U(|\psi s\rangle) + U(|\varphi s\rangle)\right) = \frac{1}{\sqrt{2}}\left(|\psi\psi\rangle + |\varphi\varphi\rangle\right)$$

Im Allgemeinen ist $\frac{1}{2}\left(|\psi\psi\rangle + |\psi\varphi\rangle + |\varphi\psi\rangle + |\varphi\varphi\rangle\right) \neq \frac{1}{\sqrt{2}}\left(|\psi\psi\rangle + |\varphi\varphi\rangle\right)$

$\Rightarrow$ es kann keine unitäre Transformation U geben kann, die beliebige Quantenzustände kopiert.

Die Kopiermaschiene kann also nur Zustände kopieren, die orthogonal zueinander sind.

Bell-Ungleichung

- Alice und Bob messen unabhängig eines zweier verschränkter Photonen
- Meßapperate A, B und C, jeweils + oder - als Meßergebniss
- $R(a_+, b_+)$ ist z.B. die Häufigkeit das Photon 1 mit + in a und Photon 2 mit + in b gemessen wird
- Nach Rechnung mit 8 verschiedenen Möglichkeiten ergibt sich

$$P(a_+, b_+) \leq P(a_+, c_+) + P(c_+, b_+)$$

- a ist nun gegenüber b um α gedreht, a gegenüber c um β ($\alpha > \beta$)
- die quantenmechanische Wahrscheinlichkeit für Photon 1 + in a zu messen ist 0.5, für Photon 2 + in b ist $\sin^2(\alpha) \rightarrow P(a_+, b_+) = 1/2 \sin^2(\alpha)$, entsprechend $P(a_+, c_+) = 1/2 \sin^2(\beta)$, $P(c_+, b_+) = 1/2 \sin^2(\alpha - \beta)$
- $\Rightarrow \quad \sin^2(\alpha) \leq \sin^2(\beta) + \sin^2(\alpha - \beta)$
  mit $\alpha = 45°$ und $\beta = 22.5°$ z.B. $0.5 \leq 0.146 + 0.146$

Verschiedene Verfahren

- QKD-Protokolle, mit dem private Schlüssel über einen öffentlichen Kanal erzeugt werden können, sind nachweißlich sicher.
- Es wird nur eine Leitung[1] benötigt, durch die Qubits mit einer geringen Fehlerrate gesendet werden können.
- Die Qubits können dann zur Erstellung eines Schlüssels für klassische Verschlüsselungsverfahren genutzt werden. Die Sicherheit des Schlüssels hängt nur von der Richtigkeit der Quantenmechanik ab.
- Der Grundgedanke ist die Beobachtung, daß es einem Abhörer[2] Eve nicht gelingt Informationen über den Zustand des zwischen Alice und Bob übertragenen Qubits zu messen, ohne diesen Zustand zu zerstören.
- Wegen des Non-Cloning-Theorems kann Eve auch nicht einfach den Zustand klonen um an die Infomationen zu gelangen.

[1] Glasfaser, Luft, ...

[2] im nachfolgenden Eve genannt

BB84-Protokoll

- Mit dem BB84-Protokoll, das 1984 von Bennet und Brassard entwickelt wurde, können Alice und Bob wie folgt einen geheimen Schlüssel generieren, um anschließend eine damit kodierte Nachricht auszutauschen.

- Alice hat vier Photonentransmitter mit den Polarisationen 0, 45, 90 und 135 Grad, die den Quantenzuständen $|1\rangle$, $|0'\rangle$, $|0\rangle$ und $|1'\rangle$ entsprechen.

- Bobs Detektor kann so eingestellt werden, daß er entweder zwischen $|0\rangle$ und $|1\rangle$ (Standartbasis) unterscheiden kann oder aber zwischen $|0'\rangle$ und $|1'\rangle$ (Dualbasis), nicht aber zwischen allen vier Möglichkeiten, was durch die Heisenberg'sche Unschärferelation verboten wird.

