Quantum entanglement as a tool for securing communications in the post-quantum era

the E91 protocol

PhD Student
Marco Mattiazzi

Università di Siena

December 19, 2022

Low-energy seminar

Outline

I. Essentials of cryptography: the Key Distribution Problem

II. Theory & results behind entanglement-based QKD protocols

III. E91 protocol

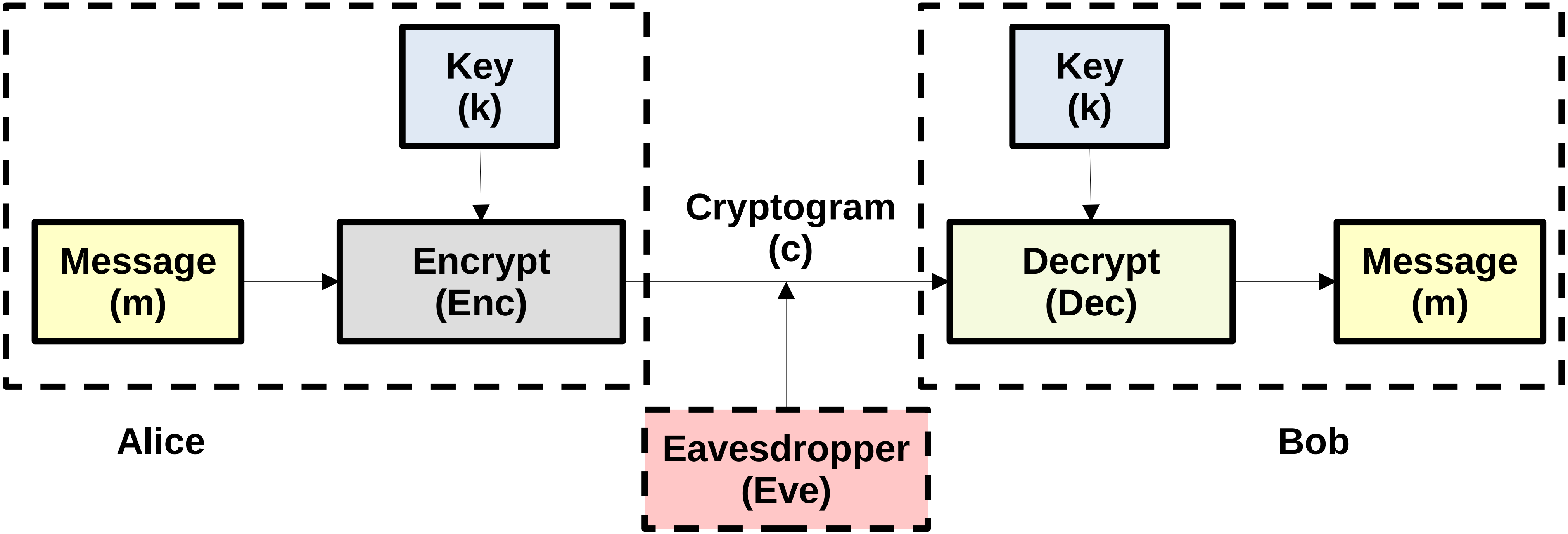
IV. Experimental realizations of entanglement-based QKD protocols

Part 1:
Basic notions of cryptography

Key Distribution Problem

What is a secure communication?

Symmetric Key Cryptography



Key (k)

Message (m)

Encrypt (Enc)

Cryptogram (c)

Key (k)

Decrypt (Dec)

Message (m)

Alice

Eavesdropper (Eve)

Bob

Encryption-Decryption Scheme

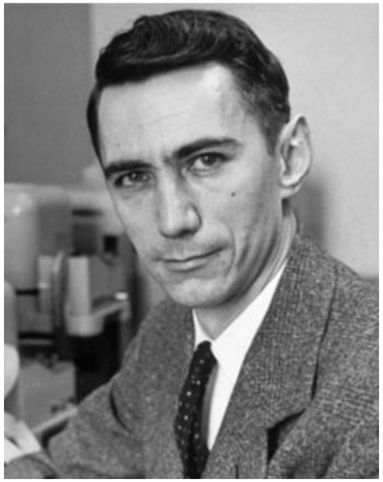
- Encryption function

$$\mathrm{Enc} : [\mathbf{k}, \mathbf{m}] \longmapsto \mathbf{c}$$

- Decryption function

$$\mathrm{Dec} : [\mathbf{k}, \mathbf{c}] \longmapsto \mathbf{m}$$

Secure communication
when **Eve**
obtains **no information** on **m**
even if she has gained
access on **c**



Shannon's lemma

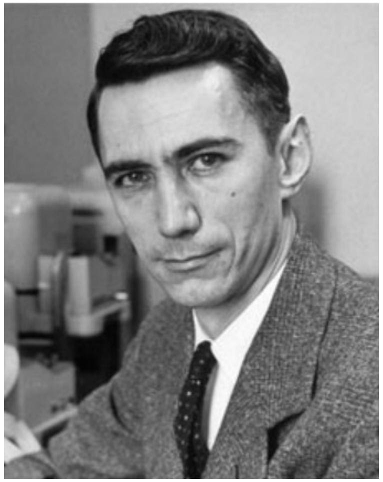
An encryption scheme (Enc,Dec) can only be secure and correct if the number of keys K is at least as large as the number of possible messages M

$$K \geq M$$

Communication theory of secrecy systems

Claude E. Shannon

01 Oct 1949 - Bell System Technical Journal (Alcatel-Lucent) - Vol. 28, Iss: 4, pp 656-715

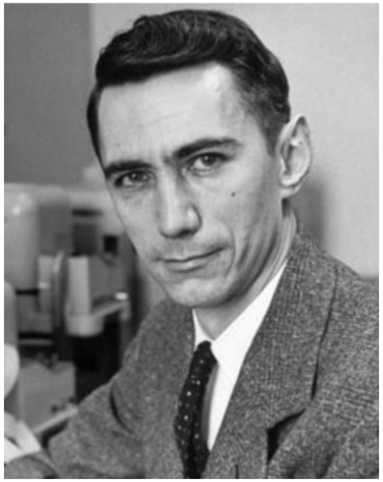


Shannon's lemma

An encryption scheme (Enc,Dec) can only be secure and correct if the number of keys K is at least as large as the number of possible messages M

$$K \geq M$$

Q: do we know a secure and correct encryption scheme?



Shannon's lemma

An encryption scheme (Enc,Dec) can only be secure and correct if the number of keys K is at least as large as the number of possible messages M

$$K \geq M$$

Q: do we know a secure and correct encryption scheme?

A: Yes, see next slide

One-Time Pad

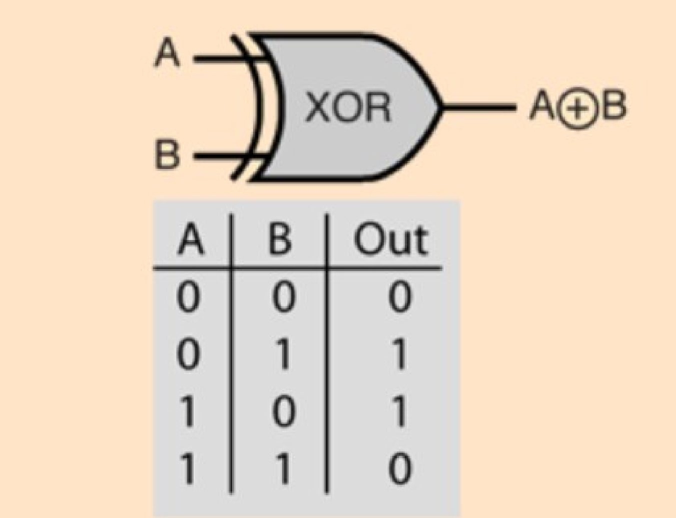
Message $\mathbf{m} \in \{0,1\}^n$ and keys $\mathbf{k} \in \{0,1\}^n$ are string of n-bits

- Encryption function

$$\mathrm{Enc} : [\mathbf{k}, \mathbf{m}] \longmapsto \mathbf{c} = \mathbf{m} \oplus \mathbf{k}$$

- Decryption function

$$\mathrm{Dec} : [\mathbf{k}, \mathbf{c}] \longmapsto \mathbf{m} = \mathbf{c} \oplus \mathbf{k}$$

