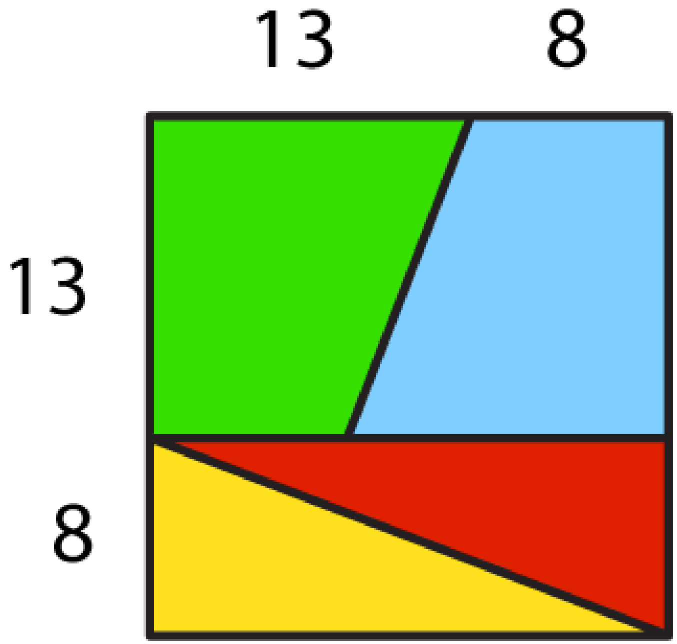
Introduction to **Quantum Computation**

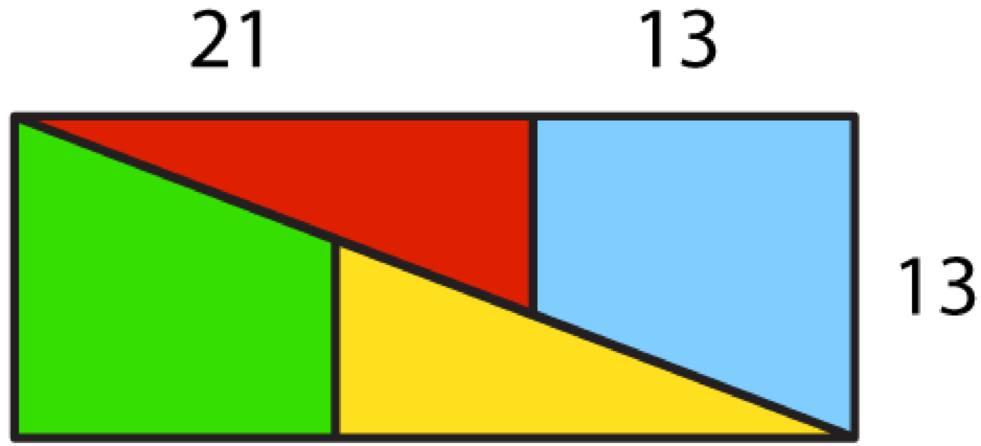
ICTP-VAST-APCTP winter school
Hanoi, 12/2013

Daniel Nagaj

universität wien

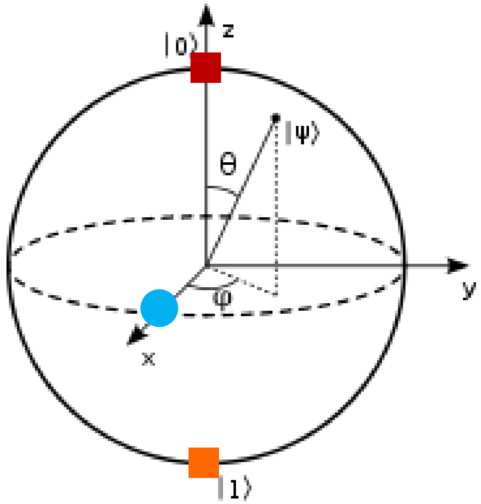


$21 \times 21 = \mathbf{441}$



$34 \times 13 = \mathbf{442}$

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

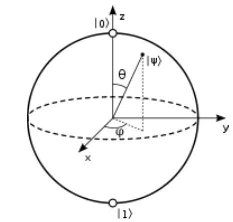
$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

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

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

1 we need a qubit

and we can use it

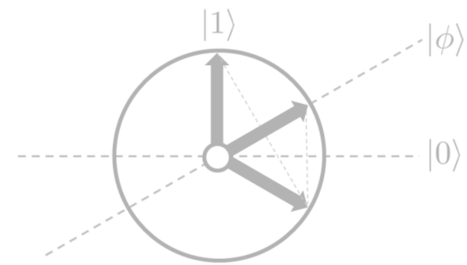


2 EPR pairs

give us cool 2-qubit protocols

3 the algorithms

that make quantum computing tick



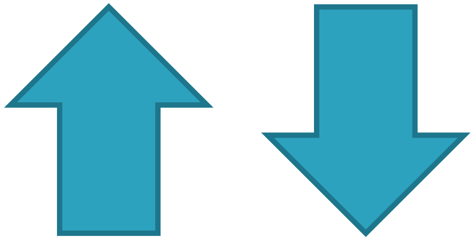
4 error correction

can we really scale up this stuff?

strange action at a distance

1 Two qubits: the basi(c)s

- how many dimensions do we need?



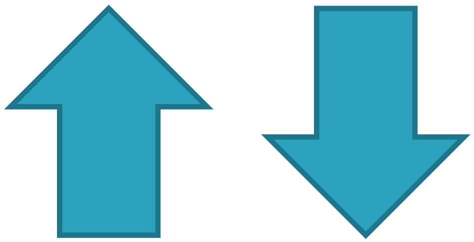
- how do 1-qubit operations look now?

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

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

1 Two qubits: the basi(c)s

- how many dimensions do we need?

