Quantenkryptographie

Spyridon Iliopoulos

04 Juni 2003

Zusammenfassung

Moderne kryptographische Verfahren haben Schwachstellen. Im Fall von asymmetrische Verfahren, wie RSA, ist es die "einfache" Primzahlzerlegung mittels des Shor Algorithmus. Obwohl symmetrische Verfahren als sicher gelten, ist die Schwachstelle die sichere Verteilung des gemeinsamen Schlüssels. Genau hier kann Quantenkryptographie helfen. Es erlaubt eine abhörsichere Kommunikation zwischen zwei (oder mehreren) Partnern für die Schlüsselverteilung. Danach kann man auf klassische Verschlüsselungverfahren wie z.B. AES zurückgreifen.

1 Einführung

Kryptographie gab es seit der Antike. Viele der früher eingesetzten Verfahren, wie z.B. Ceasars Cipher, sind durch die Hilfe heutiger Computer sehr schnell unbrauchbar geworden. Kryptographische Verfahren finden nicht nur bei Geheimdiensten oder im Internet Gebrauch, sondern werden bei Mobiltelefonen oder bei der Verschlüsselung der Pin in der Kreditkarte eingesetzt. Fehler in den Verfahren selbst oder bei der Benutzung des Verfahrens haben immer zur Katastrophe geführt und Kriege entscheiden. Das Grundprinzip aller Verfahren wird in Abb. 1 gezeigt. Man wünscht sich das man eine Nachricht mit einem Schlüssel so chiffriert, so daß nur der Empfänger mit dem richtigen Schlüssel sie dechiffrieren kann. Für alle anderen sollte die Nachricht für lange nicht lesbar sein. Hier wird nicht auf Digitale Signaturen nicht eingegangen. Unser Ziel wird es sein eine Nachricht sicher vom Sender zum Empfänger zu transportieren, ohne das ein Angreifer mit Hilfe "unbegrenzter" Ressourcen, die Nachricht nach gewisser Zeit dechiffrieren kann. "Unbegrenzt" soll bedeuten, daß der Angreifbar nur über Computer verfügt, wie sie in näher Zukunft denkbar wären.

Der Aufwand zur Verschlüsselung einer Nachricht hängt von der Wichtigkeit der Nachricht für die zwei kommunizierenden Parteien ab.

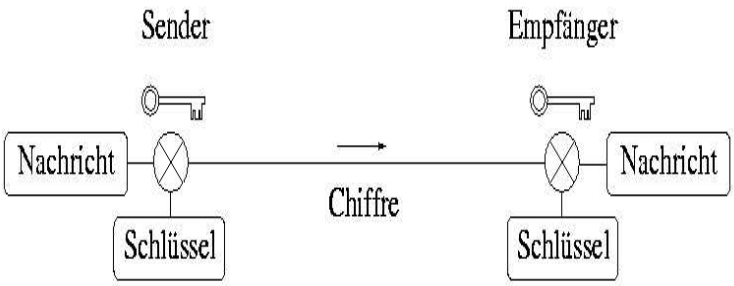

Abbildung 1: Basic Idea of Kryptographie

Es gibt zwei Arten von Verschlüsselung, wenn man sie nach der Art des Keys einteilt: symmetrische und asymmetrische Verschlüsselung. One-Time Pads gehören zur symmetrischen Verschlüsselung, wobei jeder Key nur **einmal** benutzt wird. Es gibt noch Hybrid Verfahren und im wirklichem Leben benutzt man sehr oft beide zusammen, Um ein symmetrischen Schlüssel zu verteilen wird als erstes ein asymmetrisches Verfahren benutzt.Sonst kann ein Angreifer (meistens als Eve in der Literatur bezeichnet) einfach mithören und den symmetrischen Schlüssel abfangen.

