Quantum cryptography

LEAPS meets Quantum Technology

17 May 2022, Isola d'Elba, Italy

Antonio Acín
ICREA Professor at ICFO-Institut de Ciencies Fotoniques, Barcelona
AXA Chair in Quantum Information Science

ICREA ICFO erc AXA Research Fund Fundació Privada CELLEX
MINISTERIO DE EDUCACIÓN Y CIENCIA
Generalitat de Catalunya
EXCELENCIA SEVERO OCHOA 2016 - 2019

Factorization

$6 = ?$

Factorization

$$6 = 2 \times 3$$

Factorization

6 = 2 x 3

221 =

Factorization

$6 = 2 \times 3$

$221 = 13 \times 17$

Factorization

6 = 2 x 3
221 = 13 x 17

2.160.062.083 =

Factorization

6 = 2 x 3
221 = 13 x 17

2.160.062.083 = 38699 x 55817

Factorization

6 = 2 x 3
221 = 13 x 17
2.160.062.083 = 38699 x 55817

22601385262034057849416540486101975135080389157197767183211977
68109445641817966676608593121306582577250631562886676970448070
00181114971186300211248792819948748206607013106658664608332798
28035603792053919801399464969552 61 =

Factorization

6 = 2 x 3
221 = 13 x 17
2.160.062.083 = 38699 x 55817

226013852620340578494165404861019751350803891571977671832119776810944564181796667660859312130658257725063156288667697044807000181114971186300211248792819948748206607013106658664608332798280356037920539198013994649695526 1 =

No efficient classical algorithm is known.

Factorization

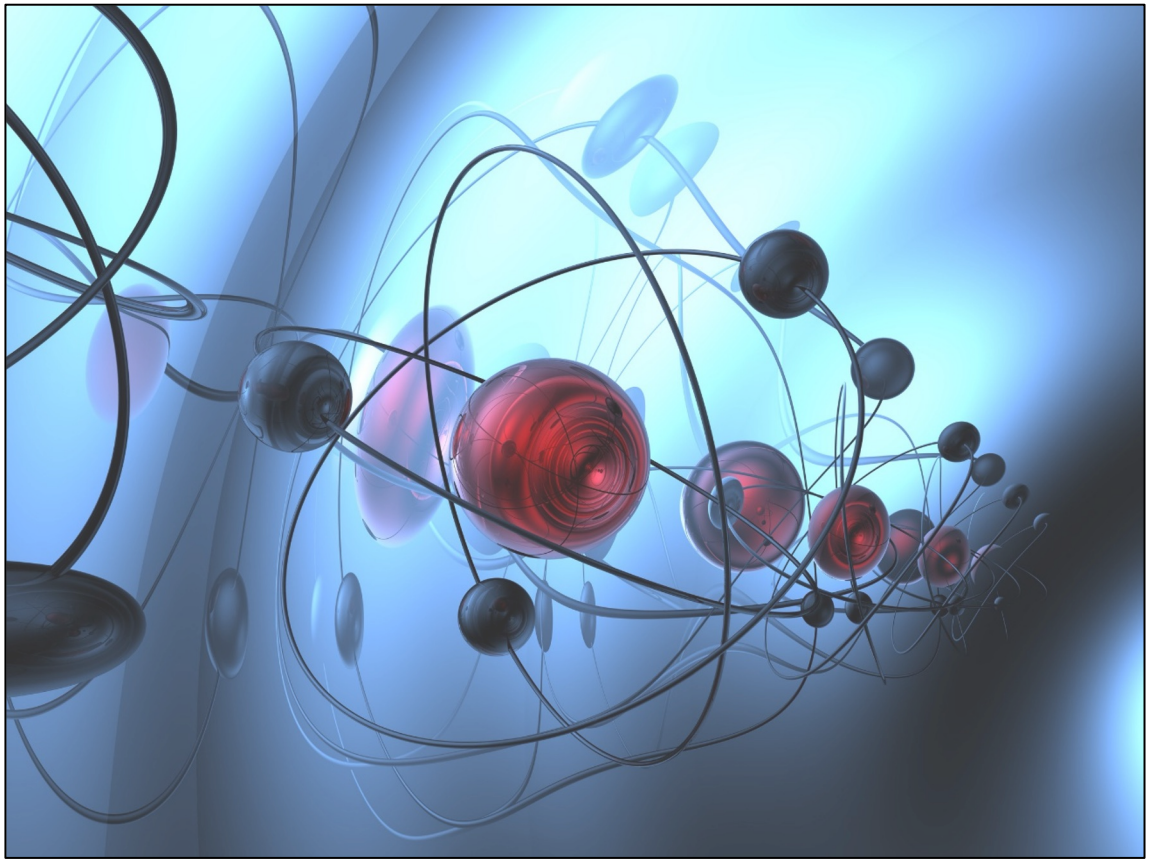
6 = 2 x 3
221 = 13 x 17
2.160.062.083 = 38699 x 55817

22601385262034057849416540486101975135080389157197767183211977
68109445641817966676608593121306582577250631562886676970448070
00181114971186300211248792819948748206607013106658664608332798
28035603792053919801399464969552 61 =

No efficient classical algorithm **is known**.

Factorization

Factoring is an easy problem for quantum computers.



Peter Shor

Factorization

226013852620340578494165404861019751350803891
571977671832119776810944564181796667660859312
130658257725063156288667697044807000181114971
186300211248792819948748206607013106658664608
33279828035603792053919801399464969552 61 =

Factorization

22601385262034057849416540486101975135080389157197767183211977681094456418179666766085931213065825772506315628866769704480700018111497118630021124879281994874820660701310665866460833279828035603792053919801399464969552615 =

6863656412267566274382371499288437800130842239979164844621244993321541061441464266793821364420842019205499968 7

x

3292907439486349812049301549212935291916455196536233952462686051169290349309465246333782486639073819176571260 3

226013852620340578494165404861019751350803891571977671832
119776810944564181796667660859312130658257725063156288667
697044807000181114971186300211248792819948748206607013106
658664608332798280356037920539198013994649695526 1 =

Hard

686365641226756627438237149928843780013084223997916484462
124499332154106144146426679382136442084201920549996 87

x

329290743948634981204930154921293529191645519653623395246
268605116929034930946524633378248663907381917657126 03

226013852620340578494165404861019751350803891571977671832
119776810944564181796667660859312130658257725063156288667
697044807000181114971186300211248792819948748206607013106
658664608332798280356037920539198013994649695526 1 =

Hard

Easy

686365641226756627438237149928843780013084223997916484462
124499332154106144146426679382136442084201920549996 87

x

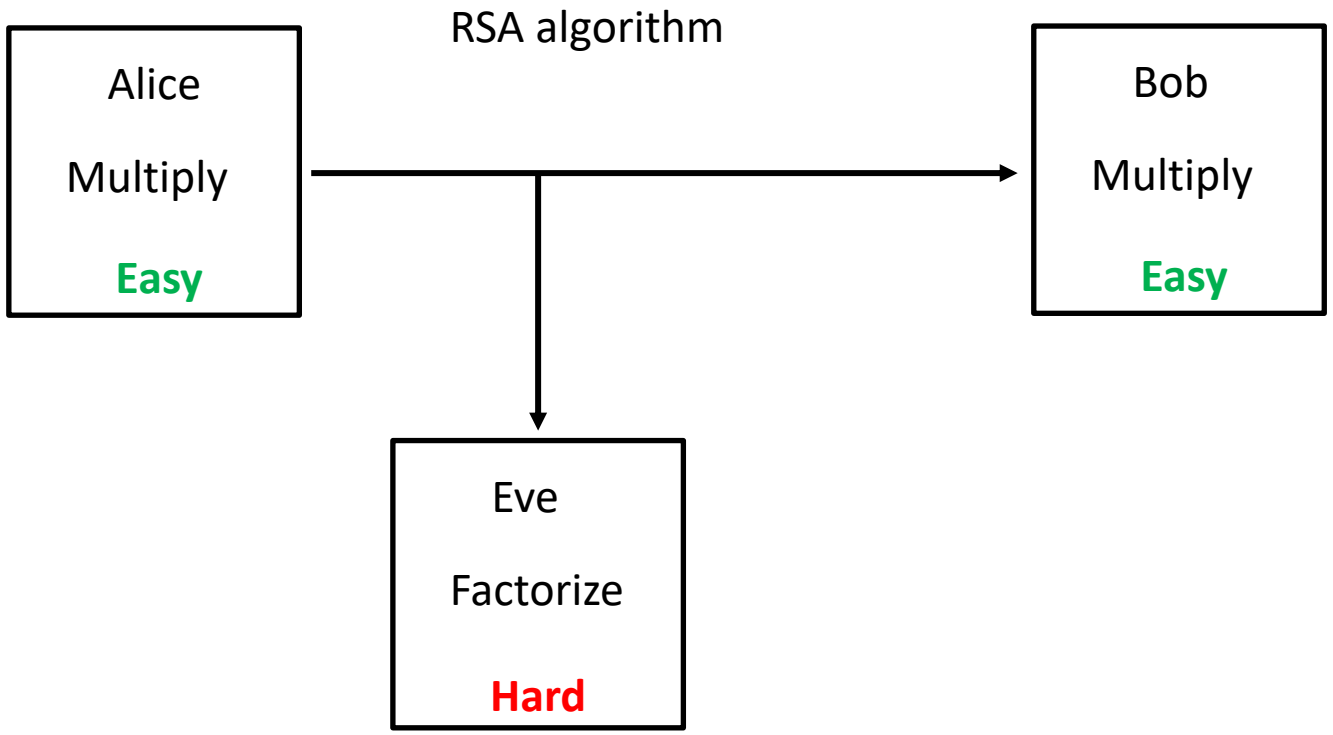
329290743948634981204930154921293529191645519653623395246
268605116929034930946524633378248663907381917657126 03

Cryptography

Factoring is an example of one-way functions, which are useful for cryptography.

