5. Quantum cryptography

Cryptos	(greek)	hidden
logos	(greek)	word

The need for secure communication is as old as human civilization. In this chapter we will discuss some problems of the most commonly used classical cryptography methods based on open keys and show that elements of quantum mechanics can be used to solve them

5.1 Some elements of classical cryptography

basic tasks of cryptography

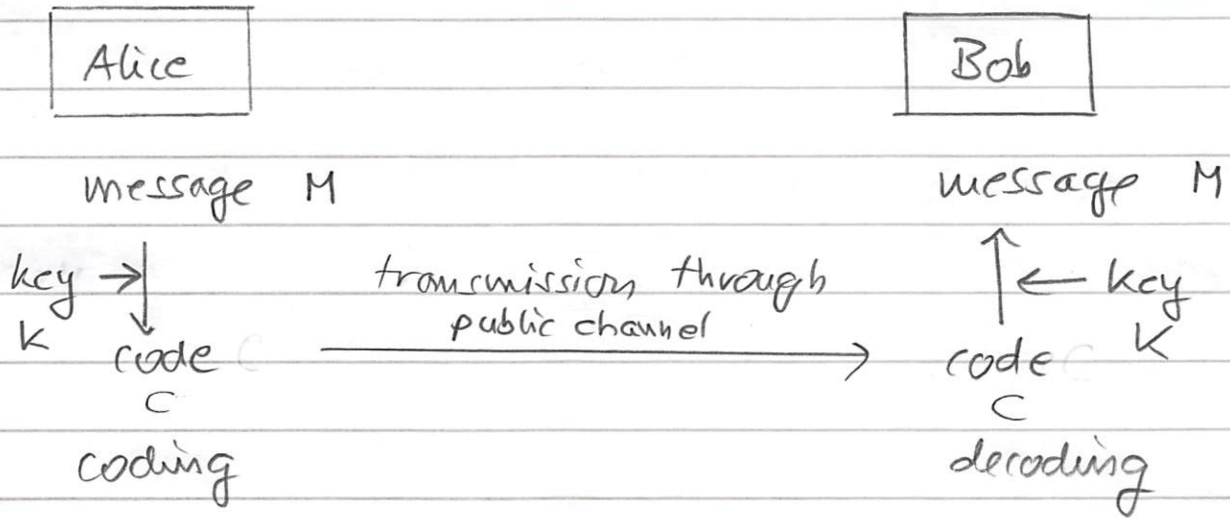
(i) secure transmission of classical information (bits) from A (Alice) to B (Bob)

(ii) autentification: How does Bob know that he is actually talking to Alice and not to a third party pretending to be Alice?

we will only consider task (i) in this lecture.

Security of a cryptographic code

- in the past: secret of encoding procedure
- today: encoding procedure known, but secret key



$$M \rightarrow C = C(K,M) \qquad\qquad M = D(K,C)$$

identical key

- example: Vernam cipher (Gilbert Vernam 1917)

message	0	0	1	1	0	1	0
$\oplus$ mod 2 key	1	0	0	1	1	0	1
code	1	0	1	0	1	1	1

decoding

code	1	0	1	0	1	1	1
$\oplus$ mod 2 key	1	0	0	1	1	0	1
message	0	0	1	1	0	1	0

- Shannon (1949): Vernam protocoll is secure, if

  (i) key is random and has the same length than message
  (ii) key is used only once

in practice this is not done as it is an overkill

$\Rightarrow$ secure cryptography $\hat{=}$ generation and distribution of secret key

<u>public key distribution</u>

use two different keys K_C and K_D for coding and decoding, which of course are interrelated, i.e.

(1) $K_C = f[K_D]$ $\qquad$ $K_D = f^{-1}[K_C]$

<u>f</u> is chosen such that its evaluation is <u>simple</u>, i.e. there is an efficient algorithm to evaluate f, while no efficient algorithm exists to evaluate f^{-1}, i.e. evaluation of <u>f^{-1}</u> is <u>hard</u>

NP problem

- solving $f^{-1}[K_C]$ is hard (effort scales more than polynomially with the size of K_C)

- but checking the result, i.e. evaluating $f[f^{-1}[K_C]] = f[K_D]$ is simple (effort scales only polynomially with the size of K_D)

public key protocol:

Bob: chooses $K_D \rightarrow$ calculates $K_C = f[K_D]$
announces K_C publically

Alice: uses K_C to encode message and transmits code over public channel to Bob

Eve: cannot decode code since $K_C \rightarrow K_D$ is a hard problem

example: RSA code (Rivest, Shamir, Adleman 1977

- number theory: let $M, P, Q, R \in \mathbb{N}$ and let $P \cdot Q = 1 \mod (\varphi(R))$, where $\varphi(R)$ is the number of integers between 1 and R that a relatively prime to R (i.e. do not have a common divisor with R). If U and V are relatively prime, then

(2) $$\varphi(U \cdot V) = \varphi(U)\, \varphi(V)$$

Thus in particular if U, V are prime numbers

(3) $$\varphi(U \cdot V) = (U-1)(V-1)$$

and can easily be calculated.
number theory now says

(4) $$M^{P \cdot Q} = M \bmod (R)$$

for all $M < R$ which are relatively prime to R.

