Quantenkryptographie

Malte Brandy
malte.brandy@maralorn.de

6. September 2014
MRMCD

Orientierung

- Schlüsselaustausch für One-Time-Pad
- Quantum Key Distribution (QKD)

Orientierung

- Schlüsselaustausch für One-Time-Pad
- Quantum Key Distribution (QKD)
- Sicherheitsbeweis durch Quantenmechanik

Orientierung

- Schlüsselaustausch für One-Time-Pad
- Quantum Key Distribution (QKD)
- Sicherheitsbeweis durch Quantenmechanik
- Spezielle Sende- und Empfangsgeräte
- Übertragung durch Glasfaserkabel oder Luft

Orientierung

- Schlüsselaustausch für One-Time-Pad
- Quantum Key Distribution (QKD)
- Sicherheitsbeweis durch Quantenmechanik
- Spezielle Sende- und Empfangsgeräte
- Übertragung durch Glasfaserkabel oder Luft
- Heute nicht: Quantencomputer

Inhaltsverzeichnis

Motivation

- Moderne Verschlüsselungsverfahren basieren auf (unbewiesener) mathematischer Komplexität

Motivation

- Moderne Verschlüsselungsverfahren basieren auf (unbewiesener) mathematischer Komplexität
- Quantencomputer könnten diese Verfahren knacken

Motivation

- Moderne Verschlüsselungsverfahren basieren auf (unbewiesener) mathematischer Komplexität
- Quantencomputer könnten diese Verfahren knacken
- Weil wir es können

Die Idee

- One-Time-Pad

Beispiel

Verschlüsselung			Entschlüsselung		
Klartext		00010001	Verschlüsselt		10100100
Schlüssel	$\oplus$	10110101	Schlüssel	$\oplus$	10110101
Verschlüsselt	$=$	10100100	Klartext	$=$	00010001

$\oplus \mathrel{\widehat{=}}$ XOR

Die Idee

- One-Time-Pad
- Beweisbar sicher (Shannon 1949)

Beispiel

Verschlüsselung			Entschlüsselung		
Klartext		00010001	Verschlüsselt		10100100
Schlüssel	$\oplus$	10110101	Schlüssel	$\oplus$	10110101
Verschlüsselt	$=$	10100100	Klartext	$=$	00010001

$\oplus \mathrel{\widehat{=}}$ XOR

Die Idee

- One-Time-Pad
- Beweisbar sicher (Shannon 1949)
- Problem: Schlüsselaustausch

Beispiel

Verschlüsselung			Entschlüsselung		
Klartext		00010001	Verschlüsselt		10100100
Schlüssel	$\oplus$	10110101	Schlüssel	$\oplus$	10110101
Verschlüsselt	$=$	10100100	Klartext	$=$	00010001

$\oplus \mathrel{\widehat{=}}$ XOR

Quantenmechanik

Die Quantenmechanik beschreibt auf mikroskopischer Ebene den Zustand und die Dynamik unseres Universums. Einige der betrachteten Systeme heißen Quanten.

Beispiel

Atome, Moleküle, Elektronen, Photonen, Quarks, Katzen, Menschen

Was ist es nicht?

- Relativitätstheorie (klein $\neq$ schnell)

Was ist es nicht?

- Relativitätstheorie (klein $\neq$ schnell)
- Die Lehre von kleinsten Energiepäckchen (gibt es nicht)

Was ist es nicht?

- Relativitätstheorie (klein $\neq$ schnell)
- Die Lehre von kleinsten Energiepäckchen (gibt es nicht)

Aber, aber ...

Was ist es nicht?

- Relativitätstheorie (klein $\neq$ schnell)
- Die Lehre von kleinsten Energiepäckchen (gibt es nicht)

Aber, aber ...

Quantisierung ist ein Nebeneffekt der Quantenmechanik, der **manchmal** auftaucht.

Eine physikalische Theorie

Wir konstruieren eine Theorie aus:

- System (z.B. ein Ball)

Eine physikalische Theorie

Wir konstruieren eine Theorie aus:

- System (z.B. ein Ball)
- Zustand des Systems (z.B. er liegt an einer Position still.)

Eine physikalische Theorie

Wir konstruieren eine Theorie aus:

- System (z.B. ein Ball)
- Zustand des Systems (z.B. er liegt an einer Position still.)
- Messungen / Fragen an das System (z.B. Wo ist der Ball?)

Eine physikalische Theorie

Wir konstruieren eine Theorie aus:

- System (z.B. ein Ball)
- Zustand des Systems (z.B. er liegt an einer Position still.)
- Messungen / Fragen an das System (z.B. Wo ist der Ball?)

Der Clou

In der Quantenmechanik passen bestimmte Fragen nur zu bestimmten Zuständen. Es sind nur bestimmte Zustände und Fragen zugelassen.