- Um einen Schlüssel der Länge n auszutauschen, erzeugt Alice zwei Reihen von Zufallsbits der Länge m, $(m > n)$. Auch Bob erzeugt solch eine zufällige Bitfolge.

- Es dürfen keinerlei Regelmäßigkeiten in den Reihen vorliegen, sodaß man diese Reihe z.B. durch Quanteneffekte erzeugen kann.

- Alice sendet nun Bob die erste Reihe Zufallbits. Dabei sendet sie die 0 als $|0\rangle$ oder $|0'\rangle$ und die 1 zufällig als $|1\rangle$ oder $|1'\rangle$. Die zweite Reihe ist Auswahlkriterium für die Sendebasis.

- Bob entscheidet anhand seiner Zufallsreihe vor jeder Messung ob er eine orthogonale oder diagonale Detektorstellung nutzt, d.h. ob er die Standartobservable $B = \{|0\rangle, |1\rangle\}$ oder die Dualobservable $D = \{|0'\rangle, |1'\rangle\}$ benutzt.

- $|0'\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$
  $|1'\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle.$

  Bei einer Messung dieser Zustände in der Standartbasis ist die Wahrscheinlichkeit je $\frac{1}{2}$. Analog wenn ein orthogonaler Zustand mit einem diagonal eingestellten Detektor gemessen wird. Entscheidet sich Bob also für die “falsche“ Basis, so ist sein Meßergebniss rein zufällig.

- Bob teilt Alice mit, wie er seinen Detektor jeweils eingestellt hatte, nicht aber die Meßergebnisse. Alice teilt Bob mit, wann er den Detektor

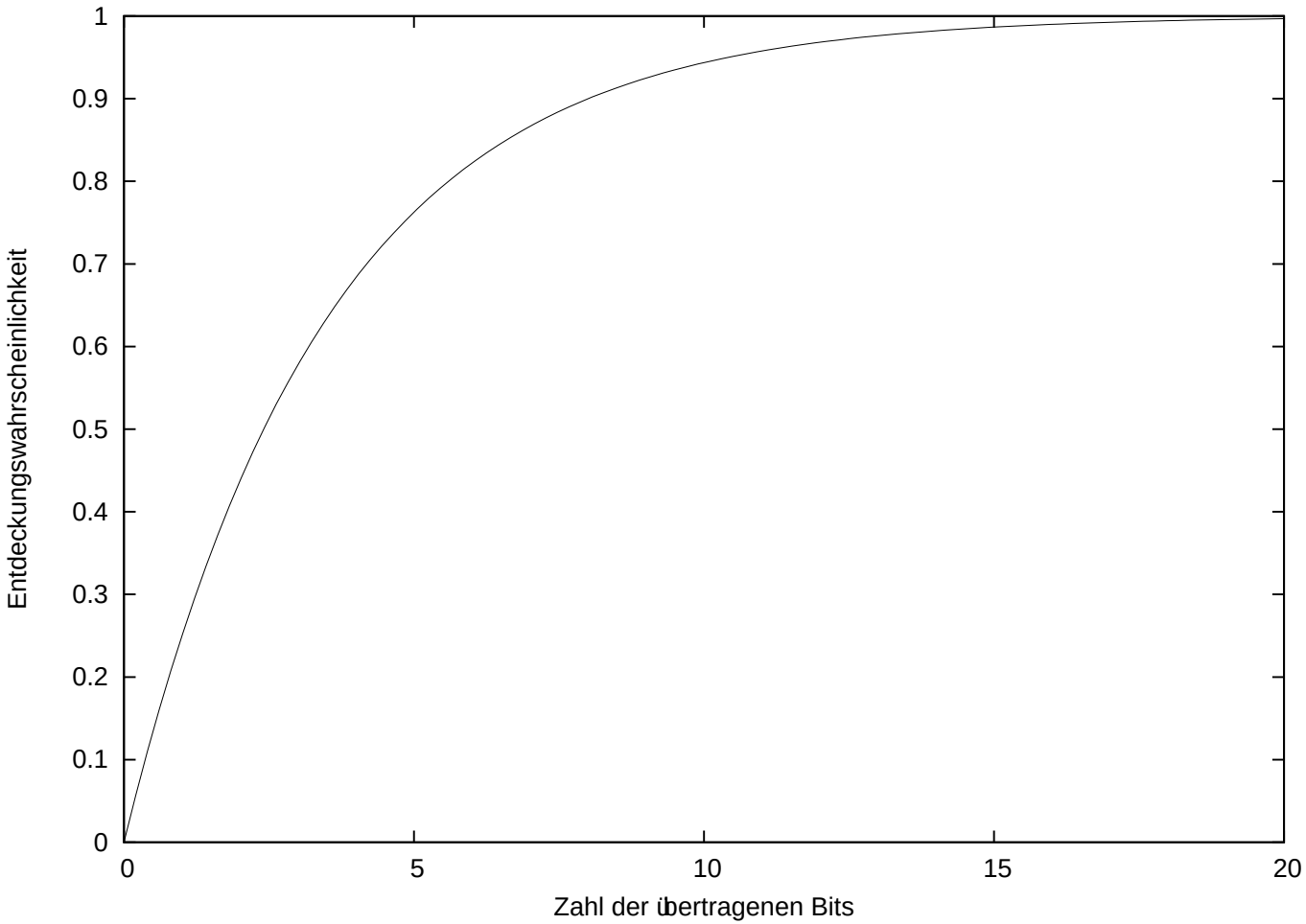
“richtig“ eingestellt hatte, Dies kann über einen öffentlichen Kanal erfolgen, da ein Lauscher ohne eine eigene Messung mit dieser Information nichts anfängt.