(i) choose 2 random prime numbers U, V
$R = U \cdot V$ and $\varphi(R) = (U-1)(V-1)$

(ii) choose an integer P that is relatively prime to $\varphi(R)$ and $1 < P < \varphi(R)$

(iii) find the integer Q such that

$$P \cdot Q = 1 \bmod (\varphi(R))$$

Q can be calculated easily, provided one knows the factorization $R = U \cdot V$ of R into prime numbers!

code: P, Q, R — U, V and $\varphi(R)$ no longer needed

(5)

public key	K_C	$= \{P, R\}$
secret key	K_D	$= \{P, Q\}$

<u>coding</u> $C = M^P \mod R$

<u>decoding</u> $M = C^Q \mod R = M^{P \cdot Q} \mod R$

$= M$

With the best known algorithms the effort for coding and decoding scales with $\log(R)$, the effort to factorize R, i.e. to find U, V with $R = U \cdot V$ scales exponentially with $\log(R)$!

$\Rightarrow$ security of RSA scheme lies in non-existence of an effective algorithm for factorization!

factorization is believed to be NP hard, i.e.

$29 \cdot 41 \Rightarrow 1189$ simple

but $1513 \Rightarrow \underbrace{\boxed{?} \times \boxed{?}}_{17 \times 89}$ difficult

<u>problem:</u> $\nexists$ mathematical proof that factorization is NP hard!

5.2 quantum key distribution with individual qubits: the BB84 protocol

To generate secure keys we can use the property of quantum systems that non-orthogonal states cannot be distinguished by measurement and that measurements of states prepared in a non-orthogonal basis will necessarily modify the states in a measurable way. Specifically we consider the protocol by Charles Bennett and Gil Brassard (1984)

$$\text{qubits in} \quad |\uparrow_z\rangle, |\downarrow_z\rangle \quad \text{or} \quad |\uparrow_x\rangle, |\downarrow_x\rangle$$
$$= |1\rangle, |0\rangle \quad \text{or} \quad |+\rangle, |-\rangle$$

(i) Alice sends 4N qubits randomly prepared in

$$\{|1\rangle, |0\rangle, |+\rangle, |-\rangle\}$$

Since the states are non-orthogonal, no measurement strategy exists that would allow to uniquely determine which qubits have been sent without prior knowledge

Bob the measures all 4N qubits in a random basis i.e. in σ_x or σ_z basis

(ii) Alice and Bob communicate publicly which basis they have used, but <u>not</u> if they have measured $|1\rangle$ or $|0\rangle$ in the case of σ_z

or $|+\rangle$ or $|-\rangle$ in the case of σ_x.

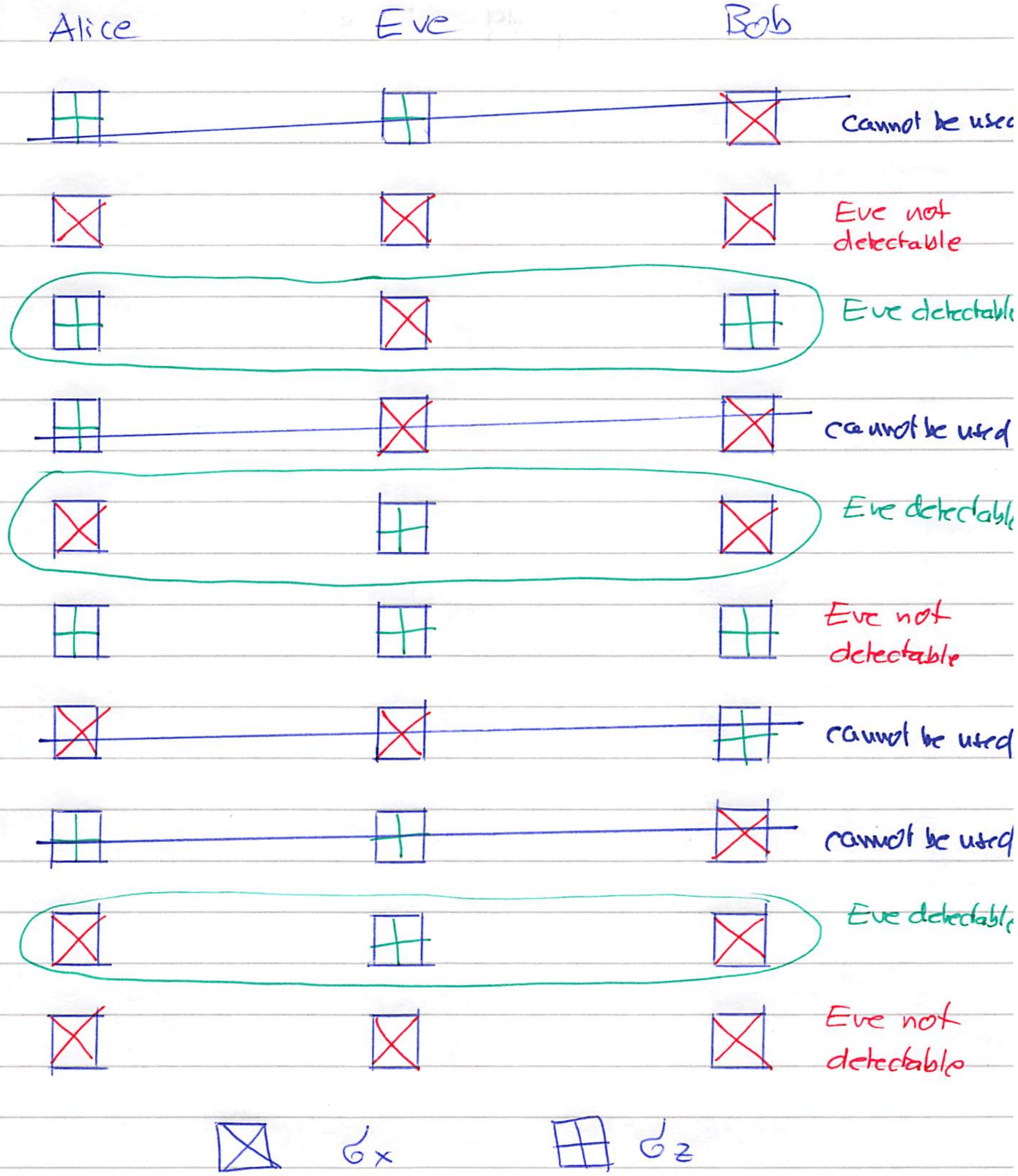
In 2N cases they will have accidentally chosen the same basis. They keep these qubits and discard the others

