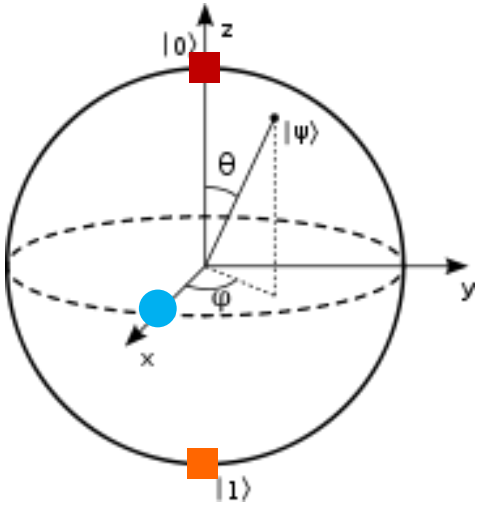
Introduction to **Quantum Computation**

letná škola FMFI UK
Svit, 9/2014

Daniel Nagaj

0 Review: a single qubit



$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$$

$|+\rangle$

$$Z|0\rangle \quad Z|1\rangle \quad X|+\rangle \quad X|-\rangle$$

- how can I distinguish $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ from a 50% mix $|0\rangle, |1\rangle$

- the Hadamard transform

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

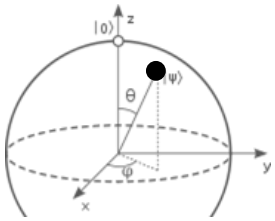
$$Z|+\rangle \quad H|0\rangle \quad XH|-\rangle$$

$$X|1\rangle \quad H|+\rangle \quad HZ|-\rangle$$


UniCredit Bank
Credit Classic
4000 1234 5678 9010
4150
0000
VALID THRU 00/00
JOSEF NOVÁK
VISA

1 **we need a qubit**

well, what can we do with it?

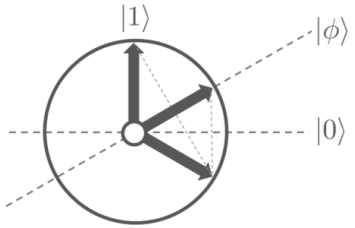


2 **EPR pairs**

and tricky 2-qubit protocols

3 **the algorithms**

that make quantum computing tick

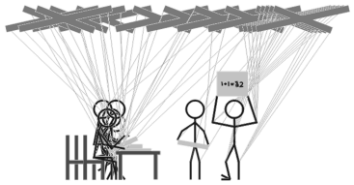


4 **error correction**

can we really scale up this stuff?

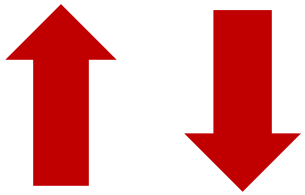
5 **the limits**

complexity & limits of q. computing



strange action at a distance

1 Two qubits: the basi(c)s



- how many dimensions do we need?
- how do 1-qubit operations look now?

$$U \otimes \mathbb{I}$$
$$\mathbb{I} \otimes V$$

- 2-qubit tensor-product operations?

$$X \otimes X$$
$$Z \otimes Z$$

- some basic 2-qubit operations?
  (action in the computational basis + linearity)

CNOT	**C –PHASE**	**SWAP**
10 … 11	11 … -11	10 … 01

1 The Bell basis

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|0\rangle \pm |1\rangle|1\rangle\right)$$

$$|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|1\rangle \pm |1\rangle|0\rangle\right)$$

- measure qubit 1... what happens to qubit 2?
- an EPR pair (the singlet): how does look in another basis?

$$\frac{1}{\sqrt{2}}\left(|0\rangle|1\rangle - |1\rangle|0\rangle\right)$$

$$= \frac{1}{\sqrt{2}}\left(|a\rangle|a^{\perp}\rangle - |a^{\perp}\rangle|a\rangle\right)$$

$$|a\rangle = \begin{bmatrix} \cos\varphi \\ \sin\varphi \end{bmatrix}$$

$$|a^{\perp}\rangle = \begin{bmatrix} \sin\varphi \\ -\cos\varphi \end{bmatrix}$$

Hippies believed that with enough LSD, everybody could be perfectly in tune with each other...

Charlie Bennett

Entanglement allows two particles to be in a perfectly definite joint state, even though each one by itself is completely random.

Like two hippies who feel **perfectly in tune** with each other, even though neither has an opinion on anything.

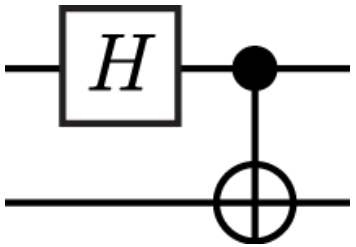
Charlie Bennett

1 The Bell states

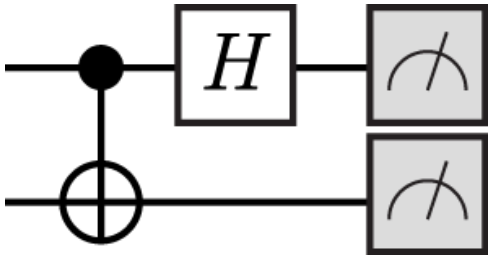
$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|0\rangle \pm |1\rangle|1\rangle\right)$$

$$|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|1\rangle \pm |1\rangle|0\rangle\right)$$

- preparing them from $|0\rangle|0\rangle$



- distinguishing them by measuring Z?



- transforming between the Bell states?

2 Super-dense coding

$$Z|\Psi^-\rangle$$

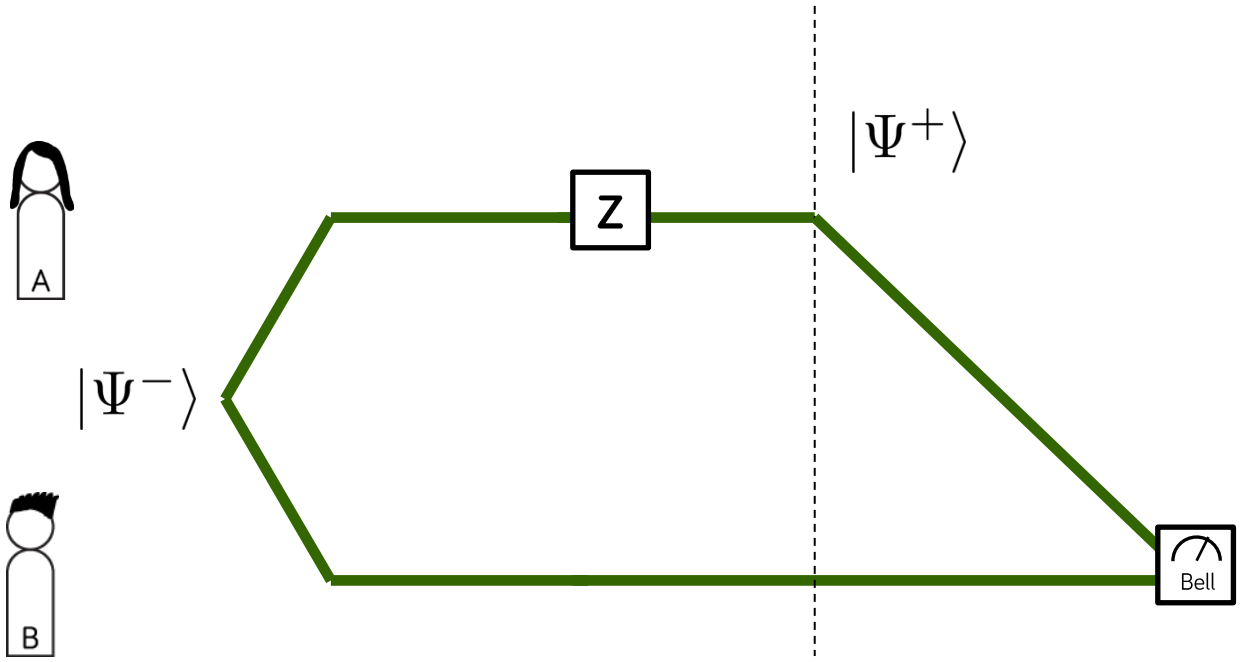
$$X|\Psi^-\rangle$$

$$XZ|\Psi^-\rangle$$

- transforming between the Bell states?

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|1\rangle - |1\rangle|0\rangle\right)$$

- what is a shared EPR pair good for?



2 Super-dense coding

$$Z|\Psi^-\rangle$$

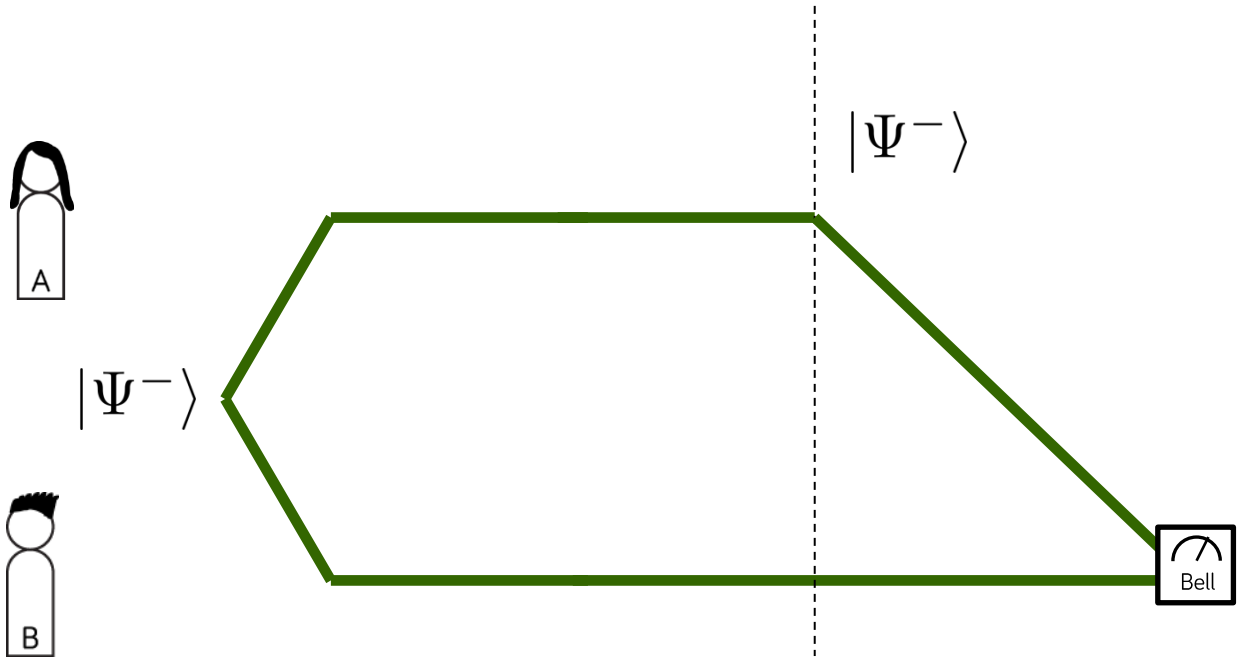
$$X|\Psi^-\rangle$$

$$XZ|\Psi^-\rangle$$

- transforming between the Bell states?

