Device-independent quantum key distribution based on Hardy's paradox

Ramij Rahaman

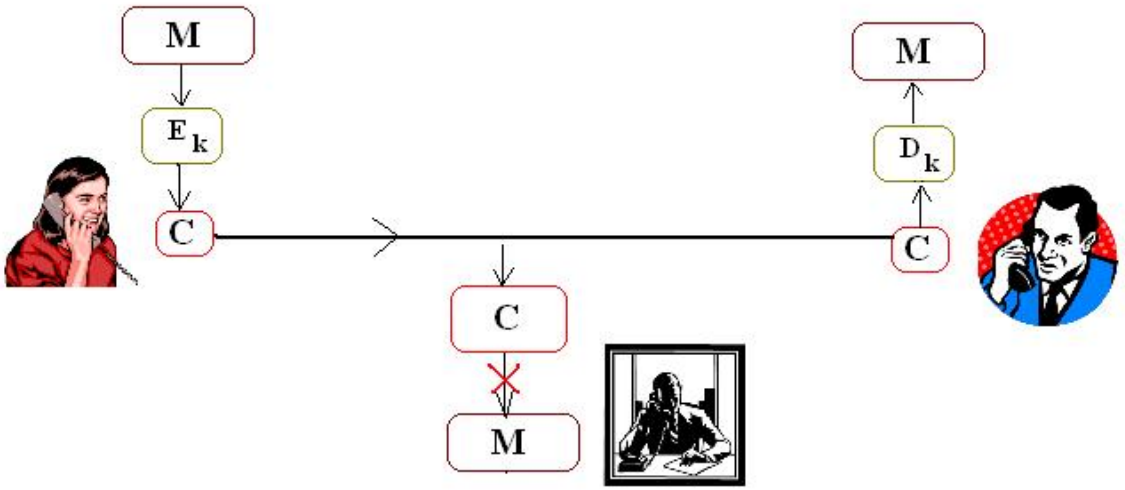
Joint work with

Matthew G. Parker, Marcin Pawłowski, Piotr Mironowicz

Department of Mathematics
University of Allahabad
Allahabad 211002, Uttar Pradesh
India

Table of contents

Art of Cryptography



In a cryptosystem, if Alice wishes to send messages to Bob then:

- Alice must have an encoding key, which allows her to encrypt her message.
- Bob also must have the matching decoding key, which allows Bob to decrypt the encrypted message.

Private key cryptography

A simple, yet highly effective private key cryptosystem is the Vernam cipher, sometimes called a one time pad cryptosystem.

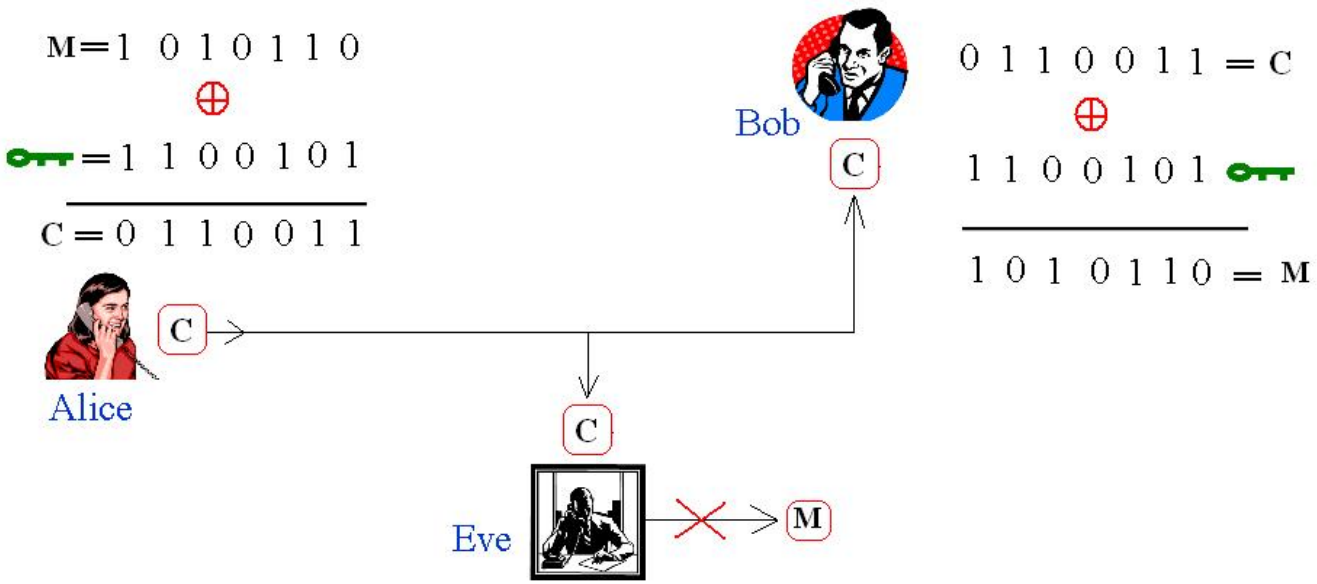


Figure: One time pad cryptosystem.

Difficulties in Private Key

- The key bits cannot be reused for any future protocol.
- key bits must be delivered in advance, guarded assiduously until used.

Possible Solutions

- Public key cryptosystems
  - Security based on computational complexity
  - Can be broken by quantum computers!
- Quantum cryptography
  1. Security based on Laws of Physics

Difficulties in Private Key

- The key bits cannot be reused for any future protocol.
- key bits must be delivered in advance, guarded assiduously until used.

Possible Solutions

- Public key cryptosystems
  - Security based on computational complexity
  - Can be broken by quantum computers!
- Quantum cryptography
  1. Security based on Laws of Physics

Quantum key distribution Protocols (QKD)

- **BB84 protocol** [C. H. Bennett, G. Brassard, 1984].
  $\{|0_z\rangle, |1_z\rangle, |0_x\rangle, |1_x\rangle\}$.

- **Ekert's QKD protocol** [A. K. Ekert, PRL 91].

$$|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}[|0_z\rangle_A|0_z\rangle_B + |1_z\rangle_A|1_z\rangle_B]$$
$$= \frac{1}{\sqrt{2}}[|0_x\rangle_A|0_x\rangle_B + |1_x\rangle_A|1_x\rangle_B].$$

Key: $\{|0_z\rangle, |0_x\rangle\} \mapsto 0$ and $\{|1_z\rangle, |1_x\rangle\} \mapsto 1$.

Quantum key distribution Protocols (QKD)

- **BB84 protocol** [C. H. Bennett, G. Brassard, 1984].
  $\{|0_z\rangle, |1_z\rangle, |0_x\rangle, |1_x\rangle\}$.