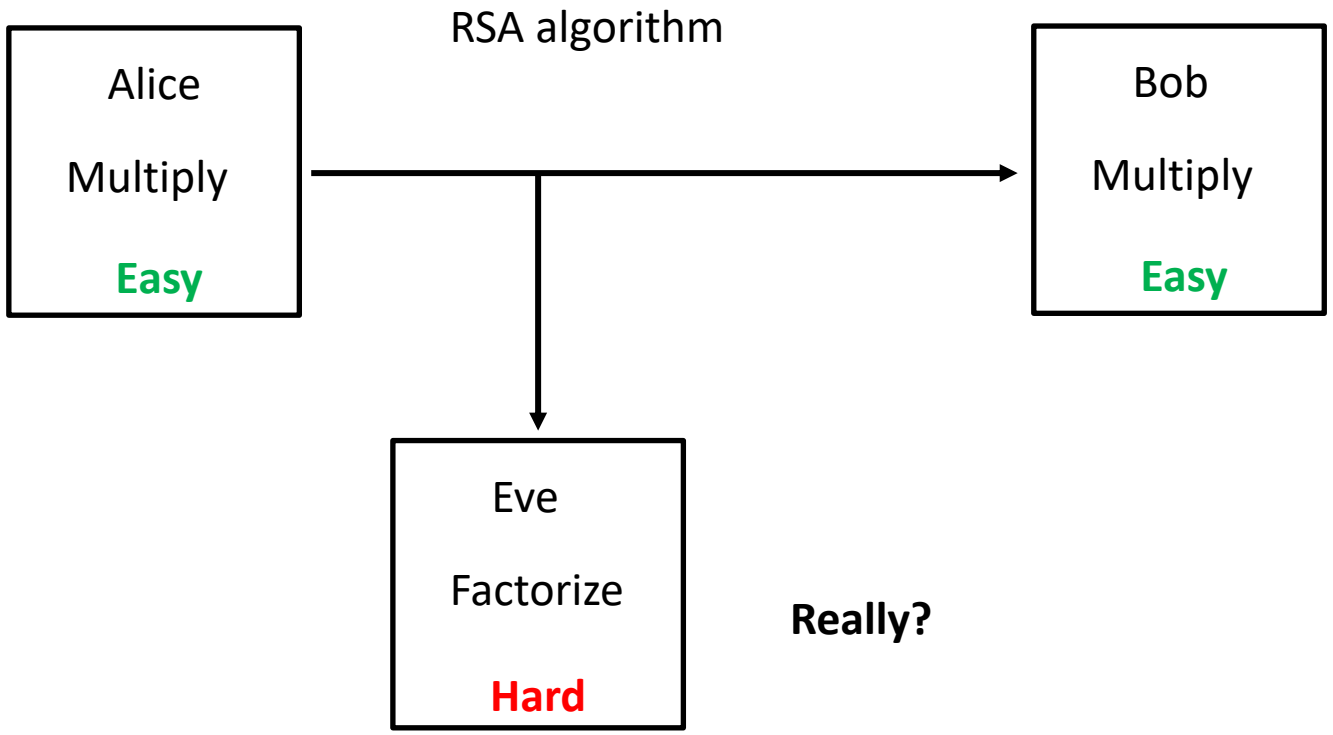
Cryptography

Factoring is an example of one-way functions, which are useful for cryptography.



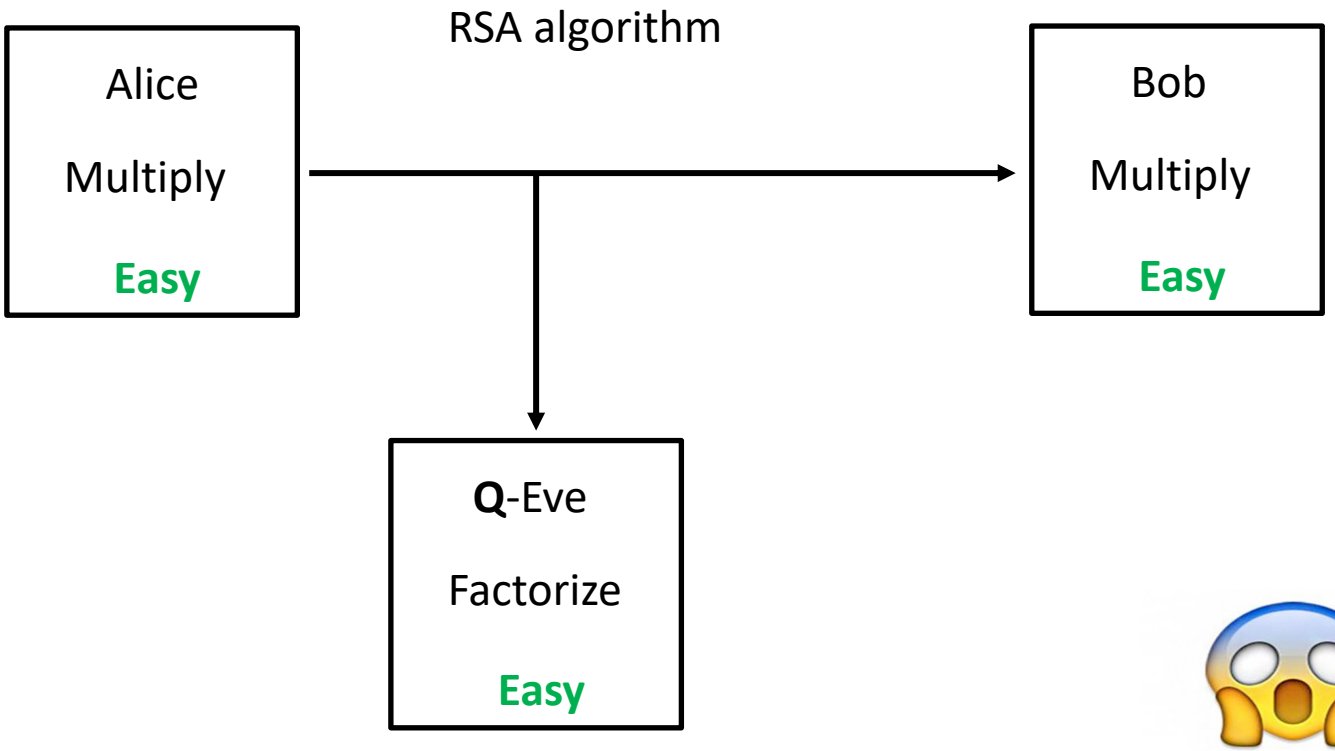
Cryptography

Factoring is an example of one-way functions, which are useful for cryptography.



Cryptography

Factoring is an example of one-way functions, which are useful for cryptography.

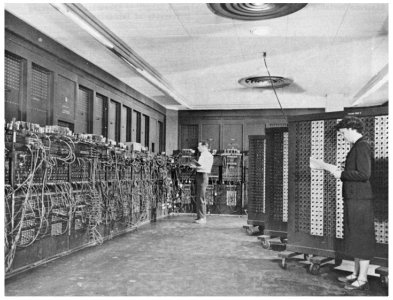


A quantum computer could break the most used scheme today for secure encryption!

Should we worry?

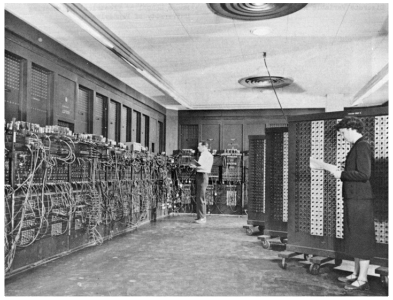
Do we have a quantum computer?

Do we have a quantum computer?



All these devices are computers.

Do we have a quantum computer?



All these devices are computers.

We do have few-qubit quantum computers, possibly without error correction.

What has not been achieved is **quantum supremacy or advantage**: a computing device solving a relevant problem in a more efficient way than any existing classical computer.

A quantum computer to break RSA will take years (possibly decades). Yet, if it happens, **security to the future** will be compromised.

Quantum-safe cryptography

There exist two main approaches to design cryptographic schemes secure against a quantum computer:

Quantum-safe cryptography

There exist two main approaches to design cryptographic schemes secure against a quantum computer:

1) Post-quantum cryptography → Computational Security

Same paradigm

Quantum-safe cryptography

There exist two main approaches to design cryptographic schemes secure against a quantum computer:

1) Post-quantum cryptography → Computational Security

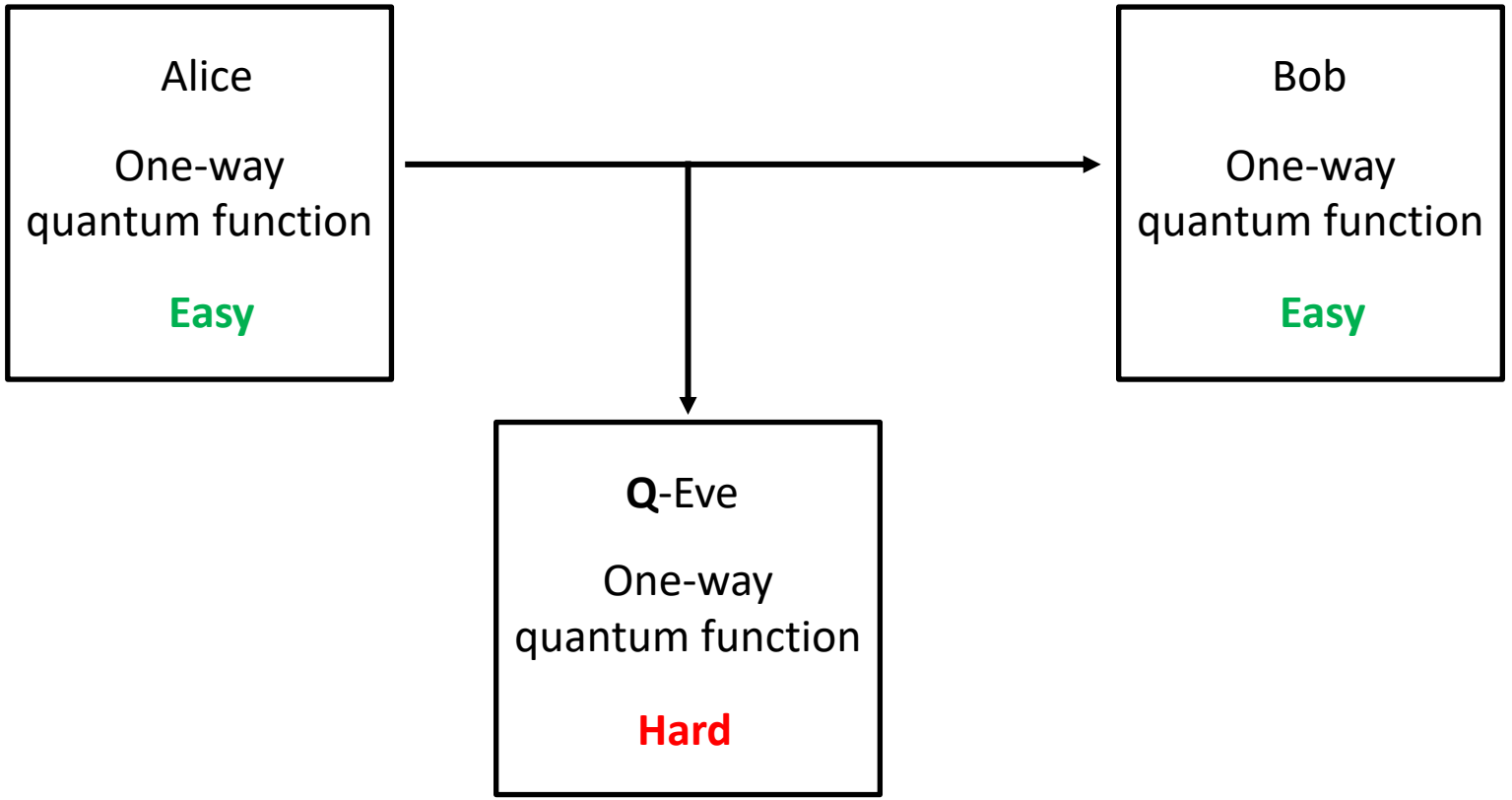
Same paradigm

2) Quantum cryptography → (Quantum) Physical Security

New paradigm

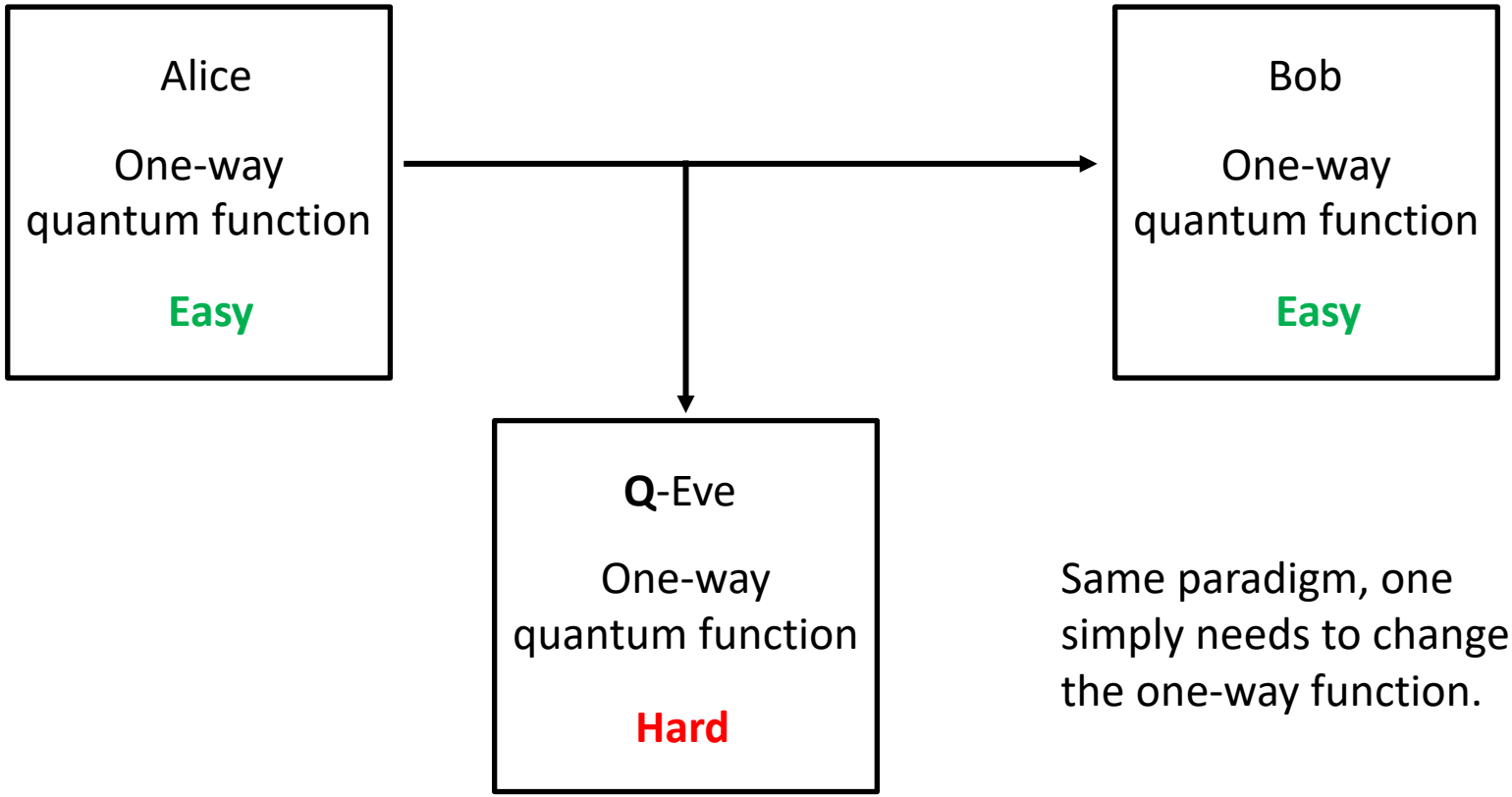
Post-quantum cryptography

Search for one-way quantum functions and construct a cryptographic protocol.



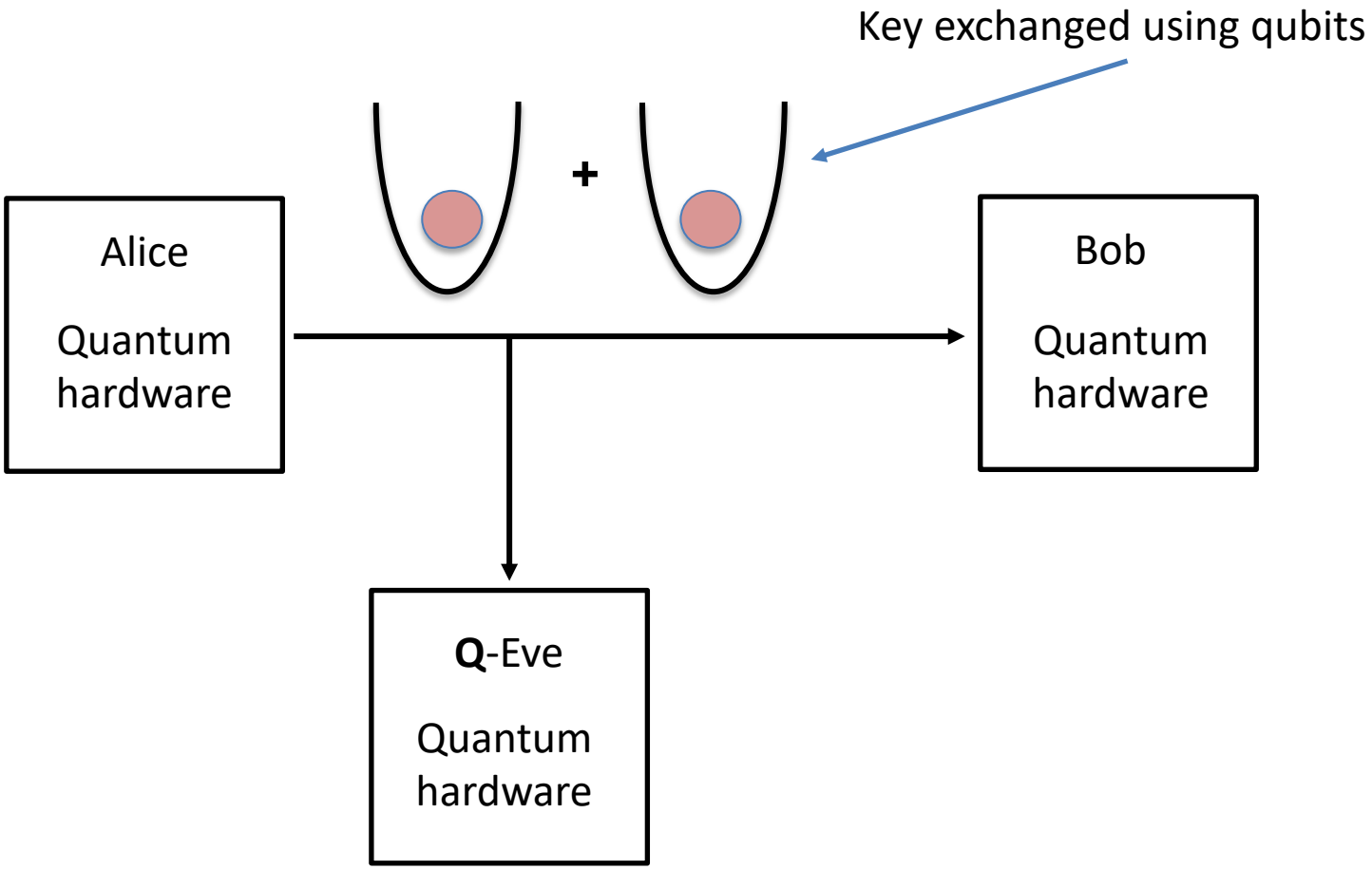
Post-quantum cryptography

Search for one-way quantum functions and construct a cryptographic protocol.

