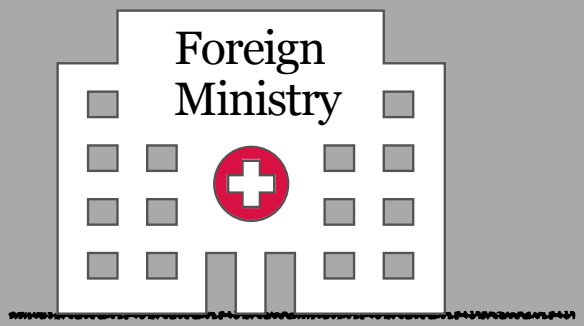
The quantum threat to communication security

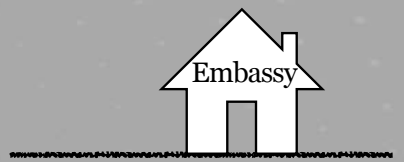
Quantum Information Theory

J.-D. Bancal, N. Sangouard
X. Valcarce, J. Zivy, V. Barizien
P. Cussenot, C. Lanore, B. Grivet
F. Grasselli, E. Gonzales Ruiz, Y.-Z. Zhang

How to transfer data safely?

Public key protocols like RSA, Elliptic Curve…
used computational problems that are hard to solve

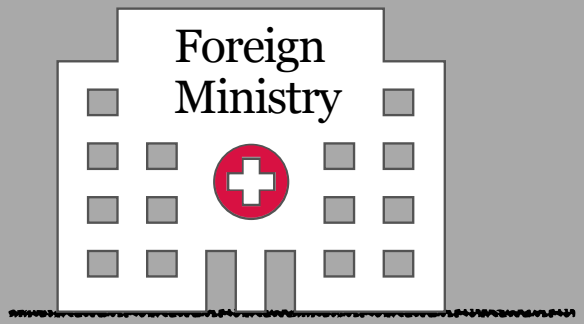


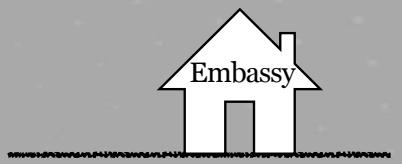


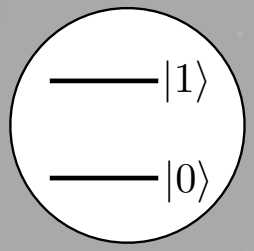
How to transfer data safely?

Public key protocols like RSA, Elliptic Curve…
used computational problems that are hard to solve

But they can be hacked with quantum computers!

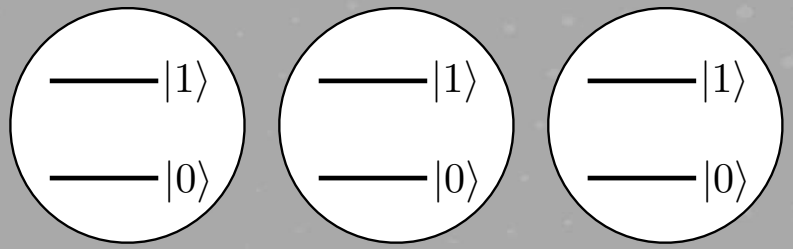






Qubit

Programming on a quantum computer

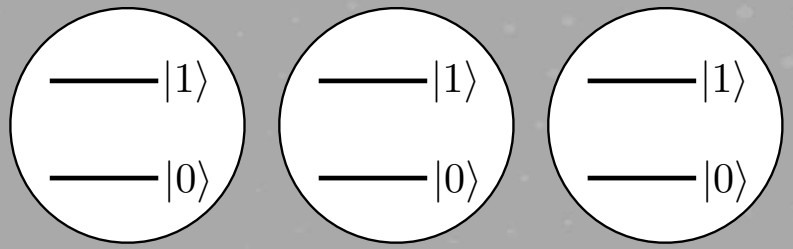


Integer Quantum encoding

$$x = 2^2.i + 2^1.j + 2^0.k \rightarrow |x\rangle = |ijk\rangle$$

$$0 \rightarrow |0\rangle = |000\rangle$$
$$1 \rightarrow |1\rangle = |001\rangle$$
$$\vdots$$
$$7 \rightarrow |7\rangle = |111\rangle$$

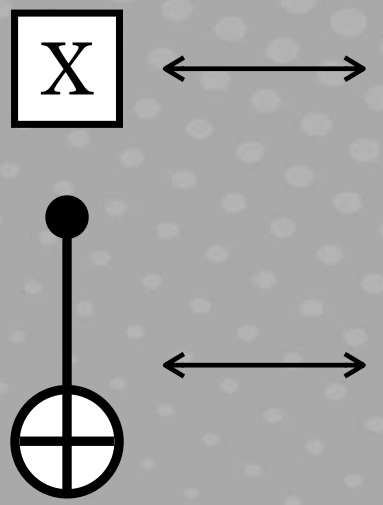
Programming on a quantum computer



Integer Quantum encoding

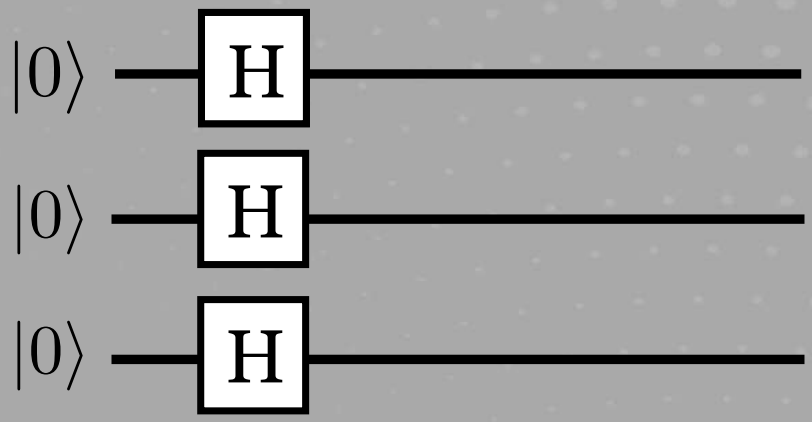
$$x = 2^2.i + 2^1.j + 2^0.k \rightarrow |x\rangle = |ijk\rangle$$

$$0 \rightarrow |0\rangle = |000\rangle$$
$$1 \rightarrow |1\rangle = |001\rangle$$
$$\vdots$$
$$7 \rightarrow |7\rangle = |111\rangle$$



$$|0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$|1\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

