

Quantenkryptographie II — Technische Umsetzung

Vortrag zum Seminar “Grundlagen der Quantenphysik”

Robert Riemann

Institut für Physik der Humboldt-Universität zu Berlin

12. Januar 2010



- 1 Dilemma der klassischen Kryptographie
 - Theorie
 - Anwendung in der Praxis
- 2 Einzelheiten zur Quanten-Kryptographie
 - Theorie
 - Vorüberlegungen zur Praxis (BB84-Protokoll)
 - Erhöhung der Sicherheit beim BB84-Protokoll
 - Alternatives Protokoll
- 3 Experimente
 - Übertragung in Luft
 - Übertragung in Glasfaser
 - Zusammenfassung

Einschränkungen klassischer Kryptographie-Verfahren

Definition

Im Sinne der Kryptographie bezeichnet man mit *Asymmetrischen Funktionen* solche, für deren Inverses sich keine einfache Rechenvorschrift finden lässt. Bei *Symmetrischen Funktionen* kann das Inverse ohne Weiteres bestimmt werden.

2 Möglichkeiten

- symmetrische Verschlüsselung
 - erfordert vorher Schlüsselaustausch \Rightarrow nicht spontan
 - prinzipiell sicher bei Verwendung von *One-Time-Pad*
- asymmetrische Verschlüsselung
 - Schlüsselaustausch nicht notwendig \Rightarrow spontan
 - prinzipiell nicht sicher

Berührungspunkte im Alltag

- Internetseitenübertragung via https-Protokoll (SSL)
- Verschlüsselt abgespeicherte Passwörter
- verschlüsselte E-Mails mittels S-MIME oder PGP
- Remotezugriff auf Rechner mit Programm ssh

Zentrales Problem der klassischen Kryptographie

Entweder ist eine Schlüsselübergabe notwendig
oder
die Verschlüsselung ist prinzipiell unsicher.

Lösung des Problems der klassischen Kryptographie

Die Quantenmechanik ermöglicht eine prinzipiell sichere Schlüsselübergabe, da

- der Messprozess den Zustand ändert
- quantenmechanisch nicht-deterministische Zufallszahlengeneratoren realisierbar sind

Zufallszahlengeneratoren

Man unterscheidet zwischen

- deterministischen Zufallszahlengeneratoren
(Zahlen werden durch eine Software-Funktion berechnet)
- nicht-deterministischen Zufallszahlengeneratoren

Quantenmechanische Realisierung

- Strahlteiler teilt in Abhängigkeit der Polarisation gemessen in $|V\rangle$ und $|H\rangle$
- Weg des Photons $|\psi\rangle$ mit $|\psi\rangle = |45^\circ\rangle = \frac{1}{2}|V\rangle + \frac{1}{2}|H\rangle$ ist nicht-deterministisch zufällig
- als USB-Stick für 600 €

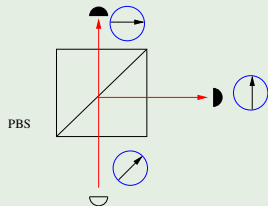


Abbildung: Zufallsgenerator auf Basis eines polarisierenden Strahlteilers (PBS)

Photon Number Splitting (PNS) Attack

Anspruch an die Signalübertragung:

- Informationskodierung in *genau einem* Quantenobjekt um PNS Attack vorzubeugen

Photon Number Splitting (PNS) Attack

Bei der *PNS Attack* wird die Anzahl der Photonen in einem Puls gemessen und Photonen für eigene Messungen abgezweigt, falls mehrere Photonen vorhanden sind.

