Mathematical methods of quantum cryptography

Anton Trushechkin

Steklov Mathematical Institute
of Russian Academy of Sciences, Moscow

Russian Quantum Center, Skolkovo
National Research Technological University "MISIS", Moscow

Seminar "Geometry, Topology, and Their Applications",
Novosibirsk, 26th April 2021

Purposes of the talk

1. To give a general introduction into mathematics of quantum cryptography (more precisely, quantum key distribution (QKD)).

   Theoretical QKD uses complicated and beautiful mathematics, requires rigorous theorems and proofs.

2. To tell about our recent results in this field published in:
   - M. K. Bochkov, A. T., "Security of quantum key distribution with detection-efficiency mismatch in the single-photon case: Tight bounds", Phys. Rev. A, 99:3 (2019), 32308, 15 pp.
   - A. T., "Security of quantum key distribution with detection-efficiency mismatch in the multiphoton case", arXiv: 2004.07809, 18 pp.

In contrast to quantum computers, QKD is a commercial technology now.

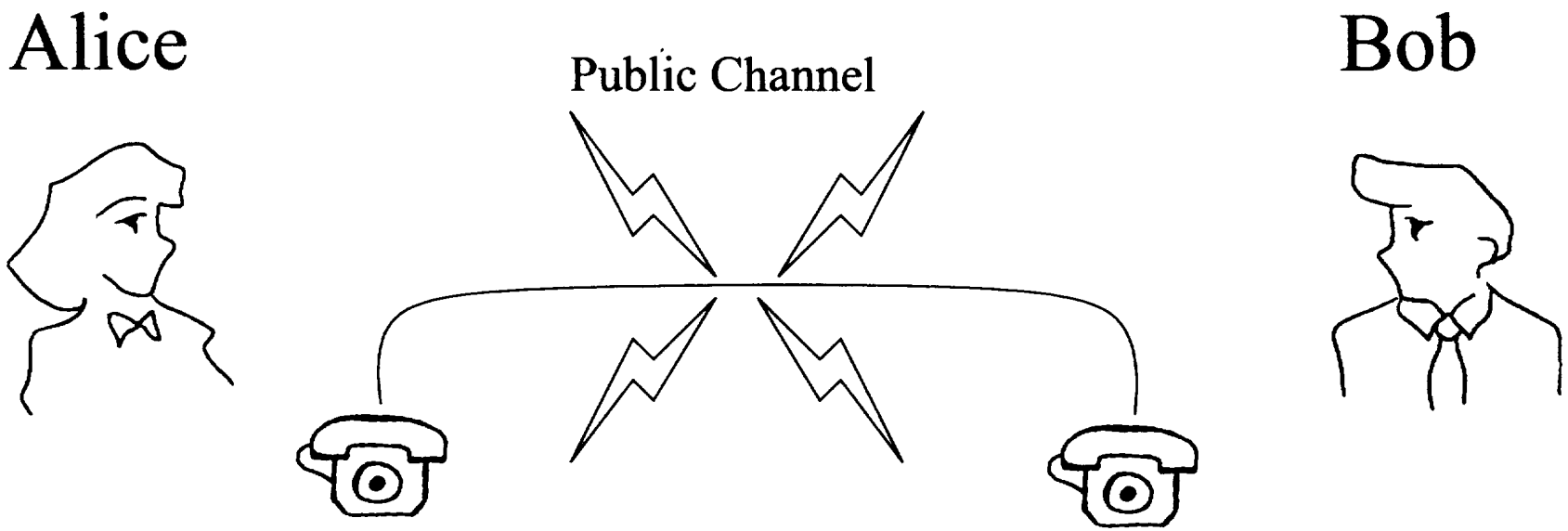
Outline

1. Key distribution problem
2. Axioms of quantum information
3. A quantum key distribution protocol
4. Security proof for the ideal case
5. Security proof for the case of detection-efficiency mismatch

Key distribution problem

Alice and Bob want to establish a common secret key (random binary string) K

This allows them to encrypt (and decrypt) a secret message M

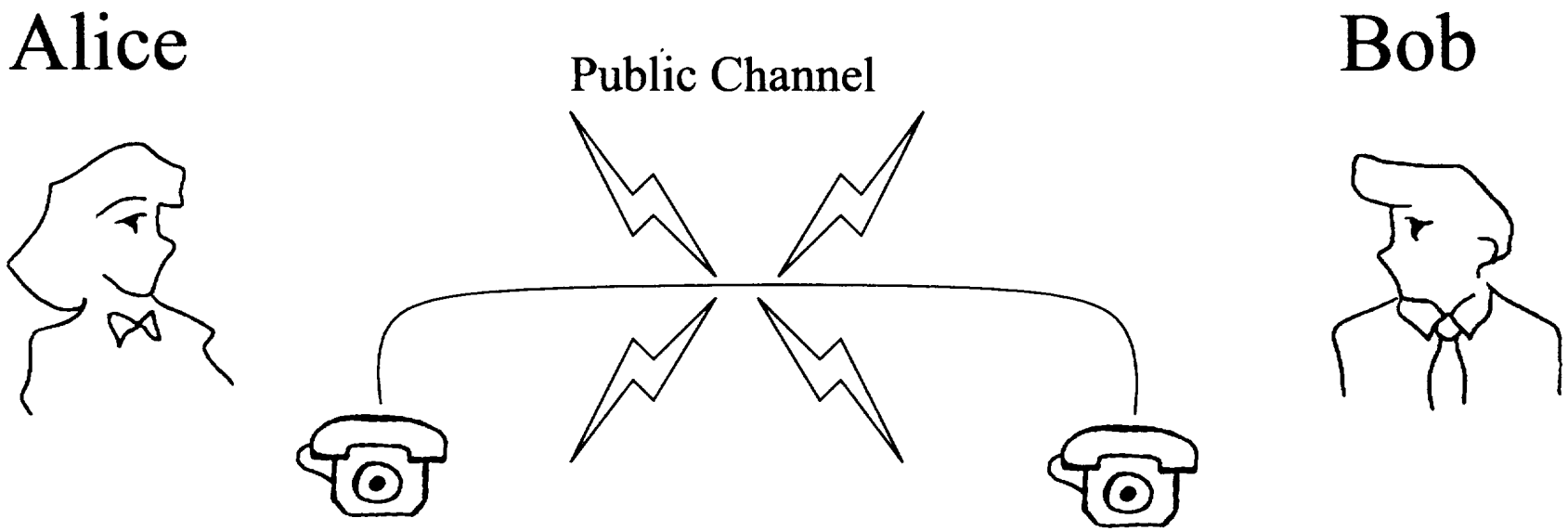


$K = 010011101$ $K = 010011101$

Key distribution problem

Alice and Bob want to establish a common secret key (random binary string) K

This allows them to encrypt (and decrypt) a secret message M



$K = 010011101$

$\oplus$

$M = 110110100$

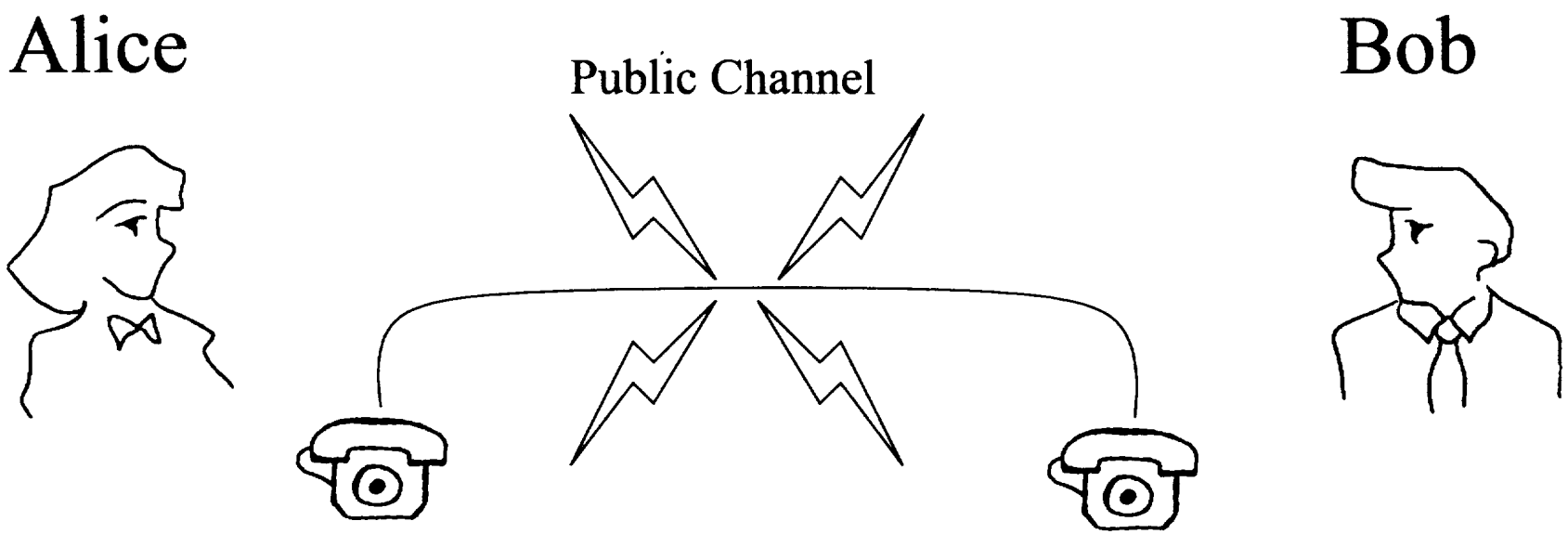
$K = 010011101$

$\oplus$

Key distribution problem

Alice and Bob want to establish a common secret key (random binary string) K

This allows them to encrypt (and decrypt) a secret message M



$K = 010011101$ $\qquad$ $K = 010011101$

$\oplus$ $\qquad$ $\oplus$

$M = 110110100$

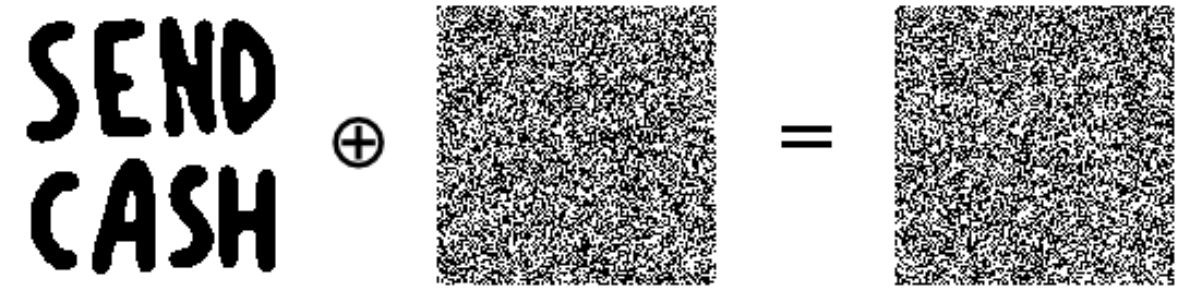
$=$

$C = 100101001$ $\xrightarrow{\text{Public channel}}$ $C = 100101001$

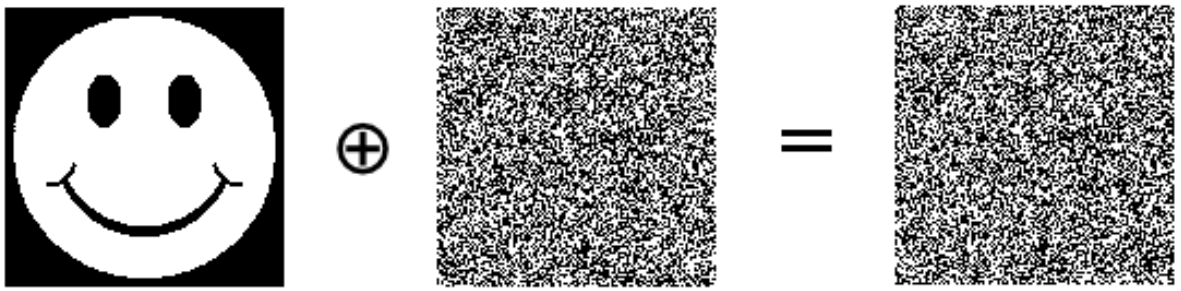
$=$

$M = 110110100$

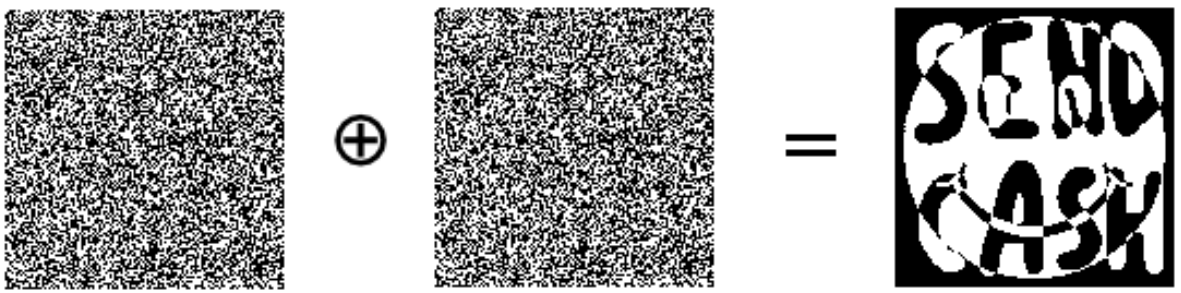
The key should be used only once!



