Einführung in die Quantenkryptographie

Tobias Mühlbauer
muehlbau@in.tum.de

Technische Universität München
12.05.2009

***Zusammenfassung*—Die rasante Entwicklung der Computertechnologie, neuste Erkenntnisse über Quantencomputer und algorithmische Weiterentwicklungen bergen eine Gefahr für klassische Kryptographieverfahren in sich. Aus dieser Unsicherheit heraus ist eine Suche nach praktikablen Alternativen, wie der im Folgenden beschriebenen Quantenkryptographie, unerlässlich.**

I. Motivation

KLASSISCHE Kryptographieverfahren beruhen meist auf den mathematisch harten Problemen der Primfaktorzerlegung oder des diskreten Logarithmus. So ist es aus heutiger Sicht einfach, große Primzahlen miteinander zu multiplizieren. Aufwändig gestaltet sich hingegen die Umkehrung, also eine große Zahl in Primfaktoren zu zerlegen. Gerade das sehr populäre **RSA-Verfahren** stützt sich auf die Annahme, dass die eben erläuterte Umkehrung nicht effektiv berechenbar ist. Quantencomputer können mit Hilfe des **Algorithmus nach Shor** das Problem der Primfaktorzerlegung und des diskreten Logarithmus in polynomieller Zeit lösen [1]. Das dies nicht länger nur theoretisch möglich ist, wurde schon im Jahr 2001 in den *IBM Laboratories* gezeigt, als in einem Experiment die Zahl 15 erfolgreich mit dem Shor-Algoritmus faktorisiert wurde [2]. Dem kommerziellen Anbieter von Quantencomputern *D-Wave* ist es 2008 gelungen, eine Recheneinheit mit 128 Qubit herzustellen [3]. Auch das *NIST* warnt vor diesen neuen Entwicklungen und beschreibt Alternativen, die auf mathematischen Problemen beruhen, für deren Umkehrung noch kein effizienter Algorithmus bekannt ist [5]. Eine weitere Alternative stellt die Quantenkryptographie dar, welche auf einer quantenkryptographischen Schlüsselerzeugung und der Anwendung des **One-Time Pad** basiert. Die One-Time Pad Verschlüsselung, welche nach Shannon perfekte Sicherheit garantiert [10], verschlüsselt eine Nachricht N durch ein One-Time-Pad O in Länge der Nachricht. Die verschlüsselte Nachricht entspricht $C = N\ XOR\ O$. Die Entschlüsselung $N = C\ XOR\ O$ wird wieder mit Hilfe von O durchgeführt. Diese Art der Verschlüsselung wird Beispielsweise von Banken und ihren Kunden genutzt. Die Bank stellt dem Kunden eine Liste von Transaktionsnummern (TAN) aus, welche dieser zuhause benutzt, um Überweisungen zu verschlüsseln. Die Schwierigkeit des Verfahrens liegt einzig bei der sicheren Schlüsselverteilung. Dieses Problem kann mit Hilfe der Quantenkryptographie behoben werden.

II. Physikalische Grundlagen

IM Folgenden werden die physikalischen Grundlagen der Quantenkryptographie erläutert.