- Der gemeinsame Schlüssel von Alice und Bob besteht aus den Meßergebnissen, die mit den gleichen Einstellungen gemacht wurden. Die “falschen“ werden verworfen.

Entdeckung eines Abhörers

- Eve benötigt zusätzlich zu den Informationen über die Stellungen der Detektoren auch die entsprechenden Meßwerte $\Rightarrow$ sie muß diese messen.
- Kein passives Abhören möglich, da jede Messung den Zustand verändert und sich Zustände nicht klonen lassen
- Durch Eves Messung wird die Fehlerrate der Übertragung automatisch größer, da sie nicht wissen kann, mit welcher Polarisation Bob messen wird
- Eve wird mit einer Wahrscheinlichkeit von $\left(\frac{3}{4}\right)^n$ entdeckt
- Alice und Bob ermitteln die Fehlerrate und verwerfen ab einem Grenzwert ihren Schlüssel
- Dazu wählt Bob zufällig eine Menge Qubits aus der Basis zur Schlüsselerzeugung aus und veröffentlicht diese Meßwerte. Alice vergleicht diese mit ihren.

- Ist die Fehlerrate zu groß, verwerfen sie den Schlüssel und beginnen von vorne. Ist die Fehlerrate im Rahmen der Übertragungsfehler werden die veröffentlichten Bits weggeworfen, und aus den restlichen der Schlüssel gebildet.


Entdeckungswahrscheinlichkeit
Zahl der übertragenen Bits
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1
0
5
10
15
20

Beispiel ohne Abhören (und ohne Rauschen)

Alice' 1. Zufallsreihe	1	1	0	0	0	1	0	1	1
Alice' 2. Zufallsreihe	0	1	1	0	0	0	0	1	1
Alice's Polarisierung	$\|1\rangle$	$\|1'\rangle$	$\|0'\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1'\rangle$	$\|1'\rangle$
Bobs Zufallsreihe	0	0	1	0	0	1	1	1	0
Bobs Basis	B	B	D	B	B	D	D	D	B
Meßergebnisse	1	Z	0	0	0	Z	Z	1	Z

