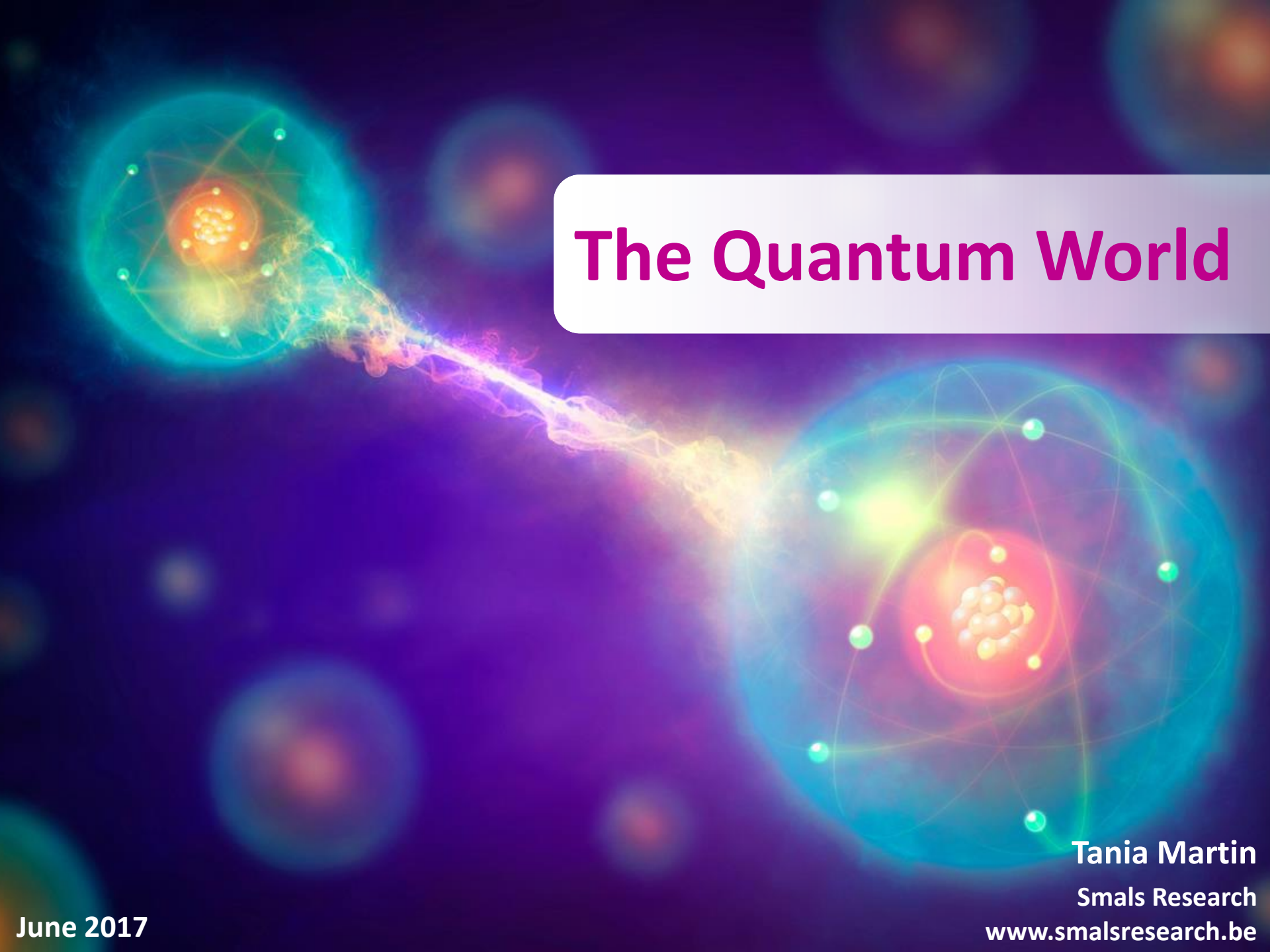


The Quantum World

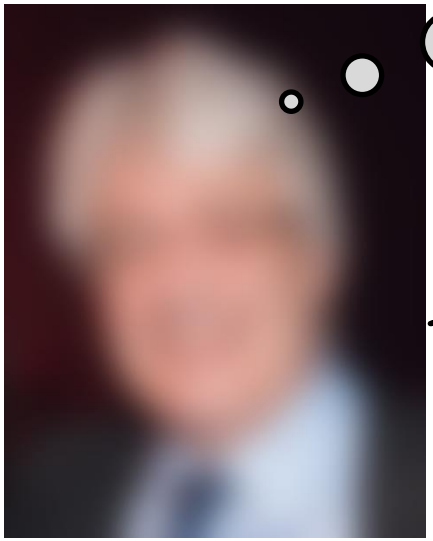
Tania Martin
Smals Research
www.smalsresearch.be

June 2017

Hypothetical scenario

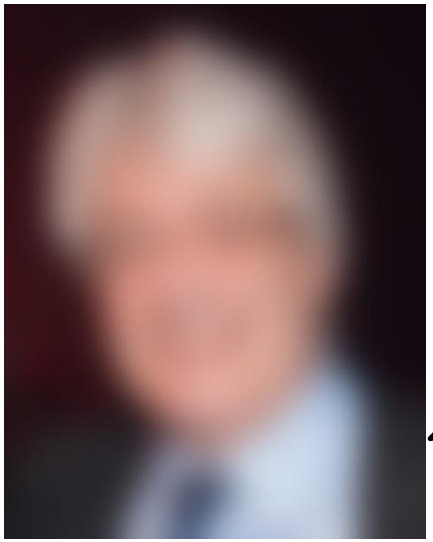
How is your company responding to the announcement of the new commercially available quantum computer that can “break” RSA and ECC?

What the hell???
I don’t have any plan for that !!!



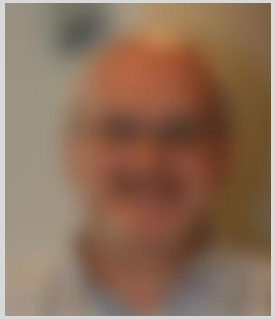
I have no comment on that…

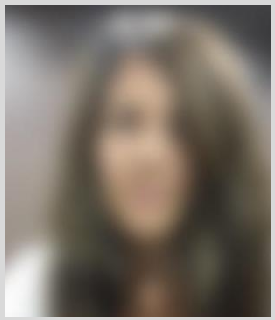
Hypothetical scenario

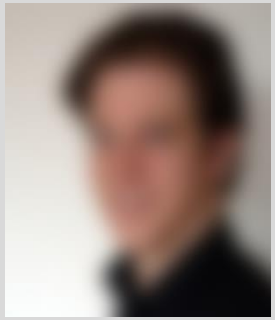


What the hell!!!
I hope for you (my dear Research team) that you have anticipated this HUGE problem that can threaten much of our business (eID, communication protocols, etc.)!!!