$M_1 \oplus K = C_1$



$M_2 \oplus K = C_2$



$C_1 \oplus C_2 = M_1 \oplus M_2$

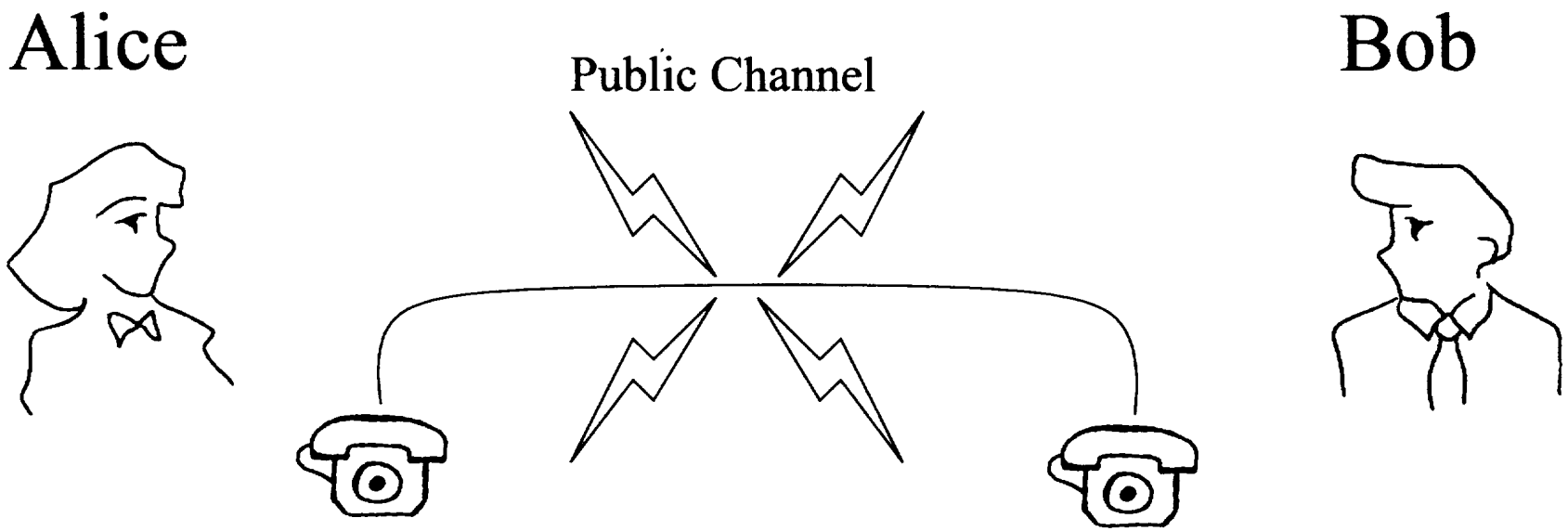
(From http://www.cryptosmith.com/)

In each cipher the key must be periodically refreshed

Key distribution problem

Alice and Bob want to establish a common secret key (random binary string) K

This allows them to encrypt (and decrypt) a secret message M

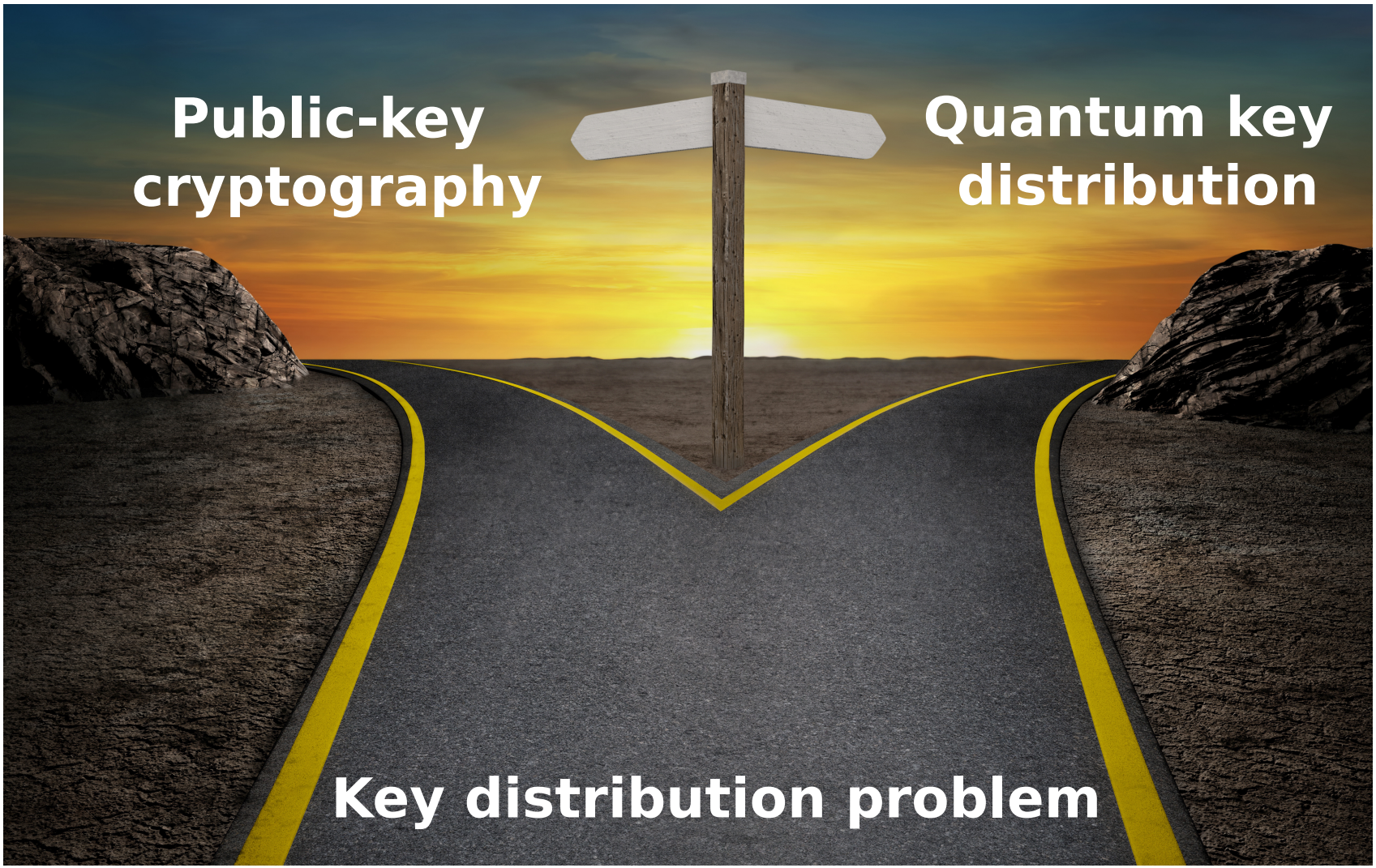


$K = 010011101$ $K = 010011101$

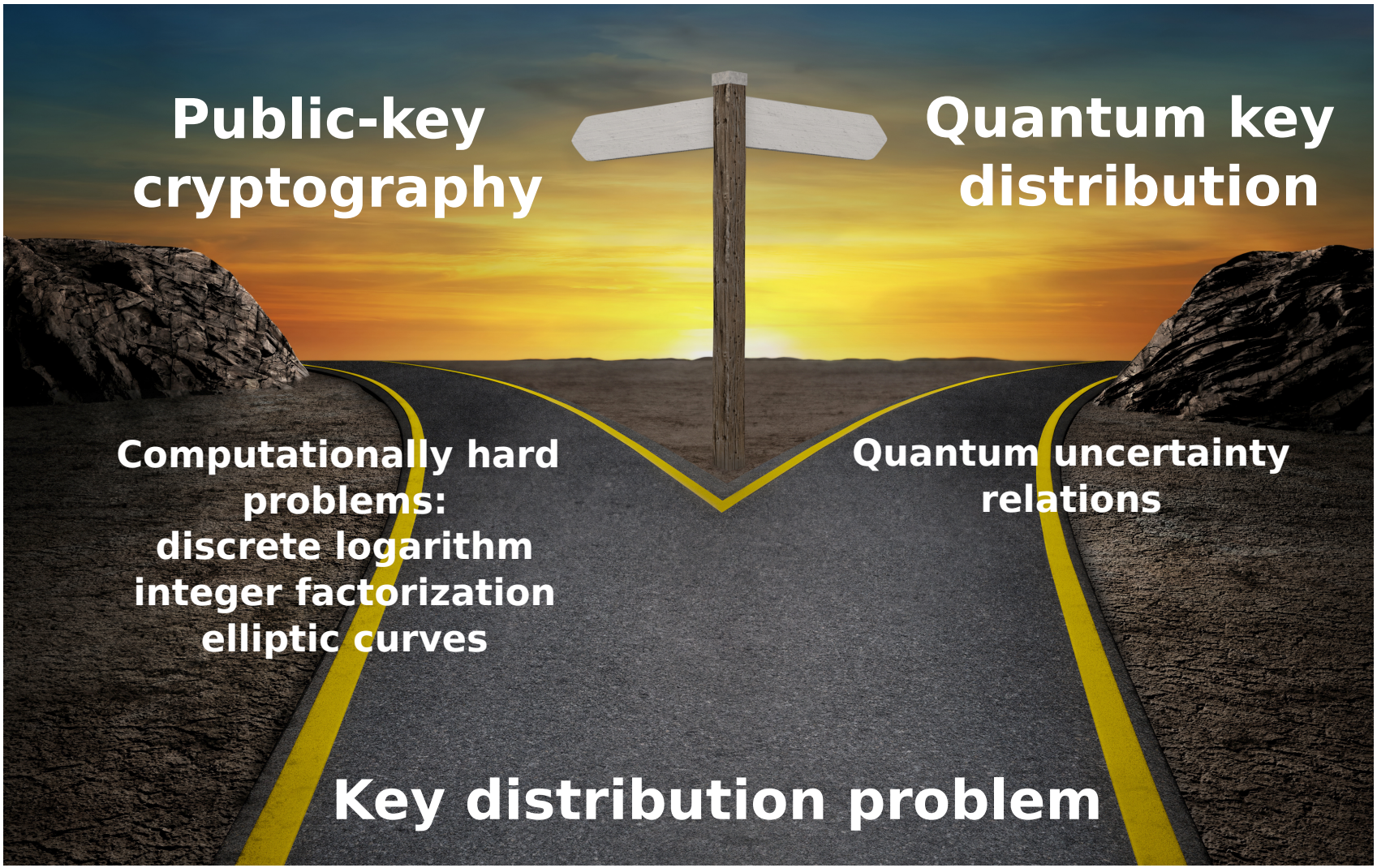
? Problem

How the common secret key using can be established using an insecure communication line? A paradox!