$\rightarrow$ Schlüssel 1 0 0 0 1

```
Alices Basis: +++++XX++XX+++XXX+++X+++XX+X+XXX+X+X+XX+XX+++XXXX+X++XX+++X+XXX+
Alice sendet: |--||\/|-\\|--///-||\-|-\/-/-\\\-\-\-//|\\--|\\/\|/|-//||-/-//\-
Bobs Basis  : X+XX++XXX+++XX++X++XXX+++X++XXXX+X++X++X++XXX+XXXX+XXXXXX++++++X
Bob misst   : /-/\||///--|\/-|/-|/\\|--/-|/\\\-\--\|-/|-///|\/\/|\\//\/-|-||-\

Bob         : X+XX++XXX+++XX++X++XXX+++X++XXXX+X++X++X++XXX+XXXX+XXXXXX++++++X
Alice       :  .  . .    .    ... . .. ..  ......          ...    ..  . .
Schluessel  :  0  1 1    1    101 0 10 00  111010          101    00  0 0
```

Beispiel mit Abhören (ohne Rauschen)

64 Bits, die Hälfte wird überprüft

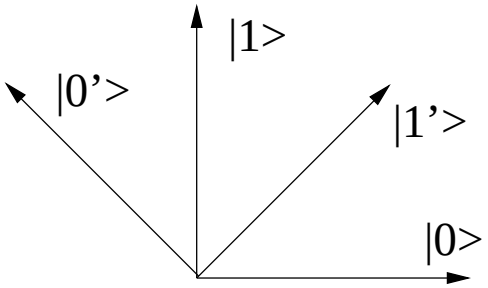
```
Senden
Alices Basis: X+XX++++++X++XX++XXXX++++X++++XX++X+X+XXX+XXX+X+XXX++XXX+++X+XXX
Alice sendet: /-/\-|---|/||/\||\//\-|--/-|||/\-|\|/-\/\|//\|/|\\\-|\//|-|/|/\\
Abhoeren
Eves Basis  : XXX+X+X+X+++XX++X++XX+XX+XX+X++X+++X+X++XX++X+++++XX+X++X+XXX+X+
Eve misst   : ///|\|\-\|-|\/||\||/\-\/-//|/|-\-|-/-/-|\\|-\|-|-|\/|\-|\-\//|\-
Empfangen
Bobs Basis  : XXXX++++XXX+XXXXXX+++XXXX+X+XX++++X++++XXX+X++X+++X+XX+++X+++X++
Bob misst   : ///\||--\/\|\//\\\||-/\//|/|//---|/----\\\|\-|/|-|\-\\-|-/|-|/|-
Vergleichen der Basis
Bob         : XXXX++++XXX+XXXXXX+++XXXX+X+XX++++X++++XXX+X++X+++X+XX+++X+++X++
Suche nach Fehlern
Alice       : / .\..-.  /| ..  .         |    ..\| - /.  / |/|  .. .  . | |/
Bob         : / .\..-.  \| ..  .         |    ../- - \.  \ |/|  .. .  . | |/
```

5 Fehler in 17 überprüften Bits $\Rightarrow$ Alice und Bob wurden abgehört

BB84 über ein unzuverlässiges Medium

- Durch das unzuverlässige Medium kann Bob manche Qubits nicht empfangen oder sie werden in einen anderen Zustand verändert
- Das Protokoll läuft im Prinzip genauso wie ohne Rauschen
- Zuerst überprüfen Alice und Bob, ob das Rauschen zu stark ist, wenn ja beginnen sie von vorne
- Zerlegen des Rohschlüssels in kleinere Stücke, überprufen der Parität, und entfernen das letzte Bit
- schlägt der Vergleich fehl, wird das Stück geteilt und wieder die Parität verglichen
- Wenn die Stücke zu klein werden muß aufgegeben werden

B92-Protokoll (Benett)



- Nur zwei nicht-othogonale Zustände benötigt, benutzt nur die Polarisation 90° und 135° bzw $|0\rangle$ und $|1'\rangle$.
- Die 1 wird über den Zustand $|1'\rangle$, die 0 über den Zustand $|0\rangle$ übertragen.
- Mißt Bob $|0\rangle$ oder $|1'\rangle$, kann er das Ergebniss verwerfen,
- Erhält er als Ergebniss den Zustand $|0'\rangle$ oder $|1\rangle$, weiß er daß Alice die andere Basis nutzte, da sie nie diese Zustände benutzt.
- Mißt er $|0'\rangle$, hat sie 0 übertragen, mißt er $|1\rangle$ hat sie 1 übertragen.
- Bob teilt dann Alice die Positionen dieser Bits mit und sie bilden damit die Basis für ihren gemeinsamen Schlüssel.