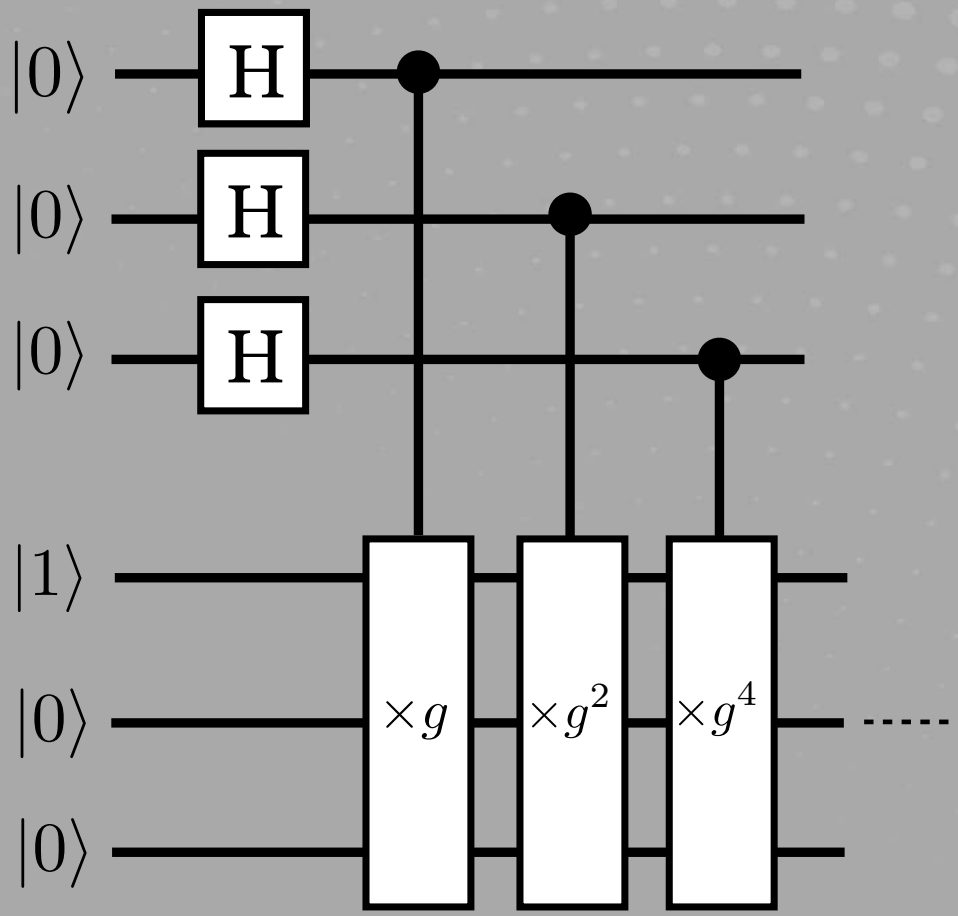
Programming on a quantum computer



Superposition principle

$$(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)$$
$$\propto |000\rangle + |001\rangle + |010\rangle + |011\rangle$$
$$+ |100\rangle + |101\rangle + |110\rangle + |111\rangle \propto \sum_{x=0}^{7} |x\rangle$$

Programming on a quantum computer



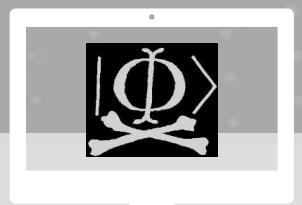
Superposition principle

$$(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)$$
$$\propto |000\rangle + |001\rangle + |010\rangle + |011\rangle$$
$$+|100\rangle + |101\rangle + |110\rangle + |111\rangle \propto \sum_{x=0}^{7} |x\rangle$$

$$f(x) : |x\rangle \rightarrow |x\rangle|g^x\rangle$$
$$g^x = g^{\sum_i 2^i x_i} = \Pi_i [g^{2^i}]^{x_i}$$

f(x) is obtained $\forall x$ from a single computation

$$\frac{1}{\sqrt{8}} \sum_{x=0}^{7} |x\rangle|f(x)\rangle$$



Programming on a quantum computer

Discrete Fourier Transform $x_0, \ldots, x_{N-1} \longrightarrow y_0, \ldots, y_{N-1}$ with $y_k = \frac{1}{\sqrt{N}} \sum_{j=0} x_j e^{2i\pi jk/N}$

Quantum Fourier Transform $\sum_{j=0}^{N-1} x_j |j\rangle \longrightarrow \sum_{k=0}^{N-1} y_k |k\rangle$

Find the period r of $f(x)$

$$\frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x\rangle|f(x)\rangle = \frac{1}{M} \sum_{x=0}^{M-1} \sum_{\ell=0}^{M-1} e^{2i\pi\ell x/M} |\ell\rangle|f(x)\rangle$$

Fourier transform register 1

$$= \frac{1}{M} \sum_{x_0=0}^{r-1} \sum_{k=0}^{M/r-1} \sum_{\ell=0}^{M-1} e^{2i\pi\ell(x_0+kr)/M} |\ell\rangle|f(x_0)\rangle$$

Mesure register 1

$$\sim \ell \propto \left| \sum_{k=0}^{M/r-1} e^{2\pi i\ell kr/M} \right|^2$$ such that $\ell r/M$ is an integer

Extract r from the result

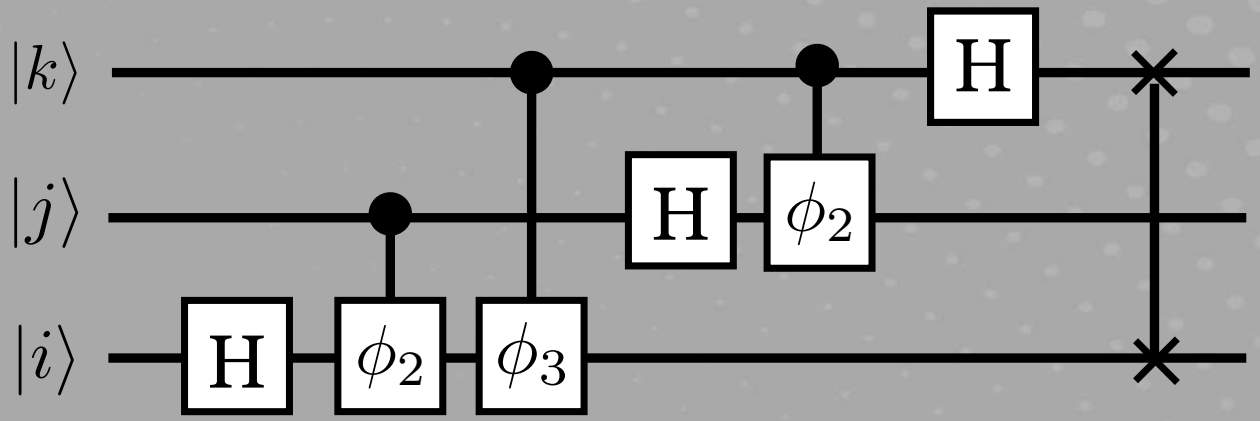
Programming on a quantum computer

QFT

$$\sum_{j=0}^{N-1} x_j|j\rangle \longrightarrow \sum_{k=0}^{N-1} y_k|k\rangle \quad \text{avec} \quad y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2i\pi jk/N}$$