- **Ekert's QKD protocol** [A. K. Ekert, PRL 91].

$$
\begin{aligned}
|\Phi^+\rangle_{AB} &= \frac{1}{\sqrt{2}}\left[|0_z\rangle_A|0_z\rangle_B + |1_z\rangle_A|1_z\rangle_B\right] \\
&= \frac{1}{\sqrt{2}}\left[|0_x\rangle_A|0_x\rangle_B + |1_x\rangle_A|1_x\rangle_B\right].
\end{aligned}
$$

Key: $\{|0_z\rangle, |0_x\rangle\} \mapsto 0$ and $\{|1_z\rangle, |1_x\rangle\} \mapsto 1$.

Is QKD unconditional secure?

Quantum key distribution Protocols (QKD)

- **BB84 protocol** [C. H. Bennett, G. Brassard, 1984].
  $\{|0_z\rangle, |1_z\rangle, |0_x\rangle, |1_x\rangle\}$.

- **Ekert's QKD protocol** [A. K. Ekert, PRL 91].

$$
\begin{aligned}
|\Phi^+\rangle_{AB} &= \frac{1}{\sqrt{2}}\left[|0_z\rangle_A|0_z\rangle_B + |1_z\rangle_A|1_z\rangle_B\right] \\
&= \frac{1}{\sqrt{2}}\left[|0_x\rangle_A|0_x\rangle_B + |1_x\rangle_A|1_x\rangle_B\right].
\end{aligned}
$$

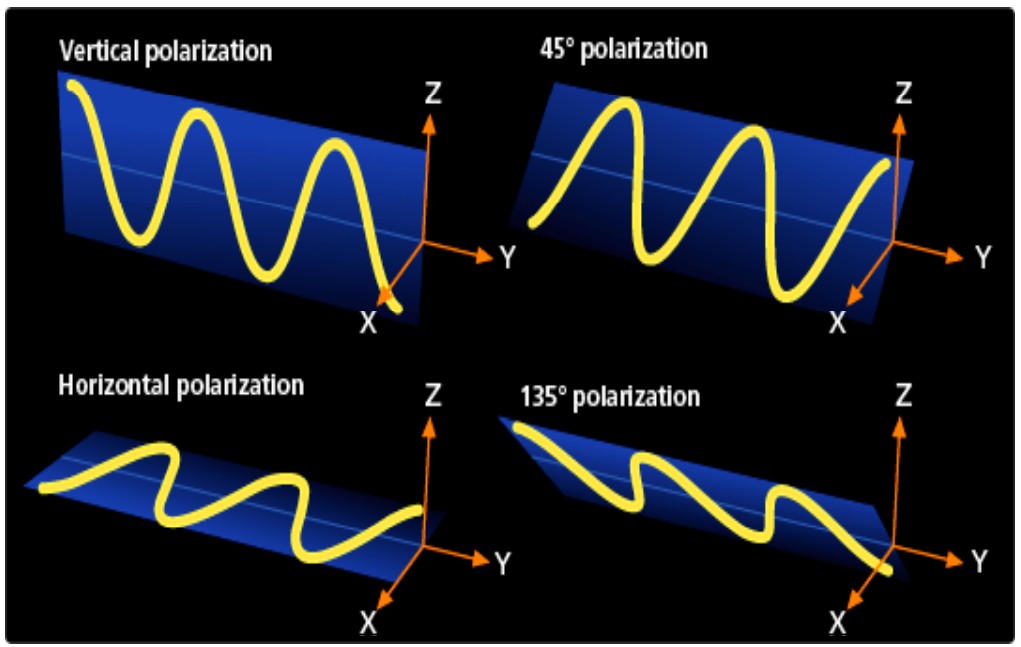
Key: $\{|0_z\rangle, |0_x\rangle\} \mapsto 0$ and $\{|1_z\rangle, |1_x\rangle\} \mapsto 1$.

Is QKD unconditional secure?

Possible attacks on BB84-QKD protocols

An adversary could easily manipulate the apparatus such that the QKD scheme becomes completely insecure.

For example, instead of encoding and measuring in two different bases, Alice always use the same basis.

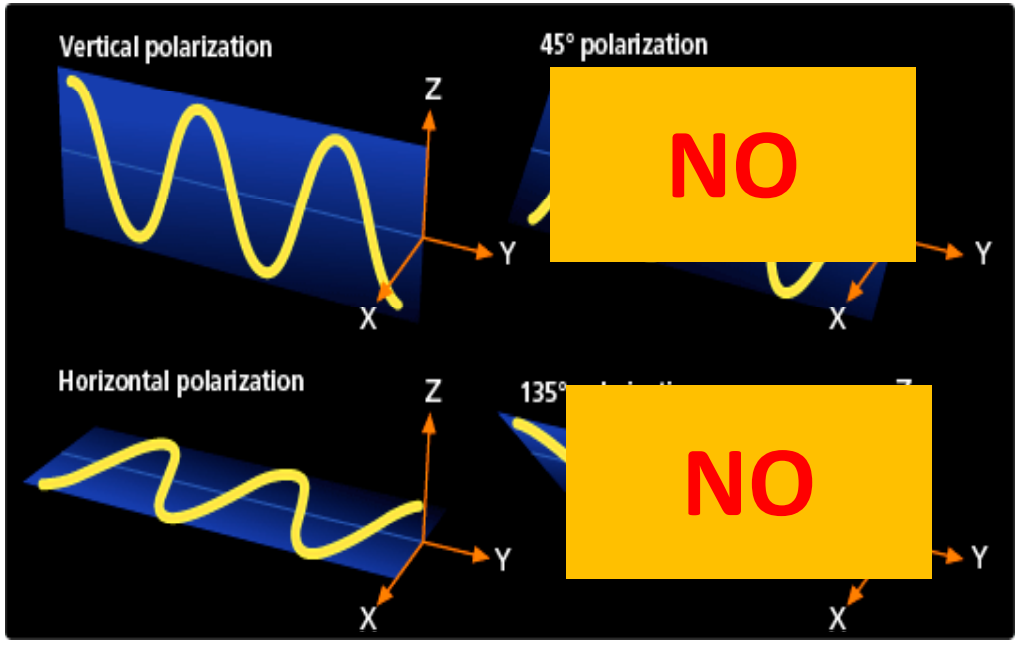


The eavesdropper can measure the photon in this basis without disturbing it.

Possible attacks on BB84-QKD protocols

An adversary could easily manipulate the apparatus such that the QKD scheme becomes completely insecure.

For example, instead of encoding and measuring in two different bases, Alice always use the same basis.