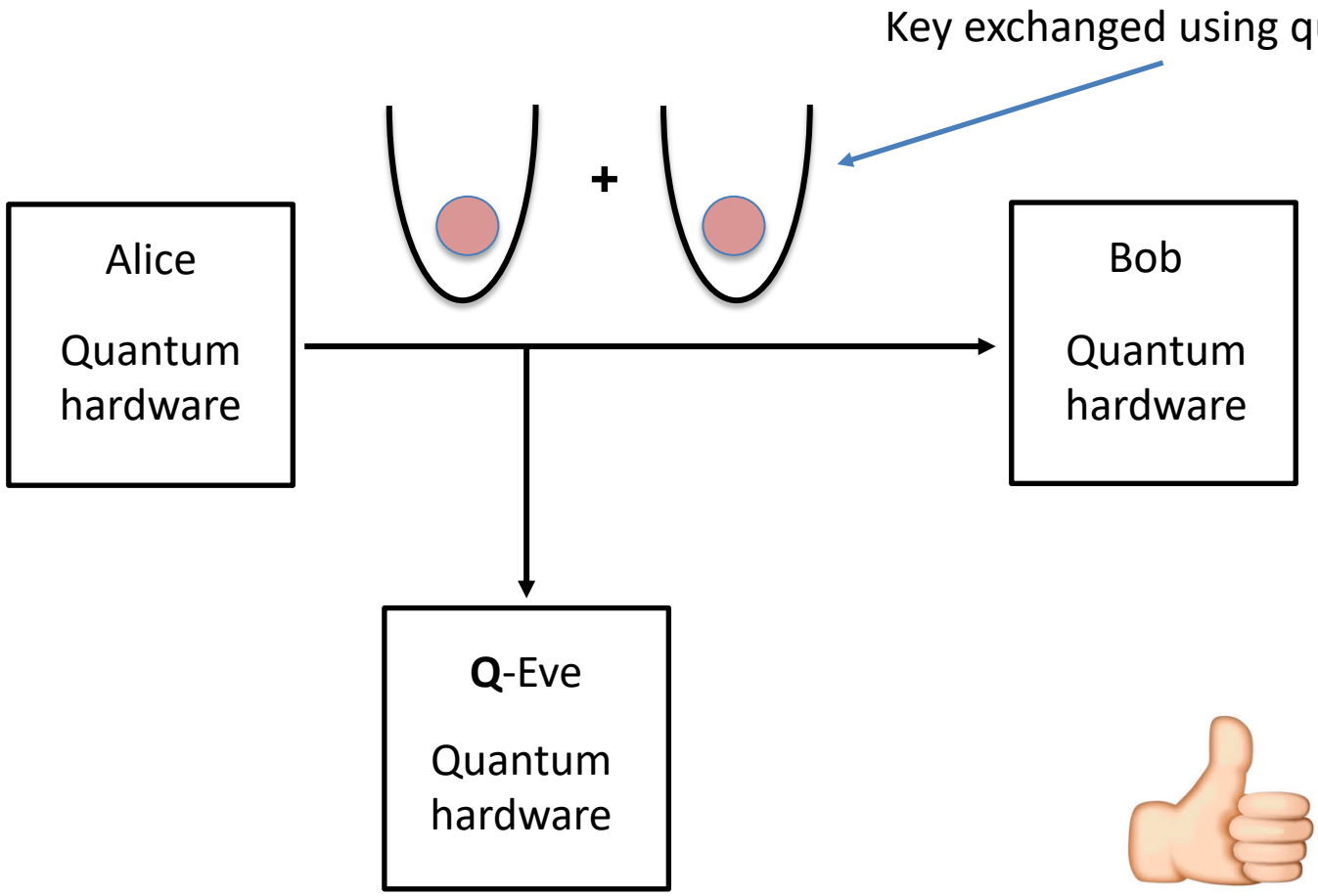


Same paradigm, one simply needs to change the one-way function.

Quantum key distribution



Quantum key distribution



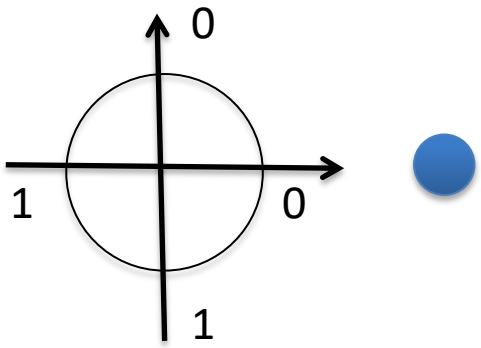
The eavesdropper, when measuring the quantum particles, modifies their state and is detected → **Quantum Secure!!**

Quantum key distribution

Standard schemes: Bennett-Brassard 84 (BB84) protocol

Alice

Bob



- Alice encodes a random bit into a two-dimensional quantum particle. The basis for encoding is also chosen randomly between x and z. The particle is sent to Bob.

Quantum key distribution

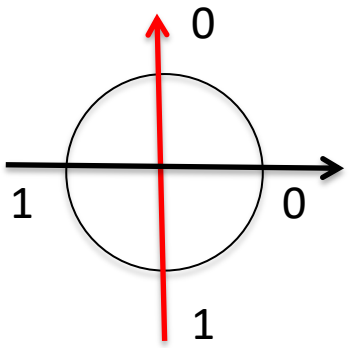
Standard schemes: Bennett-Brassard 84 (BB84) protocol

- Alice encodes a random bit into a two-dimensional quantum particle. The basis for encoding is also chosen randomly between x and z. The particle is sent to Bob.
- Bob also chooses randomly in which basis to measure the quantum particle.

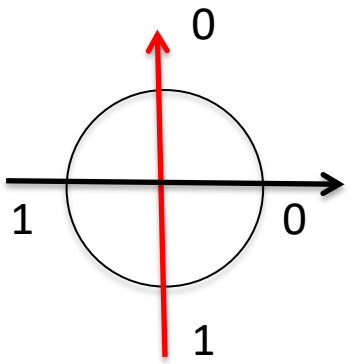
Quantum key distribution

Standard schemes: Bennett-Brassard 84 (BB84) protocol

Alice



Bob

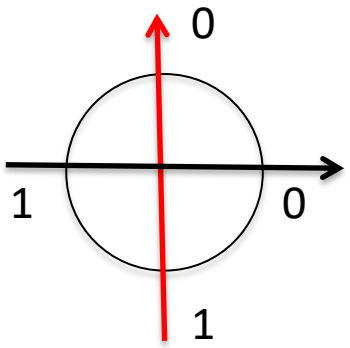


- Alice encodes a random bit into a two-dimensional quantum particle. The basis for encoding is also chosen randomly between x and z. The particle is sent to Bob.
- Bob also chooses randomly in which basis to measure the quantum particle.
- When the bases coincide the results are identical. These cases are kept.

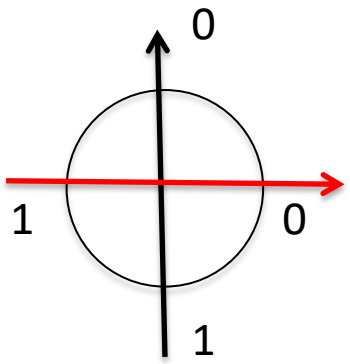
Quantum key distribution

Standard schemes: Bennett-Brassard 84 (BB84) protocol

Alice



Bob



- Alice encodes a random bit into a two-dimensional quantum particle. The basis for encoding is also chosen randomly between x and z. The particle is sent to Bob.
- Bob also chooses randomly in which basis to measure the quantum particle.
- When the bases coincide the results are identical. These cases are kept.
- When the bases are different, the results are random. These cases are removed.

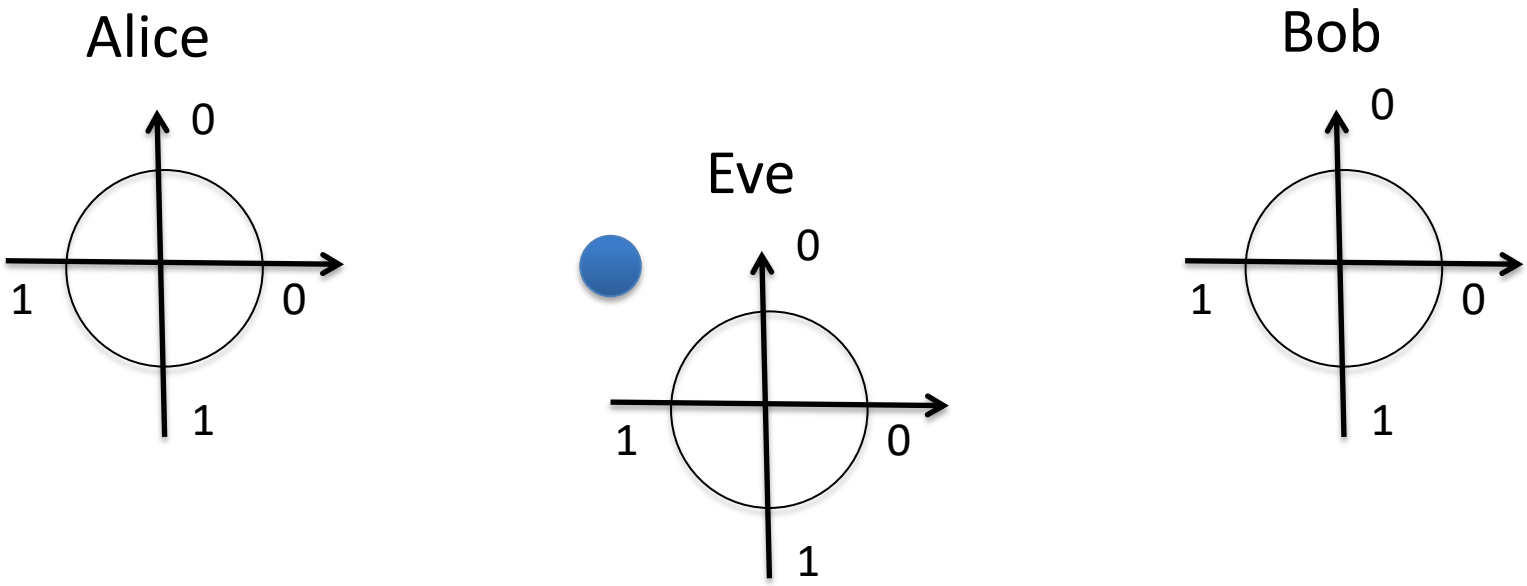
Quantum key distribution

Standard schemes: Bennett-Brassard 84 (BB84) protocol

- Alice encodes a random bit into a two-dimensional quantum particle. The basis for encoding is also chosen randomly between x and z. The particle is sent to Bob.
- Bob also chooses randomly in which basis to measure the quantum particle.
- When the bases coincide the results are identical. These cases are kept.
- When the bases are different, the results are random. These cases are removed.
- At the end, of the process, Alice and Bob share a list of perfectly correlated and random bits ➔ **a secret key**!

Quantum key distribution

Standard schemes: Bennett-Brassard 84 (BB84) protocol



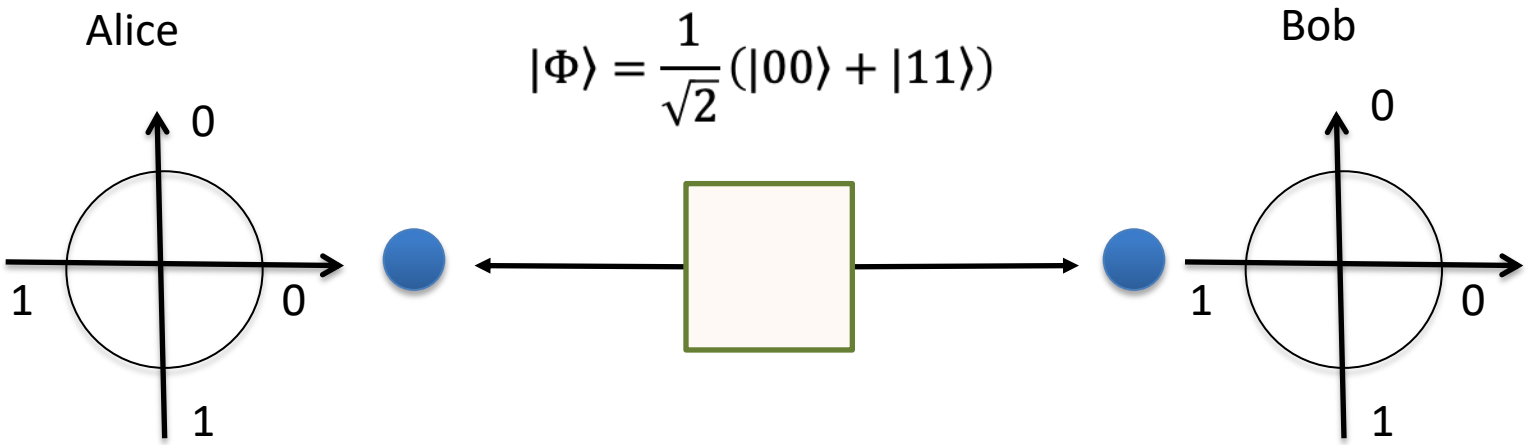
Eve intercepts the quantum particles while they travel through the channel.
However, she does not know in which basis to measure!
Heisenberg uncertainty principle: impossible to perform two non-commuting measurements.

