Security of quantum key distribution

Christopher Portmann* Renato Renner†

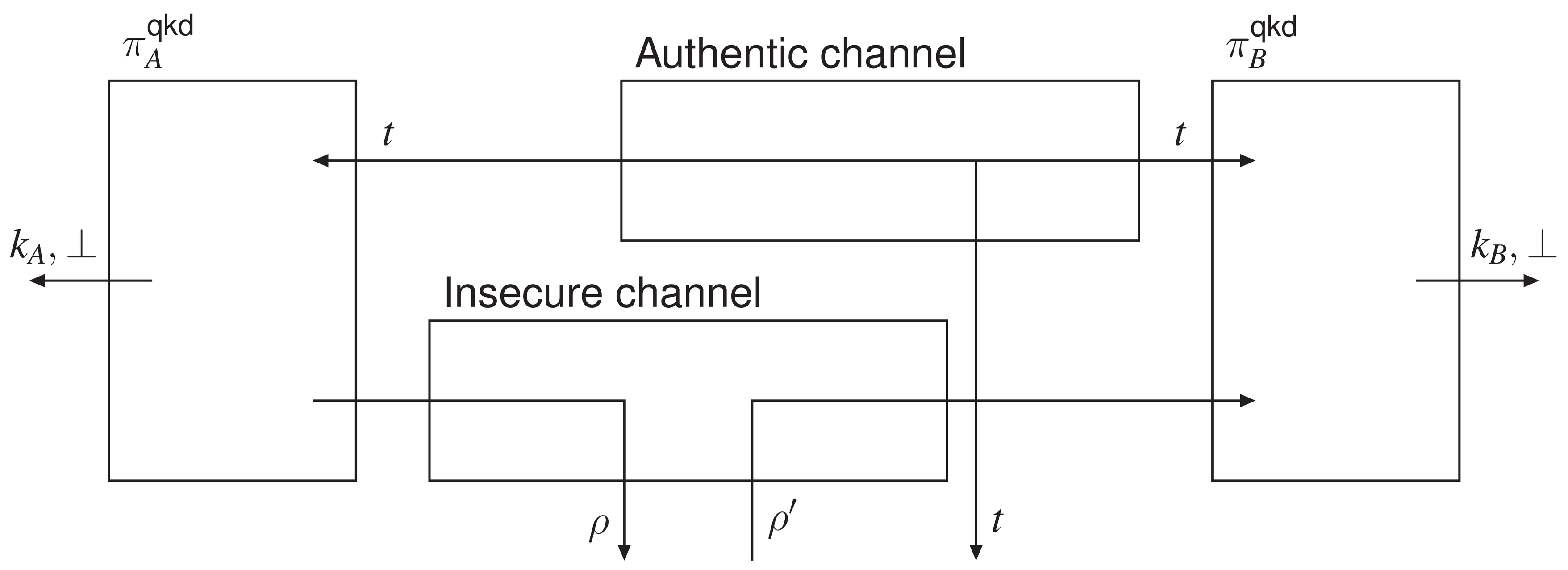
ETH zürich Institute for Theoretical Physics