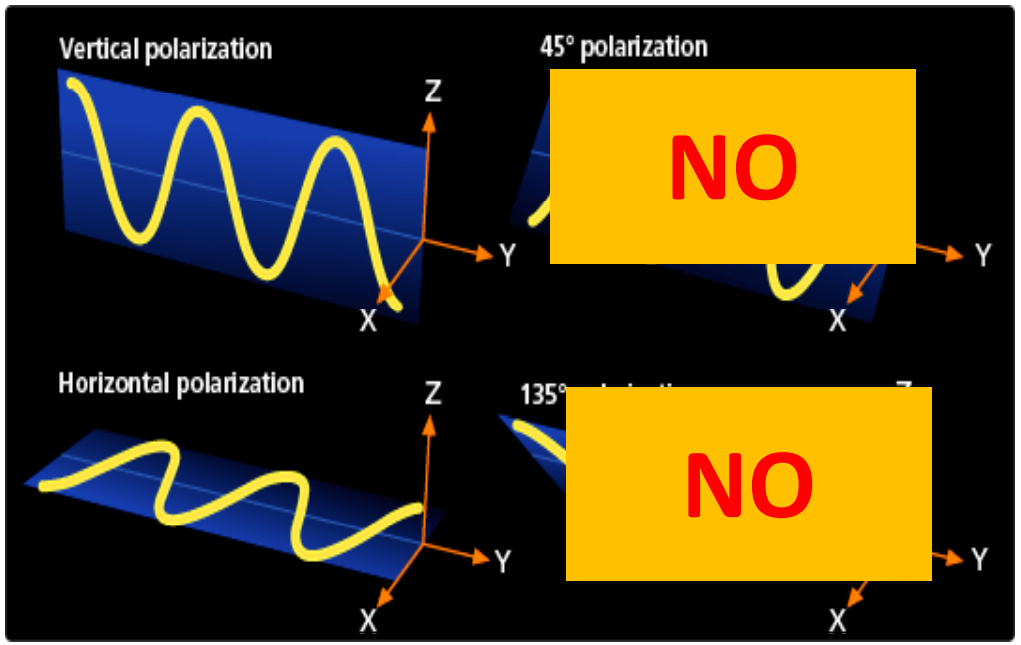
The eavesdropper can measure the photon in this basis without disturbing it.

∴ She can learn the bit perfectly.

Possible attacks on BB84-QKD protocols

An adversary could easily manipulate the apparatus such that the QKD scheme becomes completely insecure.

For example, instead of encoding and measuring in two different bases, Alice always use the same basis.



The eavesdropper can measure the photon in this basis without disturbing it.

$\therefore$ She can learn the bit perfectly.

Possible attacks on Ekert's protocols

Here, Alice and Bob assumed that $|\Phi^+\rangle_{AB} \in \mathcal{C}^2 \otimes \mathcal{C}^2$ is a two qubit state and producing the following correlations:

$$P(ab|\sigma_x\sigma_x) = P(ab|\sigma_z\sigma_z) = \frac{1}{2} \text{ if } a = b$$

$$P(ab|\sigma_x\sigma_z) = P(ab|\sigma_z\sigma_x) = \frac{1}{4} \text{ for all, } a, b$$

A separable (hence insecure) state $\rho_{AB} \in \mathcal{C}^4 \otimes \mathcal{C}^4$ also gives the same correlations.

$$\rho_{AB} = \frac{1}{4} \sum_{u,v=0}^{1} |u_z^0 v_z^1\rangle_A\langle u_z^0 v_z^1| \otimes |u_z^0 v_z^1\rangle_B\langle u_z^0 v_z^1|$$

where the measurements are $\sigma_z \otimes I$ for the setting '0' and $I \otimes \sigma_z$ for the setting '1'.

Possible attacks on Ekert's protocols

Here, Alice and Bob assumed that $|\Phi^+\rangle_{AB} \in \mathcal{C}^2 \otimes \mathcal{C}^2$ is a two qubit state and producing the following correlations:

$$P(ab|\sigma_x\sigma_x) = P(ab|\sigma_z\sigma_z) = \frac{1}{2} \text{ if } a = b$$

$$P(ab|\sigma_x\sigma_z) = P(ab|\sigma_z\sigma_x) = \frac{1}{4} \text{ for all, } a, b$$

A separable (hence insecure) state $\rho_{AB} \in \mathcal{C}^4 \otimes \mathcal{C}^4$ also gives the same correlations.

$$\rho_{AB} = \frac{1}{4} \sum_{u,v=0}^{1} |u_z^0 v_z^1\rangle_A \langle u_z^0 v_z^1| \otimes |u_z^0 v_z^1\rangle_B \langle u_z^0 v_z^1|$$

where the measurements are $\sigma_z \otimes I$ for the setting '0' and $I \otimes \sigma_z$ for the setting '1'.

Possible attacks on Ekert's protocols

Eve can now have a perfect copy of the local states of Alice and Bob, for instance if they share the tripartite state

$$\rho_{ABE} = \sum_{u,v=0}^{1} |u_z^0 v_z^1\rangle_A\langle u_z^0 v_z^1| \otimes |u_z^0 v_z^1\rangle_B\langle u_z^0 v_z^1| \otimes |u_z^0 v_z^1\rangle_E\langle u_z^0 v_z^1|$$

Thus, the security proofs only hold when the dimension of the system is known, which cannot be assumed if the adversary supplies the devices.

Possible attacks on Ekert's protocols

Eve can now have a perfect copy of the local states of Alice and Bob, for instance if they share the tripartite state

$$\rho_{ABE} = \sum_{u,v=0}^{1} |u_z^0 v_z^1\rangle_A\langle u_z^0 v_z^1| \otimes |u_z^0 v_z^1\rangle_B\langle u_z^0 v_z^1| \otimes |u_z^0 v_z^1\rangle_E\langle u_z^0 v_z^1|$$

Thus, the security proofs only hold when the dimension of the system is known, which cannot be assumed if the adversary supplies the devices.

For the security proof of quantum key distribution, it is, therefore, assumed that the devices are trustworthy and work exactly as specified.

Possible attacks on Ekert's protocols

Eve can now have a perfect copy of the local states of Alice and Bob, for instance if they share the tripartite state

$$\rho_{ABE} = \sum_{u,v=0}^{1} |u_z^0 v_z^1\rangle_A\langle u_z^0 v_z^1| \otimes |u_z^0 v_z^1\rangle_B\langle u_z^0 v_z^1| \otimes |u_z^0 v_z^1\rangle_E\langle u_z^0 v_z^1|$$

Thus, the security proofs only hold when the dimension of the system is known, which cannot be assumed if the adversary supplies the devices.

For the security proof of quantum key distribution, it is, therefore, assumed that the devices are trustworthy and work exactly as specified.

Assumptions (Hidden) for secure QKD

QKD is often claimed to be unconditionally secure but, it actually does make certain assumptions.

- The assumption always present in any key agreement is that Alice and Bob have secure laboratories. This assumption is crucial and cannot be removed.

- A further assumption is that Alice and Bob have complete control over their physical devices (i.e., only the quantum channel is corrupted) and know their exact and complete specification.

Assumptions (Hidden) for secure QKD

QKD is often claimed to be unconditionally secure but, it actually does make certain assumptions.