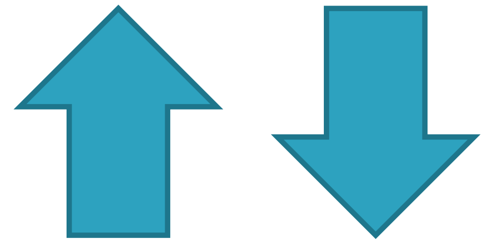


- how do 1-qubit operations look now?
- more tensor product operations?

$$X \otimes X$$

$$Z \otimes Z$$

1 Two qubits: the basi(c)s



- how many dimensions do we need?
- how do 1-qubit operations look now?
- some basic 2-qubit operations?
  (action in the computational basis + linearity)

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

- what kind of interaction is needed?

1 The Bell states

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

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

- 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.

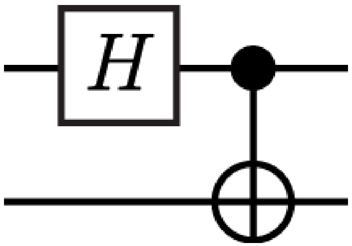
Charlie Bennett

1 The Bell states

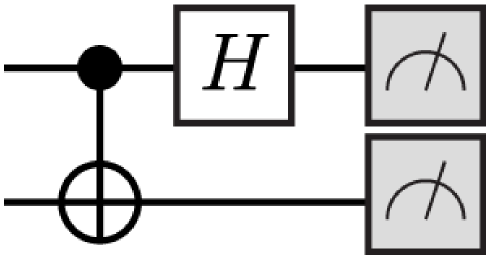
$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|0\rangle \pm |1\rangle|1\rangle\right)$$

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

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



- distinguishing them?



- transforming between the Bell states?

2 Super-dense coding

- transforming between the Bell states?

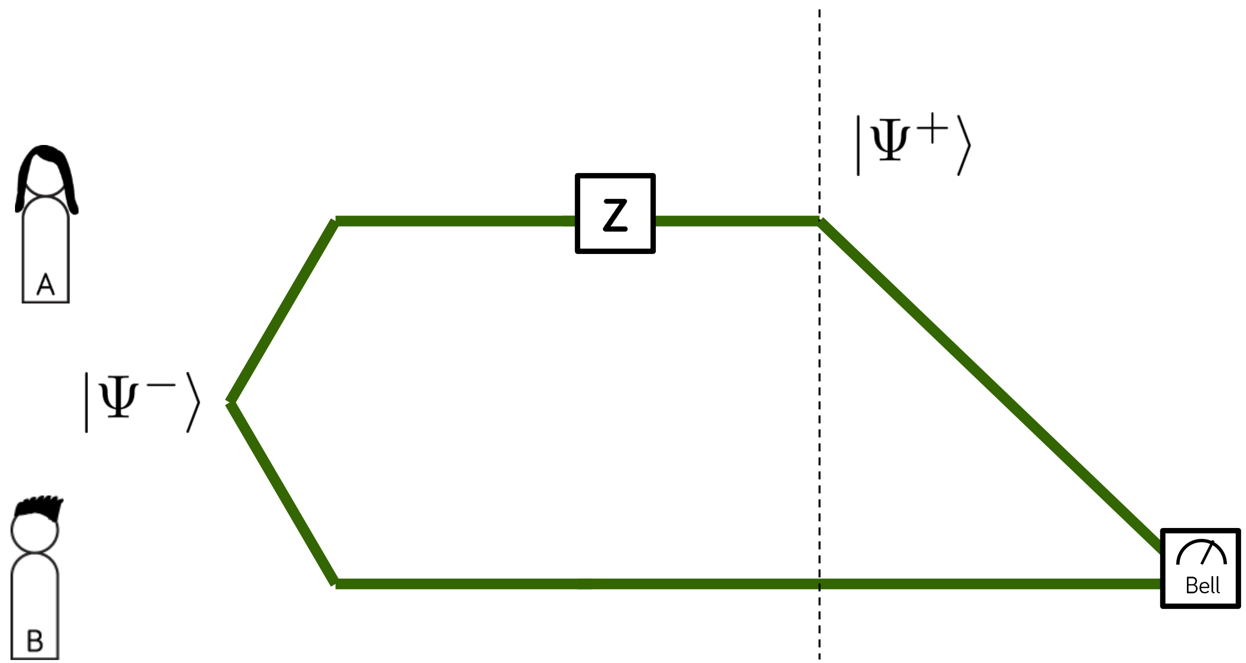
$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle)$$

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

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

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

- what is a shared EPR pair good for?



2 Super-dense coding

- transforming between the Bell states?

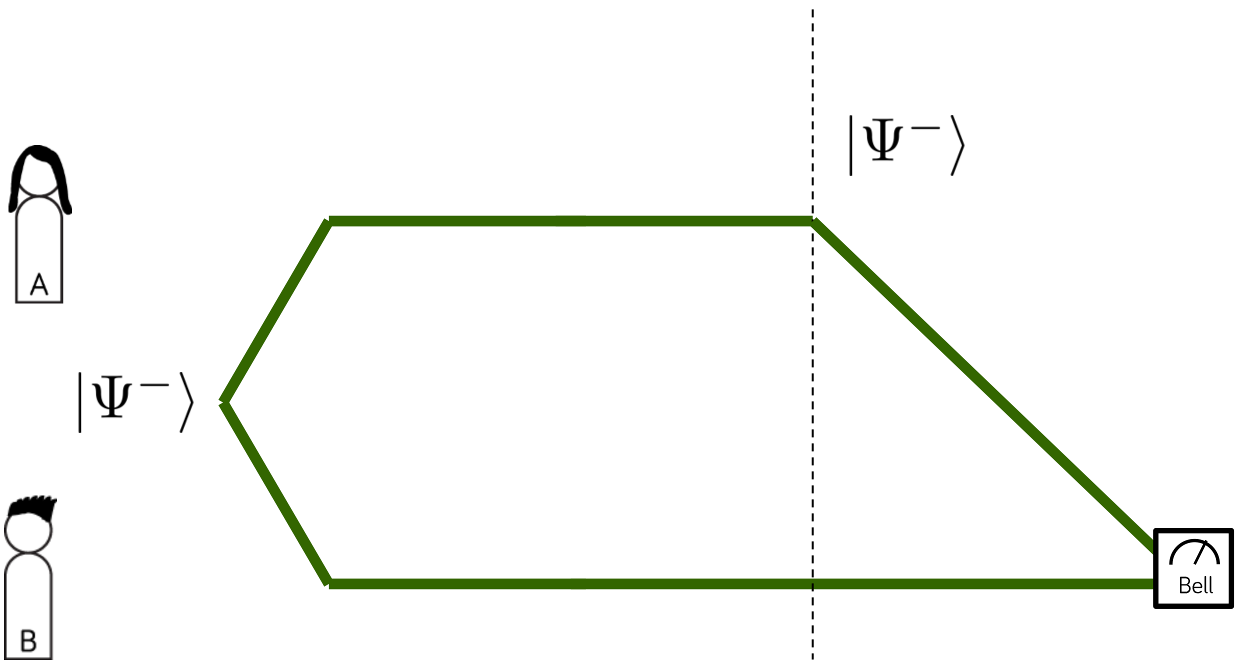
$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle)$$

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

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

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

- what is a shared EPR pair good for?



