# 1. Quantum tools and a first protocol

## Lecture 1. Introduction and Overview

The goal of quantum cryptography: Use quantum communication to achieve information security.

The most famous of: QKD — key distribution

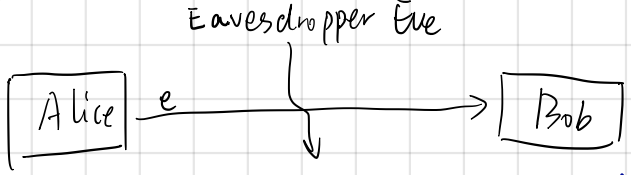
The challenge for building keys: the need for secrecy: Eve won't know the key
the demand for correctness: Alice and Bob have exactly the same key.

Advantage: No-cloning theory, Eve can't make a copy
Challenge: In long distance, it is challenging to send qubits, because we can't amplify signals in the same way classically.

## 1.1. The one-time pad

### Lecture 1. The one-time pad.

Secure Communication




Message $m$
key $k$
Encrypt $e = Enc(m,k)$

Decrypt: $m = Dec(e,k)$

Conditions:

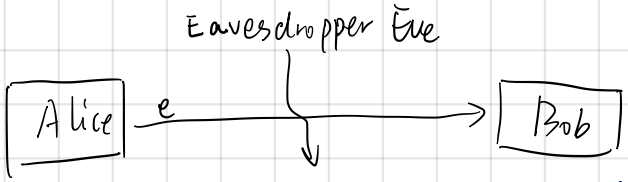
① Correct: Bob can read the message, $m = Dec(Enc(m,k),k)$

② Secure: Eve gains no information! $P(M=m|E=e) = P(M=m)$

Suppose that they key has $n$ bits, thus the probability from Eve's perspective for the key taking a certain value $k$ is:

$P(K=k) = \frac{1}{2^n}$

One-time pad




Message $m = m_1 \cdots m_n$
key $k = k_1 \cdots k_n$ (⊕ ⊕)
$Enc(m,k) = e_1 \cdots e_n$

$Dec(e,k) = m_1 \cdots m_n$
$= k_1 \cdots k_n$ (⊕ ⊕)
$e_1 \cdots e_n$

⊕: mod sum, $m_j \oplus k_j = (m_j + k_j) \bmod 2$

Why is one-time pad secure?

Security (Classical – Shannon secrecy)

$P(M=m) = P(M=m \mid E=e)\ \forall m, \forall e$ ⇒ the ciphertext $E$ is independent of message $M$.

⇓ equivalent to

$P(E=e \mid M=m) = P(E=e)$

$P(M=m, E=e) = P(M=m)P(E=e \mid M=m) = P(E=e)P(M=m \mid E=e)$

(a) (b) (c) (d)

→ if b=c, then a=d or if a=d then b=c

Why is this? Suppose $n=1$ : (the key size is n)

$M=m$

$p=\frac{1}{2}, K=0$ → $e = m \oplus 0 = m$ ⇒ equal to the message bit

$p=\frac{1}{2}, k=1$ → $e = m \oplus 1$ ⇒ equal to the message bit flipped

∴ The probability of the encrypted bit taking a particular value is a half.

∴ Encrypted bit is independent of the message.

∴ This scheme is secure

For one-time pad, we use a key as long as the message.

As Claude Shannon discovered, the length of key must at least be the same as the length of message.

