4. Quantenkryptographie

Kryptologie = geheime Kommunikation

kryptos – versteckt logos – Wort

Der Bedarf nach Methoden der geheimen Kommunikation ist so alt wie die Zivilisation. In diesem Kapitel der Vorlesung werden wir die prinzipiellen Probleme der heute üblichen Methoden der klassischen Kryptographie basierend auf öffentlichen Schlüsselsystemen diskutieren und zeigen, daß Elemente der Quantentheorie benutzt werden können, um diese Probleme zu beseitigen.

4.1. Elemente der klassischen Kryptographie

Grundaufgaben der Kryptographie

(i) sichere Übertragung klassischer Information von A (Alice) nach B (Bob)

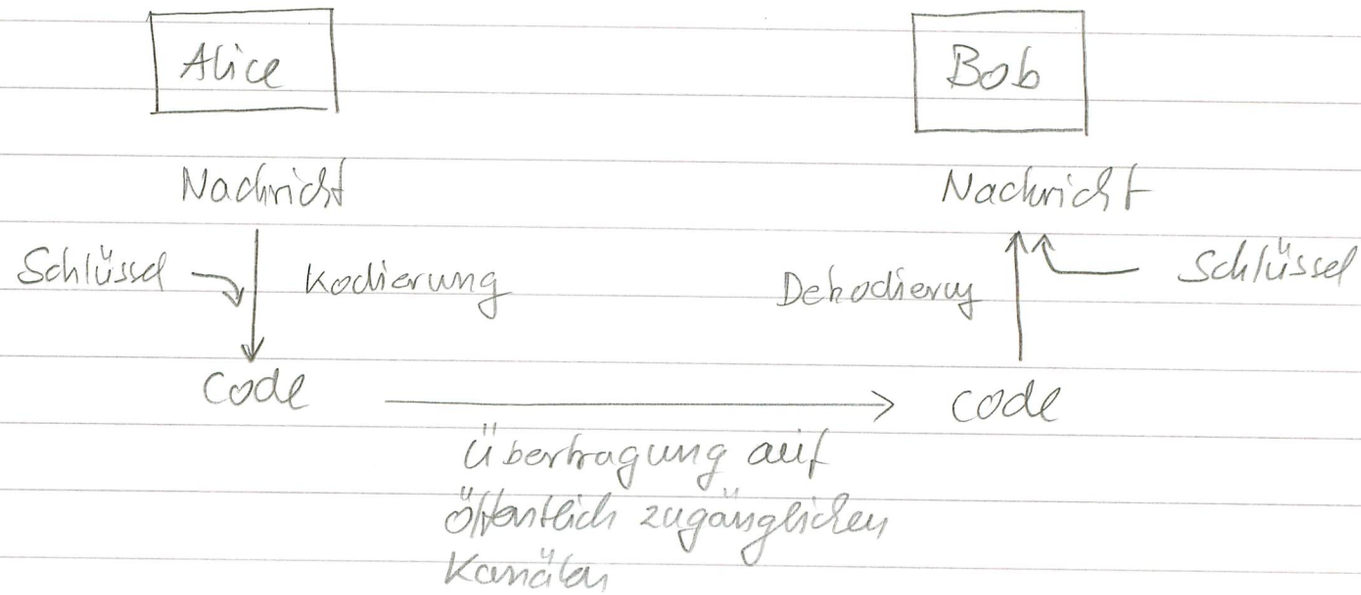
(ii) Authentifikation: Woher weiß Bob, daß er tatsächlich mit Alice kommuniziert

Wir werden hier nur Problem (i) diskutieren.

Sicherheit eines kryptographischen Codes:

früher: Geheimnis der Verschlüsselungsprozedur

heute: Prozedur weißt bekannt aber geheime Schlüssel



$$N \rightarrow G(S,N) = C \longrightarrow D(S,C) = N$$

identischer Schlüssel

Beispiel: Vernam Protokoll (Gilbert Vernam 1917)

Kodierg:	Text	0	0	1	1	0	1	0	
	⊕ Schlüssel	1	0	0	1	1	0	1	mod. 2
	Code	1	0	1	0	1	1	1	

Dekodierung

Code	1	0	1	0	1	1	1
⊕ Schlüssel	1	0	0	1	1	0	1
= Text	0	0	1	1	0	1	0

Shannon (1949): Vernam Protokoll ist sicher falls
(a) Schlüssel zufällig ist und dieselbe Länge wie der Text hat
(b) der Schlüssel nur einmal benutzt wird

Das Problem der sicheren Kryptographie reduziert sich auf die Erzeugung und Verteilung eines geheimen Schlüssels. In den 70er Jahren wurde ein sehr elegantes Verfahren entwickelt daß das Problem der Schlüsselverteilung über unsichere Kanäle scheinbar zu lösen schien: das Verfahren öffentlicher Schlüssel (public key systems). Die Idee des public key system ist, daß zu Kodierung und Dekodierung verschiedene Schlüssel S_C und S_D verwendet werden. S_C und S_D hängen natürlich umkehrbar eindeutig miteinander zusammen, d.h.

(1) $S_C = f[S_D]$ $\quad S_D = f^{-1}[S_C]$

Dabei ist die Auswertung von f einfach,

d.h. es existiert ein effizienter Algorithmus der f berechnet, die Auswertung von f^{-1} jedoch schwer, d.h. es existiert kein effizienter Algorithmus.

Bob: wählt S_D berechnet $S_C = f[S_D]$ (einfach) gibt S_C öffentlich bekannt

Alice: kann Nachricht mit S_C verschlüsseln und an Bob über öffentlichen Kanal versenden

Eve: (eavesdropper, Lauscher) kann Code nicht knacken, da $S_C \to S_D$ schwer

$$C = A(S_C, N) \longrightarrow N = D(S_D, C)$$

S_C: öffentlicher Schlüssel; S_D: geheimer Schlüssel

Beispiel: <u>RSA code</u> (Rivest, Shamir, Adleman 1977)

Zahlentheorie: Seien $N, P, Q, R \in \mathbb{N}$ und $P \cdot Q = 1 \bmod(\varphi(R))$ wobei $\varphi(R)$ die Anzahl der Zahlen zwischen 1 und R die relativ prim zu R sind. Dann gilt

$$N^{P \cdot Q} = N \pmod R \tag{2}$$

für alle $N < R$ die mit R teilerfremd sind.

Man wählt $R = U \cdot V$ mit U und V zufälligen Primzahlen. Dann gilt

$$\varphi(R) = \varphi(U \cdot V) = (U-1)(V-1) \tag{3}$$

d.h. $U \cdot V \longrightarrow \varphi(U \cdot V)$ leicht. Nun wählt man P, Q so daß $P \cdot Q = 1 \bmod \varphi(R)$. Das ist ebenfalls leicht insofern man $\varphi(R)$ kennt.

"öffentlicher Schlüssel: $S_C = (P, R)$
geheimer Schlüssel: $S_D = (P, Q)$

Auffinden von Q aus P, R erfordert Umkehrung von $P \cdot Q = 1 \bmod \varphi(R)$ das die Faktorisierung von R erfordert.

Kodierung:

$$N^P = C \pmod R$$

Dekodierung

$$C^Q = N^{P \cdot Q} \pmod R$$

$$\overset{(2)}{=} N \pmod R$$

Mit den besten bisher bekannten Verfahren skaliert der Aufwand für Kodierung und Dekodierung linear mit $\log(R)$, der Aufwand zur Faktorisierung von R jedoch exponentiell mit $\log(R)$.