2 Super-dense coding

- transforming between the Bell states?

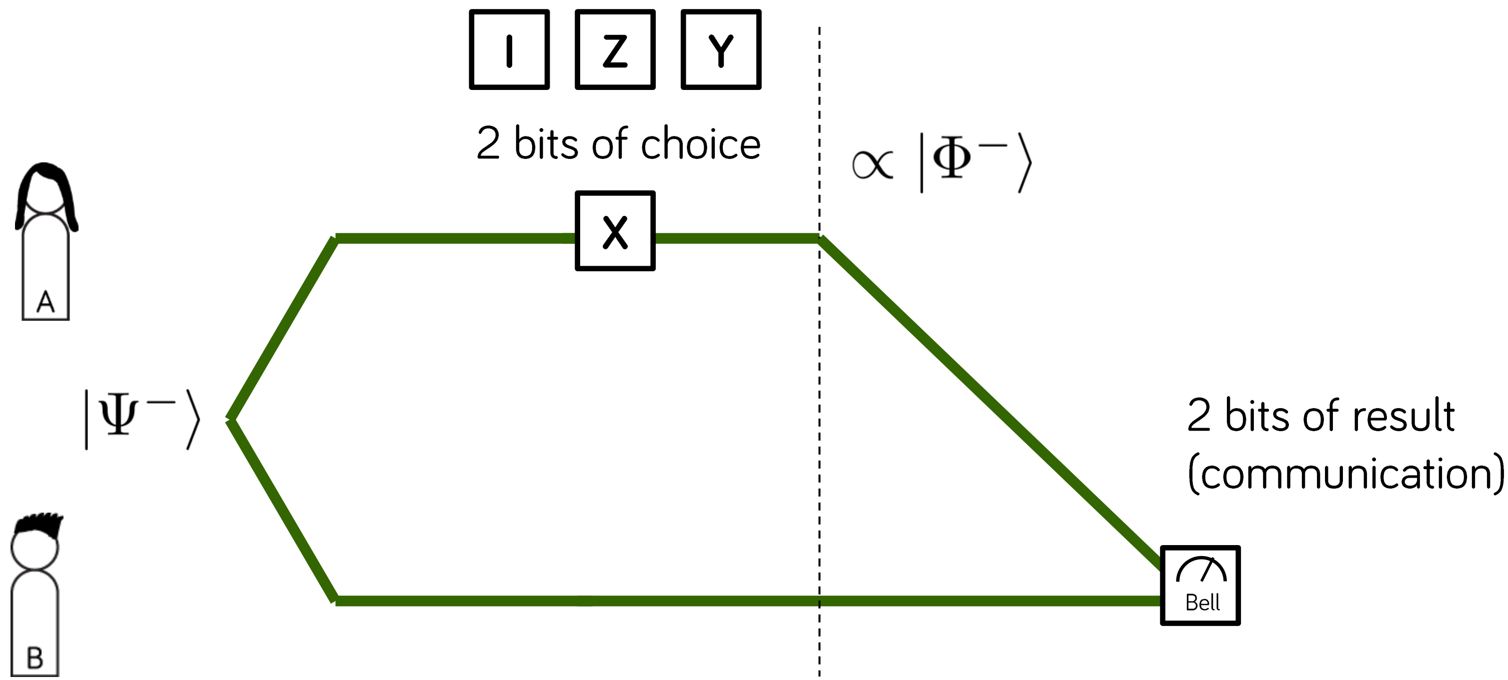
$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle)$$

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

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

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

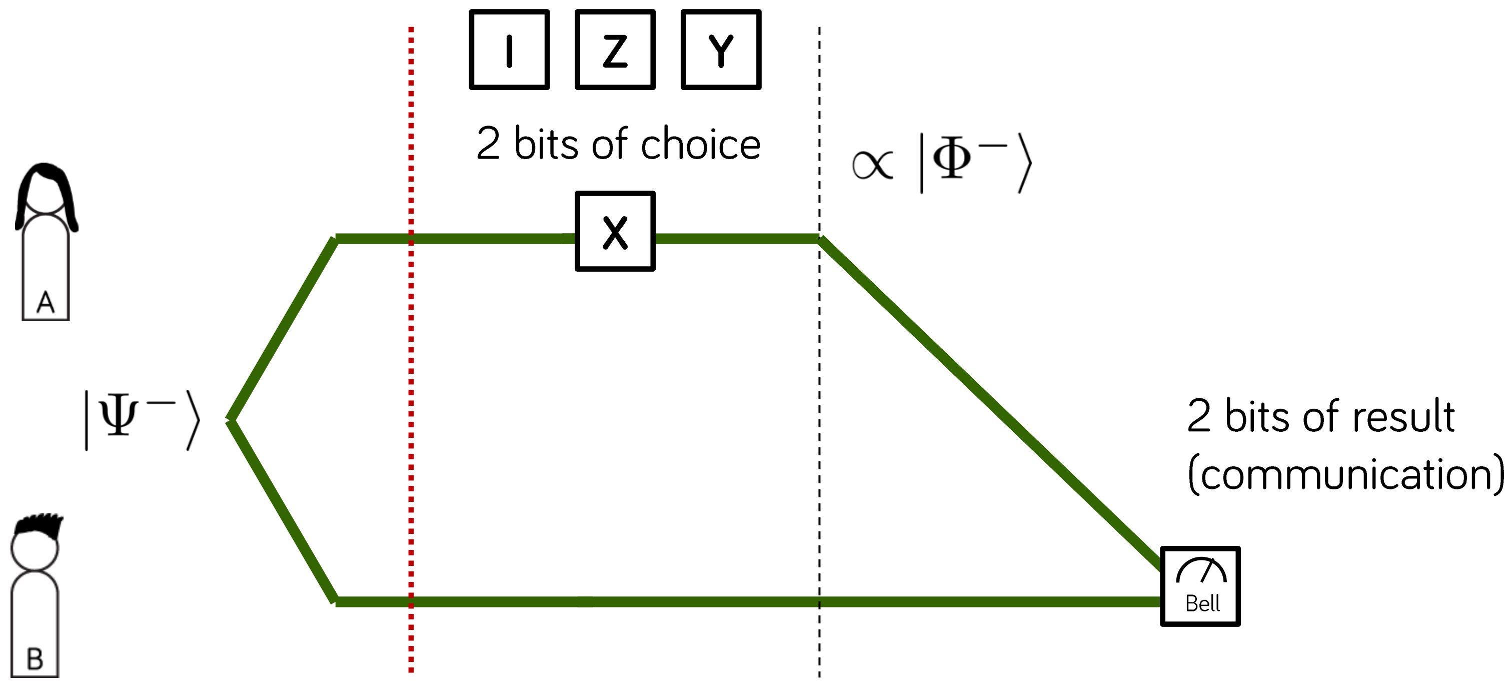
- what is a shared EPR pair good for?