- momentan technisch nicht realisierbar

Rolle der Photonen bei der Signalübertragung

- Photonen übertragen Informationen am Schnellsten
- Kritische Fehlergrenze: 11 %
- Photonen-Verlust limitiert maximale Übertragungreichweite
- Schwache Laser-Pulse (sogenannte *weak pulses*)
 - Pulse mit > 1 Photon können nicht ausgeschlossen werden
⇒ PNS Attack möglich
 - Großteil der Pulse sind leer
 - geringe Übertragsrate
 - preiswert und vergleichsweise einfach zu realisieren
- Einzelphotonen (siehe Vortrag hierzu)
 - teuer und vergleichsweise kompliziert bei Erzeugung
 - erlaubt höhere Übertragungsraten

Möglichkeiten der Signalleitung

- Ohne Medium bzw. Luft
 - bei ca. 800 nm, da geringe Absorbtion in Luft und bereits erprobte Photonendetektoren existieren
 - sehr wetterabhängig
 - Sichtlinie zwischen Sender und Empfänger erforderlich
 - Bitkodierung in Polarisisation
- Glasfaser
 - dominiert in Forschung
 - Dämpfung: 2 dB/km bei 800 nm; 0.2 dB/km bei 1550 nm
 - Problem bei Wahl der Wellenlänge:
entweder geringe Dämpfung bei 1550 nm
oder gute Photonendetektion bei 800 nm

Signalleitung in Glasfaserkabeln

- keine Sichtlinie zwischen Alice und Bob erforderlich
- Glasfaser nicht völlig zylinder-symmetrisch ↷
- Übertragung polarisationabhängig
- Verwendung von *Time Bin Encoding* für Informationsübertragung, also Phase statt Polarisation

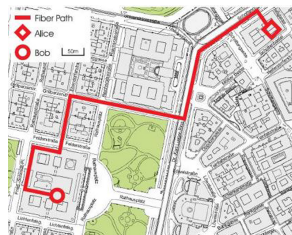


Abbildung: erste quantenkryptographisch übermittelte Überweisung via 1.5km Glasfaserkabel. [ursin]

Phase Encoding

- Information wird als Phasendifferenz durch 2 Glasfaserkabel übertragen
- Informationsrückgewinn bei Bob durch Interferenzmessung:

$$I_0 \sim \cos^2 \left(\frac{\phi_A - \phi_B + k \cdot \Delta L}{2} \right)$$

- falls I_0 oder I_1 null: Schlüsselerzeugung möglich
- Nachteil: Interferometer-Armlängen muss konstant gehalten werden

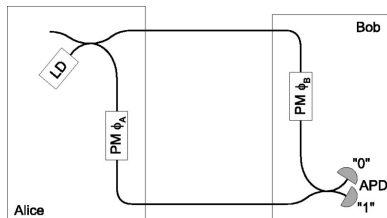


Abbildung: Schema der Informationskodierung mittels Phase Encoding. LD, Laser-Diode; PM, Phasenmodulator; APD, Detektor.

[Gisin et al., Rev. Mod. Phys. 74, 145 (2002)]

Time Bin Encoding

- Information wird als Phasendifferenz durch 1 Glasfaserkabel übertragen
- Phasenmodulation bei Alice und Bob bestimmen Höhe des mittleren Bins
- Ist mittlerer Bin gleich 0 oder maximal, lässt sich Schlüssel generieren
- Vorteil: Veränderung der Armlänge unproblematischer

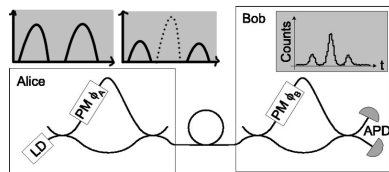


Abbildung: Schema der Informationskodierung mittels Time Bin Encoding. LD, Laser-Diode; PM, Phasenmodulator; APD, Detektor.

