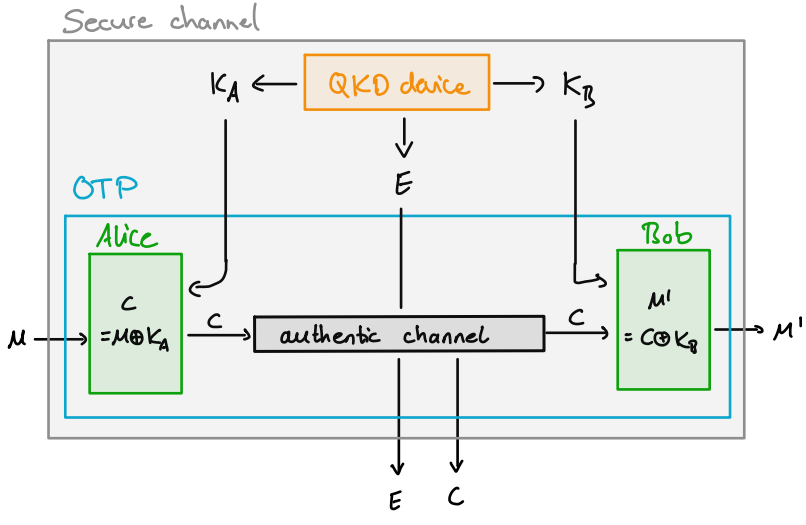
Composability

QKD Summer School
19.08.22, 13:30–14:30

QKD protocols do not exist isolated. Example: QKD device + One-time pad:

QKD device:
Security statement I

OTP protocol:
Security statement II



Goal:

Security statement of Secure channel = Security statement I + Security statement II

General idea: The security statement of a QKD protocol (or any cryptographic protocol) holds in <u>any</u> context the protocol is used.

Task: Design <u>composable</u> security definitions!

1. The problem

What can go wrong when choosing the security definition?

First, recall what we ask from a secure key:
↳ Renato's lecture (Foundation of security)

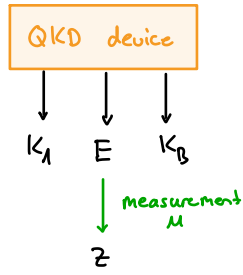
1. Alice and Bob's respective keys are equal.
2. The key is uniform.
3. Eve does not have any information about the key.

} except with probability ε

Proposal for security definition:

(i) $\Pr[K_A \neq K_B] \leq \varepsilon_1$ (captures 1.)

(ii) $\sup_M \frac{1}{2} \| P_{K_A Z} - P_U \times P_Z \| \leq \varepsilon_2$ (captures 2. + 3.)



Important: Eve is not restricted in her choice of measurement!

Remark 1: Historically, the above definition has been developed as an analog to the classical security definition. In the classical case, condition (ii) is replaced with the requirement that the mutual information between the key K_A and Eve's (classical) information Z is small:

$$I(K_A : Z) \leq \delta \quad (*)$$

A natural generalisation of this condition is to say that (*) holds for all classical information Z that Eve can get from measuring her quantum system E:

"accessible information" → $$I^{acc}(K_A:E) = \max_M I(K_A : M(E)) \leq \delta, \quad (**)$$

where $M: E \to Z$ is the map that describes Eve's measurement. It can be shown that (**) is equivalent to (ii).

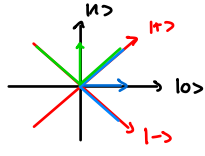
By the time this definition was developed, there was no notion of "quantum mutual information", so it was a natural choice to consider measurement outcomes, as they allow to use classical information-theoretic quantities.

This definition has been used in the early days of QKD proofs, for example by Lo & Chau and Shor & Preskill.

Remark 2: Measuring destroys information.

Example: Suppose you have a qubit in state $|0\rangle$.
If you measure it in the Hadamard basis $|+\rangle/|-\rangle$, you get the outcomes +/- both with probability $\frac{1}{2}$.
You get the same outcome distribution if your state is $|1\rangle$.