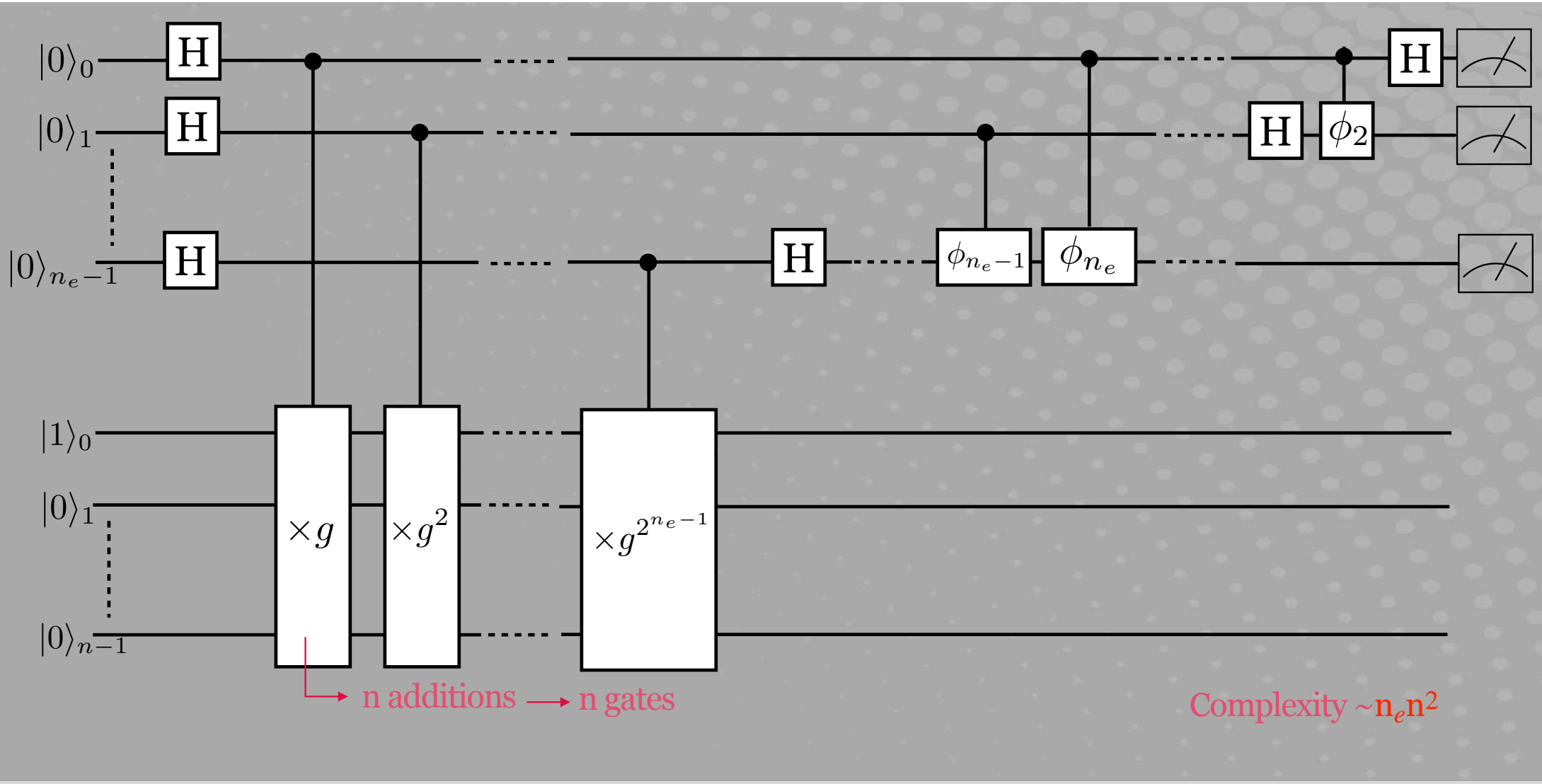
$$|ijk\rangle \rightarrow \frac{1}{\sqrt{8}}\left(|0\rangle + e^{2i\pi k/2}|1\rangle\right)\left(|0\rangle + e^{2i\pi(j/2+k/4)}|1\rangle\right)\left(|0\rangle + e^{2i\pi(i/2+j/4+k/8}|1\rangle\right)$$

Quantum circuit



Phase gate

$$|0\rangle \rightarrow |0\rangle$$
$$|1\rangle \rightarrow e^{2i\pi/2^\ell}|1\rangle$$



Programming on a quantum computer : Period of an exponentiation

Problem : Given the product of two prime integers N=p x q, find p et q

Step 1 : Choose an integer g

Step 2 : Compute the period r of

$$f(x) : x \rightarrow g^x \mod N$$

i.e. find the smallest r such that

$$g^r \equiv 1 \mod N$$

$$(g^{r/2} - 1)(g^{r/2} + 1) \equiv 0 \mod N$$

Step 3 : gcd ($g^{r/2}$-1,N) is one of the desired prime number

Problem : modular exponentiation

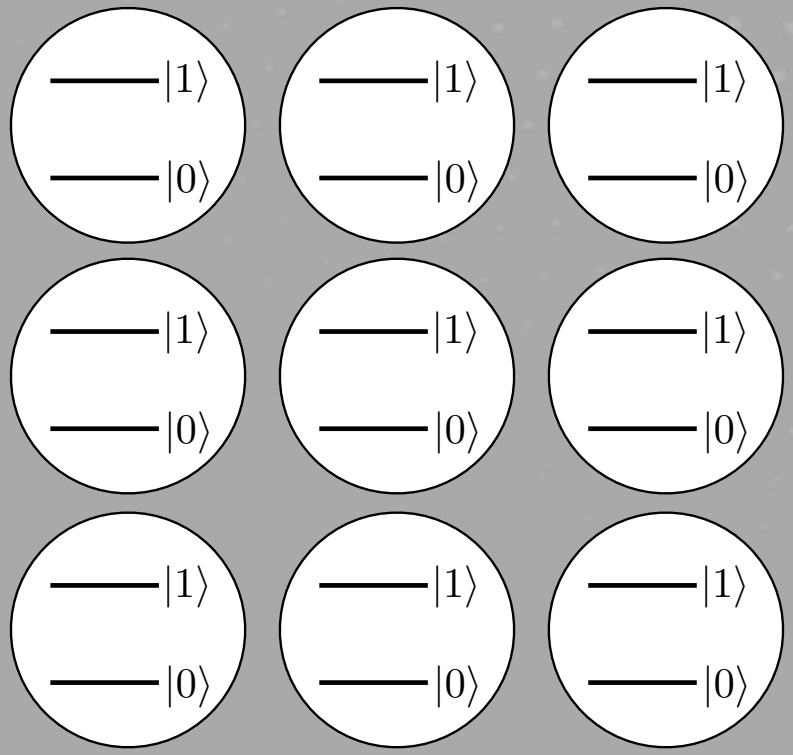
$$f(x) : x \rightarrow g^x \mod N$$

Problem : Given the product of two prime integers N=p x q, find p et q

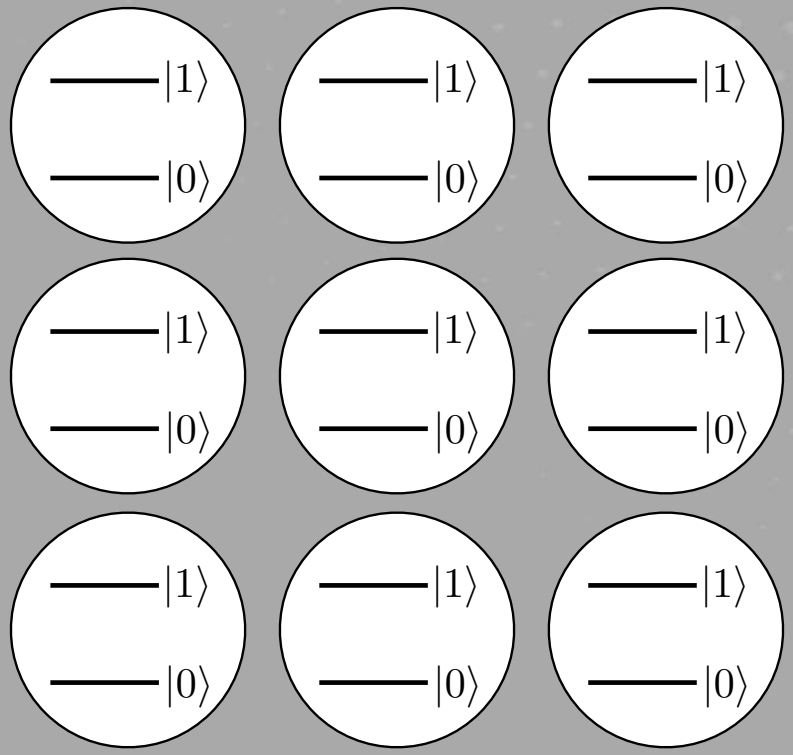
Classical : no polynomial algorithme $O\left((\log N)^k\right)$