Key distribution problem: Establishing a secret key using an insecure channel



Key distribution problem: Establishing a secret key using an insecure channel



Problems with public-key cryptography

- Full-scale quantum computer could solve these hard problems (the celebrated Shor's algorithm, 1994)

Problems with public-key cryptography

- Full-scale quantum computer could solve these hard problems (the celebrated Shor's algorithm, 1994)

  Answer: Post-quantum public-key cryptography

Problems with public-key cryptography

- Full-scale quantum computer could solve these hard problems (the celebrated Shor's algorithm, 1994)

  Answer: Post-quantum public-key cryptography

- Progress in algorithms, computers, distributed computation, etc.

Problems with public-key cryptography

- Full-scale quantum computer could solve these hard problems (the celebrated Shor's algorithm, 1994)

  Answer: Post-quantum public-key cryptography

- Progress in algorithms, computers, distributed computation, etc.

Famous example

A message encrypted by the RSA cipher in 1977 was read in 1994

Problems with public-key cryptography

- Full-scale quantum computer could solve these hard problems (the celebrated Shor's algorithm, 1994)

  Answer: Post-quantum public-key cryptography

- Progress in algorithms, computers, distributed computation, etc.

Famous example

A message encrypted by the RSA cipher in 1977 was read in 1994

Key question

If you encrypt a secret message in 2021, are you sure that the adopted hard problem still cannot be solved in 2041?

Quantum key distribution is the only way to provide:

- Unconditional security, i.e., not relying on computational or other technological assumptions,

  and

- Everlasting security: If you do not break a QKD protocol during its operation, then you have no way to compute the key in future.

Quantum key distribution

General idea

Utilization the quantum uncertainty relations

Quantum key distribution

General idea

Utilization the quantum uncertainty relations

- For a classical (macroscopic) signal: no uncertainty, all information can be read out

Quantum key distribution

General idea

Utilization the quantum uncertainty relations

- For a classical (macroscopic) signal: no uncertainty, all information can be read out

Reduce the intensity down to the single-photon level

Quantum key distribution

General idea

Utilization the quantum uncertainty relations

- For a classical (macroscopic) signal: no uncertainty, all information can be read out

Reduce the intensity down to the single-photon level

- For single photon: Quantum uncertainty relations prevent one to read the full information about its state.

Outline

1. Key distribution problem
2. **Axioms of quantum information**
3. A quantum key distribution protocol
4. Security proof for the ideal case
5. Security proof for the case of detection-efficiency mismatch

Axioms of quantum information: 1. Systems and states

- Quantum system: a Hilbert space $\mathcal{H}$
- Quantum state (density operator): a trace-class, self-adjoint, and positive-definite operator ρ on $\mathcal{H}$: $\rho = \rho^*$, $\rho \geq 0$, $\mathrm{Tr}\,\rho = 1$
- If $\rho = P_\psi$ is a projector onto a unit vector ψ, then the state ρ is pure, otherwise – mixed.

Axioms of quantum information: 2. Observables

- Observable: self-adjoint operator X
  (an analogue of a random variable), the expectation value:

$$\mathbb{E}[X] = \mathrm{Tr}(X\rho); \qquad \mathrm{Tr}(XP_\psi) = (\psi, X\psi)$$

- Spectrum of X is the set of possible outcomes of the measurement

Axioms of quantum information: 3. Composite systems

$$\left.\begin{array}{l} \text{Space } \mathcal{H}_A, \text{ state } \rho_A \\ \text{Space } \mathcal{H}_B, \text{ state } \rho_B \end{array}\right\}$$

Axioms of quantum information: 3. Composite systems

$$\left.\begin{array}{l}\text{Space } \mathcal{H}_A,\ \text{state } \rho_A \\ \text{Space } \mathcal{H}_B,\ \text{state } \rho_B\end{array}\right\} \text{Space } \mathcal{H}_A \otimes \mathcal{H}_B,\ \text{state } \rho_A \otimes \rho_B$$

Axioms of quantum information: 3. Composite systems

$$\left.\begin{array}{l}\text{Space } \mathcal{H}_A,\ \text{state } \rho_A \\ \text{Space } \mathcal{H}_B,\ \text{state } \rho_B\end{array}\right\} \text{Space } \mathcal{H}_A \otimes \mathcal{H}_B,\ \text{state } \rho_A \otimes \rho_B$$

$$\begin{array}{l}\text{Space } \mathcal{H}_A \otimes \mathcal{H}_B, \text{ state } \rho_{AB} \\ \text{(not necessarily } \rho_A \otimes \rho_B)\end{array} \begin{array}{l}\nearrow\ \rho_A = \\ \searrow\ \rho_B =\end{array}$$

Axioms of quantum information: 3. Composite systems

$$\left.\begin{array}{l}\text{Space } \mathcal{H}_A,\ \text{state } \rho_A \\ \text{Space } \mathcal{H}_B,\ \text{state } \rho_B\end{array}\right\} \text{Space } \mathcal{H}_A \otimes \mathcal{H}_B,\ \text{state } \rho_A \otimes \rho_B$$

$$\text{Space } \mathcal{H}_A \otimes \mathcal{H}_B, \text{ state } \rho_{AB} \text{ (not necessarily } \rho_A \otimes \rho_B) \begin{array}{l}\nearrow\ \rho_A = \operatorname{Tr}_B \rho_{AB} \\ \searrow\ \rho_B = \operatorname{Tr}_A \rho_{AB}\end{array}$$

Axioms of quantum information: 3. Composite systems

$$\left.\begin{array}{l}\text{Space } \mathcal{H}_A,\ \text{state } \rho_A \\ \text{Space } \mathcal{H}_B,\ \text{state } \rho_B\end{array}\right\} \text{Space } \mathcal{H}_A \otimes \mathcal{H}_B,\ \text{state } \rho_A \otimes \rho_B$$

$$\text{Space } \mathcal{H}_A \otimes \mathcal{H}_B, \text{ state } \rho_{AB} \quad (\text{not necessarily } \rho_A \otimes \rho_B) \quad \nearrow \rho_A = \operatorname{Tr}_B \rho_{AB} \quad \searrow \rho_B = \operatorname{Tr}_A \rho_{AB}$$

Partial trace Tr_B: $\mathfrak{T}(\mathcal{H}_A \otimes \mathcal{H}_B) \to \mathfrak{T}(\mathcal{H}_A)$,

$$\operatorname{Tr}(\rho_A X) = \operatorname{Tr}[\rho_{AB}(X \otimes I_B)]$$

for all $X \in \mathfrak{B}(\mathcal{H}_A)$

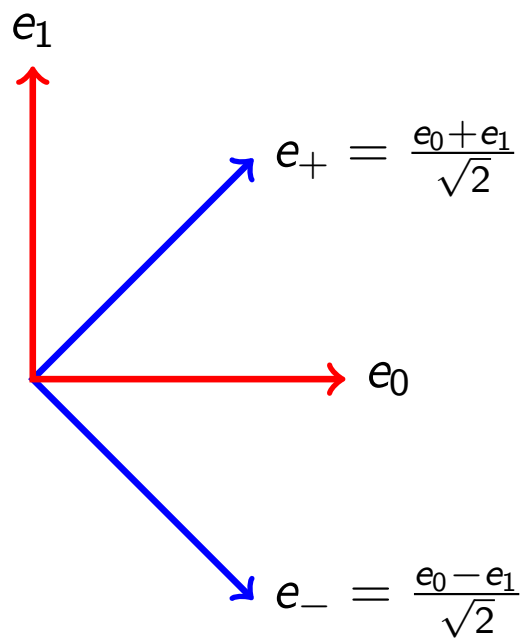
$\mathfrak{T}$ – trace-class operators
$\mathfrak{B}$ – bounded operators

Qubit. Pauli operators

- A single photon with the polarization as an information carrier: the Hilbert space $\mathbb{C}^2$ (qubit, quantum bit)

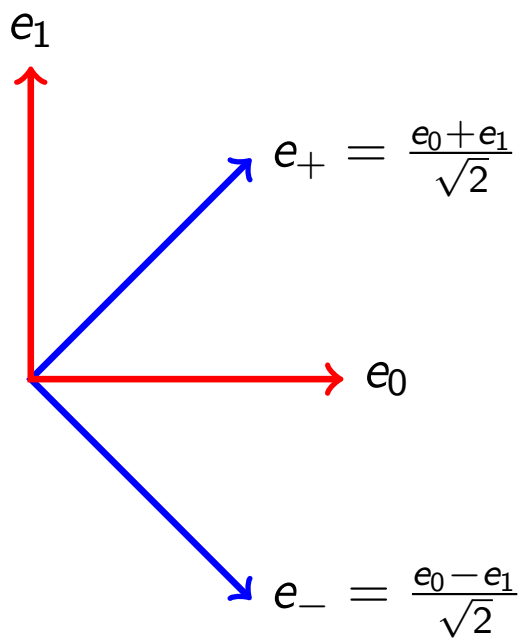
Qubit. Pauli operators

- A single photon with the polarization as an information carrier: the Hilbert space $\mathbb{C}^2$ (qubit, quantum bit)
- Two orthonormal bases:



Qubit. Pauli operators

- A single photon with the polarization as an information carrier: the Hilbert space $\mathbb{C}^2$ (qubit, quantum bit)
- Two orthonormal bases:



- Pauli operators (observables):

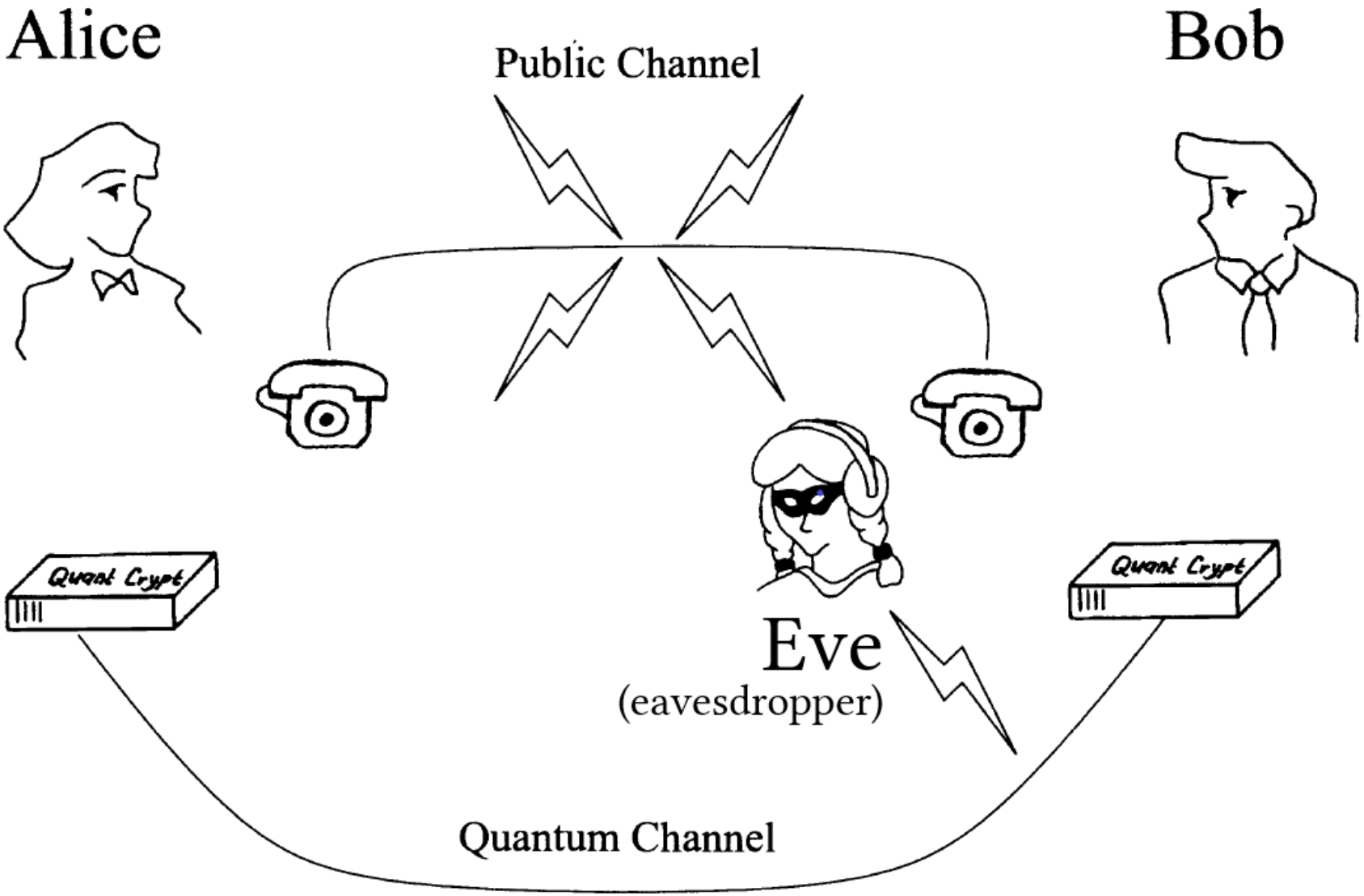
$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = P_{e_0} - P_{e_1}, \qquad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = P_{e_+} - P_{e_-}$$