→ You cannot distinguish between $|0\rangle$ and $|1\rangle$ from measuring in $|+\rangle/|-\rangle$ basis.

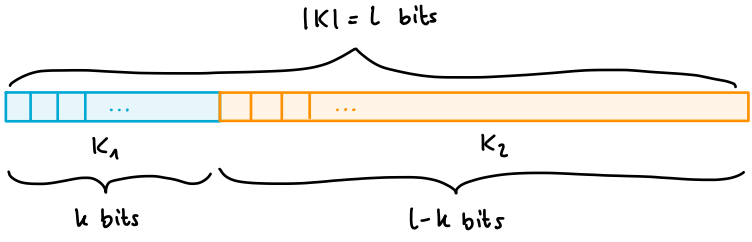


In a high-dimensional space, if you have a given basis and randomly choose another basis, with high probability the overlap is the same for all basis vectors.
→ cannot distinguish states in the original basis from measuring in a randomly chosen basis.

Q: Is a key that fulfills (i) and (ii) secure in any application?

We can construct a scenario where (i) & (ii) are fulfilled but Eve learns the key with certainty.

The weak spot is part (ii), so let's set $K \equiv K_A = K_B$.
Partition it into two parts:



Note: The following is not a situation that is very likely to actually happen during a protocol, but it is not excluded by the security definition.
It is constructed to show the weakness of the definition.

Suppose the bit string K fulfills (ii). Eve then (for some reason) learns the following information:

1. Choose a family of random unitaries (w.r.t. Haar measure):
$$\mathcal{U} \equiv \{ U_i : \mathbb{C}^{2^{l-k}} \to \mathbb{C}^{2^{l-k}}, \; i \in \{0,1\}^k \}$$
(indexed by bit strings of length k)

2. Encode K into qubits.

3. Apply the unitary $U_{K_1} \in \mathcal{U}$ (determined by K_1) to the part of the state that corresponds to K_2 and give it to Eve.

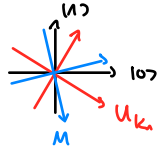
State of the system after this process:
$$\rho_{K_1 K_2 E} = \frac{1}{2^l} \sum_{k_1, k_2} |k_1 \times k_1| \otimes |k_2 \times k_2| \otimes \underbrace{U_{k_1} |k_2 \times k_2| U_{k_1}^*}_{= \rho_E^{k_1 k_2}}$$

Q: Is K still secure? I.e., is (ii) still fulfilled?

Eve measures: $(\mathcal{I}_{K_1} \otimes \mathcal{I}_{K_2} \otimes \mathcal{M}_{E \to Z})(\rho_{K_1 K_2 E})$

Eve has no information on which unitary has been applied, so her choice of measurement is random

Remark 2 ⟶



⇒ For every $|K_2 \times K_2|$, Eve sees (roughly) the same distribution, so she cannot distinguish the states

⇓

Eve has no information on the value of K_2.

Note: If $\mathcal{U}$ is small, it is possible that Eve can choose her measurement in a way that tells her some information in either basis. So $\mathcal{U}$ (and hence k) needs to be chosen large enough. (This can be quantified, but we don't do that here.)

↳ Z is independent of K, even if Eve knows $\mathcal{U}$ (given k is large enough)

⇒ K still fulfills the security criterion (ii)!

Q: Does this guarantee that it is safe to use K in any application? (It better does, otherwise this would be a useless QKD device!)

Suppose Alice and Bob use the key to encrypt messages using the OTP.

Suppose also that Eve has somehow learned the first k bits of the key (this is not unrealistic; the first part of the message could be some header information, e.g., the date or the weather forecast).

⟶ Eve knows K_1.

Does this give her access to the rest of the message (it shouldn't for a secure key)?

Case 1: Eve only holds the classical information Z she has obtained from measuring her quantum state, which does not contain information about K.
→ Learning K_1 does not help in learning K_2.

Case 2: Eve has not measured E but kept her quantum system. (Nothing forces her to actually carry out the measurement M).