2 Super-dense coding

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

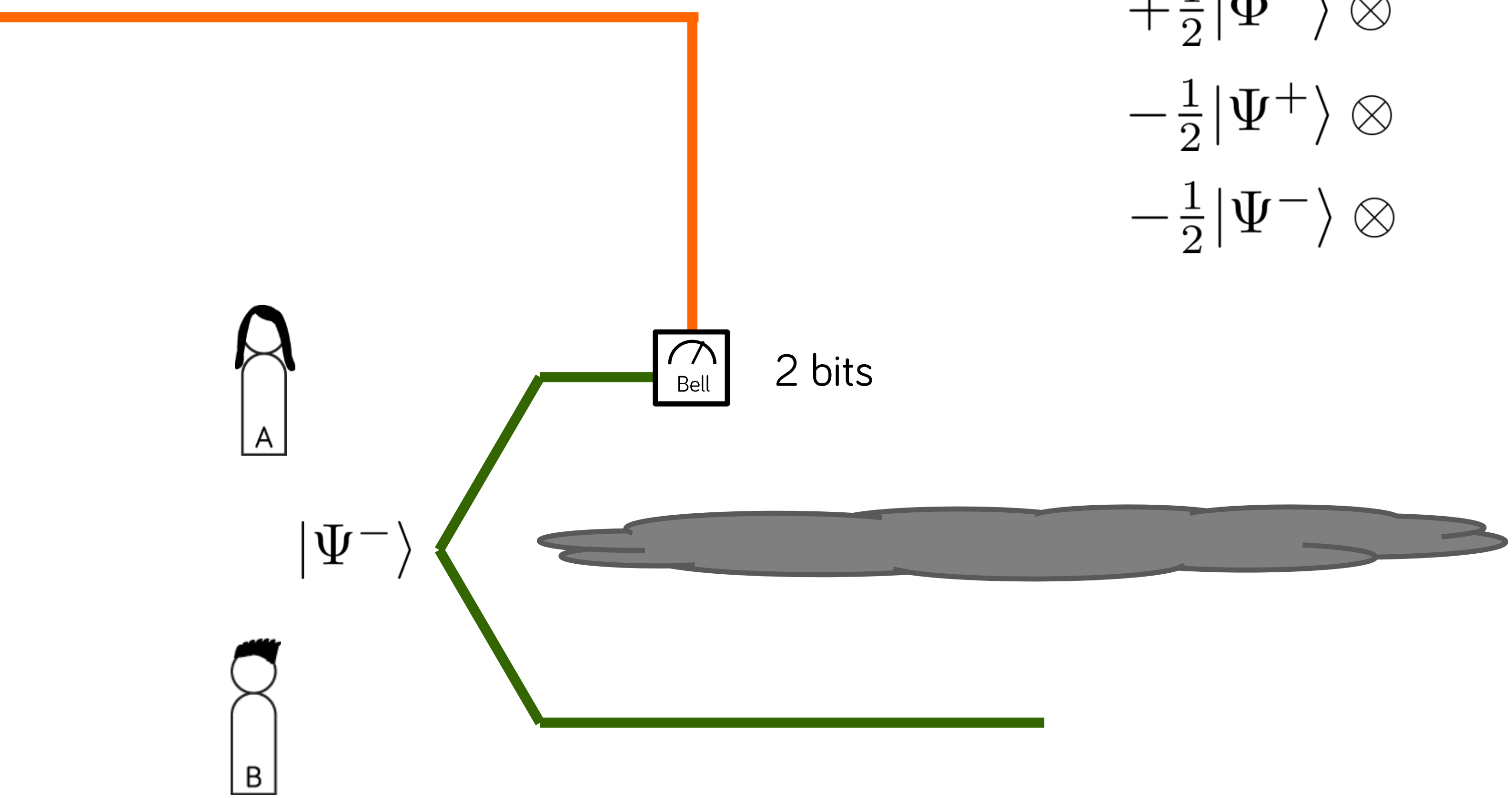
- what is a shared EPR pair good for?