Ekert 91

In 1991 Artur Ekert, unaware of BB84, rediscovered QKD using a completely different approach based on entanglement and Bell inequalities.

Ekert 91

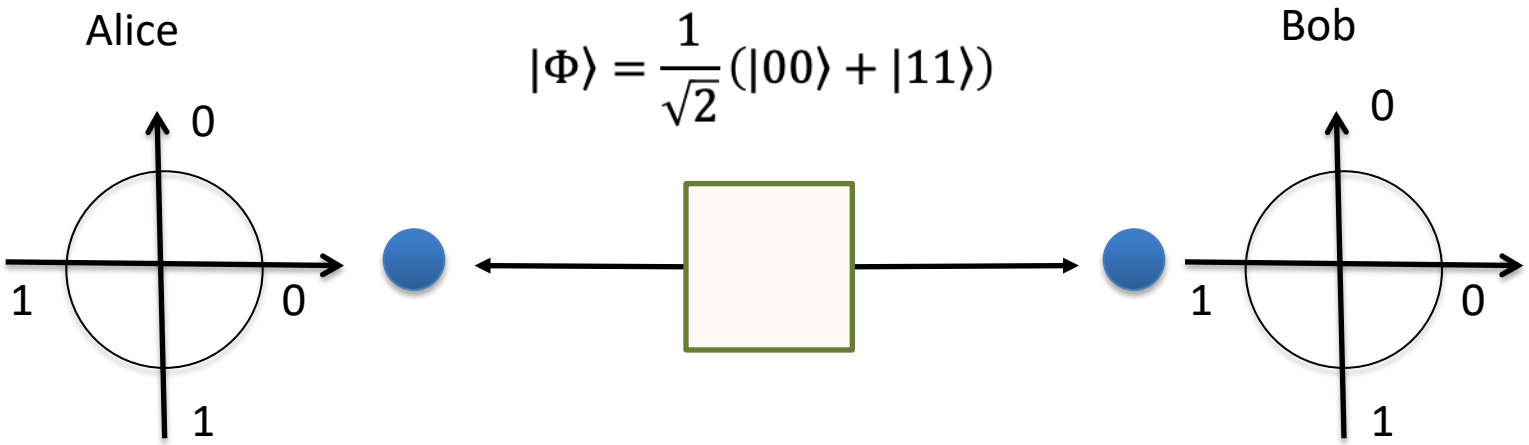
In 1991 Artur Ekert, unaware of BB84, rediscovered QKD using a completely different approach based on entanglement and Bell inequalities.



A source prepares a maximally entangled state of two qubits and sends one particle to Alice and Bob. They observe the violation of a Bell inequality.

Ekert 91

In 1991 Artur Ekert, unaware of BB84, rediscovered QKD using a completely different approach based on entanglement and Bell inequalities.



A source prepares a maximally entangled state of two qubits and sends one particle to Alice and Bob. They observe the violation of a Bell inequality.

Idea of security: an attack deteriorates the quantum correlations observed between Alice and Bob, witnessed by the Bell inequality violation.

Quantum cryptography

- Quantum Cryptography protocols are based on physical security.
- Assumption: Quantum Mechanics offers a correct physical description of the devices.
- No assumption is required on the eavesdropper's power, provided it does not contradict any quantum law.
- Using this (these) assumption(s), the security of the schemes can be proven.

Quantum hacking

NATURE PHOTONICS | LETTER

Hacking commercial quantum cryptography systems by tailored bright illumination

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

Published online 29 August 2010 | Nature | doi:10.1038/news.2010.436

News

Hackers blind quantum cryptographers

Lasers crack commercial encryption systems, leaving no trace.

Zeeya Merali

Quantum hacking

NATURE PHOTONICS | LETTER

Hacking commercial quantum cryptography systems by tailored bright illumination

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

Published online 29 August 2010 | Nature | doi:10.1038/news.2010.436

News

Hackers blind quantum cryptographers

Lasers crack commercial encryption systems, leaving no trace.

Zeeya Merali

How come?!

Quantum hacking

Quantum hacking attacks break the implementation, not the principle.

Quantum hacking

Quantum hacking attacks break the implementation, not the principle.

Theory

- Prepare states in a Hilbert space of dimension two.
- Measure observables in the same space, e.g. spin-1/2 measurements.

Quantum hacking

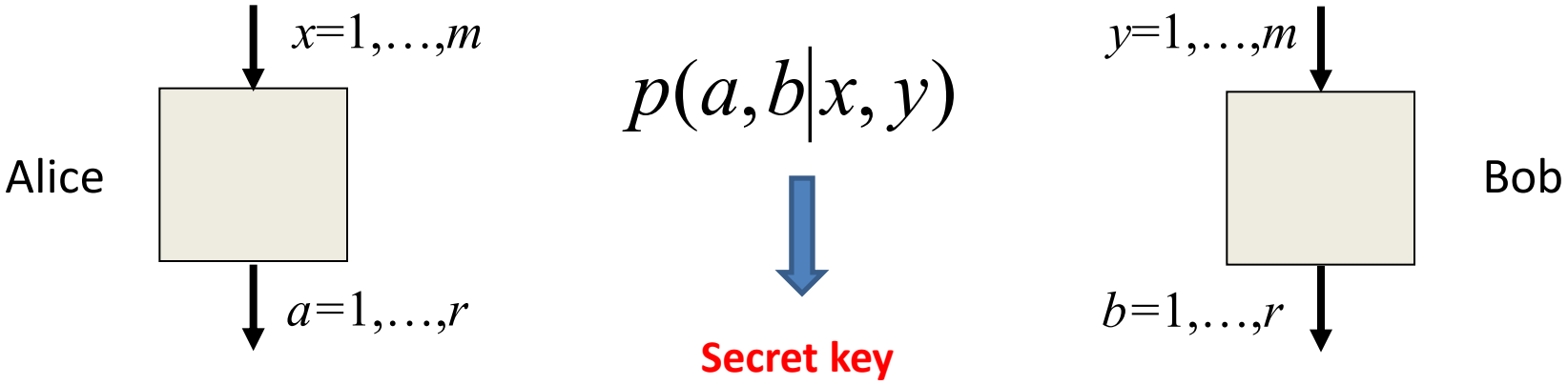
Quantum hacking attacks break the implementation, not the principle.

Theory	Implementation
• Prepare states in a Hilbert space of dimension two. • Measure observables in the same space, e.g. spin-1/2 measurements.	• Prepare states using an attenuated laser source. • Measure polarization of light using single-photon detectors.

Moral: the unavoidable mismatch between theoretical requirements and implementation is an important weakness in quantum information protocols, especially in adversarial scenarios. Physical details become a weakness!

A solution to the hacking problem

Device-Independent Quantum Key Distribution

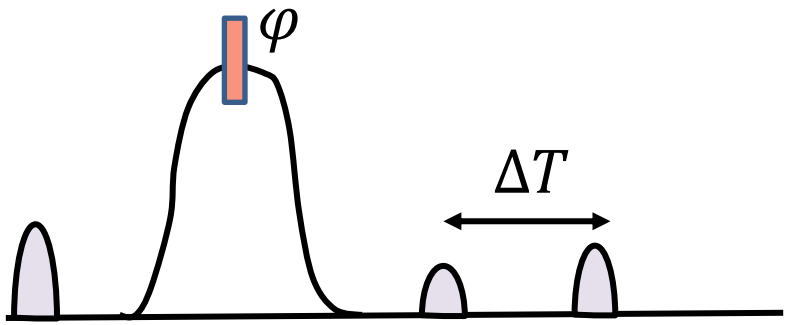


Protocols that establish a secure key only from the observed correlations and without making any assumption about the internal working of the devices used to obtain these correlations.

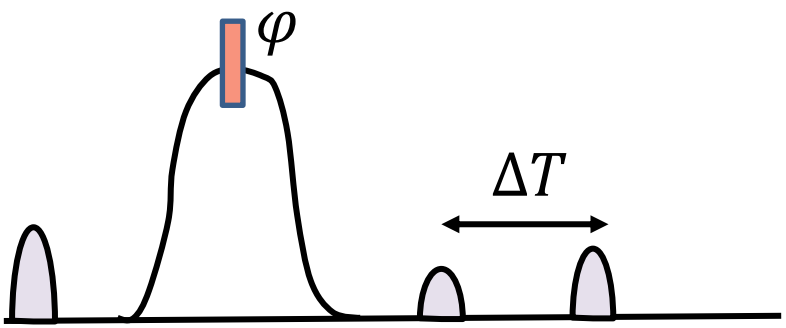
A. Acín *et al.*, Phys. Rev. Lett. 98, 230501 (2007)