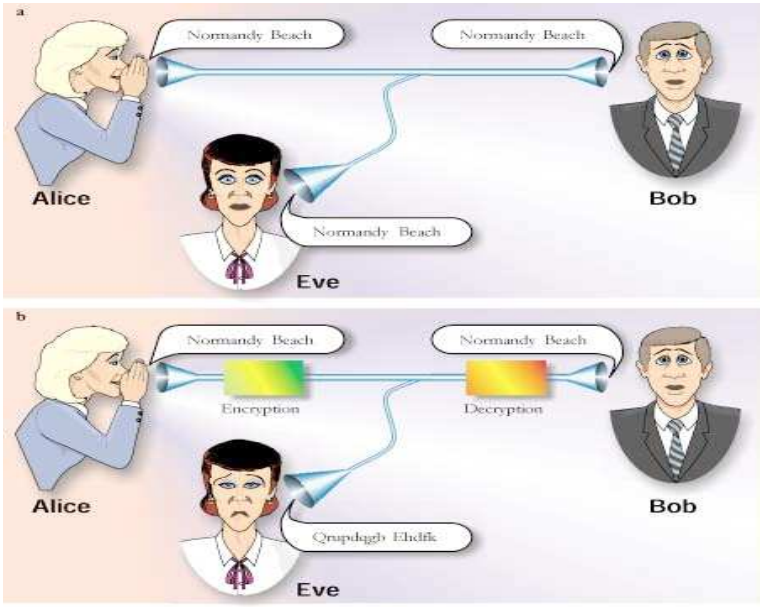

Abbildung 2: Problem with the Key Distribution

2 Asymmetrische Kryptographie

Bekannte Beispiele dafür sind RSA und PGP. Das Prinzip ist das gleiche. Man hat zwei Arten von Keys:einen öffentlichen (Public) und einen privaten Schlüssel. Wenn Alice mit Bob kommunizieren will, verschlüsselt Alice mit dem öffentlichen Schlüssel von Bob und schickt die Nachricht an Bob weiter. Bob -und nur Bob- sollte mit Hilfe seines privaten Keys die Nachricht wieder entschlüsseln können. Lassen wir im Moment das Problem der Authentifizierung außer acht. Wir sind sicher, daß der öffentlicher Schlüssel zu Bob gehört, wie sicher können wir sein, daß Eve nicht mithört UND die Nachricht entschlüsseln kann? Das Prinzip von RSA (Rivest, Shamir, Adleman) basiert drauf, daß es einfach ist das Produkt zweier Primzahlen (151*157) zu berechnen, aber sehr viel schwieriger, d.h. zeitintensiver eine große Zahl (23707) in Primzahlen zu zerlegen.

Prinzip von RSA:

1. Als erstes werden zwei -große- Primzahl p und q genommen. In der praktischen Implementierung wird ein Algorithmus benutzt um kurz zu überprüfen, ob die zwei Zahlen wirklich Prim sind. Da bis jetzt dieses Verfahren noch kein Fehler machte, hofft man das es sich bei den zwei Zahlen um Primzahlen handelt.

2. Danach werden zwei Zahlen d und e berechnet und das Produkt $N = ed$. Es gilt
   - d und $(p-1)(q-1)$ sind teilerfremd
   - $[(p-1)(q-1)]$ ist Vielfaches von ed
3. Verschlüsselung von w: $c = w^e \, mod N$
   Entschlüsselung von c: $w = c^d \, mod N$