Quantum : can be solved $O\left((\log N)^3\right)$

Shor is an algorithm with a exponential quantum advantage



Error correction : stabilizer codes

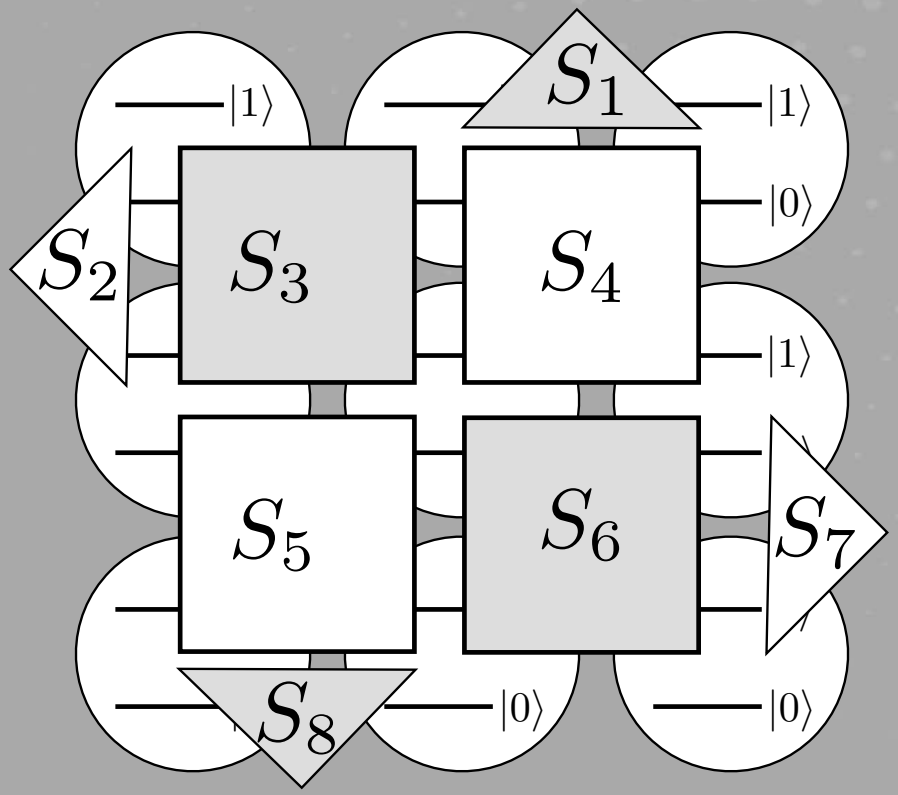


$\{S_i\}$ is a set of independent commuting Pauli operators

Logical states are in the subspace

$$\{|\psi\rangle | \forall i \; S_i|\psi\rangle = |\psi\rangle\}$$

Error correction : stabilizer codes



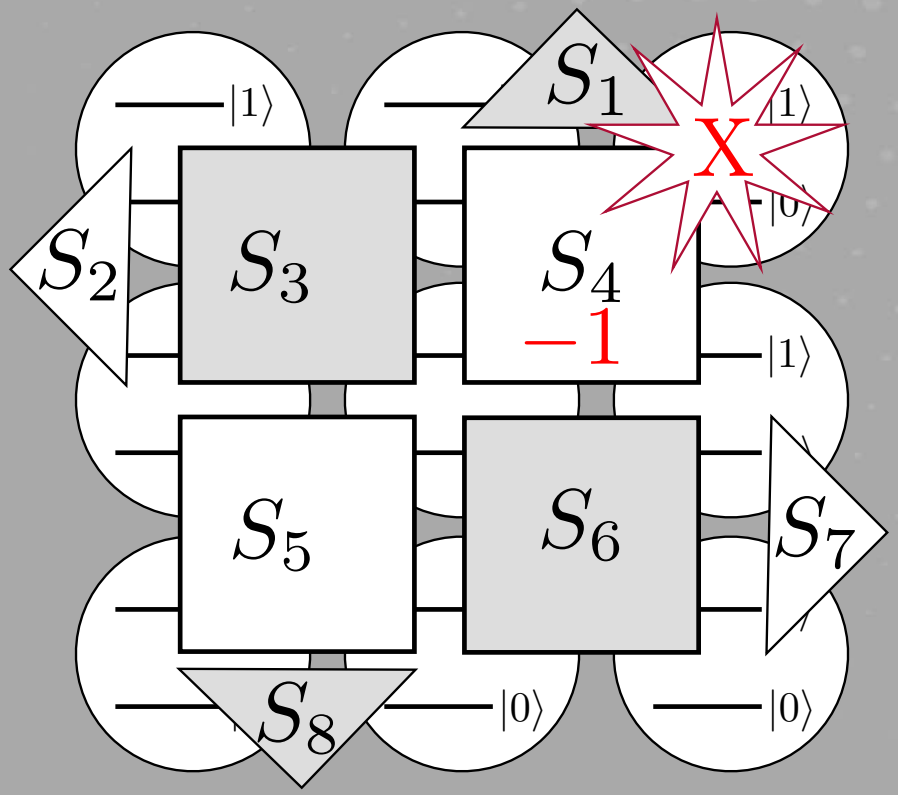
$\{S_i\}$ is a set of independent commuting Pauli operators

Logical states are in the subspace

$$\{|\psi\rangle | \forall i \; S_i|\psi\rangle = |\psi\rangle\}$$

$$S_i = \mathrm{X...X} \text{ for odd } i$$
$$S_i = \mathrm{Z...Z} \text{ for even } i$$