(iii) Alice and Bob take N of the remaining qubits (randomly) and compare publicly the prepared with the measured polarization

(iv) If their results agree in all N cases ($N \to \infty$) they can conclude that there was no evesdropp in the line. Then they use the remaining N qubits as random key. If their results disagree in N/4 cases ($N \to \infty$) then there was an evesdropper in the line with certainty and they have to discard all qubits.

$\Rightarrow$ What to do if there is some disagreement but it is less than N/4

$\Rightarrow$ classical key purification (classical privacy amplification)


Alice
Eve
Bob
cannot be used
Eve not detectable
Eve detectable
cannot be used
Eve detectable
Eve not detectable
cannot be used
cannot be used
Eve detectable
Eve not detectable
σx
σz

classical privacy amplification

If N testbits have an error rate ε, than among the N bits of the key $N\varepsilon$ are erroneous. Exchanging

(6) $$N H(\varepsilon)$$

bits via a public channel, Alice and Bob can correct this error. This leads to a smaller, a <u>sifted key</u> with

(7) $$N' = N\left(1 - H(\varepsilon)\right)$$

bits and no errors. Assuming that all errors are created by Eve, the amount of information Eve possesses about the key is

(8) $$N' H(2\varepsilon) \leq N'$$

As long as $H(2\varepsilon) < 1$ sifting the key reduces the information that Eve has about the sifted key.

$\underline{K}^{(n')}$ error corrected key of length n'

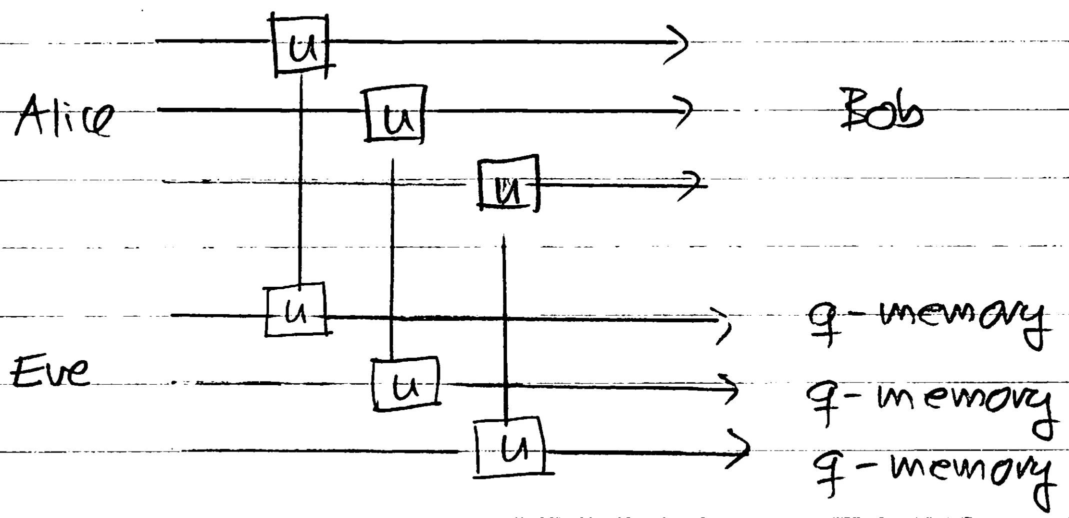
$\underline{\underline{R}}$ random matrix $(n' - \tau) \times n'$ of 0 and 1 announced by Alice

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

information of Eve about sifted key: $(n'-\tau)\, H(2\varepsilon)$
τ is chosen to match a tolerance threshold of information left to Eve