- The assumption always present in any key agreement is that Alice and Bob have secure laboratories. This assumption is crucial and cannot be removed.

- A further assumption is that Alice and Bob have complete control over their physical devices (i.e., only the quantum channel is corrupted) and know their exact and complete specification.

Minimum assumptions

Goal: To reduce the above assumptions to a minimum, in particular, to remove all assumptions about the exact working of the physical devices.

- Therefore, the devices could be manufactured by the adversary.
- The security should only rely on testable features of the devices, for example, the statistics of their behaviour.
- The honest parties would then only need to trust their ability to do classical calculations (to compute the statistics) and the shielding of their laboratories.

Minimum assumptions

Goal: To reduce the above assumptions to a minimum, in particular, to remove all assumptions about the exact working of the physical devices.

- Therefore, the devices could be manufactured by the adversary.
- The security should only rely on testable features of the devices, for example, the statistics of their behaviour.
- The honest parties would then only need to trust their ability to do classical calculations (to compute the statistics) and the shielding of their laboratories.

Device-independent QKD

In a device-independent QKD analysis, Alice and Bob would not only distrust the source of particles, but they would also distrust their measuring apparatuses.

- They assume that the measurement directions may for instance drift with time due to imperfections in the apparatuses, or the entire apparatuses may be untrusted because they have been fabricated by a malicious party.

- Also they cannot even make assumptions about the dimension of the Hilbert space in which they are defined.

Device-independent QKD

In a device-independent QKD analysis, Alice and Bob would not only distrust the source of particles, but they would also distrust their measuring apparatuses.

- They assume that the measurement directions may for instance drift with time due to imperfections in the apparatuses, or the entire apparatuses may be untrusted because they have been fabricated by a malicious party.

- Also they cannot even make assumptions about the dimension of the Hilbert space in which they are defined.

Device-independent quantum key distribution

Figure: Alice and Bob see their quantum devices as black boxes producing classical outputs, a and b, as a function of classical inputs X and Y.

Goal of Alice & Bob: From the observed statistics, and without making any assumption on the internal working of the devices, they should be able to conclude whether they can establish a secret key secure against a quantum eavesdropper.

Previous works on Device-independent QKD

- In 2007, Acín *et al.*, introduced a device-independent QKD protocol based on Bell-CHSH inequality secure against collective attacks.
- In 2011, Masanes *et al.* provided a more general security scheme based on causally independent measurement processes.

But the security of all these protocols is undermined as the measurement at step k may depend on the classical or quantum memory of all previous inputs and outputs.

Recently secure protocols where device re-use is allowed were introduced.

Previous works on Device-independent QKD

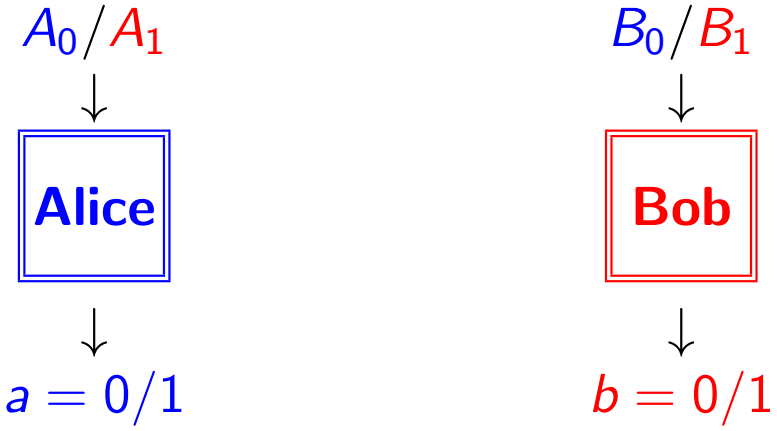
- In 2007, Acín *et al.*, introduced a device-independent QKD protocol based on Bell-CHSH inequality secure against collective attacks.
- In 2011, Masanes *et al.* provided a more general security scheme based on causally independent measurement processes.

But the security of all these protocols is undermined as the measurement at step k may depend on the classical or quantum memory of all previous inputs and outputs.

Recently secure protocols where device re-use is allowed were introduced.

Hardy's Paradox [*L. Hardy, PRL 1992*].

Consider a physical system consisting of two subsystems shared between Alice and Bob.



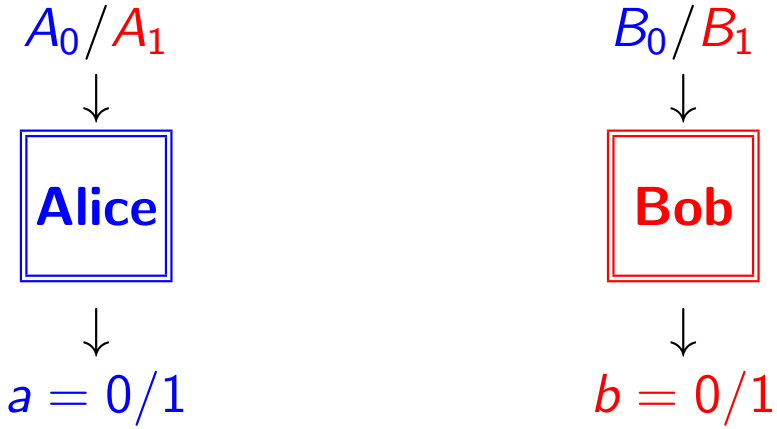
Hardy's conditions: (*L.Hardy, PRL, 92*)

$$P(A_0 = 0, B_0 = 0) = q > 0$$
$$P(A_1 = 0, B_0 = 0) = 0$$
$$P(A_0 = 0, B_1 = 0) = 0$$
$$P(A_1 = 1, B_1 = 1) = 0$$

This set of conditions cannot be satisfied by any LHVT.

Hardy's Paradox [*L. Hardy, PRL 1992*].

Consider a physical system consisting of two subsystems shared between Alice and Bob.

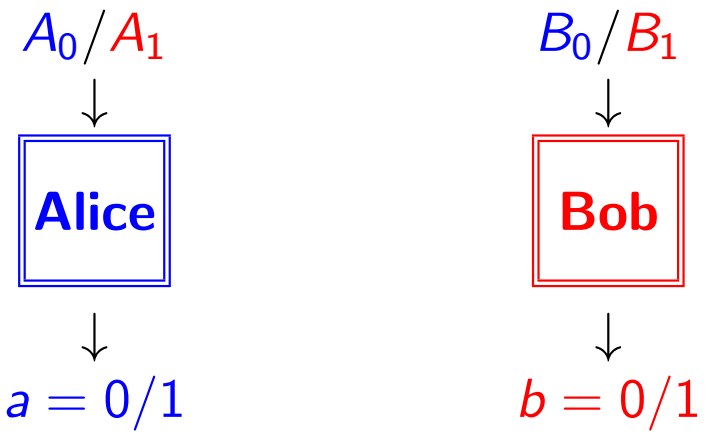


Hardy's conditions: (*L.Hardy*, *PRL*, 92)

$$
\begin{aligned}
P(A_0 = 0, B_0 = 0) &= q > 0 \\
P(A_1 = 0, B_0 = 0) &= 0 \\
P(A_0 = 0, B_1 = 0) &= 0 \\
P(A_1 = 1, B_1 = 1) &= 0
\end{aligned}
$$

This set of conditions cannot be satisfied by any LHVT.