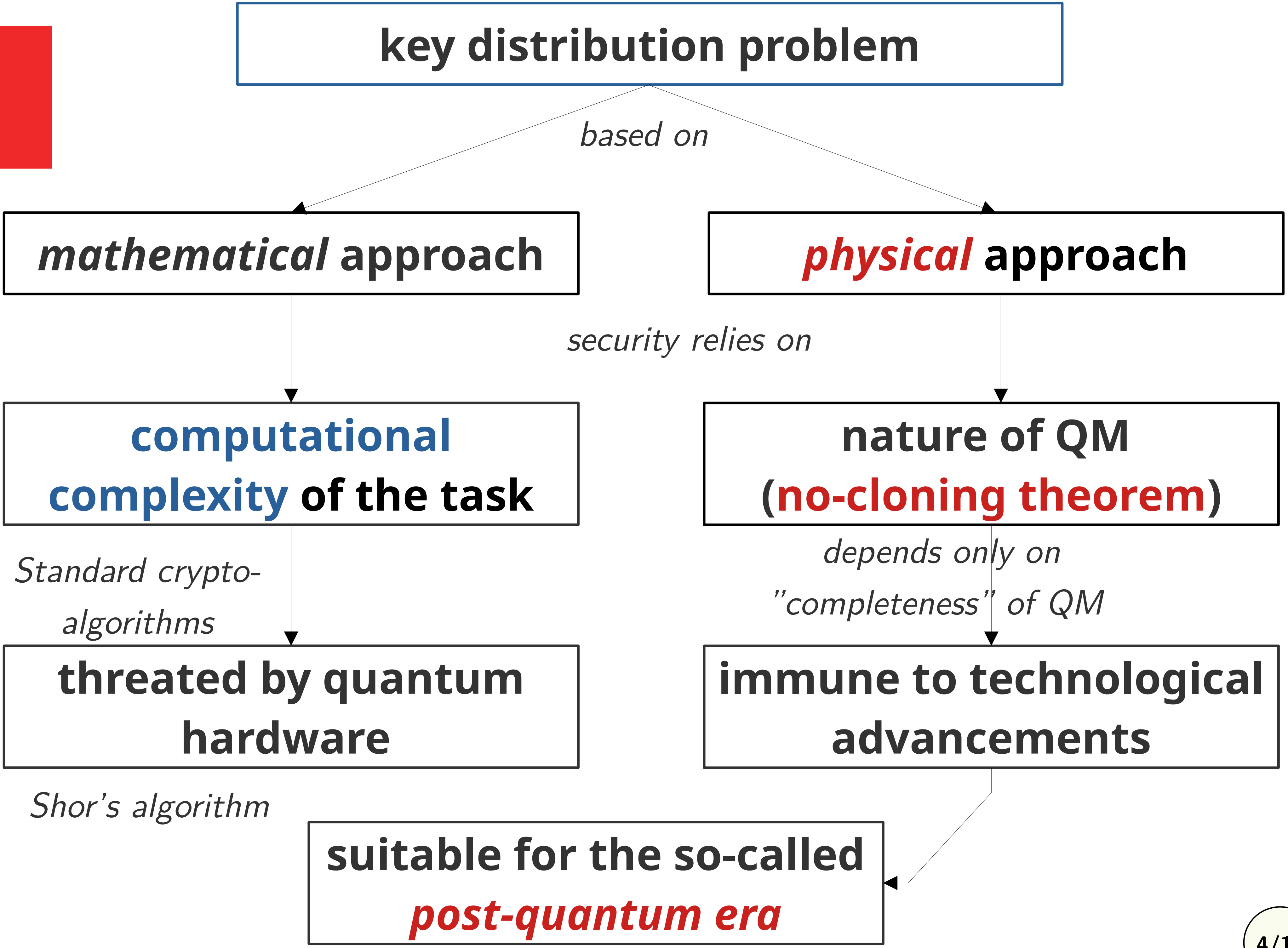


A	B	Out
0	0	0
0	1	1
1	0	1
1	1	0

Requirements for keys

- uniformly distributed
- **used once**

Main Problem: key distribution in a *secure* way



key distribution problem

based on

***mathematical* approach**

***physical* approach**

security relies on

computational complexity of the task

nature of QM (no-cloning theorem)

Standard crypto-algorithms

depends only on ”completeness” of QM

threated by quantum hardware

immune to technological advancements

Shor's algorithm

suitable for the so-called *post-quantum era*

quantum key distribution (QKD)

prepare-and-measure

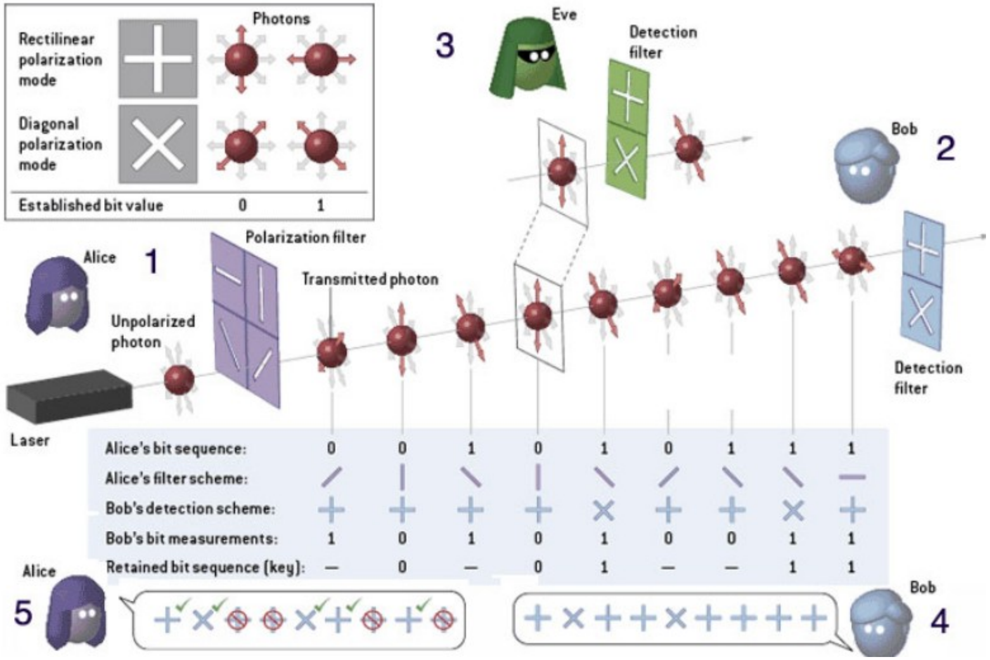
feature

source located on one side

Eve detected by

higher QBER

e.g. ***BB84 protocol***



Alice's bit sequence:	0	0	1	0	1	0	1	1	1
Alice's filter scheme:	/	|	\	|	\	/	\	\	—
Bob's detection scheme:	+	+	+	+	×	+	+	×	+
Bob's bit measurements:	1	0	1	0	1	0	0	1	1
Retained bit sequence (key):	–	0	–	0	1	–	–	1	1

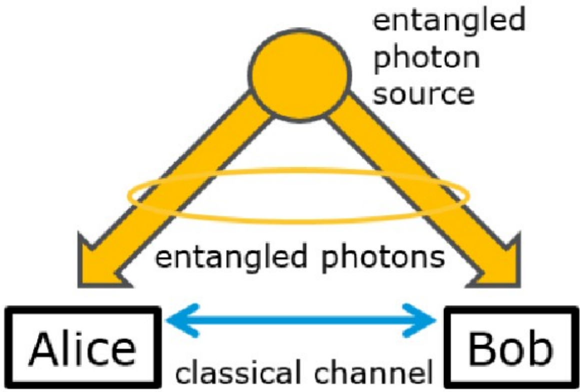
entanglement-based

feature

source independent on (Alice & Bob)

security based on

monogamy of entanglement



e.g. ***E91 protocol***

Part 2:

Theory & results behind the entanglement-based QKD protocols

EPR-Bell states

Maximally entangled *two-qubit basis*

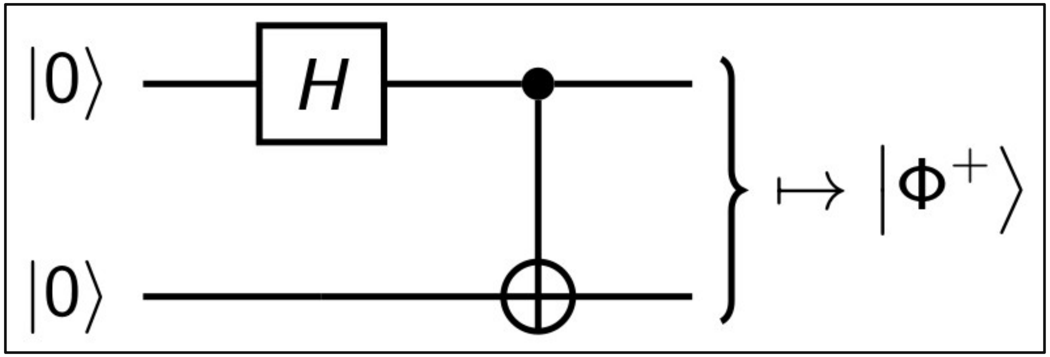
$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

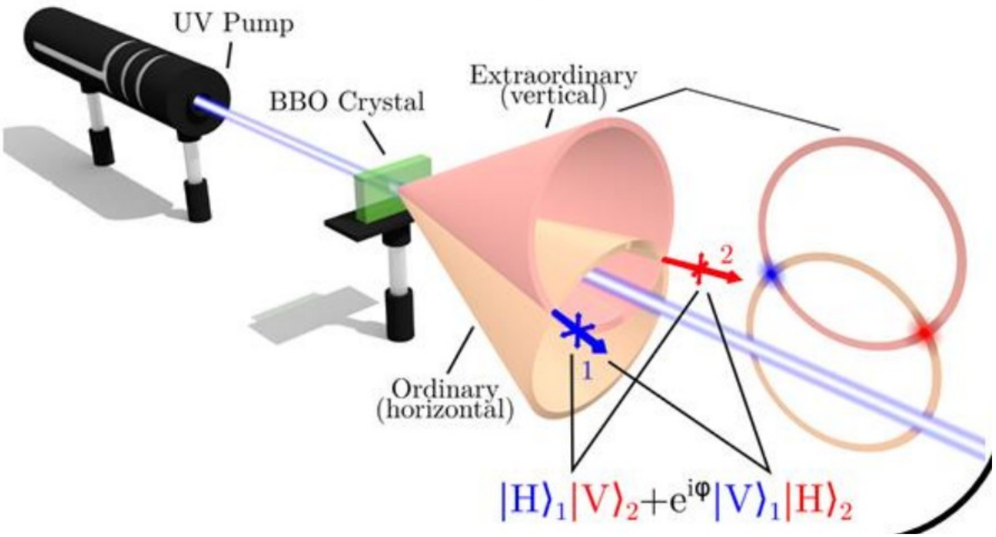
$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Quantum circuit to generate EPR-pairs



Polarization-entangled *photon pairs*

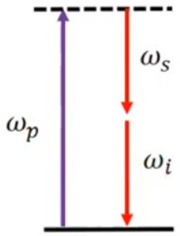


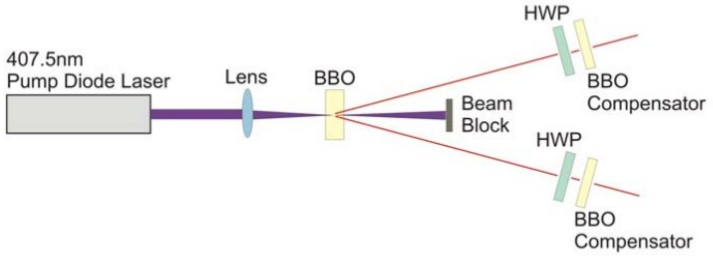
Credit: Christophe Couteau (2018) Spontaneous parametric down-conversion, Contemporary Physics, 59:3, 291-304,