Error correction : stabilizer codes



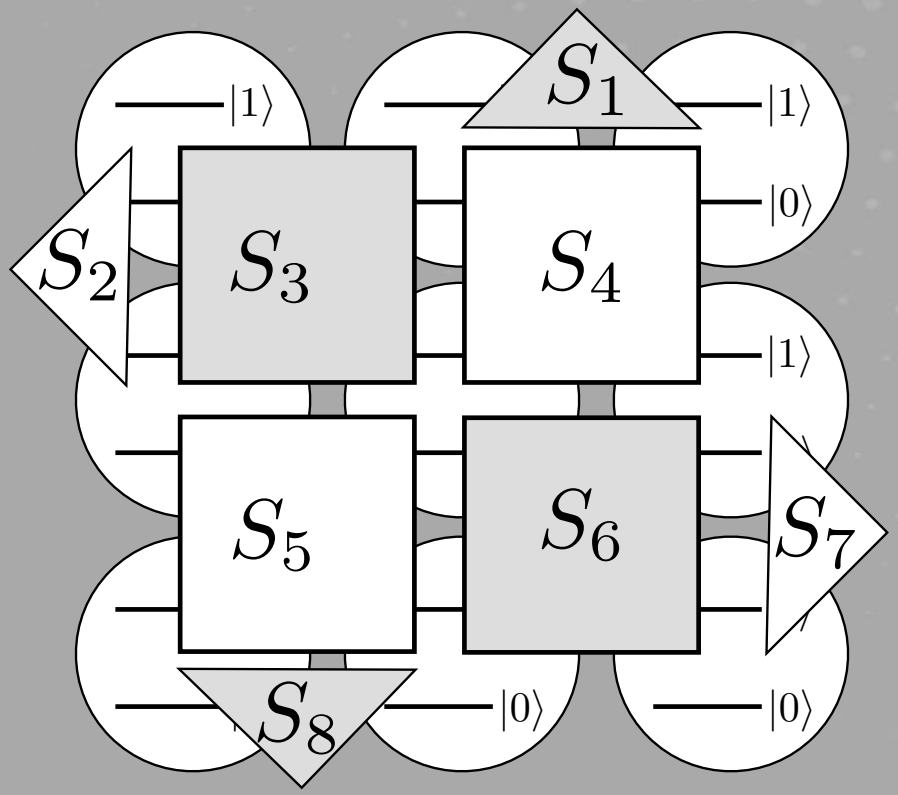
$\{S_i\}$ is a set of independent commuting Pauli operators

Logical states are in the subspace

$$\{|\psi\rangle | \forall i \; S_i|\psi\rangle = |\psi\rangle\}$$

$$S_i = \mathrm{X...X} \text{ for odd } i$$
$$S_i = \mathrm{Z...Z} \text{ for even } i$$

Error correction : stabilizer codes



The code performance depends on
1-the choice of stabilizers
2-the implementation of these stabilizers
3-the decoder

Many decoders for stabilizer codes based on Tensor networks contraction, Neural networks, Lookup tables, Simulated annealing, Cellular automation, Renormalization group, Belief propagation, Reinforcement learning, Ising model, combinatorial optimization solvers....

Error correction : stabilizer codes

What kind of quantum computers is actually a threat?

Factoring 2048-RSA integers with 20 000 000 superconducting qubits and a surface code

C. Gidney and M. Ekera, Quantum 5, 433 (2021)

Factoring 2048-RSA integers takes 13436 qubits and a multimode memory

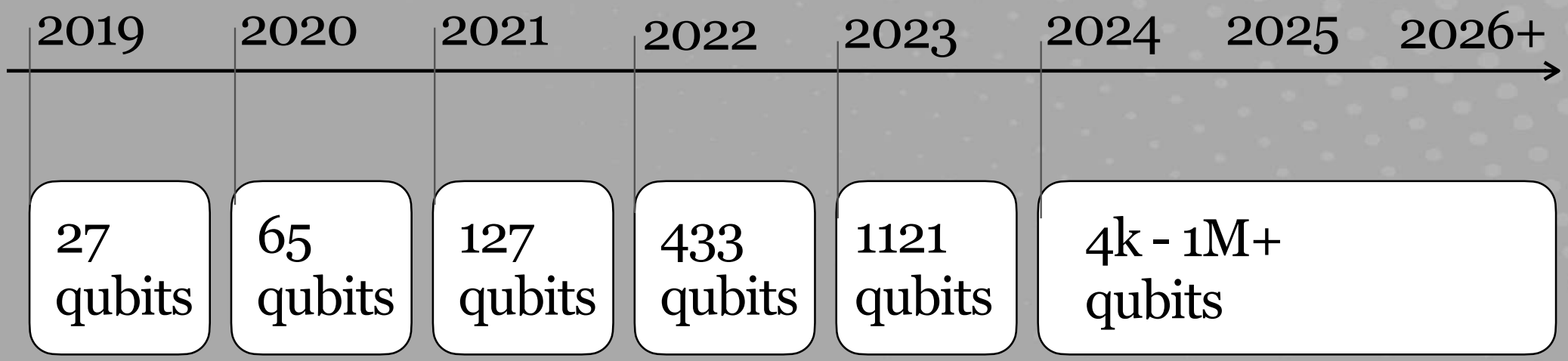
E. Gouzien and N. Sangouard Phys. Rev. Lett. 127, 140503 (2021)

Computing 256-bit elliptic curve logarithm with 126133 cat qubits and a repetition code

E. Gouzien, D. Ruiz, F.-M. Le Régent, J. Guillaud and N. Sangouard Phys. Rev. Lett. 131, 046002 (2023)

IBM quantum development roadmap

https://research.ibm.com/blog/quantum-development-roadmap



Prepare now against the quantum computer threat!