Die Sicherheit des RSA Schemas liegt in der Nichtexistenz eines effektiven Faktorisierungsalgorithmus.

Problem: ∄ mathematischer Beweis, daß kein effizienter Faktorisierungsalg. existiert!

4.2. Quantenschlüsselverteilung mit einzelnen qubits: Das BB84 Protokoll

Zur Erzeugung eines zufälligen, sicheren klassischen Schlüssels machen wir uns die Eigenschaft von Quantensystemen zunutze, daß nicht orthogonale Zustände durch Messung nicht eindeutig unterscheidbar sind und daß Messungen in nicht orthogonalen Basen einen Quantenzustand meßbar verändern. Dazu betrachten wir das Protokoll von Bennett und Brassard (1984):

(i) Alice versendet 4n qubits in zufällig ausgewählten Zuständen $|\uparrow_x\rangle, |\downarrow_x\rangle$ oder $|\uparrow_z\rangle, |\downarrow_z\rangle$. Die Zustände sind nicht paarweise orthogonal, können durch Messung also nicht eindeutig unterschieden werden. Bob mißt die qubits zufällig in der x oder z Basis.

(ii) Alice und Bob geben öffentlich bekannt in welcher Basis sie die qubits präpariert bzw. gemessen haben. Sie veröffentlichen natürlich nicht welche Polarisation

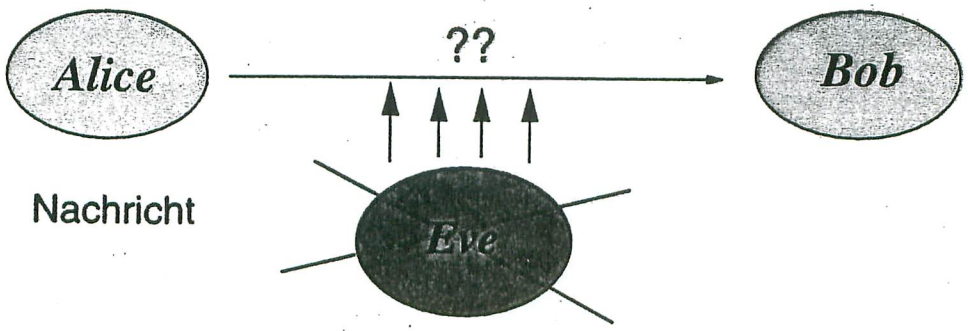
die qubits hatten ($|\uparrow\rangle$ oder $|\downarrow\rangle$ in der jeweiligen Basis). In der Hälfte aller Fälle ($2n$) werden sie in derselben (ii) Basis gearbeitet haben. Diese qubits behalten sie.

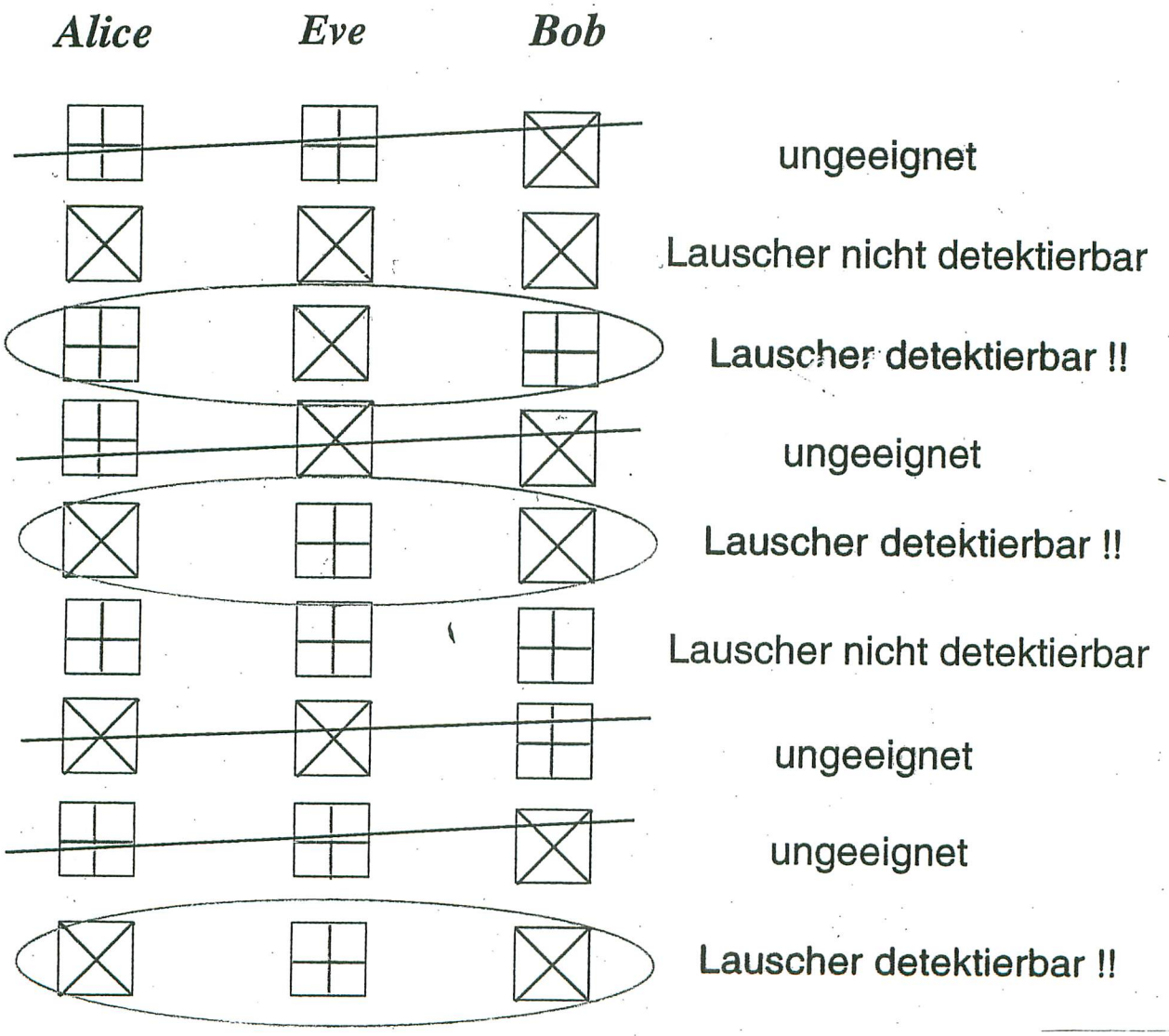
(iii) Alice und Bob wählen aus den $2n$ übriggebliebenen qubits n zufällig aus und vergleichen die präparierte und gemessene Polarisation.

(iv) Stimmen die Polarisationen in allen n Tests überein war mit an Sicherheit grenzender Wahrscheinlichkeit ($n \to \infty$) kein Lauscher in der Leitung und sie können die anderen n qubits als zufälligen Schlüssel verwenden ($|\uparrow\rangle = 1, |\downarrow\rangle = 0$). Stimmen die Polarisationen in $n/4$ Tests nicht überein war mit an Sicherheit grenzender Wahrscheinlichkeit ein Lauscher in der Leitung bzw. war der Kanal verrauscht. Dann müssen auch die n verbliebenen qubits verworfen werden.