After learning K_1, she can now apply $U^{-1}_{K_1}$ to $\rho_E^{K_1 K_2}$ and obtain ρ_{K_2}, and therefore K_2 with certainty.

⇒ Even though the security definition is fulfilled, Eve learns the key/message.

What went wrong?

The security definition did not consider that Eve can keep her quantum system instead of measuring it

Measuring is irreversible!

This ignores the possibility that information that Eve learns at a later time (i.e., when the key is used in an application) can help her choose the best measurement.

As protocols never exist isolated, but are part of a larger cryptographic scheme, introducing a measurement at any point is a bad idea.

→ The definition is not composable!

2. The solution

Q: How do we get a composable security definition?

↳ use the real world - ideal world paradigm (Renato's lecture)
(with trace distance)

ρ_{KE}^{real} $\qquad$ $\rho_{KE}^{ideal} = \rho_U \otimes \rho_E$

Does the state $\rho_{K_1K_2E}$ of the previous example fulfill the definition?

$$\rho_{KE}^{real} = \rho_{K_1K_2E} = \frac{1}{2^l} \sum_{k_1,k_2} |k_1\rangle\langle k_1| \otimes |k_2\rangle\langle k_2| \otimes \underbrace{U_{k_1} |k_2\rangle\langle k_2| U_{k_1}^*}_{= \rho_E^{k_1k_2}}$$

→ not close to the ideal scenario!

Remark 3: A distinguisher could perfectly distinguish between ρ_{KE}^{real} and ρ_{KE}^{ideal}. He can take the values of k_1 and k_2 and check whether Eve's state is compatible with $U_{k_1} |k_2\rangle\langle k_2| U_{k_1}^*$

In the real world, this is always the case, while in the ideal world this does not happen (except with very small probability).

→ This security definition directly shows that the key is not secure!

3. Why does the solution work?

Suppose the real world is described by a state $S_{KE}^{real} \approx^{\varepsilon} S_{KE}^{ideal}$.
Can we run into similar problems when using the key, e.g. in the OTP?
I.e., is it possible that we forgot to take something into account that Eve can exploit?

Recall: Probabilistic interpretation

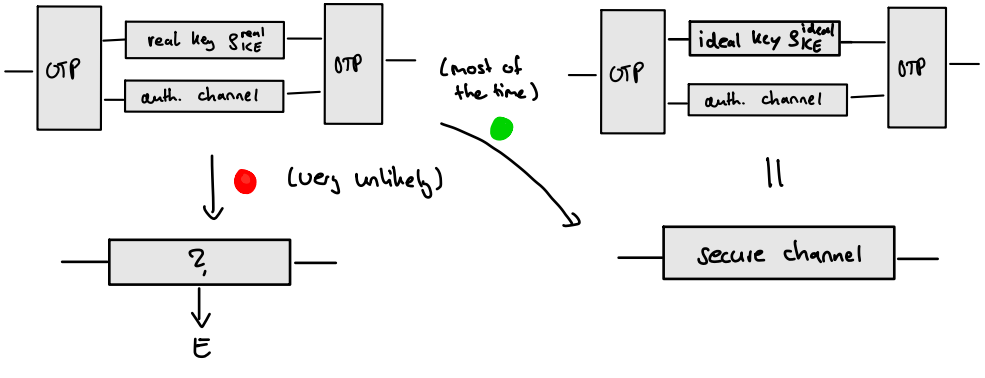
→ the events where the real system does not behave identically to the ideal system are very unlikely.

Remark 4: We have only seen this for classical random variables, but it can be generalized to quantum states.
We're not gonna do it here because it takes too much time.

Events: 🟢 $(K^{real}, E^{real}) = (K^{ideal}, E^{ideal})$ $\quad Pr[🟢] = 1-\varepsilon$

🔴 —— " —— $\neq$ —— " —— $\quad Pr[🔴] = \varepsilon$

Use the key in the OTP:



Conclusion: Using the real world - ideal world paradigm, we can be certain that when using the key in any application, the probability that something goes wrong is still at most ε.