Implementations

Example: time-bin qubits

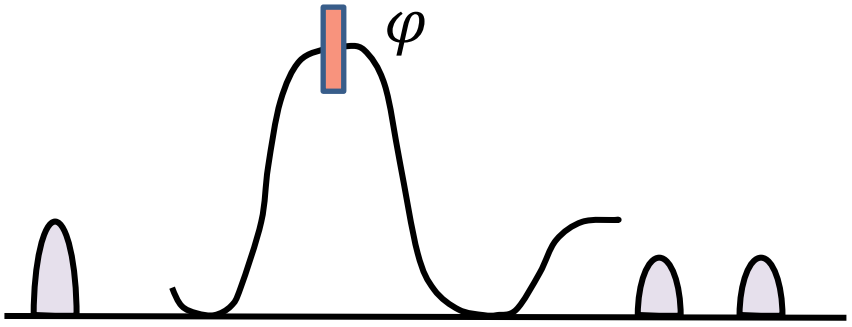


Example: time-bin qubits



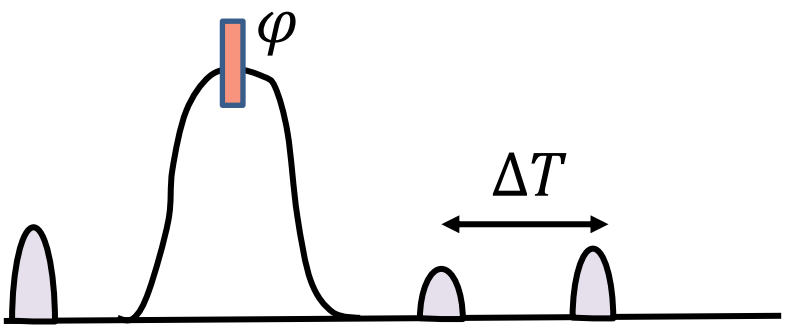
T

$\sqrt{T}|s\rangle + \sqrt{R}e^{i\varphi}|\ell\rangle$



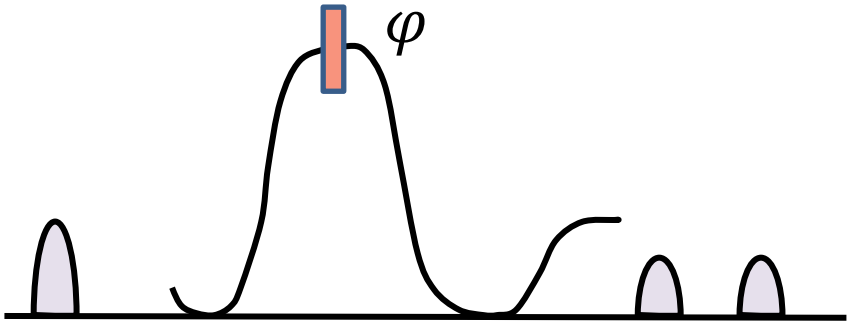
$T = \frac{1}{2}$ $T = \frac{1}{2}$

Example: time-bin qubits



T

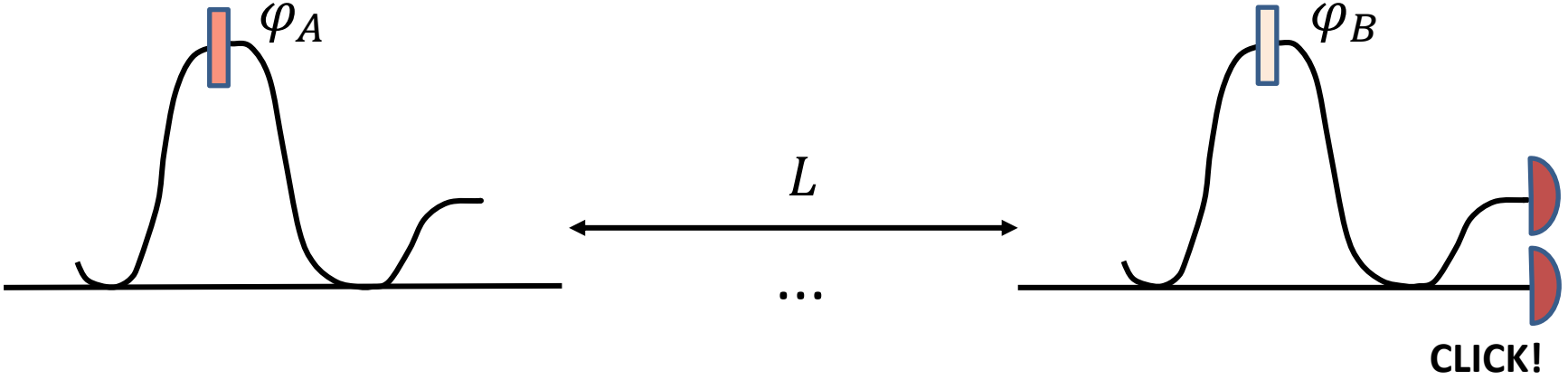
$\sqrt{T}|s\rangle + \sqrt{R}e^{i\varphi}|\ell\rangle$



$T = \frac{1}{2}$ $T = \frac{1}{2}$

Alice

Bob



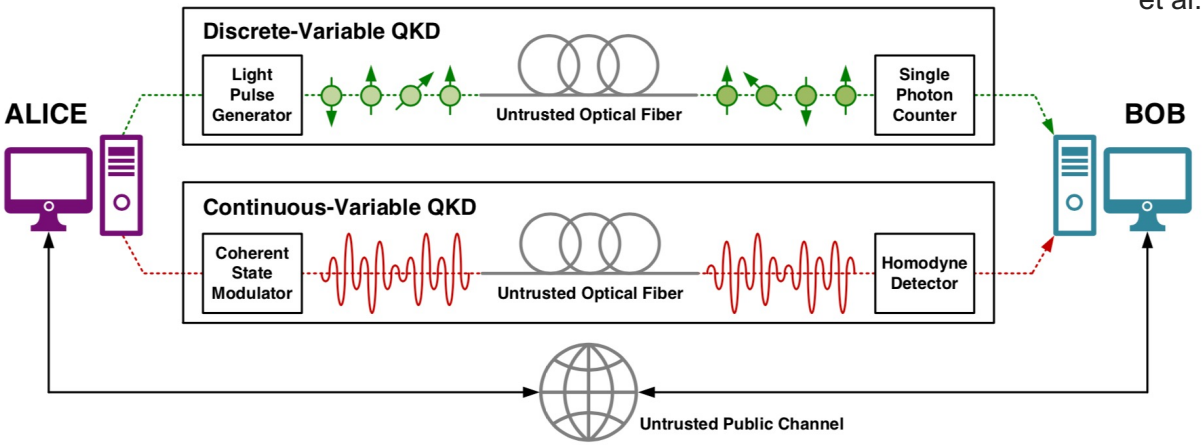
Implementations

Free space quantum key distribution

Satellite quantum key distribution

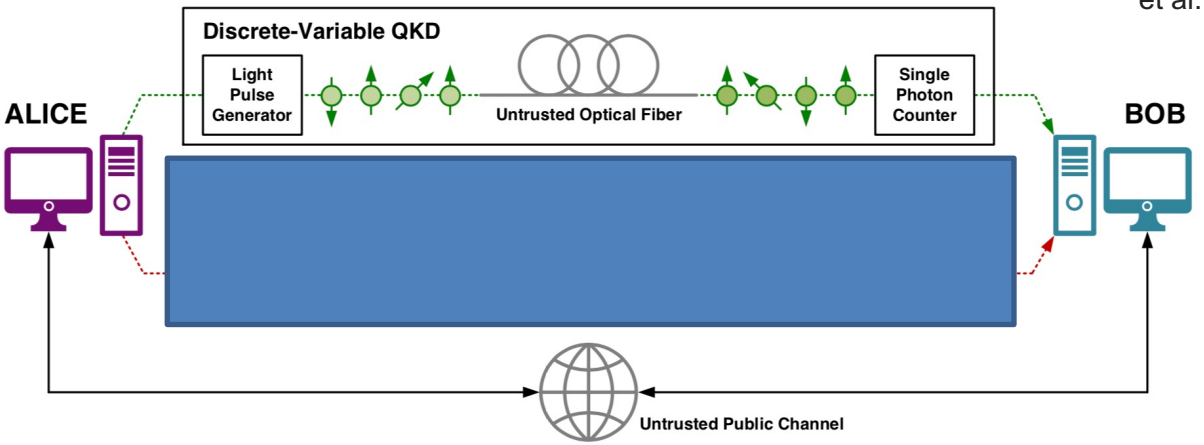
Fiber-optic implementations

Picture taken from Milicevic, et al. Arxiv 1702.07740



Fiber-optic implementations

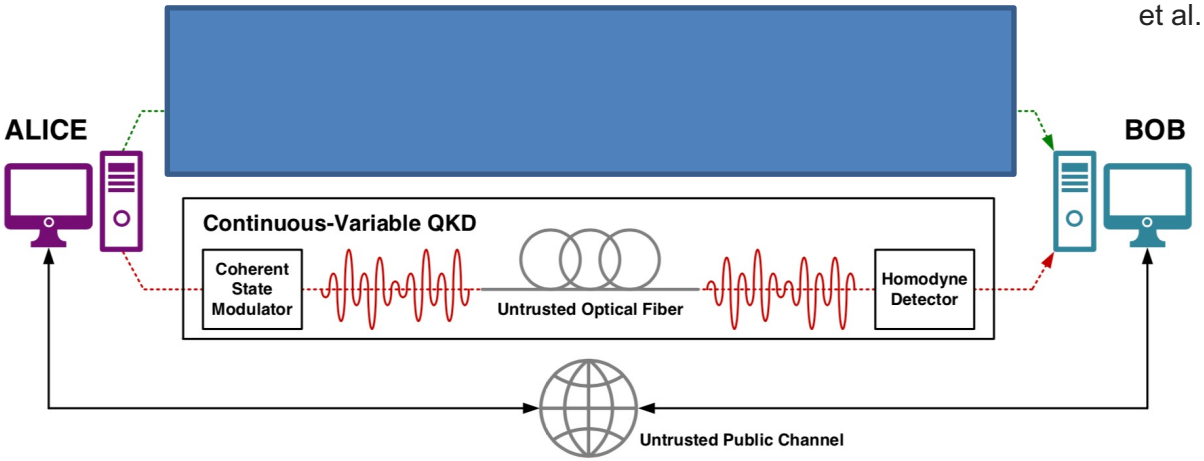
Picture taken from Milicevic, et al. Arxiv 1702.07740



- The key is encoded on a degree of freedom, say polarization or phase, of a coherent state with < 1 photon on average.
- It requires single-photon detection.
- Easy post-processing, well-established security proofs.
- Difficult co-existence with existing infrastructures (often dark fiber).
- Decent key rates at long distances: 10 bps / 10kbps over 400 / 250 km.

Fiber-optic implementations

Picture taken from Milicevic, et al. Arxiv 1702.07740



- The key is encoded on the quadratures of the electromagnetic field, with 10 photons per pulse.
- System based on coherent detection techniques used in classical communications.
- Complex post-processing, room for improvement in security proofs.
- Potentially suitable for seamless integration in current classical networks.
- Good key rates at short distances: 10 bps / 10kbps over 200 / 100 km.

Pros and cons

👍 Provable security based on the laws of quantum physics.

👍 Hackers need to know quantum physics and master quantum hardware.

👎 Expensive.

👎 It requires authentication.

👎 It “just” establishes a secret key between two distant honest users in a point-to-point configuration.

Standard cryptography

- Standard cryptography is today based on **computational security**.
- Assumption: eavesdropper computational power is limited.
- The implementation of these schemes is easy (software).
- Risk 1: quantum computers sheds doubts on the long-term applicability of some of these schemes: factoring is easy on quantum computers. Security to the future compromised.
- Risk 2: is there a proof that factoring is hard? NO! Can we exclude that tomorrow a very smart adversary will find an algorithm for efficient factorization? NO!

Post-quantum cryptography

- Post-quantum cryptography is still based on **computational security**.
- Assumption: eavesdropper **quantum** computational power is limited.
- The implementation of these schemes is easy (software). One only needs to change the algorithm.
- The algorithm is based on one-way quantum functions.
- Risk: is there a proof that any of these functions is hard? NO! Can we exclude that tomorrow a very smart adversary will find a quantum, or even classical algorithm to solve any of these functions? NO!