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|1\rangle - |1\rangle|0\rangle\right)$$

- what is a shared EPR pair good for?



2 Super-dense coding

$$Z|\Psi^-\rangle$$

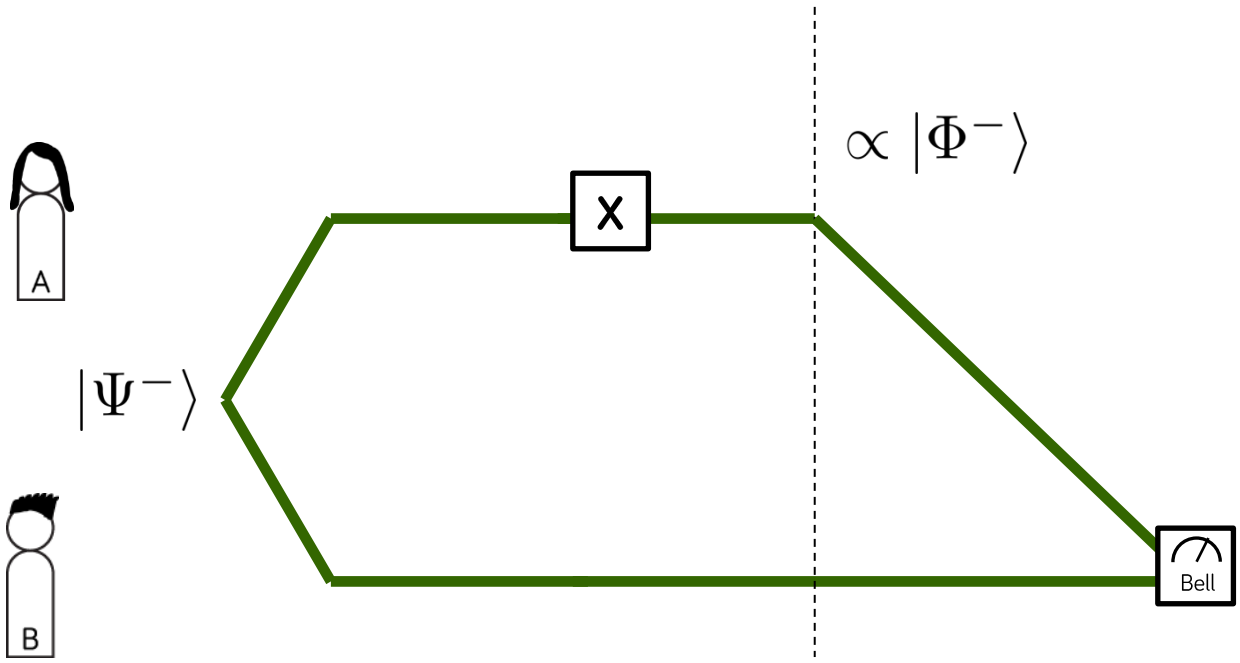
- transforming between the Bell states?

$$X|\Psi^-\rangle$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|1\rangle - |1\rangle|0\rangle\right)$$

$$XZ|\Psi^-\rangle$$

- what is a shared EPR pair good for?



2 Super-dense coding

$$Z|\Psi^-\rangle$$

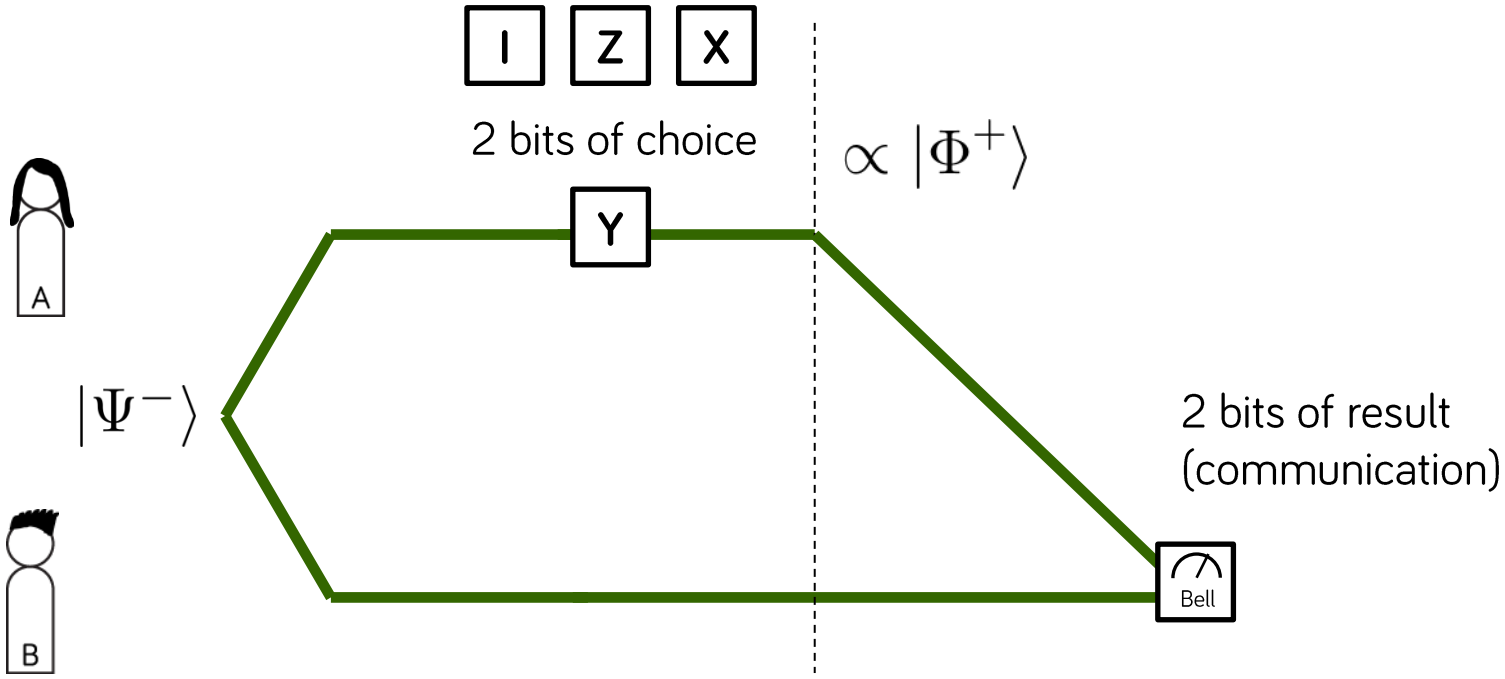
$$X|\Psi^-\rangle$$

$$XZ|\Psi^-\rangle$$

- transforming between the Bell states?

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|1\rangle - |1\rangle|0\rangle\right)$$

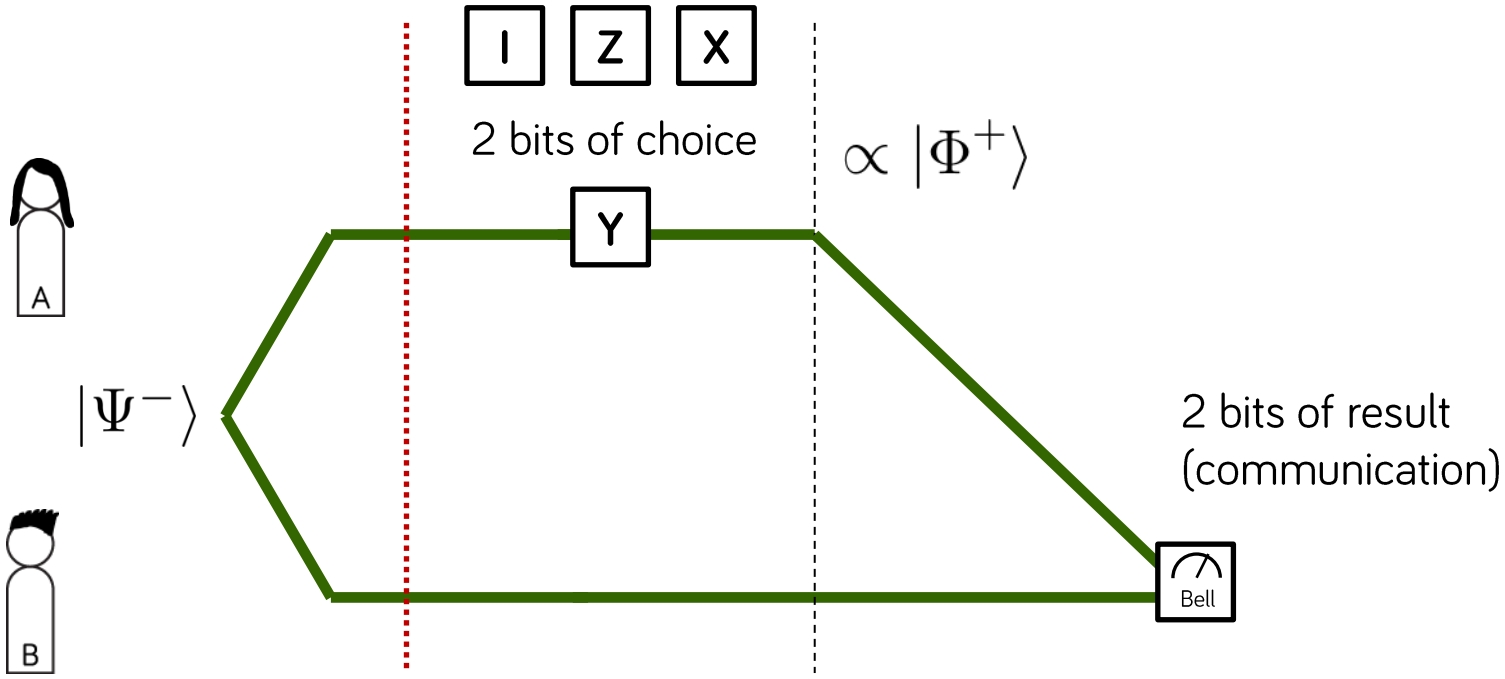
- what is a shared EPR pair good for?



2 Super-dense coding

1 EPR + 1 Q = 2 C

- what is a shared EPR pair good for?

