Padova, 25.05.23
Q comm School

Security of QKD — Ramona Wolf (ETH Zürich)

We can give a mathematical security proof for QKD protocols

→ this is the advantage of quantum cryptography over its classical counterpart!

→ we have to be very precise in various aspects; definitions, assumptions, ...

Questions:

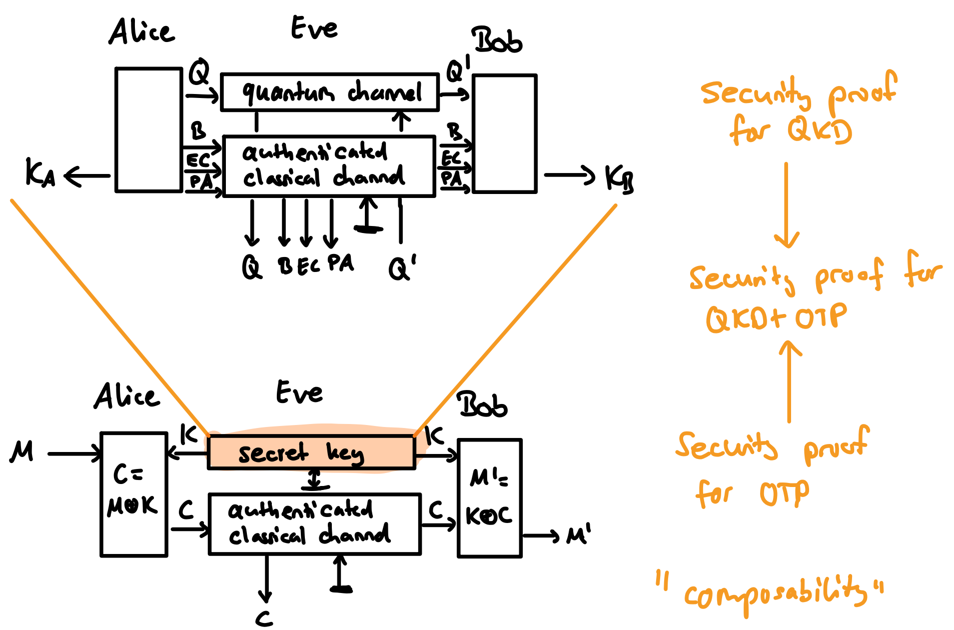
1. What does it mean for a cryptographic scheme to be secure?
   Security definition; approximations; quantitative measures

2. What assumptions enter the security proof?
   What does it mean that the security is based on quantum theory? Where does the Schrödinger equation enter? Quantum gravity?

Before we attempt to answer these questions, we need to emphasize that cryptographic schemes do not exist isolated;
(graphical notation shows flow of information)

QKD:

OTP:

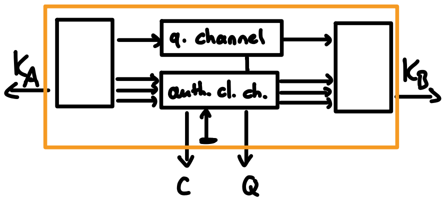


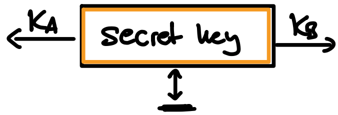
Let's move to the first question: How to define security for a cryptographic scheme?

<u>The "real world - ideal world" paradigm</u>: Define ideal functionality and show that the real scheme is close to it.

Real world | Ideal world

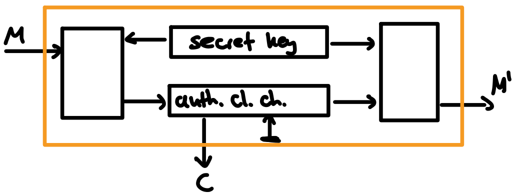
QKD:

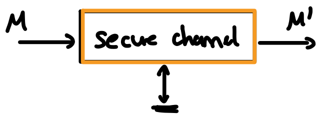




such that $K_A = K_B$ uniformly random

OTP:





such that $M = M'$

Note: The ideal cryptosystem is secure by definition.
"security" $\longrightarrow$ "functionality of the ideal system"
(can capture more general properties, e.g., randomness)

<u>Tasks</u>: (i) Identify ideal functionality for QKD scheme

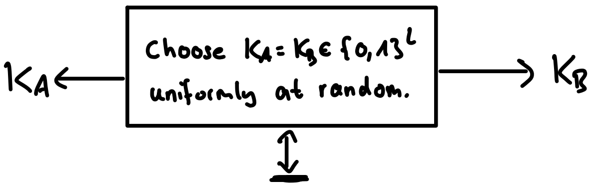
(ii) Identify a distance measure to estimate how far the real system is from the ideal one.

(i) What is the ideal QKD functionality?