A. Klassische Experimente

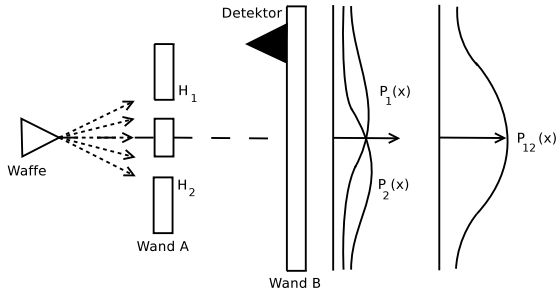

Abbildung 1. Doppelspaltexperiment mit Patronen

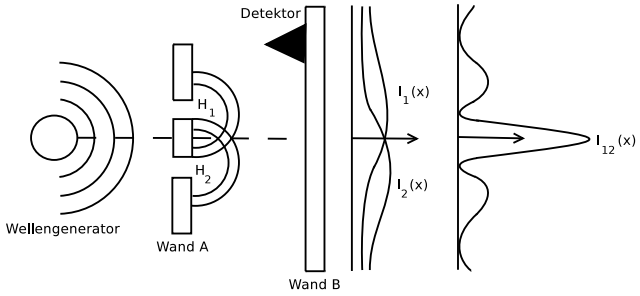

Abbildung 2. Doppelspaltexperiment mit Wellen

Wir wollen als Erstes einen **Doppelspaltversuch** mit Patronen betrachten (Abbildung 1). In diesem Versuch werden gleichmäßig in alle Richtungen Patronen aus einer Waffe auf eine Wand abgefeuert. In dieser Wand befinden sich zwei Schlitze, H_1 und H_2, in welchen die Patronen reflektiert werden können. Hinter der ersten Wand befindet sich eine zweite Wand mit einem Detektor. Dieser misst die Anzahl der ankommenden Patronen in Abhängigkeit vom Ankunftsort. $P_1(x)$ und $P_2(x)$ geben die Wahrscheinlichkeitsverteilung an, wenn man jeweils nur einen Schlitz öffnet. $P_{12}(x)$ hingegen zeigt die Wahrscheinlichkeitsverteilung, wenn beide Schlitze geöffnet sind.

Führt man dasselbe Experiment mit Wellen durch, kann man, sofern beide Schlitze geöffnet sind, ein Interferenzmuster erkennen (Abbildung 2). Eine Erklärung hierfür liefert die Vorstellung, dass hinter den Schlitzen H_1 und H_2 neue Wellen entstehen. Diese Wellen beeinflussen sich im Weiteren Verlauf des Experiments gegenseitig, sodass es zu maximaler Verstärkung und maximaler Auslöschung kommt.

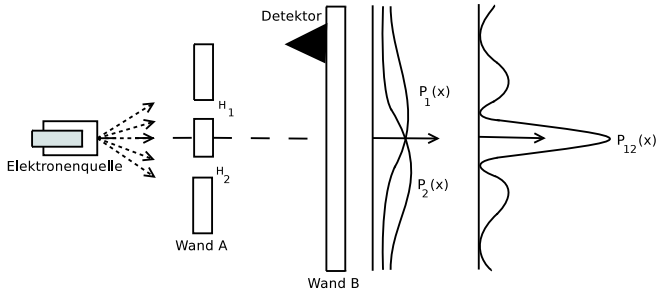

Abbildung 3. Doppelspaltexperiment mit Elektronen

B. Experimente in der Quantenwelt

In der Welt der Quanten werden erneut Doppelspaltversuche durchgeführt. Im Gegensatz zu den klassischen Experimenten werden nun jedoch Elektronen für den Versuch genutzt. Wie Abbildung 3 zeigt, kommt es bei Elektronen, obwohl wir sie als Teilchen betrachten, auch zum Welleninterferenzmuster.

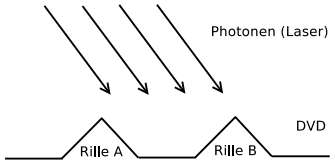

Abbildung 4. Doppelspaltexperiment mit Photonen

Auch Photonen zeigen das Interferenzmuster beim Doppelspaltversuch. Ein Interferenzmuster mit Photonen kann in einem Versuch mit einer DVD und einem Laser erzeugt werden (Abbildung 4). Die DVD dient dabei als Mehrfachspalt. Die Photonen des Lasers werden an den Rillen der DVD wie in einem Schlitz reflektiert.

Die Experimente der Quantenmechanik legen die Betrachtungsweise nahe, dass die Elektronen (bzw. Photonen) beide Schlitze gleichzeitig passieren und sich im Weiteren Verlauf gegenseitig beeinflussen. Dieses Phänomen wird in der Quantenmechanik als **Superpositionsprinzip** bezeichnet. Um den Fall auszuschließen, dass das Phänomen nur bei Anwesenheit von mehreren Elektronen (bzw. Photonen) zu beobachten ist, wurde das Experiment auch in der Form durchgeführt, dass erst dann erneut ein Elektron (bzw. Photon) abgefeuert wird, wenn der Vorgänger die Detektorwand erreicht hat.