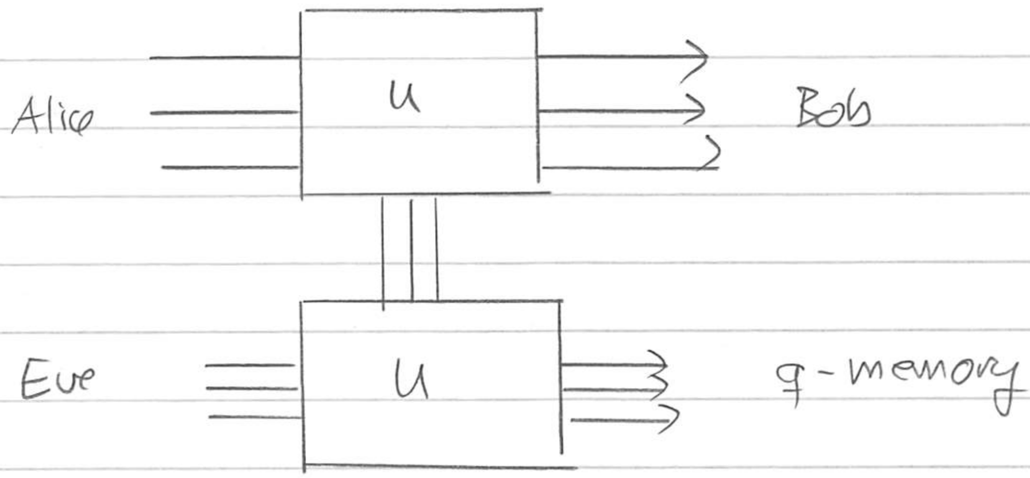
Mathematical proofs about quantifyable security of the BB84 protocol are involved and have to consider different attacks.

- Eve will not perform measurements immediately but entangle the qubits of the key with auxilla qubits and perform measurements on those after announcements of Alice and Bob



incoherent attack

- Eve can also perform collective unitary operations



coherent attack

5.3 quantum key distribution with EPR pairs: the Deutsch-Eckert protocol

Here we use the fact that a two-particle state with maximum entanglement, such as a Bell state

$$(10) \qquad |\psi_-\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle_A |1\rangle_B - |1\rangle_A |0\rangle_B \right)$$

measured in the computational basis $\{|0\rangle, |1\rangle\}$ leads to a totally random but correlated string of c-bits 0 or 1 for Alice and Bob. Furthermore a maximally entangled state between two parties cannot have entanglement with a third party. The degree of entanglement can be detected by measurements of the Bell inequality. Here a potential evesdropper would correspond to a hidden variable.

<u>protocol:</u>

(i) Alice has source of EPR pairs in state (say)

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

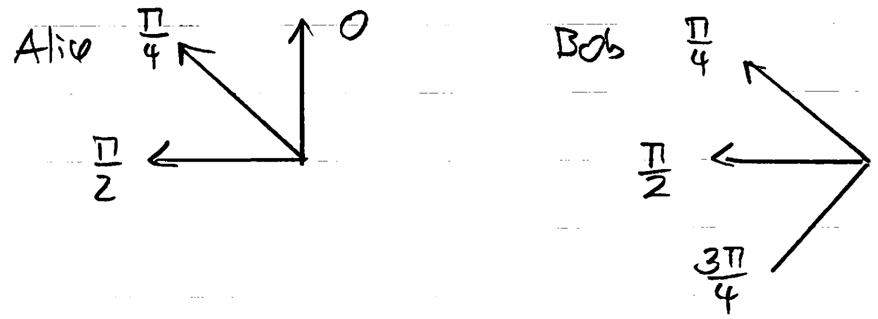
sends one particle to Bob

(ii) Alice and Bob perform randomly spin measurements in non-orthogonal directions $\vec{n}$

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

Alice $\vec{n} \in \{ \vec{e}_x , \frac{1}{\sqrt{2}}(\vec{e}_x + \vec{e}_y) , \vec{e}_y \}$

Bob $\vec{n} \in \{ \frac{1}{\sqrt{2}}(\vec{e}_x + \vec{e}_y) , \vec{e}_y , \frac{1}{\sqrt{2}}(\vec{e}_y - \vec{e}_x$



(iii) Alice and Bob exchange publically which basic $\vec{n}$ they have chosen

(iv) On pairs with $\vec{n}_A \neq \vec{n}_B$ they measure Bell inequalities

(13) $E_{EPR} = \langle \hat{\vec{\sigma}}_A \cdot \vec{a} \; \hat{\vec{\sigma}}_B \cdot \vec{b} \rangle = -\cos(\varphi_A - \varphi_B)$

<u>Clauser-Horne-Shimony Holt (CHSH) variant</u> of Bell inequality

(14) $$\boxed{|S| = |E(a,b) - E(a,b') + E(a',b) + E(a',b')| \leq 2}$$

classical $\quad E(a,b) = \cos(a-\theta_A)\cos(b-\theta_B)$

$$S_{cl} = \int d\theta_A \int d\theta_B \, P(\theta_A,\theta_B) \Big[\cos(a-\theta_A)\cos(b-\theta_B)$$
$$- \cos(a-\theta_A)\cos(b'-\theta_B) + \cos(a'-\theta_A)\cos(b-\theta_B)$$
$$+ \cos(a'-\theta_A)\cos(b'-\theta_B) \Big]$$
$$= \int d\theta_A \int d\theta_B \, P(\theta_A,\theta_B) \, 2\cos(\theta_A-\theta_B)$$