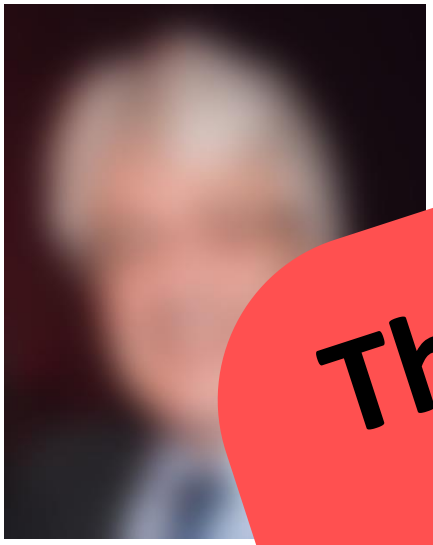
Euh, sorry but no, we decided that it was not urgent…







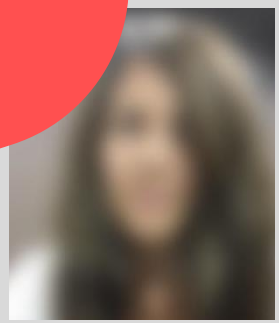
Hypothetical scenario

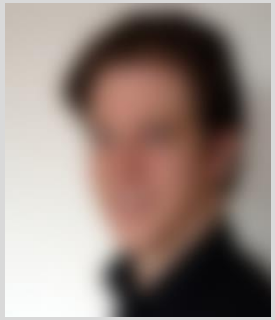


What the hell!!!
I hope for you (my dear Research team) that you hav
anticipated this HUGE
that can thr
busi

This scenario should never happen!!!

ut no, we decided
t was not urgent…





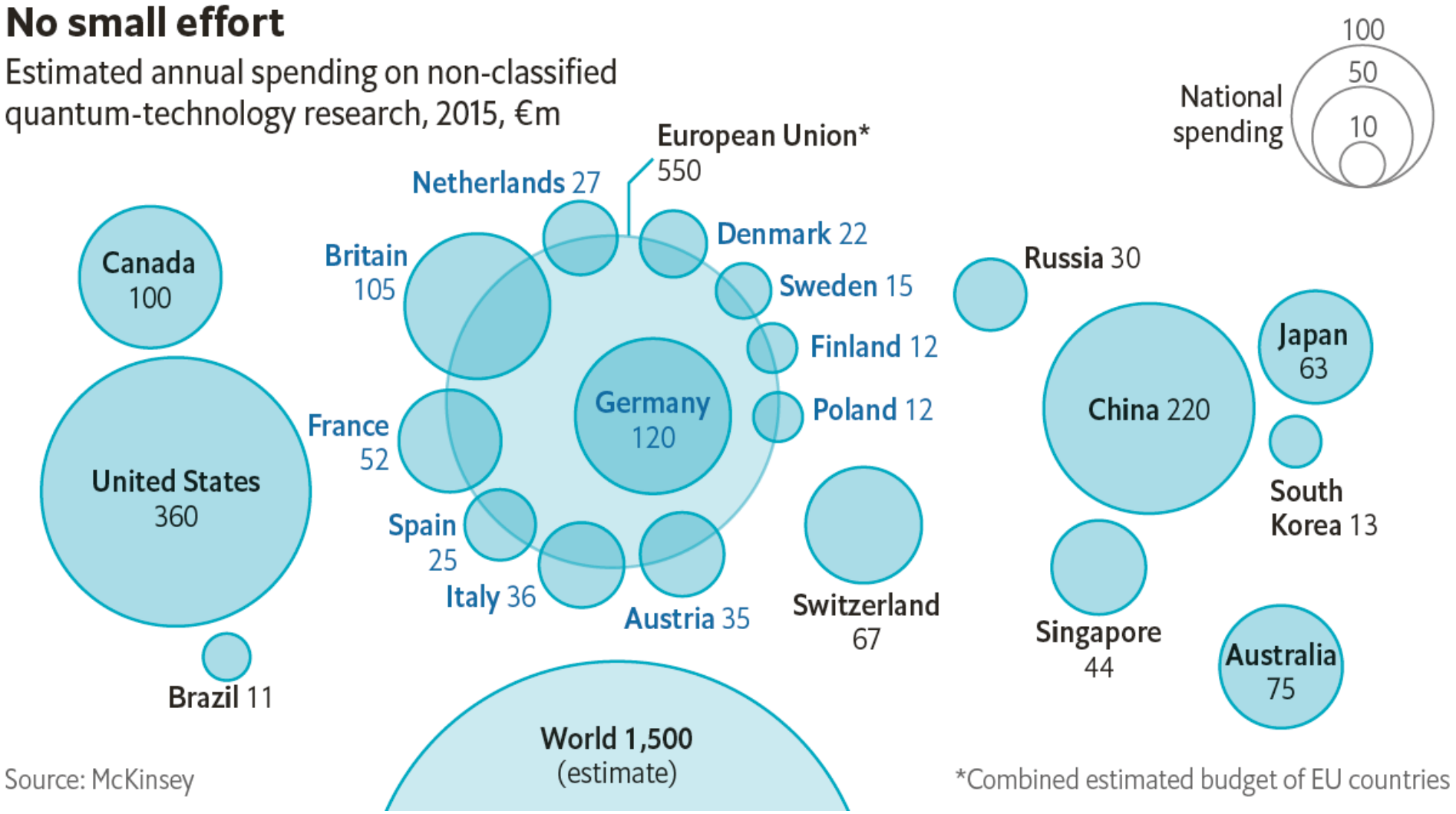
It’s too important to be set aside!!!

House Homeland Security Committee Chairman Michael McCall is calling on Congress to **increase spending on quantum computing research** to ensure that the U.S. is the first nation to employ quantum computing as a tool to decrypt data.