SPDC *phenomenon*

$$\omega_{\text{pump}} = \omega_{\text{signal}} + \omega_{\text{idler}}$$

$$\vec{k}_{\text{pump}} = \vec{k}_{\text{signal}} + \vec{k}_{\text{idler}}$$

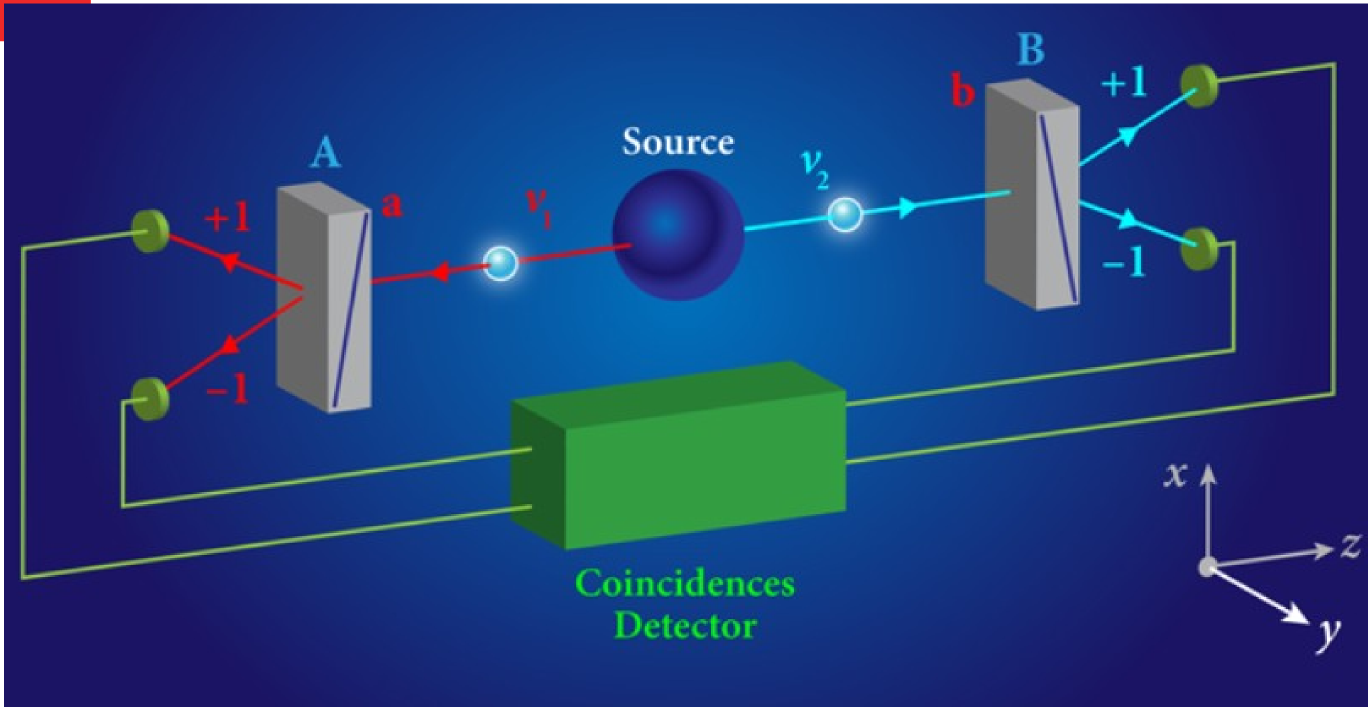




Credit: C. Erven (2007) Free Space Quantum Key Distribution and its Implementation with a Polarization-Entangled Parametric Down Conversion Source

EPR(B)- gedankenexperiment scheme

Credit: https://physics.aps.org/articles/v8/123



Source of EPR-pairs

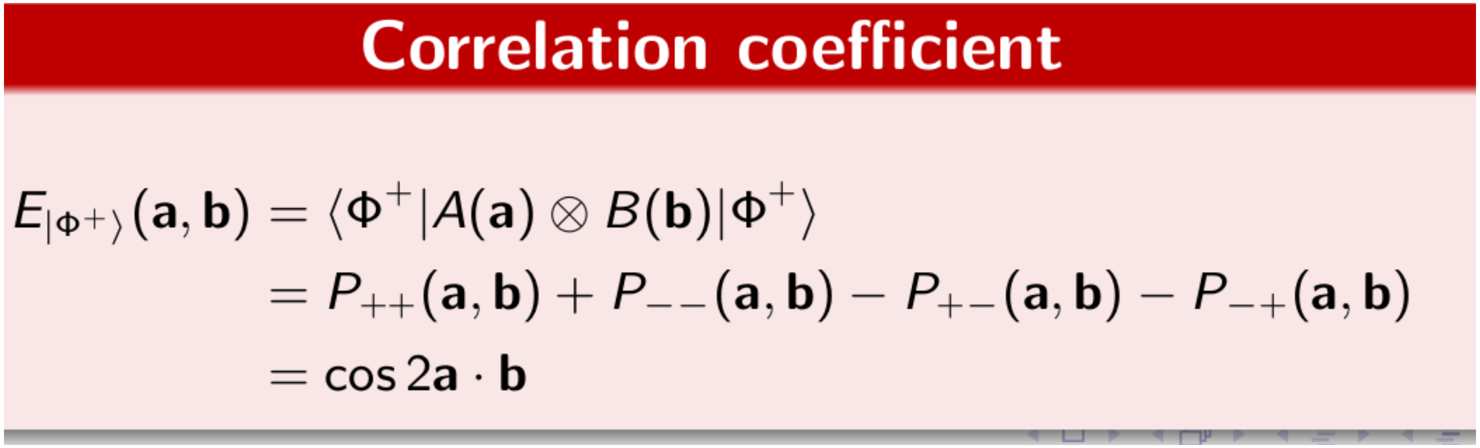
$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

orientations **a, b**

lie on ***x-y plane***

$\perp$

particle's trajectories



Correlation coefficient

$$\begin{aligned} E_{|\Phi^+\rangle}(\mathbf{a},\mathbf{b}) &= \langle\Phi^+|A(\mathbf{a})\otimes B(\mathbf{b})|\Phi^+\rangle \\ &= P_{++}(\mathbf{a},\mathbf{b}) + P_{--}(\mathbf{a},\mathbf{b}) - P_{+-}(\mathbf{a},\mathbf{b}) - P_{-+}(\mathbf{a},\mathbf{b}) \\ &= \cos 2\mathbf{a}\cdot\mathbf{b} \end{aligned}$$

CHSH inequality

a.k.a. ***Generalized Bell's theorem***

$$\mathbf{S} = E(\mathbf{a}_1, \mathbf{b}_1) - E(\mathbf{a}_1, \mathbf{b}_2) + E(\mathbf{a}_2, \mathbf{b}_1) + E(\mathbf{a}_2, \mathbf{b}_2)$$

Classical correlations

$$|S| \leq \mathbf{2}$$

QM correlations

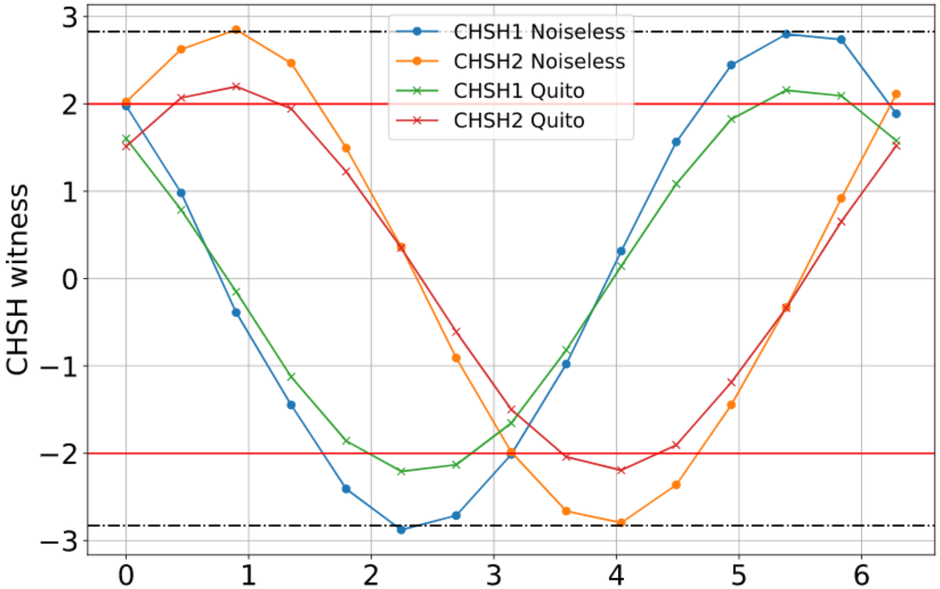
$$|S|_{\mathrm{EPR}} \leq \mathbf{2\sqrt{2}}$$

Ill. Niklas Elmehed © Nobel Prize Outreach

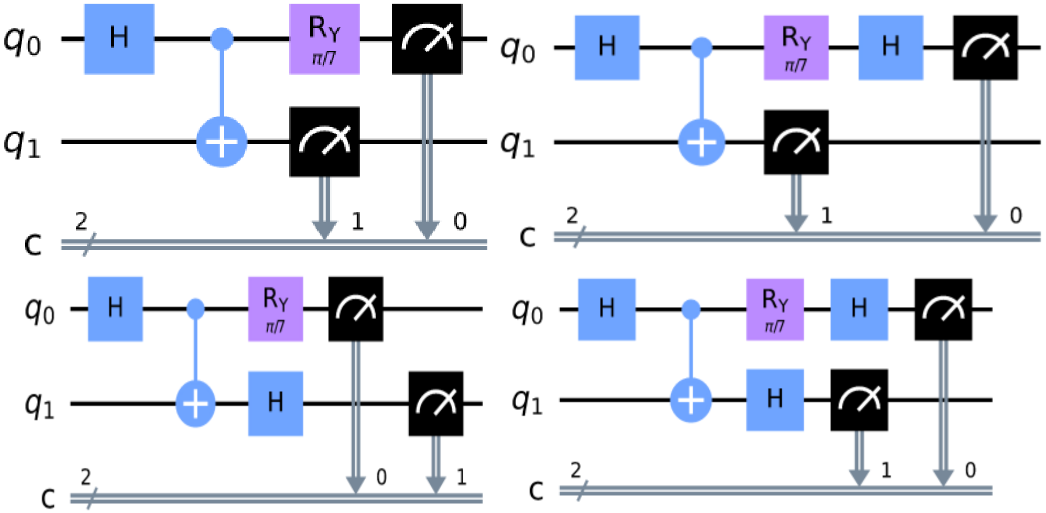
John F. Clauser

IBM Quantum Lab

$$\theta_i = i \times \frac{2\pi}{14},\ i \in (0, 14)$$



$\langle CHSH1 \rangle = \langle AB \rangle - \langle Ab \rangle + \langle aB \rangle + \langle ab \rangle$ $\langle CHSH2 \rangle = \langle AB \rangle + \langle Ab \rangle - \langle aB \rangle + \langle ab \rangle.$