(15) $$-2 \leq S_{cl} \leq 2$$

for EPR state $\quad a = 0 \quad a' = \frac{\pi}{2}$
$\quad b = \frac{\pi}{4} \quad b' = \frac{3}{4}\pi$

(16) $\underline{\underline{|S_{EPR}|}} = |-\frac{1}{2}\sqrt{2} - \frac{1}{2}\sqrt{2} - \frac{1}{2}\sqrt{2} - \frac{1}{2}\sqrt{2}| = \underline{\underline{2\sqrt{2}}}$

If CHSH inequality maximally violated $\Rightarrow$ no eavesdropper

(v) If there was no eavesdropper, Alice and Bob use measurements in the <u>same</u> direction to create random key of 0 and 1

Alice	1 0 0 1 1 0 1 0 1 ...
Bob	0 1 1 0 0 1 0 1 0 ...

- What if

$$2 < |S_{\text{measure}}| < 2\sqrt{2} \qquad ?$$

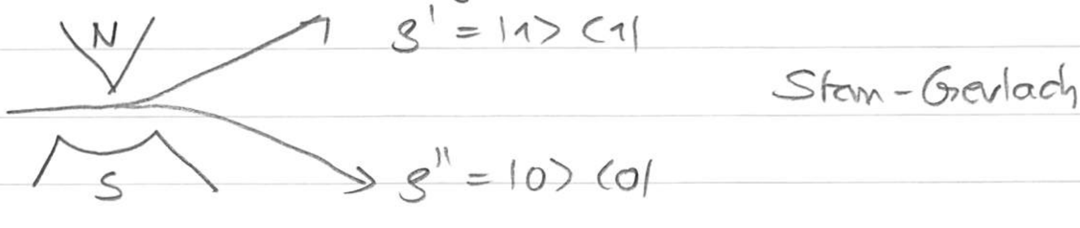
5.4 entanglement purification

Deutsch et al. PRA 54, 3824 (1996)
proof of convergence: Macchiavello PLA 246, 385 (1998)

(A) idea: destillation of pure states of single qubits
(later generalization to pairs)

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

in principle destillation by measurement



question: destillation without measurement?

(18) $$\rho \;\rightarrow\; \rho \otimes |0\rangle_A\langle 0| \qquad \text{ancilla}$$

$$\xrightarrow[\text{CNOT}]{} f\,|0\rangle\langle 0| \otimes |0\rangle_A\langle 0| + (1-f)\,|1\rangle\langle 1| \otimes |1\rangle_A\langle 1|$$

- measurement of ancilla qubit: projection to $|0\rangle\langle 0|$ (or $|1\rangle\langle 1|$) without measurement of system qubit!

problem: we used ancilla in a pure state
so we turn "gold into gold"

but we can purify ρ with a second system in the same state ρ

(19)

$$\rho_{AB} = \rho \otimes \rho = \big(f|0\rangle\langle 0| + (1-f)|1\rangle\langle 1|\big)_A \big(f|0\rangle\langle 0| + (1-f)|1\rangle\langle 1|\big)$$

CNOT

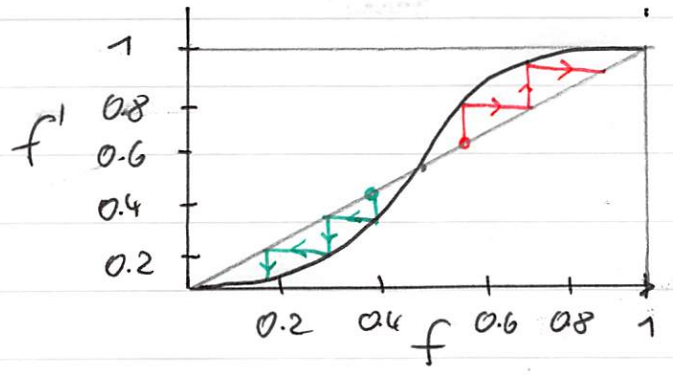
$$\Rightarrow \rho_{AB}' = \big(f^2 |0\rangle\langle 0| + (1-f)^2 |1\rangle\langle 1|\big)_A \otimes |0\rangle\langle 0|_B$$
$$+ f(1-f)\big(\underbrace{|0\rangle\langle 0| + |1\rangle\langle 1|}_{\text{totally mixed}}\big) \otimes |1\rangle\langle 1|_B$$

projection to $|0\rangle\langle 0|_B$ yields

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

$$= f'|0\rangle\langle 0| + (1-f')|1\rangle\langle 1|$$

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



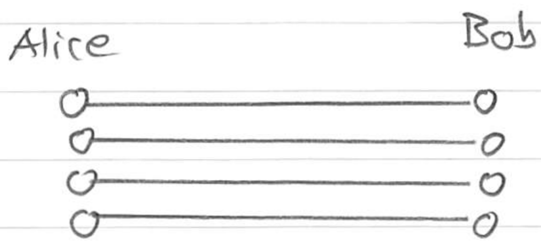
- iterative purification
  $f > 0.5 \Rightarrow f \to 1$
  $f < 0.5 \Rightarrow (1-f) \to$