Quantum cryptography

- Quantum cryptographic is based on **(quantum) physical security**.
- The implementation of these schemes is more demanding (hardware).
- Assumption: quantum physics offers a correct description of nature at the microscopic scale.
- To break the protocol, the eavesdropper should hack the physical implementation.

Standard vs quantum cryptography

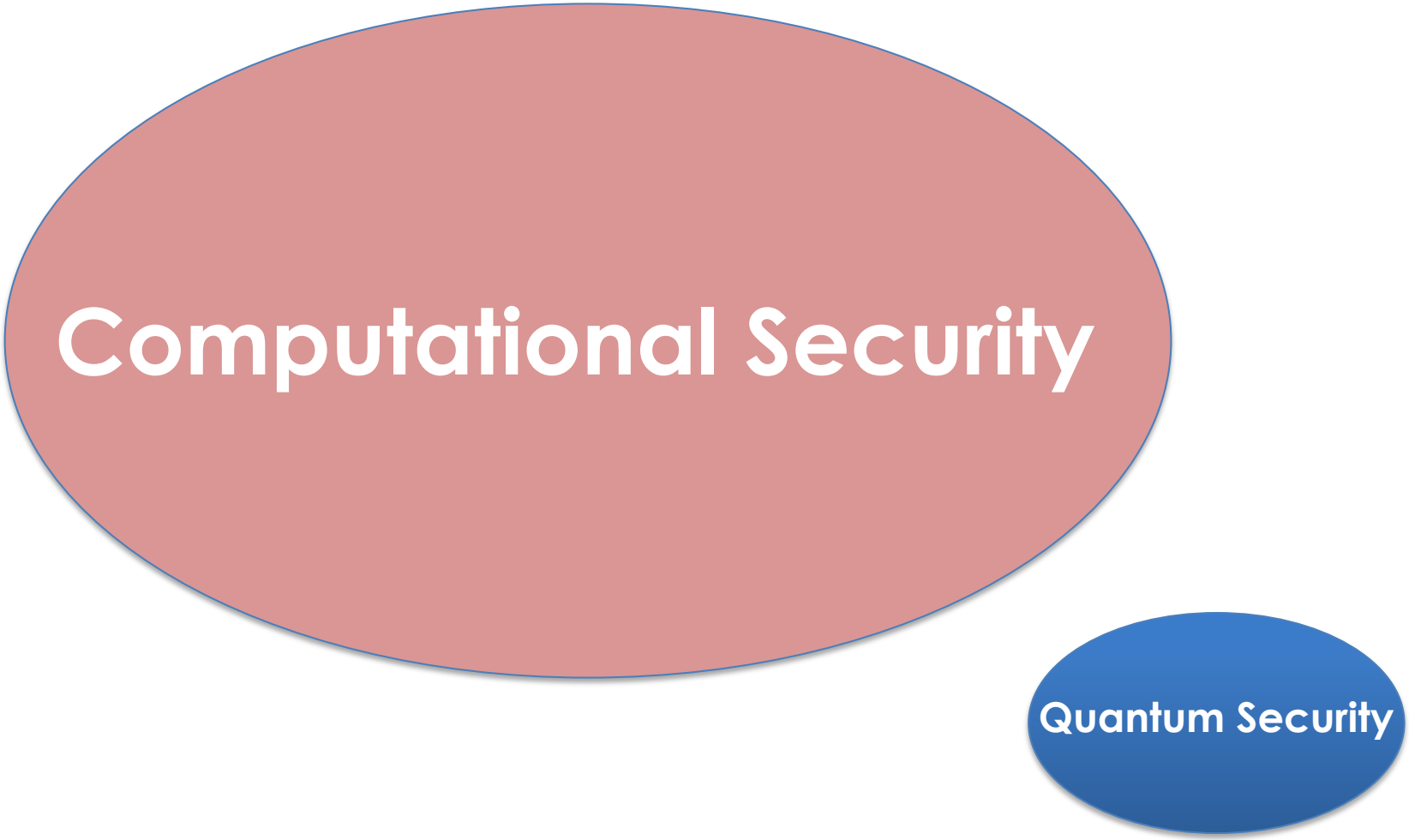
Cryptographic paradigm	Implementation	Integration	Cost	Security classical adversaries	Security quantum adversaries
Computational (RSA)	Software	Easy	Cheap	Plausible but unproven	No
QKD	Hardware	Difficult	Expensive	Proven	Proven
Post-quantum	Software	Easy	Cheap	Plausible but unproven	Plausible?

Standard vs quantum cryptography

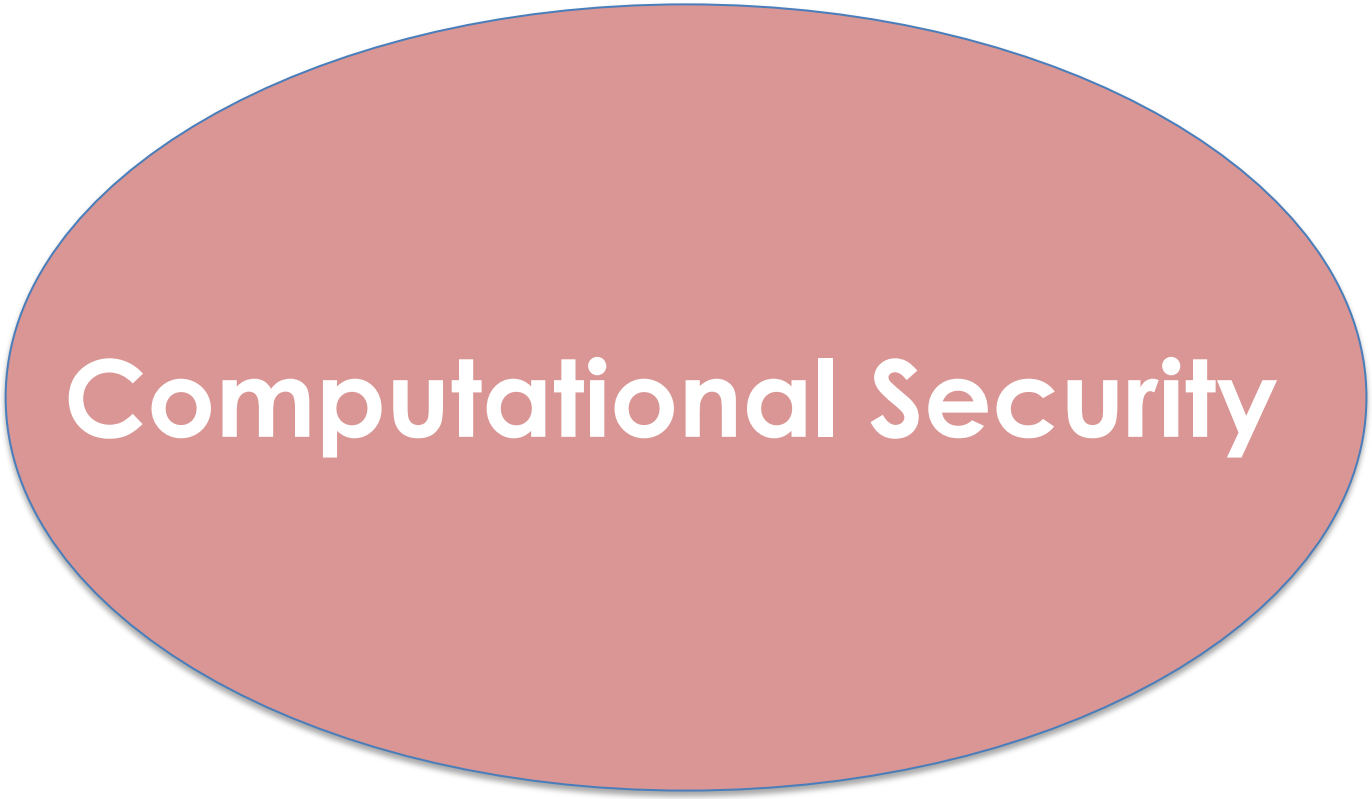
Cryptographic paradigm	Implementation	Integration	Cost	Security classical adversaries	Security quantum adversaries
Computational (RSA)	Software	Easy	Cheap	Plausible but unproven	No
QKD	Hardware	Difficult	Expensive	Proven	Proven
Post-quantum	Software	Easy	Cheap	Plausible but unproven	Plausible?

Will quantum cryptography ever replace standard cryptography?

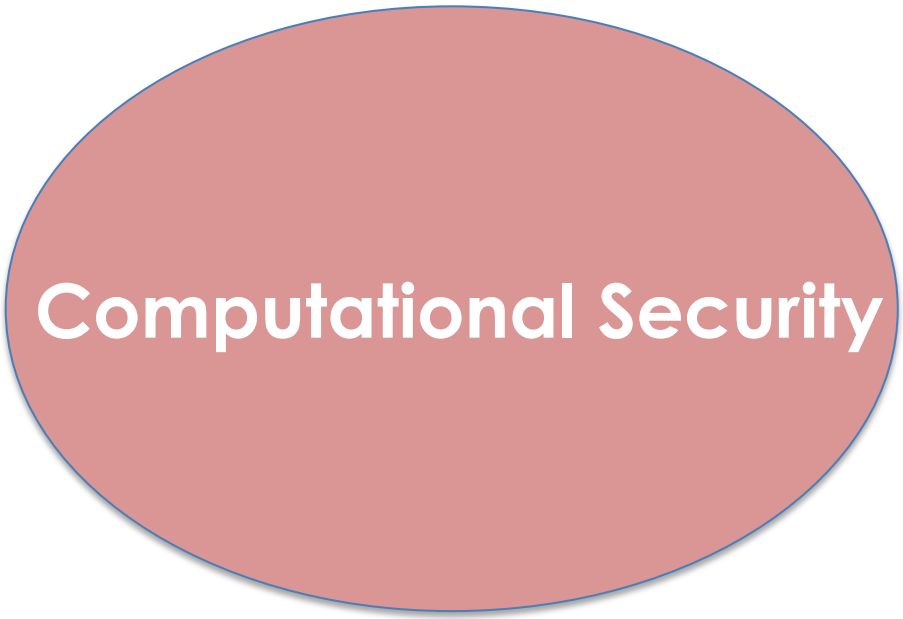
Crypto today

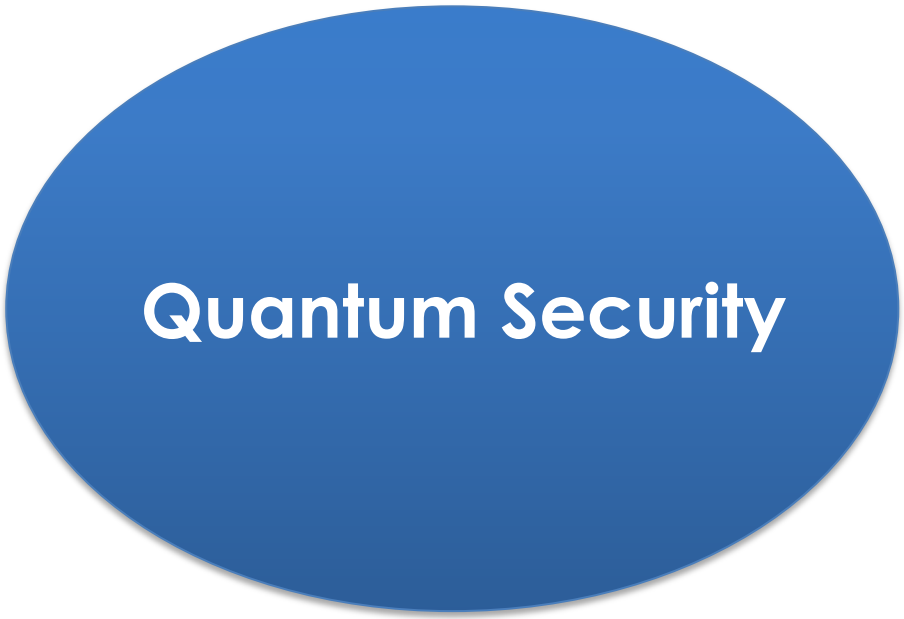


Crypto today



Quantum cryptography: an opportunity





Challenges

- Feasible protocols more robust against hacking attacks
- Integration with existing infrastructures
- Longer distances: quantum internet
- Use cases
- Other applications of quantum physics in cryptography