This means that if Alice and Bob already have a few GB of keys, and they use it to send a video from Alice to Bob, after the video arrives they essentially run out of key. There is no way for them to send another video if they don't have any key bits left. Keys are thus an important resource.
By using classical communication, it is impossible for Alice and Bob to produce new keys, if they can just communicate over an open communication channel that Eve can listen to.
The cool thing is, that we'll later see that with Quantum Key Distribution we can extend the amount of key.
Alice and Bob can take GB of keys and turn it into an arbitrary long, possibly infinitely long encryption key to keep communicating securely.

e.g. Message $m = m_1 \cdots m_n$

Key $k = k_1 \cdots k_n$

$= Enc(m,k)$ $e = e_1 \cdots e_n$

$m = 1011$, $k = 1110$, $e = 0101$

key $k = k_1 \cdots k_n$, $e = e_1 \cdots e_n$

$= Dec(e,k) = m_1 \cdots m_n$

$k = 1110$, $e = 0101$, $m = 1011$

same

# 1.2 The density matrix

## Lecture 1: the density matrix

Quantum states of n qubits:

$|\psi\rangle \in \mathbb{C}^d$, $d = 2^n$, with $\langle\psi|\psi\rangle = 1$

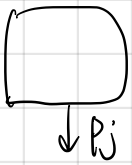
Problem 1: How to write down the state of one of many qubits?

(A) (B)

$|\psi\rangle_{AB} \neq |\psi\rangle_A \otimes |\psi\rangle_B$ [Because of entanglement]

e.g. $|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$

Problem 2. How to write down mixtures?




measurement

$|\psi_j\rangle$

A more general description of qubits!

① From vectors to matrices

$|\psi\rangle \longrightarrow \rho = |\psi\rangle\langle\psi|$

density matrix

e.g. $|0\rangle \to \rho = \begin{pmatrix}1\\0\end{pmatrix}(1\ 0) = \begin{pmatrix}1 & 0\\0 & 0\end{pmatrix}$

$|+\rangle \to \rho = \begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{pmatrix}\left(\frac{1}{\sqrt{2}}\ \frac{1}{\sqrt{2}}\right) = \begin{pmatrix}\frac{1}{2} & \frac{1}{2}\\ \frac{1}{2} & \frac{1}{2}\end{pmatrix}$

△Solving Problem 2 - mixtures

States generates with some probability:

$|\psi_j\rangle$ with probability $p_j$, $\rho = \sum_j p_j |\psi_j\rangle\langle\psi_j|$

Does this make any sense?

$P_{0|j} = |\langle\psi_j|0\rangle|^2 = \mathrm{Tr}[\langle 0|\psi_j\rangle\langle\psi_j|0\rangle] = \mathrm{Tr}[|0\rangle\langle 0|\psi_j\rangle\langle\psi_j|]$

(trace; The trace is cyclic (循环的))

$P_0 = \sum_j p_j P_{0|j} = \sum_j p_j \mathrm{Tr}[|0\rangle\langle 0|\psi_j\rangle\langle\psi_j|] = \mathrm{Tr}\left[|0\rangle\langle 0| \sum_j p_j |\psi_j\rangle\langle\psi_j|\right] = \mathrm{Tr}[|0\rangle\langle 0|\rho]$

## ○ Density Matrix

Definition: $\rho \in L(H)$ with $H = \mathbb{C}^d$

$\rho \geq 0$ No negative eigenvalues ! (Hermitian $\rho^\dagger = \rho$)

$Tr(\rho) = 1$

Measure in basis: $\{|b\rangle\}_b$ $\quad p_b = Tr[|b\rangle\langle b|\rho]$

Why these conditions: $p_b = \langle b|\rho|b\rangle \geq 0$

$$1 = \sum_b p_b = \sum_b Tr[|b\rangle\langle b|\rho] = Tr[\mathbb{I}\cdot\rho] = Tr[\rho]$$

$$\sum_b Tr[|b\rangle\langle b|] = \mathbb{I}$$

## △ Pure and mixed

$|\psi\rangle \to \rho = |\psi\rangle\langle\psi|$

if $rank(\rho) = 1 \Leftrightarrow$ pure state

if $rank(\rho) > 1 \Leftrightarrow$ mixed state.

e.g. $\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|+\rangle\langle +|$ (Probability)

$$= \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} \frac{3}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} \end{pmatrix}$$