3 Quantum teleportation

- sending quantum states when quantum channels no longer work

$$(a|0\rangle + b|1\rangle)$$



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

$$= \frac{1}{2}|\Phi^+\rangle \otimes$$

$$+\frac{1}{2}|\Phi^-\rangle \otimes$$

$$-\frac{1}{2}|\Psi^+\rangle \otimes$$

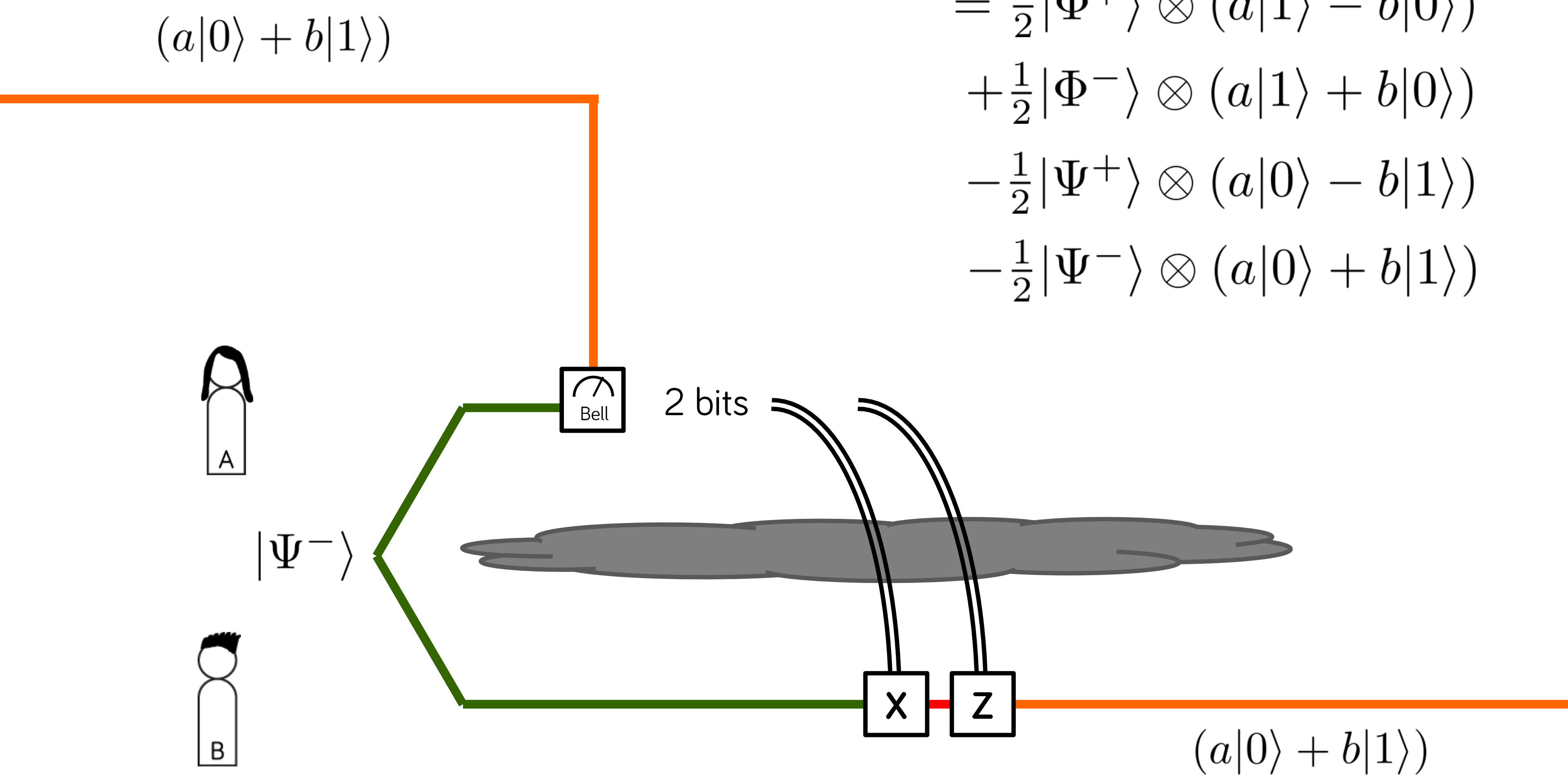
$$-\frac{1}{2}|\Psi^-\rangle \otimes$$

3 Quantum teleportation

- sending quantum states when quantum channels no longer work

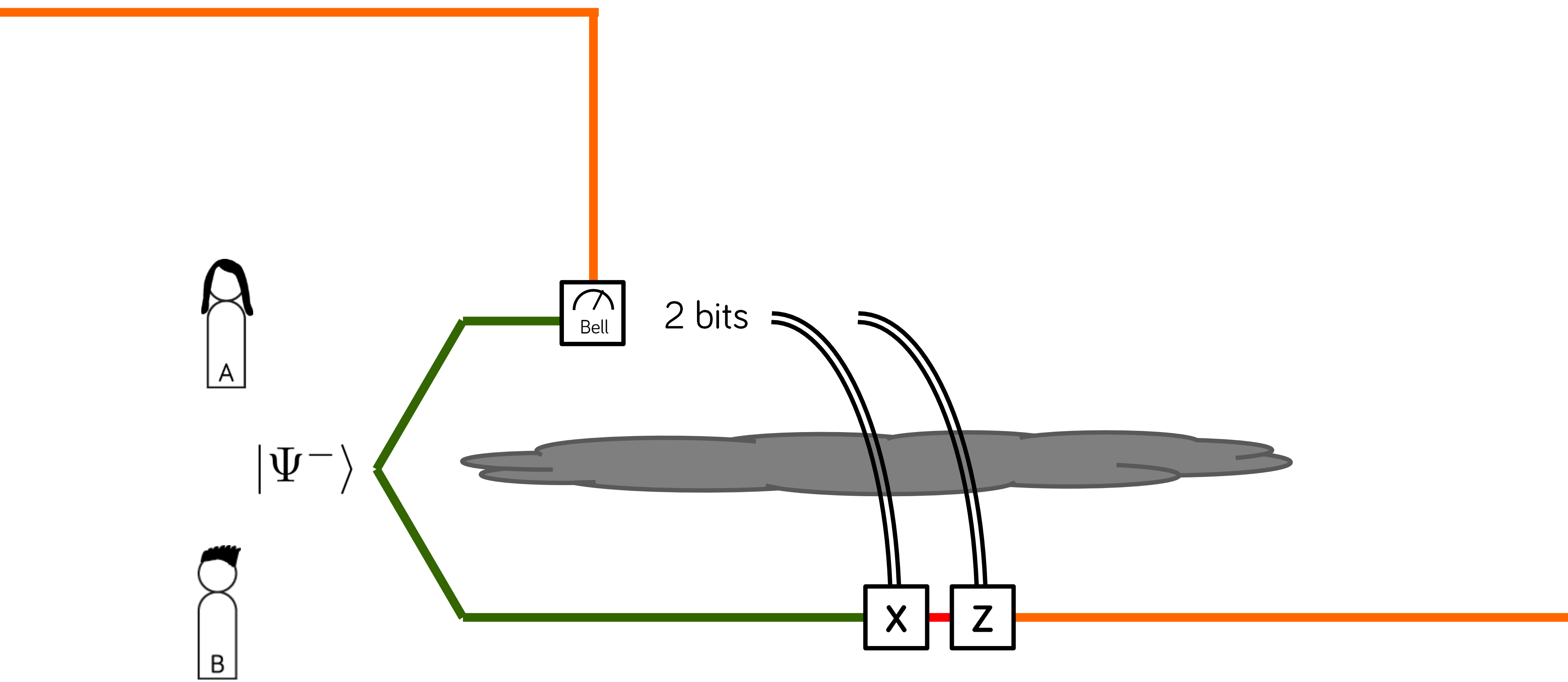
$$(a|0\rangle + b|1\rangle) \otimes |\Psi^-\rangle$$