- Da hier nur zwei Zustände benutzt werden fällt ein Kommunikationsschritt weg
- Nur jedes vierte Bit kann verwendet werden

EPR-Protokoll

- Von Arthur Ekert 1991 vorgeschlagen
- Die Basis bildet ein System mit drei Zuständen $|\Omega_1\rangle$, $|\Omega_2\rangle$ und $|\Omega_3\rangle$

$$
\begin{aligned}
|\Omega_1\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle_1|\frac{3\pi}{6}\rangle_2 - |\frac{3\pi}{6}\rangle_1|0\rangle_2\right) \\
|\Omega_2\rangle &= \frac{1}{\sqrt{2}}\left(|\frac{\pi}{6}\rangle_1|\frac{4\pi}{6}\rangle_2 - |\frac{4\pi}{6}\rangle_1|\frac{\pi}{6}\rangle_2\right) \\
|\Omega_3\rangle &= \frac{1}{\sqrt{2}}\left(|\frac{2\pi}{6}\rangle_1|\frac{5\pi}{6}\rangle_2 - |\frac{5\pi}{6}\rangle_1|\frac{2\pi}{6}\rangle_2\right)
\end{aligned}
$$

- Es wird folgende Vereinbarung getroffen

Zustand	Bit	Zustand	Bit	Zustand	Bit
$\|0\rangle$	0	$\|\frac{\pi}{6}\rangle$	0	$\|\frac{2\pi}{6}\rangle$	0
$\|\frac{3\pi}{6}\rangle$	1	$\|\frac{5\pi}{6}\rangle$	1	$\|\frac{6\pi}{6}\rangle$	1

- Die zugehrigen Meßoperatoren sind M_1, M_2 und M_3

Kommunikation über einen Quantenkanal

- Ein EPR-Paar wird von der Quelle generiert und jeweils teilweise zu Alice bzw Bob gesendet.
- Beide wählen unabhängig voneinander, zufällig einen der drei Meßoperator M_1, M_2 oder M_3, also z.B. eine Polarisationsrichtung. Sie messen den Zustand.
- Alice merkt sich das Meßergebniss, Bob das Komplement seines Ergbenisses.
- Dieser Vorgang wird solange wiederholt bis genügend Qubits vorhanden sind.

Kommunikation über einen öffentlichen Kanal

- Alice und Bob vergleichen nun wieder ihre Meßeinstellungen.
- Sie extrahieren die bei denen sie die selben Einstellungen benutzt haben zu ihrem Schlüssel und zu einem Rest
- Mit der Annahme das die Fernwirkung die Bell'sche Ungleichung verletzt, kann Eve entdeckt werden. Sobald die Ungelichung erfüllt wird, ist Eve in der Leitung