Pseudoklassisches Beispiel

Beispiel

- System: Ein Ball

Pseudoklassisches Beispiel

Beispiel

- System: Ein Ball
- Zustand: Der Ball ist an (0,0).

Pseudoklassisches Beispiel

Beispiel

- System: Ein Ball
- Zustand: Der Ball ist an (0,0).
- Messung: Wo ist der Ball?

Pseudoklassisches Beispiel

Beispiel

- System: Ein Ball
- Zustand: Der Ball ist an (0,0).
- Messung: Wo ist der Ball?
- Ergebnis: (0,0)

Pseudoklassisches Beispiel

Beispiel

- System: Ein Ball

Pseudoklassisches Beispiel

Beispiel

- System: Ein Ball
- Zustand: Der Ball fliegt mit 25 km/h.

Pseudoklassisches Beispiel

Beispiel

- System: Ein Ball
- Zustand: Der Ball fliegt mit 25 km/h.
- Messung: Wo ist der Ball?

Pseudoklassisches Beispiel

Beispiel

- System: Ein Ball
- Zustand: Der Ball fliegt mit 25 km/h.
- Messung: Wo ist der Ball?
- Ergebnis: öh?

Pseudoklassisches Beispiel

Beispiel

- System: Ein Ball

Pseudoklassisches Beispiel

Beispiel

- System: Ein Ball
- Zustand: Der Ball liegt still an (0,0).

Pseudoklassisches Beispiel

Beispiel

- System: Ein Ball
- Zustand: Der Ball liegt still an (0,0).
- Messung: Wo ist der Ball?

Pseudoklassisches Beispiel

Beispiel

- System: Ein Ball
- Zustand: Der Ball liegt still an (0,0).
- Messung: Wo ist der Ball?
- Ergebnis: (0,0)

Pseudoklassisches Beispiel

Beispiel

- System: Ein Ball
- Zustand: Der Ball liegt still an (0,0).
- Messung: Wo ist der Ball?
- Ergebnis: (0,0)

Heisenbergsche Unschärferelation

So einen Zustand gibt es nicht.

Pseudoklassisches Beispiel

Beispiel

- System: Ein Ball
- Zustand: Der Ball liegt still an (0,0).
- Messung: Wo ist der Ball?
- Ergebnis: (0,0)

Heisenbergsche Unschärferelation

So einen Zustand gibt es nicht.

Klassische Lösung

Zustand: Der Ball ist ziemlich genau an (0,0) und hält fast still.

Das Qubit

Beispiel

- System: Ein Strich (Qubit)

Das Qubit

Beispiel

- System: Ein Strich (Qubit)
- Zustand: —

Das Qubit

Beispiel

- System: Ein Strich (Qubit)
- Zustand: —
- Messung: +?

Das Qubit

Beispiel

- System: Ein Strich (Qubit)
- Zustand: —
- Messung: +?
- Ergebnis: —

Das Qubit

Beispiel

- System: Ein Strich (Qubit)
- Zustand: —
- Messung: $+$?
- Ergebnis: —
- Messung: $\times$?

Das Qubit

Beispiel

- System: Ein Strich (Qubit)
- Zustand: —
- Messung: $+$?
- Ergebnis: —
- Messung: $\times$?
- Ergebnis: öh?

Wichtig

Die Zustände — ($\diagup$) und | ($\diagdown$) sind nicht mit der Messung $\times$ ($+$) kompatibel.

Die Quantenmechanische Messung

- Jede Messung hat ein Ergebnis.

Die Quantenmechanische Messung

- Jede Messung hat ein Ergebnis.
- Ist das Ergebnis nicht klar, nehmen wir zufällig eines wahr.

Die Quantenmechanische Messung

- Jede Messung hat ein Ergebnis.
- Ist das Ergebnis nicht klar, nehmen wir zufällig eines wahr.
- Nach der Messung ist das System in dem dazu passenden Zustand.

Das Qubit

Beispiel

- System: Ein Strich (Qubit)
- Zustand: —

Das Qubit

Beispiel

- System: Ein Strich (Qubit)
- Zustand: —
- Messung: $\times$?