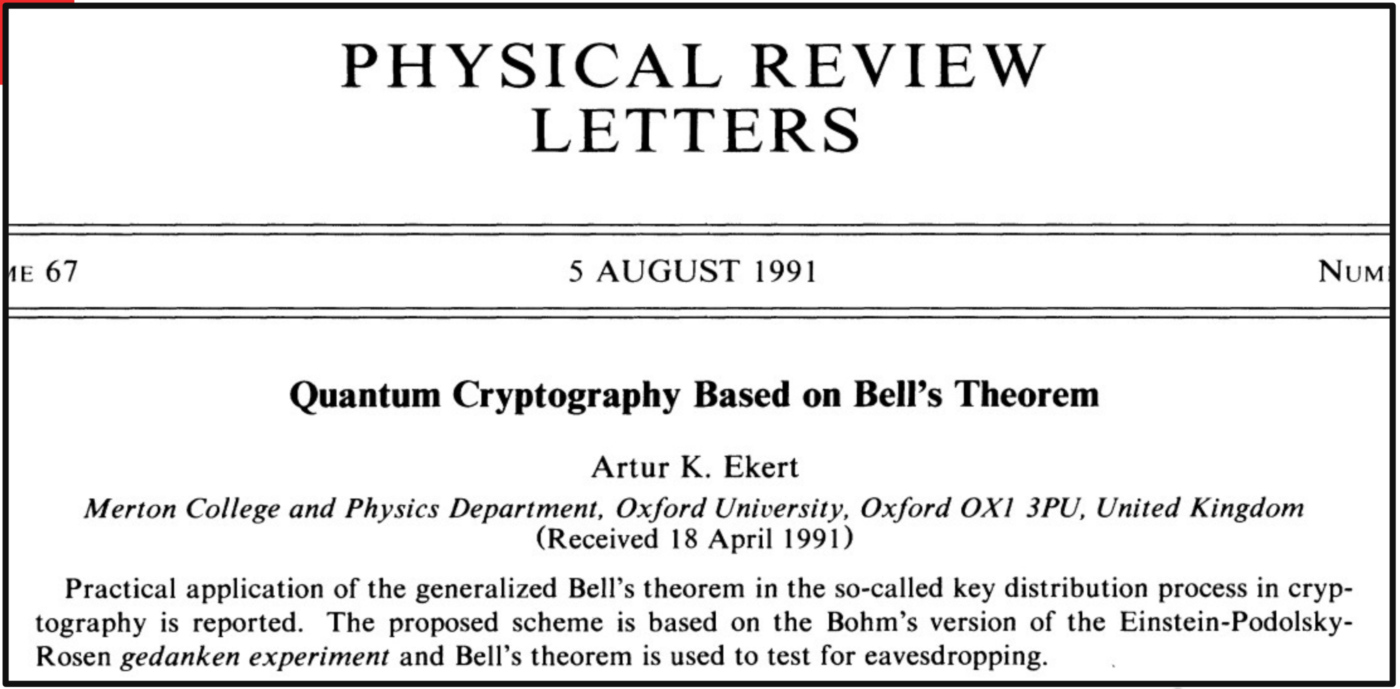
- q_1 → Bob, uses computational (Z) & X bases
- q_0 → Alice, rotated (angle θ) w.r.t. Bob bases

https://qiskit.org/textbook/ch-demos/chsh.html

Part 3:

the E91 protocol

Ekert Protocol (E91)



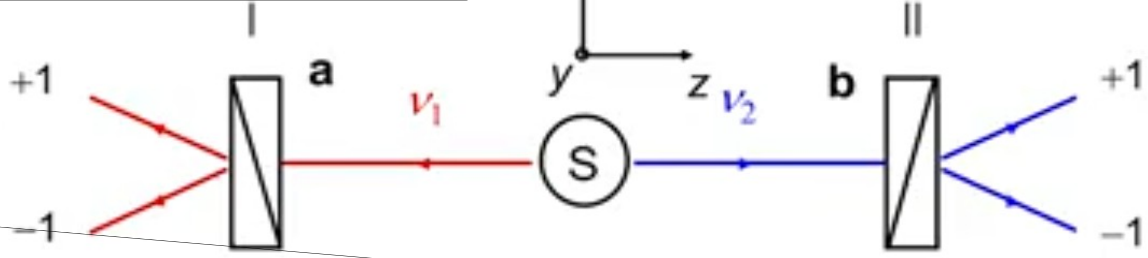
PHYSICAL REVIEW
LETTERS

E 67 5 AUGUST 1991 NUM

Quantum Cryptography Based on Bell's Theorem

Artur K. Ekert
Merton College and Physics Department, Oxford University, Oxford OX1 3PU, United Kingdom
(Received 18 April 1991)

Practical application of the generalized Bell's theorem in the so-called key distribution process in cryptography is reported. The proposed scheme is based on the Bohm's version of the Einstein-Podolsky-Rosen *gedanken experiment* and Bell's theorem is used to test for eavesdropping.



Ideas

testing for eavesdropping

check if the system violates Bell's theorem (CHSH form)

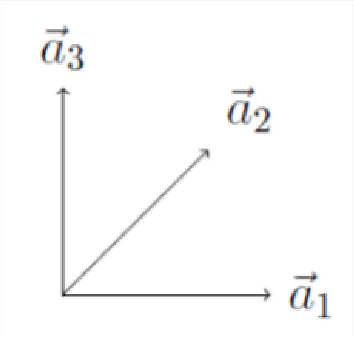
key generation

measurements performed in the same basis

Ekert Protocol (E91): configuration

Alice

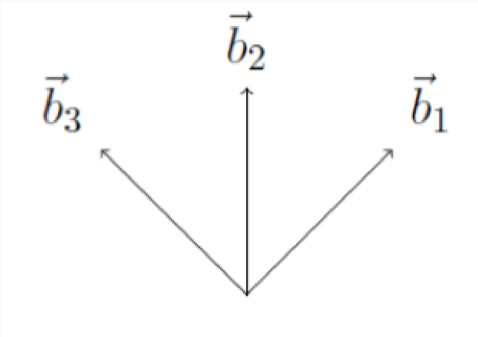
analyzer **randomly** oriented between $\{\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3\}$



such that $\phi_a^1 = 0°$, $\phi_a^2 = 45°$, $\phi_a^3 = 90°$

Bob

analyzer **randomly** oriented between $\{\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3\}$



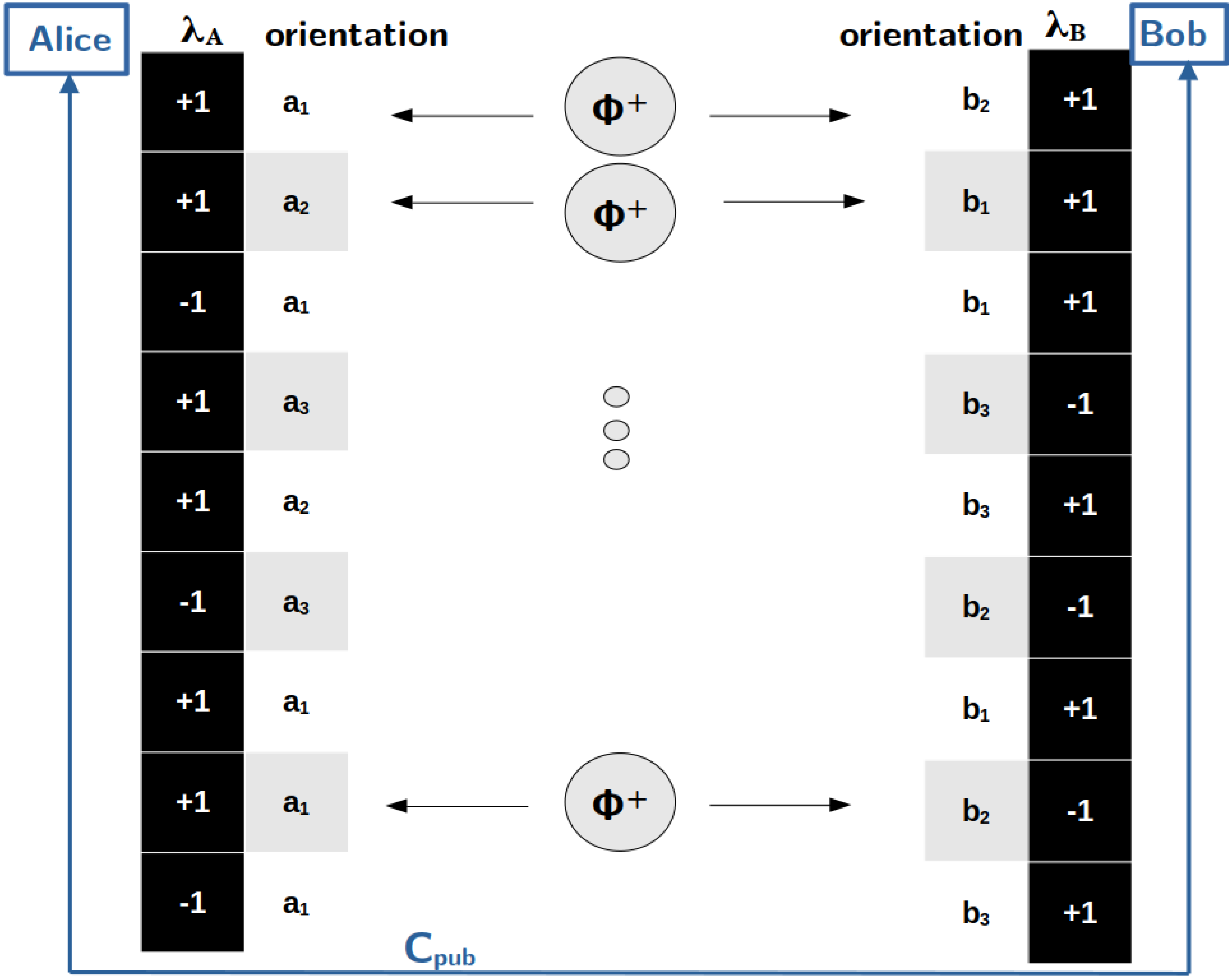
with $\phi_b^1 = 45°$, $\phi_b^2 = 90°$, $\phi_b^3 = 135°$