- σ_z and σ_x do not commute $\Rightarrow$ Uncertainty relations

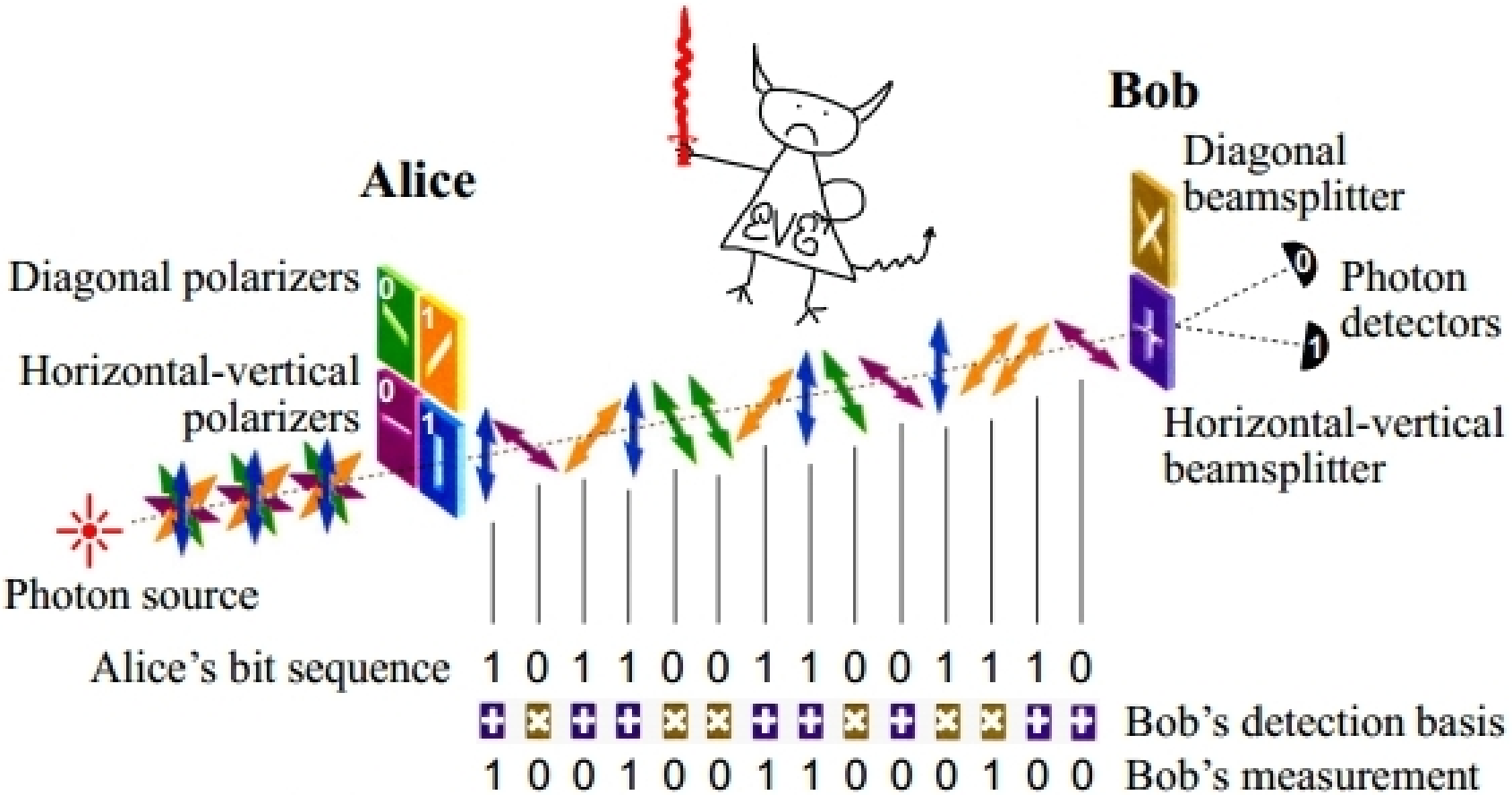
Outline

1. Key distribution problem
2. Axioms of quantum information
3. **A quantum key distribution protocol**
4. Security proof for the ideal case
5. Security proof for the case of detection-efficiency mismatch

Quantum and classical (public) channels



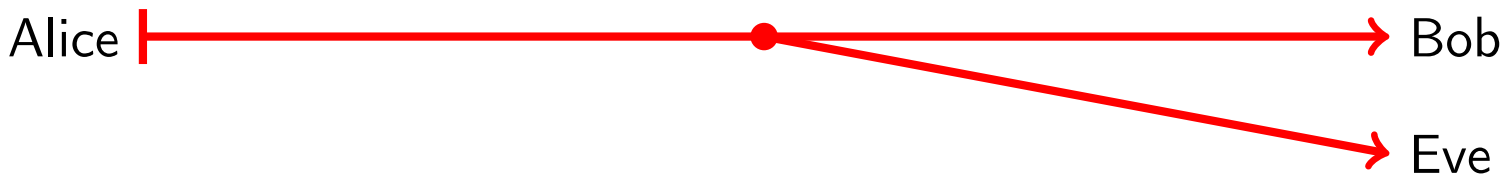
BB84 protocol: Quantum channel



C. H. Bennett, G. Brassard, Quantum cryptography: Public key distribution and Coin tossing, 1984

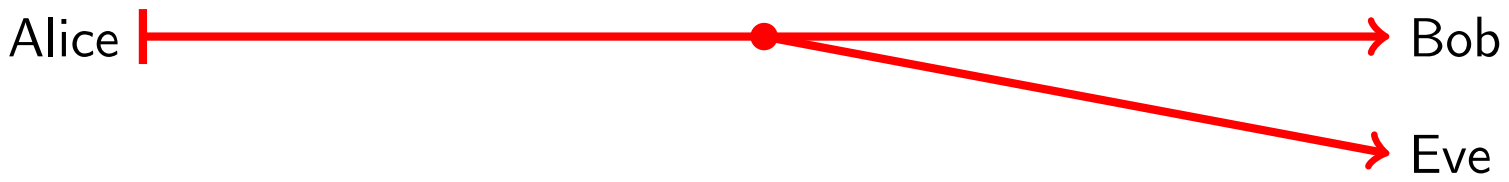
Symmetric (entanglement-based) formulation

Actual picture: Alice prepares and sends quantum states, Bob measures

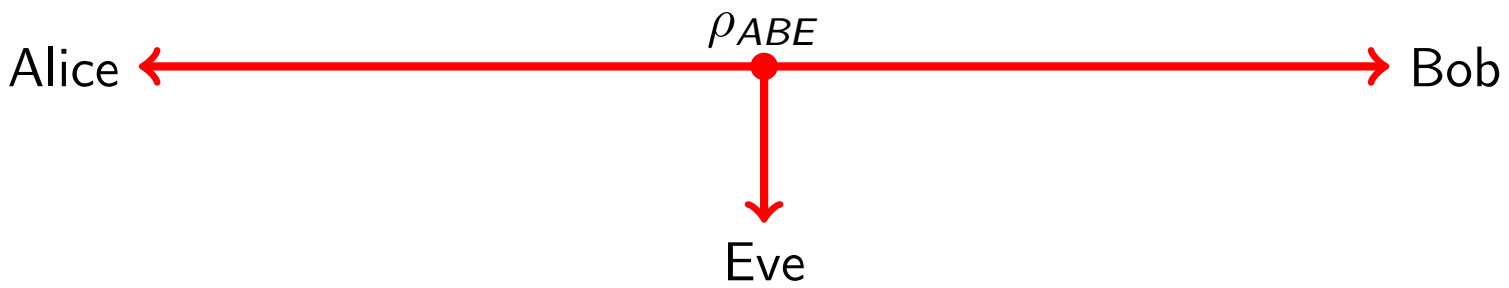


Symmetric (entanglement-based) formulation

Actual picture: Alice prepares and sends quantum states, Bob measures

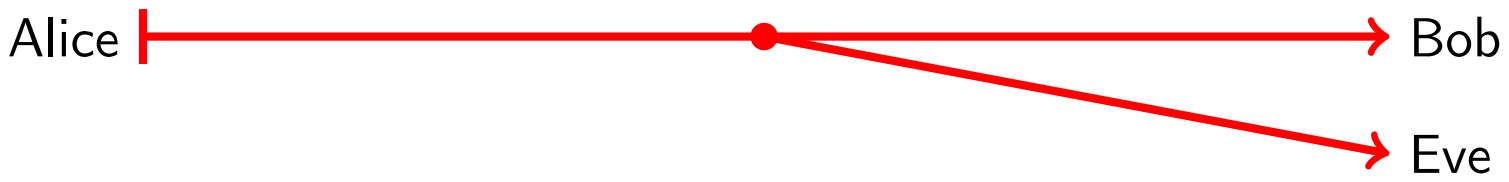


Equivalent symmetric picture: A source (controlled by Eve) prepares a (pure) tripartite state ρ_{ABE}, Alice and Bob measure their parts