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



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

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

plaintext → ciphertext, key

5 Unconditional security: one-time pad

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

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

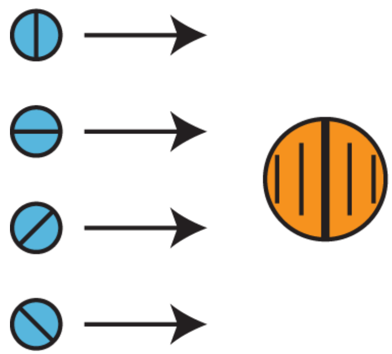
The BB84 protocol (no entanglement).

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

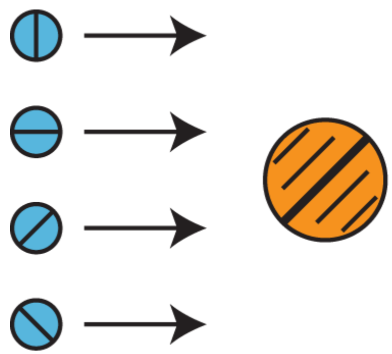
prepare a photon

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

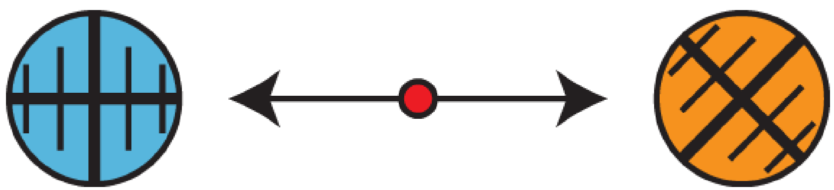
send 1 photon to B

choose a basis & measure

Bob

choose a basis

measure the photon



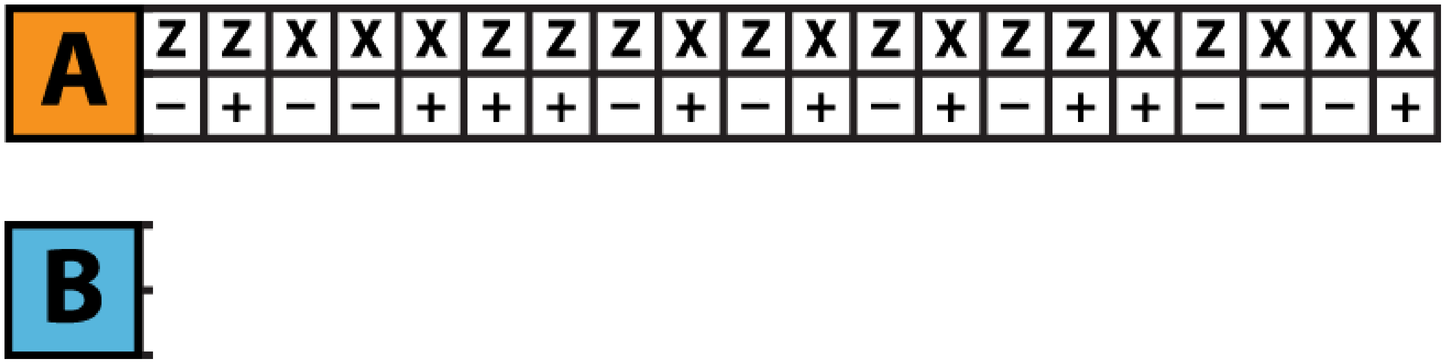
compare the basis choices (publicly)