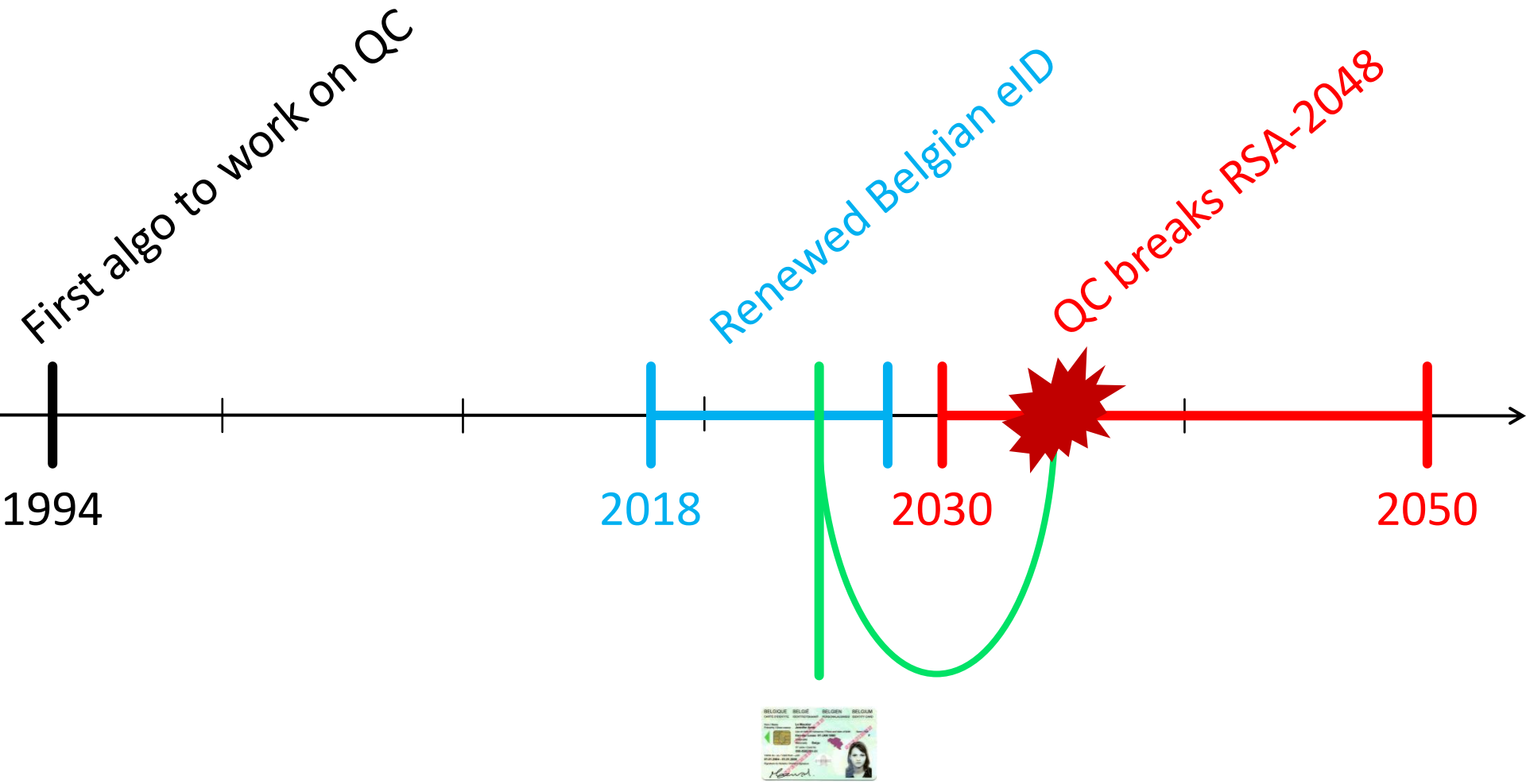
— September 2016

http://www.bankinfosecurity.com/rep-mccaul-us-must-gain-decryption-edge-a-9422

It’s too important to be set aside!!!

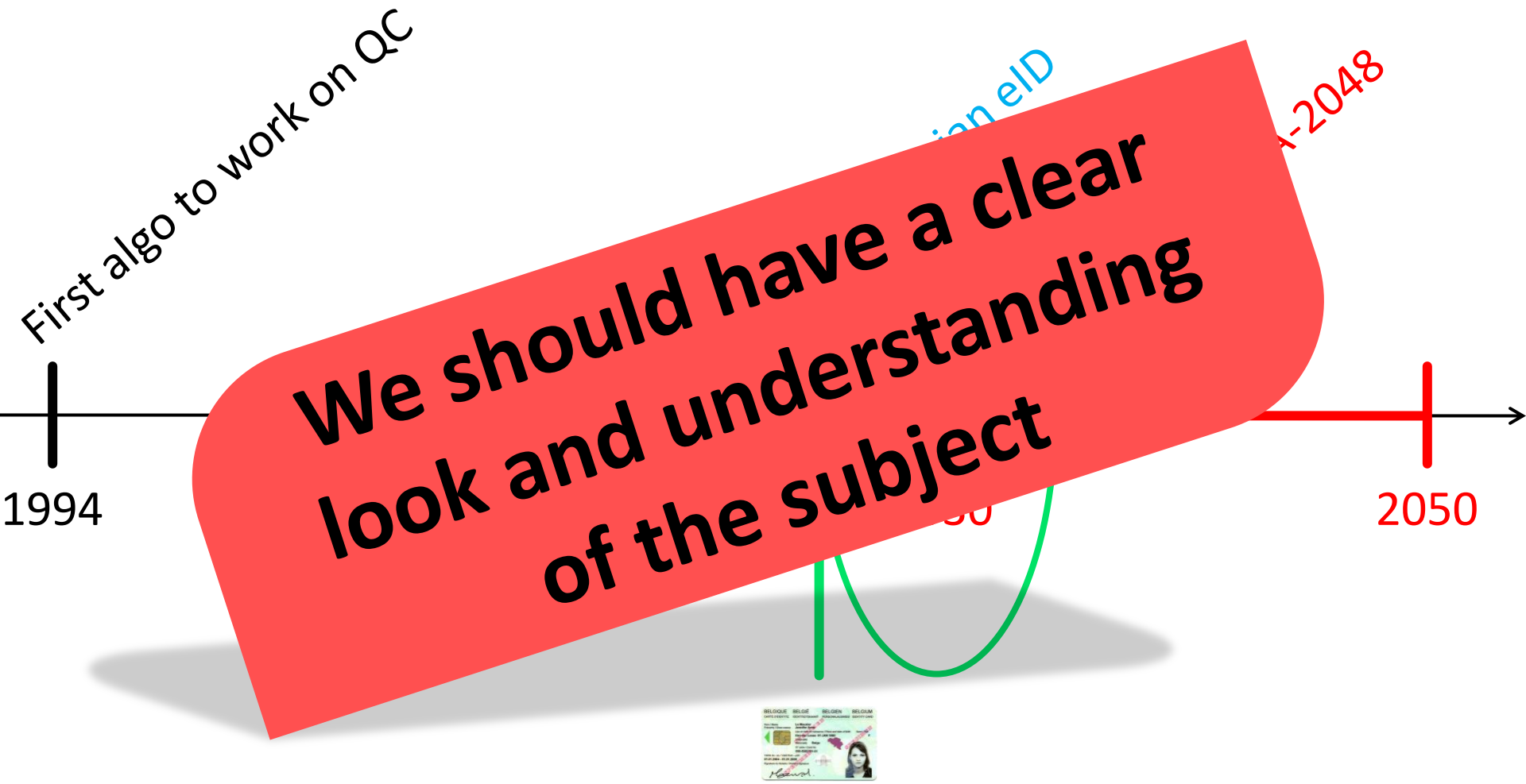


A certain future



QC = Quantum Computer

A certain future

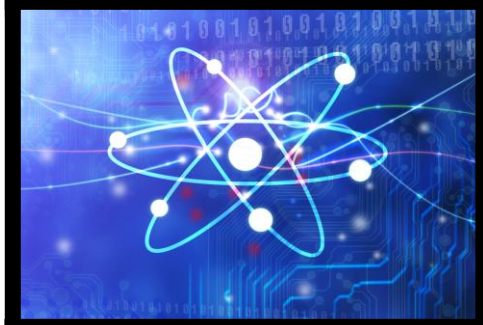


QC = Quantum Computer

AGENDA

Quantum computer technology

[*Know the enemy*]