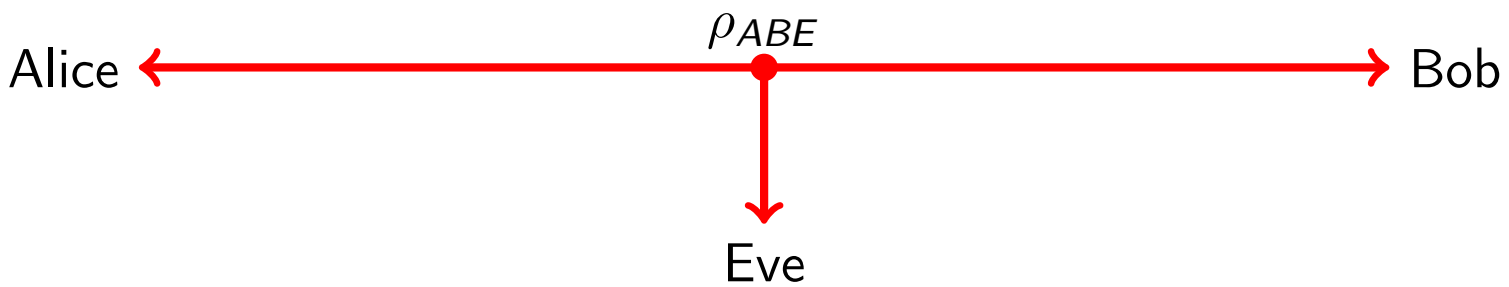


Symmetric (entanglement-based) formulation

Actual picture: Alice prepares and sends quantum states, Bob measures



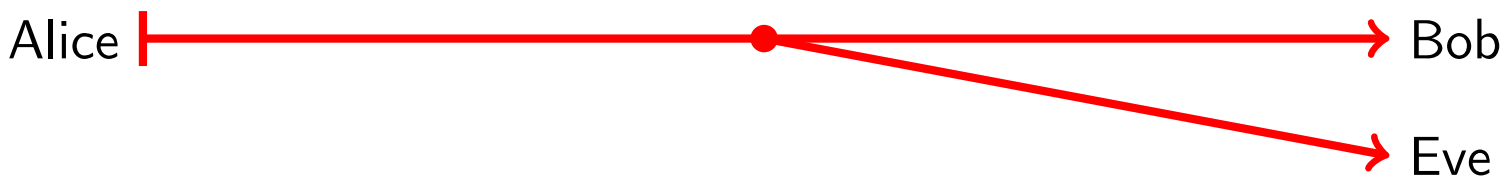
Equivalent symmetric picture: A source (controlled by Eve) prepares a (pure) tripartite state ρ_{ABE}, Alice and Bob measure their parts



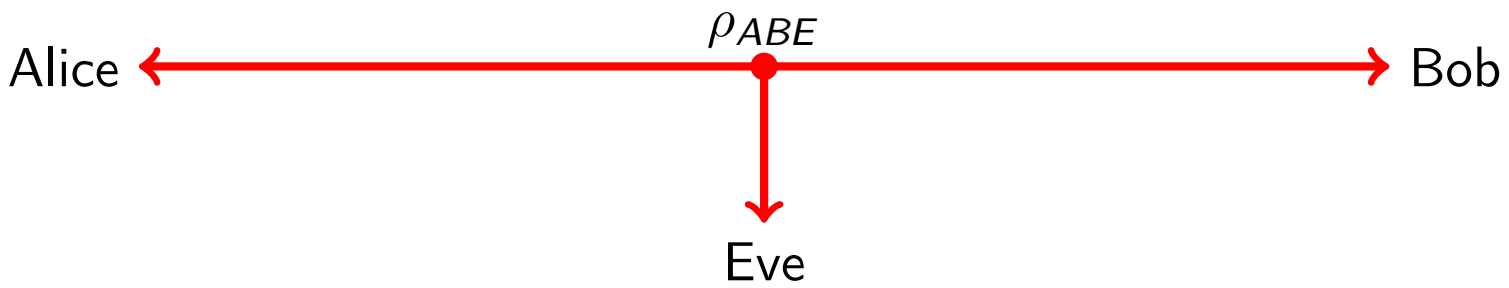
Intuition: Alice "measures" her part and get knowledge what she has sent.

Symmetric (entanglement-based) formulation

Actual picture: Alice prepares and sends quantum states, Bob measures



Equivalent symmetric picture: A source (controlled by Eve) prepares a (pure) tripartite state ρ_{ABE}, Alice and Bob measure their parts



Intuition: Alice "measures" her part and get knowledge what she has sent.

The state $\rho_{ABE} \in \mathfrak{T}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E)$ and even the dimensionality of the Eve's Hilbert space $\mathcal{H}_E$ are unknown for Alice and Bob

Outline

1. Key distribution problem
2. Axioms of quantum information
3. A quantum key distribution protocol
4. **Security proof for the ideal case**
5. Security proof for the case of detection-efficiency mismatch

Transformations of quantum states after the Alice's measurement

$\rho_{ABE} \in \mathfrak{T}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E)$

- $\mathcal{H}_A = \mathbb{C}^2$ (polarized single photon)
- $\mathcal{H}_B = \mathbb{C}^2$, but an infinite-dimensional later
- $\mathcal{H}_E$: unknown (arbitrary)

Alice's measurement of σ_z:

$$\mathcal{Z}(\rho_{ABE}) = (P_{e_0} \otimes I_{BE})\rho_{ABE}(P_{e_0} \otimes I_{BE}) + (P_{e_1} \otimes I_{BE})\rho_{ABE}(P_{e_1} \otimes I_{BE}) = \rho_{ZBE}$$

Alice's measurement of σ_x:

$$\mathcal{X}(\rho_{ABE}) = (P_{e_+} \otimes I_{BE})\rho_{ABE}(P_{e_+} \otimes I_{BE}) + (P_{e_-} \otimes I_{BE})\rho_{ABE}(P_{e_-} \otimes I_{BE}) = \rho_{XBE}$$

Von Neumann entropy and relative entropy

Von Neumann entropy of a quantum state:

$$H(\rho) = -\operatorname{Tr}(\rho \log_2 \rho) = -\sum_j \alpha_j \log_2 \alpha_j,$$

where α_j are eigenvalues of ρ

Von Neumann entropy and relative entropy

Von Neumann entropy of a quantum state:

$$H(\rho) = -\operatorname{Tr}(\rho \log_2 \rho) = -\sum_j \alpha_j \log_2 \alpha_j,$$

where α_j are eigenvalues of ρ

Conditional entropy: for a given state of a composite system ρ_{AB},

$$H(A|B) = H(\rho_{AB}) - H(\rho_B)$$

Von Neumann entropy and relative entropy

Von Neumann entropy of a quantum state:

$$H(\rho) = -\operatorname{Tr}(\rho \log_2 \rho) = -\sum_j \alpha_j \log_2 \alpha_j,$$

where α_j are eigenvalues of ρ

Conditional entropy: for a given state of a composite system ρ_{AB},

$$H(A|B) = H(\rho_{AB}) - H(\rho_B) = -D(\rho_{AB} \| I_A \otimes \rho_B)$$

Relative entropy:

$$D(\rho\|\sigma) = \operatorname{Tr}(\rho \log_2 \rho) - \operatorname{Tr}(\rho \log_2 \sigma)$$

Von Neumann entropy and relative entropy

Von Neumann entropy of a quantum state:

$$H(\rho) = -\operatorname{Tr}(\rho \log_2 \rho) = -\sum_j \alpha_j \log_2 \alpha_j,$$

where α_j are eigenvalues of ρ

Conditional entropy: for a given state of a composite system ρ_{AB},

$$H(A|B) = H(\rho_{AB}) - H(\rho_B) = -D(\rho_{AB} \| I_A \otimes \rho_B)$$

Relative entropy:

$$D(\rho\|\sigma) = \operatorname{Tr}(\rho \log_2 \rho) - \operatorname{Tr}(\rho \log_2 \sigma)$$

$D(\rho\|\sigma)$ is jointly convex (Lieb, 1973)

Von Neumann entropy and relative entropy

Von Neumann entropy of a quantum state:

$$H(\rho) = -\operatorname{Tr}(\rho \log_2 \rho) = -\sum_j \alpha_j \log_2 \alpha_j,$$

where α_j are eigenvalues of ρ

Conditional entropy: for a given state of a composite system ρ_{AB},

$$H(A|B) = H(\rho_{AB}) - H(\rho_B) = -D(\rho_{AB} \| I_A \otimes \rho_B)$$

Relative entropy:

$$D(\rho\|\sigma) = \operatorname{Tr}(\rho \log_2 \rho) - \operatorname{Tr}(\rho \log_2 \sigma)$$

$D(\rho\|\sigma)$ is jointly convex (Lieb, 1973)

$$D(\Phi(\rho)\|\Phi(\sigma)) \leq D(\rho\|\sigma)$$

for any positive and trace-preserving map Φ (Lindblad, 1976; Müller-Hermes and Reeb, 2017)

Devetak–Winter formula for the maximal secret key rate

- For a given tripartite state ρ_{ABE},

$$R_{\max} = H(Z|E)_{\rho_{ZBE}} - H(Z|B)_{\rho_{ZBE}}$$

(Devetak and Winter, 2005)

- Intuitively:

$$R = \text{Eve's ignorance} - \text{Bob's ignorance}$$

Devetak–Winter formula for the maximal secret key rate

- For a given tripartite state ρ_{ABE},

$$R_{\max} = H(Z|E)_{\rho_{ZBE}} - H(Z|B)_{\rho_{ZBE}}$$

(Devetak and Winter, 2005)

- Intuitively:

$$R = \text{Eve's ignorance} - \text{Bob's ignorance}$$

- The second term is easy: $H(Z|B) \leq h(Q_z)$ (Fano's inequality)

$$h(x) = -x \log_2 x - (1-x) \log_2 (1-x) \quad \text{(binary entropy)}$$

  - Q_z is the error probability of a Bob's prediction of the σ_z Alice's outcome
  - E.g., if $\mathcal{H}_B = \mathbb{C}^2$,

$$Q_z = \frac{1 - \mathrm{Tr}[(\sigma_z \otimes \sigma_z)\rho_{ZB}]}{2}$$

Entropic uncertainty relations

For any tripartite state ρ_{ABE},

$$H(Z|E)_{\rho_{ZBE}} + H(X|B)_{\rho_{XBE}} \geq 1$$

(Maassen and Uffink, 1988;
Berta, Christandl, Colbeck, Renes, and Renner, 2010;
Coles, Gheorghiu, and Griffiths, 2011)

Intuitively

There is no way to Eve to get knowledge on Z without introducing errors in Bob's knowledge of X. If Alice and Bob observe that Bob can predict the Alices's outcomes of the x observable, then the Eve's information on the z outcomes must be small.

Convex minimization problem

$$R_{\max} \geq H(Z|E)_{\rho_{ZBE}} - h(Q_z) \geq 1 - H(X|B)_{\rho_{XB}} - h(Q_z)$$

Convex minimization problem

$$R_{\max} \geq H(Z|E)_{\rho_{ZBE}} - h(Q_z) \geq 1 - H(X|B)_{\rho_{XB}} - h(Q_z)$$

- "Profit": we have get rid of the Eve's subsystem of an unknown dimensionality

Convex minimization problem

$$R_{\max} \geq H(Z|E)_{\rho_{ZBE}} - h(Q_z) \geq 1 - H(X|B)_{\rho_{XB}} - h(Q_z)$$

- "Profit": we have get rid of the Eve's subsystem of an unknown dimensionality
- But ρ_{AB} is still unknown. Hence, we should minimize over it:

$$R_{\max} \geq R = \min_{\rho_{AB} \in \mathbf{S}} [1 - H(X|B)_{\rho_{XB}}] - h(Q_z)$$

$$\mathbf{S} = \{\rho_{AB} \in \mathfrak{T}(\mathcal{H}_A \otimes \mathcal{H}_B) \| \, \rho_{AB} \geq 0, \ \mathrm{Tr}(\Gamma_i \rho_{AB}) = \gamma_i, i = 1, \ldots, m\},$$

Γ_i are observables.

Minimization of a convex function subject to linear constraints

Solution

$$R_{\max} \geq R = \min_{\rho_{AB} \in \mathbf{S}} [1 - H(X|B)_{\rho_{XB}}] - h(Q_z) \geq 1 - h(Q_x) - h(Q_z)$$

- Constraints:
  - $\Gamma_1 = I_{AB}$, $\gamma_1 = 1$ (trace equal to one)
  - $\Gamma_2 = \sigma_x \otimes \sigma_x$, $Q_x = (1 + \gamma_2)/2$ (error rate in the eigenbasis of σ_x).