To guarantee information-theoretic security, a key has to fulfill the following properties:

1. $K_A = K_B$
2. uniformly random key (each possible key is equally likely, i.e., for a key of length l: $\Pr[K=k] = 2^{-l}$ for all $k \in \{0,1\}^l$)
3. It is secret, i.e., only Alice and Bob know it.

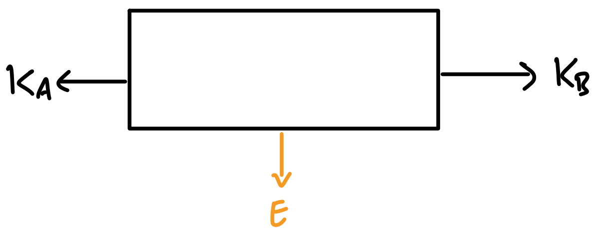
Perfect l-bit key:



$$\rho^{\text{ideal}}_{K_A K_B} = \frac{1}{2^l} \sum_{k \in \{0,1\}^l} |k\rangle\langle k|_{K_A} \otimes |k\rangle\langle k|_{K_B}$$

Trivially different from real scheme because of different interface for Eve

Add interface for Eve:



$$\rho^{\text{ideal}}_{K_A K_B E} = \frac{1}{2^l} \sum_{k \in \{0,1\}^l} |k\rangle\langle k|_{K_A} \otimes |k\rangle\langle k|_{K_B} \otimes \rho_E$$

We don't need the real scheme to be equal to the ideal one; It suffices if it is (arbitrarily) close.

$\longrightarrow$ We need a distance measure that captures this in a sensible way

(ii) Identify a distance measure

(Keep in mind the aspect of composability)

How far is ρ^{real} from ρ^{ideal}?

Trace distance: $D(\rho^{real}, \rho^{ideal}) = \frac{1}{2} \| \rho^{real} - \rho^{ideal} \|_1$,

$$\| \rho \|_1 = \mathrm{Tr} \sqrt{\rho^\dagger \rho}$$

Why is this a good choice? Operational interpretation:

- $D(\rho, \sigma)$ quantifies how distinguishable two states are fundamentally.
  $\longrightarrow$ Independent of how Alice & Bob use the key, if it is close to a perfect key this doesn't change:
  $$D(\mathcal{E}(\rho^{real}), \mathcal{E}(\rho^{ideal})) \leq D(\rho^{real}, \rho^{ideal})$$
- $D(\rho^{real}, \rho^{ideal}) = \varepsilon$ can be interpreted as the failure probability of the protocol generating ρ^{real}: With probability $1-\varepsilon$, the protocol generates ρ^{ideal}.

Security definition

A QKD protocol is ε-secure if

$$\frac{1}{2} \| \rho^{real}_{K_A K_B E} - \rho^{ideal}_{K_A K_B E} \|_1 \leq \varepsilon,$$

where $\rho^{ideal}_{K_A K_B E} = \frac{1}{2^l} \sum_{k \in \{0,1\}^l} |k\rangle\langle k|_{K_A} \otimes |k\rangle\langle k|_{K_B} \otimes \rho_E$.

Remark on composability: Two keys can be composed to a single key:

Two security guarantees:

a) $\frac{1}{2} \| \rho_{K_1 E_1} - \rho_{U_{K_1}} \otimes \rho_{E_1} \|_1 \le \varepsilon_1$

b) $\frac{1}{2} \| \rho_{K_2 E_2} - \rho_{U_{K_2}} \otimes \rho_{E_2} \|_1 \le \varepsilon_2$

$$\frac{1}{2} \| \rho_{K_1 K_2 E} - \rho_{U_{K_1}} \otimes \rho_{U_{K_2}} \otimes \rho_E \|_1$$

Triangle ineq.
$$\le \underbrace{\frac{1}{2} \| \rho_{K_1 \underbrace{K_2 E}_{E_1}} - \rho_{U_{K_1}} \otimes \rho_{\underbrace{K_2 E}_{E_1}} \|_1}_{(a) \le \varepsilon_1} + \underbrace{\frac{1}{2} \| \rho_{U_{K_1}} \otimes \rho_{K_2 E} - \rho_{U_{K_1}} \otimes \rho_{U_{K_2}} \otimes \rho_E \|_1}_{\overset{\text{property of trace dist.}}{=} \underbrace{\frac{1}{2} \| \rho_{K_2 E} - \rho_{U_{K_2}} \otimes \rho_E \|_1}_{(b) \le \varepsilon_2}}$$

$$\le \varepsilon_1 + \varepsilon_2$$

$\Rightarrow$ The key $K = K_1 K_2$ is $(\varepsilon_1 + \varepsilon_2)$-secure

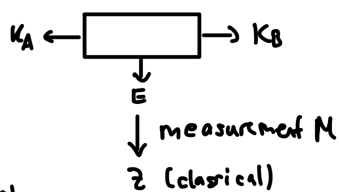
Other possible security definitions:

(To gain some intuition which properties are important)

(i) $$\underbrace{\min_{\sigma_E} \| \rho^{real}_{K_A K_B E} - \rho_{U_{K_A} U_{K_B}} \otimes \sigma_E \|_1}_{D'(\rho, \sigma)} \le \varepsilon$$

$D'(\rho, \sigma) \le D(\rho, \sigma) \le 2 D'(\rho, \sigma)$ (Connection to trace-distance)

<u>But:</u> We cannot directly add ε's as above.