Es stellt sich die Frage auf ob Alice und Bob die verbleibenden n qubits verwenden können, wenn weniger als $n/4$ Tests nicht übereinstimmen und wie wär die Sicherheit des Protokolls quantifizieren können.

Bennett–Brassard Protokoll





$\hat{\sigma}_x$ Präparation $\hat{\sigma}_z$ Präparation

klassische Schlüsselreinigung (classical privacy amplification) und Sicherheit des BB84 Protokolls

Potentieller Lauscher kann zwischen $|\uparrow_x\rangle, |\downarrow_x\rangle$ und $|\uparrow_z\rangle, |\downarrow_z\rangle$ nicht vollständig unterscheiden. D.h. Eve (Lauscher oder evesdropper) kann nicht Zst. messen und unbeeinflußt weitersenden bzw. kann Zst. nicht klonen die Kopie behalten und das Original weiterschicken.

$$(4)\quad \begin{aligned} U_c\,|\uparrow_z\rangle\,|\phi_0\rangle\,|\phi_M\rangle &\longrightarrow |\uparrow_z\rangle\,|\uparrow_z\rangle\,|\phi_{M'}\rangle \\ U_c\,|\uparrow_x\rangle\,|\phi_0\rangle\,|\phi_M\rangle &\longrightarrow |\uparrow_x\rangle\,|\uparrow_x\rangle\,|\phi_{M''}\rangle \end{aligned}$$

$$0 \neq |\langle\uparrow_x|\uparrow_z\rangle| = |\langle\uparrow_x|\uparrow_z\rangle|^2\,|\langle\phi_{M'}|\phi_{M''}\rangle|$$

$$\Rightarrow \quad 1 = \underbrace{|\langle\uparrow_x|\uparrow_z\rangle|}_{<1}\;\underbrace{|\langle\phi_{M'}|\phi_{M''}\rangle|}_{\leq 1} \quad \lightning$$

Falls bei den n Testbits eine Fehlerrate von ε auftritt, sind auch unter den n Schlüsselbits εn Fehler. Durch Austausch von

$$(5)\qquad n\,H(\varepsilon)$$

bits über öffentliche Kanäle können Alice und Bob diese Fehler korrigieren. Dann besitzen sie einen kleineren $n' = n(1-H(\varepsilon))$ fehlerfreien

Schlüssel. Unter der Annahme, daß alle Fehler durch Eve erzeugt wurden, hat Eve eine gewisse Information über diesen Schlüssel.

(6) $$n' H(2\varepsilon) \leq n'$$

Diese Information kann durch Verkürzung des Schlüssels vernichtet werden solange $H(2\varepsilon) < 1$. Das Verfahren dazu ist die sog. klassische Schlüsselreinigung:

$\underline{k}^{(n')}$ fehlerhaftige Schlüssel Länge n'

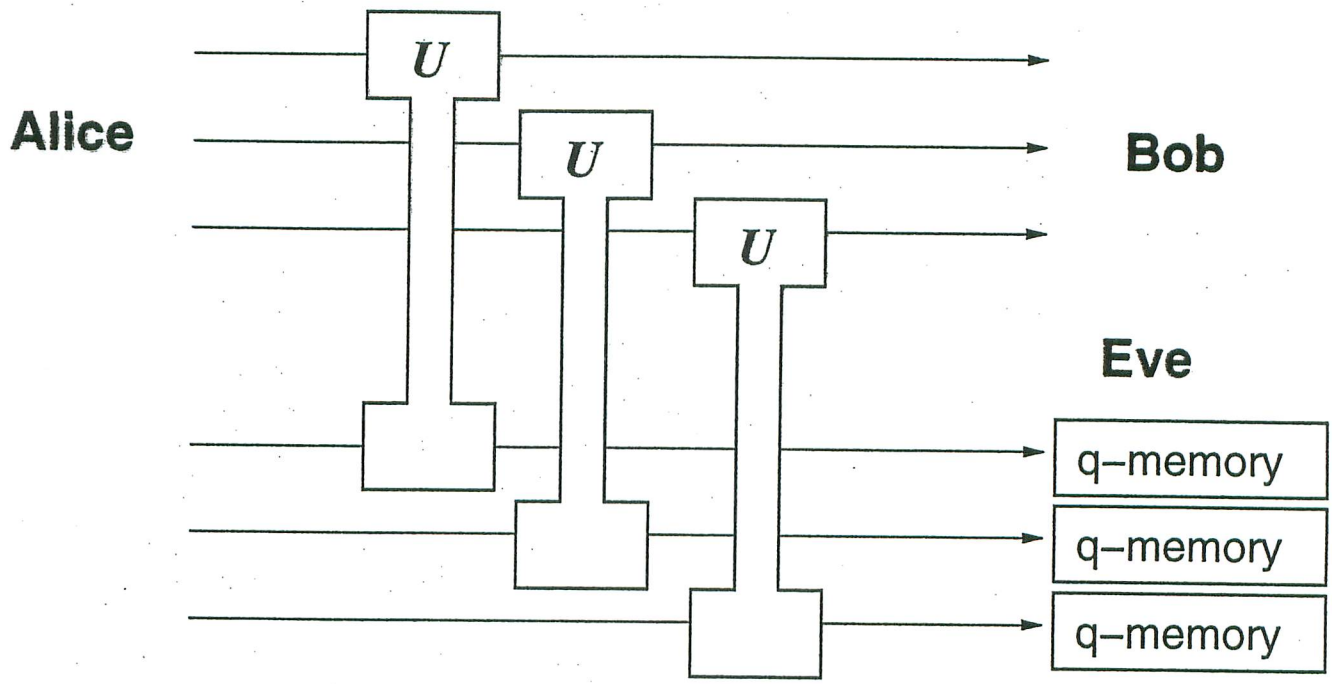
$\underline{\underline{K}}$ Zufallsmatrix $(n'-\tau) \times n'$ aus 0 und 1; wird von Alice bekannt gegeben

(7) $$\underline{k}^{(n'-\tau)} = \underline{\underline{K}}\, \underline{k}^{(n')} \pmod 2$$