Das Qubit

Beispiel

- System: Ein Strich (Qubit)
- Zustand: —
- Messung: $\times$?
- Ergebnis: $\diagup$ (50%), $\diagdown$ (50%)

Ein echtes Qubit

- System: Ein Photon (Lichtquant)

Ein echtes Qubit

- System: Ein Photon (Lichtquant)
- Qubiteigenschaft: Polarisierung

Ein echtes Qubit

- System: Ein Photon (Lichtquant)
- Qubiteigenschaft: Polarisierung
- Messapparatur: Polarisationsfilter, Polarisierender Strahlteiler

Ein echtes Qubit

- System: Ein Photon (Lichtquant)
- Qubiteigenschaft: Polarisierung
- Messapparatur: Polarisationsfilter, Polarisierender Strahlteiler
- Bauteile: Laser, Spiegel, Glasfaserkabel, Strahlteiler, Detektor (APD)

Schlüsselaustausch

- Alice und Bob wollen einen Schlüssel tauschen

Schlüsselaustausch

- Alice und Bob wollen einen Schlüssel tauschen
- Annahme: Authentische klassische Verbindung

Schlüsselaustausch

Schlüsselaustausch

1. Alice sendet zufällig Photon mit —, |, ／ oder ＼ Polarisation.

Schlüsselaustausch

1. Alice sendet zufällig Photon mit —, |, ／ oder ＼ Polarisation.
2. Bob misst zufällig $+$ oder $\times$.

Schlüsselaustausch

1. Alice sendet zufällig Photon mit —, |, ／ oder ＼ Polarisation.
2. Bob misst zufällig $+$ oder $\times$.
3. Sie verwerfen alle Photonen, die Bob nicht passend gemessen hat.

Schlüsselaustausch

1. Alice sendet zufällig Photon mit —, |, ／ oder ＼ Polarisation.
2. Bob misst zufällig $+$ oder $\times$.
3. Sie verwerfen alle Photonen, die Bob nicht passend gemessen hat.
4. Der Schlüssel wird nach folgendem Schema berechnet:

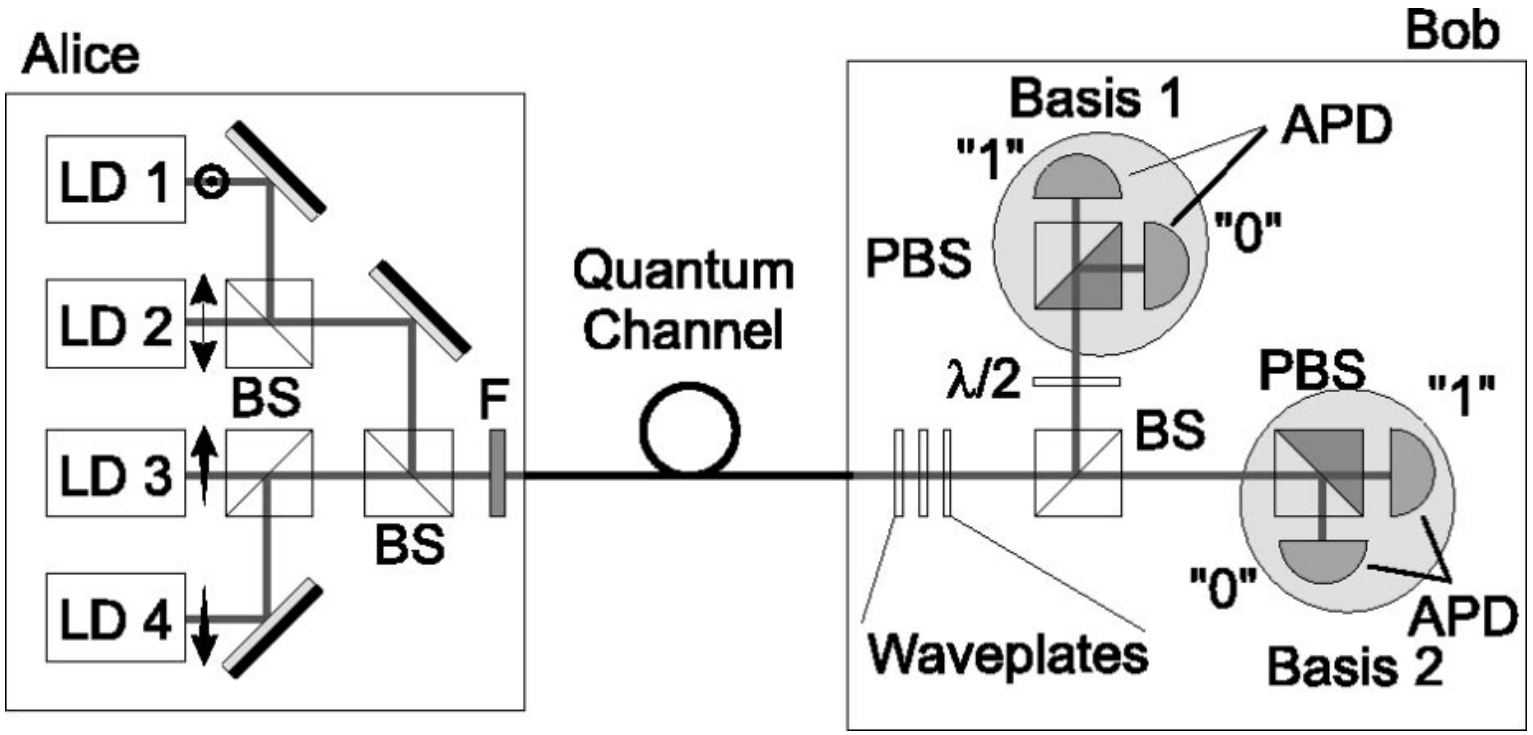
	1	0
$+$	—	|
$\times$	／	＼

Schlüsselaustausch

Beispiel

A. sendet	／	＼	＼	—	|	|	／	／	—	＼
B. misst	+	×	+	+	×	+	+	×	+	×
Gültig?		✓		✓		✓		✓	✓	✓
Key		0		1		0		1	1	0

Realisierung



Gisin et al., 2002

Sicherheitsanalyse

- No Cloning Theorem

Sicherheitsanalyse

- No Cloning Theorem
- Möglicher Angriff: Intercept Resend

Sicherheitsanalyse

- No Cloning Theorem
- Möglicher Angriff: Intercept Resend
- Alice und Bob vergleichen Teile des Keys um Verbindung zu sichern

Intercept Resend Attack

Beispiel

Alice	Eve		Bob		Gültig	Fehler	Key
	M	E	M	E			
↖	+	|	×	↖	✓		0
↗	×	↗	+	|			
↖	×	↖	×	↖	✓		0
|	×	↖	+	|	✓		0
↗	+	|	+	↖			
—	×	↖	×	↖			
↗	×	↗	×	↗	✓		1
—	×	↖	+	|	✓	!	
↗	×	↗	×	↗	✓		1
↖	×	↖	+	|			
↖	+	↗	+	—			

Der Teufel steckt im Detail

- Geräte sind nicht perfekt

Der Teufel steckt im Detail

- Geräte sind nicht perfekt
- Kanäle sind fehlerbehaftet

Der Teufel steckt im Detail

- Geräte sind nicht perfekt
- Kanäle sind fehlerbehaftet
- Viele Seitenkanäle

Der Teufel steckt im Detail

- Geräte sind nicht perfekt
- Kanäle sind fehlerbehaftet
- Viele Seitenkanäle
- Photon Number Splitting Attack

Der Teufel steckt im Detail

- Geräte sind nicht perfekt
- Kanäle sind fehlerbehaftet
- Viele Seitenkanäle
- Photon Number Splitting Attack
- Faszinierende Hacks kommerzieller Systeme

Weiteres

- Vorgestellt: Protokoll BB84 mit Polarisation

Weiteres

- Vorgestellt: Protokoll BB84 mit Polarisation
- weitere Protokolle (SARG, CV, COW . . .)

Weiteres

- Vorgestellt: Protokoll BB84 mit Polarisation
- weitere Protokolle (SARG, CV, COW . . .)
- weitere Codierungen (Phasencodierung, Intensitätscodierung)

Weiteres

- Vorgestellt: Protokoll BB84 mit Polarisation
- weitere Protokolle (SARG, CV, COW . . .)
- weitere Codierungen (Phasencodierung, Intensitätscodierung)
- Vielzahl an Aufbauten

State of the Art

- Kommerzielle Systeme mit Glasfaser über bis zu 80 km verfügbar

State of the Art

- Kommerzielle Systeme mit Glasfaser über bis zu 80 km verfügbar
- Wenige Bit/s über 250km durch Hochleistungsfaser

State of the Art

- Kommerzielle Systeme mit Glasfaser über bis zu 80 km verfügbar
- Wenige Bit/s über 250km durch Hochleistungsfaser
- Wenige Bit über 144km durch Luft auf den Kanaren

State of the Art

- Kommerzielle Systeme mit Glasfaser über bis zu 80 km verfügbar
- Wenige Bit/s über 250km durch Hochleistungsfaser
- Wenige Bit über 144km durch Luft auf den Kanaren
- konventionelle und QKD Benutzung von Glasfasern

Rocket Science

- Weiterentwicklung von Theorie (Sicherheitsbeweise neue Protokolle)

Rocket Science

- Weiterentwicklung von Theorie (Sicherheitsbeweise neue Protokolle)
- Bessere Sender und Detektoren

Rocket Science

- Weiterentwicklung von Theorie (Sicherheitsbeweise neue Protokolle)
- Bessere Sender und Detektoren
- Quantennetzwerke

Rocket Science

- Weiterentwicklung von Theorie (Sicherheitsbeweise neue Protokolle)
- Bessere Sender und Detektoren
- Quantennetzwerke
- Quantenrepeater

Rocket Science

- Weiterentwicklung von Theorie (Sicherheitsbeweise neue Protokolle)
- Bessere Sender und Detektoren
- Quantennetzwerke
- Quantenrepeater
- Satellitenkommunikation

Zeit für Fragen!

Vielen Dank!