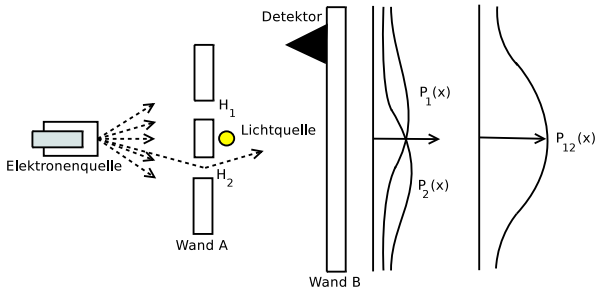

Abbildung 5. Doppelspaltexperiment mit Elektronen und einer Lichtquelle

Um zu beobachten, welchen Schlitz ein Elektron passiert, wird eine Lichtquelle hinter der ersten Wand mit den Schlitzen platziert (Abbildung 5). Durch Reflexion von Photonen kann der Schlitz bestimmt werden, welchen das Elektron passiert hat. Das nicht intuitive Resultat ist, dass durch diese Beobachtung scheinbar die Superposition zerstört wurde. Man erhält eine ähnliche Wahrscheinlichkeitsverteilung wie im klassischen Doppelspaltversuch mit Patronen. Dieses weitere Phänomen der Quantenmechanik wird als **Dekohärenz** bezeichnet.

C. Zustände eines Quantensystems

Quantensysteme werden mathematisch als Hilberträume modelliert. Das Buch [4, Kapitel 1.4 - 1.6] bietet hierfür eine ausführliche Beschreibung. Für das Weitere Verständnis reicht es, sich einen Zustand eines Quantensystems als Vektor vorzustellen. Ein Beobachtungssystem kann nur Zustände voneinander unterscheiden, falls diese orthogonal zueinander sind. Ein Beobachtungssystem wird auch als Messbasis bezeichnet. Ein Zustand eines Elektrons nach der ersten Wand im Doppelspaltversuch mit Elektronen ohne Beobachtung (Abbildung 3) ist eine Superposition der Messbasis (Elektron passierte H_1, Elektron passierte H_2). Dekohärenz tritt beim Messen eines zur Messbasis nicht orthogonaler Zustands auf. Zur Veranschaulichung kann man das Messen als eine Projektion des Zustands auf die Messbasis interpretieren.

D. Polarisation von Photonen

Zustände eines Quantensystems lassen sich praktikabel durch polarisierte Photonen übertragen. Eine einfache Möglichkeit der Polarisation ergibt sich durch die Verwendung von Polarisationsfiltern. Ein Qubit, also eine Kodierung einer binären Konstante, kann durch die Polarisation eines Photons in Richtung ϕ oder $\phi + 90°$ realisiert werden werden. Ein Dekodieren mit der Messbasis ϕ und $\phi + 90°$ liefert ein eindeutiges Ergebnis, da es zu keiner Dekohärenz kommt.

III. Quantenkryptographische Protokolle

DIE gezeigten physikalischen Beobachtungen und die Phänomene des Modells der Quantenmechanik können nun für Verschlüsselungsprotokolle herangezogen werden.

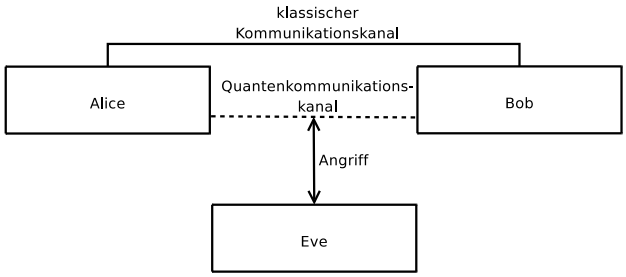

Abbildung 6. Ausgangslage für die Quantenkryptographie

Wie Abbildung 6 zeigt, existieren zwischen Alice und Bob, welche eine geheime Nachricht austauschen wollen, zwei Kommunikationskanäle. Neben einem klassischen Kommunikationskanal benötigt ein quantenkryptographisches Protokoll außerdem einen Quantenkommunikationskanal. Dieser wird meist als Glasfaserkabel realisiert und überträgt Quantenzustände. Ein Angreifer Eve versucht eben auf diesem Kanal einen Angriff durchzuführen und Zustände abzuhören.