(B) entanglement purification using pairs

ensemble of pairs in mixed state

$$\rho_{AB} = A|\phi_+\rangle\langle\phi_+| + B|\phi_-\rangle\langle\phi_-| + C|\psi_+\rangle\langle\psi_+| + D|\psi_-\rangle\langle\psi_-| \tag{22}$$

without loss of generality $A \geq B, C, D$
$\{|\phi_\pm\rangle, |\psi_\pm\rangle\}$ Bell states of Alice and Bob

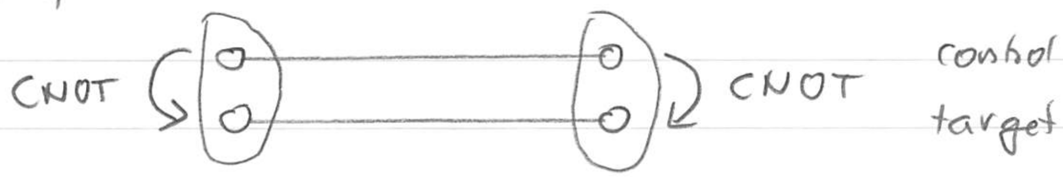


protocol:

(i) Alice: operation on bit $U_A = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix}$

Bob: operation on bit $U_B = U_A^{-1} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}$

(ii) Alice and Bob perform CNOT on a pair of qubits



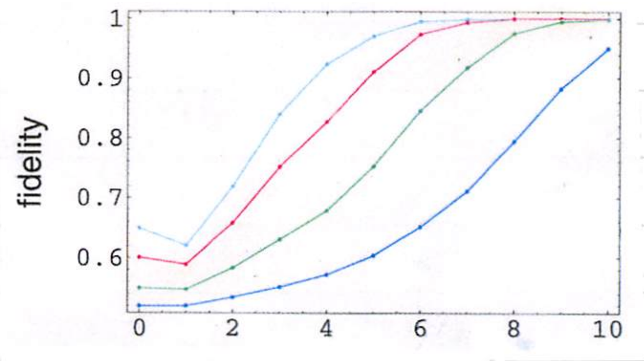
(iii) Alice and Bob measure target spin in the same basis
- if results agree the keep control qubit
- if results disagree they discard control qubit

$\Rightarrow$

(23)
$$\boxed{\begin{array}{ll} A' = \dfrac{A^2+B^2}{N} & B' = \dfrac{2CD}{N} \\[2ex] C' = \dfrac{C^2+D^2}{N} & D' = \dfrac{2AB}{N} \\[2ex] \multicolumn{2}{c}{N = (A+B)^2 + (B+C)^2} \end{array}}$$

if $A > \frac{1}{2}$ iteration (23) has fixed point

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



A'

# of iterations

<u>entanglement purification in the presence of noise</u>

So far we have assumed that purification is error free.

- If operations are errorness purification is only possible with initial fidelity

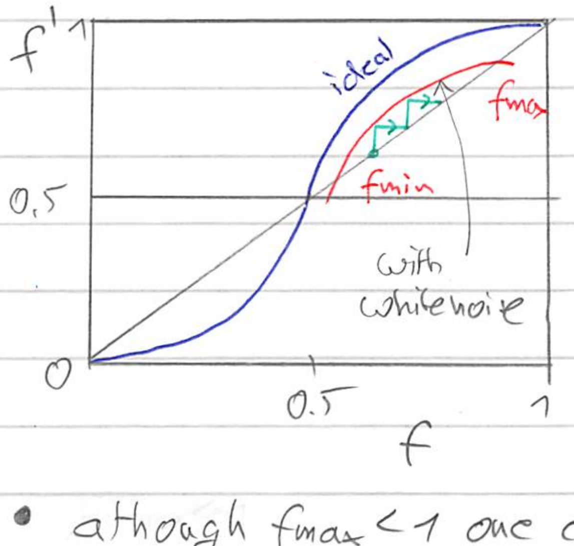
$$f \geq f_{min} > \frac{1}{2} \qquad (25)$$

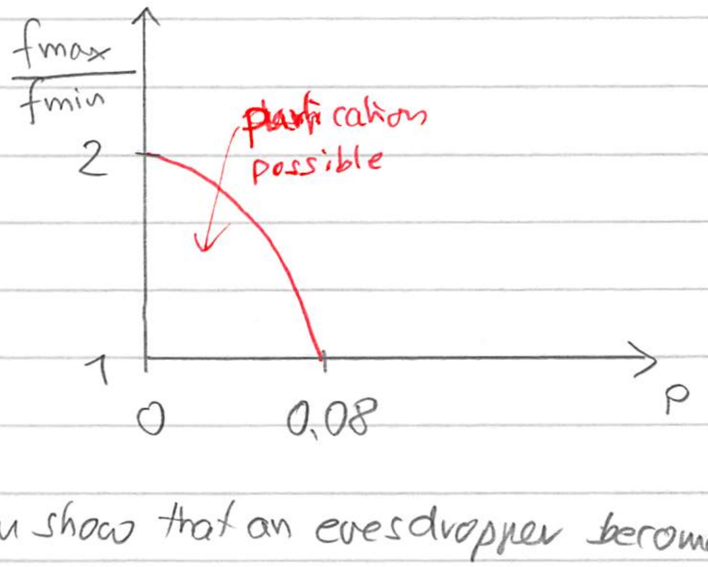
- The asymptotic fidelity of the protocol does not reach unity

$$f' \to f_{max} < 1 \qquad (26)$$

different noise processes are discussed in
Briegel, Dür, Cirac and Zoller PRA <u>59</u>, 169 (1999)
PRL <u>81</u>, 5932 (1998) and Giedke, Briegel, Cirac and Zoller PRA <u>59</u>, 2641 (1999)