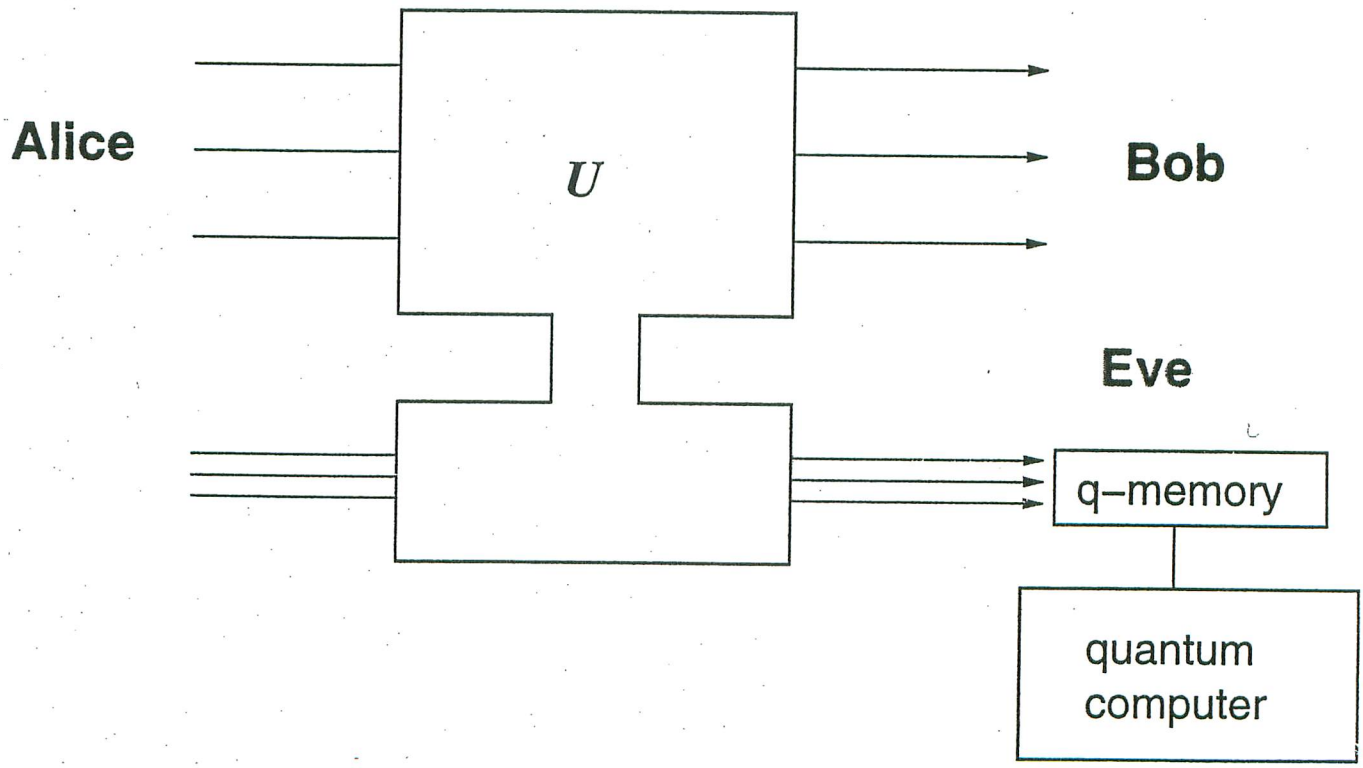
verkürzte Schlüssel. Die Information die Eve über den verkürzten Schlüssel hat ist kleiner als $(n'-\tau) H(2\varepsilon)$, falls $H(2\varepsilon) < 1$. Dies liegt an der Kompositionseigenschaft (Abschnitt 3 Gl. 3). Die Größe von τ wird durch die tolerierte Restinformation von Eve über den Schlüssel bestimmt (C. Bennett et al IEEE Int. Symp. on Information Theory 1994).

Strenge Beweise über die Sicherheit des BB84 Protokolls sind kompliziert da sie alle möglichen Attacken abdecken

incoherent attacks:



coherent attacks:



Eve wird in keinem Fall sofort Messungen ausführen, sondern Alice bit mit einem Probenbit verschränken und erst nach öffentlicher Bekanntgabe der Basis (x oder z) Messungen an den Probenbits ausführen.
Bei einem <u>inkohärenten Lauschangriff</u> verschränkt Eve Alice i-ten qubit mit individuellen Systemen mit Zust. $|E\rangle_i$:

$$(8)\quad \begin{aligned} |E\rangle\ |\uparrow_z\rangle_{Alice} &\xrightarrow{U} |E^z_{00}\rangle\ |\uparrow_z\rangle_{Alice} + |E^z_{01}\rangle\ |\downarrow_z\rangle_{Alice} \\ |E\rangle\ |\downarrow_z\rangle_{Alice} &\longrightarrow |E^z_{10}\rangle\ |\uparrow_z\rangle_{Alice} + |E^z_{11}\rangle\ |\downarrow_z\rangle_{Alice} \end{aligned}$$

wobei die $|E^z_j\rangle$ <u>unnormiert</u> sind. Entsprechend

$$(9)\quad \begin{aligned} |E\rangle\ |\uparrow_x\rangle &\longrightarrow |E^x_{00}\rangle\ |\uparrow_x\rangle_{Alice} + |E^x_{01}\rangle\ |\downarrow_x\rangle_{Alice} \\ |E\rangle\ |\downarrow_x\rangle &\longrightarrow |E^x_{10}\rangle\ |\uparrow_x\rangle_{Alice} + |E^x_{11}\rangle\ |\downarrow_x\rangle_{Alice} \end{aligned}$$

wobei

$$(10)\quad |E^x_{00/11}\rangle = \frac{|E^z_{00}\rangle + |E^z_{10}\rangle \pm \left(|E^z_{01}\rangle + |E^z_{11}\rangle\right)}{2}$$

$$|E^x_{10/11}\rangle = \frac{|E^z_{00}\rangle - |E^z_{10}\rangle \pm \left(|E^z_{01}\rangle - |E^z_{11}\rangle\right)}{2}$$

Eve's Strategie muß sein (i) die Wahrscheinlichkeit so gering wie möglich zu halten, daß Alice und Bob eine Diskrepanz ihrer Testbits feststellen,

$$(11)\quad \langle E^x_{ij} | E^x_{ij}\rangle;\ \langle E^z_{ij} | E^z_{ij}\rangle \overset{!}{=} \min \quad \text{für } i \neq j$$

(ii) die Wahrscheinlichkeit des korrekten Ratens des von Alice gesendeten qubits nach Bekanntgabe der Basis maximieren.

Falls Eve erfährt, daß das ite qubit in der z Basis gesendet wurde, muß sie die Fälle

$$|\uparrow_z\rangle_{Alice} \rightarrow \rho_{Eve}^{\uparrow_z} = Tr_{Alice}\left[U|E\rangle|\uparrow_z\rangle_A \left(U|E\rangle|\uparrow_z\rangle_A\right)^+\right]$$

(12)
$$= |E_{00}^z\rangle\langle E_{00}^z| + |E_{01}^z\rangle\langle E_{01}^z|$$

$$|\downarrow_z\rangle_{Alice} \rightarrow \rho_{Eve}^{\downarrow_z} = Tr_{Alice}\left[U|E\rangle|\downarrow_z\rangle_A \left(U|E\rangle|\downarrow_z\rangle_A\right)^+\right]$$

(13)
$$= |E_{11}^z\rangle\langle E_{11}^z| + |E_{10}^z\rangle\langle E_{10}^z|$$

unterscheiden. Dazu mißt sie die Observable

(14)
$$P_z = \rho_{Eve}^{\uparrow_z} - \rho_{Eve}^{\downarrow_z}$$

Die Wahrscheinlichkeit der Fehlinterpretation von Eve ist somit

(15)
$$Tr\{\rho^{\uparrow_z}\rho^{\downarrow_z}\} \stackrel{!}{=} min$$

Gleichzeitig muß aber auch

(16)
$$Tr\{\rho^{\uparrow_x}\rho^{\downarrow_x}\} \stackrel{!}{=} min$$

Aus (11), (15), (16) läßt sich die maximale Information die Eve durch einen inkohärenten Rauschangriff gewinnen

kann abschätzen. Für kohärente Lauschangriffe, d.h. solche bei denen Eve allg. unitäre Operationen zwischen allen qubits von Alice und beliebigen Probenqubits ausführt, ist die Diskussion weitaus komplizierter. Für allg. Sicherheitsbeweise siehe: H.K. Lo and H.F. Chau, Science 283 (1999) 2050, P.W. Shor and J. Preskill Phys. Rev. Lett. 85 (2000) 441. Im Zweiten Beweis werden Eigenschaften von CSS Quantencodes ausgenutzt.

