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 (bit) from A (Alice) to B (Bob)

(ii) authentication: 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

Alice

message M

\[ M \rightarrow C = C(K, M) \]

transmission through public channel

Bob

message M

\[ M = D(K, C) \]

identical key

Example: Vernam cipher (Gilbert-Vernam 1977)

message 0 0 1 1 0 1 0

\[ \oplus \text{key} \]

mod 2 1 0 0 1 1 0 1

code 1 0 1 0 1 1 1

decoding

code 1 0 1 0 1 1 1

\[ \oplus \text{key} \]

mod 2 1 0 0 1 1 0 1

message 0 0 1 1 0 1 0
Shannon (1949): Vermon protocol 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

Secure cryptography = generation and distribution
of secret key

Public key distribution

Use two different keys, $K_c$ and $K_D$ for coding
and decoding, which of course are interrelated, i.e.

$$K_c = f[K_D] \quad K_D = f^{-1}[K_c]$$

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

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
\[ f[f^{-1}[K_c]] = f[K_0] \]
is simple (effort scales
only polynomially with the size of \(K_0\)).

public key protocol:

\textbf{Bob:} chooses \(K_0 \rightarrow \) calculates \(K_c = f[K_0]\)
announces \(K_c\) publically

\textbf{Alice:} uses \(K_c\) to encode message and transmits
code over public channel to \textbf{Bob}

\textbf{Eve:} cannot decode code since \(K_c \rightarrow K_0\)
is a hard problem

**Example:** \underline{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 are relatively prime
to \(R\) (i.e. do not have a common divisor with \(R\)).

If \(U\) and \(V\) are relatively prime, then

\[(2)\quad \varphi(U \cdot V) = \varphi(U) \cdot \varphi(V)\]

Thus in particular if \(U, V\) are prime numbers

\[(3)\quad \varphi(U \cdot V) = (U-1)(V-1)\]
and can easily be calculated. Number theory now says

\[(4) \quad M^{p \cdot q} \equiv M \pmod{P}\]

for all \(M < R\) which are relatively prime to \(R\).

(i) choose 2 random prime numbers \(U, V\)
\[R = U \cdot V \quad \text{and} \quad \phi(R) = (U-1)(V-1)\]

(ii) choose an integer \(P\) that is relatively prime to \(\phi(R)\) and \(1 \leq P \leq \phi(R)\)

(iii) find the integer \(Q\) such that
\[P \cdot Q = 1 \pmod{\phi(R)}\]

\(Q\) 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 \(\phi(R)\) no longer needed

\[(5) \quad \text{public key } K_c = \{ P, R \} \]
\[\quad \text{secret key } K_d = \{ P, Q \} \]
\[ C = M^p \mod R \]

**Decoding**
\[ M = C^q \mod R = M^{p \cdot q} \mod R = M \]

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 \( \log(R) \)!

\[ \Rightarrow \text{Security of RSA scheme lies in non-existence of an effective algorithm for factorization!} \]

factorization is believed to be \( \text{NP hard, i.e.} \)

\[ 29 \cdot 41 = 1189 \quad \text{Simple} \]

but \[ 1513 = ? \times ? \quad \text{Difficult} \]
\[ 17 \times 89 \]

**Problem:**

\[ \neg \text{Mathematical proof that factorization is NP hard.} \]
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)

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

(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 measures all $4N$ qubits in a random basis i.e. in $|\uparrow_x\rangle$ or $|\downarrow_z\rangle$ basis

(ii) Alice and Bob communicate publicly which basis they have used, but not if they have measured $|1\rangle$ or $|0\rangle$ in the case of $|\downarrow_z\rangle$
\( v \rightarrow u \rightarrow u \) in the case of \( \theta \).

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 polynomials.

(iv) If their results agree in all \( N \) cases (\( N \rightarrow \infty \)) they can conclude that there was no eavesdropper in the line. Then they use the remaining \( N \) qubits as random key. If their results disagree in \( N/4 \) cases (\( N \rightarrow \infty \)) then there was an eavesdropper 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)
Classical privacy amplification

If $N$ test bibs have an error rate $\varepsilon$, then
among the $N$ bibs of the key $N\varepsilon$ are erroneous.

