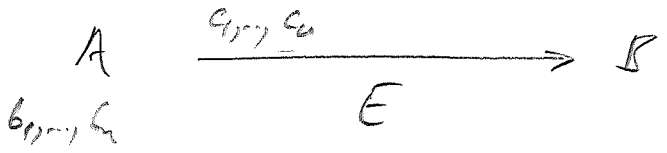
VII. Quantum cryptography

1) Cryptography

Scenario:

Alice wants to send secret message to Bob over a public communication channel. Eve, the eavesdropper, should not be able to learn the secret message.



typ: message = bit string $b_1, \ldots, b_n$

2) Classical cryptography:

Private key cryptography:

A private (= secret) key is used to encode the message.

Simple examples: permute letters, or permutations of letters, following some simple rule.

problem: safety relies on secrecy of method/key

→ easy to break w/ statistical analysis

One-time pad (Vernam cipher):

A & B share secret + random bit string $r_1, \dots, r_n$

Encode message $b_1, \dots, b_n$ as

$$c_1, \dots, c_n = b_1 \oplus r_1, b_2 \oplus r_2, \dots, b_n \oplus r_n.$$

Advantage:

- Provably (information-theoretically) secure – if $(r_1, \dots, r_n)$ is completely random, so is $(c_1, \dots, c_n)$.

Problem:

- Key can only be used once: length of key = length of message ⇒ lots of shared secret randomness needed,
- Eve could try to copy $r_1, \dots, r_n$ – either beforehand (as $r_1, \dots, r_n$ must be shared in advance) or later (if not destroyed properly)

Public key cryptosystems:

Based on functions which are hard to invert ("one-way functions"), e.g. primes p_1, p_2

$$p_1, p_2 \xrightarrow[\text{hard}]{\text{easy}} p_1 \cdot p_2$$

Message can be encoded using $p_1 p_2$, but decoding requires p_1, p_2 (or some simple function of them).

Method: - B finds large p_1, p_2 primes.

- B announces $p_1 p_2$ publicly.
- A uses $p_1 p_2$ to encrypt message + sends it.
- B can decode message.

→ E.g. RSA (Rivest, Shamir, Adleman '77)

Advantage:

- public key: key need not be kept secret
- keypair can be created when needed → lower risk of stealing it

Disadvantage:

- requires authenticated one (i.e., A & B need to know it is them)

⇒ can be ensured given some initial (small) shared secret or using a trusted authority

(Otherwise E can do a "man-in-the-middle attack", i.e.,

A ⟷ E ⟷ B

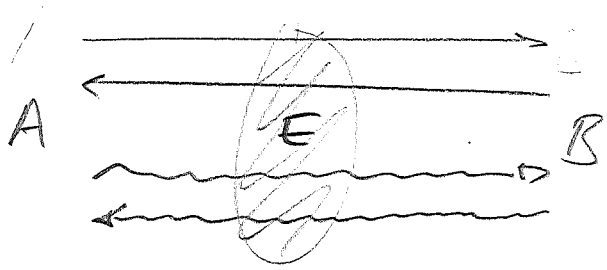
decode encode w/ diff. keys.

- Encr. messages can be stored by Eve and decrypted in the future (e.g. w/ stronger computers)
- Based on hardness assumptions: challenged by Shor's algorithm.
  (Note: Pure post public key cryptosystems not based on factoring.)

Can we combine the best of both worlds — create a provably secure key (i.e., a one-time pad) publicly?

3. Quantum cryptography

Idea: A+B share a (authenticated) classical + a quantum communication channel, which are in control of Eve.



Can A+B establish a secret key (= random bit string unknown to E)?

BB84 protocol (Bennett + Brassard '84):

Step 1:

A creates random strings

$a_1, \ldots, a_n$ (the "bases")

and $r_1, \ldots, r_n$ (the random string)

For each (a_i, r_i), A prepares a qubit $|\psi_i\rangle$ and sends it to Bob, where:

$$\text{If } a_i = 0: \quad |\psi\rangle = \begin{cases} |0\rangle, & r_i = 0 \\ |1\rangle, & r_i = 1 \end{cases}$$

$$\text{If } a_i = 1: \quad |\psi\rangle = \begin{cases} |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, & r_i = 0 \\ |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}, & r_i = 1 \end{cases}$$

Step 2:

B measures each qubit randomly (string $a_1', \ldots, a_n'$)

in bases:

$$\text{If } a_i' = 0: \text{ basis} = \{|0\rangle, |1\rangle\} \to \text{outcome } r_i'$$

$$a_i' = 1: \text{ basis} = \{|+\rangle, |-\rangle\} \to \text{outcome } r_i'$$

Note: Step 1+2 can be done "on the fly" — i.e. A sends 1 photon per bit & Bob measures it immediately.