Basic idea of cryptographic security

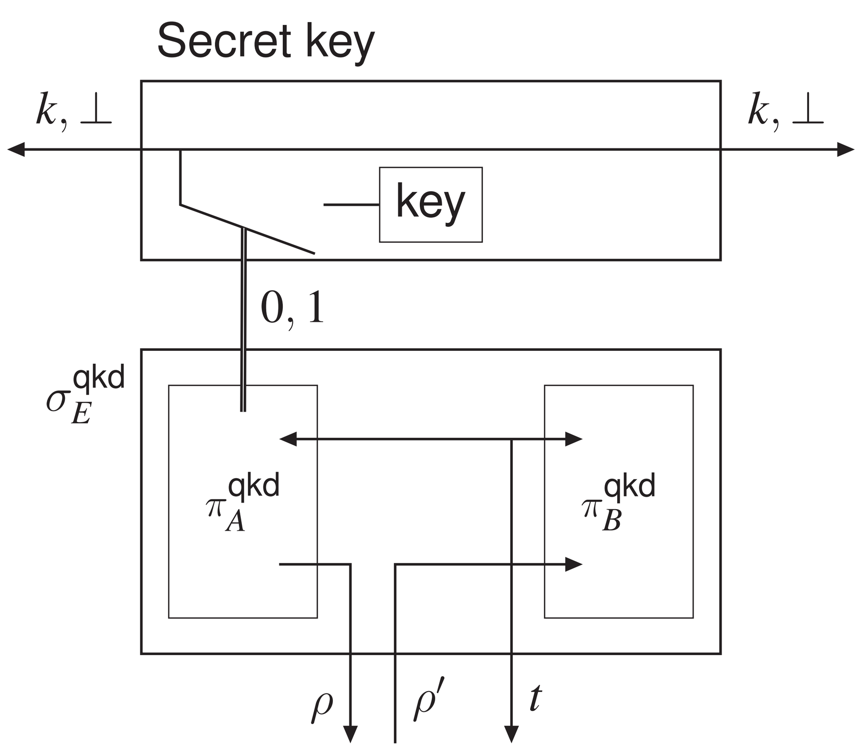
- View a protocol as constructing some resource $\mathcal{S}$ from a resource $\mathcal{R}$.
  - QKD: (authentic channel, quantum channel) $\longrightarrow$ secret key.
  - OTP: (authentic channel, secret key) $\longrightarrow$ secure channel.
- ε-security: the real and ideal systems are ε-(in)distinguishable.
  - Real system: protocol and resources used.
  - Ideal system: (ideal) resource constructed and simulator.
- Simulator:
  - Creates the real (dishonest) interface given access to the ideal interface.
  - $\Longrightarrow$ the real world does not allow a stronger attack than the ideal world.

Quantum key distribution (QKD)

A QKD protocol is ε-secure if the two systems below are ε-close in the distinguishing metric.



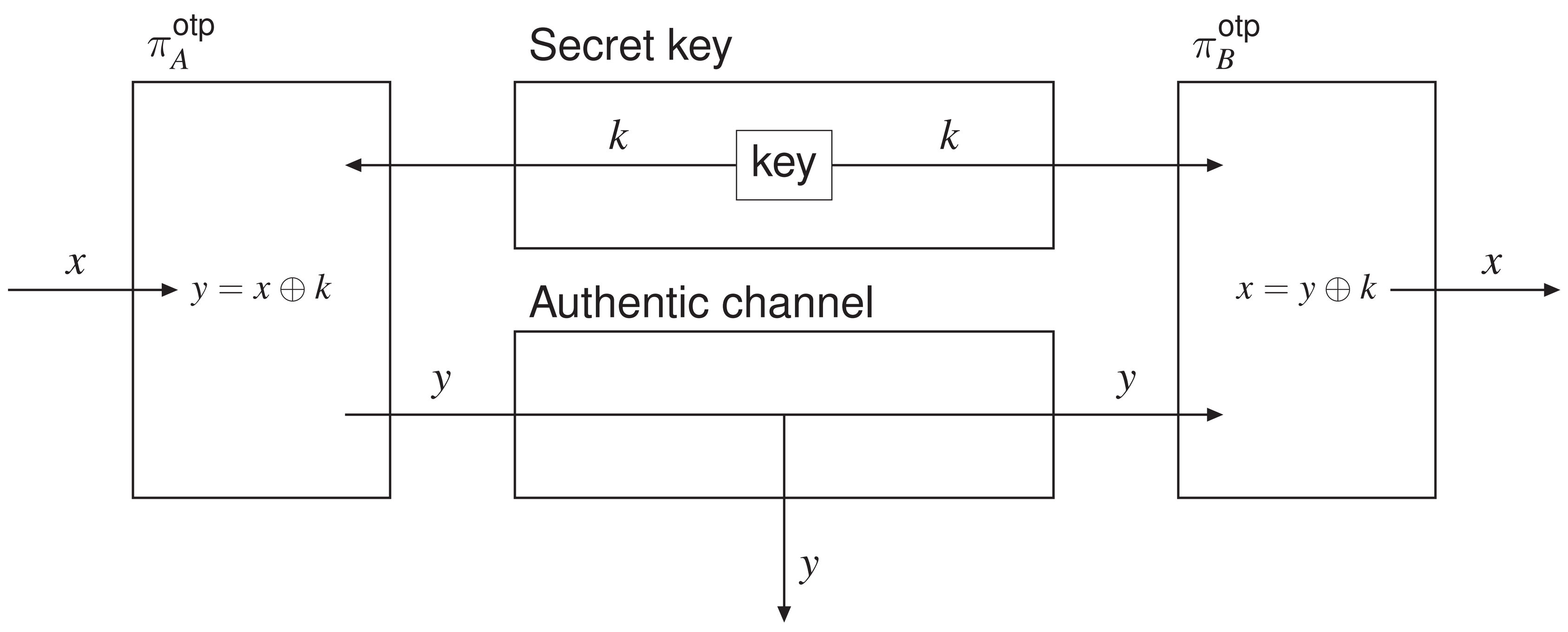
QKD protocol π^{qkd}, classical authentic channel and quantum insecure channel.