Proof:

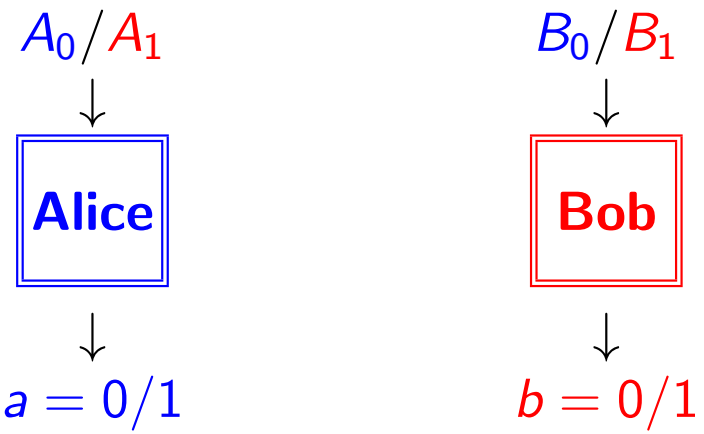


Hardy's Conditions

$$P(A_0 = 0, B_0 = 0) = q > 0$$
$$P(A_1 = 0, B_0 = 0) = 0$$
$$P(A_0 = 0, B_1 = 0) = 0$$
$$P(A_1 = 1, B_1 = 1) = 0$$

First	$P(A_0 = 0, B_0 = 0)$	$=$	$q > 0$		
Second	$P(A_1 = 0, B_0 = 0)$	$=$	0	$\Longrightarrow$	$A_1 = 1$
Third	$P(A_0 = 0, B_1 = 0)$	$=$	0	$\Longrightarrow$	$B_1 = 1$

Proof:



Hardy's Conditions

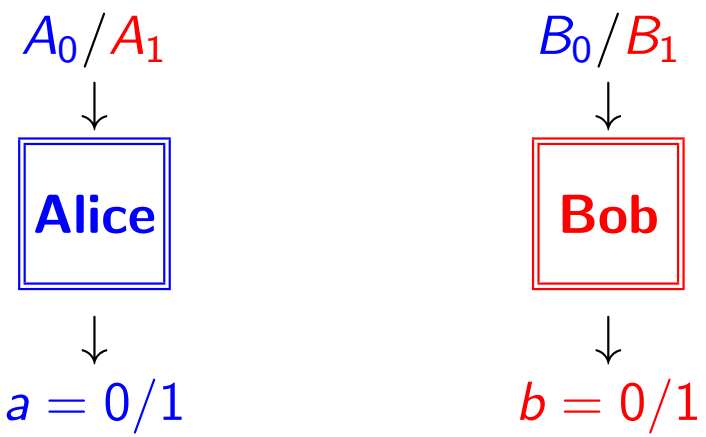
$P(A_0 = 0, B_0 = 0) = q > 0$
$P(A_1 = 0, B_0 = 0) = 0$
$P(A_0 = 0, B_1 = 0) = 0$
$P(A_1 = 1, B_1 = 1) = 0$

First $P(A_0 = 0, B_0 = 0) = q > 0 \implies A_1 = 1$

Third $P(A_0 = 0, B_1 = 0) = 0 \implies B_1 = 1$

Last $P(A_1 = 1, B_1 = 1) = 0$ contradiction...

Proof:



Hardy's Conditions

$$P(A_0 = 0, B_0 = 0) = q > 0$$
$$P(A_1 = 0, B_0 = 0) = 0$$
$$P(A_0 = 0, B_1 = 0) = 0$$
$$P(A_1 = 1, B_1 = 1) = 0$$

First	$P(A_0 = 0, B_0 = 0)$	$=$	$q > 0$	
Second	$P(A_1 = 0, B_0 = 0)$	$=$	$0 \implies$	$A_1 = 1$
			$0 \implies$	$B_1 = 1$
Last	$P(A_1 = 1, B_1 = 1)$	$=$	0	contradiction...

Hardy's argument and two qubit entangled state

The product states associated with all the conditions

$$
\begin{array}{lll}
|\phi_3\rangle = |A_0 = 0\rangle|B_0 = 0\rangle; & P(A_0 = 0, B_0 = 0) = q > 0 \\
|\phi_2\rangle = |A_1 = 0\rangle|B_0 = 0\rangle; & P(A_1 = 0, B_0 = 0) = 0 \\
|\phi_1\rangle = |A_0 = 0\rangle|B_1 = 0\rangle; & P(A_0 = 0, B_1 = 0) = 0 \\
|\phi_0\rangle = |A_1 = 1\rangle|B_1 = 1\rangle; & P(A_1 = 1, B_1 = 1) = 0,
\end{array}
$$

where $|X_i = j\rangle$ denotes the eigenstate of the observable X_i for the outcome j.
Let $|X_1 = 0\rangle = \alpha_X|X_0 = 0\rangle + \beta_X|X_0 = 1\rangle$ and
$|X_1 = 1\rangle = \beta_X^*|X_0 = 0\rangle - \alpha_X^*|X_0 = 1\rangle$, where $|\alpha_X|^2 + |\beta_X|^2 = 1$ and $0 < |\alpha_X| < 1$ for $X = A, B$.

Let $S = \{|\phi_0\rangle, |\phi_1\rangle, |\phi_2\rangle\}$, then **dim($S$)=3**.

If $|\psi\rangle$ satisfies the Hardy's conditions, then $|\psi\rangle \perp S$. i.e., $|\psi\rangle \in S^{\perp}$.

$\therefore |\psi\rangle$ is unique pure entangled state [*G. Kar, PLA 1997*].

Hardy's argument and two qubit entangled state

The product states associated with all the conditions

$$
\begin{array}{lll}
|\phi_3\rangle = |A_0 = 0\rangle|B_0 = 0\rangle; & P(A_0 = 0, B_0 = 0) & = \quad q > 0 \\
|\phi_2\rangle = |A_1 = 0\rangle|B_0 = 0\rangle; & P(A_1 = 0, B_0 = 0) & = \quad 0 \\
|\phi_1\rangle = |A_0 = 0\rangle|B_1 = 0\rangle; & P(A_0 = 0, B_1 = 0) & = \quad 0 \\
|\phi_0\rangle = |A_1 = 1\rangle|B_1 = 1\rangle; & P(A_1 = 1, B_1 = 1) & = \quad 0,
\end{array}
$$

where $|X_i = j\rangle$ denotes the eigenstate of the observable X_i for the outcome j.
Let $|X_1 = 0\rangle = \alpha_X|X_0 = 0\rangle + \beta_X|X_0 = 1\rangle$ and
$|X_1 = 1\rangle = \beta_X^*|X_0 = 0\rangle - \alpha_X^*|X_0 = 1\rangle$, where $|\alpha_X|^2 + |\beta_X|^2 = 1$ and $0 < |\alpha_X| < 1$ for $X = A, B$.