4.3. Quantenschlüsselverteilung mit EPR Paaren: Das Deutsch-Ekert Protokoll

In dem zweiten Verfahren zur Erzeugung eines geheimen Quantenschlüssels machen wir uns die Eigenschaft zu Nutze daß ein maximal verschränktes Paar von qubits z.B. ein Bell Zustand

$$(17) \qquad \frac{1}{\sqrt{2}}\left(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B\right) = |\Psi^-\rangle$$

bei einer Messung absolut zufällig und absolut korreliert bei Alice und Bob eine 0 oder 1 liefert und somit eine ideale Quelle für einen zufälligen Schlüssel ist. Darüberhinaus kann ein reiner Zustand zweier Parteien mit keiner dritten Partei verschränkt sein. D.h. die Zustandsreduktion durch Messung von Alice (oder Bob) kann an keine dritte Partei Information liefern.

(i) Alice besitzt eine Quelle von EPR Paaren im Zustand

(18) $$\frac{1}{\sqrt{2}}\left(|\uparrow_x\rangle|\downarrow_x\rangle - |\downarrow_x\rangle|\uparrow_x\rangle\right)$$

Eines der beiden qubits verschickt sie an Bob.

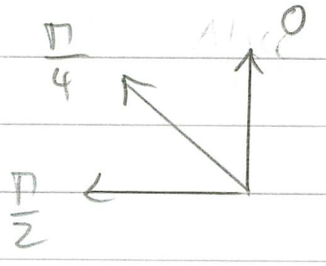
(ii) Alice und Bob führen statistisch Spinmessungen aus

(19) $$\vec{\sigma}_{\vec{n}} = \vec{n} \cdot \vec{\sigma}$$

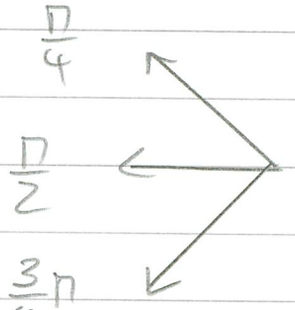
in den Richtungen

Alice: $\vec{n} = \left\{\vec{e}_x, \frac{1}{\sqrt{2}}(\vec{e}_x + \vec{e}_y), \vec{e}_y\right\}$

Bob: $\vec{n} = \left\{\frac{1}{\sqrt{2}}(\vec{e}_x + \vec{e}_y), \vec{e}_y, \frac{1}{\sqrt{2}}(-\vec{e}_x + \vec{e}_y)\right\}$



Alice



Bob

(iii) Alice und Bob tauschen öffentlich Information über gewählten $\vec{n}$ aus.

(iv) An der Menge der Paare bei denen Messungen in verschiedenen Richtungen durchgeführt wurden,

werden die Bellschen Ungleichungen überprüft.
Gemäß Gl. (2-6) gilt für einen Bell-Zustand:

$$(20)\qquad E_{EPR}(\varphi_A, \varphi_B) = -\cos(\varphi_A - \varphi_B)$$

Clauser-Horn-Shimony-Holt (CHSH) Variante der Bell'schen Ungleichung ($\phi_1^A = 0$, $\phi_2^A = \frac{\pi}{4}$, $\phi_3^A = \frac{\pi}{2}$; $\phi_1^B = \frac{\pi}{4}$, $\phi_2^B = \frac{\pi}{2}$, $\phi_3^B = \frac{3\pi}{4}$)

$$(21)\qquad S = E(\phi_1^A, \phi_2^B) + E(\phi_1^A, \phi_3^B) + E(\phi_2^A, \phi_3^B) - E(\phi_2^A, \phi_2^B)$$

$$(22)\qquad S_{EPR} = -\underbrace{\cos\left(\frac{\pi}{2}\right)}_{0} - \underbrace{\cos\left(\frac{3\pi}{4}\right)}_{\sqrt{2}} - \underbrace{\cos\left(\frac{\pi}{2}\right)}_{0} + \underbrace{\cos\left(\frac{\pi}{4}\right)}_{\sqrt{2}}$$

$$= 2\sqrt{2}$$

klassisches Ergebnis: $p(\theta_A, \theta_B)$ Wahrscheinlichkeitsverteilung, daß Spin in A Orientierung θ_A und in B θ_B hat

$$(23)\qquad S_{kl} = \int_{-\pi/2}^{\pi/2} d\theta_A\, d\theta_B\; p(\theta_A, \theta_B) \Big\{ \cos(\phi_1^A - \theta_A)\cos(\phi_2^B - \theta_B) + \cos(\phi_1^A - \theta_A)\cos(\phi_3^B - \theta_B) + \cos(\phi_2^A - \theta_A)\cos(\phi_3^B - \theta_B) - \cos(\phi_2^A - \theta_A)\cos(\phi_2^B - \theta_B) \Big\}$$

$$S_{kl} = \int_{-\pi/2}^{\pi/2} d\theta_A \, d\theta_B \; p(\theta_A, \theta_B) \; \sqrt{2} \cos(\theta_A - \theta_B)$$

$\Rightarrow$

$$-\sqrt{2} \leq S_{kl} \leq \sqrt{2} \tag{24}$$

Die Bellschen Ungleichungen (CHSH Ungleichungen) werden nur durch rein maximal verschränkte Zustände (Bell Zustände) maximal verletzt. Für den Alice und Bob daß die Testmessungen $S = 2\sqrt{2}$ liefern, können sie sicher sein, daß kein Lauscher in der Leitung war.

(iv) Die Paare bei denen gleiche Meßrichtungen verwendet wurden liefern einen Satz zufälliger strong korrelierter Bits 0 und 1 die als Schlüssel verwendet werden können.

Auch hier tat sich die Frage auf, was machen Alice und Bob wenn

$$2\sqrt{2} > S_{mess} > \sqrt{2} \quad ? \tag{25}$$

Wir werden sehen, daß es möglich ist aus einem großen Satz nicht maximal verschränkter Teilchenpaare einen kleineren Satz nahezu maximal verschränkter Paare zu destillieren.