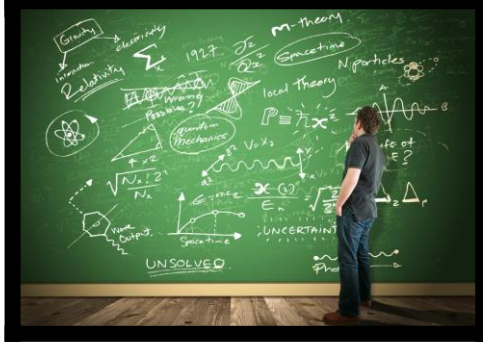


Quantum cryptography

[*Enhance cryptography*]

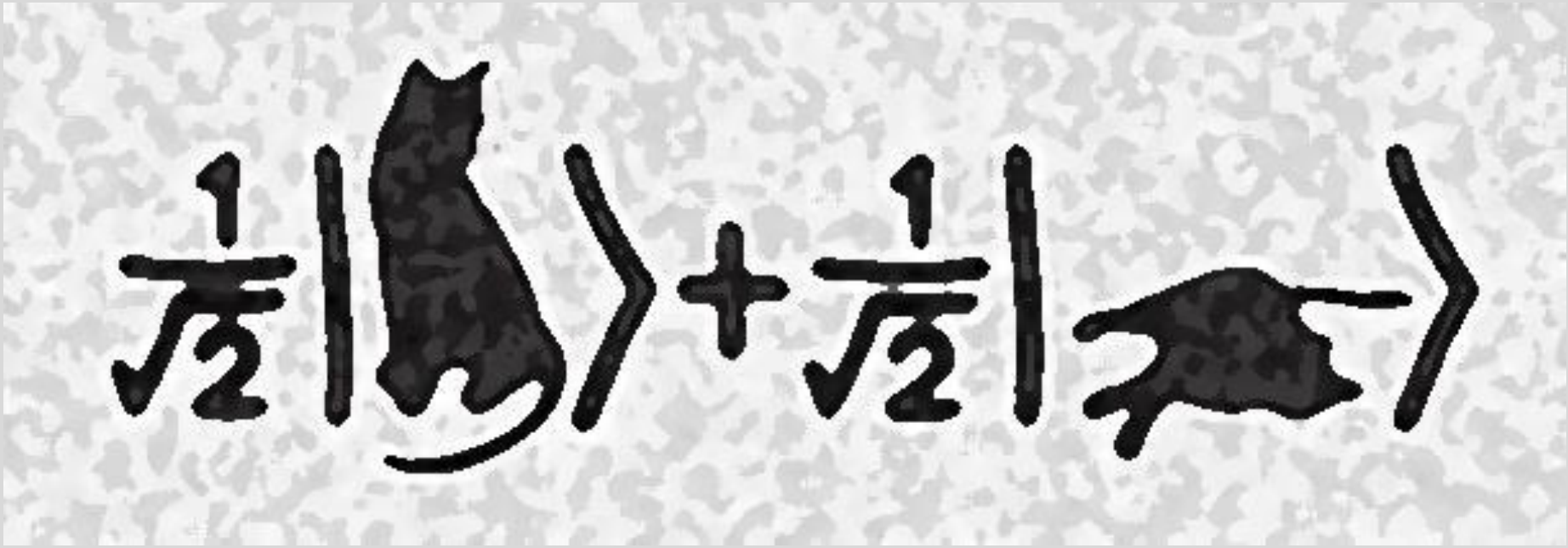
Quantum attacks

[*Break actual cryptography*]



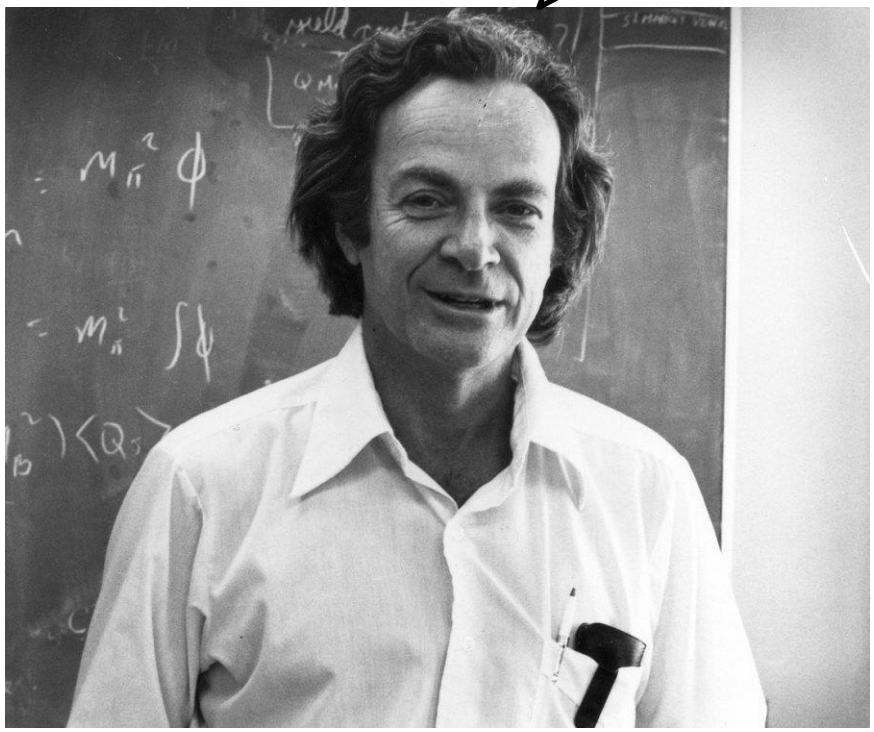
Post quantum cryptography

[*Counter quantum attacks*]



Quantum computer technology

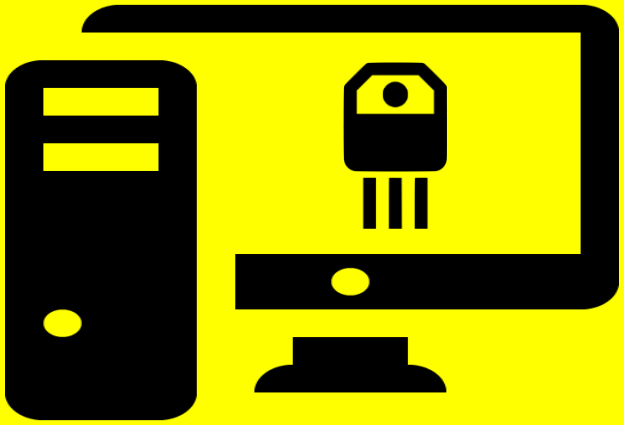
I can safely say that no one understands quantum mechanics



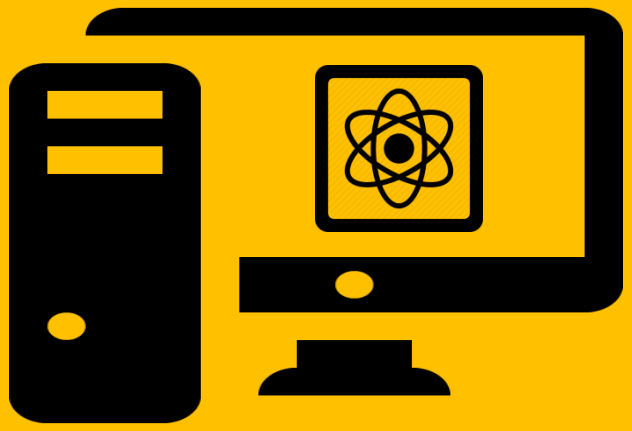
Richard Feynman
(1918-1988)

Father of the new way to conceive quantum mechanics

What is a quantum computer?