A. Theoretischer Ablauf eines Protokolls

Ziel eines quantenkryptographischen Protokolls ist das sichere und geheime Erstellen eines One-Time Pad in Länge einer zu verschlüsselnden Nachricht. Dieser Schlüssel soll Alice und Bob gleichermaßen, sonst aber niemandem bekannt sein.

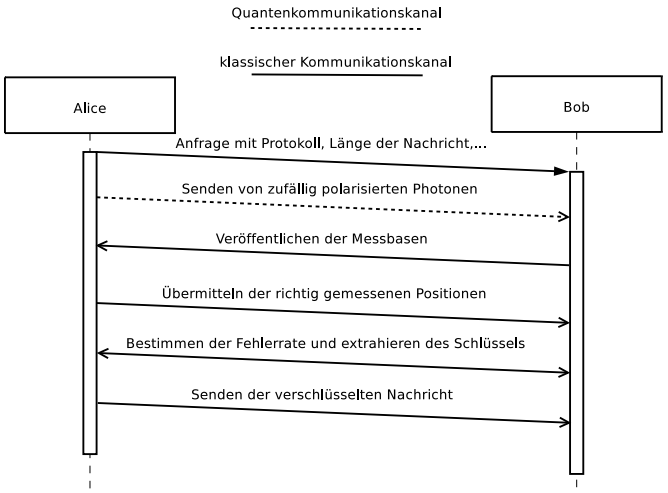

Abbildung 7. Theoretischer Ablauf eines Protokolls

Abbildung 7 zeigt den theoretischen Ablauf eines solchen Protokolls: Alice sendet eine Nachricht über den klassischen Kanal an Bob. In dieser Nachricht wird das zu verwendende Protokoll, die Länge der Nachricht und weitere Parameter übertragen. Da sich Alice und Bob auf ein Protokoll geeinigt haben und wir von Photonen als Quantenzustandsüberträger ausgehen wollen, kennt Alice die Polarisationen mit denen sie Photonen polarisieren kann und Bob kennt die zu verwendenden Messbasen. Alice fährt nun damit fort, zufällige Bits zufällig zu kodieren und die Zustände über den Quantenkommunikationskanal an Bob zu schicken. Dieser misst mit einer der Messbasen und erhält damit entweder ein zufälliges oder richtiges Messergebnis. Am Ende dieser Übertragungen sendet Bob seine verwendeten Messbasen an Alice und sie sendet Bob daraufhin eine Übersicht der Stellen, an denen er sich für die richtige Messbasis entschieden hat. In einem letzten Schritt bestimmen Alice und Bob gemeinsam eine Fehlerrate und, sofern sie sich sicher genug sind, einen gemeinsamen Schlüssel. Diesen Schlüssel verwendet Alice, um ihre Nachricht zu verschlüsseln. Nach erfolgreichem Senden über den klassischen Kanal kann Bob die Nachricht mit gleichem Schlüssel entschlüsseln.