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

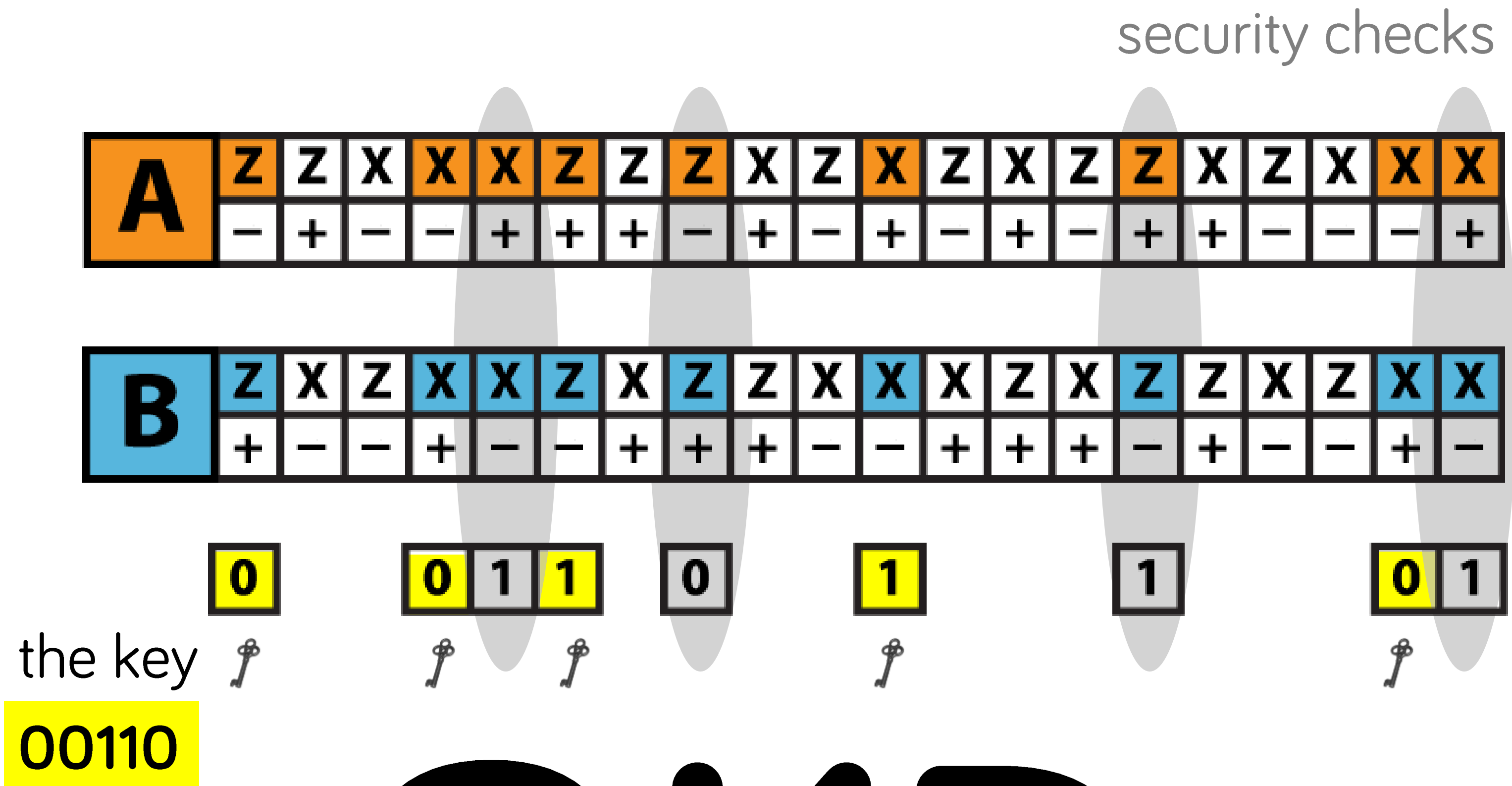
[Ekert91]

A	Z	Z	X	X	X	Z	Z	Z	X	Z	X	Z	X	Z	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
	+	−	−	+	−	−	+	+	+	−	−	+	+	+	−	+	−	−	+	−

QKD

[Ekert91]


security checks
A
Z Z X X X Z Z Z X Z X Z X Z 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]

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.

5 QKD in practice today

NATURE PHOTONICS | LETTER

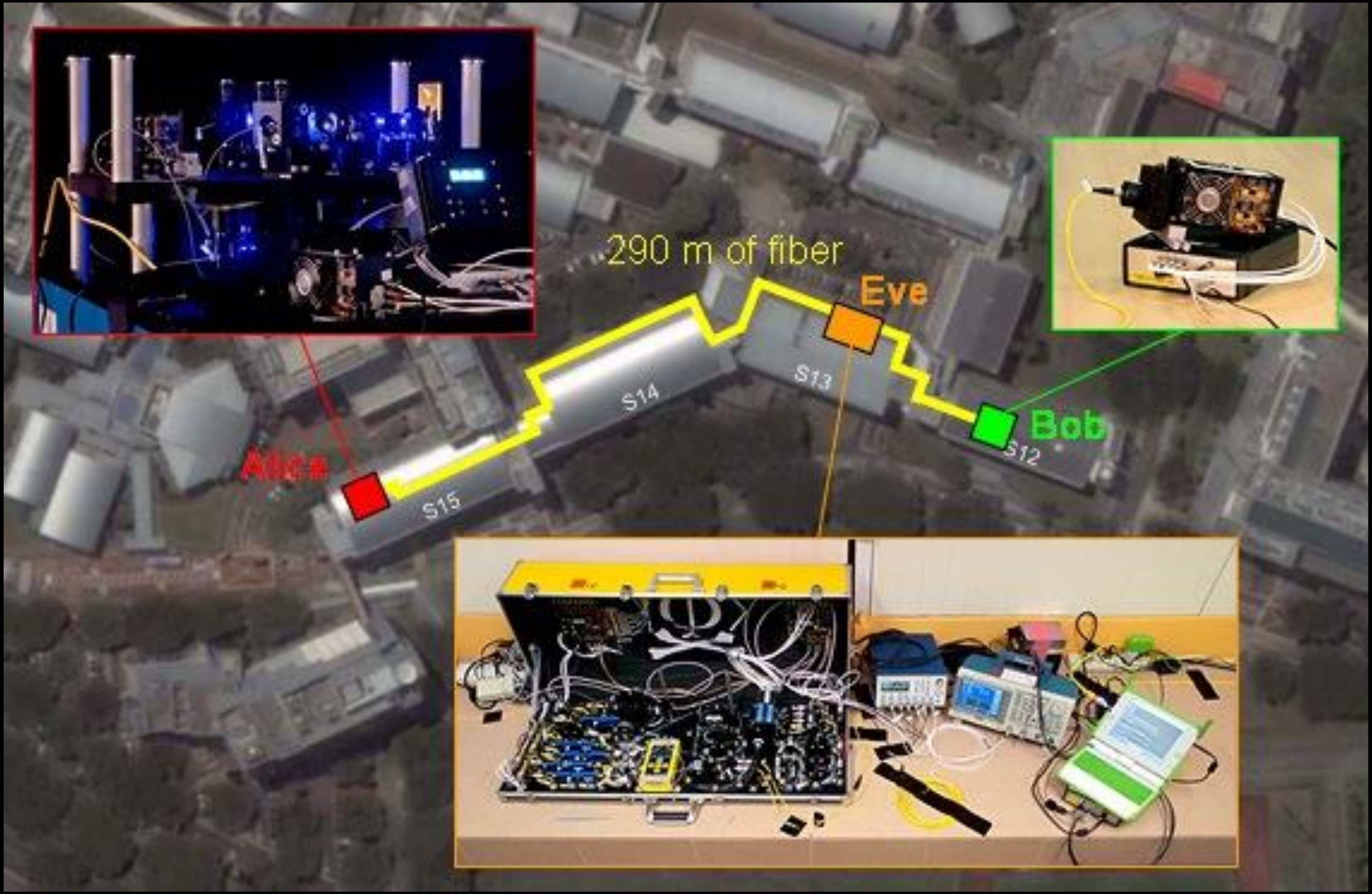
Hacking commercial quantum cryptography systems by tailored bright illumination