A digital computer uses **transistors** to perform computation of data

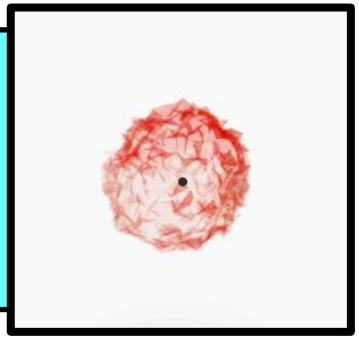


A quantum computer uses quantum properties of the **matter** to perform computation of data

Examples of used *matter*

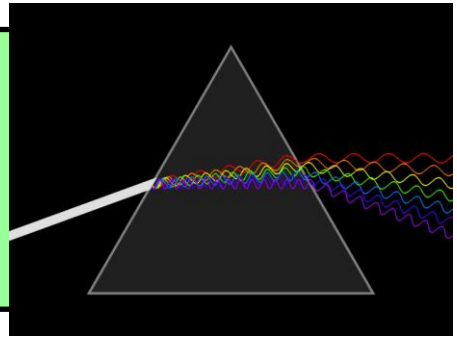
An **atom** can be

- not excited
- excited
- both



The polarization of a **photon** can be

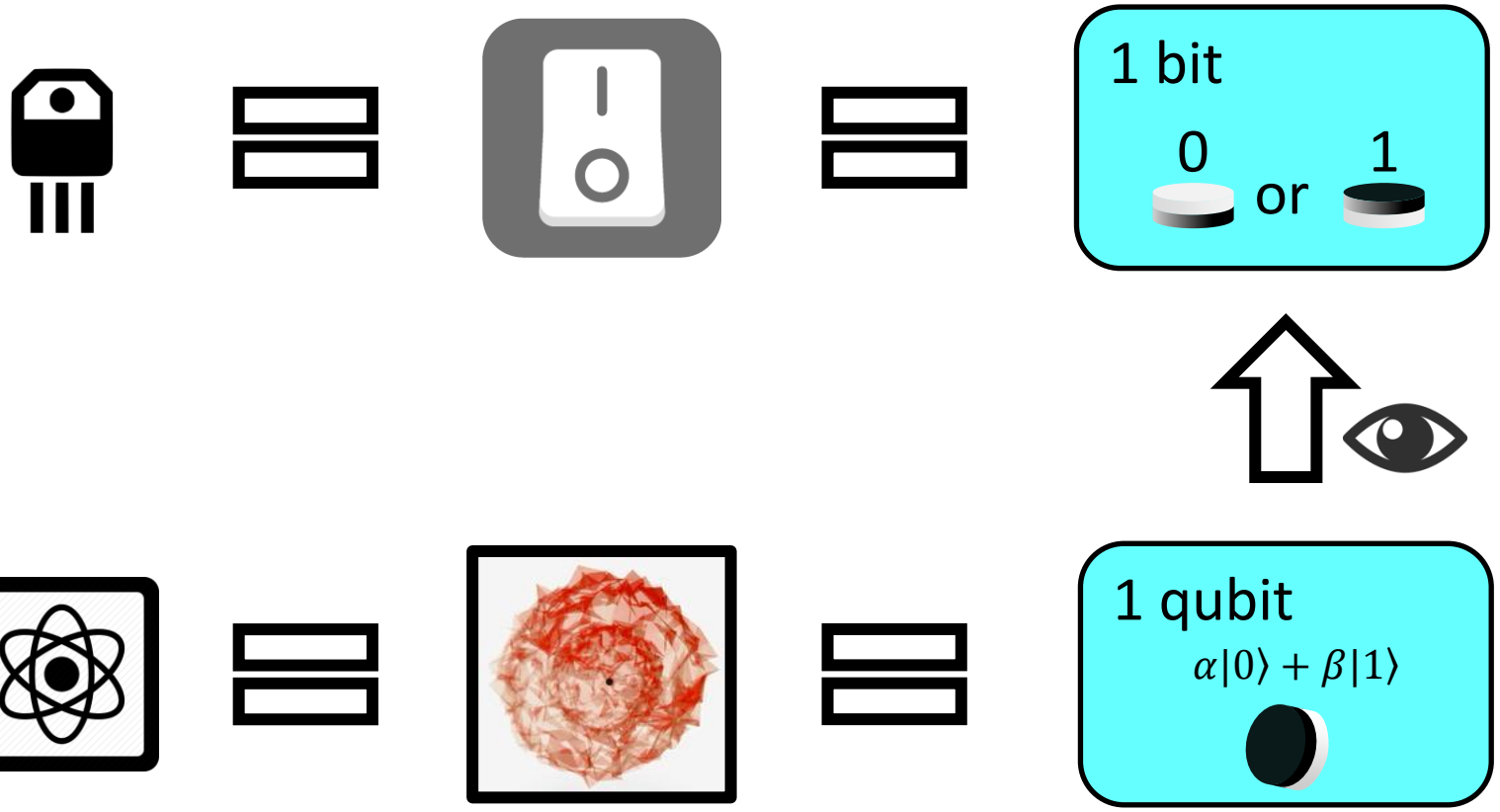
- horizontal
- vertical
- both



Formally, any matter used
in quantum mechanics can be in
a **superposition** of 2 states