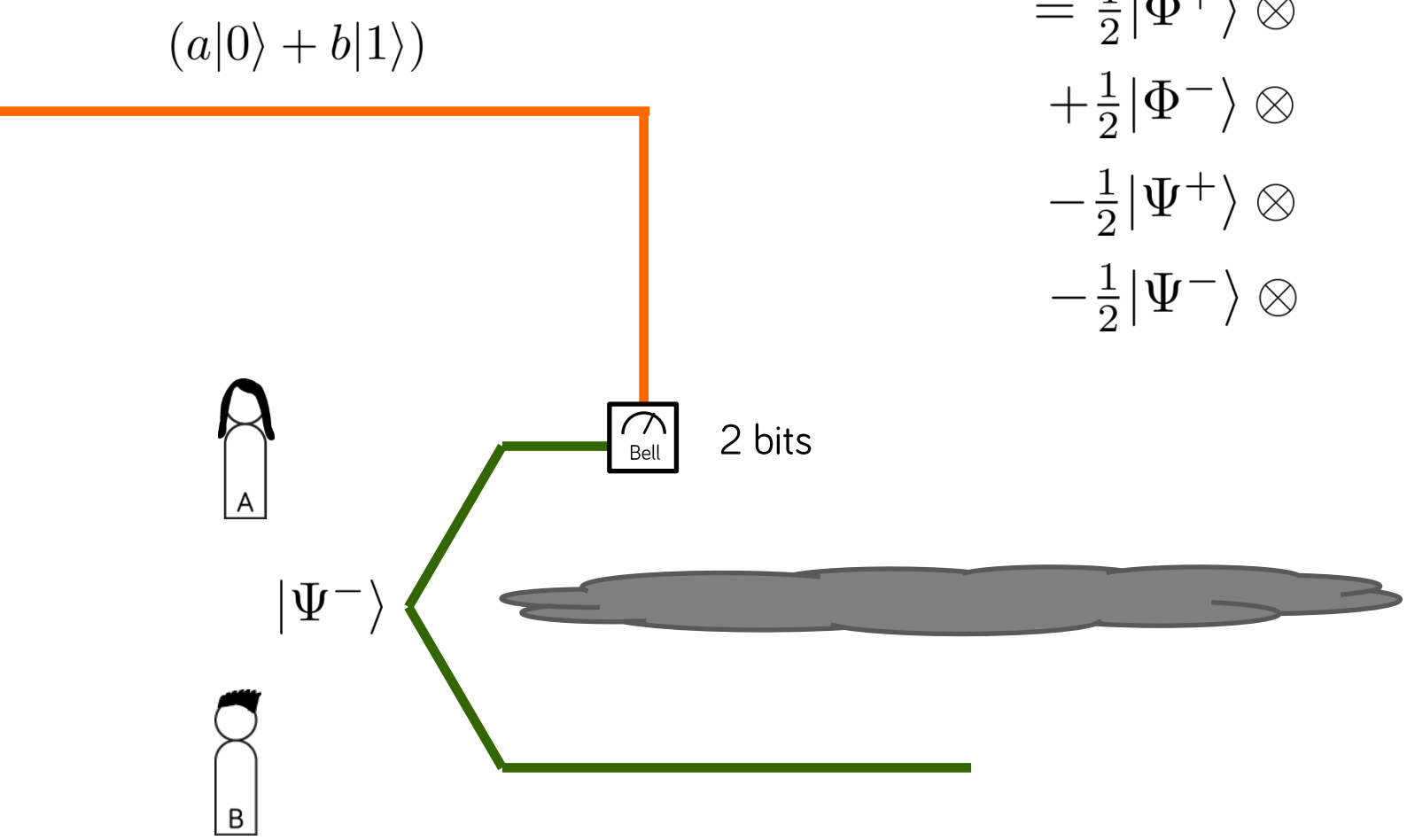


3 Quantum teleportation

- sending quantum states when quantum channels no longer work

$$(a|0\rangle + b|1\rangle) \otimes |\Psi^-\rangle$$

$$= \tfrac{1}{2}|\Phi^+\rangle \otimes$$
$$+\tfrac{1}{2}|\Phi^-\rangle \otimes$$
$$-\tfrac{1}{2}|\Psi^+\rangle \otimes$$
$$-\tfrac{1}{2}|\Psi^-\rangle \otimes$$

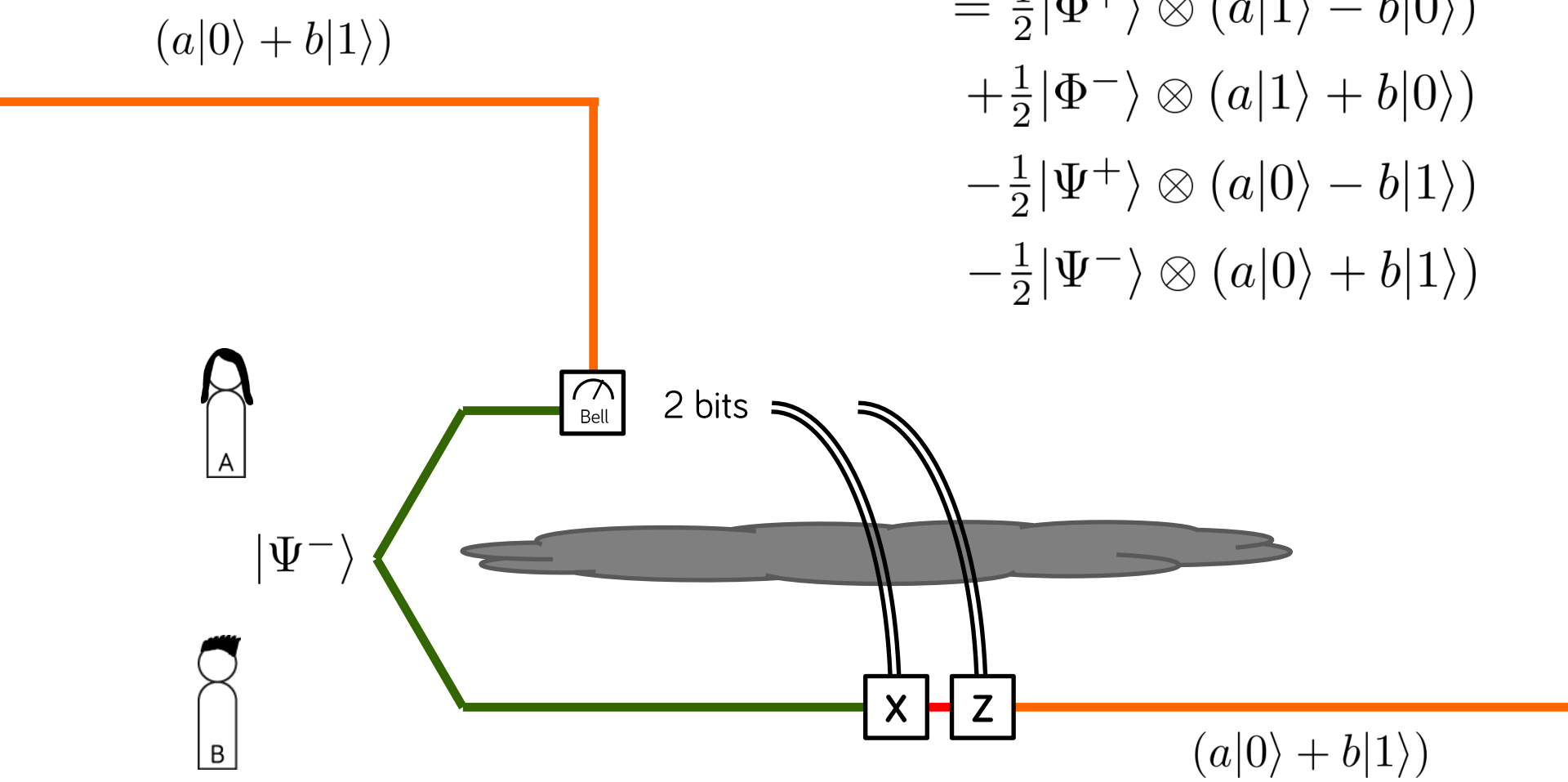


3 Quantum teleportation

- sending quantum states when quantum channels no longer work

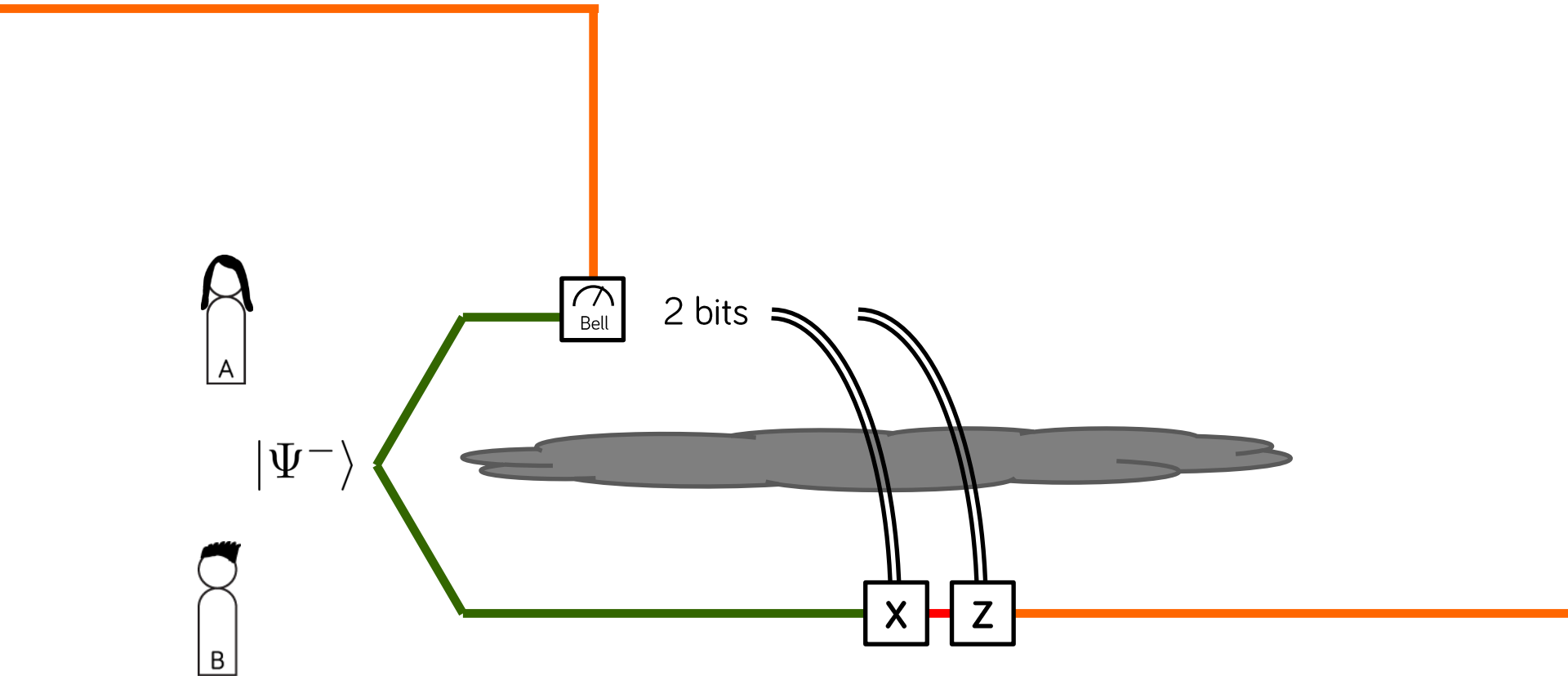
$$(a|0\rangle + b|1\rangle) \otimes |\Psi^-\rangle$$

$$= \tfrac{1}{2}|\Phi^+\rangle \otimes (a|1\rangle - b|0\rangle)$$
$$+\tfrac{1}{2}|\Phi^-\rangle \otimes (a|1\rangle + b|0\rangle)$$
$$-\tfrac{1}{2}|\Psi^+\rangle \otimes (a|0\rangle - b|1\rangle)$$
$$-\tfrac{1}{2}|\Psi^-\rangle \otimes (a|0\rangle + b|1\rangle)$$