Let $S = \{|\phi_0\rangle, |\phi_1\rangle, |\phi_2\rangle\}$, then **dim($S$)=3**.

If $|\psi\rangle$ satisfies the Hardy's conditions, then $|\psi\rangle \perp S$. i.e., $|\psi\rangle \in S^{\perp}$.

$\therefore$ $|\psi\rangle$ is unique pure entangled state [*G. Kar, PLA 1997*].

Gram-Schmidt orthonormalization to find the Hardy-type state $|\psi\rangle$:

$$\begin{aligned} |\phi_0'\rangle &= |\phi_0\rangle \\ |\phi_i'\rangle &= \frac{|\phi_i\rangle - \sum_{j=0}^{i-1}\langle\phi_j'|\phi_i\rangle|\phi_j'\rangle}{\sqrt{1-\sum_{j=1}^{i-1}|\langle\phi_j'|\phi_i\rangle|^2}} \quad i = 1, 2. \end{aligned}$$

$$\begin{aligned} |\phi_0\rangle &= |A_1 = 1\rangle|B_1 = 1\rangle \\ |\phi_1\rangle &= |A_1 = 0\rangle|B_0 = 0\rangle \\ |\phi_2\rangle &= |A_0 = 0\rangle|B_1 = 0\rangle \\ |\phi_3\rangle &= |A_0 = 0\rangle|B_0 = 0\rangle \end{aligned}$$

$\therefore$ The Hardy state $|\psi\rangle$:

$$|\psi\rangle = \frac{|\phi_3\rangle - \sum_{i=0}^{2}\langle\phi_i'|\phi\rangle|\phi_i'\rangle}{\sqrt{1-\sum_{i=0}^{2}|\langle\phi_i'|\phi_3\rangle|^2}}.$$

The probability **q** for this state:

$$q = |\langle\psi|\phi_3\rangle|^2 = 1 - \sum_{i=1}^{7}|\langle\phi_i'|\phi_3\rangle|^2 = \frac{|\alpha_A\alpha_B|^2|\beta_A\beta_B|^2}{1-|\alpha_A\alpha_B|^2}.$$

The maximum value of **q** is $\frac{5\sqrt{5}-11}{2} = 0.0901699$ for $|\alpha_A| = |\beta_B| = \sqrt{\frac{\sqrt{5}-1}{2}}$ [*T. F. Jordan, PRA 1994*].

Gram-Schmidt orthonormalization to find the Hardy-type state $|\psi\rangle$:

$$\begin{aligned} |\phi_0'\rangle &= |\phi_0\rangle \\ |\phi_i'\rangle &= \frac{|\phi_i\rangle - \sum_{j=0}^{i-1}\langle\phi_j'|\phi_i\rangle|\phi_j'\rangle}{\sqrt{1-\sum_{j=1}^{i-1}|\langle\phi_j'|\phi_i\rangle|^2}} \quad i = 1, 2. \end{aligned}$$

$$\begin{aligned} |\phi_0\rangle &= |A_1 = 1\rangle|B_1 = 1\rangle \\ |\phi_1\rangle &= |A_1 = 0\rangle|B_0 = 0\rangle \\ |\phi_2\rangle &= |A_0 = 0\rangle|B_1 = 0\rangle \\ |\phi_3\rangle &= |A_0 = 0\rangle|B_0 = 0\rangle \end{aligned}$$

$\therefore$ The Hardy state $|\psi\rangle$:

$$|\psi\rangle = \frac{|\phi_3\rangle - \sum_{i=0}^{2}\langle\phi_i'|\phi\rangle|\phi_i'\rangle}{\sqrt{1-\sum_{i=0}^{2}|\langle\phi_i'|\phi_3\rangle|^2}}.$$

The probability **q** for this state:

$$q = |\langle\psi|\phi_3\rangle|^2 = 1 - \sum_{i=1}^{7}|\langle\phi_i'|\phi_3\rangle|^2 = \frac{|\alpha_A\alpha_B|^2|\beta_A\beta_B|^2}{1-|\alpha_A\alpha_B|^2}.$$

The maximum value of **q** is $\frac{5\sqrt{5}-11}{2} = 0.0901699$ for $|\alpha_A| = |\beta_B| = \sqrt{\frac{\sqrt{5}-1}{2}}$ [*T. F. Jordan, PRA 1994*].

Device-independence of Hardy-test [Rabelo *et.al.*, PRL 2012]

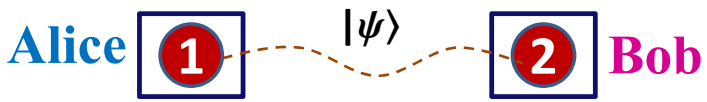
If the maximum success probability $q_{max} = \frac{5\sqrt{5}-11}{2}$ is observed in a Hardy test, the state of the system is equivalent to

$$|\psi^H\rangle_{12} \otimes |\eta\rangle_{1'2'},$$

where $|\psi^H\rangle_{12}$ is the unique two-qubit *Hardy state* for q_{max}.

Device-independent QKD based on Hardy's argument

S1. Alice and Bob share many copies of Hardy states $|\psi\rangle$

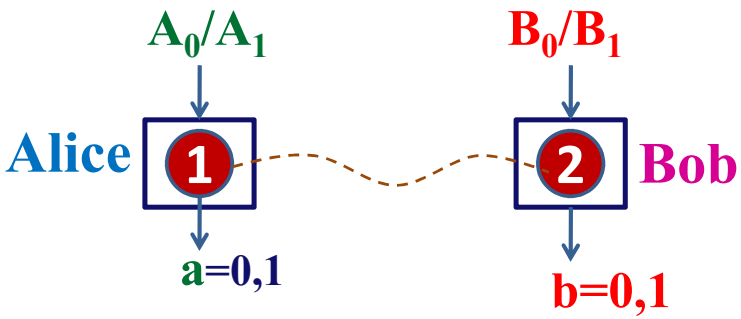


S2. For each $|\psi\rangle$, Alice randomly chooses whether to measure A_0, or A_1 on her qubit. Bob does the same, measures (B_0 or B_1) on his qubit.

S3. Both announce their results but not measurement settings for all runs.