Post-quantum algorithms

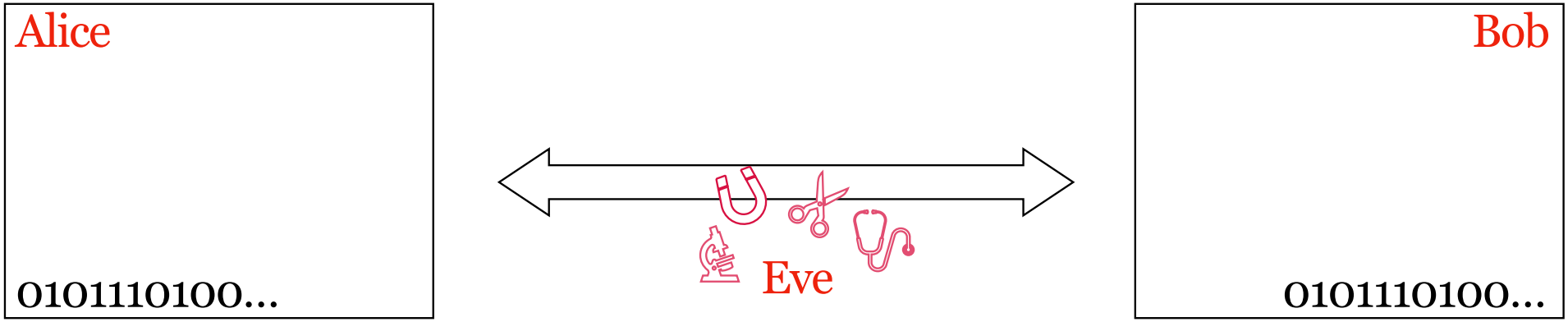
Lattice-based or code based algorithm

Believed to be secure against known quantum attacks

Quantum key distribution

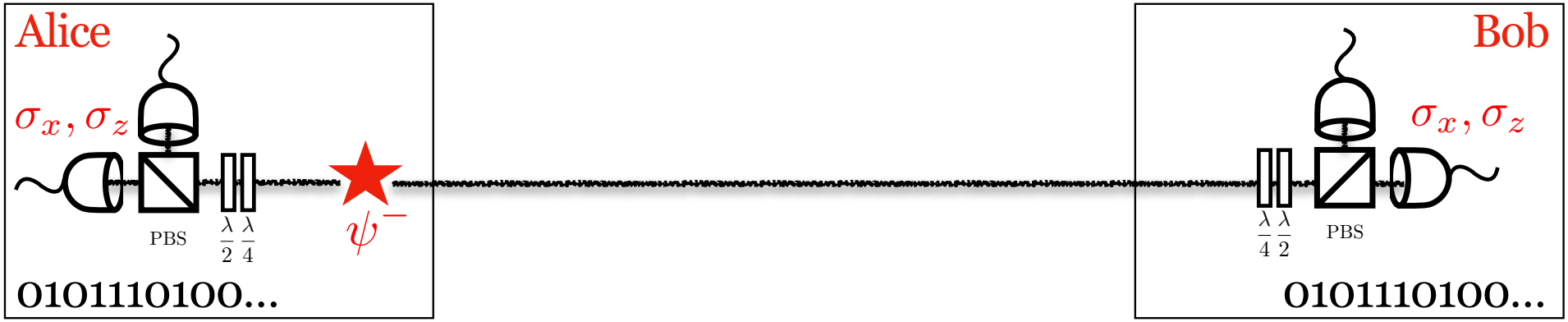
Information theoretic security

Recommended for high-value information requiring long term confidentiality



Goal : share a random private key

key + one time pad = provable security

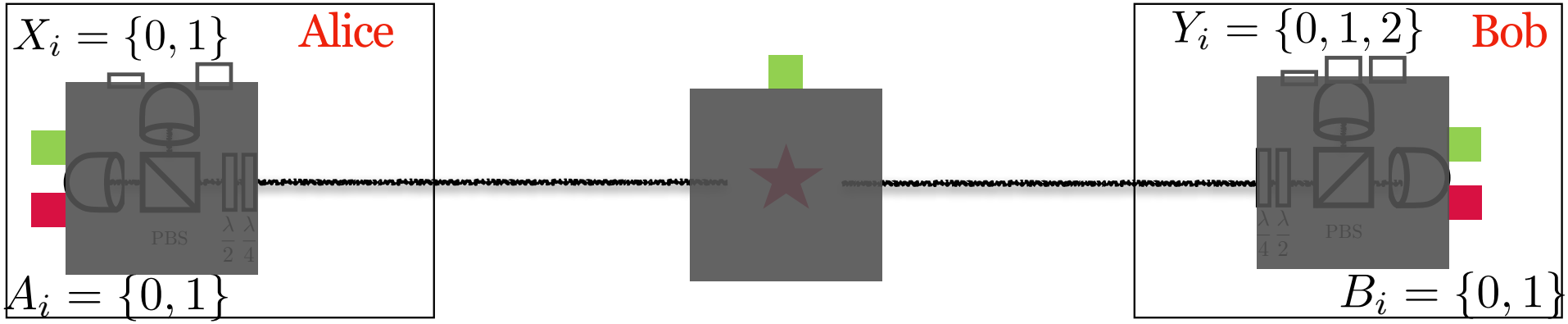


Quantum principle : Pauli measurements on a two-qubit maximally entangled state yield identical outcomes that are fundamentally unpredictable to any third party.

↳ a random private key

A.K. Eckert, Phys. Rev. Lett. 67, 661 (1991)

Quantum key distribution based on Bell's theorem: Intuition



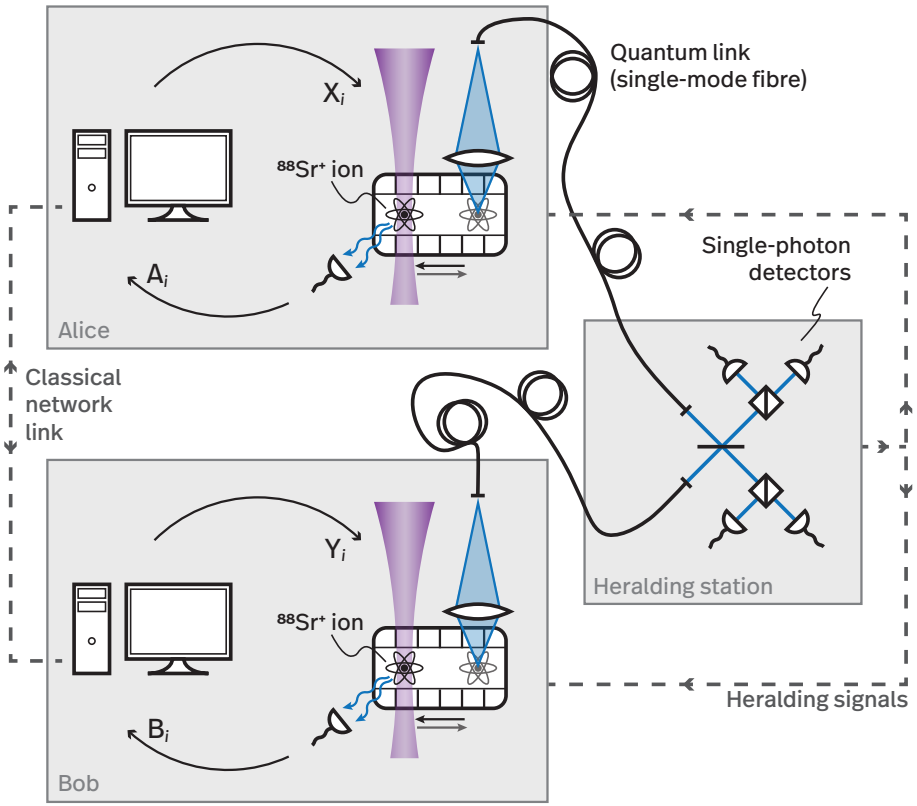
How can we check that the proper measurements operates on an appropriate entangled state?

Play a non-local game!
Winning condition: $A_i \oplus B_i = X_i.Y_i$
Best classical strategy : 75% winning probability
Best quantum strategy : ~85% winning probability } quantum advantage

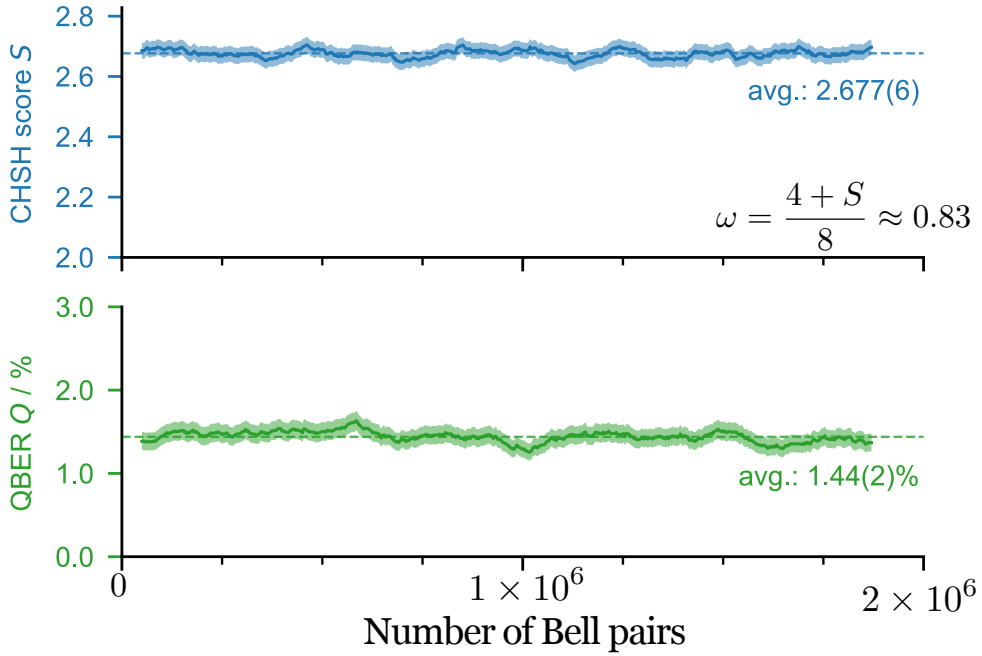
↳ State is closed to the singlet

CHSH rigidity : the Tsirelson bound (~85%) can only be obtained with a two qubit maximally entangled state (defined up to local isometries)