3 Quantum teleportation

1 EPR + 2 C = 1 Q



$$1\,\mathbf{EPR} + 2\,\mathbf{C} = 1\,\mathbf{Q}$$

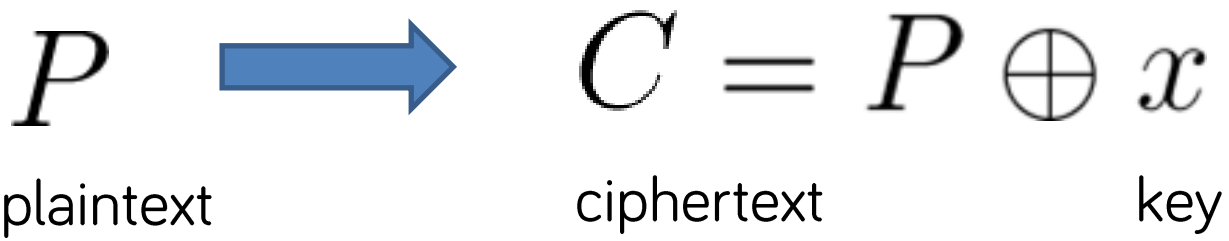
quantum teleportation

$$1\,\mathbf{EPR} + 1\,\mathbf{Q} = 2\,\mathbf{C}$$

superdense coding

[Physics World]

5 Unconditional security: one-time pad



5 Unconditional security: one-time pad

$$P \longrightarrow C = P \oplus x$$

plaintext ciphertext key

$$P = C \oplus x \oplus x$$

- the key can be safely used only once!

$$D = Q \oplus x$$

$$C \oplus D = P \oplus Q$$

- a different option: **computational security**
  C=F(P), and computing F^{-1} is hard

[wiki]

5 Sharing a password using a public channel

- Share an EPR pair.
- Local operations.
- Announce the results!
- Do some checking.
- Get **a secret key** (for a one-time pad).

5 Making up a password using a public channel

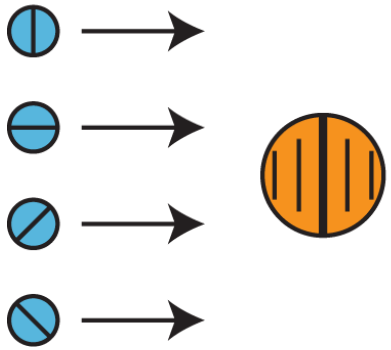
The BB84 protocol (no entanglement).

Alice

choose a basis

prepare a photon

send it



Bob

choose a basis

measure the photon

1

0

random

random

[Bennett & Brassard]

5 Making up a password using a public channel

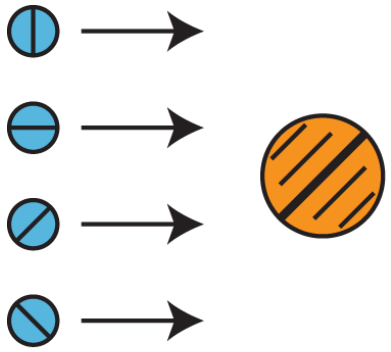
The BB84 protocol (no entanglement).

Alice

choose a basis

prepare a photon

send it



Bob

choose a basis

measure the photon

random

random

1

0

compare the basis choices (publicly)
correlated results wherever the bases match
those results make up the **secret key**

[Bennett & Brassard]

5 Making up a secure password with EPR

The Ekert91 protocol (with EPR pairs).

Alice

make an EPR pair

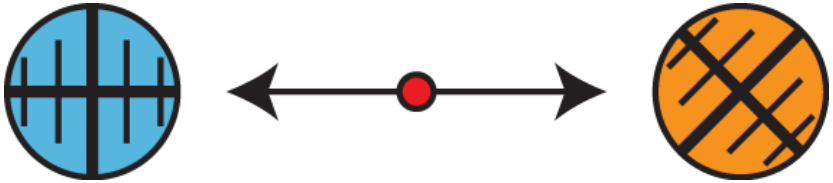
send 1 photon to B

choose a basis & measure

Bob

choose a basis

measure the photon



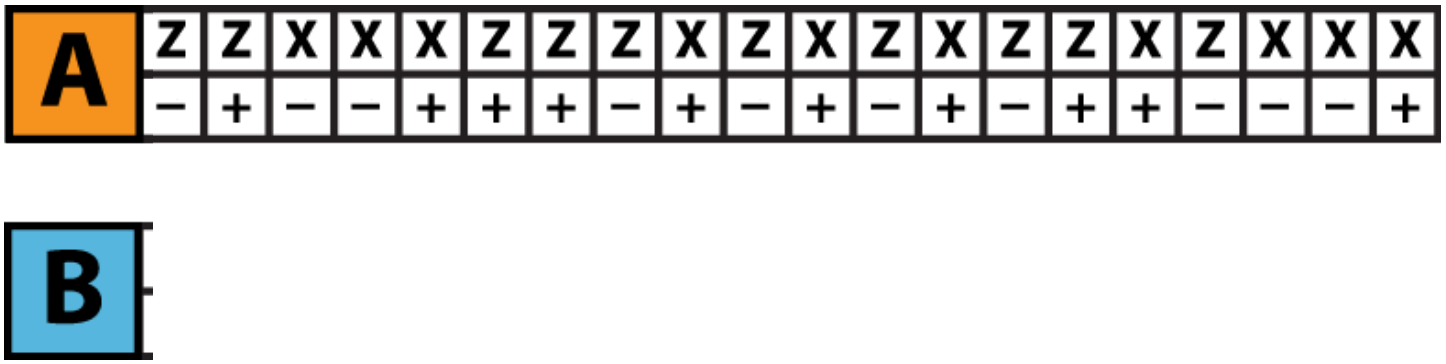
compare the basis choices (publicly)

anticorrelated results wherever the bases match

use some of the results for Bell tests (**check for Eve**)

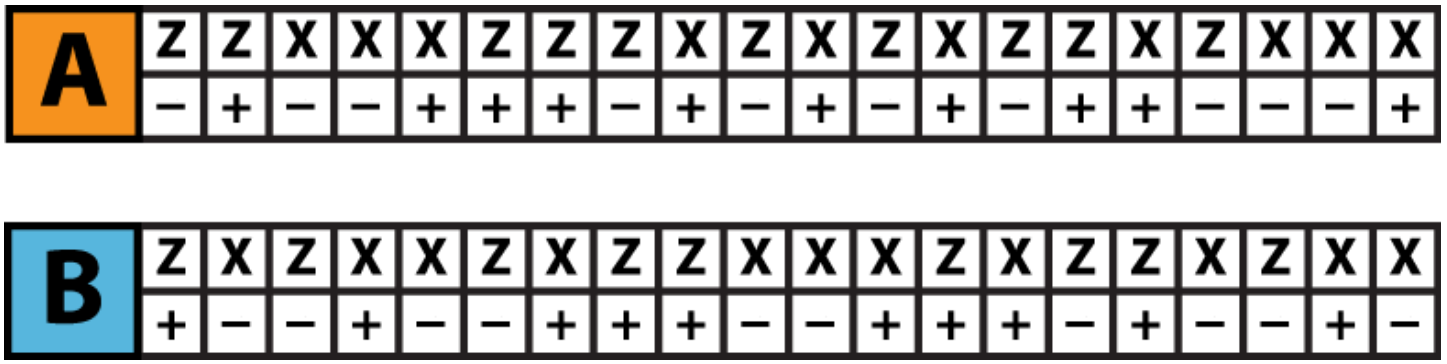
the rest make up the **secret key**

[Ekert]