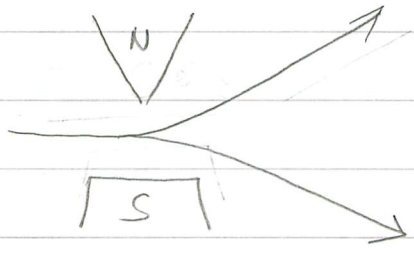
4.4. Verschränkungsreinigung (Quantum privacy amplification)

Deutsch, Ekert, Jozsa, Macchiavello, Popescu, Sanpera PRA 54, 3824 (1996); Konvergenzbeweis: Ch. Macchiavello PLA 246, 385 (1998)

Idee: Destillation von Teilchen in reinem Zustand; ONB $\{|0\rangle, |1\rangle\}$ (später Verallgemeinerung auf Teilchenpaare)

(26) $$\rho = f\,|0\rangle\langle 0| + (1-f)\,|1\rangle\langle 1|$$

Im Prinzip Destillation durch Messung möglich



Frage: Ist dies auch ohne Messung möglich? Das ist wichtig für Verschränkungsreinigung. Antwort: Ja

(27) $$\rho \longrightarrow \rho \otimes \underset{AA}{|0\rangle\langle 0|} \qquad \text{Anzilla}$$

$$\xrightarrow{CNOT} f\,|0\rangle\langle 0| \otimes \underset{AA}{|0\rangle\langle 0|} + (1-f)\,|1\rangle\langle 1| \otimes \underset{AA}{|1\rangle\langle 1|}$$

Messung des Anzilla qubits: Projektion auf $|0\rangle\langle 0|$ bzw. $|1\rangle\langle 1|$ ohne Messung des ursprünglichen qubits. Problem: Man benötigt reinen Zustand um gemischten Zustand zu reinigen. Man kann den gemischten Zustand ρ jedoch

mit Hilfe eines zweiten qubits ins selben gemischten Zustand reinigen:

$$\rho_{AB} = \rho\otimes\rho = \left(f|0\rangle_A\langle 0| + (1-f)|1\rangle_A\langle 1|\right)\left(f|0\rangle_B\langle 0| + (1-f)|1\rangle_B\langle 1|\right)$$

CNOT

(28)

$$\rho'_{AB} = \left(f^2|0\rangle_A\langle 0| + (1-f)^2|1\rangle_A\langle 1|\right)|0\rangle_B\langle 0|$$

$$+ f(1-f)\left(|0\rangle_A\langle 0| + |1\rangle_A\langle 1|\right)|1\rangle_B\langle 1|$$

Projektion auf $|0\rangle_{BB}\langle 0|$ durch Messung von B; Messungen die $|1\rangle_B$ liefern werden verworfen:

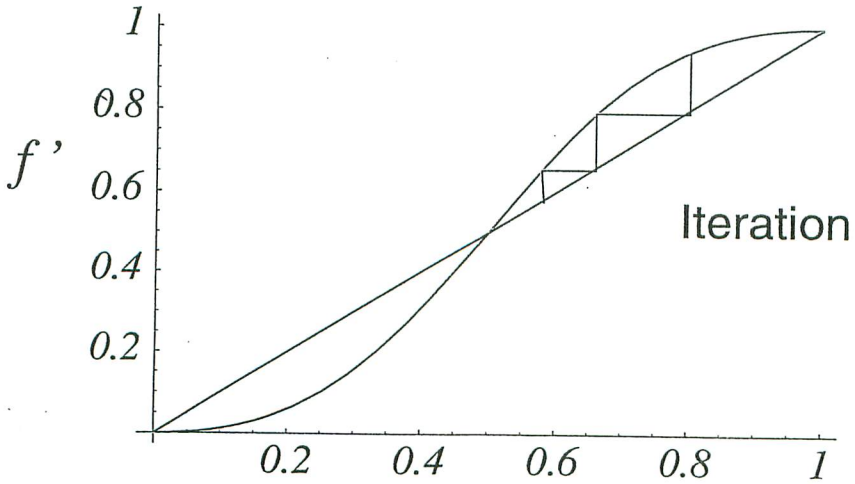
(29)

$$\rho_A' = \frac{f^2|0\rangle_{AA}\langle 0| + (1-f)^2|1\rangle_{AA}\langle 1|}{f^2+(1-f)^2}$$

$$= f'|0\rangle_{AA}\langle 0| + (1-f')|1\rangle_{AA}\langle 1|$$

(30)

$$\boxed{f' = \frac{f^2}{f^2+(1-f)^2}}$$



- iterative Anwendung führt auf $f' \to 1$ falls $f > 0.5$
- Ensemble bei jedem Schritt auf ein Viertel reduziert!

Verschränkungsreinigung: N vom Teilchenpaare

Ensemble von Paaren in gemischten Zustand

$$S_{AB} = A|\phi_+\rangle\langle\phi_+| + B|\psi_-\rangle\langle\psi_-| + C|\psi_+\rangle\langle\psi_+|$$

(31)

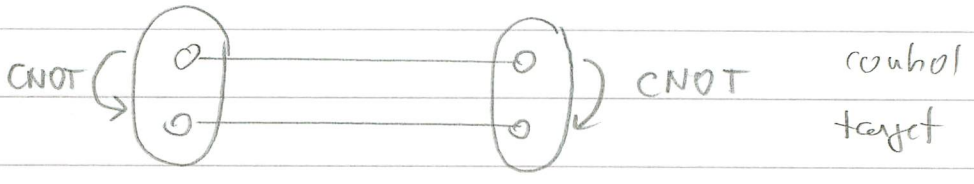
$$+ D|\phi_-\rangle\langle\phi_-| \qquad \text{O.B.d.A sei } A \geq B, C, D$$

$\{|\phi_\pm\rangle, |\psi_\pm\rangle\}$ Bellzustände von Alice und Bob

(i) Alice führt Operation $U_A = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix}$

Bob führt Operation $U_B = U_A^{-1} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}$ aus

(ii) Alice und Bob führen jeweils ein CNOT Gatter an einem Paar von Paaren aus



(iii) Alice und Bob führen Spin Messung jeweils am target bit aus und vergleichen Messergebnis über einen öffentlichen Kanal. Falls die Ergebnisse übereinstimmen behalten sie die control bits, ansonsten verwerfen sie diese.

Durch Nachrechnen aller Fälle kann man leicht zeigen, daß für die behaltenen Paare von target qubits gilt

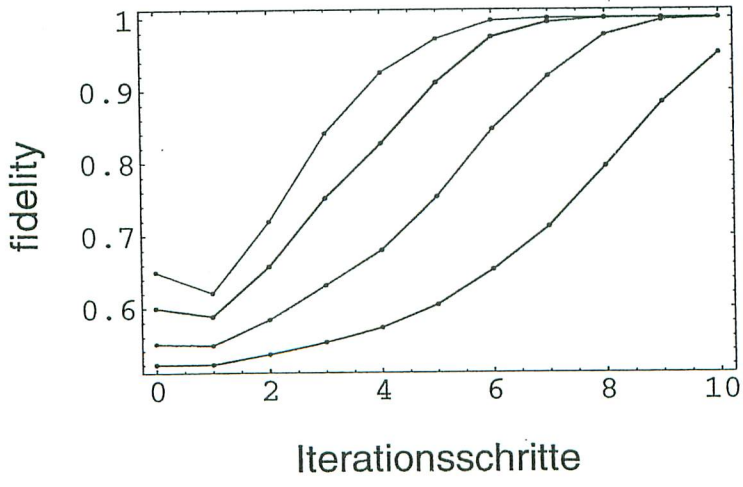
(32)
$$A' = \frac{A^2+B^2}{N} \qquad B' = \frac{2CD}{N}$$
$$C' = \frac{C^2+D^2}{N} \qquad D' = \frac{2AB}{N}$$

(33) $$N = (A+B)^2 + (C+D)^2$$

Falls der Anfangswert $A > \frac{1}{2}$ ist, hat die Iteration der Abbildung (32) einen Fixpunkt

(34) $$A' \to 1 \qquad B', C', D' \to 0$$

Verschraenkungsdestillation nach Deutsch et al.