Solution

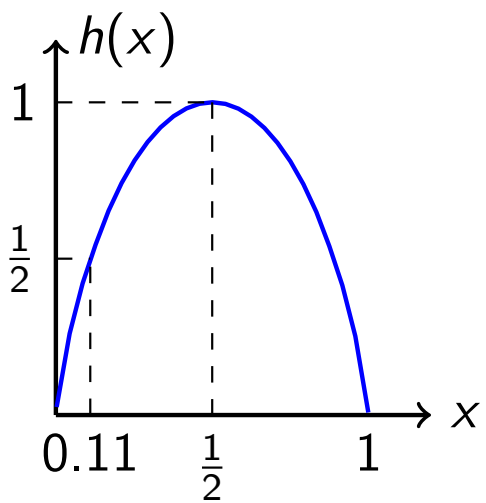
$$R_{\max} \geq R = \min_{\rho_{AB} \in \mathbf{S}} [1 - H(X|B)_{\rho_{XB}}] - h(Q_z) \geq 1 - h(Q_x) - h(Q_z)$$

- Constraints:
  - $\Gamma_1 = I_{AB}$, $\gamma_1 = 1$ (trace equal to one)
  - $\Gamma_2 = \sigma_x \otimes \sigma_x$, $Q_x = (1 + \gamma_2)/2$ (error rate in the eigenbasis of σ_x).
- One can prove that the bound is tight: $R_{\max} = 1 - h(Q_x) - h(Q_z)$,

Solution

$$R_{\max} \geq R = \min_{\rho_{AB} \in \mathbf{S}} [1 - H(X|B)_{\rho_{XB}}] - h(Q_z) \geq 1 - h(Q_x) - h(Q_z)$$

- Constraints:
  - $\Gamma_1 = I_{AB}$, $\gamma_1 = 1$ (trace equal to one)
  - $\Gamma_2 = \sigma_x \otimes \sigma_x$, $Q_x = (1 + \gamma_2)/2$ (error rate in the eigenbasis of σ_x).
- One can prove that the bound is tight: $R_{\max} = 1 - h(Q_x) - h(Q_z)$,



- If $Q_x = Q_z = Q$, then $R_{\max} = 1 - 2h(Q)$
- $R_{\max} > 0$ whenever $Q < Q_{\text{crit}} \approx 0.11$

(Mayers, 1996; Shor and Preskill, 2000)

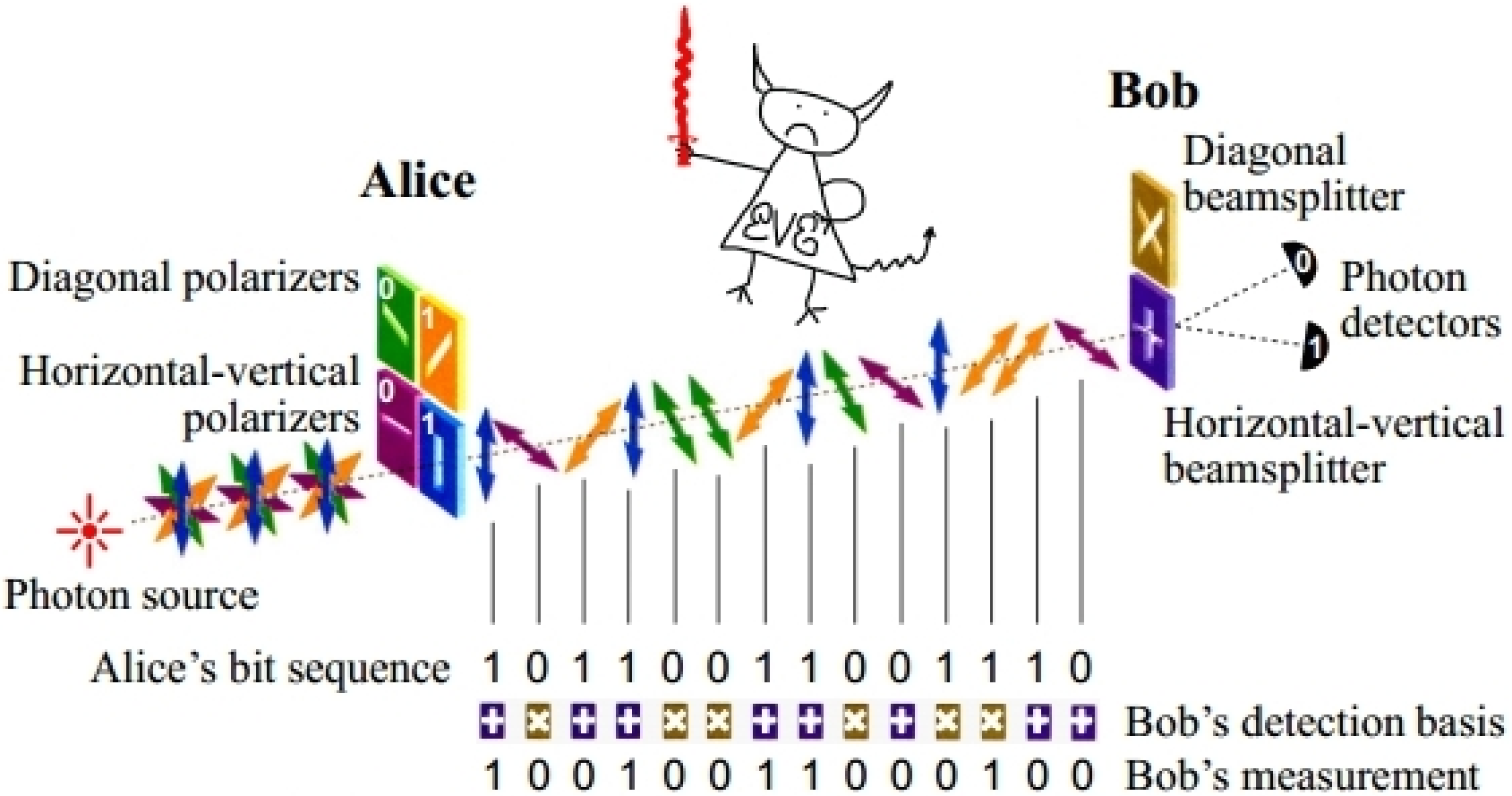
Outline

1. Key distribution problem
2. Axioms of quantum information
3. A quantum key distribution protocol
4. Security proof for the ideal case
5. **Security proof for the case of detection-efficiency mismatch**

Ideal vs real devices

- We assumed that the devices (source and the measurement devices) are ideal and perform exactly according to the protocol:
  - Source emits true single photons
  - Source does not have side channels
  - Detectors are perfect
- Current research: security proofs for realistic (imperfect) devices
- Here: detection-efficiency mismatch

BB84 protocol: Quantum channel



C. H. Bennett, G. Brassard, Quantum cryptography: Public key distribution and Coin tossing, 1984

Detection-efficiency mismatch

- Two single-photon detectors are required for measurements (one for each outcome)
- Quantum efficiency of detectors η_0 and η_1: probabilities of the registration of a photon.
- If $\eta_0 \neq \eta_1$, then the previous analysis cannot be applied

Extreme case

If $\eta_0 > 0$, $\eta_1 = 0$, then only zeros are registrated.
The key is just $00\ldots0$.

Detection-efficiency mismatch

- Two single-photon detectors are required for measurements (one for each outcome)
- Quantum efficiency of detectors η_0 and η_1: probabilities of the registration of a photon.
- If $\eta_0 \neq \eta_1$, then the previous analysis cannot be applied

Extreme case

If $\eta_0 > 0$, $\eta_1 = 0$, then only zeros are registrated.
The key is just $00\ldots0$.

- We assume that η_0 and η_1 are constant (mismatch is caused by manufacturing and setup) and known to all parties
- Without loss of generality, $\eta_0 = 1$, $\eta_1 = \eta \in (0, 1]$.

Bosonic Fock space

- Actually, the Bob's input is not a single photon ($\mathbb{C}^2$), but an arbitrary number of photons: the bosonic Fock space $\mathcal{F}(\mathbb{C}^2) = \bigoplus_{n=0}^{\infty} (\mathbb{C}^2)^{\otimes_s n}$
- If $\eta_0 = \eta_1$, then it can be reduced to the single-photon input (squashing model) (Gittsovich, Beaudry, Narasimhachar, Romero Alvarez, Moroder, and Lütkenhaus, 2014)
- If $\eta_0 \neq \eta_1$, then this reduction is no longer valid and we must analyse the infinite-dimensional case

Bosonic Fock space (2)

$$\mathcal{F}(\mathbb{C}^2) = \bigoplus_{n=0}^{\infty} (\mathbb{C}^2)^{\otimes_s n} = \mathbb{C} \oplus \mathbb{C}^2 \oplus (\mathbb{C}_2)^{\otimes_s 2} \oplus (\mathbb{C}_2)^{\otimes_s 3} \oplus \dots$$

- $e_{00} \in \mathbb{C}$ — the vacuum vector,
- Single-photon subspace $\mathbb{C}^2$: e_0, e_1, e_+, e_-
- The z orthonormal basis: $e^z_{n_0 n_1} \in (\mathbb{C}^2)^{\otimes_s (n_0+n_1)}$, $n_0, n_1 = 0, 1, 2, \dots$
  (n_0 photons in the state e_0 and n_1 photons in the state e_1,
  $e_0 = e^z_{1,0}, e_1 = e^z_{0,1}$)
- Analogously, the x orthonormal basis: $e^x_{n_0 n_1}$,
  $e_+ = e^x_{1,0}, e_- = e^x_{0,1}$

Imperfect Bob's detection in the basis $b \in \{x, z\}$: Events

$$\Pi_{\varnothing}^{(b)} = \sum_{n_1=0}^{\infty} (1-\eta)^{n_1} P_{e^b_{0,n_1}} \quad \text{(no click)},$$

$$\Pi_{0}^{(b)} = \sum_{n_0=1}^{\infty} \sum_{n_1=0}^{\infty} (1-\eta)^{n_1} P_{e^b_{n_0 n_1}} \quad \text{(only detector 0 clicks)},$$

$$\Pi_{1}^{(b)} = \sum_{n_1=1}^{\infty} [1-(1-\eta)^{n_1}] P_{e^b_{0,n_1}} \quad \text{(only detector 1 clicks)},$$

$$\Pi_{01}^{(b)} = \sum_{n_0,n_1=1}^{\infty} [1-(1-\eta)^{n_1}] P_{e^b_{n_0 n_1}} \quad \text{(double click)}.$$

Losses due to detector imperfections are now basis-dependent!

- Attenuation in the z basis (used for key generation):

$$\rho'_{ABE} = \mathcal{G}(\rho_{ABE}) \equiv G \rho_{ABE} G,$$
$$G = \sqrt{I_B - \Pi_{\varnothing}^{(z)}}$$

$$p_{\mathrm{det}} = \mathrm{Tr}\, \rho'_{ABE} \leq 1 \quad \text{(probability of detection)}$$
$$\tilde{\rho}'_{ABE} = p_{\mathrm{det}}^{-1} \rho'_{ABE} \quad \text{(trace equal to unity again)}$$

Losses due to detector imperfections are now basis-dependent!

- Attenuation in the z basis (used for key generation):

$$\rho'_{ABE} = \mathcal{G}(\rho_{ABE}) \equiv G\rho_{ABE}G,$$
$$G = \sqrt{I_B - \Pi_{\varnothing}^{(z)}}$$

$$p_{\mathrm{det}} = \mathrm{Tr}\,\rho'_{ABE} \leq 1 \quad \text{(probability of detection)}$$
$$\tilde{\rho}'_{ABE} = p_{\mathrm{det}}^{-1}\rho'_{ABE} \quad \text{(trace equal to unity again)}$$

- Devetak–Winter formula:

$$R_{\max} \geq H(Z|E)_{\mathcal{Z}(\tilde{\rho}'_{ABE})} - h(Q_z) \geq 1 - H(X|B)_{\mathcal{X}(\tilde{\rho}'_{ABE})} - h(Q_z)$$

Losses due to detector imperfections are now basis-dependent!