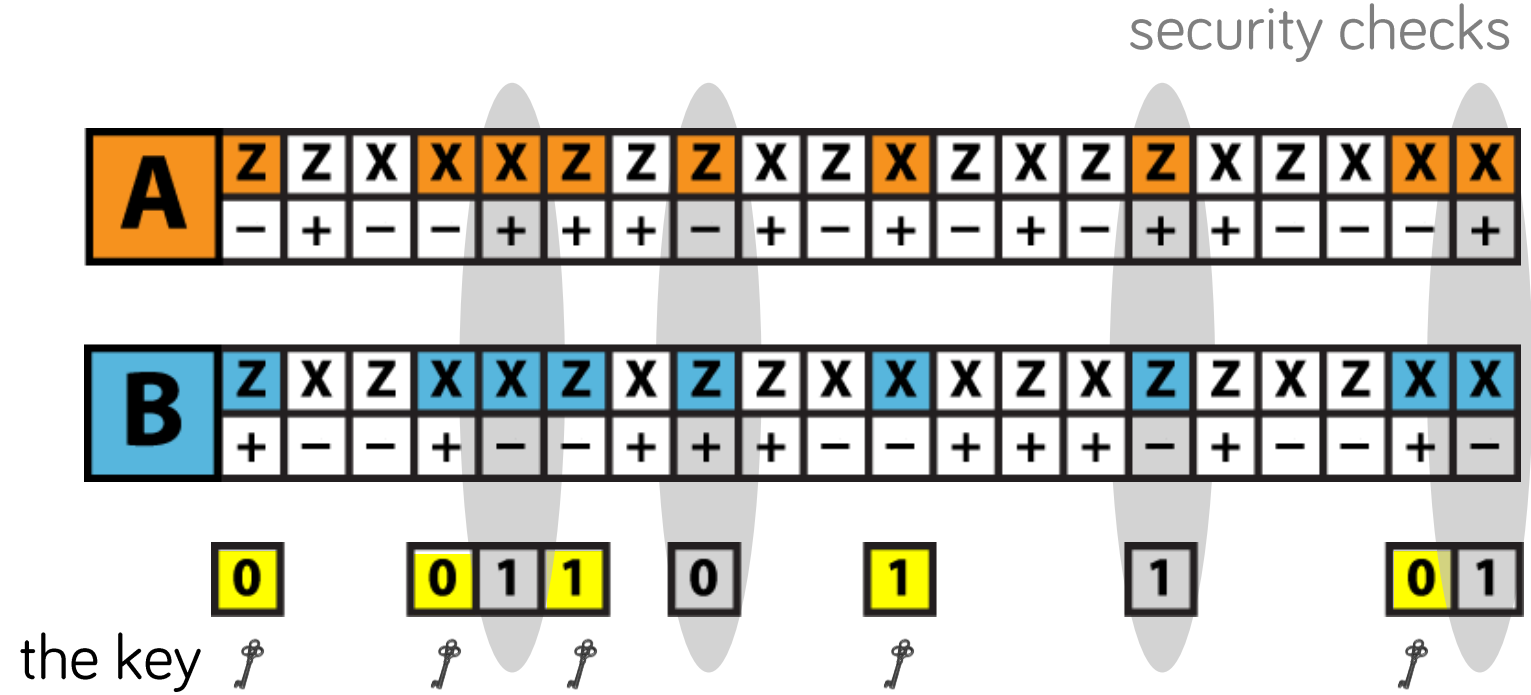
QKD

[Ekert91]



QKD

[Ekert91]


security checks
A
Z Z X X X Z Z Z X Z X Z X Z X Z X Z X X X
− + − − + + + − + − + − + − + + − − − +
B
Z X Z X X Z X Z Z X X X Z X Z Z X Z X X
+ − − + − − + + + − − + + + − + − − + −
0 0 1 1 0 1 1 0 1
the key
00110

QKD

[Ekert91]

5 Why is QKD safe? Bell (CHSH) inequality violation.

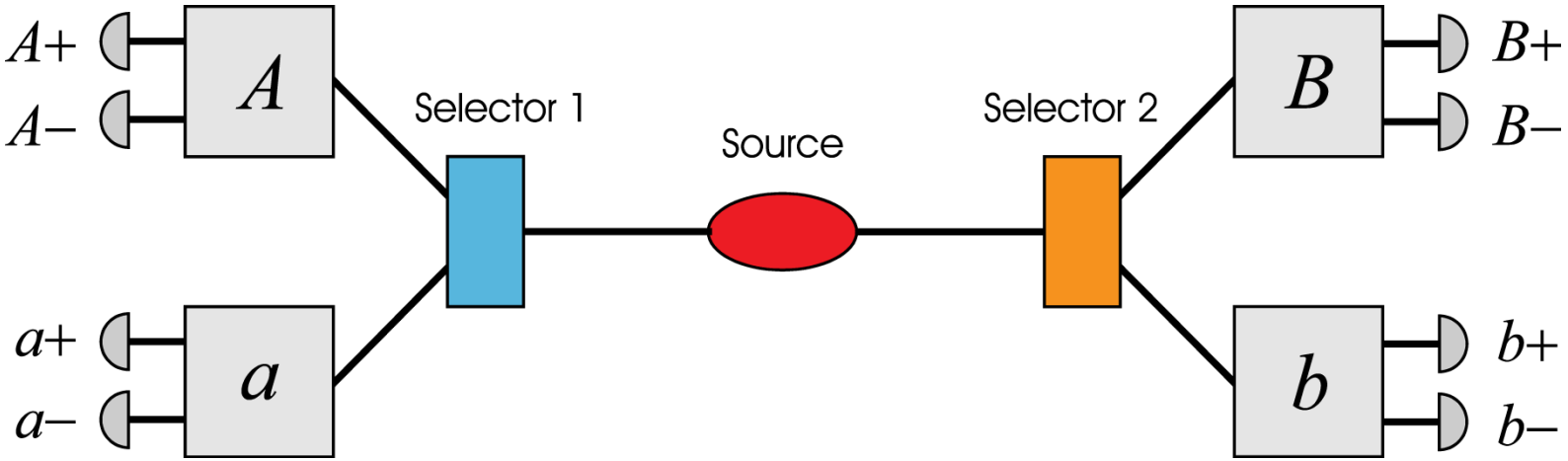
Nobody can classically prepare such correlations!

$$
\begin{aligned}
A, a, B, b & \quad \pm 1 \\
(B - b, B + b) & \quad (0, \pm 2), (\pm 2, 0) \\
A(B - b) + a(B + b) & \quad \pm 2 \\
|AB + aB + ab - Ab| & \quad \leq 2
\end{aligned}
$$

$$
|\langle AB \rangle + \langle aB \rangle + \langle ab \rangle - \langle Ab \rangle| \leq 2
$$

5 Why is QKD safe? Bell (CHSH) violation.

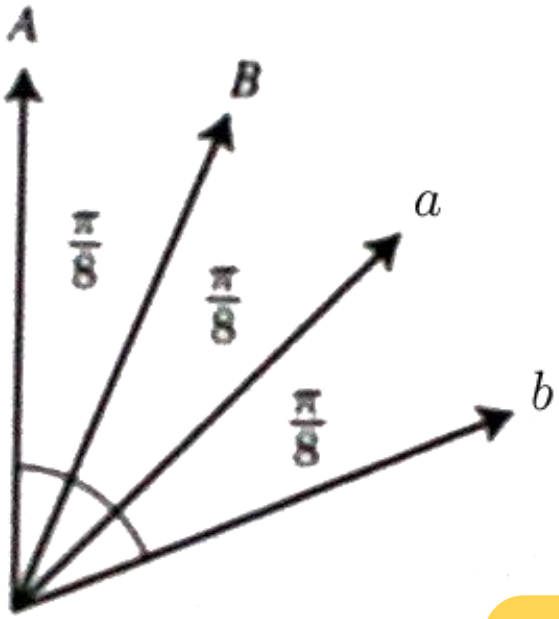
Nobody can classically prepare such correlations!

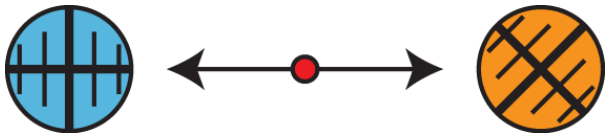


$$|\langle AB\rangle + \langle aB\rangle + \langle ab\rangle - \langle Ab\rangle| \leq 2$$

5 Why is QKD safe? Bell (CHSH) violation.

Nobody can classically prepare such correlations!





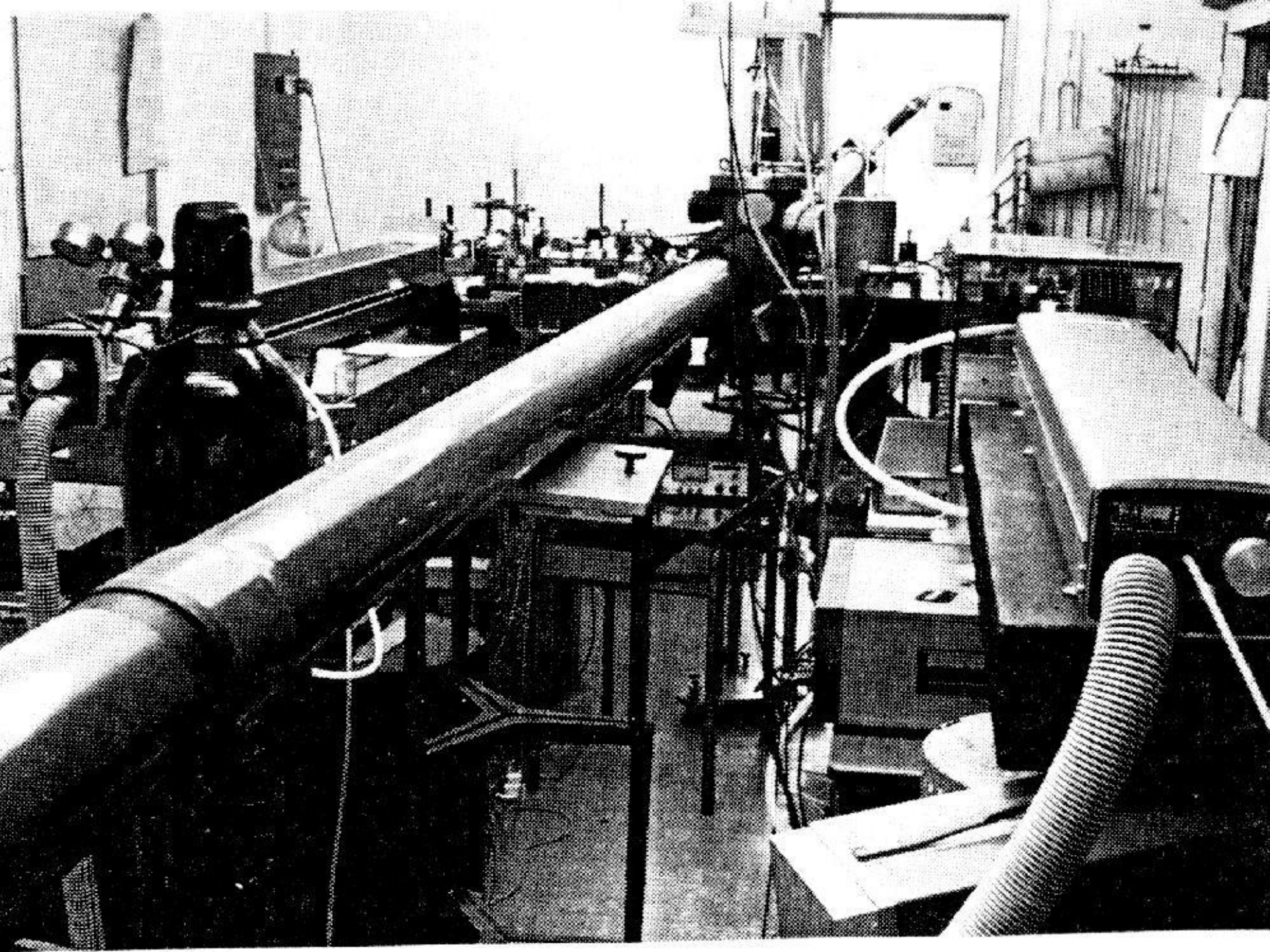
$$\langle AB \rangle = \cos 2\theta$$

$$\langle AB \rangle = \langle aB \rangle = \langle ab \rangle = \frac{1}{\sqrt{2}}$$

$$\langle Ab \rangle = -\frac{1}{\sqrt{2}}$$

$$2\sqrt{2} \approx 2.83 \not\leq 2$$

$$|\langle AB \rangle + \langle aB \rangle + \langle ab \rangle - \langle Ab \rangle| \leq 2$$