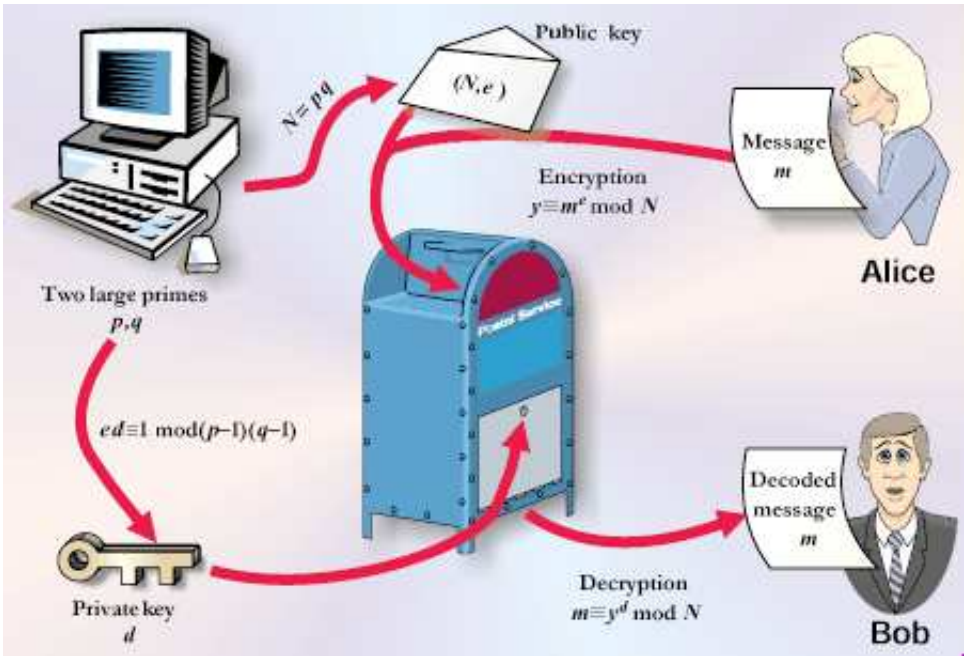

Abbildung 3: How RSA works

Mit Kenntnis von N und e (öffentlicher Schlüssel) können Daten verschlüsselt werden, ohne Kenntnis der Primfaktoren von N sollte Entschlüsselung nicht möglich sein. [Bau00]

Da jeder im Besitz des öffentlichen Schlüssels ist, kann man einen zeitintensiven Versuch die Primzahlen herauszufinden starten. Zwar gibt es seit letztes Jahr ein neuen Algorithmus zur Primzerlegung, der 3 mal schneller funktionieren soll, aber viel gefährlicher ist der Quantenalgorithmus von Shor, wo man in polynomialer Zeit ($O(n^3)$) statt exponentieller $O\left(\exp\left((\frac{64}{9}n)^{\frac{1}{3}}(\log n)^{\frac{2}{3}}\right)\right)$ (General Number Field Sieve) faktorisieren kann, der das ganze Prinzip mit den Primzahlen unbrauchbar macht. Es wird in [Cle97] beschrieben, wie man RSA mit Quantencomputer knacken kann.

Schlüssellänge	1024 Bit	4096 Bit
Rechenzeit	10^5 Jahre	$3 * 10^{29}$ Jahre

Tabelle 1: Netzwerk von 1000 Rechnern:

Schlüssellänge	1024 Bit	4096 Bit
Rechenzeit	**4.5 Minuten**	**4.8 Stunden**

Tabelle 2: Quantencomputer mit Taktfrequenz von 100 MHz

Zwar wurde 2000 mit Hilfe des Deutsch-Joska-Algorithmus eine 4-Bit Funktion in einen 5-Bit Quantencomputer realisiert und IBM hat im Dezember 2001 die Zerlegung von 15 (mittels Shors Algorithmus) auf einen 7-Bit Quantencomputer realisiert, allerdings dauert es noch ein bisschen bis man es praktisch anwenden kann. Um ein 4096-Bit Schlüssel zu faktorisieren braucht man aber 20484 Qubits!!

3 Symmetrische Kryptographie

Wieso benutzt man nicht einfach symmetrische Verfahren wie DES, IDEA, Blowfish oder AES? Erstens sind die Verfahren langsamer und zweitens besteht das Problem der Schlüsselübergabe, wobei man für jeden Kommunikationspartner einen eigenen Schlüssel braucht. Die Zahl der Schlüssel wächst sehr schnell an, im Vergleich zu den asymmetrischen Verfahren, wo man nur ein Schlüsselpaar braucht. Da asymmetrische Verfahren schwach gegen Quantencomputer sind, ist das Problem durchaus realistisch. Die Verfahren selbst sind excellent und sind außer DES (und ein paar Ausnahmen) gut gegen Angriffen von Kryptoanalysten geschützt. Es bleibt die Frage: Wie kann ihn Alice zu Bob schicken, per Telefon, Internet, Post,... und sicher sein, daß Eve nicht im Besitz des Schlüssels kommt, oder mithört?

Eine Unterkategorie von symmetrischen Verfahren sind One-Time-Pads. Bei jeder Kommunikation wird ein neuer zufälliger Schlüssel generiert. Es muss ein neuer zufälliger Schlüssel generiert werden, da sonst falls man zweimal den gleichen Schlüssel benutzt, das Verfahren angreifbar wird. Da jeder Schlüssel **höchstens** einmal benutzt wird, ist die Sicherheit gewährleistet.

Auf Block/ Bitstrom-Chiffrierung wird hier nicht näher eingegangen.

Wie kompliziert ein symmetrisches Protokoll sein kann, sieht man am Beispiel von DES (Anhang Abbildung 6). Weitere Infos -und wie man DES

knackt- gibt es unter Record-Breaking DES Search Completed

4 Quantenkryptographie

Die ersten wissenschaftlichen Beiträge gab es bereit 1970. Der erste vorgestellte Algorithmus war von Bennett 1984. Weitere Protokolle wurden 1992 (BB92), 1991 (EPR) vorgestellt. Mit besseren Laserquellen und praktischen Implementierungen steigt das Interesse und mehr Protokolle werden entwickelt. Es ist mehr als *Key Distribution Protokoll* gedacht.