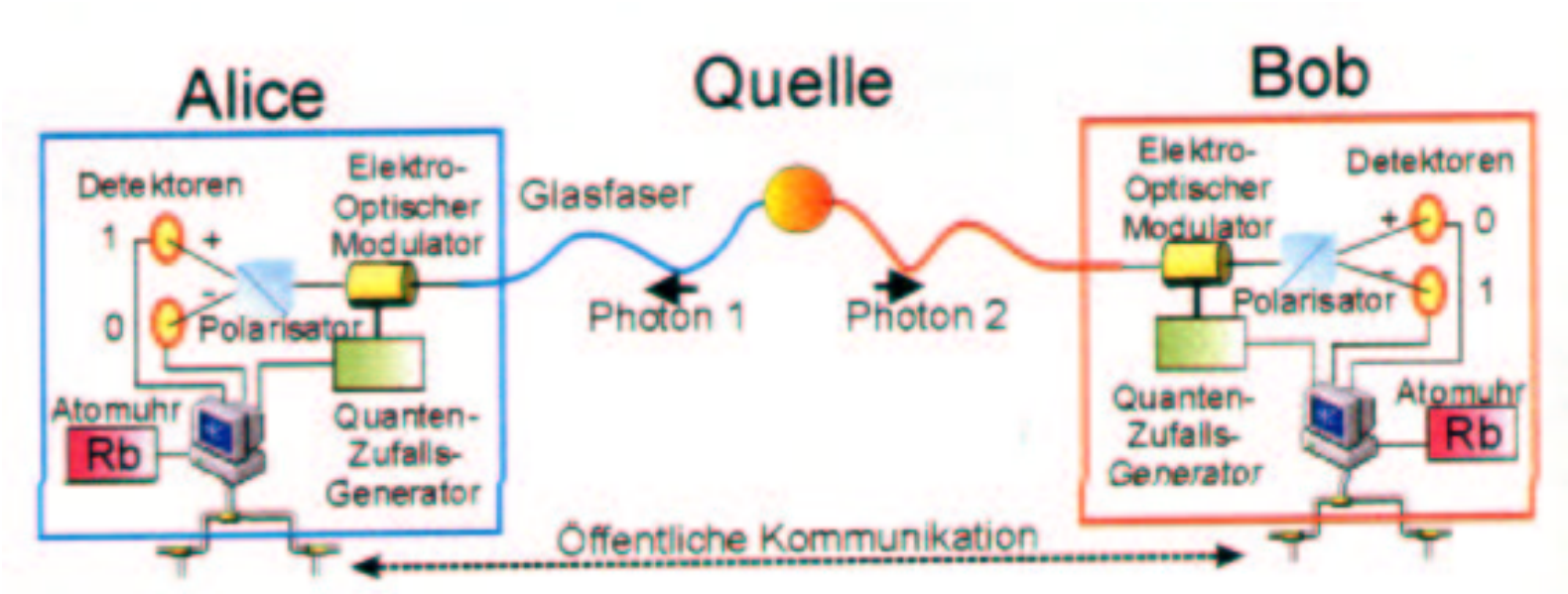
Experimentelle Umsetzung

Allgemein

- 1989 von IBM-Forschern zum ersten mal über eine Strecke von 30 cm Luft
- 1995 dann über 23 km Glasfaser (in Genf)
- 1997/98 per EPR-Protokoll über ca. 10 km (auch in Genf)