B. Grundlagen der Sicherheit

Im Folgenden wird nur die Sicherheit der Schlüsselerzeugung betrachtet. Im späteren Verlauf greift die perfekte Sicherheit des One-Time-Pad. Um die Sicherheit einer Schlüsselübertragung zu messen wird die Fehlerrate der Übertragung bestimmt. Sie bezeichnet den Anteil der übertragenen Zustände, die bei der Übertragung zerstört wurden. Natürliche Ursachen dafür sind ein fehlerhafter Kanal, das Rauschen des Kanals (natürliche Dekohärenz), aber auch Fehler an der Quelle und im Detektor. Natürliche Fehler kann man durch eine Taktung des Übertragungsvorgangs und Error Correction Codes erkennen. Im Gegensatz dazu gibt es Fehler, welche durch einen Angriff eingeführt werden. Im schlimmsten Fall kennt Eve die verwendeten Messbasen und versucht Zustände zu kopieren oder abzuhören. Für einen Abhörvorgang seitens Eve gilt:

- Pr[Eve macht einen Fehler] = $\frac{1}{4}$
- Pr[Eve macht bei n Messungen keinen Fehler] = $(\frac{3}{4})^n$

Schwierigkeiten bereitet die Differenzierung natürlicher Fehlern und derer, die durch Eve eingeführt werden. Aus Sicherheitsgründen wird davon ausgegangen, dass alle Fehler eines nicht natürlichen Ursprungs sind.

C. Funktionsweise des BB84-Protokolls

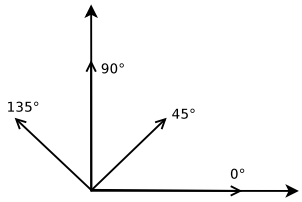

Abbildung 8. Polarisationsrichtungen eines Photons beim BB84-Protkoll

Das BB84-Proktoll ist nach seinen Erfindern Bennett und Brassard bekannt, welche es 1984 entwickelten. Wie in Abbildung 8 dargestellt, benutzt Alice die Polarisationen $0°$: $\rightarrow$, $90°$: $\uparrow$, $45°$: $\nearrow$ und $135°$: $\nwarrow$ und Bob misst entweder mit der Standardbasis $\mathcal{B} = \{\uparrow, \rightarrow\} = +$ oder der dualen Basis $\mathcal{D} = \{\nwarrow, \nearrow\} = \times$.

In Abbildung 9 sind Alices Polarisationen und die möglichen Messergebnisse für Bob verzeichnet. Eine Beispielübertragung für das BB84-Proktoll findet sich in Abbildung 10.

Alices Polarisation	Bobs Messbasis	Resultat	Wahrscheinlichkeit
$0 \mapsto \uparrow$	$0 \rightarrow \mathcal{B} = +$	0	1
	$1 \rightarrow \mathcal{D} = \times$	$0/1$	$0,5$
$0 \mapsto \nearrow$	$0 \rightarrow \mathcal{B} = +$	$0/1$	$0,5$
	$1 \rightarrow \mathcal{D} = \times$	1	1
$1 \mapsto \rightarrow$	$0 \rightarrow \mathcal{B} = +$	0	1
	$1 \rightarrow \mathcal{D} = \times$	$0/1$	$0,5$
$1 \mapsto \nwarrow$	$0 \rightarrow \mathcal{B} = +$	$0/1$	$0,5$
	$1 \rightarrow \mathcal{D} = \times$	1	1

Abbildung 9. Polarisationen und Messergebnisse beim BB84-Protokoll

1	0	0	1	Alices Zufallsstring
$\rightarrow$	$\nearrow$	$\uparrow$	$\nwarrow$	Alices Polarisation
0	1	1	0	Bobs Zufallsstring
$\mathcal{B} = +$	$\mathcal{D} = \times$	$\mathcal{D} = \times$	$\mathcal{B} = +$	Bobs Messbasis
1	0	Z	Z	Resultat

Abbildung 10. Beispielübertragung mit dem BB84-Protokoll (Z: Zufällig)

D. Vergleich zu weiteren Protokollen

Das **B92-Protokoll** wurde 1992 ebenfalls von Bennett entwickelt und stellt das minimale Protokoll der quantenbasierten Schlüsselerzeugung dar. Alice verwendet hier nur die Polarisationen $90°$: $\uparrow$ und $135°$: $\nwarrow$.

Ein weiteres Protokoll geht auf Eckert und das Jahr 1991 zurück. In seiner Funktionsweise ähnelt es derer des BB84-Protokolls, nutzt allerdings das Phänomen der Quantenverschränkung, um Zustände zu übertragen.