5 Prinzipien der Quantenkryptographie

Es gibt ein paar Prinzipien der Quantenmechanik, die die QC zu nutzen macht und die für alle Protokolle gelten.

- Jede Messung stört die Messgrösse
- Ein unbekannter Quantenmechanischer Zustand ist nicht perfekt kopierbar.

6 BB84 Protokoll

"Amazing, Holmes."
"Elementary, my dear Watson, elementary"

Sir Arthur Conan Doyle
(1859-1930)

Das älteste Protokoll, aber immer noch interessant, wegen seiner Einfachheit, wurde von Bennett 1984 vorgestellt. Es wurde schon erfolgreich implementiert mit Hilfe von schwachen Laserpulsen. Es funktioniert zwischen Partnern bis zu einer Entfernung von 67 km http://www.idquantique.com/

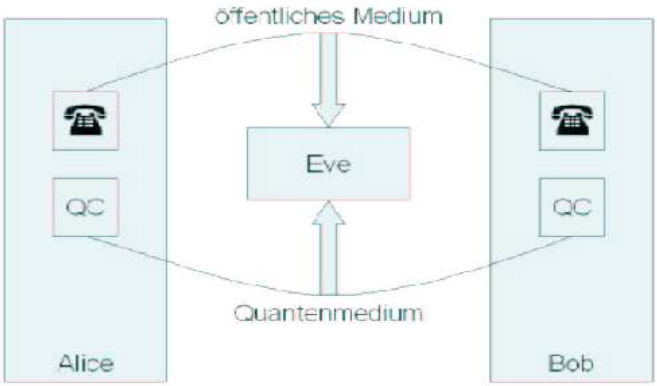

Abbildung 4: BB84

Dazu benutzt man zwei Kanäle, einen klassischen und ein Quantenkanal. Man braucht zwei nicht orthogonale Basen mit dem man 4 Zustände kodieren kann. Eine Messung in der eine Basis verändert auch die Observable in der anderen Basis. Man denke z.B. an Spin in der x und in der z Richtung.

Das Prinzip ist sehr einfach:

1. Alice schickt Bob eine Reihe von Qubits, jedes in eine von vier zufälligen States.
2. Für jedes Qubit wählt zufällig eine Basis.
3. Bob mißt jedes Qubit.
4. Bob veröffentlicht die Basis, welche er für jede Messung benutzt hat.
5. Alice veröffentlicht (durch den authentifizierten öffentlichen Kanal) für welche Messungen die Basis stimmte.
6. Alice und Bob werfen alle Qubit, in denen die Basis in Bobs Messung nicht stimmte.
7. Alice und Bob überprüfen, ob Eve mithörte .
8. Alice und Bob machen Fehlerkorrektur.
9. Alice und Bob machen Privacy Amplification.

Als erstes schickt Alice N Qubits, wobei jedes Qubit sich in einen der vier möglichen Zustände befindet. Bob (und Eve auch,s.u.) wissen nichts über Alice Basiswahl. Bob wählt zufällig eine Basis und mißt. In 50% der Fälle wählt er die falsche Basis. Danach veröffentlicht er welche Basis er benutzt hat. Alice ihrerseits veröffentlicht für welche Messungen die Basis stimmte. Für alle Messungen,für die die Basis falsch war, werden die Ergebnisse nicht mehr betrachtet. Von der Fehlerrate kann man schon Rückschlüsse machen, ob Eve mithörte oder nicht.

Bob wählt aus der verbleibende Liste $n << \frac{N}{2}$ und schickt die gemessene Werte zu Alice (öffentlich)

Fall 1) Ein oder mehrere Test-Bits unterscheiden sich von Alice Liste ⇒ Abbruch der Kommunikation
"Eve hört mit"

Fall 2) Alle n Meßwerte stimmen überein ⇒ Alice und Bob verwenden die verbliebenden $\frac{N}{2} - n$ als Schlüssel.

Man darf zu diesem Zeitpunkt bzw davor keine Fehlerkorrektur machen (s.u.). Zum dem Zeitpunkt Eve kann höchstens die benutzte Basis wissen. Danach kann man Fehlerkorrektur machen. Am Ende werden $\frac{N}{2} - n$ Bits als Schlüssel benutzt.