Device-independent QKD based on Hardy's argument

S1. Alice and Bob share many copies of Hardy states $|\psi\rangle$



S2. For each $|\psi\rangle$, Alice randomly chooses whether to measure A_0, or A_1 on her qubit. Bob does the same, measures (B_0 or B_1) on his qubit.

S3. Both announce their results but not measurement settings for all runs.

Cont....Protocol

S4. *Check for eavesdropping*:

For some randomly selected runs, Alice and Bob both announce their measurement choices (A_i, B_j) and check the corresponding outcomes (a, b) are satisfied the Hardy's argument.

S5. From rest of the runs they generate the desire key:
For $|\psi\rangle$,

$P(A_1 = 0, B_1 = 0) > P(A_0 = 0, B_0 = 0) > 0$ and
$P(A_0 = 0, B_1 = 0) = P(A_1 = 0, B_0 = 0) = 0$.

Hence, they have correlated settings for $(0, 0)$ outcomes.

Table for generating key

Run	Alice		Bob		Useful for Key (Bit value)
	Measurement basis(A_s)	Outcome (a)	Measurement basis(B_t)	Outcome (b)	
⋮	⋮	⋮	⋮	⋮	
i_1	A_0	0	B_1	1	
i_2	A_0	0	B_0	0	✓(0)
i_3	A_1	1	B_1	0	
i_4	A_0	1	B_1	1	
i_5	A_1	0	B_1	0	✓(1)
i_6	A_0	0	B_0	0	✓(0)
i_7	A_0	1	B_0	1	
i_8	A_1	0	B_1	0	✓(1)
⋮	⋮	⋮	⋮	⋮	
i_k	A_1	1	B_0	1	
i_{k+1}	A_0	0	B_1	1	
i_{k+2}	A_1	0	B_1	0	✓(1)
i_{k+3}	A_1	1	B_0	1	
⋮	⋮	⋮	⋮	⋮	

Device-independent QKD

- **Alice** and **Bob** choose their settings and the Hardy state $|\psi\rangle$ corresponding to maximum probability of success $q_{\max} = 0.0901699$ i.e.,

$$|\alpha_A| = |\beta_B| = \sqrt{\frac{\sqrt{5}-1}{2}} \text{ and } |\psi\rangle = |\psi^H\rangle.$$

- For $|\psi^H\rangle$,
  $P(A_0 = 0, B_0 = 0) = 0.0901699 < P(A_1 = 0, B_1 = 0) = 0.236068$.
  So, Alice and Bob further drop some runs of settings 1 to make equal number of 0s and 1s in the key.
- Key rate: $\frac{2*0.0901699}{4} = 0.04509$.
- But for non-uniform settings *e.g.*,
  $(A_0/B_0 : A_1/B_1) = (0.618 : 0.382)$, the key rate is 0.06888.

Device-independent QKD

- **Alice** and **Bob** choose their settings and the Hardy state $|\psi\rangle$ corresponding to maximum probability of success $q_{\max} = 0.0901699$ i.e.,

$$|\alpha_A| = |\beta_B| = \sqrt{\frac{\sqrt{5}-1}{2}} \text{ and } |\psi\rangle = |\psi^H\rangle.$$

- For $|\psi^H\rangle$,
  $P(A_0 = 0, B_0 = 0) = 0.0901699 < P(A_1 = 0, B_1 = 0) = 0.236068$.
  So, Alice and Bob further drop some runs of settings 1 to make equal number of 0s and 1s in the key.
- Key rate: $\frac{2*0.0901699}{4} = 0.04509$.
- But for non-uniform settings *e.g.*,
  $(A_0/B_0 : A_1/B_1) = (0.618 : 0.382)$, the key rate is 0.06888.

Hardy paradox in Noise Case

$$\begin{aligned} P(A_0 = 0, B_0 = 0) &\geq q - \epsilon, \\ P(A_1 = 0, B_0 = 0) &\leq \epsilon, \\ P(A_0 = 0, B_1 = 0) &\leq \epsilon, \\ P(A_1 = 1, B_1 = 1) &\leq \epsilon. \end{aligned}$$

Goal: For $\epsilon > 0$ small enough the protocol remains secure against general attacks.

In other words,

$$P_{guess}(\mathcal{A}|a = b = 0) = \max_{A_s} P(A_s|a = b = 0) \leq G(\epsilon).$$

where G is a concave function.

Hardy paradox in Noise Case

$$\begin{aligned} P(A_0 = 0, B_0 = 0) &\geq q - \epsilon, \\ P(A_1 = 0, B_0 = 0) &\leq \epsilon, \\ P(A_0 = 0, B_1 = 0) &\leq \epsilon, \\ P(A_1 = 1, B_1 = 1) &\leq \epsilon. \end{aligned}$$

Goal: For $\epsilon > 0$ small enough the protocol remains secure against general attacks.

In other words,

$$P_{guess}(\mathcal{A}|a = b = 0) = \max_{A_s} P(A_s|a = b = 0) \leq G(\epsilon).$$

where G is a concave function.

How to calculate G?

To find G we first use Bayes rule to express the conditional probability $P(A_0|a=0,b=0)$ as

$$P(A_0|a=0,b=0) = \frac{x}{x+y}$$

where

$$\begin{aligned} x \equiv\ & P(a=0,b=0|A_0,B_0)P(A_0,B_0) + \\ & P(a=0,b=0|A_0,B_1)P(A_0,B_1) \\ y \equiv\ & P(a=0,b=0|A_1,B_0)P(A_1,B_0) + \\ & P(a=0,b=0|A_1,B_1)P(A_1,B_1) \end{aligned}$$

Similarly we have $P(A_1|a=0,b=0) = \frac{y}{x+y}$.

Guessing probability

Let $g_0 = P(A_0|a = 0, b = 0)$, $g_1 = P(A_1|a = 0, b = 0)$ and $G \geq \max\{g_0, g_1\}$.

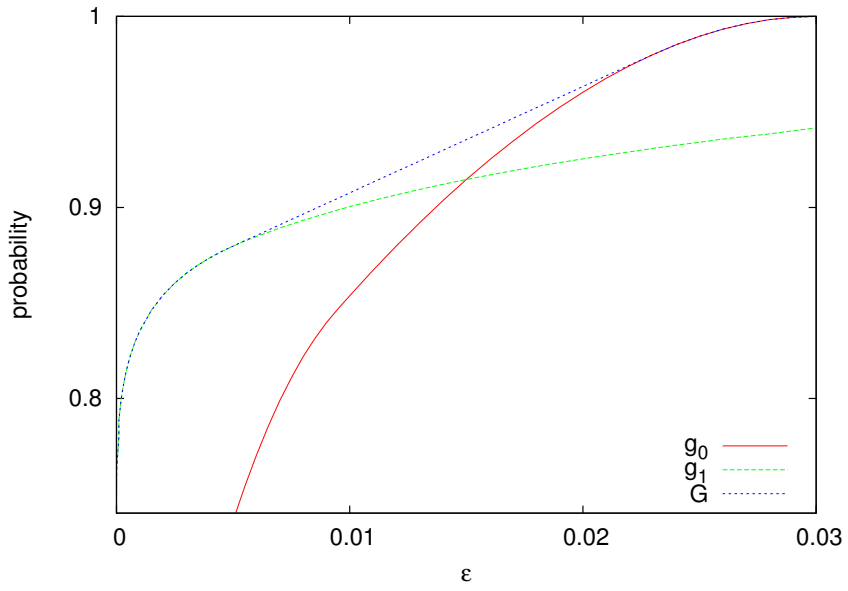


Figure: Guessing probability with uniform settings.