Aktuelle Experimente

Übertragung durch Glasfaser

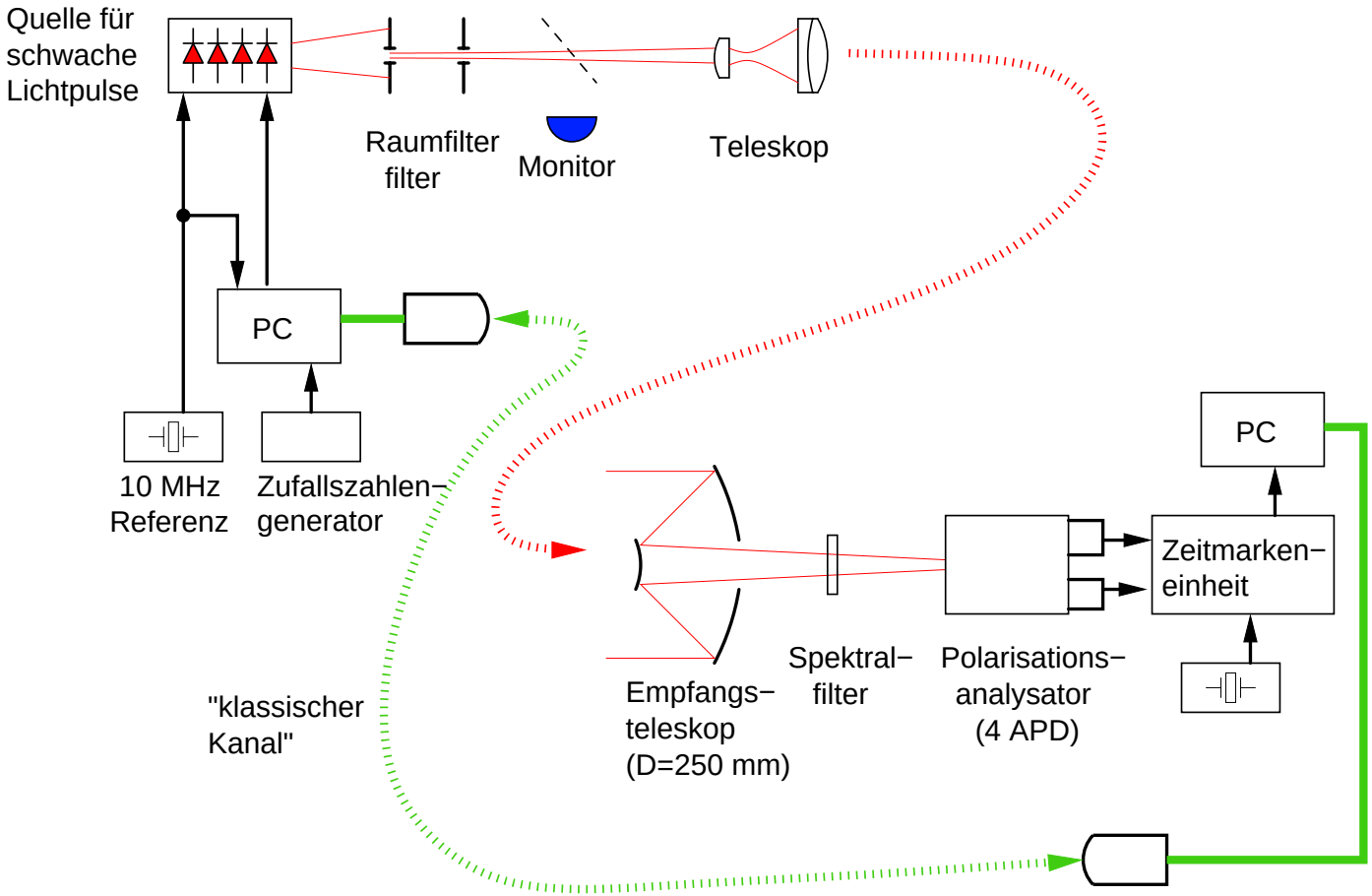


- an der Universität Innsbruck über 360 m

Übertragung durch Luft

- größte Entfernung: 23.4 km zwischen Zugspitze (Alice) und Karvendelspitze (Bob) im Herbst 2002 durch Münchner Team
- die große Höhe der Berge bieten ruhige , klare und dünne Luft, weniger Hintergrundlicht,d.h wenig Fehler
- Benutzung des BB84-Protokolls
- nur 1 kHz Übertragungsfrequenz

Gesamtes System



Experimentelle Probleme

- Erzeugung von nur einem Photon in der Leitung → dadurch geht die Übertragungsrate stark runter
- Wirklich zufällige Meßpolarisation
- Strörung durch Rauschen
- Autentifizierung der Gegenstelle

- sogar schon kommerzielle Produkte... 70 000 Euro

- über 67 km mit 1000 Bit/s
- per USB an jedem Windowsrechner zu betreiben

Literatur

[1] M.A. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press 2000

[2] Jürgen Audretsch, *Verschränkte Welt*, WILEY-VCH 2002

[3] C.Cohen-Tannoudji, B. Diu, F. Laloë, *Quantenmechanik*, de Gruyter 1999

[4] T. Jennewein, G. Weihs, A. Zeilinger, *Schrödingers Geheimnisse*, c't 6/2001, Seite 260ff, Verlag Heinz Heise 2001

[5] http://www.cs.dartmouth.edu/ henle/Quantum/cgi-bin/Q3e.cgi

[6] Christian Kurtsiefer *Experimentelle Quantenkryptografie*, PDF-Document