5 Bell test experiments from AA to AZ.

- Alain Aspect

VOLUME 47, NUMBER 7 PHYSICAL REVIEW LETTERS 17 AUGUST 1981

Experimental Tests of Realistic Local Theories via Bell's Theorem

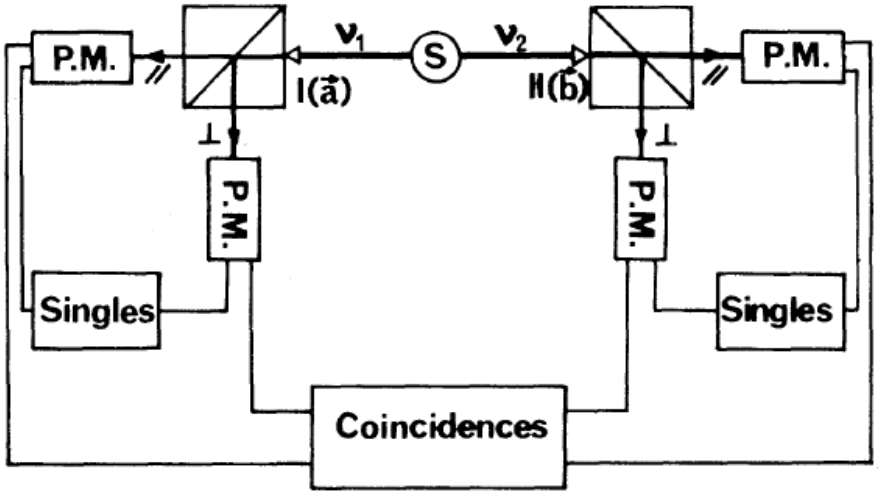
Alain Aspect, Philippe Grangier, and Gérard Roger
Institut d'Optique Théorique et Appliquée, Université Paris-Sud, F-91406 Orsay, France
(Received 30 March 1981)

VOLUME 49, NUMBER 2 PHYSICAL REVIEW LETTERS 12 JULY 1982

Experimental Realization of Einstein-Podolsky-Rosen-Bohm *Gedankenexperiment*: A New Violation of Bell's Inequalities

Alain Aspect, Philippe Grangier, and Gérard Roger
Institut d'Optique Théorique et Appliquée, Laboratoire associé au Centre National de la Recherche Scientifique, Université Paris-Sud, F-91406 Orsay, France
(Received 30 December 1981)

$$S_{\text{expt}} = 2.697 \pm 0.015$$



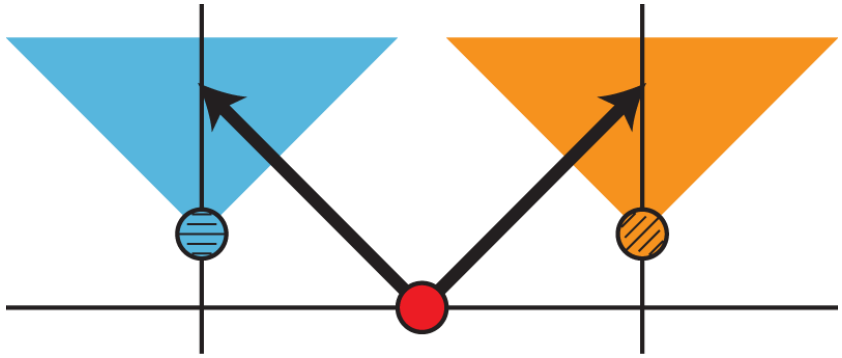
5 Bell test experiments: loopholes?

- detection loophole
  (missing clicks)

  http://www.micro-photon-devices.com/mpd.aspx
  50% @550nm, 30% @630nm

- communication (locality) loophole
  (do the photons “know” what we’ll ask?)

  relativistically local
  measurement choices?



5 Bell test experiments from AA to AZ.

- Alain Aspect

VOLUME 47, NUMBER 7 PHYSICAL REVIEW LETTERS 17 AUGUST 1981

Experimental Tests of Realistic Local Theories via Bell's Theorem

Alain Aspect, Philippe Grangier, and Gérard Roger
Institut d'Optique Théorique et Appliquée, Université Paris-Sud, F-91406 Orsay, France
(Received 30 March 1981)

VOLUME 49, NUMBER 2 PHYSICAL REVIEW LETTERS 12 JULY 1982

Experimental Realization of Einstein-Podolsky-Rosen-Bohm *Gedankenexperiment*: A New Violation of Bell's Inequalities

Alain Aspect, Philippe Grangier, and Gérard Roger
Institut d'Optique Théorique et Appliquée, Laboratoire associé au Centre National de la Recherche Scientifique, Université Paris-Sud, F-91406 Orsay, France
(Received 30 December 1981)

- Anton Zeilinger

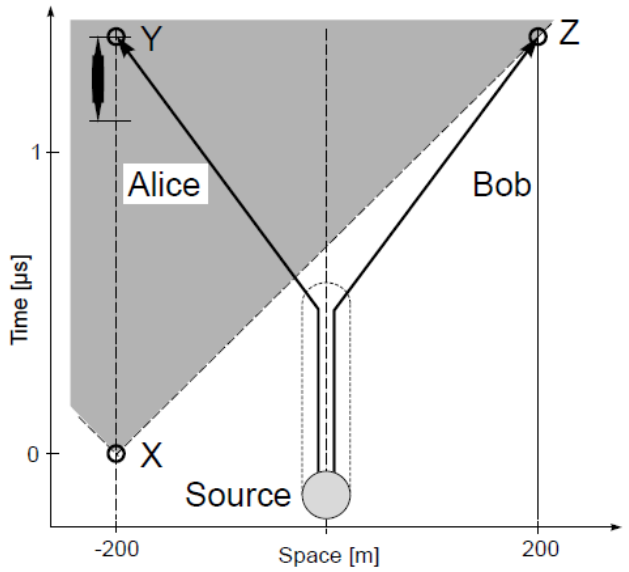
PHYSICAL REVIEW LETTERS

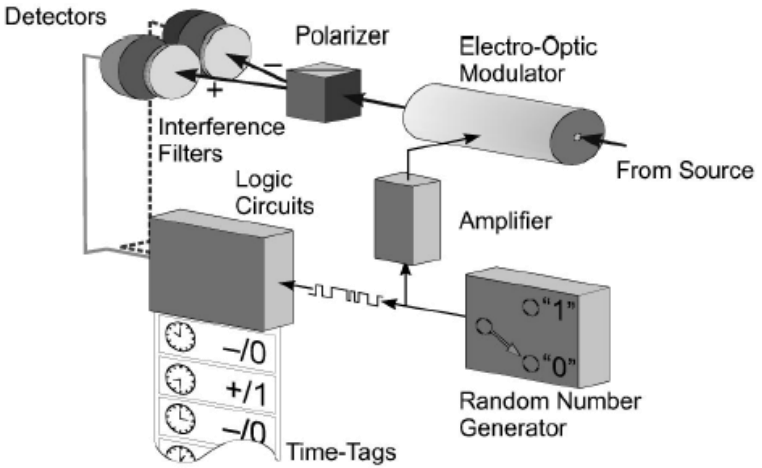
VOLUME 81 7 DECEMBER 1998 NUMBER 23

Violation of Bell's Inequality under Strict Einstein Locality Conditions

Gregor Weihs, Thomas Jennewein, Christoph Simon, Harald Weinfurter, and Anton Zeilinger
Institut für Experimentalphysik, Universität Innsbruck, Technikerstraße 25, A-6020 Innsbruck, Austria
(Received 6 August 1998)

5 Bell test experiments from AA to AZ.





- Anton Zeilinger

PHYSICAL REVIEW
LETTERS

VOLUME 81 | 7 DECEMBER 1998 | NUMBER 23

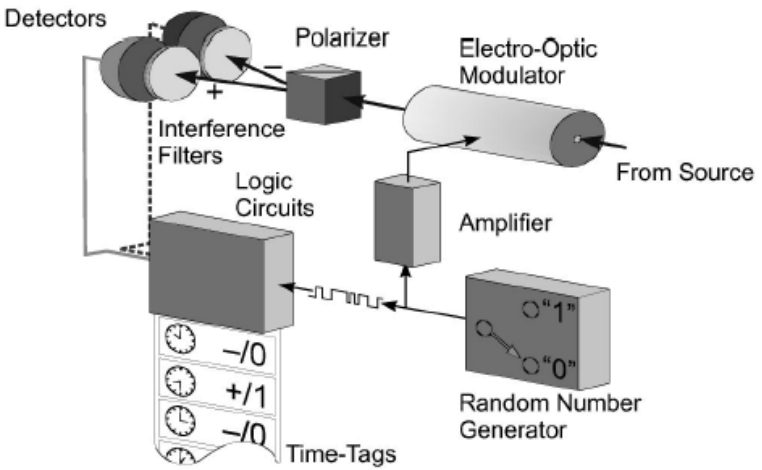
Violation of Bell's Inequality under Strict Einstein Locality Conditions

Gregor Weihs, Thomas Jennewein, Christoph Simon, Harald Weinfurter, and Anton Zeilinger
Institut für Experimentalphysik, Universität Innsbruck, Technikerstraße 25, A-6020 Innsbruck, Austria
(Received 6 August 1998)