1. for compatible bases $\mathbf{a}_2, \mathbf{b}_1$ and $\mathbf{a}_3, \mathbf{b}_2$ there is **total correlation**, $E(\mathbf{a}_2, \mathbf{b}_1) = E(\mathbf{a}_3, \mathbf{b}_2) = 1$
2. for incompatible bases, one can compute $\mathbf{S} = E(\mathbf{a}_1, \mathbf{b}_1) - E(\mathbf{a}_1, \mathbf{b}_3) + E(\mathbf{a}_3, \mathbf{b}_1) + E(\mathbf{a}_3, \mathbf{b}_3)$

additional **public channel** $(\mathrm{C}_{\mathrm{pub}})$ is available

Ekert Protocol (E91): implementation

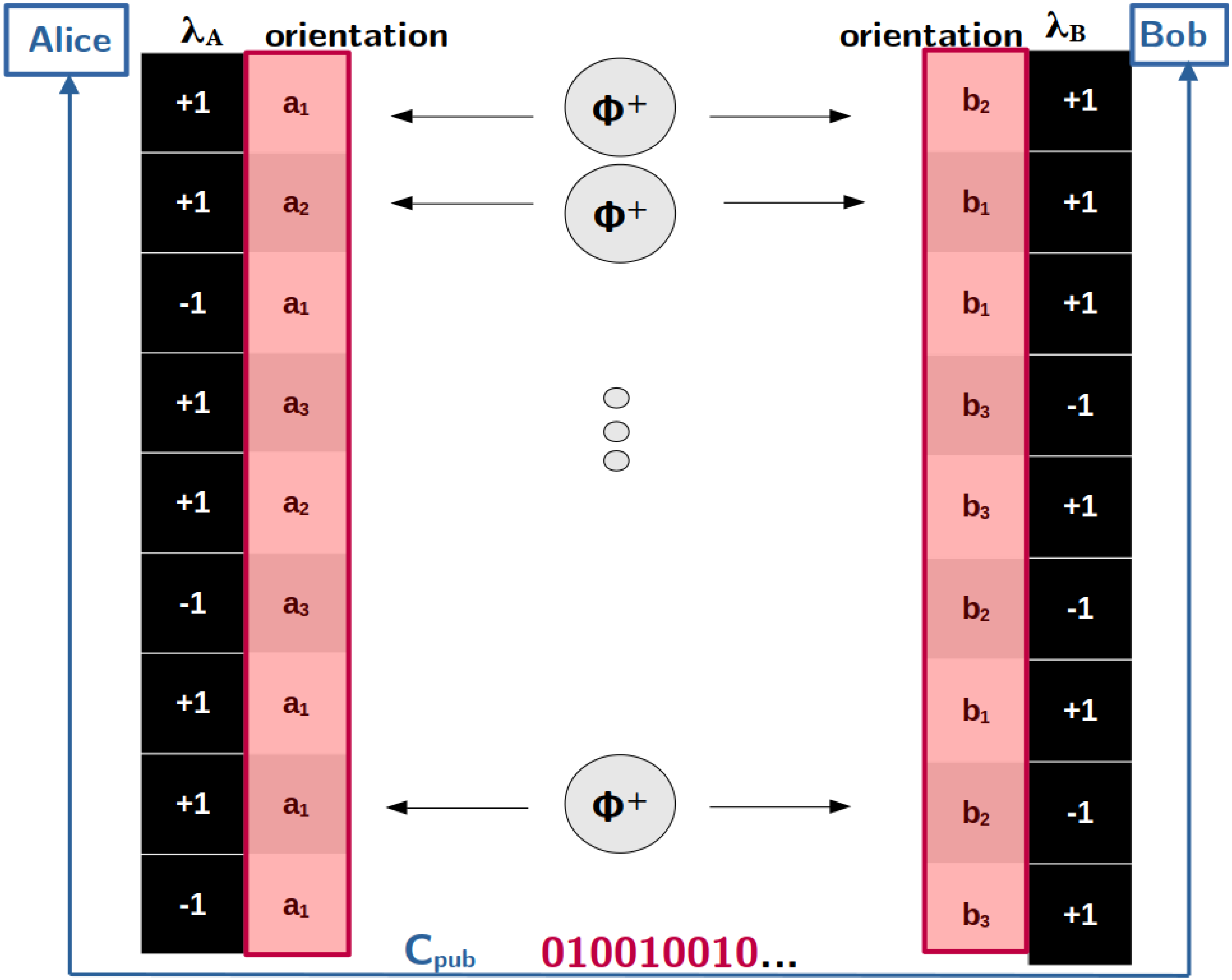
Step 1 Alice and Bob perform N measurements (*run*) and store both the experimental result (λ_A or λ_B) and the analyzer's orientation ($\mathbf{a_i}$ or $\mathbf{b_i}$)



λ_A	orientation	orientation	λ_B
+1	a_1	b_2	+1
+1	a_2	b_1	+1
-1	a_1	b_1	+1
+1	a_3	b_3	-1
+1	a_2	b_3	+1
-1	a_3	b_2	-1
+1	a_1	b_1	+1
+1	a_1	b_2	-1
-1	a_1	b_3	+1

Ekert Protocol (E91): implementation

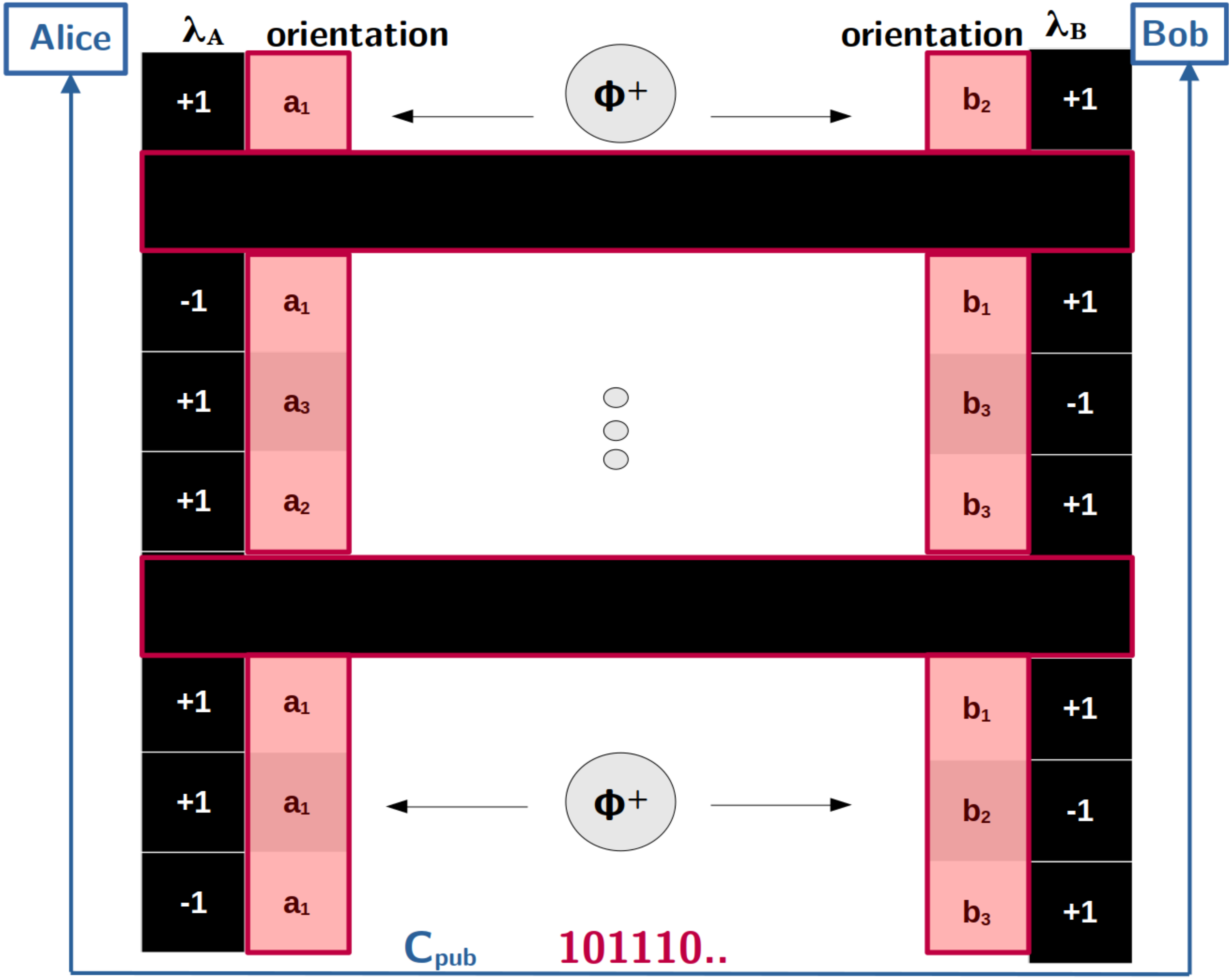
Step 2 Alice and Bob communicate in public (C_{pub}) the selected orientations



λ_A	orientation	orientation	λ_B
+1	a_1	b_2	+1
+1	a_2	b_1	+1
-1	a_1	b_1	+1
+1	a_3	b_3	-1
+1	a_2	b_3	+1
-1	a_3	b_2	-1
+1	a_1	b_1	+1
+1	a_1	b_2	-1
-1	a_1	b_3	+1

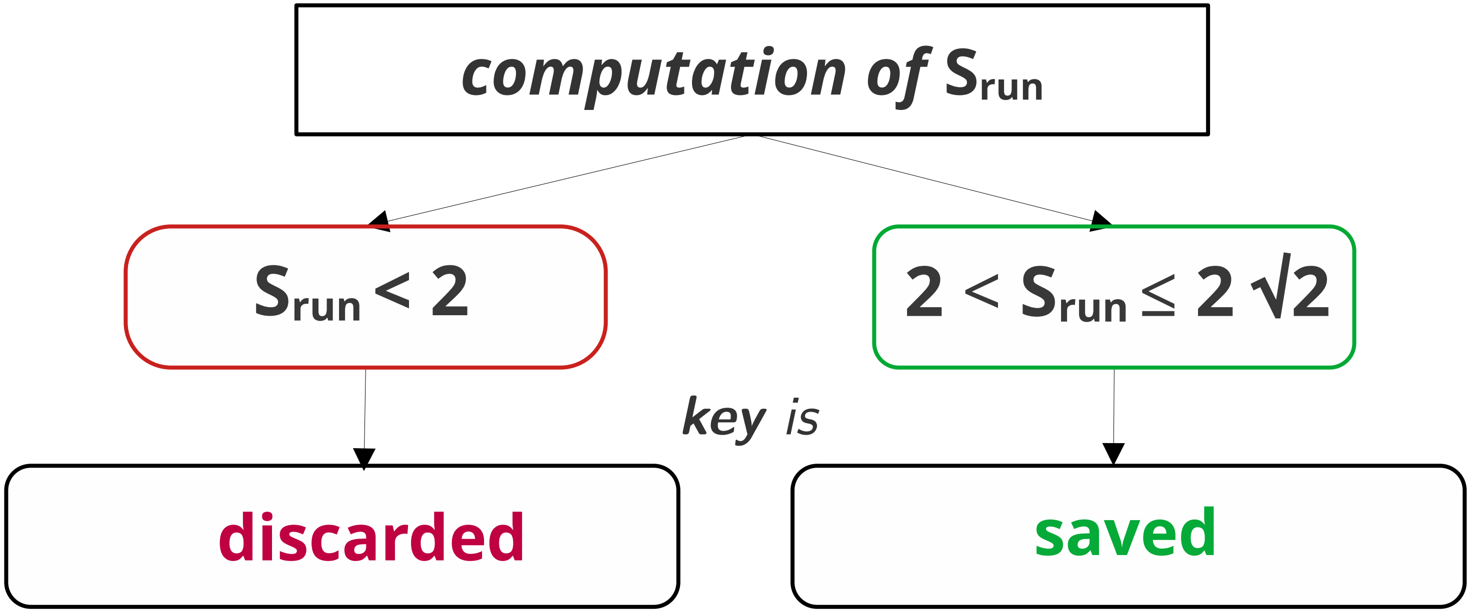
Ekert Protocol (E91): implementation

Step 3 Alice and Bob keep secret the results of their measurements performed in *compatible* bases, whereas they share the **outcomes** in **incompatible** bases