Exchanging $N^\mathcal{H}(\varepsilon)$

bib via a public channel, Alice and Bob can
correct this error. This leads to a smaller,
a sifted key with

$N' = N (1 - \mathcal{H}(\varepsilon))$

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

$N'^\mathcal{H}(2\varepsilon) \leq N'$

As long as $\mathcal{H}(2\varepsilon) < 1$, sifting the key
reduce the information that Eve has about the
sifted key.

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

$R$ random matrix $(n' - 1) \times n'$
of 0 and 1 announced by Alice
\begin{equation}
K^{(n'-2)} = R \cdot K^{(n')} \pmod{2}
\end{equation}

Information of Eve about sifted key: $H(2^{(2-n'-1)})$

It is chosen to match a tolerance threshold of information left to Eve.

Mathematical proofs about quantifiable 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 an eavesdropper qubit and perform measurements on those after announcement of Alice and Bob.

\begin{center}
\begin{tikzpicture}
  \node (Alice) at (0,0) {Alice};
  \node (Eve) at (0,-3) {Eve};
  \node (Bob) at (4,0) {Bob};
  \node[draw] (U) at (2,-1) {$U$};
  \node[draw] (W) at (2,-2) {$W$};
  \node[draw] (X) at (1,-3) {$U$};
  \node[draw] (Y) at (1,-4) {$U$};
  \node[draw] (Z) at (3,-3) {$U$};
  \node[draw] (Q) at (3,-4) {$U$};
  \draw[->] (Alice) -- (U);
  \draw[->] (Eve) -- (X);
  \draw[->] (U) -- (W);
  \draw[->] (W) -- (Y);
  \draw[->] (X) -- (Z);
  \draw[->] (Z) -- (Q);
  \draw[->] (Q) -- (Bob);
  \node at (2,-5) {q-memory};
  \node at (3,-5) {q-memory};
  \node at (3,-6) {q-memory};
\end{tikzpicture}
\end{center}

\underline{Incoherent attack}
Eve can also perform collective unitary operations.

\[ \text{coherent attack} \]

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

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

\[ \begin{align*}
|22\rangle &= \frac{1}{\sqrt{2}} (|0\rangle_A |1\rangle_B - |1\rangle_A |0\rangle_B) 
\end{align*} \]

measured in the computational basis $\{|0\rangle, |1\rangle\}$ leads to a totally random but correlated string of 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 measurement of the Bell inequality. Here a potential eavesdropper would correspond to a
hidden variable.

**Protocol:**

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

\[(11) \quad \frac{1}{\sqrt{2}} \left( |\uparrow_x\rangle |\downarrow_x\rangle - |\downarrow_x\rangle |\uparrow_x\rangle \right) = \text{IEPR}_x \]

sends one particle to Bob

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

\[(12) \quad \hat{S}_n = \hat{n} \cdot \hat{S} \]

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

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

(iii) Alice and Bob exchange publicly which basis \( \hat{n} \) they have chosen.

(iv) on pairs with \( \hat{n}_A \neq \hat{n}_B \) they measure Bell inequalities.
(13) \[ E_{EPR} = \langle \hat{S}_a \cdot \hat{S}_b \rangle = -\cos(\theta_A - \theta_B) \]

**Clauser-Horne-Shimony-Holt (CHSH) Variant of Bell Inequality**

(14) \[ |S| = |E(a,b) - E(a',b') + E(a',b) + E(a,b')| \leq 2 \]

**Classical** \[ E(a,b) = \cos(a - \theta_A) \cos(b - \theta_B) \]

\[ S_{Cl} = \int d\theta_A \int d\theta_B \rho(\theta_A, \theta_B) \left[ \cos(a - \theta_A) \cos(b - \theta_B) - \cos(a - \theta_A) \cos(b' - \theta_B) + \cos(a' - \theta_A) \cos(b - \theta_B) + \cos(a' - \theta_A) \cos(b' - \theta_B) \right] \]

\[ = \int d\theta_A \int d\theta_B \rho(\theta_A, \theta_B) 2 \cos(\theta_A - \theta_B) \]

(15) \[-2 \leq S_{Cl} \leq 2\]