5 Bell test experiments from AA to AZ.

$$S = 2.73 \pm 0.02$$

for 14 700 coincidence events collected in 10 s



- Anton Zeilinger

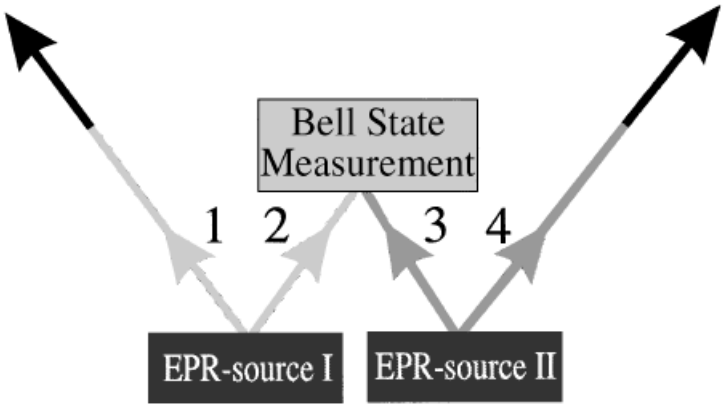
PHYSICAL REVIEW LETTERS

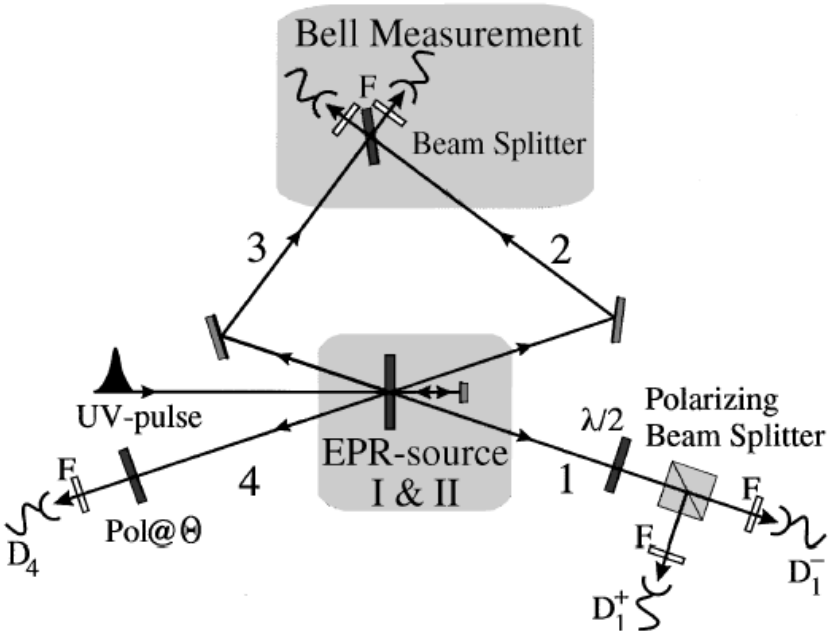
VOLUME 81 | 7 DECEMBER 1998 | NUMBER 23

Violation of Bell's Inequality under Strict Einstein Locality Conditions

Gregor Weihs, Thomas Jennewein, Christoph Simon, Harald Weinfurter, and Anton Zeilinger
Institut für Experimentalphysik, Universität Innsbruck, Technikerstraße 25, A-6020 Innsbruck, Austria
(Received 6 August 1998)

5 Bell test experiments from AA to AZ.





- Anton Zeilinger

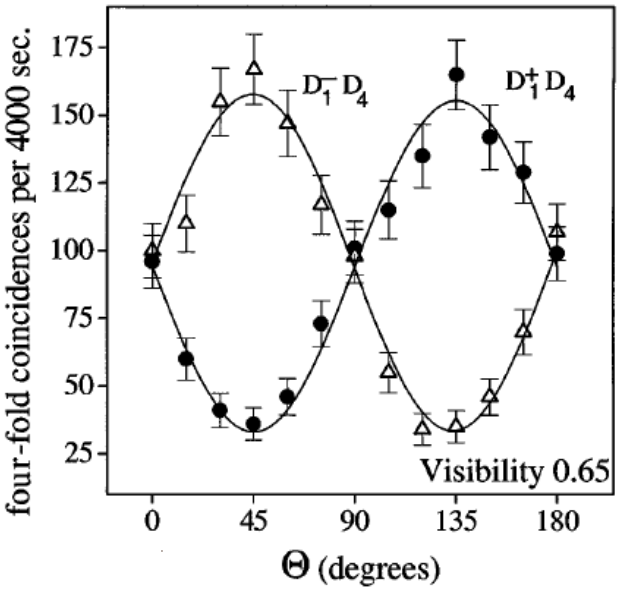
PHYSICAL REVIEW
LETTERS

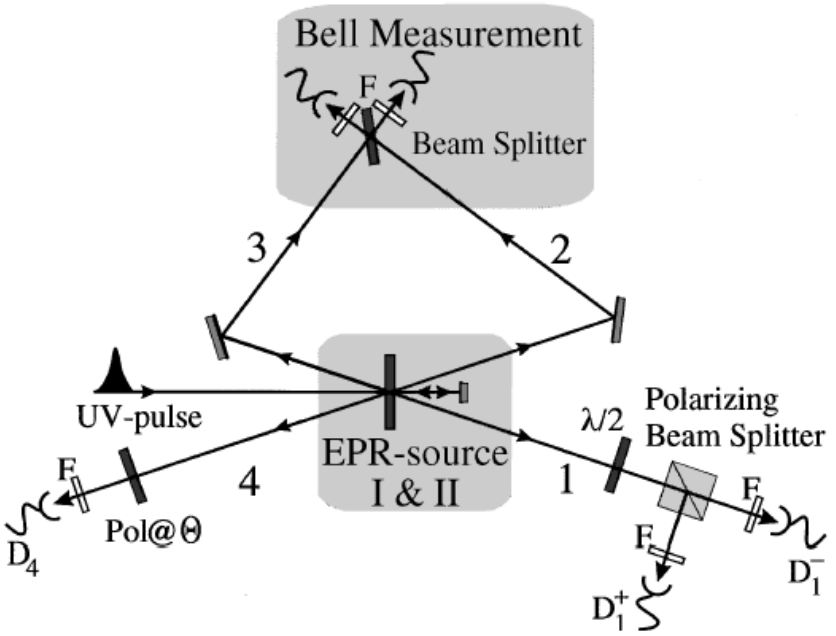
VOLUME 81 | 7 DECEMBER 1998 | NUMBER 23

Violation of Bell's Inequality under Strict Einstein Locality Conditions

Gregor Weihs, Thomas Jennewein, Christoph Simon, Harald Weinfurter, and Anton Zeilinger
Institut für Experimentalphysik, Universität Innsbruck, Technikerstraße 25, A-6020 Innsbruck, Austria
(Received 6 August 1998)

5 Bell test experiments from AA to AZ.





- Anton Zeilinger

PHYSICAL REVIEW
LETTERS

VOLUME 81 | 7 DECEMBER 1998 | NUMBER 23

Violation of Bell's Inequality under Strict Einstein Locality Conditions

Gregor Weihs, Thomas Jennewein, Christoph Simon, Harald Weinfurter, and Anton Zeilinger
Institut für Experimentalphysik, Universität Innsbruck, Technikerstraße 25, A-6020 Innsbruck, Austria
(Received 6 August 1998)

5 Bell test experiments from AA to AZ.

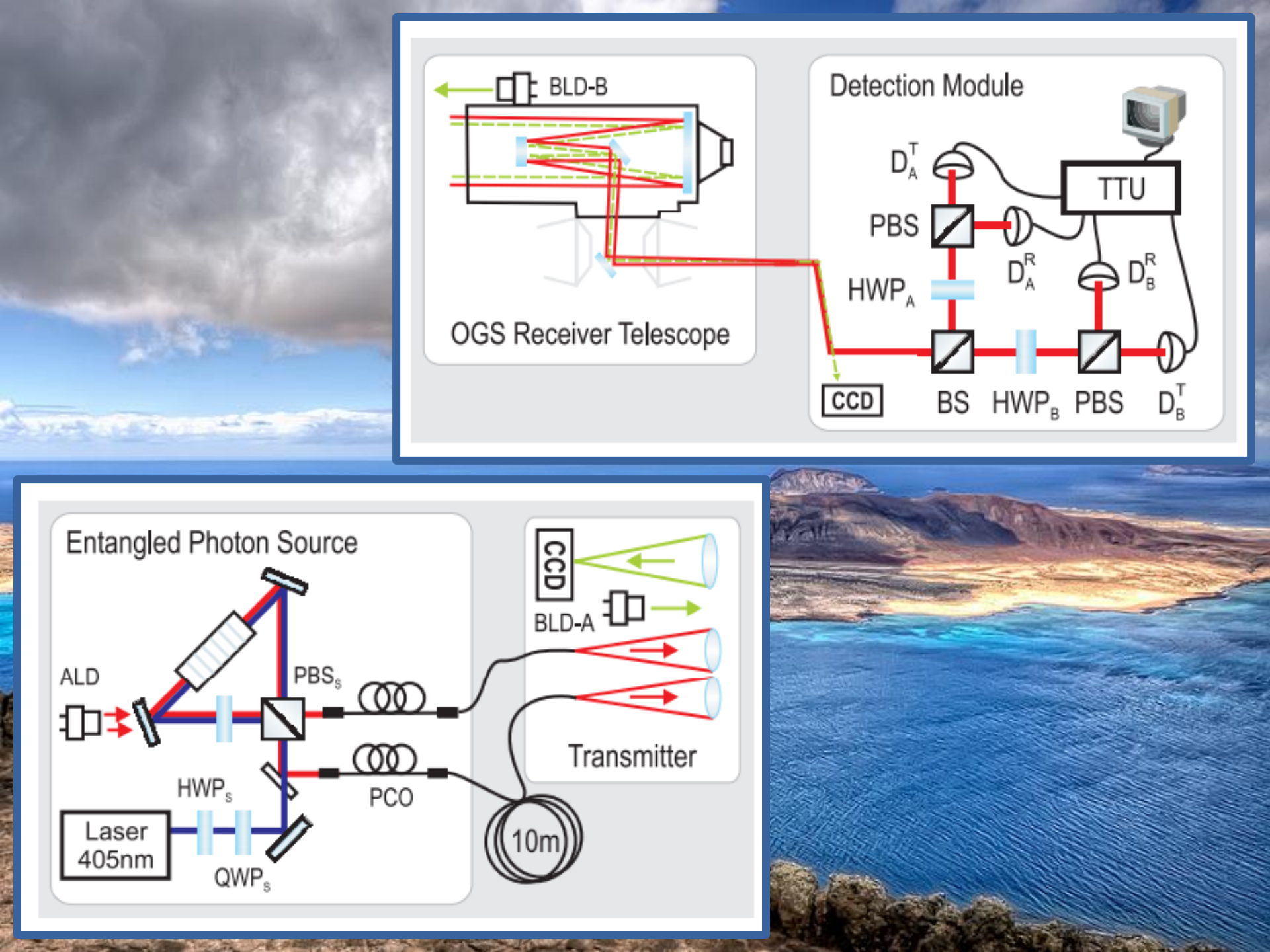
- Anton Zeilinger

Nature Physics **5**, 389 - 392 (2009)
Published online: 3 May 2009 | doi:10.1038/nphys1255

Subject Categories: Quantum physics | Techniques and instrumentation | Information theory and computation

High-fidelity transmission of entanglement over a high-loss free-space channel

Alessandro Fedrizzi[1], Rupert Ursin[1], Thomas Herbst[1], Matteo Nespoli[1], Robert Prevedel[1,2], Thomas Scheidl[1], Felix Tiefenbacher[1], Thomas Jennewein[1] & Anton Zeilinger[1,2]


BLD-B
OGS Receiver Telescope
Detection Module
D_A^T
TTU
PBS
D_A^R
D_B^R
HWP_A
CCD
BS
HWP_B
PBS
D_B^T
Entangled Photon Source
ALD
PBS_S
HWP_S
PCO
Laser 405nm
QWP_S
10m
CCD
BLD-A
Transmitter

search

SWISS QUANTUM

PROJECT | NETWORK | PERFORMANCE | PARTNERS | STAY INFORMED | CONTACT

NEWS

SwissQuantum Project Completes Longest-Running Testbed of Quantum Crytography
Geneva, Switzerland - ID Quantique SA announced the successful completion (...)

read more

SwissQuantum network dismantled
The SwissQuantum network has been dismantled after almost two years of (...)

read more

Quantum encryption to secure World Cup link
In the first use of ultra secure quantum encryption at a world public (...)

read more

IDQ and UNIGE go one step further with the European research project QuRep
The SwissQuantum network highlights the reliability of Quantum Key (...)