- with increasing error probability p per operation f_{min} and f_{max} approach each other





- although $f_{max} < 1$ one can show that an eavesdropper becomes asymptotically factorized

5.5 quantum repeater

In order to perform q-cryptography and teleportation over large distances one has to create entanglement over large distances

problems: (i) sources of entangled particle pairs employ usually <u>local</u> interactions

(ii) decoherence probability increases exponentially with distance l in any transport protocol

(27) $$P = 1 - e^{-\alpha l} \quad \text{i.e.} \quad f = e^{-\alpha l}$$

purification protocols require however minimum fidelity f_{min}. This fixes a maximum distance l_{max}

(28) $$f_{min} = e^{-\alpha l_{max}}$$

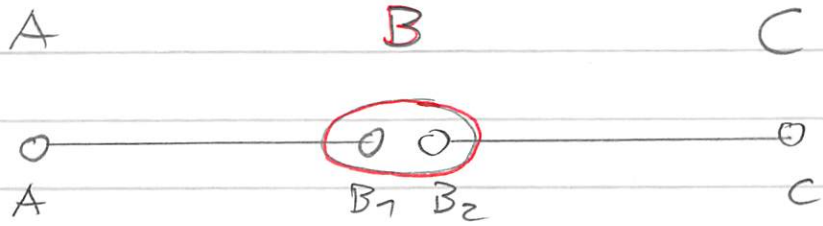
- classical solution: amplifiers (repeater)
  $\Rightarrow$ how to transfer to quantum systems?

solution: <u>quantum repeater</u>

iterative entanglement purification and entanglement swapping

entanglement swapping

C.H. Bennett et al. PRL 70, 1895 (1993)
M. Zukowski et al. PRL 71, 4287 (1993)



$$|\psi\rangle = |\phi_+\rangle_{AB_1} |\phi_+\rangle_{B_2C}$$

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

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

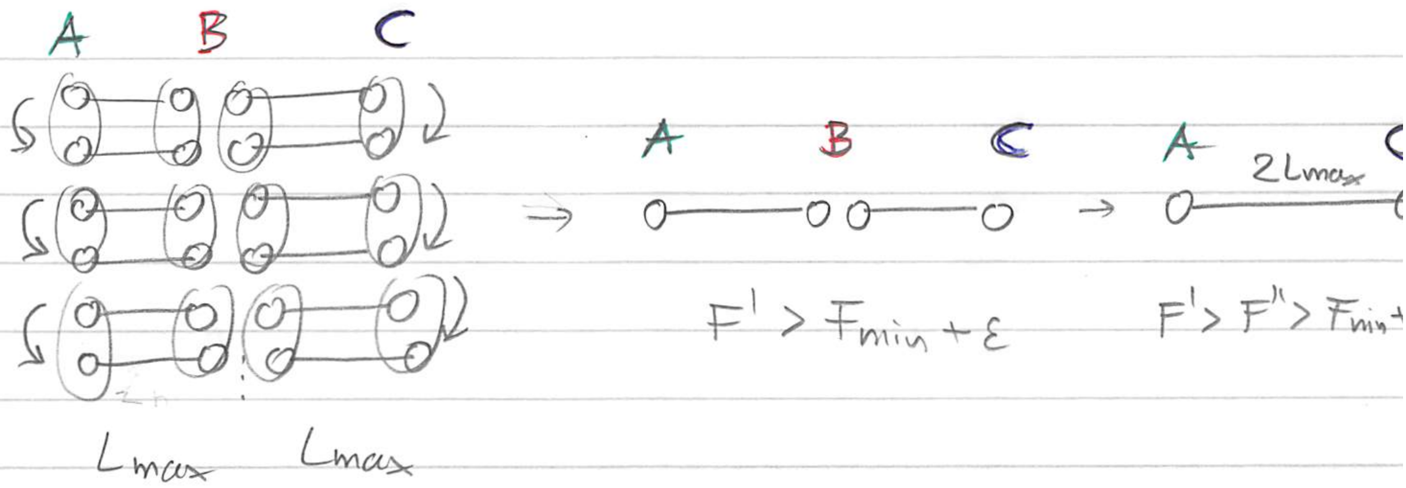
$$+ |1\rangle_A \left[\psi_+ - \psi_-\right]_{B_1B_2} |0\rangle_C + |1\rangle_A \left[\phi_+ - \phi_-\right]_{B_1B_2} |1\rangle_C \tag{29}$$