For EPR state \[ a = 0, \quad b = -\frac{\pi}{4}, \quad a' = \frac{\pi}{2}, \quad b' = \frac{3\pi}{4} \]

(16) \[ |S_{EPR}| = | -\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}| = 2 \sqrt{2} \]

If CHSH inequality maximally violated \(\Rightarrow\) no eavesdropper

If there was no eavesdropper, Alice and Bob use measurements in the **same** 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

\[ 2 < |S_{\text{measure}}| < 2\sqrt{2} \]

5.4 entanglement purification

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

\[ (\forall) \text{ idea: distillation of pure states of single qubits} \]
(later generalization to pairs)

\[ (17) \quad S = f \left| 0 \right> \left< 0 \right| + (1-f) \left| 1 \right> \left< 1 \right| \]

in principle distillation by measurement

\[ N \quad \xrightarrow{} \quad S' = \left| 1 \right> \left< 1 \right| \]

\[ S \quad \xrightarrow{} \quad S'' = \left| 0 \right> \left< 0 \right| \]

Stem-Gielach

question: distillation without measurement?

\[ (18) \quad S \rightarrow S \otimes \left| 0 \right> \left< 0 \right|_A \quad \text{ancilla} \]

\[ \text{CNOT} \rightarrow f \left| 0 \right> \left< 0 \right| \left< 0 \right| + (1-f) \left| 1 \right> \left< 1 \right| \left< 1 \right| \left< 1 \right|_A \]
measurement of ancilla qubit: projection to $|0\rangle|0\rangle$ (or $|1\rangle|1\rangle$) without measurement of system qubit!

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

but we can purify $\mathcal{S}$ with a second system in the same state $\mathcal{S}$

$$\mathcal{S}_{AB} = \mathcal{S} \otimes \mathcal{S} = \left( f |0\rangle|0\rangle + (1-f) |1\rangle|1\rangle \right) \left( f |0\rangle|0\rangle + (1-f) |1\rangle|1\rangle \right)$$

\begin{equation}
\Rightarrow \mathcal{S}'_{AB} = \left( f^2 |0\rangle|0\rangle + (1-f)^2 |1\rangle|1\rangle \right) \otimes |0\rangle|0\rangle_B + f(1-f) \left( |0\rangle|0\rangle + |1\rangle|1\rangle \right) \otimes |1\rangle|1\rangle_B
\end{equation}

totally mixed

projection to $|0\rangle|0\rangle_B$ yields

\begin{equation}
\mathcal{S}'_A = \frac{f^2 |0\rangle|0\rangle + (1-f)^2 |1\rangle|1\rangle}{f^2 + (1-f)^2} = f' |0\rangle|0\rangle + (1-f') |1\rangle|1\rangle
\end{equation}

\begin{align}
f' &= \frac{f^2}{f^2 + (1-f)^2} \\
(1-f') &= \frac{(1-f)^2}{f^2 + (1-f)^2}
\end{align}
(B) **Entanglement purification using pairs**

**Ensemble of pairs in mixed state**

\[ S_{AB} = A |\phi^+\rangle\langle\phi^+| + B |\phi^-\rangle\langle\phi^-| + C |\psi^+\rangle\langle\psi^+| + D |\psi^-\rangle\langle\psi^-| \]

without loss of generality \( A \geq B, C, D \)

\( \left\{ 1 (\phi^\pm), 1, 2^\pm \right\} \) Bell states of Alice and Bob

**Protocol:**

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

Bob: operation \( U_B = U_A^{-1} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \)
(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, keep control qubit.
- If results disagree, discard control qubit.

\[
A' = \frac{A^2 + B^2}{N} \quad B' = \frac{2CD}{N} \\
C' = \frac{C^2 + D^2}{N} \quad D' = \frac{2AB}{N} \\
N = (A+B)^2 + (B+C)^2
\]

If \( A > \frac{1}{2} \), iteration (23) has fixed point

(24) \( A' \to 1 \quad B', C', D' \to 0 \)
entanglement purification in the presence of noise

So far we have assumed that purification is error free.