Gl. (32) kann wie folgt interpretiert werden

$$\Phi_+ \otimes \Phi_+ \text{ oder } \Psi_- \otimes \Psi_- \longrightarrow \Phi_+$$

$$\Psi_+ \otimes \Phi_- \longrightarrow \Psi_-$$

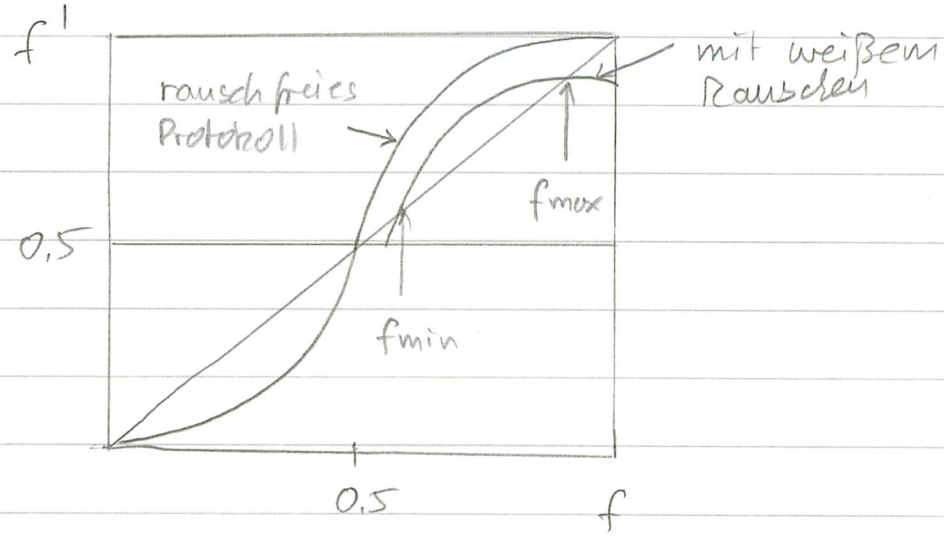
$$\Psi_+ \otimes \Psi_+ \text{ oder } \Phi_- \otimes \Phi_- \longrightarrow \Psi_+$$

$$\Phi_+ \otimes \Psi_- \longrightarrow \Phi_-$$

Alle anderen Kombinationen (z.B $\Phi_+ \otimes \Psi_+$ oder $\Phi_+ \otimes \Phi_-$) führen zu unterschiedlichen Messresultaten für die target bits.

Verschränkungsreinigung bei Vorhandensein von Rauschen

Bisher waren wir davon ausgegangen, daß das Reinigungsverfahren fehlerfrei durchgeführt werden kann.
Falls die Operationen fehlerbehaftet sind, ist eine Reinigung nur noch mit Anfangsfidelity $f \geq f_{min} > \frac{1}{2}$ möglich. Die asymptotische fidelity erreicht nicht mehr den Wert 1: $f' \rightarrow f'_{max} < 1$. Verschiedene Rauschprozesse sind von Briegel, Dür, Cirac und Zoller PRA 59, 169 (1999), PRL 81, 5932 (1998) und Giedke Briegel, Cirac und Zoller PRA 59, 2641 (1999) untersucht worden.



Mit zunehmender Wahrscheinlichkeit p eines Fehlers pro Operation nähern sich die Werte von fmin und fmax an

exakter Wert hängt von verwendetem Protokoll ab

Unterhalb einer best. Fehlerwahrscheinlichkeit (einige %) ist Verschränkungsreinigung möglich aber mit $f_{max} < 1$ d.h. es ist nicht möglich reine Bellpaare zu destillieren. Briegel und Aschauer haben jedoch gezeigt, daß die Verschränkungsreinigung stets dazu führt, daß nur eine Verschränkung der Paare mit den Meßapparaturen und der Laborumgebung übrigbleibt, ein Rauschen jedoch asymptotisch faktorisiert. (PRL 88, 047902 (2002); PRA 66, 032302 (2002))

4.5. Quantenrepeater: Verschränkungserzeugung über makroskopische Abstände

Um Quantenkryptographie oder Teleportation über große Abstände betreiben zu können, bedarf es der Erzeugung von maximal verschränkten Paaren über große Entfernung.

Problem: (i) Quellen von max. verschränkten Teilchenpaaren erfordern lokale Wechselwirkungen

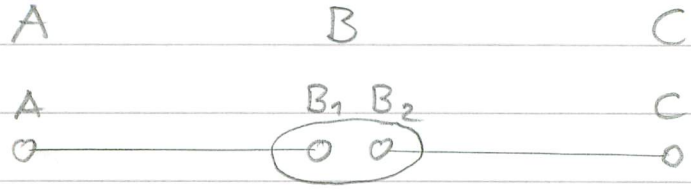
(ii) Dekohärenzwahrscheinlichkeit bei Transport eines qubits skaliert exponentiell mit der Länge l der Übertragungsstrecke, d.h. $F \sim e^{-\alpha l}$

Reinigungsprotokolle erlauben nun diese Dekohärenzeffekte zu beseitigen, wenn Ausgangsfidelity $F > F_{min}$. D.h. F_{min} legt maximale Distanz l_{max} fest $e^{-\alpha l_{max}} = F_{min}$.

klass. Lösungsansatz: Verstärkerstationen (repeater) in regelmäßigen Abständen; $\Rightarrow$ Übertragung auf q.m. Systeme?

Als ersten wichtigen Bestandteil eines quantum repeaters betrachten wir das sog. entanglement swapping (C.H. Bennett et al. PRL 70, 1895 (1993), H. Zukowski et al. PRL 71, 4287 (1993)), d.h. die Erzeugung eines maximal verschränkten Zustandes zwischen A und C aus zwei paaren A-B und B-C maximal verschränkter Zustände:

entanglement swapping



$$|\Psi\rangle = |\Phi_+\rangle_{AB_1} |\Phi_+\rangle_{B_2C}$$

$$= \frac{1}{2}\left(|0\rangle_A|0\rangle_{B_1} + |1\rangle_A|1\rangle_{B_1}\right)\left(|0\rangle_{B_2}|0\rangle_C + |1\rangle_{B_2}|1\rangle_C\right)$$

$$= \frac{1}{2\sqrt{2}}\Big\{|0\rangle_A\left[\Phi_+ + \Phi_-\right]_{B_1B_2}|0\rangle_C + |0\rangle_A\left[\Psi_+ + \Psi_-\right]_{B_1B_2}|1\rangle_C$$