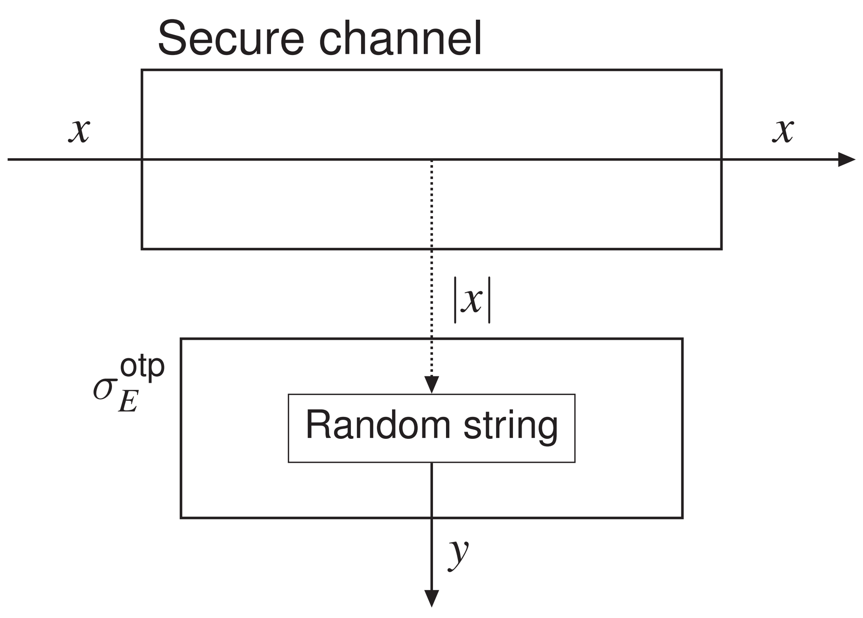
Ideal secret key and simulator σ_E^{qkd}.

One-time pad (OTP)

The OTP is perfectly (0-)secure, since the two systems below are indistinguishable.



OTP protocol π^{otp}, ideal secret key and authentic channel.



Ideal secure channel and simulator σ_E^{otp}.

Distinguishing metric

- View systems $\mathcal{R}$ and $\mathcal{S}$ as interactive black boxes.
- A distinguisher Γ can interact arbitrarily with the systems, and outputs a bit. Its advantage is
$$d(\mathcal{R},\mathcal{S}) := \max_{\Gamma} \{\Pr[\Gamma(\mathcal{R})=1] - \Pr[\Gamma(\mathcal{S})=1]\}.$$
- This metric is contractive: $d(\mathcal{RT},\mathcal{ST}) \leq d(\mathcal{R},\mathcal{S})$.
- It respects the triangle inequality: $d(\mathcal{R},\mathcal{S}) \leq d(\mathcal{R},\mathcal{T}) + d(\mathcal{T},\mathcal{S})$.