Ekert Protocol (E91): implementation

Step 4



computation of S_{run}

$S_{run} < 2$

$2 < S_{run} \leq 2\sqrt{2}$

key is

discarded

saved

Advanced Steps

- evaluation of quantum bit error rate (**QBER**) sharing small sample of the key

Classical post-processing

- error reconciliation
- privacy amplification

Summary of E91 protocol

- The presence of an *eavesdropper* (Eve) along the channel is detected testing the *violation of CHSH inequality*. Indeed Eve disturbs the system to gain information on it, lowering the degree of correlations below the classical bound

- The key generation part is independent on the testing procedure, thus no information leakage occurs in the testing part

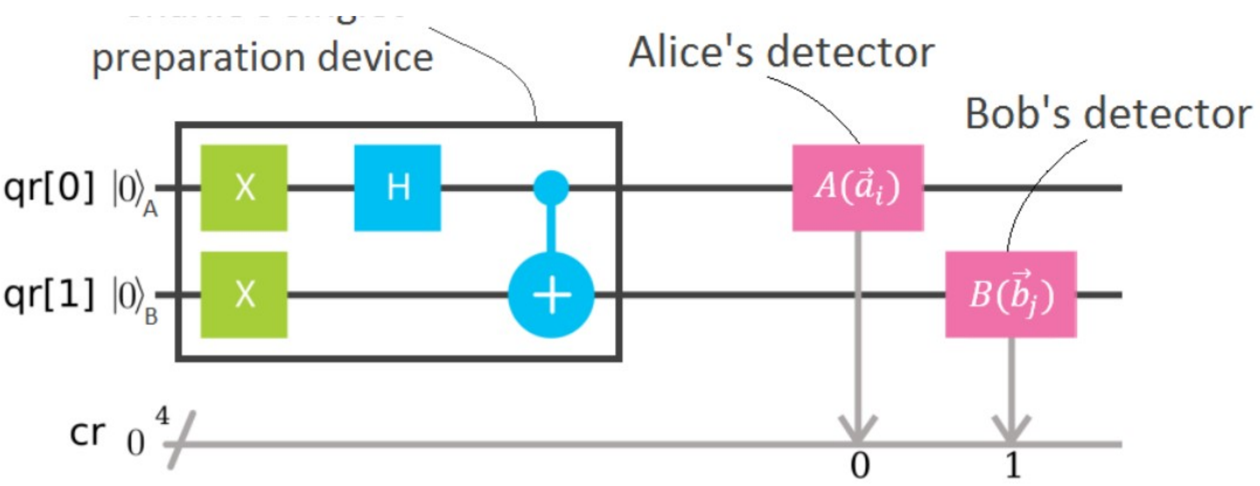
- The security of the key distribution, as in all QKD protocols, does not depend on the computational complexity of the task but on fundamental laws of physics → suitable for the coming of quantum computers with sufficiently large numbers of qubits (the so-called post-quantum era)

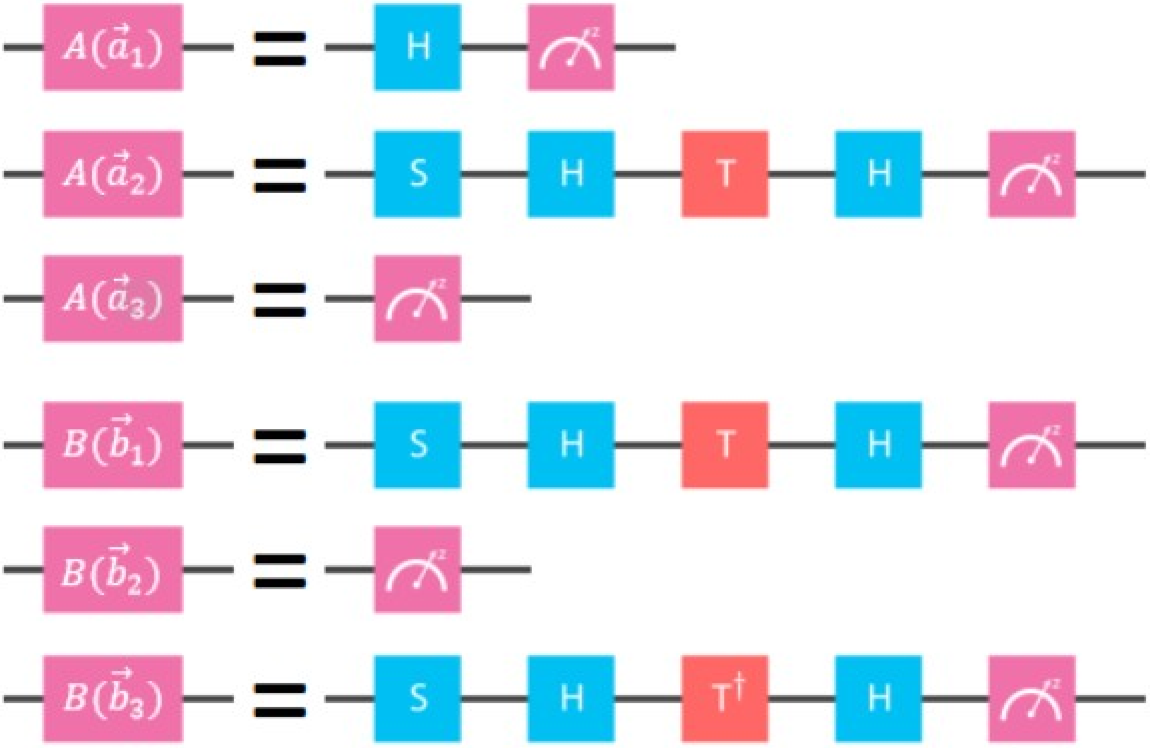
> *"It is not a mathematical difficulty of a particular computation, but a fundamental physical law that protects the system, and as long as quantum theory is not refuted as a complete theory the system is secure"*

from Ekert PRL paper

Part 4:
Experimental realizations of entanglement-based QKD

E91 protocol with quantum gates





$$W = \frac{1}{\sqrt{2}}(X+Z), V = \frac{1}{\sqrt{2}}(-X+Z)$$

$\vec{a}_1 = (1,0,0)$ (X observable)

$\vec{a}_2 = \left(\frac{1}{\sqrt{2}}, 0, \frac{1}{\sqrt{2}}\right)$ (W observable)

$\vec{a}_3 = (0,0,1)$ (Z observable)

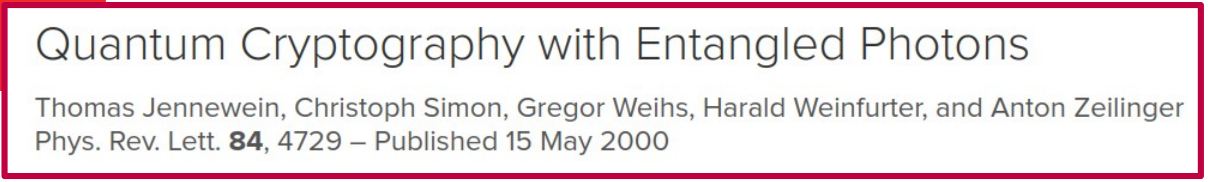
$\vec{b}_1 = \left(\frac{1}{\sqrt{2}}, 0, \frac{1}{\sqrt{2}}\right)$ (W observable)

$\vec{b}_2 = (0,0,1)$ (Z observable)

$\vec{b}_3 = \left(-\frac{1}{\sqrt{2}}, 0, \frac{1}{\sqrt{2}}\right)$ (V observable)

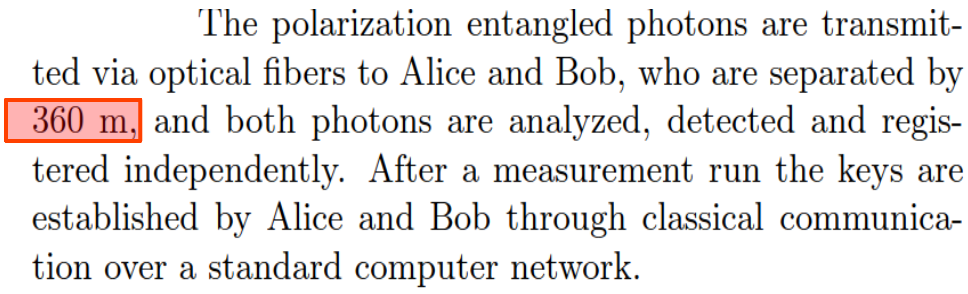
https://github.com/kardashin/E91_protocol/blob/master/E91_tutorial/E91_tutorial.ipynb

First report of complete entanglement-based QKD system over dedicated optical fibers