- Attenuation in the z basis (used for key generation):

$$\rho'_{ABE} = \mathcal{G}(\rho_{ABE}) \equiv G\rho_{ABE}G,$$
$$G = \sqrt{I_B - \Pi_{\varnothing}^{(z)}}$$

$$p_{\mathrm{det}} = \mathrm{Tr}\,\rho'_{ABE} \leq 1 \quad \text{(probability of detection)}$$
$$\tilde{\rho}'_{ABE} = p_{\mathrm{det}}^{-1}\rho'_{ABE} \quad \text{(trace equal to unity again)}$$

- Devetak–Winter formula:

$$R_{\max} \geq H(Z|E)_{\mathcal{Z}(\tilde{\rho}'_{ABE})} - h(Q_z) \geq 1 - H(X|B)_{\mathcal{X}(\tilde{\rho}'_{ABE})} - h(Q_z)$$

- $H(X|B)_{\mathcal{X}(\tilde{\rho}'_{ABE})}$ is a "hybrid" quantity: entropy of the x observable calculated for the state attenuated according to the measurement in the z basis!
- By this reason $H(X|B)_{\mathcal{X}(\tilde{\rho}'_{ABE})}$ cannot be estimated by a direct measurement of the x observable.

Linear constraints

$$R = \min_{\rho_{AB} \in \mathbf{S}} [1 - H(X|B)_{\mathcal{X}(\tilde{\rho}'_{ABE})}] - h(Q_z)$$

1. Probability of detection (for the z basis)

$$\Gamma_1 = I_A \otimes (I_B - P_{\varnothing}^{(z)}), \quad \operatorname{Tr} \Gamma_1 \rho_{AB} = p_{\mathrm{det}}.$$

2. Weighted mean erroneous detection rate in the x basis

$$\Gamma_2 = \eta^{-1} P_{e_+} \otimes \left(P_1^{(x)} + \frac{1}{2} P_{01}^{(x)} \right) + P_{e_-} \otimes \left(P_0^{(x)} + \frac{1}{2} P_{01}^{(x)} \right), \quad \operatorname{Tr} \Gamma_2 \rho_{AB} = q$$

3. Probability of a single click of detector 1 for the measurement in the z basis

$$\Gamma_3 = I_A \otimes P_1^{(z)}, \quad \operatorname{Tr} \Gamma_3 \rho_{AB} = p_1.$$

4. Mean probability of a double click

$$\Gamma_4 = I_A \otimes \frac{1}{2} (P_{01}^{(z)} + P_{01}^{(x)}), \quad \operatorname{Tr} \Gamma_3 \rho_{AB} = p_{01}.$$

Numerical and analytic solutions

- Reduction to such problem of convex optimization and numerical solutions of it: Coles, Metodiev, and Lütkenhaus, 2016; Winick, Lütkenhaus, and Coles, 2018
- Numerical solution of the problem for detection-efficiency mismatch, but using the numerical conjecture: Zhang, Coles, Winick, Lin, and Lütkenhaus, arXiv:2004.04383
- Analytic solutions for the case of the single-photon Bob's input ($\mathbb{C}^2$): Fung, Tamaki, Qi, Lo, and X. Ma, 2009; J. Ma, Zhou, Yuan, and X. Ma, 2019; Bochkov and A.T., 2019
- Analytic solution for the multiphoton input (bosonic Fock space): A.T., arXiv: 2004.07809

Main theorem

Theorem

The maximal secret key rate is lower bounded by

$$R_{\max} \geq \min_{p_{\mathrm{det}}^{(2)}} \frac{p_{\mathrm{det}}^{(1),\mathrm{L}}}{p_{\mathrm{det}}} \left[1 - h\left(\frac{1-\delta_x^{\mathrm{L}}}{2}\right)\right] - h(Q_z), \tag{1}$$

where

$$\delta_x^{\mathrm{L}} = \frac{\sqrt{\eta}(t_1^{\mathrm{L}} - 2q_1^{\mathrm{U}})}{p_{\mathrm{det}}^{(1),\mathrm{L}}}.$$

The minimization is performed over the segment $p_{\mathrm{det}}^{(2)} \in \left[0, p_{\mathrm{det}}^{(2),\mathrm{U}}\right]$. *The expression under minimization in Ineq. (??) is a convex function of* $p_{\mathrm{det}}^{(2)}$.

Here $p_{\mathrm{det}}^{(1),\mathrm{L}}$, $p_{\mathrm{det}}^{(2),\mathrm{U}}$, t_1^{L}, q_1^{U} are estimations obtained from the linear restrictions.

An infinite-dimensional optimization is reduced to one-dimensional

Method of proof: Two cornerstones

$$\mathcal{F}(\mathbb{C}^2) = \bigoplus_{n=0}^{\infty} (\mathbb{C}^2)^{\otimes_s n} = \mathbb{C} \oplus \mathbb{C}^2 \oplus \underbrace{(\mathbb{C}_2)^{\otimes_s 2} \oplus (\mathbb{C}_2)^{\otimes_s 3} \oplus \dots}_{\text{Multiphoton subspace}}$$

- Analytic bound for the case of the single-photon Bob's subspace based on symmetry properties and monotonicity of quantum relative entropy
- Estimation of the norm of the multiphoton part of the density operator based on the entropic uncertainty relations

Reduction of the search space due to symmetries

Proposition

Let Φ be a positive trace-preserving linear map acting on $\mathfrak{T}(\mathcal{H}_A \otimes \mathcal{H}_B)$ which commutes with $\mathcal{X}$ and $\mathcal{G}$ and such that $\Phi^*(\Gamma_i) = \Gamma_i$ for all i. We assume that p_{det} is included in the set of constraints. Then

$$\max_{\rho_{AB} \in \mathbf{S}} H(X|B)_{\mathcal{X}(\tilde{\rho}'_{ABE})} = \max_{\rho_{AB} \in \mathbf{S}'} H(X|B)_{\mathcal{X}(\tilde{\rho}'_{ABE})},$$

where $\mathbf{S}' = \mathbf{S} \cap \{\rho_{AB} \,\|\, \Phi(\rho_{AB}) = \rho_{AB}\}$.

Dual map:

$$\mathrm{Tr}[\Phi^*(X)\rho_{AB}] = \mathrm{Tr}[X\Phi(\rho_{AB})]$$

for any $X \in \mathfrak{B}(\mathcal{H}_A \otimes \mathcal{H}_B)$.

Reduction of the search space due to symmetries

$$\max_{\rho_{AB}\in\mathbf{S}} H(X|B)_{\mathcal{X}(\tilde{\rho}'_{ABE})} = \max_{\rho_{AB}\in\mathbf{S}'} H(X|B)_{\mathcal{X}(\tilde{\rho}'_{ABE})},$$

where $\mathbf{S}' = \mathbf{S} \cap \{\rho_{AB} \,\|\, \Phi(\rho_{AB}) = \rho_{AB}\}$.

Informally

If a problem obeys certain symmetry property $\Phi^*(\Gamma_i) = \Gamma_i$, then the optimal solution can be found among the states with such symmetry

Idea

A consequence of monotonicity of the quantum relative entropy

Particular application

Exact solution for the optimization problem with an additional linear constraint: $\mathrm{Tr}[(I_A \otimes P_1)\rho_{AB}] = 1$, where P_1 is a projection onto the single-photon subspace on the Bob's side

From infinite-dimensional to finite-dimensional

$$\mathcal{F}(\mathbb{C}^2) = \bigoplus_{n=0}^{\infty} (\mathbb{C}^2)^{\otimes_s n} = \mathbb{C} \oplus \mathbb{C}^2 \oplus \underbrace{(\mathbb{C}_2)^{\otimes_s 2} \oplus (\mathbb{C}_2)^{\otimes_s 3} \oplus \dots}_{\text{Multiphoton subspace}}$$

We need to estimate $\mathrm{Tr}[(I_A \otimes P_{\geq 2})\rho_{AB}]$ from above,
where $P_{\geq 2}$ is a projection onto the multiphoton subspace.

From infinite-dimensional to finite-dimensional

$$\mathcal{F}(\mathbb{C}^2) = \bigoplus_{n=0}^{\infty} (\mathbb{C}^2)^{\otimes_s n} = \mathbb{C} \oplus \mathbb{C}^2 \oplus \underbrace{(\mathbb{C}_2)^{\otimes_s 2} \oplus (\mathbb{C}_2)^{\otimes_s 3} \oplus \dots}_{\text{Multiphoton subspace}}$$

We need to estimate $\mathrm{Tr}[(I_A \otimes P_{\geq 2})\rho_{AB}]$ from above,
where $P_{\geq 2}$ is a projection onto the multiphoton subspace.

Idea

Multiphoton (more precisely, three- or more photon) states have positive double click probability in at least one of two bases (numerical conjecture in Zhang et al., arXiv: 2004.04383).

From infinite-dimensional to finite-dimensional

$$\mathcal{F}(\mathbb{C}^2) = \bigoplus_{n=0}^{\infty} (\mathbb{C}^2)^{\otimes_s n} = \mathbb{C} \oplus \mathbb{C}^2 \oplus \underbrace{(\mathbb{C}_2)^{\otimes_s 2} \oplus (\mathbb{C}_2)^{\otimes_s 3} \oplus \dots}_{\text{Multiphoton subspace}}$$

We need to estimate $\mathrm{Tr}[(I_A \otimes P_{\geq 2})\rho_{AB}]$ from above,
where $P_{\geq 2}$ is a projection onto the multiphoton subspace.

Idea

Multiphoton (more precisely, three- or more photon) states have positive double click probability in at least one of two bases (numerical conjecture in Zhang et al., arXiv: 2004.04383).

But how to prove it rigorously?

From infinite-dimensional to finite-dimensional

$$\mathcal{F}(\mathbb{C}^2) = \bigoplus_{n=0}^{\infty} (\mathbb{C}^2)^{\otimes_s n} = \mathbb{C} \oplus \mathbb{C}^2 \oplus \underbrace{(\mathbb{C}_2)^{\otimes_s 2} \oplus (\mathbb{C}_2)^{\otimes_s 3} \oplus \dots}_{\text{Multiphoton subspace}}$$

We need to estimate $\mathrm{Tr}[(I_A \otimes P_{\geq 2})\rho_{AB}]$ from above,
where $P_{\geq 2}$ is a projection onto the multiphoton subspace.

Idea

Multiphoton (more precisely, three- or more photon) states have positive double click probability in at least one of two bases (numerical conjecture in Zhang et al., arXiv: 2004.04383).

But how to prove it rigorously?

Use the entropic uncertainty relations!

Estimation of the number of multiphoton detection events

- $H(Z^{\otimes n})$ and $H(Z^{\otimes n})$ are the entropies of the results of the measurements of the n-qubit observables $Z^{\otimes n}$ and $X^{\otimes n}$, respectively.