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

Affiliations | Contributions | Corresponding author

Nature Photonics **4**, 686–689 (2010) | doi:10.1038/nphoton.2010.214
Received 02 April 2010 | Accepted 11 July 2010 | Published online 29 August 2010

5 QKD in practice



[Gerhadt et al., NUS]

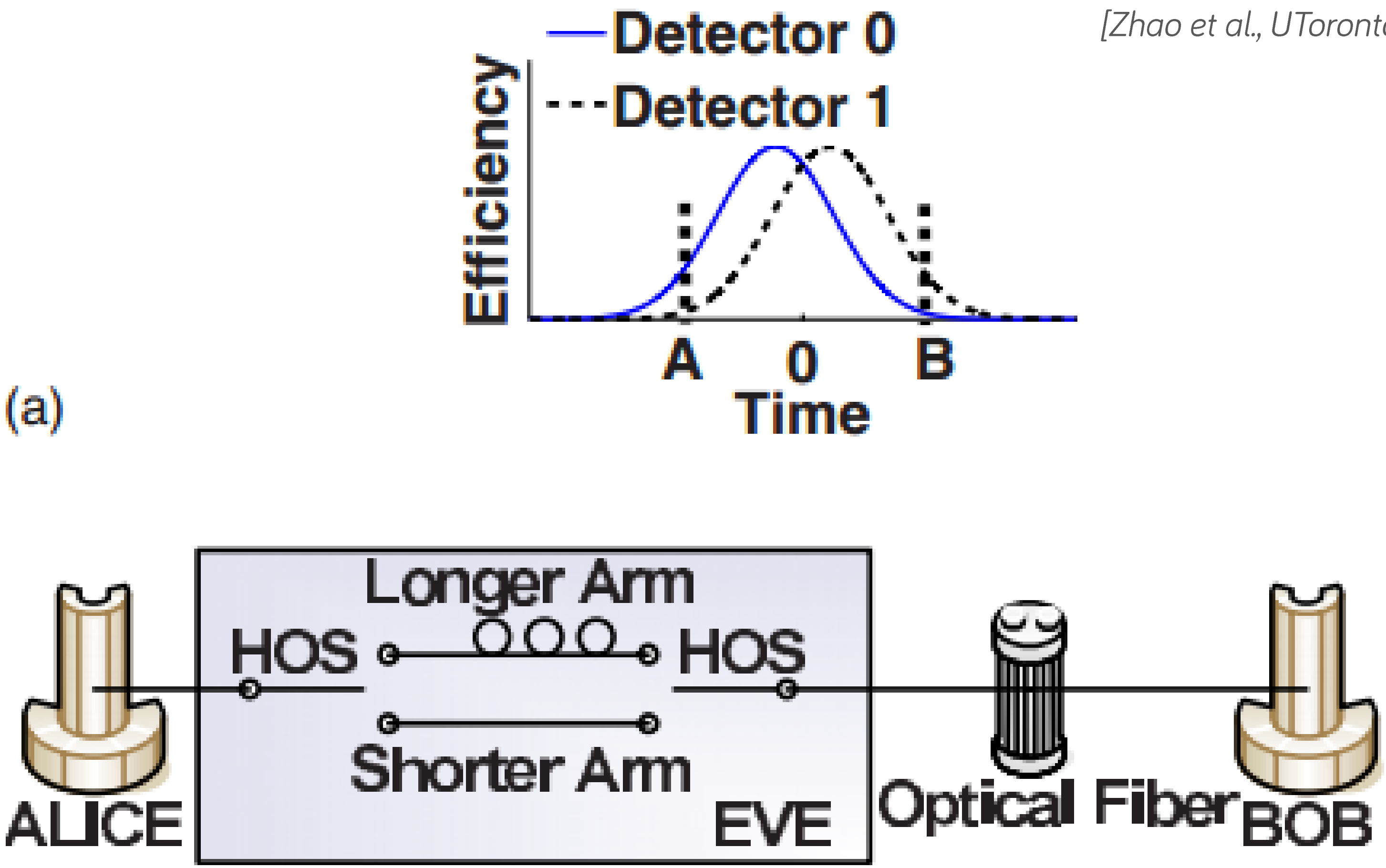
5 QKD in practice

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

[Gerhadt et al., NUS]

5 QKD in practice

[Zhao et al., UToronto]



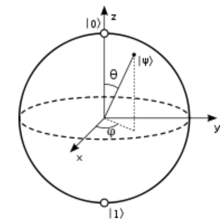
Use imperfections: measure, shift in time, pretend to be a “noise”.

superdense coding
q. teleportation
secure QKD

[QIP 2012, UMontréal]

1 we need a qubit

and we can use it

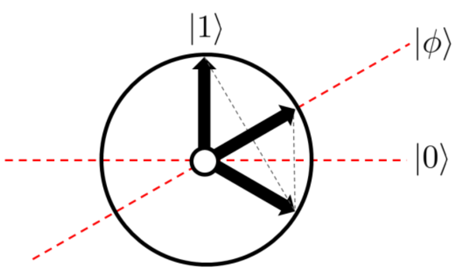


2 EPR pairs

give us cool 2-qubit protocols

3 the algorithms

that make quantum computing tick



4 error correction

can we really scale up this stuff?