Understand the superposition

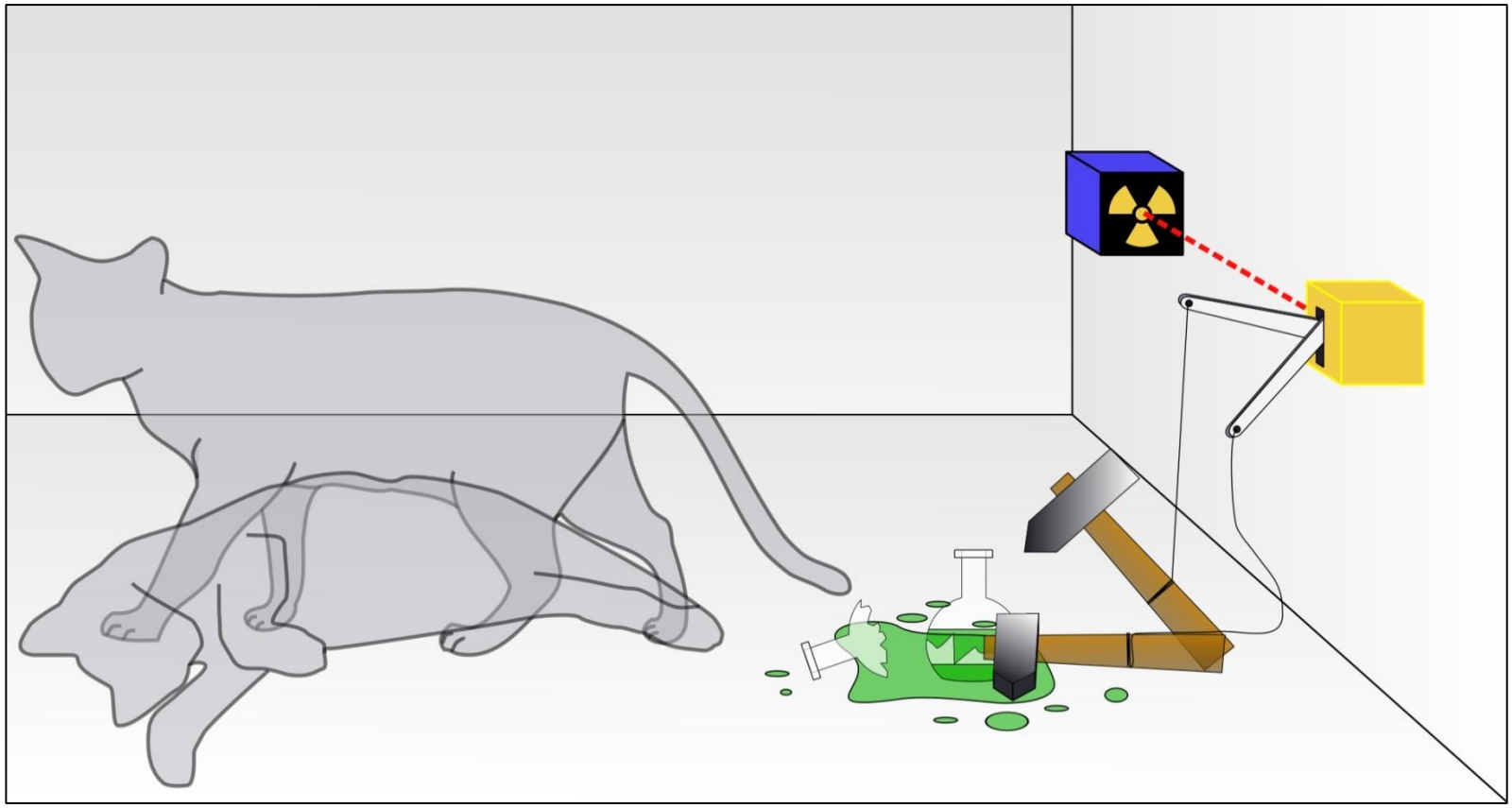
Recap



$|0\rangle$ and $|1\rangle$ are pronounced "ket 0" and "ket 1"

What does $\frac{1}{\sqrt{2}}|\text{alive}\rangle + \frac{1}{\sqrt{2}}|\text{dead}\rangle$ mean?

1. Reference to Schrödinger's cat



What does $\frac{1}{\sqrt{2}}|\text{alive}\rangle + \frac{1}{\sqrt{2}}|\text{dead}\rangle$ mean?

1

Reference to Schrödinger's cat

2

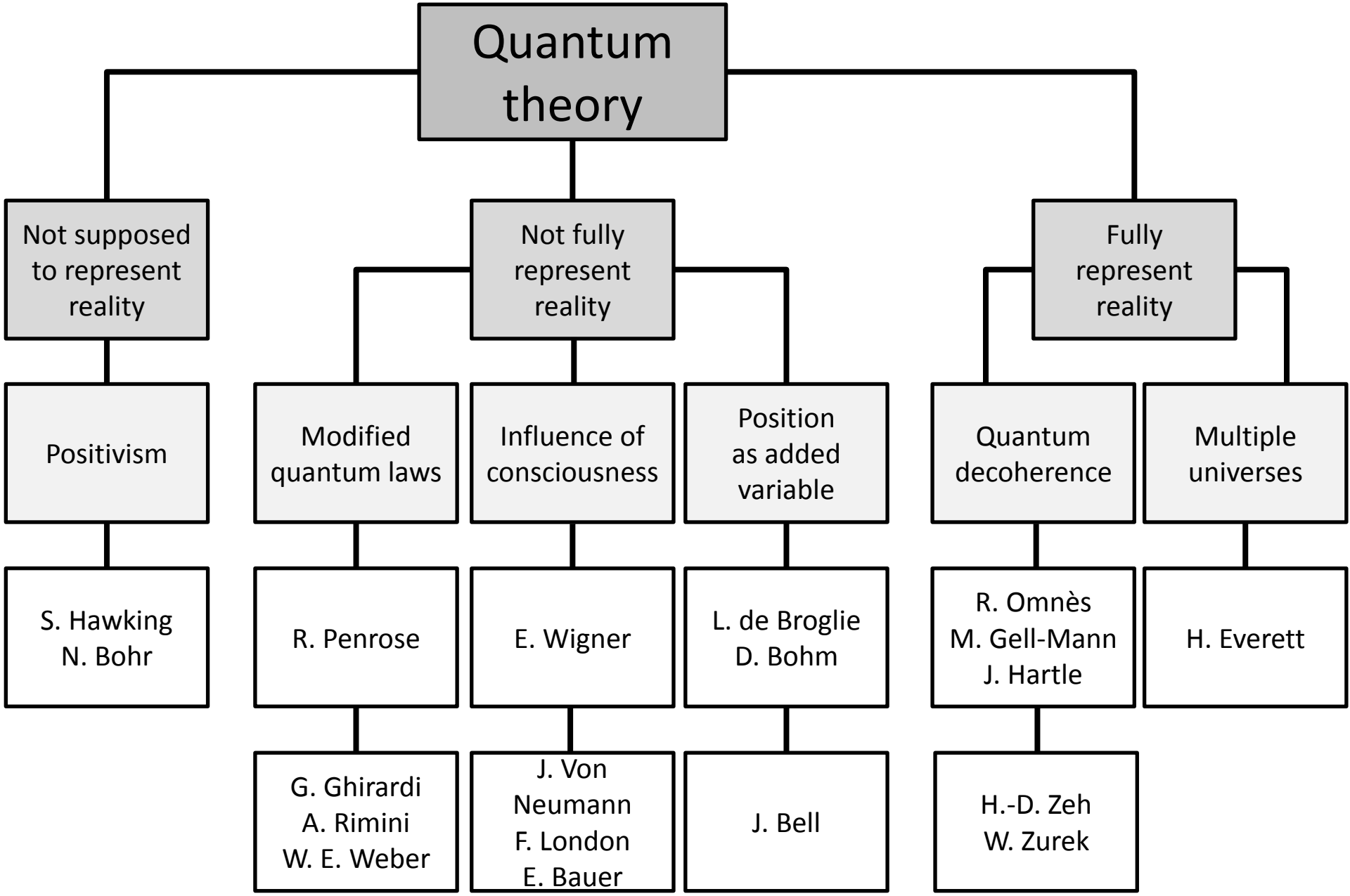
2 states:

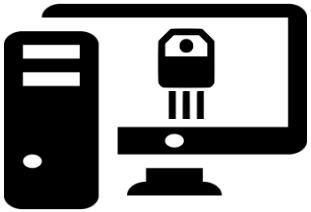
- Cat alive $|\text{alive}\rangle$
- Cat dead $|\text{dead}\rangle$

3

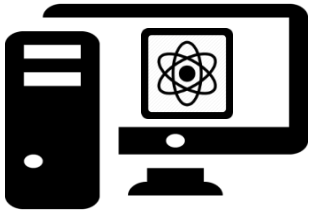
Equal probability that cat is alive or dead:

$$\alpha = \beta = \frac{1}{\sqrt{2}}$$


Quantum theory
Not supposed to represent reality
Not fully represent reality
Fully represent reality
Positivism
Modified quantum laws
Influence of consciousness
Position as added variable
Quantum decoherence
Multiple universes
S. Hawking
N. Bohr
R. Penrose
E. Wigner
L. de Broglie
D. Bohm
R. Omnès
M. Gell-Mann
J. Hartle
H. Everett
G. Ghirardi
A. Rimini
W. E. Weber
J. Von Neumann
F. London
E. Bauer
J. Bell
H.-D. Zeh
W. Zurek



vs.



1 bit

0 or 1

Either 0 or 1

1 qubit

$\alpha|0\rangle + \beta|1\rangle$

Both 0 and 1

N bits

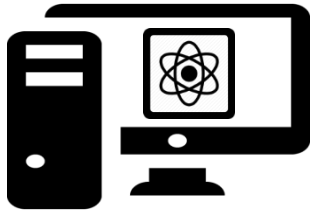
0 1 0 0 1 0 1

1 out of 2^N possible states

N qubits

$\alpha_1|00\ldots0\rangle + \alpha_2|00\ldots1\rangle + \ldots + \alpha_{2^N}|11\ldots1\rangle$