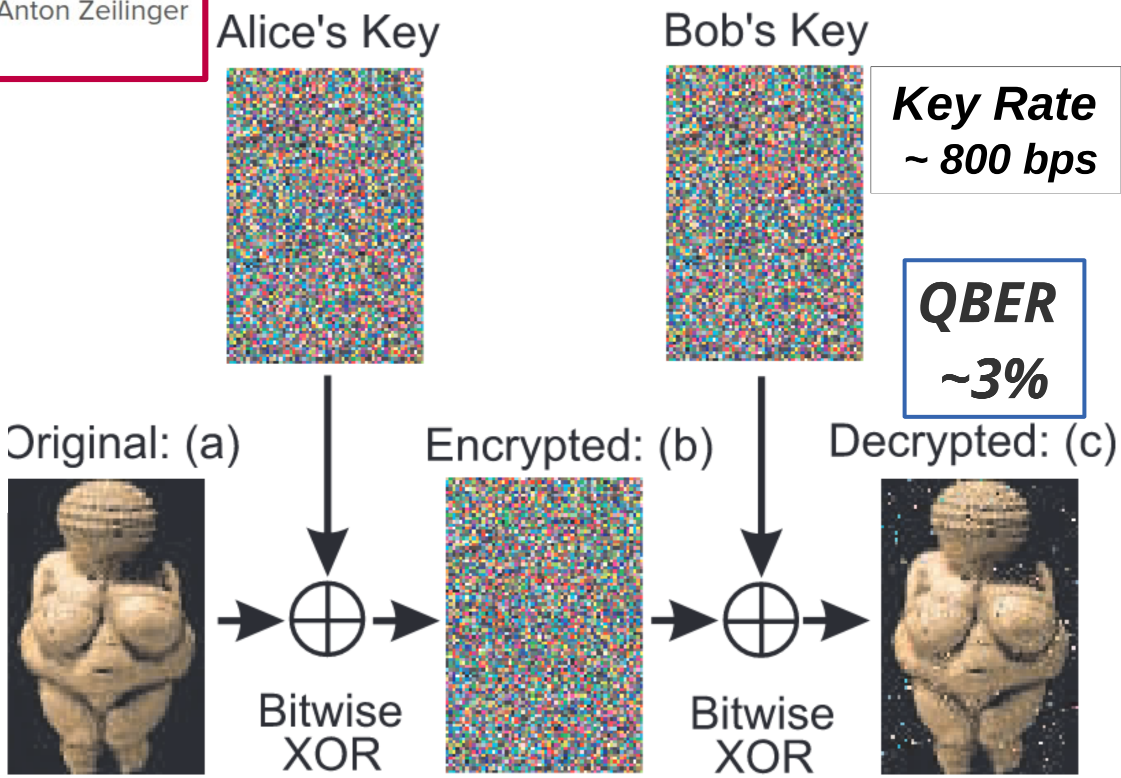
Quantum Cryptography with Entangled Photons

Thomas Jennewein, Christoph Simon, Gregor Weihs, Harald Weinfurter, and Anton Zeilinger
Phys. Rev. Lett. **84**, 4729 – Published 15 May 2000



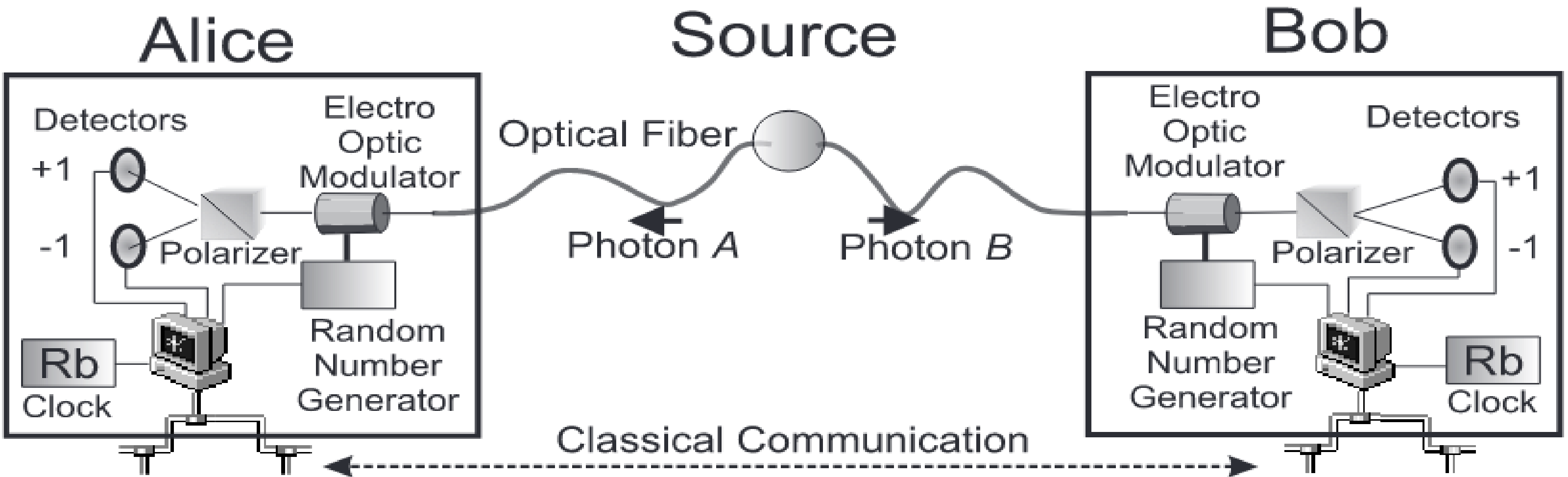
The polarization entangled photons are transmitted via optical fibers to Alice and Bob, who are separated by 360 m, and both photons are analyzed, detected and registered independently. After a measurement run the keys are established by Alice and Bob through classical communication over a standard computer network.

variant of BB84 protocol



Key Rate ~ 800 bps

QBER ~3%



Experimental E91 quantum key distribution

Alexander Ling [*], Matt Peloso, Ivan Marcikic, Antía Lamas-Linares and Christian Kurtsiefer

[1] Department of Physics, National University of Singapore, Singapore, 117542

ABSTRACT

We report on a field implementation of an E91 protocol. In this experiment, we make use of the violation of a Bell inequality to derive a secure key.

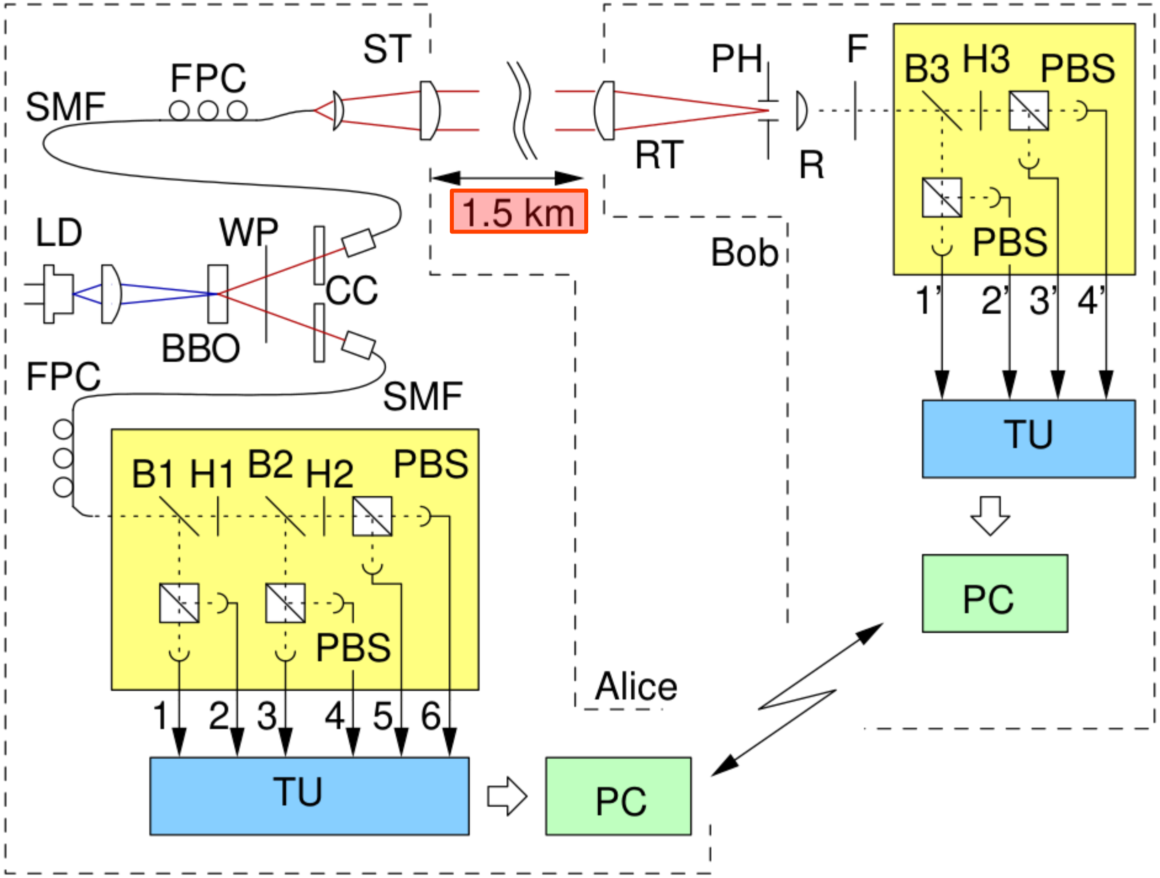
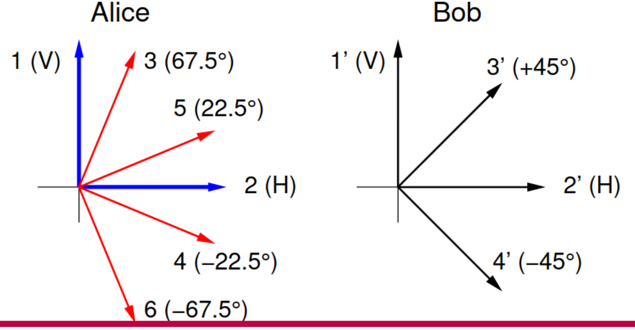
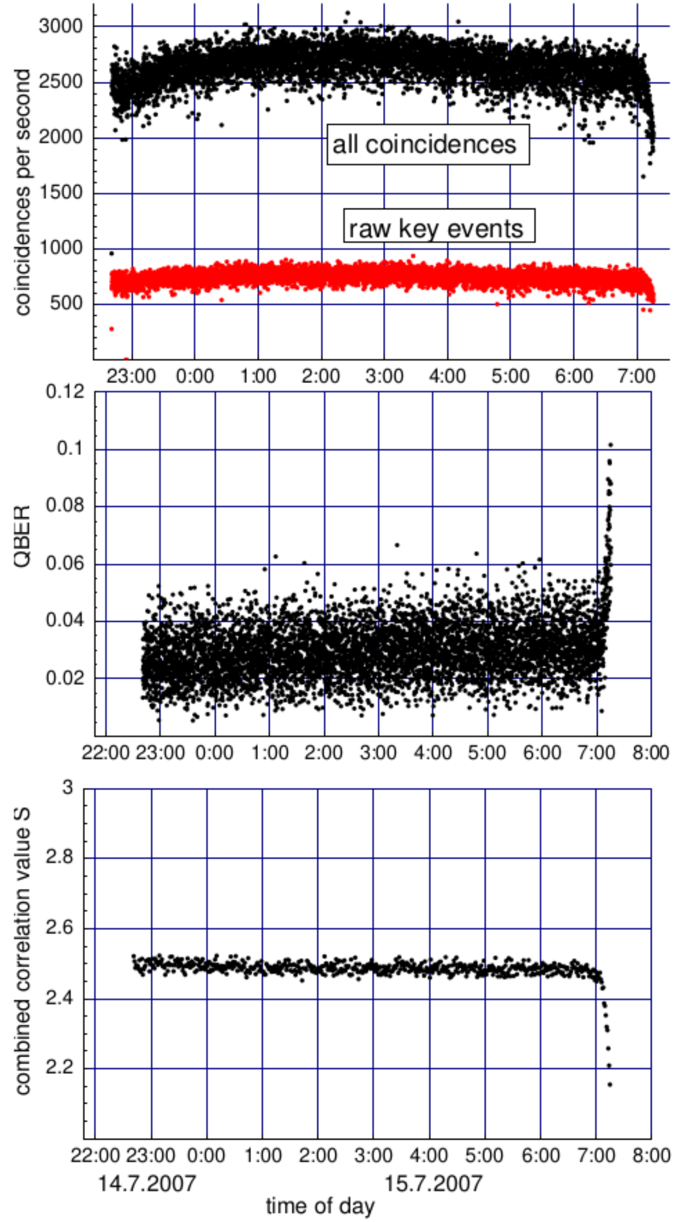
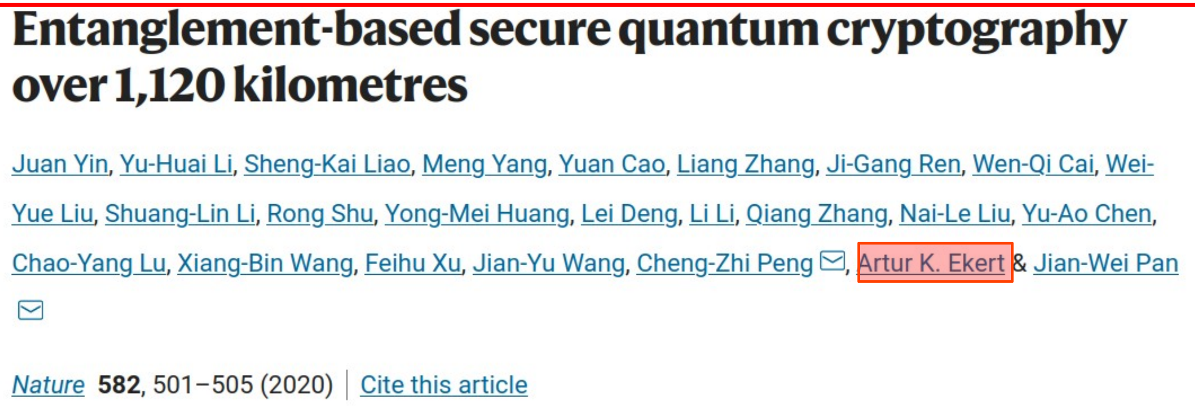