Experimental setup



Link performance



$n = 1.5 \times 10^6$

Data acquisition

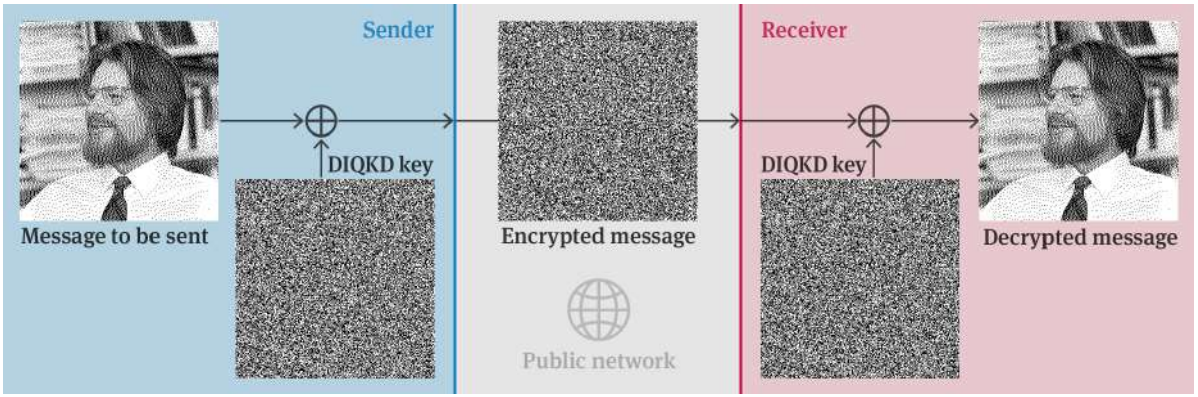
Certified entropy (EAT) — 392401 secret bits

Key size — 95884 bits

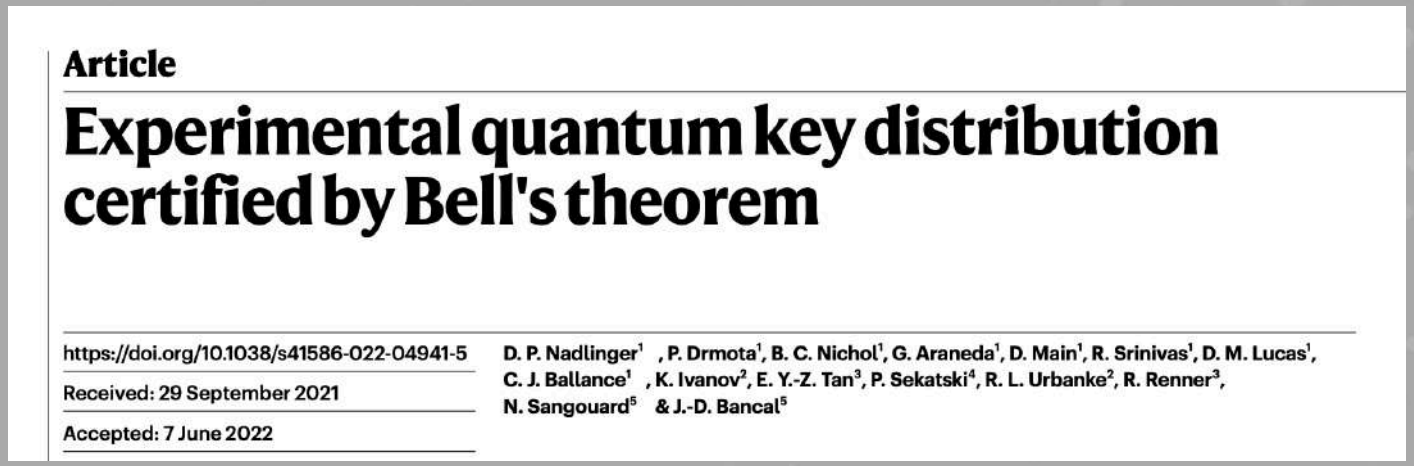
($m = 296517$ used for error correction)

Protocol step	Consumed	Used (reusable)
Validation of error correction	64	1280
Authentication	128	
Key activation	64	
Privacy amplification	0	1 201 886
Total	256	1 203 166

95884 bits generated
256 bits of a shared random key used



Quantum-safe cryptography is unique as it provides information-theoretic security



Article

Experimental quantum key distribution certified by Bell's theorem

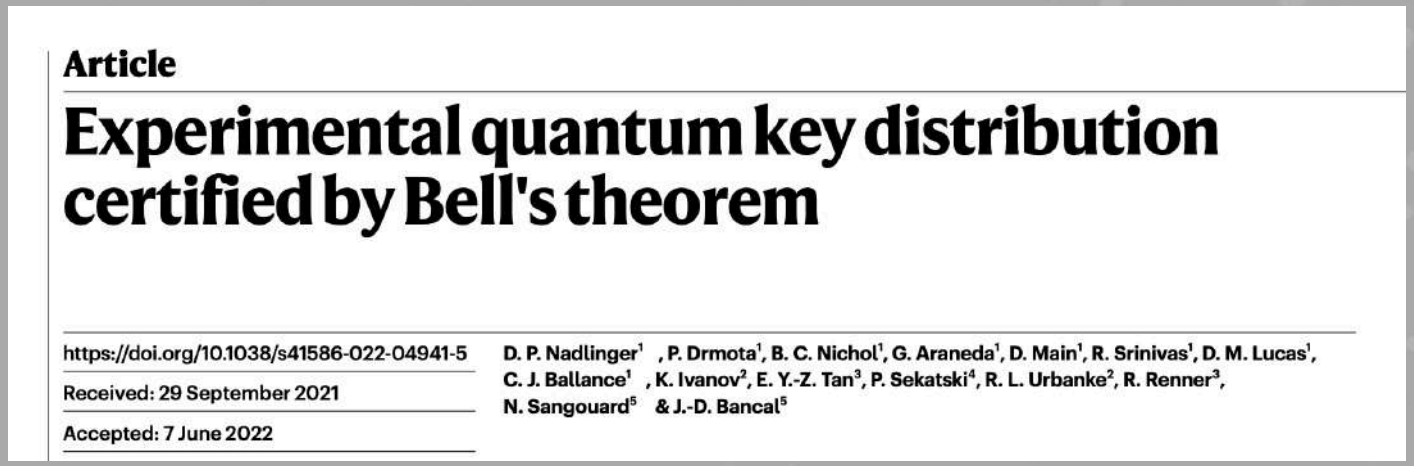
https://doi.org/10.1038/s41586-022-04941-5