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

$$+ |\psi_+^{AC}\rangle\, \underline{|\psi_+^{B_1B_2}\rangle} + |\psi_-^{AC}\rangle\, \underline{|\psi_-^{B_1B_2}\rangle}\Big\}$$

Bell measurement on the pair of particles at B projects to one of the 4 Bell states $|\phi_\pm^{AC}\rangle$ or $|\psi_\pm^{AC}\rangle$ between A and C

$\Rightarrow$ swapping of entanglement to A — C combination of swapping and purification allows to create entanglement over large distances



$F = F_{min} + \varepsilon$

entanglement purification   swapping

iteration of procedure creates entanglement over large distance

(30) $$L = N L_0 \qquad (L_0 < L_{max})$$

but: requires protocol whose ressources do not scale exponentially with N

sequentiell increase of entanglement distance not useful since

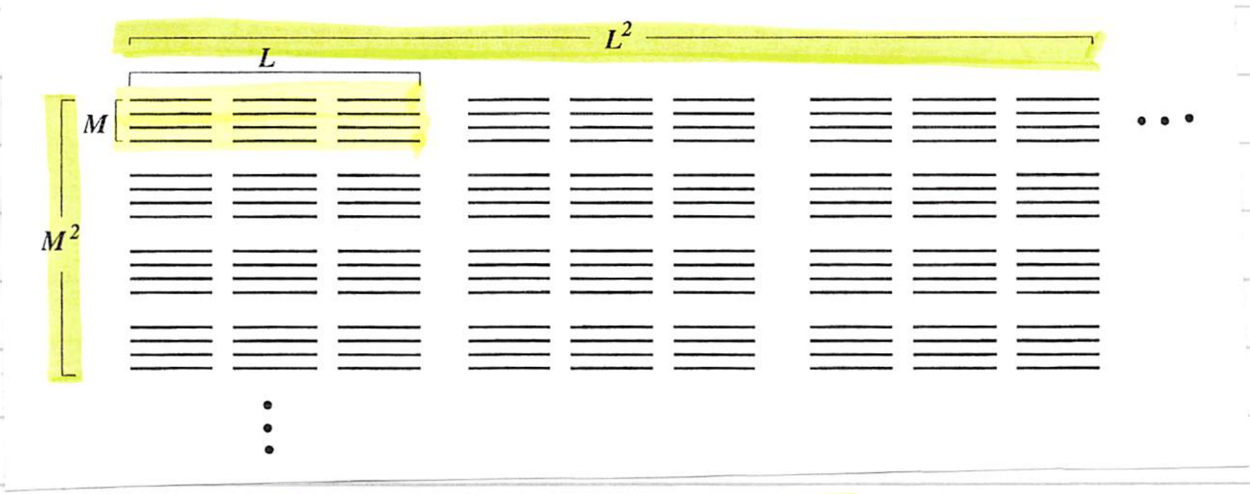
(i) total number of pairs would scale exponentially
1 step reduction by factor $1/\eta$

(31) $$N\text{steps} \quad \left(\frac{1}{\eta}\right)^N = \eta^{-N} = 2^{N(-\log \eta)}$$

(ii) total time scales exponentially in N

$\Rightarrow$ concatinated purification & swapping protocol

H. J. Briegel et al. PRL 81, 5932 (1998)
W. Dür et al. PRA 59, 169 (1999)



: block in 1st iteration   : block in 2nd iteration

set $N = L^n$

(i) blockwise connection of L segments

(ii) entanglement purification in every block and generation of entangled pair of distance L from M pairs of length 1 (in units of l_0)

(iii) iteration of procedure

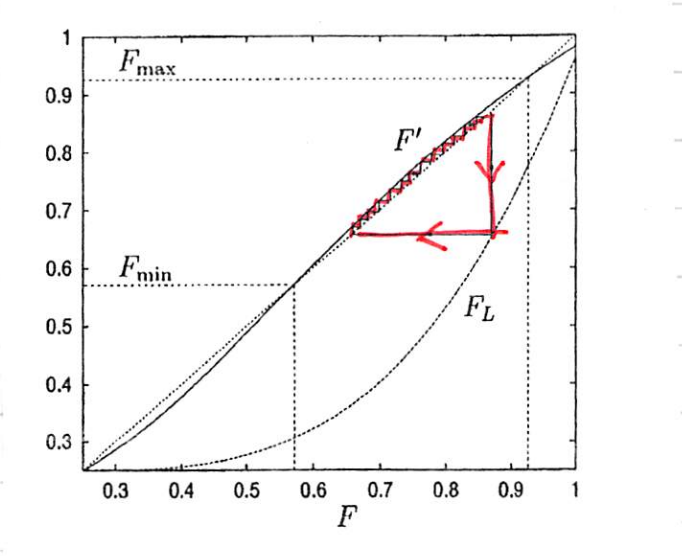
- entanglement distance $\sim L^k$
  k - number of iterations

- total number of elementary pairs to reach L^n

$$R = (ML)^n = L^n M^n = N L^{n \log_L M} \tag{32}$$

$$= N^{\log_L M + 1}$$ only <u>polynomial</u> increase!

the fidelity of the protocol can be calculated, see e.g. Dür et al. PRA <u>59</u>, 169 (1999)



- single purification step $F \to F'$

- fidelity after connection of L segments