- If operations are errorless purification is only possible with initial fidelity.

\[ f \geq f_{\text{min}} > \frac{1}{2} \]

- The asymptotic fidelity of the protocol does not reach unity.

\[ f' \rightarrow f_{\text{max}} < 1 \]

Different noise processes are discussed in:

- Briegel, Dur, Cirac and Zoller PRA 59, 169 (1999)
- PRL 81, 5332 (1998) and Giedke, Briegel, Cirac and Zoller PRA 59, 2641 (1999)

- With increasing error probability \( p \) per operation, \( f_{\text{min}} \) and \( f_{\text{max}} \) approach each other.

Although \( f_{\text{max}} < 1 \) one can show that an eavesdropper becomes asymptotically factorized.
5.5 quantum repeater

In order to perform quantum cryptography and teleportation over large distances one has to create entanglement over large distances.

Problems: 
(i) Sources of entangled particle pairs employ usually local interactions

(ii) decoherence probability increases exponentially with distance $L$ in any transport protocol.

\[ P = 1 - e^{-\alpha L} \quad \text{i.e.} \quad f = e^{-\alpha L} \]

Purification protocols require however minimum fidelity $f_{\text{min}}$. This fixes a maximum distance $L_{\text{max}}$:

\[ f_{\text{min}} = e^{-\alpha L_{\text{max}}} \]

- Classical solution: amplification (repeater)
  \[ \Rightarrow \text{how to transfer to quantum systems?} \]

  Solution: quantum repeater
  \[ \text{iterative entanglement purification and entanglement swapping} \]
Entanglement Swapping

C.H. Bennett et al., PRL 70, 1895 (1993)
L. Zubakov et al., PRL 71, 4207 (1993)

\( |\psi\rangle = |\Phi_+\rangle_{AB_7} |\Phi_+\rangle_{B_2C} \)

\[ = \frac{1}{2} \left( |10\rangle_A |0\rangle_{B_7} + |1\rangle_A |1\rangle_{B_7} \right) \left( |10\rangle_{B_2} |0\rangle_C + |1\rangle_{B_2} |1\rangle_C \right) \]

\[ = \frac{1}{\sqrt{2}} \left\{ |10\rangle_A \left[ |\Phi_+\rangle_{B_1B_2} + |\Phi_-\rangle_{B_1B_2} \right] |0\rangle_C + |1\rangle_A \left[ |\Phi_+\rangle_{B_1B_2} - |\Phi_-\rangle_{B_1B_2} \right] |1\rangle_C \right\} \]

(29)

\[ = \frac{1}{2} \left\{ |\Phi_+\rangle_{AC} |\Phi_+\rangle_{B_1B_2} \right\} + |\Phi_-\rangle_{AC} |\Phi_-\rangle_{B_1B_2} \right\} \]

\[ + |\Psi_+\rangle_{AC} |\Psi_+\rangle_{B_1B_2} \right\} + |\Psi_-\rangle_{AC} |\Psi_-\rangle_{B_1B_2} \right\} \]

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:

\[ \Rightarrow \text{swapping of entanglement} \]

\[ 10 \quad \text{A} \quad \text{---} \quad \text{C} \]
combination of swapping and purification allows to create entanglement over large distances

\[ F' > F_{\text{min}} + \varepsilon \quad F' > F'' > F_{\text{min}} \]

\[ F = F_{\text{min}} + \varepsilon \]

entanglement purification \quad \text{Swapping}

iteration of procedure creates entanglement over large distances

\[ L = N \cdot L_0 \quad (L_0 < L_{\text{max}}) \]

but: requires protocol whose resources do not scale exponentially with \( N \)

sequential increase of entanglement distance not useful since

1. total number of pairs would scale exponentially
2. 1 step reduction by factor \( 1/2 \)

\[ \text{1 steps} \quad \left( \frac{1}{2} \right)^N = 2^N = 2^N \times 2^{-1} = 2^{-1} \]
(ii) total time scale exponentially in $N$

$=)$ concatenated purification & swapping protocol

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

Set $N = L^n$

(i) block-wise 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 $a_0$)

(iii) iteration of procedure

- entanglement distance $\sim L^k$
  
  $k$ - number of iterations
\[
R = (ML)^n = L^n M^n = N L^n \log_L M
\]

\[
= N \log_L M + 1 \quad \text{only polynomial increase}
\]

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

- Single purification step: \( F \to F' \)
- Fidelity after connection of \( L \) segments