Estimation of the number of multiphoton detection events

- $H(Z^{\otimes n})$ and $H(Z^{\otimes n})$ are the entropies of the results of the measurements of the n-qubit observables $Z^{\otimes n}$ and $X^{\otimes n}$, respectively.
- $H(Z^{\otimes n}) + H(X^{\otimes n}) \geq n$ (entropic uncertainty relations)

Estimation of the number of multiphoton detection events

- $H(Z^{\otimes n})$ and $H(Z^{\otimes n})$ are the entropies of the results of the measurements of the n-qubit observables $Z^{\otimes n}$ and $X^{\otimes n}$, respectively.
- $H(Z^{\otimes n}) + H(X^{\otimes n}) \geq n$ (entropic uncertainty relations)
- If the detectors are perfect and if the double click probability in the z (x) basis is zero, then $H(Z^{\otimes n})$ $[H(X^{\otimes n})]$ is at most one, since only two outcomes correspond to a single click (all zeros or all ones)

Estimation of the number of multiphoton detection events

- $H(Z^{\otimes n})$ and $H(Z^{\otimes n})$ are the entropies of the results of the measurements of the n-qubit observables $Z^{\otimes n}$ and $X^{\otimes n}$, respectively.
- $H(Z^{\otimes n}) + H(X^{\otimes n}) \geq n$ (entropic uncertainty relations)
- If the detectors are perfect and if the double click probability in the z (x) basis is zero, then $H(Z^{\otimes n})$ $[H(X^{\otimes n})]$ is at most one, since only two outcomes correspond to a single click (all zeros or all ones)
- Since $H(Z^{\otimes n})$ and $H(Z^{\otimes n})$ cannot be small simultaneously, double click rates in two bases also cannot be small simultaneously if $n \geq 3$

$$p_{01} \geq \eta \tilde{p}_{01}, \quad \text{where} \quad 2\tilde{p}_{01} \log(2^{n-1} - 1) + 2h(\tilde{p}_{01}) \geq n - 2$$

Two-photon subspace

- We have estimated $\mathrm{Tr}[(I_A \otimes P_{\geq 3})\rho_{AB}]$ instead of $\mathrm{Tr}[(I_A \otimes P_{\geq 2})\rho_{AB}]$

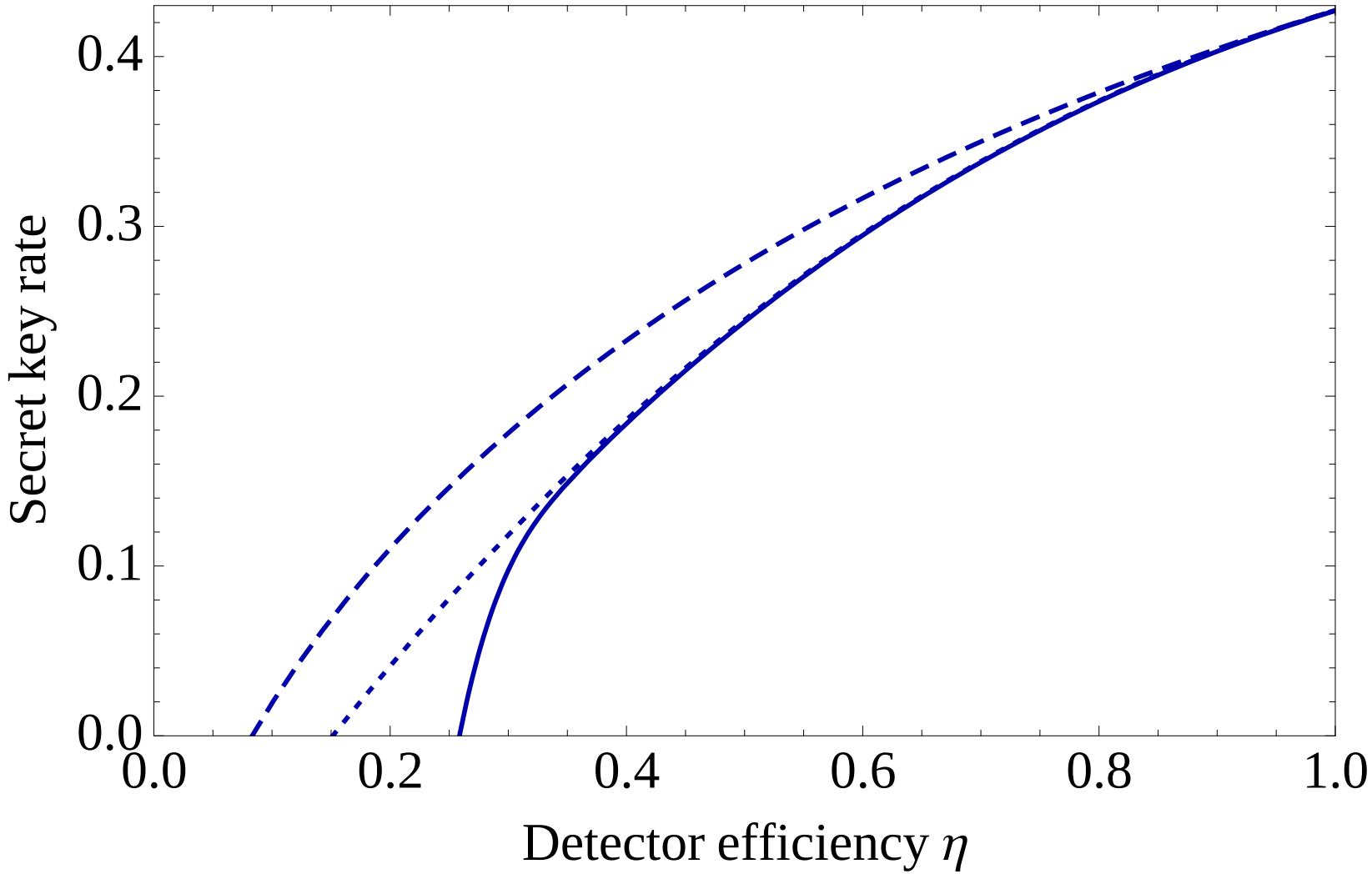
Two-photon subspace

- We have estimated $\mathrm{Tr}[(I_A \otimes P_{\geq 3})\rho_{AB}]$ instead of $\mathrm{Tr}[(I_A \otimes P_{\geq 2})\rho_{AB}]$
- For two-photon subspace, the Bell state

$$\Phi^{(B)}_{\mathrm{Bell}} = \frac{1}{\sqrt{2}}(e^z_{2,0} + e^z_{0,2}) = \frac{1}{\sqrt{2}}(e^x_{2,0} + e^x_{0,2})$$

  produces no double clicks in both bases.
- However, if two Bob's photons are in a pure state, they are uncorrelated with the Alice's photon, hence, produce high error rate.

Simulation



Error rate $Q = 0.05$ (for both bases)

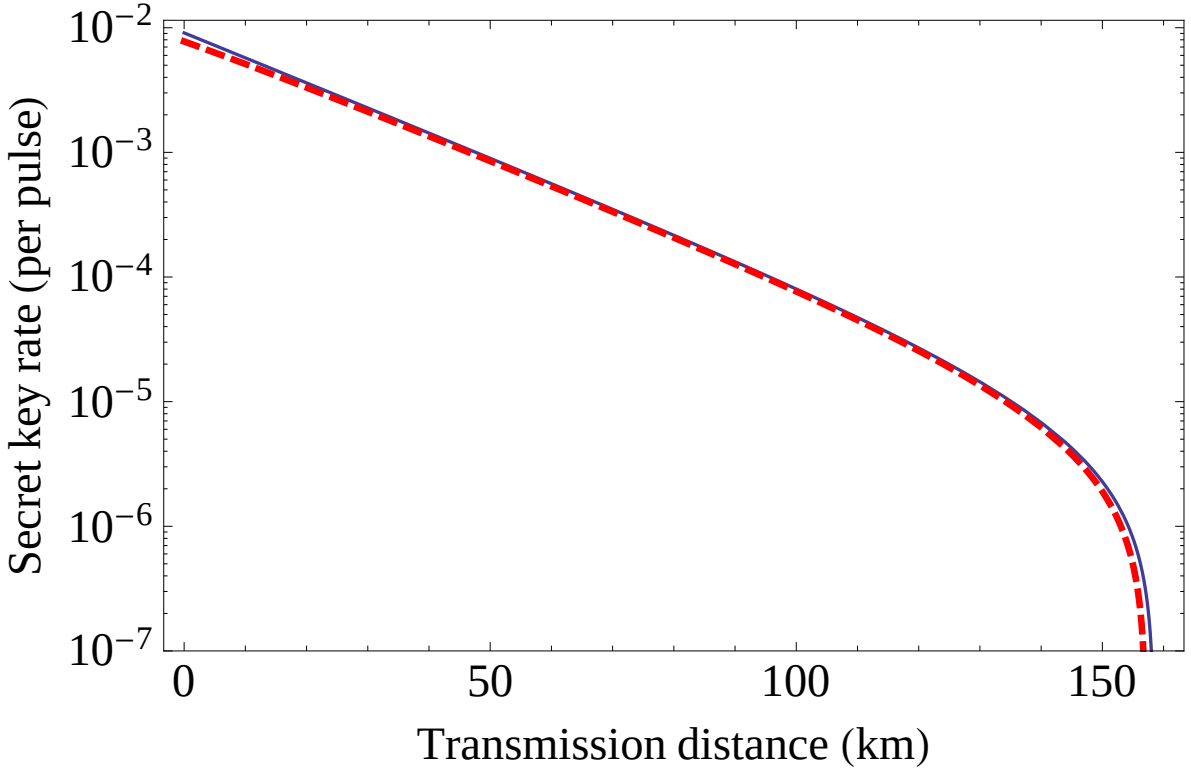
Solid line: calculated lower bound for the secret key rate ($p_{\mathrm{det}} R$)

Dashed line: tight bound for the single-photon subspace (upper bound)

Decoy states for the case of detection-efficiency mismatch

- The laser emits not true single photons, but weak coherent pulses (Poisson distribution of the number of photons)
- Decoy state method is used to address this problem: The use of pulses with different intensities (parameters of the Poisson distributions)
- Decoy state method was adopted to the case of detection-efficiency mismatch

Perfomance of the decoy state protocol with practical parameters



Secret key rate of the decoy state BB84 protocol with detection-efficiency mismatch. Intensities (parameters of the Poisson distributions for the signal and two decoy types of pulses): $\mu = 0.5, \nu_1 = 0.1, \nu_2 = 0$
Detector efficiencies: $\eta_0 = 0.1$ and $\eta_1 = 0.09$ (i.e., $\eta = \eta_1/\eta_0 = 0.9$).
Red dashed line: the case of detection-efficiency mismatch.
Blue line: the case of no efficiency mismatch but the same average detection

Further work (in progress)

- Detection-efficiency mismatch induced by Eve (not constant)
- Dark count rate mismatch

Proposed analysis for BB84 vs MDI QKD

- Measurement-device-independent (MDI) QKD: protocols of another type, where we completely do not care about the imperfections of detectors. The detectors are assumed to be under the Eve's control
- What is better: BB84 with the detector imperfections taken into account or MDI QKD where we do not care about them at all?
- I don't know: Now various concepts of QKD coexist
- The developed new analytic tools (e.g., reduction of the dimensionality using symmetries) are general

Mathematical apparatus not mentioned in this talk

Finite-key analysis (finite number of sendings N):

- Quantum Renyi entropies, smooth min- and max-entropies (Kraus, Gisin, Renner, 2005; Renner, 2005; Tomamichel, 2013; Tomamichel&Leverrier, 2017, etc.)
- Entropic uncertainty relations for min- and max-entropies,
- Leftover hashing lemma: estimation of the trace distance ε after applying the hash-function for a given smooth min-entropy
- Entropy accumulation theorem: estimation of min-entropy by von Neumann entropies (Dupuis, Fawzi, Renner, 2016)

Continuous-variable QKD (based on coherent quantum states)

Main results

- We prove the security of the BB84 protocol with detection-efficiency mismatch for the case when both Alice's output and Bob's input are multiphoton.

New analytic techniques of security proofs of the QKD protocols:

- Analytic proof of bounds for multiphoton detection events.
- Use the symmetries to reduce the search space in the optimization problem and, possibly, solve this problem analytically.

Main results

- We prove the security of the BB84 protocol with detection-efficiency mismatch for the case when both Alice's output and Bob's input are multiphoton.

New analytic techniques of security proofs of the QKD protocols:

- Analytic proof of bounds for multiphoton detection events.
- Use the symmetries to reduce the search space in the optimization problem and, possibly, solve this problem analytically.

Thank you for attention!

Main results

- We prove the security of the BB84 protocol with detection-efficiency mismatch for the case when both Alice's output and Bob's input are multiphoton.

New analytic techniques of security proofs of the QKD protocols:

- Analytic proof of bounds for multiphoton detection events.
- Use the symmetries to reduce the search space in the optimization problem and, possibly, solve this problem analytically.

Thank you for attention!

Further reading:

- M. K. Bochkov, A. T., "Security of quantum key distribution with detection-efficiency mismatch in the single-photon case: Tight bounds", Phys. Rev. A, 99:3 (2019), 32308, 15 pp.
- A. T., "Security of quantum key distribution with detection-efficiency mismatch in the multiphoton case", arXiv: 2004.07809, 18 pp.

trushechkin@mi-ras.ru