In der Praxis benutzt man schwache Laserpulsen (was einzelnen Photonen entsprechen soll) und mit doppelbrechenden Materialien setzt man eine Polarisationsrichtung (linear, Zirkular) fest. Tabelle 3 und 4 illustrieren das Protokoll.

Qubit	↻	↕	↻	↔	↕	↕	↔	↔	↻	↺	↕	↻	↺	↺
Basis	⊗	⊕	⊗	⊕	⊕	⊕	⊕	⊕	⊗	⊗	⊕	⊗	⊗	⊗
Bit	0	1	1	0	1	1	0	0	1	0	1	1	0	0

Tabelle 3: Beispiel Übertragung von Alice für das BB84 Protokoll

Basis	⊕	⊗	⊗	⊗	⊕	⊗	⊗	⊕	⊕	⊕	⊗	⊗	⊕	⊗
Messung	↕	↻	↻	↺	↕	↕	↔	↔	↕	↕	↻	↻	↔	↺
Result	n	n	✓	n	✓	n	n	✓	n	n	n	✓	n	✓
Key	1	1	1	0	1	1	0	0	1	1	1	1	0	0
shifted Key			1		1			0				1		0

Tabelle 4: Beispiel Übertragung empfangen von Bob für BB84 Protokoll

Alice schickt Photonen in einem der vier Zustände, ↻ ,↺ , ↕ ,↔ . Bob wählt zufällig eine Basis ⊕ oder ⊗ und mißt jedes angekommene Photon. Dann teilt er Alice die Basissequence, die er benutzt hat, d.h. ⊕, ⊗, ⊗, ⊗, ⊕, ⊗, ⊗, ... mit. Dann teilt Alice mit, dass Bobs Wahl für die QBits 3, 5, 8, 12, 14 stimmt. Danach testet man für eine Menge, ob Eve mitgehört hat, evtl. Fehlerkorrektur und Privacy Amplification. Der Schlüssel der sich ergibt, nach dem alle Bit, für die die Basis nicht stimmte, weggeworfen würden, heißt shifted Key. Dann haben sie einen gemeinsamen sicheren Schlüssel.

7 BB84 Protokoll Sicherheit

Betrachten wir welche Angriffe Eve führen kann und wie groß die Wahrscheinlichkeit ist, daß Eve entdeckt wird. Natürlich muß man noch überlegen welche praktische Probleme, d.h. bei der Implementierung auftreten können.

Attacke auf BB84:

- Intercepting Resending
- Beam Splitting
- Attacke auf den klassischen Kanal (Man-in-the-Middle)

Attacke auf den klassischen Kanal(Man-in-the-Middle):
Als erstes könnte Eve versuchen den klassischen Kanal anzugreifen, um eine Man in the Middle Attacke zu machen. Das kann man mittels

Authentifizierung einfach lösen.

Intercepting Resending:
Zwar kennt Eve das Nocloning Theorem, versucht aber trotzdem den Zustand zu messen und einen unvollständigen Zustand weiter an Bob zu schicken. Wann merken Alice und Bob, daß Eve mithört?

Wahrscheinlichkeit, daß Eve <u>auffliegt</u>:

Fall 1) Eve wählt die gleiche Basis wie Alice,Bob

$\circlearrowleft \longrightarrow \circlearrowleft \longrightarrow \circlearrowleft$ Keine Störung

Fall 2) Eve wählt die falsche Basis
$\circlearrowleft \longrightarrow \updownarrow \longrightarrow \circlearrowleft$ Störung in 50% aller Fälle

Insgesamt wird Eve Messung in $p = \frac{1}{4}$ aller Fälle detektiert und damit in $\frac{3}{4}$ aller Fälle <u>nicht</u> detektiert.

Bei n Testbits:
$1 - p^{-n} = 1 - (\frac{3}{4})^n \longrightarrow 1$

Beam Splitting: Dieses Problem ist das gefährlichste von allen und ist leider in der Praxis immer wieder anzutreffen. Leider gibt es keine perfekten Laserquellen. Es kann passieren, daß unsere Laserquellen zwei Photonen statt eine schickt. dann könnte Eve eins speichern (was praktisch sehr schwierig ist) und eins weiterschicken. Dann bleibt Eve unerkannt und kann nach Bekanntmachen der Basis die gespeicherten Photonen in der richtigen Basis messen. Dann erhält sie ein Teil des Schlüssels. Aber nach der Privacy Amplification sollte, da nicht immer zwei Photonen produziert werden, Eve nicht genug Informationen über den Schlüssel erhalten.