IV. AUSBLICK

QUANTENKRYPTOGRAPHIE ist nicht länger nur im Labor durchführbar, auch wenn dies noch für einige Zeit der dominante Ort für ihres Einsatzes sein wird. Schon im Jahr 2004 kam es zu einer testweisen praktischen Durchführung. In Wien wurde ein Banktransfer zwischen dem Rathaus und einer in der Stadt ansässigen Bank durch ein quantenkryptographisches Verfahren verschlüsselt [6]. Im Jahr 2006 wurde der bisherige Rekord für die Strecke einer Schlüsselerzeugung aufgestellt. Quantenzustände wurden auf einer Strecke von 184,6 km über ein Glasfaserkabel übertragen [9]. Im gleichen Jahr kam es allerdings auch zu einem Rückschlag für die Quantenkryptographie. In einem *MIT-Labor* wurde erstmals erfolgreich ein Teil der Schlüsselerzeugung nach dem BB84-Protokoll abgehört [8]. 2007 wurde schließlich ein quantenkryptographisches Verfahren erstmals zur Nachrichtenübertragung während der Schweizer Parlamentswahl eingesetzt [7].

LITERATUR

[1] P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” *SIAM J.SCI.STATIST.COMPUT.*, vol. 26, p. 1484, 1997. [Online]. Available: http://www.citebase.org/abstract?id=oai:arXiv.org:quant-ph/9508027

[2] L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang, “Experimental realization of shor’s quantum factoring algorithm using nuclear magnetic resonance,” *Nature*, vol. 414, p. 883, 2001. [Online]. Available: http://www.citebase.org/abstract?id=oai:arXiv.org:quant-ph/0112176

[3] D. Robson, “Most powerful ever quantum chip undergoing tests,” *NewScientist*, 2009. [Online]. Available: http://www.newscientist.com/article/mg20126965.600-most-powerful-ever-quantum-chip-undergoing-tests.html

[4] J. Gruska, “Quantum computing,” *McGraw-Hill*, 1999.

[5] R. Perlner and D. Cooper, “Quantum resistant public key cryptography: a survey,” *IDtrust ’09: Proceedings of the 8th Symposium on Identity and Trust on the Internet*, Apr 2009. [Online]. Available: http://portal.acm.org/citation.cfm?id=1527017.1527028

[6] “World premiere: Bank transfer via quantum cryptography based on entangled photons,” *Pressekonferenz*, Apr 2004. [Online]. Available: http://www.secoqc.net/downloads/pressrelease/Banktransfer_english.pdf

[7] F. Patalong, “Quantenkrypotografie: Die sicherste datenleitung der welt,” *Spiegel-Online*, Oct 2007. [Online]. Available: http://www.spiegel.de/netzwelt/tech/0,1518,511087,00.html

[8] T. Kim, I. S. genannt Wersborg, F. N. C. Wong, and J. H. Shapiro, “Complete physical simulation of the entangling-probe attack on the bb84 protocol,” in *Conference on Lasers and Electro-Optics/Quantum Electronics and Laser Science Conference and Photonic Applications Systems Technologies*. Optical Society of America, 2007, p. QML6. [Online]. Available: http://www.opticsinfobase.org/abstract.cfm?URI=URI=QELS-2007-QML6

[9] D. Rosenberg, C. G. Peterson, J. Harrington, P. Rice, N. Dallmann, K. T. Tyagi, K. P. McCabe, R. J. Hughes, J. E. Nordholt, R. H. Hadfield, B. Baek, and S. Nam, “Long-distance quantum key distribution in optical fiber,” in *Optical Fiber Communication Conference and Exposition and The National Fiber Optic Engineers Conference*. Optical Society of America, 2008, p. OWJ1. [Online]. Available: http://www.opticsinfobase.org/abstract.cfm?URI=URI=OFC-2008-OWJ1

[10] C. E. Shannon, “Communication theory of secrecy systems,” *Bell Systems Technical Journal*, vol. 28, pp. 656–715, 1949.