Before starting Step 3, Bob must have <u>meas. all qubits</u> (correct timing or by communication).

<u>Step 3:</u>

A & B exchange all information about a_ℓ & a_ℓ' (i.e. their basis choice).

<u>We know:</u> $a_\ell = a_\ell' \Rightarrow r_\ell = r_\ell'$

$a_\ell \neq a_\ell' \Rightarrow r_\ell, r_\ell'$ uncorrelated.

A & B discard all ℓ with $a_\ell \neq a_\ell'$.

$\Rightarrow$ remaining random bits perfectly correlated!

<u>What if Eve intercepts?</u>

Information gain by Eve = disturbance of state (unless states all in same basis)

E does not know basis q_E beforehand →

E could copy in fixed basis:

$$U: |0\rangle_1|0\rangle_2 \longmapsto |0\rangle_1|\alpha\rangle_2$$
$$|1\rangle_1|0\rangle_2 \longmapsto |1\rangle_1|\beta\rangle_2$$

& meas. $|\alpha\rangle/|\beta\rangle$.

Acts for A/B like $\mathcal{E}(\rho) = \mathrm{tr}_2\left(U(\rho \otimes |0\rangle\langle 0|)U^+\right)$.

In particular: $U|\pm\rangle|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|\alpha\rangle \pm |1\rangle|\beta\rangle\right)$

$$\Rightarrow \mathcal{E}\left(|+\rangle\langle+|\right) = \frac{1}{2}\left(|0\rangle\langle 0| + |1\rangle\langle 1| + \langle\alpha|\beta\rangle\,|1\rangle\langle 0| + \langle\beta|\alpha\rangle\,|0\rangle\langle 1|\right)$$

$$= p\,|+\rangle\langle+| + \underbrace{(1-p)\,|-\rangle\langle-|}_{\text{disturbance.}}$$

Similar: any other info which tries to acquire any info will cause disturbance on some of the states:

$$U: |\varphi\rangle|0\rangle \longmapsto |\varphi\rangle|\alpha\rangle$$
$$|\psi\rangle|0\rangle \longmapsto |\psi\rangle|\beta\rangle$$

} disturbance free for $|\varphi\rangle, |\psi\rangle$, $\langle\varphi|\psi\rangle \neq 0$.

$$\Rightarrow (\langle\varphi|\langle\alpha|)(|\psi\rangle|\beta\rangle) = (\langle\varphi|\langle 0|)(|\psi\rangle|\beta\rangle)$$

$$\Rightarrow \langle\alpha|\beta\rangle = 1 \Rightarrow \text{no info!}$$

$\Rightarrow$ A & B can test for Eve:

Step 4: A & B compare some of their $r_i \stackrel{?}{=} r_i'$

$\Rightarrow$ can detect if E is listening.

If all tested $r_i = r_i' \Rightarrow$ no Eve w/ high confidence.

But: There is always noise $\Rightarrow$ some ratio of $r_i \neq r_i'$.

$\Rightarrow$ i) Attribute all noise to Eve.

(= Eve is in control of environment)

$\rightarrow$ Most conservative assumption

$\rightarrow$ Noise = Eve who ignores (traces) some info

ii) A & B estimate noise level by comparing some of the $r_i \stackrel{?}{=} r_i'$.

iii) A & B perform privacy amplification:

Simple version:

E knows every bit w/ prob. p

$\Rightarrow$ make "super-bit" $= r_1 \oplus r_2 \oplus \dots \oplus r_k$

$\Rightarrow$ known by Eve w/ prob p^k / dep.

on knowledge of all bits!!

In practice: Use Hash functions $\{0,1\}^* \to \{0,1\}^k$

- some kind of checksum w/ strong dep. (distance!)
  or flipping any bit – similar to ECC.

$\Longrightarrow$ Secret 1-time pad!

Note: • Rigorous proof very subtle, & dep. on proof etc. E.g. Eve could use collective attacks,
or store q. info until A&B communicate etc.

• Hardware can be susceptible to attacks $\longrightarrow$
$\to$ device-indep. q. crypto only based on correlations of classical output distribution ($\to$ Bell!)