Was noch man beachten muß ist, daß falls ein Quantenkanal mit Rauschen benutzt wird, man <u>keinesfalls</u> Fehlerkorrektur direkt anwendet. Sonst könnt Eve selber Fehlerkorrektur machen, die Photonen(States) messen und dann unbemerkt an Bob weiterschicken.Solange es unter der Rauschgrenze bleibt, bleibt Eve unentdeckt! Der Beweis, dass das Protokoll trotzdem sicher ist (für die meisten Angriffe), hat [May96](auch [Deu96]) geliefert.

Es gibt noch Angriffe, wo Fred - ein weiterer Angreifer- nur Kenntnis über die Basiswahl hat und mit Eve kooperiert. Ich will aber nicht drauf eingehen. [Got02]

Ein praktisches Problem ist auch -neben der Quelle und den beide Kanälen- der Detektor. Es sollen keine Photonen verloren gehen bzw Photonen angezeigt die nicht existieren. Für den Fall, dass Photonen verloren gehen, hat Mayers [May98] gezeigt, dass das Protokoll sicher ist. Ein Beweis für den Fall, dass der Kanal nicht rauchenfrei ist und Photonen verloren gehen, wurde in [Bra99], [Lo99] vorgestellt.

Allerdings gehen alle Beweise davon aus, dass man entweder eine nicht perfekte Quelle oder einen nicht idealen Detektor hat. Der Beweis, wenn beide Detektor und Quelle nicht ideal sind, ist zum diesem Zeitpunkt nicht fertig. [Got02] .

Bis jetzt wurde nicht berücksichtigt, dass Eve evtl. eine "Trojan Horse Attacke" machen könnte, d.h. sie könnte selber versuchen Photonen zu Alice und Bob schicken. Eve war bisher nur passiv, d.h. sie hat nur die Photonen gemessen und weitergeschickt (Intercept/Resend). Sie hat aber selber keine *neue* Photonen in den Quantenkanal geschickt. Eve kann Lichtpulse zu Bob (oder Alice) schicken und das zurückgestreute Licht analysieren. So kann sie Rückschlüsse ziehen, welche Laser (d.h.Rückschlüsse auf die Basis) gerade Photonen geschickt hat, oder welcher Detektor gerade Photonen detektiert hat.
Man kann solche Attacken sicher technisch durch Filter lösen. Es soll uns nur klar machen, dass es solche Attacken existieren und die Sicherheit von quantenkryptographischen Verfahren nicht **nur** durch quantenmechanischen Prinzipien allein gewährleistet wird. [Gis01]

Es sollte klar sein, dass gilt:

Infinite Security ⇒ Infinite Cost ⇒ Zero practical interest

8 Weitere Protokolle und was noch bleibt

Es gibt weitere Protokolle z.B. das 2-State-, 6-State-Protokoll. Es wurde schon bewiesen, dass auch diese Protokolle sicher sind. Die erlaubte Fehlerrate ist unterschiedlich im Vergleich zum BB84. Im Beispiel von 6-State liegt die erlaubte Fehlerrate bei 33% statt 25% in BB84 [Lo01]:

$$QBER = \frac{N_{wrong}}{N_{right} + N_{wrong}} \approx \frac{R_{error}}{R_{shift}}$$

wobei N die Anzahl der gesendeten Photonen ist und R die Anzahl der empfangenen Photonen ist. Das hängt zusammen, dass wir 3 nicht ortho-

gonale Basen haben und Eve mit 30% (50% in BB84) Wahrscheinlichkeit die richtige Basis auswählt. Das bedeutet auch, dass Eve weniger Informationen über den Schlüssel bekommt. Man kann auch EPR Photonen benutzen, um Quantenkryptographie zu betreiben. Außerdem sollte die Sicherheit der Protokolle (BB84/92,EPR) beweisen werden.