(ii) Mutual information:

$$\max_M I(K_A : Z) \le \varepsilon$$

Makes sense if one considers an isolated QKD protocol, but not if you embed it into larger crypto system (e.g. with OTP).

How to prove security of a QKD protocol?

We need to show: $\frac{1}{2} \| \rho^{real}_{K_A K_B E} - \rho_{U_{K_A} U_{K_B}} \otimes \rho_E \|_1 \leq \varepsilon$

Steps in the protocol:

After the quantum phase: Raw keys R_A, R_B
- partially correlated
- partially secret

$\downarrow$ Error correction

- new strings $\tilde{K}_A = \tilde{K}_B$ (perfectly correlated)
- still partially secret

$\downarrow$ Privacy amplification (randomness extraction)

- $\tilde{K}_A = \tilde{K}_B$ still holds
- uniformly random
- independent of Eve's knowledge

Error correction

(Example that is optimal in theory)

Alice sends a compressed version of R_A to Bob, i.e., a "hash" C of R_A (public communication).

Bob guesses Alice's string R_A based on his bit string R_B and the hash C.

The length of C for optimal hash function is given by the smooth max-entropy, i.e.,

$$|C| = H_{max}^{\varepsilon_{EC}}(R_A | R_B),$$ (up to a small additive constant of order $\log \frac{1}{\varepsilon_{EC}}$)

where ε_{EC} is the failure probability of the error correction procedure.

$\rightarrow \tilde{K}_A = R_A, \quad \tilde{K}_B = f_{EC}(R_B, C)$

Privacy amplification

Alice and Bob apply a hash function f_{PA} to $\tilde{K}_A, \tilde{K}_B$.
The number of uniformly random bits K_A that can be extracted from $\tilde{K}_A$ such that

$$\rho_{K_A E} = \rho_{U_{K_A}} \otimes \rho_E$$

is given by the smooth min-entropy:

$$H_{min}^{\tilde{\varepsilon}}(\tilde{K}_A | E),$$

where $\tilde{\varepsilon}$ is the probability that the privacy amplification scheme fails

$\longrightarrow$ $K_A = f_{PA}(\tilde{K}_A)$, $K_B = f_{PA}(\tilde{K}_B)$

Connection to the security definition:

Quantum leftover hashing lemma:

$$\frac{1}{2} \| \rho_{f_{PA}(\tilde{K}_A) FE} - \rho_{U_{K_A}} \otimes \rho_{FE} \|_1 \leq 2\tilde{\varepsilon} + 2^{-1/2 (H_{min}^{\tilde{\varepsilon}}(\tilde{K}_A | E) - L + 2)}$$

$$\overset{!}{\leq} \varepsilon_{PA}$$

Choose L (the length of the key s.t. this holds)

$\longrightarrow$ The QKD protocol is $\varepsilon = \varepsilon_{EC} + \varepsilon_{PA}$ - secure.

Important quantities to evaluate in the security proof:

$$H_{max}^{\varepsilon_{EC}}(R_A, R_B)$$

$$H_{min}^{\tilde{\varepsilon}}(\tilde{K}_A | E)$$

2. Assumptions

$$\boxed{\text{Assumptions}} \xrightarrow{\text{security proof}} \boxed{\text{Security guarantee}}$$

→ Security only holds if assumptions are fulfilled!

* Alice and Bob have access to an authenticated classical channel
  (can be achieved with a small initial secret, a "password")

* The labs are isolated
  (necessary to insure that no unauthorized information leaks)

* Trust in the devices: (every trust is an assumption)
  - Device-dependent, device-independent, semi-DI
  - Trust in classical devices such as RNGs

* Quantum theory is correct:
  - We need the state space formalism + quantum channels
  - We do not need the Schrödinger equation

  What about quantum gravity?
  → Depends on what aspects of quantum theory has to be adapted
  → Can gravitational effects increase Eve's predictive power?

* Quantum theory is complete: No other theory can have improved predictive powers

  (follows from correctness + existence of free randomness)

  Counterexample: "Kish cypher", which is based on thermodynamics
  → secure within thermodynamics, not within QM.