Figure 2. Experimental setup. Polarization-entangled photon-pairs are generated via parametric down conversion pumped by a laser diode (LD, PO) in a nonlinear optical crystal (BBO) with walk-off compensation (WP, CC) into single mode optical fibers (SMF). A free-space optical channel for one detector set (Bob) is realized using small telescopes on both sides (ST, RT) with some spatial and spectral filtering (PH, F). Both parties perform polarization measurements in bases randomly chosen by beam splitters (B1-B3), and defined by properly oriented wave plates (H1-H3) in front of polarizing beam splitters (PBS) and photon counting detectors. Photo events are registered separately with time stamp units (TU) connected to two personal computers (PC) linked via a classical channel.





The new frontier: space-based QKD

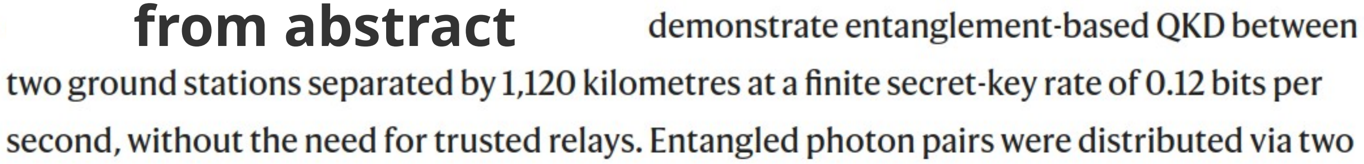


Entanglement-based secure quantum cryptography over 1,120 kilometres

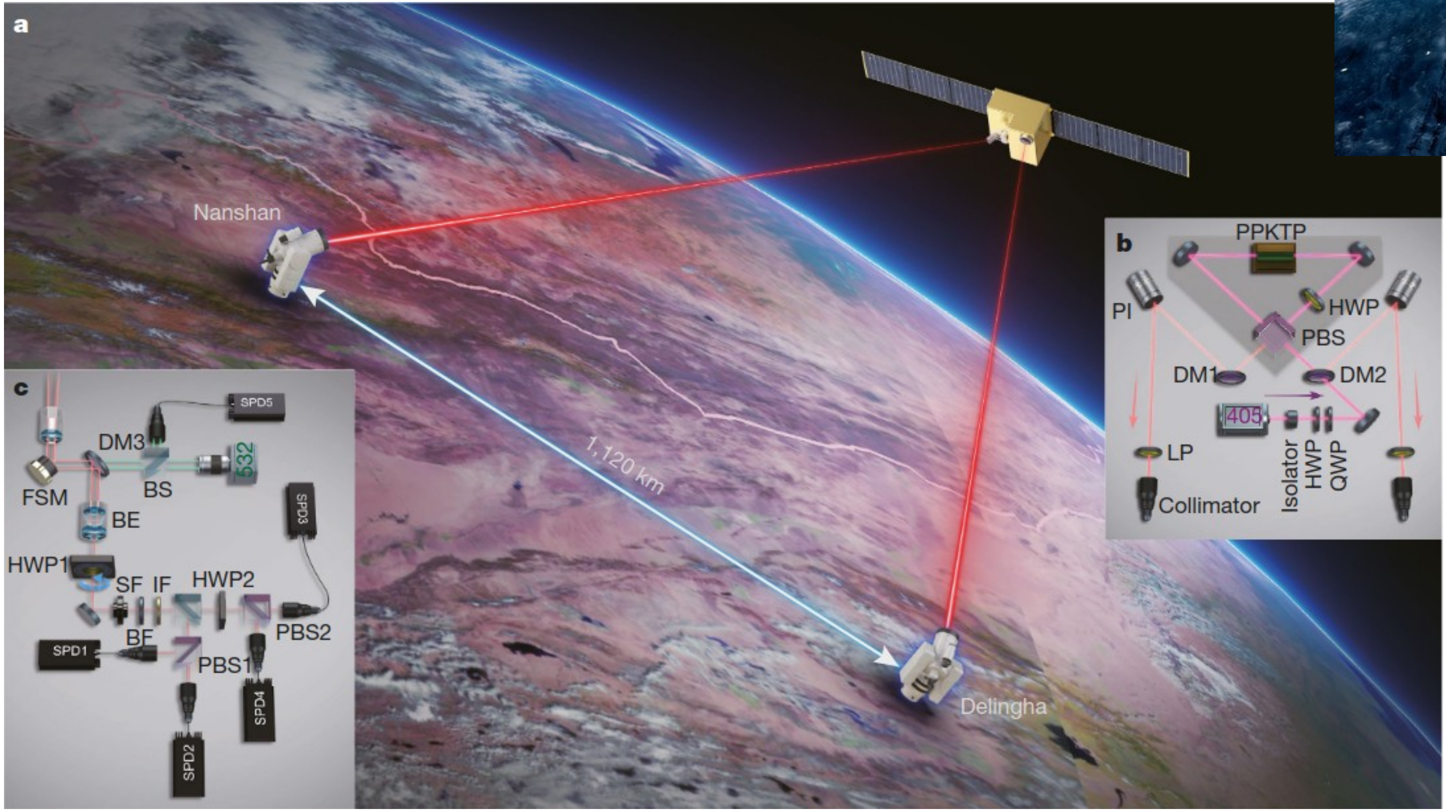
Juan Yin, Yu-Huai Li, Sheng-Kai Liao, Meng Yang, Yuan Cao, Liang Zhang, Ji-Gang Ren, Wen-Qi Cai, Wei-Yue Liu, Shuang-Lin Li, Rong Shu, Yong-Mei Huang, Lei Deng, Li Li, Qiang Zhang, Nai-Le Liu, Yu-Ao Chen, Chao-Yang Lu, Xiang-Bin Wang, Feihu Xu, Jian-Yu Wang, Cheng-Zhi Peng ✉, Artur K. Ekert & Jian-Wei Pan ✉

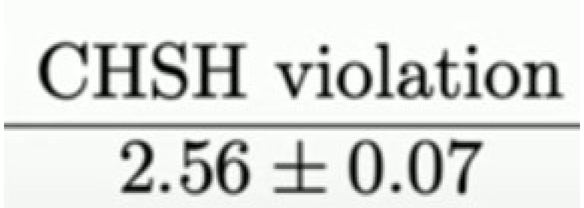
Nature **582**, 501–505 (2020) | Cite this article

from abstract

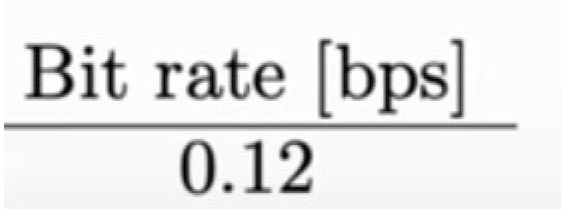


demonstrate entanglement-based QKD between two ground stations separated by 1,120 kilometres at a finite secret-key rate of 0.12 bits per second, without the need for trusted relays. Entangled photon pairs were distributed via two





CHSH violation
2.56 ± 0.07



Bit rate [bps]
0.12

Thanks
for
your attention