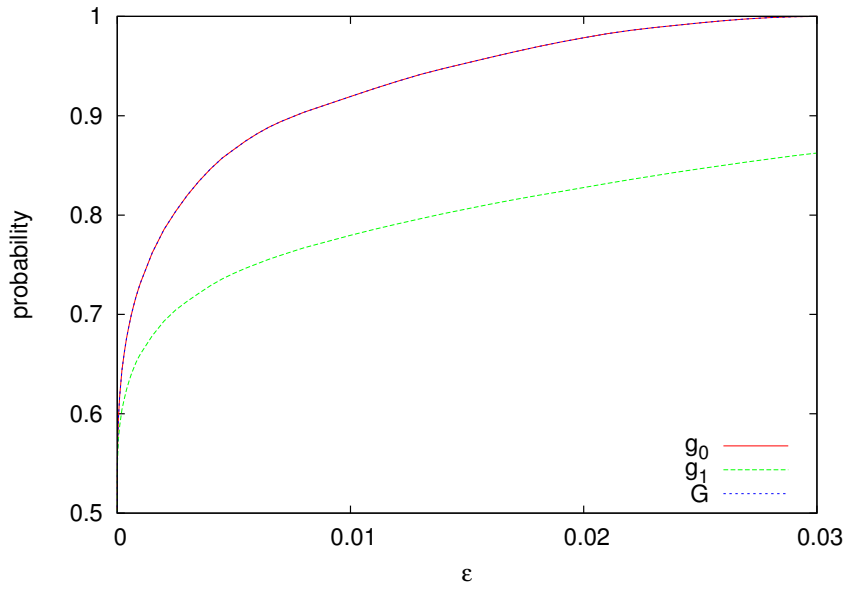
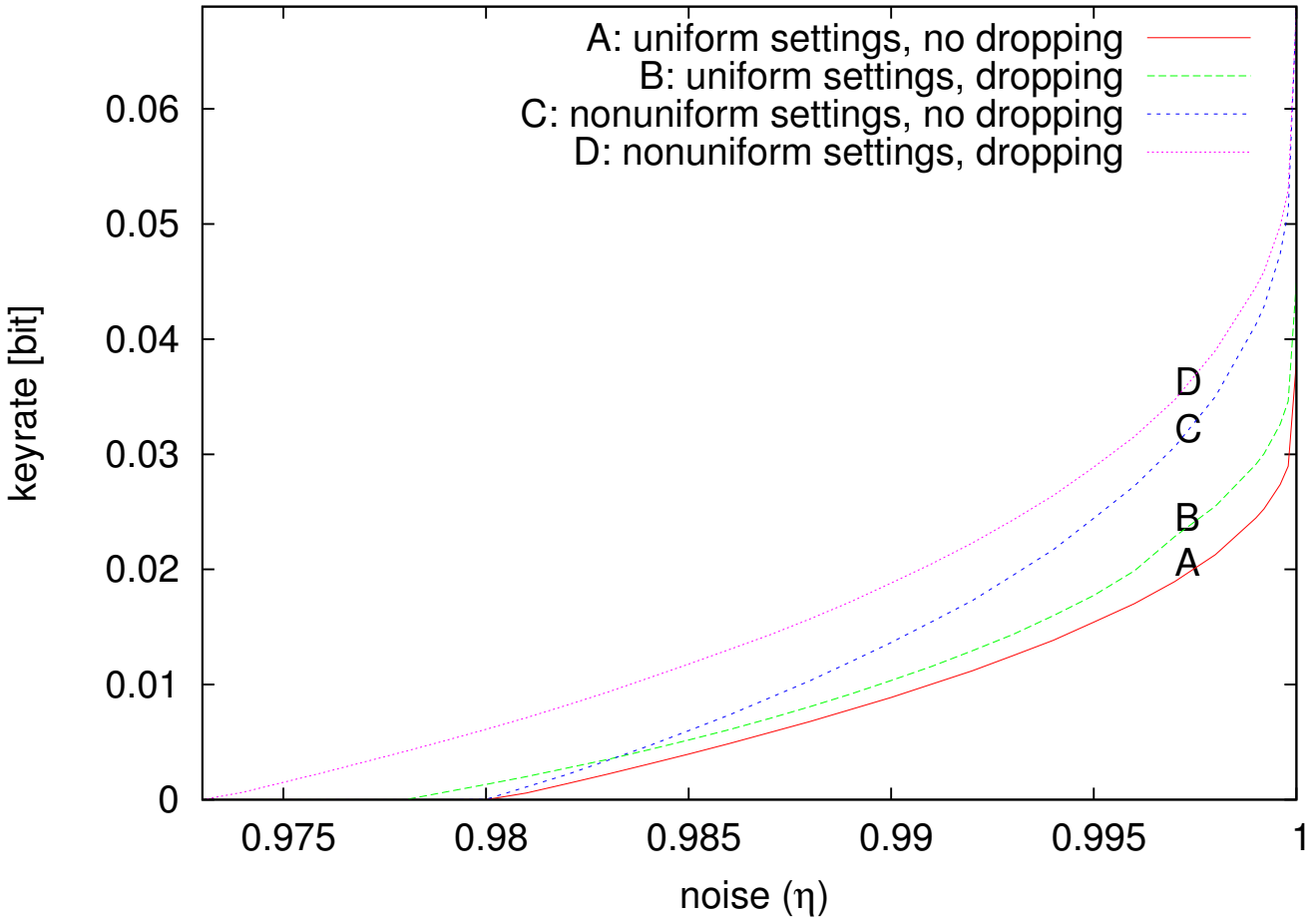


Figure: Non-uniform settings: 0 is chosen with the probability 0.61803405.

Key rate



$$\rho(\eta) = \frac{(1-\eta)}{2}\mathbb{I} + \eta|\,\psi^H\rangle\langle\psi^H\,|$$

Conclusion

- In our QKD protocol, the bits used for secret key do not come from the results of the measurements on an entangled state but from the choices of settings which are harder for an eavesdropper to influence.
- Instead of a single security parameter (a violation of some Bell inequality) a set of them is used to estimate the level of trust in the secrecy of the key.
- Ref.: arXiv:1308.6447.


THANK YOU