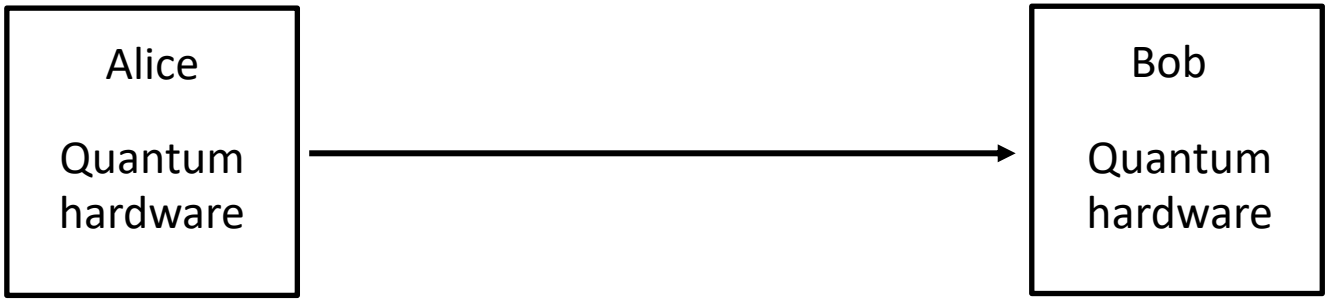
Challenges

- Feasible protocols more robust against hacking attacks
- Integration with existing infrastructures
- Longer distances: quantum internet

Implementations

- Use cases
- Other applications of quantum physics in cryptography

Implementation challenges

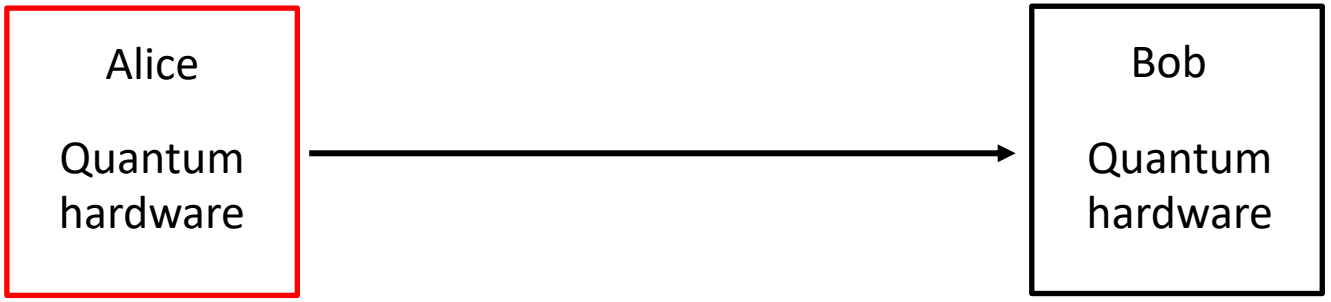


Implementation challenges

Channel: it can be free space or fibres. Not in our hands, so not much to be done here. However, it imposes many requirements on the implementation:

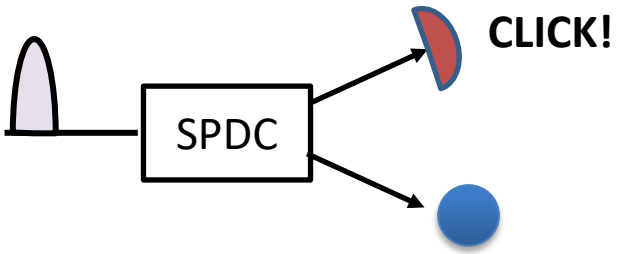
- Wavelengths.
- Quantum degree of freedom.
- Rate. E.g. in fibre optics: $R \sim f\eta$ with $\eta \sim 10^{-\frac{\alpha L}{10}}$. Good values are $\alpha \sim 0.02$ dB/km, which gives $\eta \sim 1/2$ at $L \sim 15$ km, but $\eta \sim 1/64$ at $L \sim 90$ km.

Implementation challenges

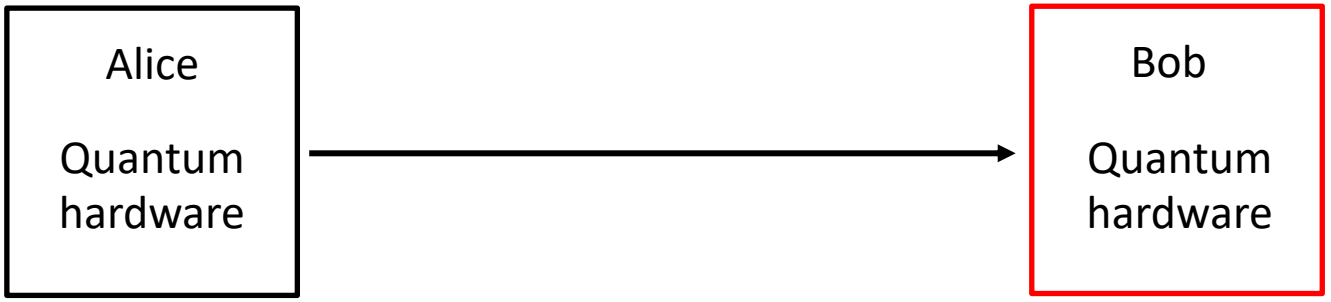


Good quantum sources: good performance and control, and adapted to the channel properties.

- Single and entangled photon sources.
- On demand or, at least, heralded. Example:
- Light (satellite), cheap, room temperature,…



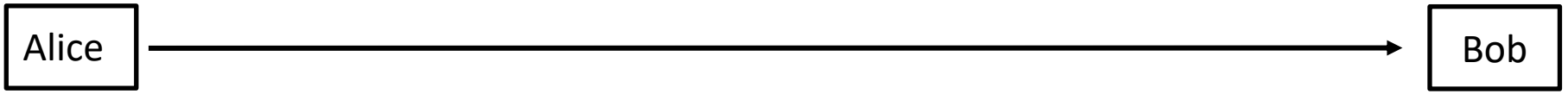
Implementation challenges



Good light detection schemes: good performance and control, and adapted to the channel properties.

- Single-photon or intensity detectors.
- Light (satellite), cheap, room temperature, good collection…

Implementation challenges



Even if all these nice devices are developed, at long distances, direct quantum information transmission is effectively impossible.

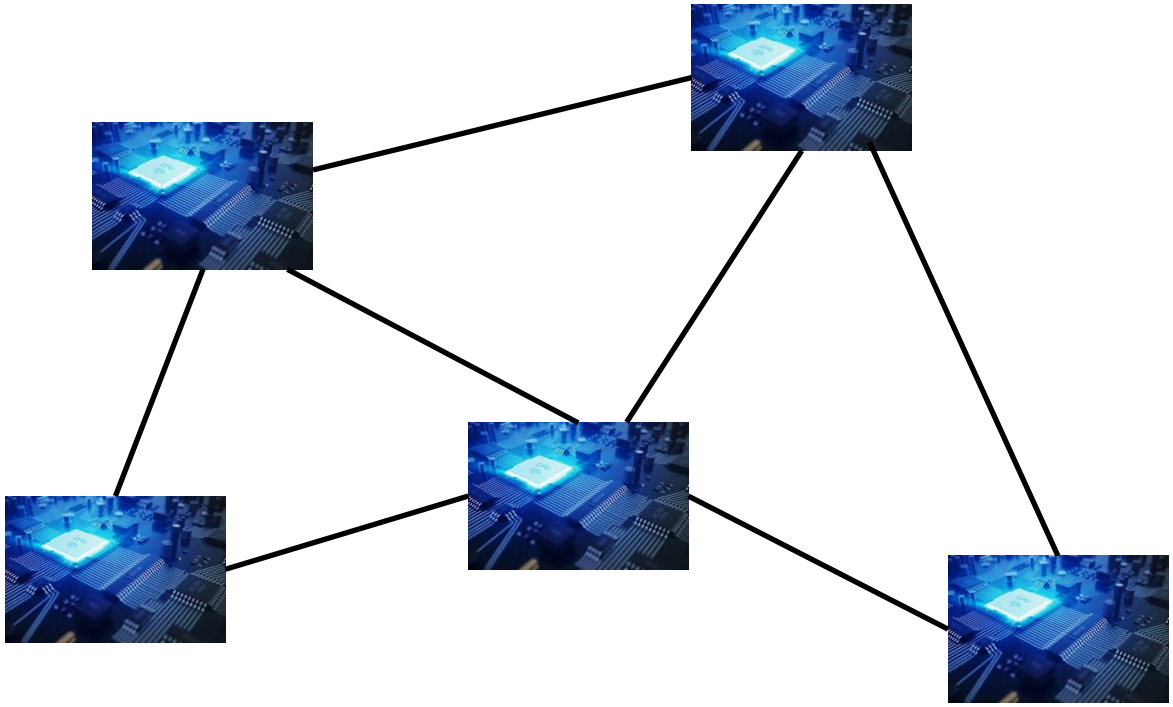
Implementation challenges

Even if all these nice devices are developed, at long distances, direct quantum information transmission is effectively impossible.

Solutions: satellites or **quantum repeaters**.

- Quantum memories: store quantum information in a reliable way so that it can be extracted on demand.
- Light-matter interface at the quantum level.

The quantum internet



Lots of relevant quantum technologies need to be developed!