[Gisin et al., Rev. Mod. Phys. 74, 145 (2002)]

Decoy State Protokoll

- “Decoy State” = “Köder Zustand”
- gegen PNS Attack bei Verwendung von schwachen Pulsen
- benötigt nur bekannte Technologien

Funktionsweise

- sog. Signal-Puls und Decoy-Puls gleichen sich in allen Eigenschaften außer durchschnittlicher Photonenanzahl
- PNS Attack kann nur von Photonenanzahl abhängen
- Vergleich von erwarteter Detektions- und Fehlerrate lässt Eve auffliegen

Protokoll auf Basis von verschränkten Zuständen

- Idee 1991 von Artur Ekert vorgestellt: Ekert-Protokoll oder Eke91
- Verwendung von One-Time-Pad
- Ablauf
 - Alice und Bob messen in zufälligen Basen die Polarisation
 - bei gleicher Basis: Schlüsselgenerierung, da selbe Ergebnisse
 - bei versch. Basis: Test auf Verletzung der Bell'schen Ungleichung
 - falls Test negativ: keine Verschränkung \Rightarrow Lauschangriff

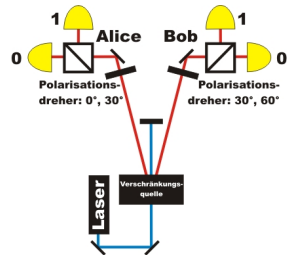


Abbildung: Schema zum Ekert-Protokoll.
[uni-erlangen]

144 km in Luft (2007)

- durchgeführt von Gruppe um T. Schmitt-Manderbach
- Distanz 144 km zwischen La Palma und Teneriffa (vergleichbar zu erdnahen Satelliten)
- Verwendung des BB84 Protokolls mit Decoy-State Erweiterung
- stetige Nachjustierung durch bidirektionale Kalibrationslaser von Bob zu Alice

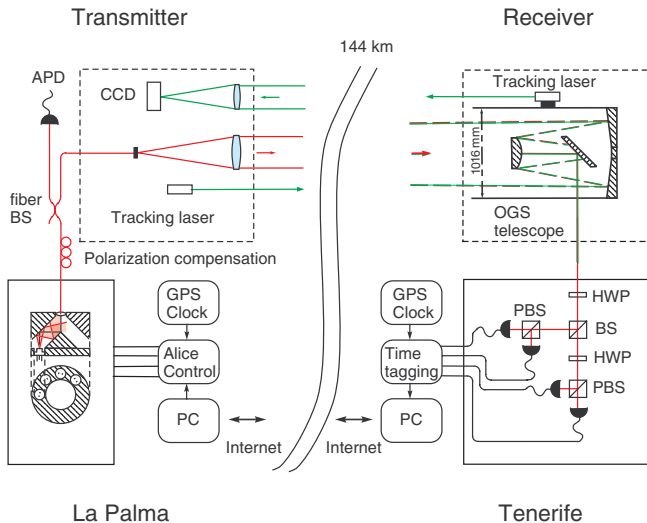


Abbildung: Schema zum Experiment.

[Schmitt-Manderbach et al., Phys. Rev. Lett. 98, 010504 (2007)]

Fotos



Abbildung: Transmitter (Alice). [ursin]

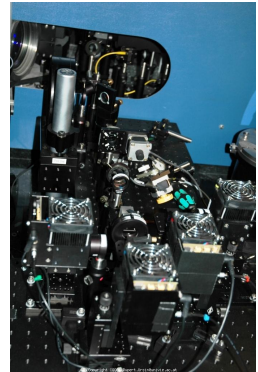


Abbildung: Receiver (Bob). [ursin]

122 km über Standard-Kommunikations-Glasfaser (2005) I

Aufbau

- Verbesserung durch Minimierung von
 - “detector dark count noise”
 - “stray”-Photons
- Mach-Zehnder Interferometer mit Phasenmodulation



Abbildung: Produktfoto Toshiba

122 km über Standard-Kommunikations-Glasfaser (2005) II

Ergebnis

- Fehler gemittelt über 2 min. bei 122km: 8.9 %
- Schlüsselbildungsrate: bis zu 1.9 kbit/s
- Dämpfung: ca. 0.21 dB/km (vgl. Telek. 0.2 dB/km)
- Verbesserungsmöglichkeiten
 - bessere Photonendetektion
 - anderes Protokoll