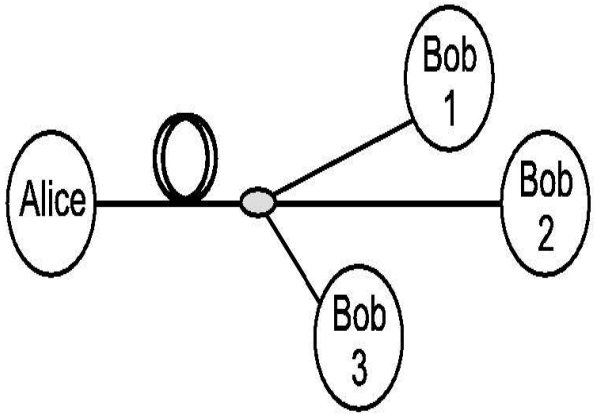

Abbildung 5: BB84 für mehrere Empfänger

9 Zusammenfassung

Mittels Quantenkryptographie kann man das prinzipielle Problem der klassischen Kryptographie, den Schlüssel zu verteilen sicher zu lösen.Es ist nicht möglich, daß Eve unentdeckt den Quantenkanal horcht und genug Informationen über den Schlüssel sammelt. Es bleibt noch die Sicherheit des Protokolls zu beweisen. Die Beweise basieren meistens auf einen perfekten Sender (Quelle), Empfänger und ein Kanal ohne Rauschen. In der Praxis hat man eine beliebige Kombination davon.

Online Demo http://www.cs.dartmouth.edu/ henle/Quantum/

On-line Zeitschrift http://www.rintonpress.com/journals/qiconline.html

Es wird versucht BB84 auch für Satelliten brauchbar zu machen http://scotty.quantum.physik.uni-muenchen.de.

Literatur

[Bau00] Bauer F.L.: Entzifferte Geheimnisse. Springer, 2000.

[Bra99] Brassardand G., Lutkenhaus N., Mor T. and Sanders B.C.: Security Aspects of Practical Quantum Cryptography. quant-ph/9911054, 1999:.

[Cle97] Cleve R., Ekert A., Macchiavello C. and Mosca M.: Quantum Algorithms Revisited. quant-ph/9708016, 1997:.

[Deu96] Deutsch D., Ekert R., Jozsa R., Macchiavello C., Popescu S. and Sanpera A.: Quantum privacy amplification and the security of quantum cryptography over noisy channels. quant-ph/9604039, 1996:.

[Gis01] Gisin N., Ribordy G., Tittel W. and Zbinden H.: Quantum Cryptography. quant-ph/0101098, 2001:.

[Got02] Gottesman Daniel ans Lo H.K.: Proof of security of quantum key distribution with two-way classical communications. quant-ph/0105121, 2002:.

[Lo99] Lo H.K. and Chau H.F.: Unconditional Security Of Quantum Key Distribution Over Arbitrarily Long Distances. Science, 1999: (283):2050–2056.

[Lo01] Lo H.K.: Proof of unconditional security of six-state quantum key distribution scheme. quant-ph/010213, 2001:.

[May96] Mayers D.: Quantum Key Distribution and String Oblivious Transfer in Noisy Channels. quant-ph/9606003, 1996:.

[May98] Mayers D.: Unconditional security in Quantum Cryptography. quant-ph/9802025, 1998:.

Danksagung

Danke an Steffen Jost für seine Hilfe und für seine Vorschläge.

Special Thanks to God for playing Dices.

Anhang

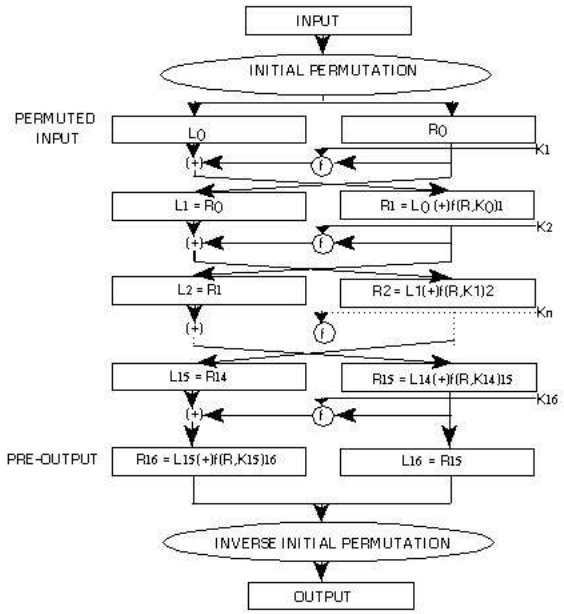

Abbildung 6: How DES works