Received: 29 September 2021

Accepted: 7 June 2022

D. P. Nadlinger[1], P. Drmota[1], B. C. Nichol[1], G. Araneda[1], D. Main[1], R. Srinivas[1], D. M. Lucas[1], C. J. Ballance[1], K. Ivanov[2], E. Y.-Z. Tan[3], P. Sekatski[4], R. L. Urbanke[2], R. Renner[3], N. Sangouard[5] & J.-D. Bancal[5]

Quantum-safe cryptography is unique as it provides information-theoretic security



Article

Experimental quantum key distribution certified by Bell's theorem

https://doi.org/10.1038/s41586-022-04941-5

Received: 29 September 2021

Accepted: 7 June 2022

D. P. Nadlinger[1], P. Drmota[1], B. C. Nichol[1], G. Araneda[1], D. Main[1], R. Srinivas[1], D. M. Lucas[1], C. J. Ballance[1], K. Ivanov[2], E. Y.-Z. Tan[3], P. Sekatski[4], R. L. Urbanke[2], R. Renner[3], N. Sangouard[5] & J.-D. Bancal[5]

Article

Loophole-free Bell inequality violation with superconducting circuits

https://doi.org/10.1038/s41586-023-05885-0

Received: 22 August 2022

Accepted: 24 February 2023

Published online: 10 May 2023

Simon Storz[1], Josua Schär[1], Anatoly Kulikov[1], Paul Magnard[1,10], Philipp Kurpiers[1,11], Janis Lütolf[1], Theo Walter[1], Adrian Copetudo[1,12], Kevin Reuer[1], Abdulkadir Akin[1], Jean-Claude Besse[1], Mihai Gabureac[1], Graham J. Norris[1], Andrés Rosario[1], Ferran Martin[2], José Martinez[2], Waldimar Amaya[2], Morgan W. Mitchell[3,4], Carlos Abellan[2], Jean-Daniel Bancal[5], Nicolas Sangouard[5], Baptiste Royer[6,7], Alexandre Blais[7,8] & Andreas Wallraff[1,9]

Quantum-safe cryptography is unique as it provides information-theoretic security

Article

Experimental quantum key distribution certified by Bell's theorem

https://doi.org/10.1038/s41586-022-04941-5
Received: 29 September 2021
Accepted: 7 June 2022

D. P. Nadlinger[1], P. Drmota[1], B. C. Nichol[1], G. Araneda[1], D. Main[1], R. Srinivas[1], D. M. Lucas, C. J. Ballance[1], K. Ivanov[2], E. Y.-Z. Tan[3], P. Sekatski[4], R. L. Urbanke[2], R. Renner[3], N. Sangouard[5] & J.-D. Bancal[5]

Article

Loophole-free Bell inequality violation with superconducting circuits

https://doi.org/10.1038/s41586-023-05885-0
Received: 22 August 2022
Accepted: 24 February 2023
Published online: 10 May 2023

Simon Storz[1], Josua Schär[1], Anatoly Kulikov[1], Paul Magnard[1,10], Philipp Kurpiers, Janis Lütolf[1], Theo Walter[1], Adrian Copetudo[1,12], Kevin Reuer[1], Abdulkadir Akin[1], Jean-Claude Besse[1], Mihai Gabureac[1], Graham J. Norris[1], André, José Martinez[2], Waldimar Amaya[2], Morgan W. Mitchell[3,4], Carlo, Nicolas Sangouard[5], Baptiste Royer[6,7], Alexandre Blais[7,8] & And

Latest Reviews & Analysis >

Superconducting qubits cover new distances

Superconducting quantum bits, a promising platform for future quantum computers, have been entangled over a separation of 30 metres, with a performance that enabled the demonstration of a milestone in quantum physics.

Marissa Giustina
News & Views 10 May 2023

NewScientist

News Features Newsletters Podcasts Video Comment Culture Crosswords | This week's magazine
Health Space Physics Technology Environment Mind Humans Life Mathematics Chemistry Earth Society

Physics

Superconducting qubits have passed a key quantum test

A Bell test can confirm whether two systems are truly entangled – it has now been used to confirm entanglement between qubits in a superconducting circuits

ars TECHNICA BIZ & IT TECH SCIENCE POLICY

GOING THE DISTANCE —

Qubits 30 meters apart used to confirm Einstein was wrong about quantum

Experiment linked qubits using a supercold wire over 30 meters long.

EL PAÍS

Tecnología

TU TECNOLOGÍA · CIBERSEGURIDAD · PRIVACIDAD · INTELIGENCIA ARTIFICIAL · INTERNET · GRANDES TECNOLÓGICAS

FÍSICA CUÁNTICA >

Un experimento demuestra la acción fantasmal cuántica con cúbits superconductores separados 30 metros

D-PHYS

Entangled quantum circuits

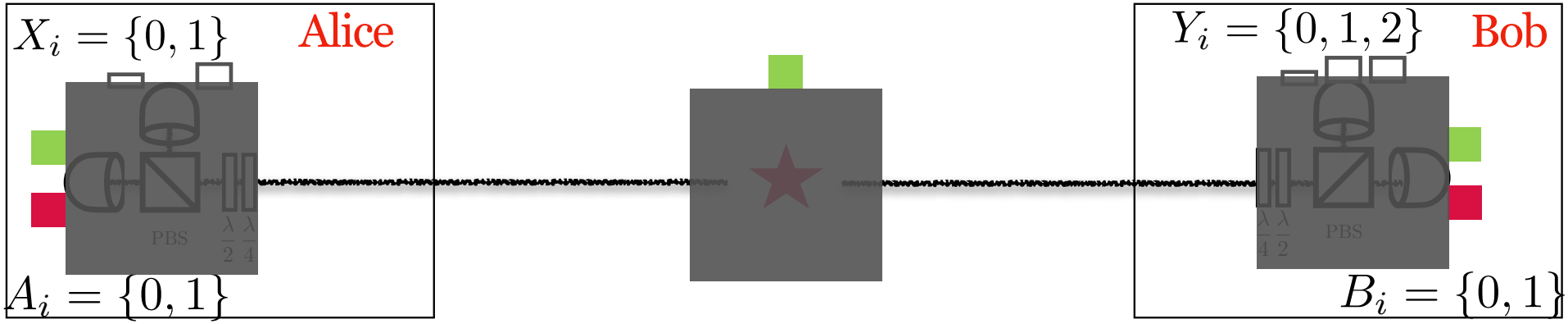
ETH Zurich researchers have succeeding in demonstrating that quantum mechanical objects

If you know

Tensor networks contraction, Neural networks,
Conventional neural network, Lookup tables,
Simulated annealing, Cellular automation,
Renormalization group, Belief propagation,
Reinforcement learning, Ising model or
combinatorial optimization solvers

and are interested in quantum information, please come to us!

Quantum key distribution based on Bell's theorem: Intuition



How random A is from Eve's point of view

$$H(A|E) = H(A) - \left(H(\rho_E) - \sum_a p_a H(\rho_{E|a}) \right)$$