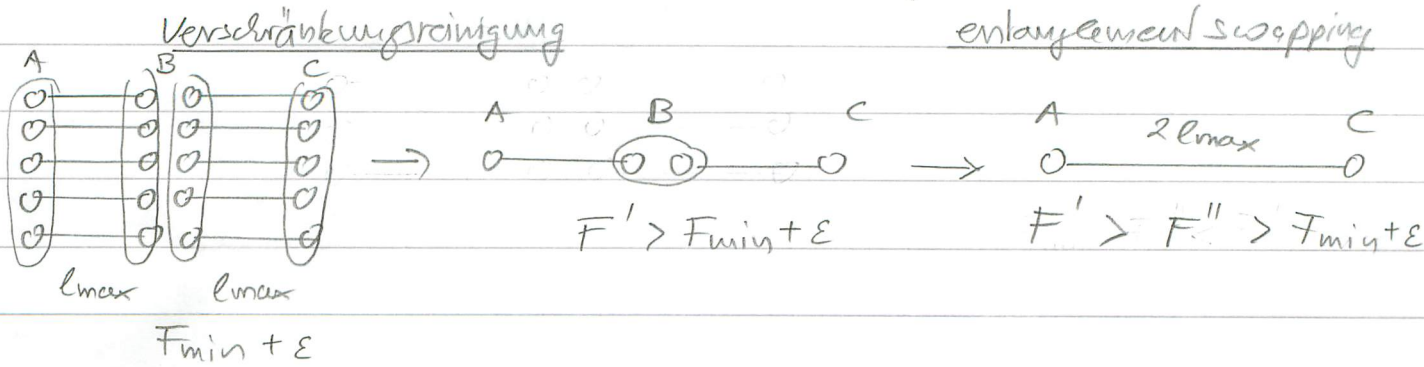
(35) $$+ |1\rangle_A\left[\Psi_+ - \Psi_-\right]_{B_1B_2}|0\rangle_C + |1\rangle_A\left[\Phi_+ - \Phi_-\right]_{B_1B_2}|1\rangle_C\Big\}$$

$$= \frac{1}{2}\Big\{|\Phi_+^{AC}\rangle|\Phi_+^{B_1B_2}\rangle + |\Phi_-^{AC}\rangle|\Phi_-^{B_1B_2}\rangle$$

$$+ |\Psi_+^{AC}\rangle|\Psi_+^{B_1B_2}\rangle + |\Psi_-^{AC}\rangle|\Psi_-^{B_1B_2}\rangle\Big\}$$

Bell-Messung an $B_1 + B_2$ projiziert auf einen der vier Bell-Zustände $|\Phi_\pm^{AC}\rangle$, $|\Psi_\pm^{AC}\rangle$ von A und C.

Eine Kombination von Verschränkungsreinigung (siehe 4.4.) und entanglement swapping erlaubt es verschränkte Paare über Distanzen $\ell > \ell_{max}$ zu erzeugen:



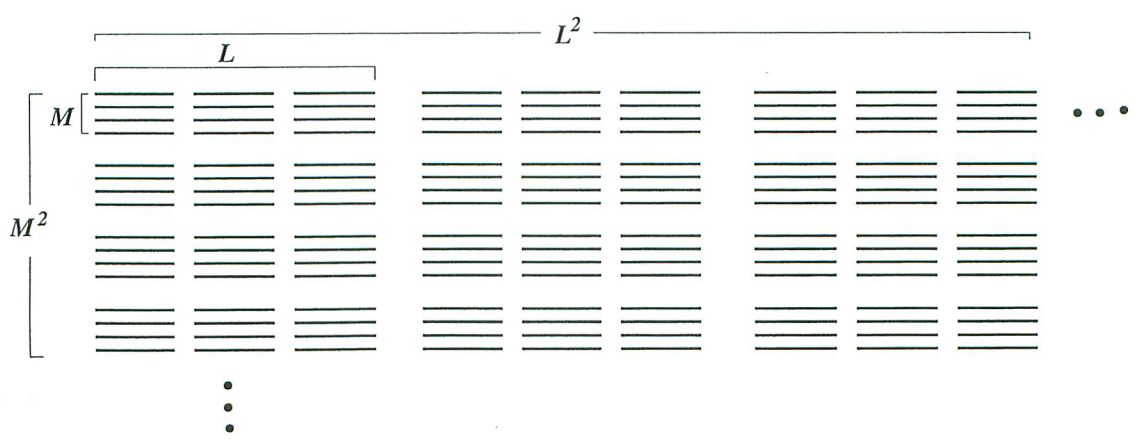
Um Verschränkung über große Distanzen $\ell = N l_0$, $l_0 < l_{max}$ zu erreichen, kann obige Prozedur iteriert werden. Dazu muß ein Protokoll gefunden werden, bei dem die erforderlichen Ressourcen nicht exponentiell mit N anwachsen. Eine schrittweise Vergrößerung der Verschränkungsdistanz zum Abschnitte der Länge l_{max} ist offensichtlich ungeeignet da jeder Schritt die Anzahl der Teilchenpaare um einen bestimmten Faktor η reduziert und damit die Gesamtzahl der benötigten Teilchenpaare wie

$$(36) \qquad \left(\frac{1}{\eta}\right)^N = \eta^{-N} = 2^{N(-\log_2 \eta)}$$

skaliert. Gleichsam würde die Zeit zur Vollendung des Protokolls exponentiell mit N skalieren.

Um diese Probleme zu beheben muß ein <u>verschachteltes Reinigungs- und Verknüpfungsprotokoll</u> verwendet werden. (H.J. Briegel et al Phys. Rev. Lett. <u>81</u>, 5932 (1998); W. Dür et al. Phys. Rev. A <u>59</u>, 169 (1999))

<u>verschachteltes Reinigungsprotokoll</u>



Wenn $\ell = N l_0 \gg l_{max}$ Verknüpfung von allen N Teilstücken nicht möglich. Sei $L l_0 < l_{max} \Rightarrow$ Verknüpfung von $L \ll N$ Teilstücken mittels entanglement swapping möglich. Sei O.B.d.A. $N = L^n$.

(i) Blockweise Verknüpfung von jeweils L Segmenten.

(ii) Verschränkungsreinigung in jedem Block und Destillation eines hinreichend gut verschränkten Paares mit Abstand L aus M Paaren der Länge 1 (Länge in Einheiten von l_0)

(iii) Iteration der Prozedur

Verschränkungsdistanz wächst wie L^k mit Anzahl k der Iterationen. Die Gesamtzahl der benötigten elementaren Paare verschränkter Teilchen ist (im Mittel)

$$R = (ML)^n = L^n M^n = N L^{n \log_L M} = N N^{\log_L M}$$

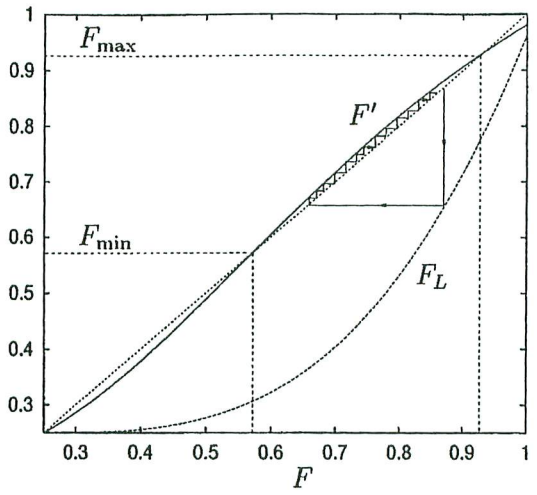
(37)

$$= N^{\log_L M + 1}$$

polynomiales Anwachsen in N

Zur Berechnung der Fidelity des repeater Protokolls kann man vom Prinzip her wie in Gl. (28) – (30) vorgehen, wobei bei allen 1-bit und 2-bit Operationen der Reinigungsschritte und des entanglement swappings sowie bei der [illegible] entanglement swapping enthaltenen Bell-

Messung Fehler zulässt.



Dür et al PRA 59, 169 (1999)

F_L - fidelity nach Verknüpfung von L Segmenten

F' - fidelity nach Reinigungsschritt

prinzipieller Operationszyklus des vorgestellten Reinigungsprotokolls