Derivation of the trace distance security criterion

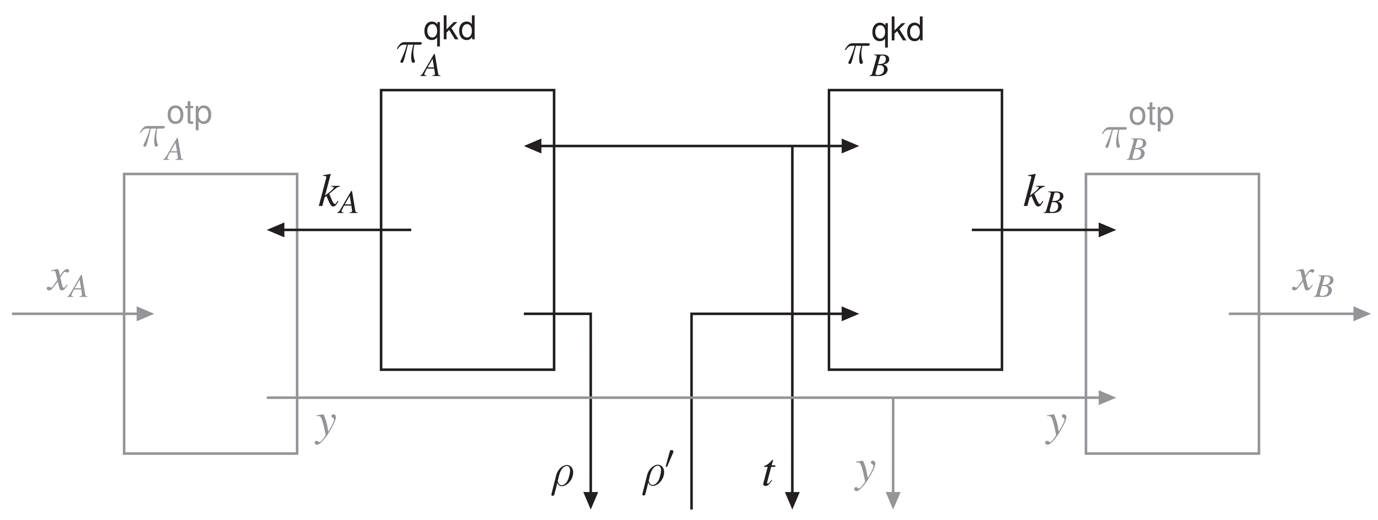
- A QKD protocol is $\varepsilon_{\mathsf{cor}}$-correct if
$$\Pr[K_A \neq K_B] \leq \varepsilon_{\mathsf{cor}},$$
where K_A and K_B are Alice and Bob's final keys.
- A QKD protocol is $\varepsilon_{\mathsf{sec}}$-secure if
$$(1 - p_{\mathsf{abort}}) d(\rho_{AE}, \tau_A \otimes \rho_E) \leq \varepsilon_{\mathsf{sec}},$$
where $d(\cdot,\cdot)$ is the trace distance, τ_A the fully mixed state and p_{abort} the probability of aborting.

Theorem: If a QKD protocol is $\varepsilon_{\mathsf{cor}}$-correct and $\varepsilon_{\mathsf{sec}}$-secure, it is $(\varepsilon_{\mathsf{cor}} + \varepsilon_{\mathsf{sec}})$-secure.