SWISS QUANTUM

In January 2011 Swissquantum successfully completed the longest running project for testing Quantum Key Distribution (QKD) in a field environment. The main goal of the SwissQuantum network, installed in the Geneva metropolitan area in March 2009, was to validate the reliability and robustness of QKD in continuous operation in a network over a long time period in a field environment. The quantum layer ran stably for nearly 2 years, confirming the viability of QKD as a commercial encryption technology in telecommunication networks.

The network consisted of three nodes located in the Geneva metropolitan area.

This network served as a platform for:
- Research & Development
- Demonstration and
- Education

in the field of quantum communications.

This website presents the project, the technology used as well as the results of the extensive test campaign.

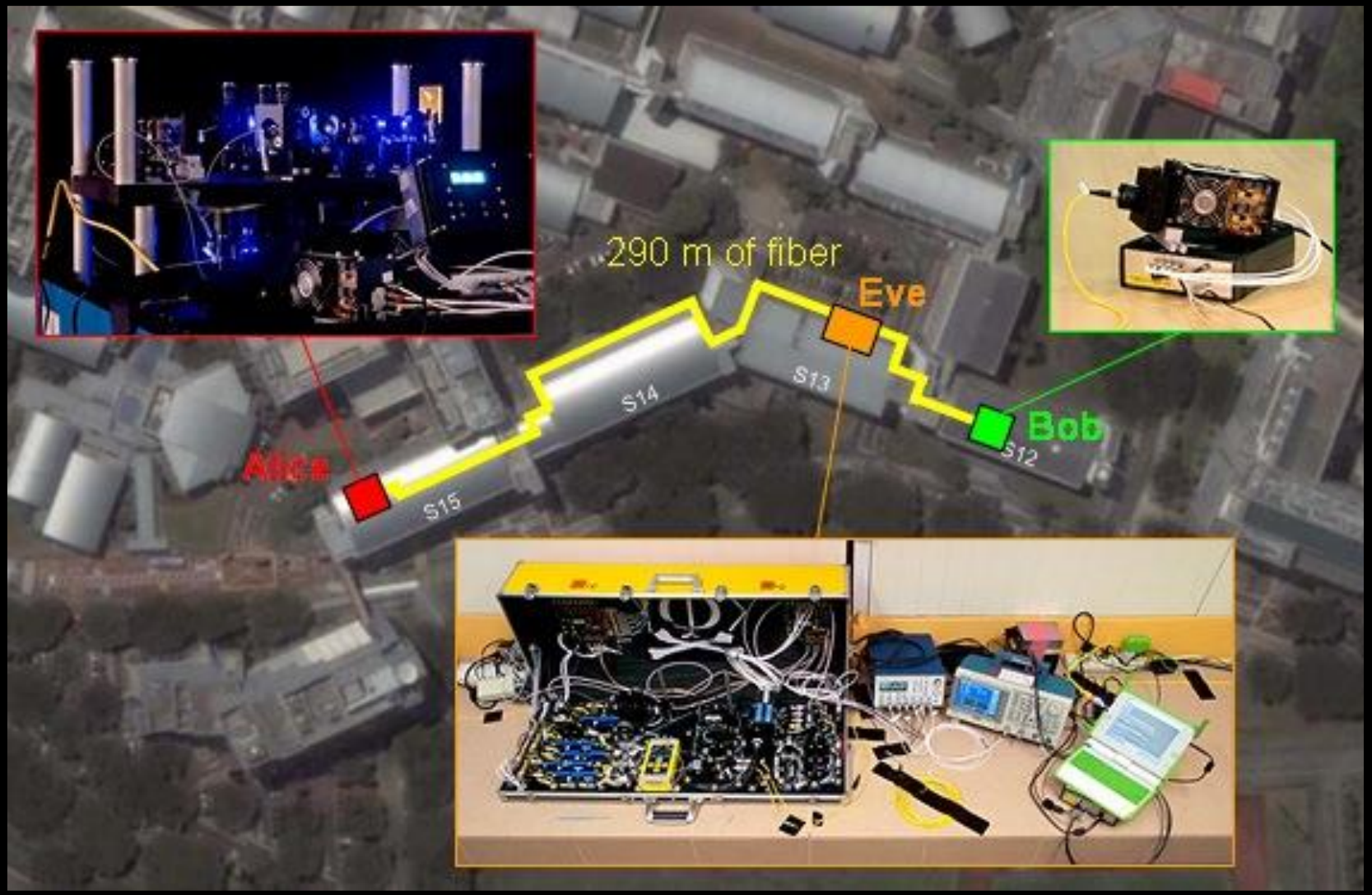
NATURE PHOTONICS | LETTER

Hacking commercial quantum cryptography systems by tailored bright illumination

Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, Dominique Elser, Johannes Skaar & Vadim Makarov

Nature Photonics **4**, 686–689 (2010)

5 Hacking commercial QKD



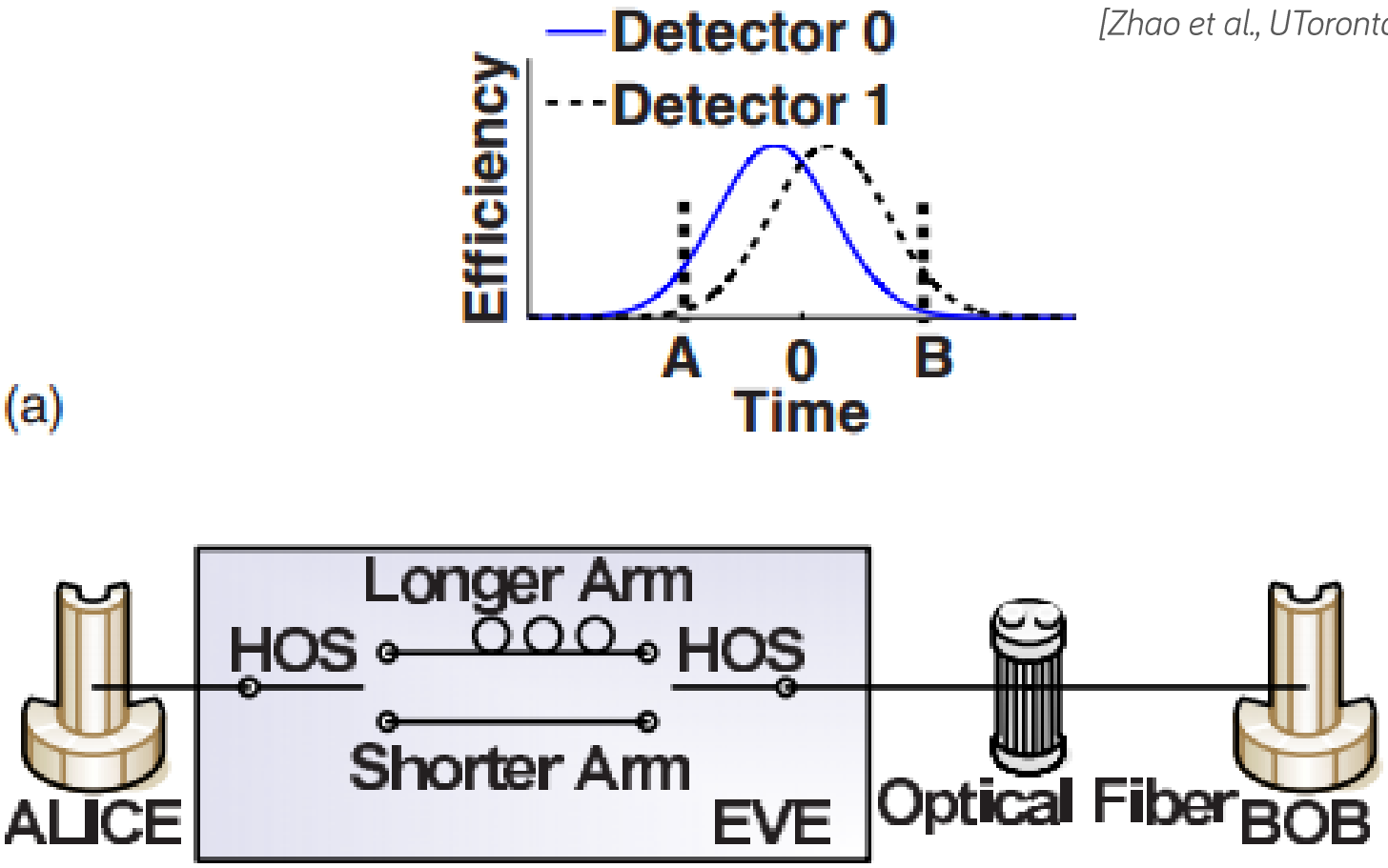
[Gerhadt et al., NUS]

5 Hacking commercial QKD

Measure, resend, blind B's detector & make it see what you want.

[Gerhadt et al., NUS]

5 Hacking QKD in practice



[Zhao et al., UToronto]

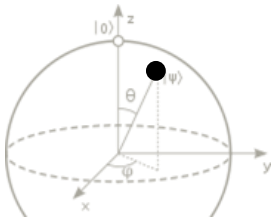
Use imperfections: measure, shift in time, pretend to be a “noise”.

superdense coding
q. teleportation
secure QKD

[QIP 2012, UMontréal]

1 **we need a qubit**

well, what can we do with it?

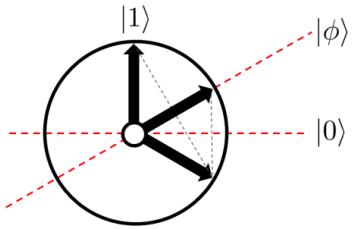


2 **EPR pairs**

and tricky 2-qubit protocols

3 **the algorithms**

that make quantum computing tick



4 **error correction**

can we really scale up this stuff?

5 **the limits**

complexity & limits of q. computing