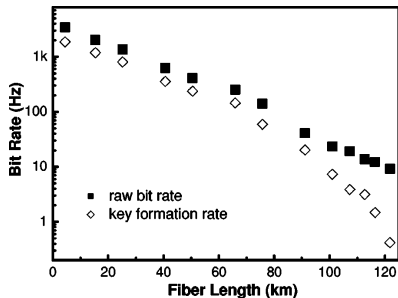








Abbildung: Bitrate in Abhängigkeit von der Glasfaserkabellänge.
 [Gobby et al., Appl. Phys. Lett. 84, 3762 (2004)]

Bisherige Ergebnisse und Ausblick

- Bisher erreicht
 - Größenordnung 150 km Übertragungreichweite in Luft und Glasfaser
 - bei gleichzeitigem Fehler unterhalb von 11% (Stand 2007)
- Aktuelle Forschungsschwerpunkte
 - Erhöhung der Reichweite
 - Erhöhung der Übertragungsgeschwindigkeit
 - Forschung an Einzelphotonenquellen
 - Verbesserung von Detektoren
 - Methoden zur Signalverstärkung
 - globale Quantenkryptographie über erdnahe Satelliten

-  [Gisin et al.] Quantum Cryptography
N. Gisin et al., Rev. Mod. Phys. 74, 145 (2002)
-  [ursin] Grafiken und Fotos.
Dr. Rupert Ursin, <http://homepage.univie.ac.at/rupert.ursin/>
-  [Gobby et al.] Quantum key distribution over 122 km of standard telecom fibre
C. Gobby et al., Appl. Phys. Lett. 84, 3762 (2004)
-  [Schmitt-Manderbach et al.] Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km
Schmitt-Manderbach et al., Phys. Rev. Lett. 98, 010504 (2007)
-  Experimental Decoy State Quantum Key Distribution Over 15km
Yi Zhao et al., Arxiv preprint quant-ph/0503192 v2 (2005)
-  [uni-erlangen] Fotos
<http://www.didaktik.physik.uni-erlangen.de/quantumlab/>

Beispiel einer asymmetrischen Verschlüsselung

Verschlüsselung

$$f(x) = x^a \pmod{b}$$

Entschlüsselung

$$x(f) = f^c \pmod{b}$$

- (a, b) speziell gewählt, bilden öffentlichen Schlüssel
- Sicherheit beruht auf Schwierigkeit $c = c(a, b)$ zu finden
- c ist privater Schlüssel

Phase Encoding - alte Version

- Information wird als Phasendifferenz durch 2 Glasfaserkabel übertragen
- Informationsrückgewinn bei Bob durch Interferenzmessung:

$$I_0 \sim \cos^2 \left(\frac{\phi_A - \phi_B + k \cdot \Delta L}{2} \right)$$

- $\phi_A = 0, \frac{\pi}{2}$ entspricht Bit 0,
 $\phi_A = \pi, \frac{3\pi}{2}$ entspricht Bit 1
- Bob wählt Basis: $\phi_B = 0, \frac{\pi}{2}$
- Bei entsprechender Basiswahl: Schlüsselbildung möglich

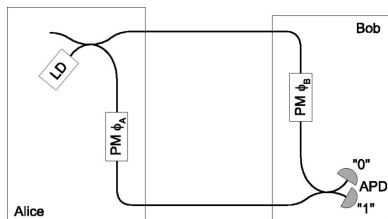


Abbildung: Schema der Informationskodierung mittels Phase Encoding. LD, Laser-Diode; PM, Phasenmodulator; APD, Detektor. [Gisin et al.]



Abbildung: Zufallsgenerator als USB-Modul. [uni-erlangen]