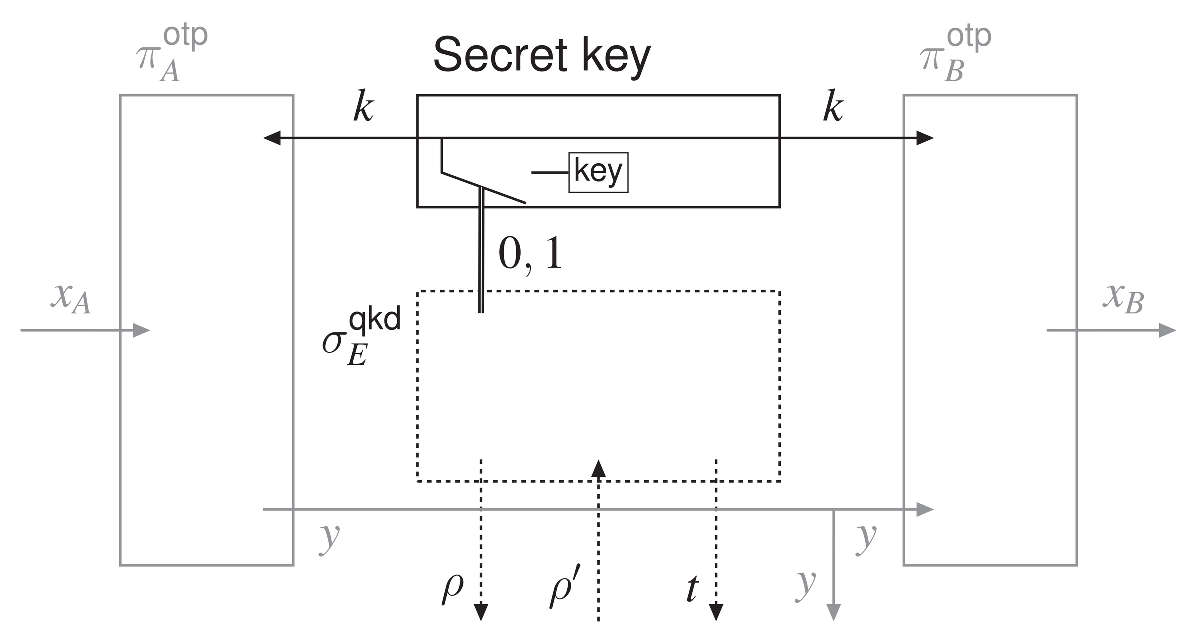
Proof sketch: Let ρ_{ABE} and $\tilde{\rho}_{ABE}$ be the states held by the distinguisher after interacting with the real and ideal systems, respectively. Define σ_{ABE} to be the state obtained from ρ_{ABE} by replacing the B system with a copy of the key in A. Then
$$\begin{aligned} d(\rho_{ABE}, \tilde{\rho}_{ABE}) &\leq d(\rho_{ABE}, \sigma_{ABE}) + d(\sigma_{ABE}, \tilde{\rho}_{ABE}) \\ &\leq \Pr[K_A \neq K_B] + (1 - p_{\mathsf{abort}}) d(\rho_{AE}, \tau_A \otimes \rho_E). \end{aligned}$$

Protocol composition

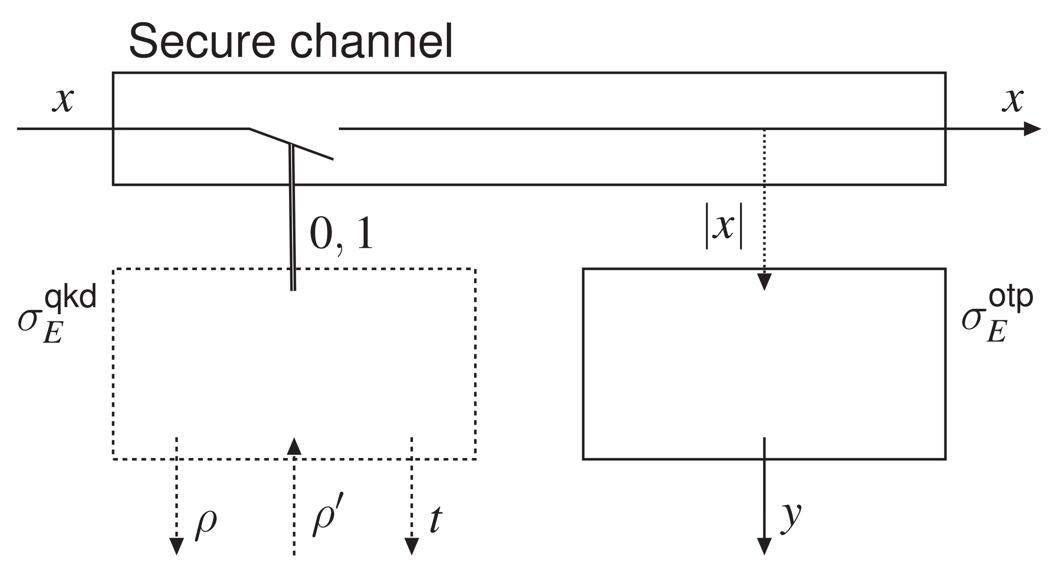
From the triangle inequality and contractivity of the distinguishing advantage, the first and last systems below are ε-close.



OTP protocol π^{otp}, QKD protocol π^{qkd}, and (implicit) communication channels.



Ideal secret key, OTP protocol π^{otp} and QKD simulator σ_E^{qkd}.



Ideal secure channel and composition of QKD and OTP simulators $\sigma_E^{\mathsf{qkd}}\sigma_E^{\mathsf{otp}}$.

*chportma@phys.ethz.ch †renner@phys.ethz.ch

QCRYPT, August 2013