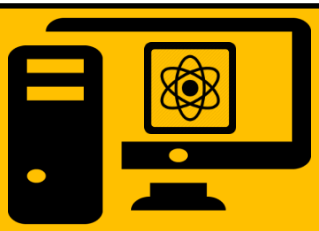
All out of 2^N possible states

Consequences of 

Mathematical operation on N 

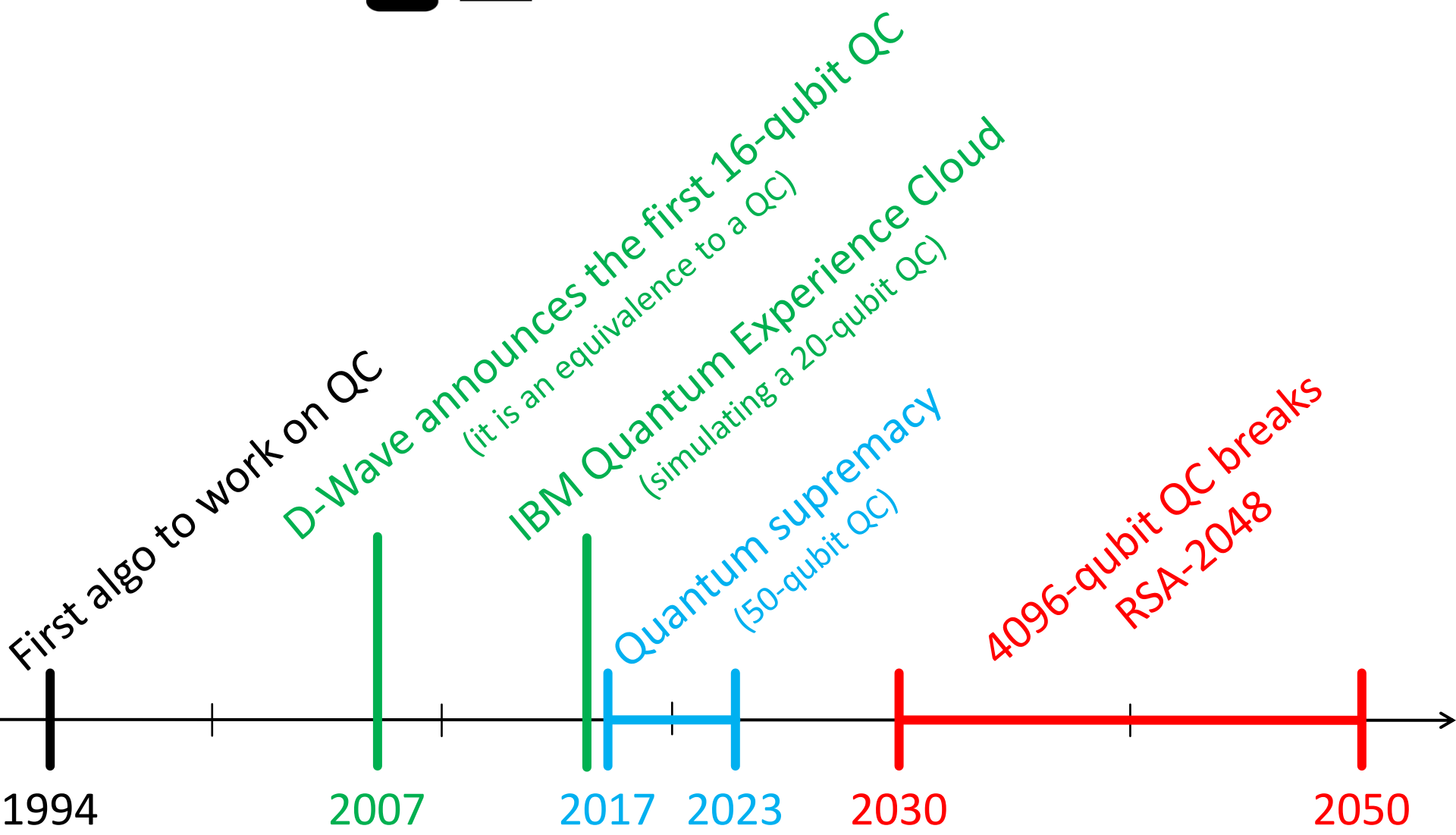
⇩

Parallel computation on $\mathbf{2}^{\boldsymbol{N}}$ data

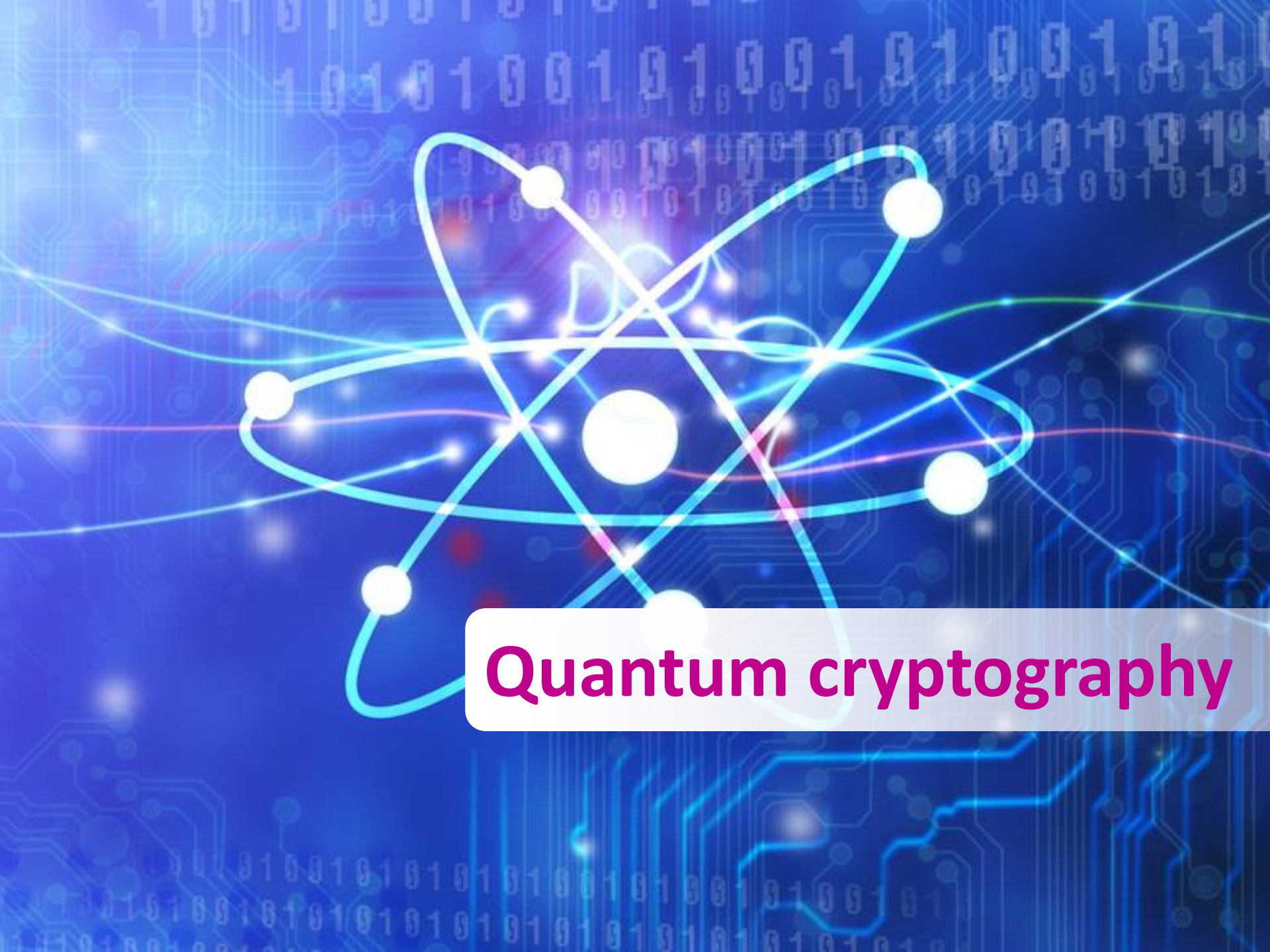
Computation power of a 

x2 each time a  is added

in real life



QC = Quantum Computer


Quantum cryptography

Goal

Exploit the  mechanical properties to **perform crypto tasks**

Quantum Random Number Generator

Quantum Key Distribution

Quantum Commitment

Oblivious Transfer

Secure Multi-Party Computation

Quantum Random Number Generator

Generate better **high-quality** random numbers

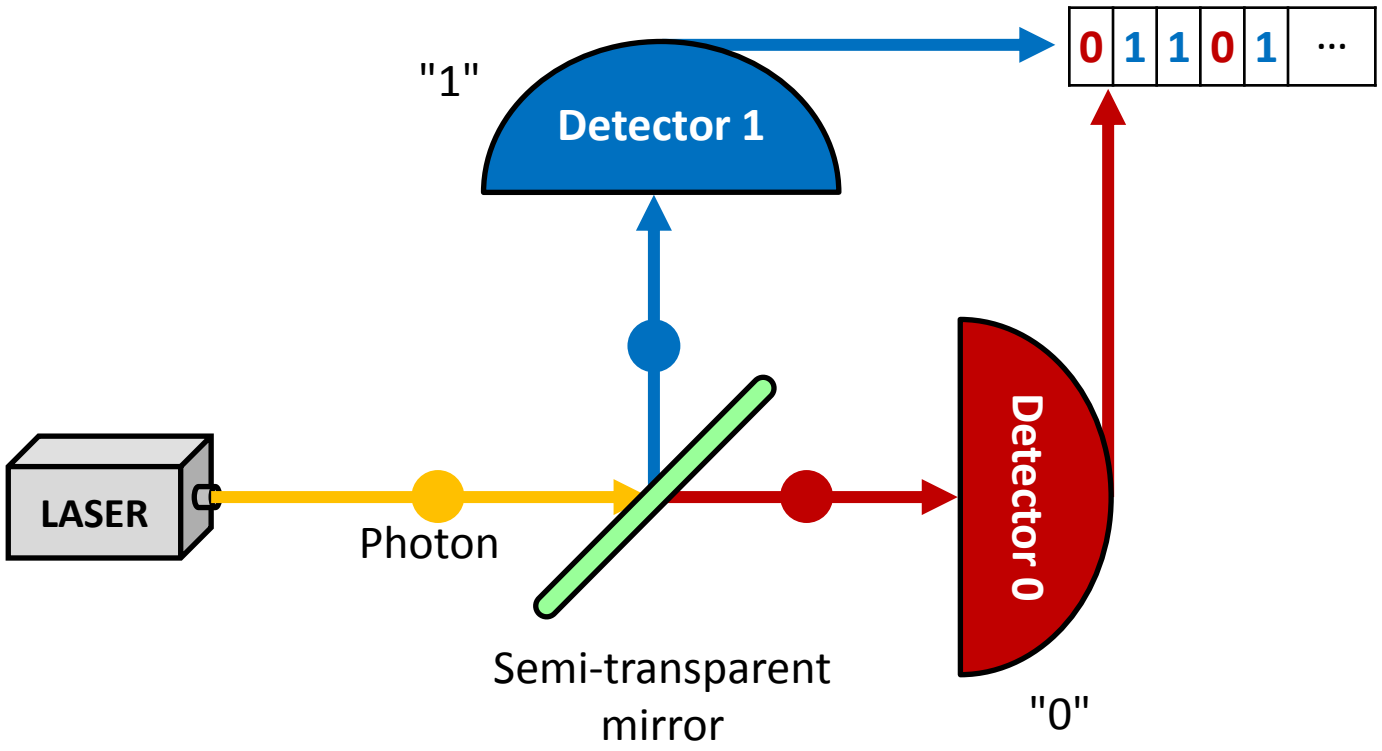
Based on:

- Radioactive decay
- Noise
- Quantum optics

most used

Quantum Random Number Generator

Single-photon splitting



Example based on quantum optics

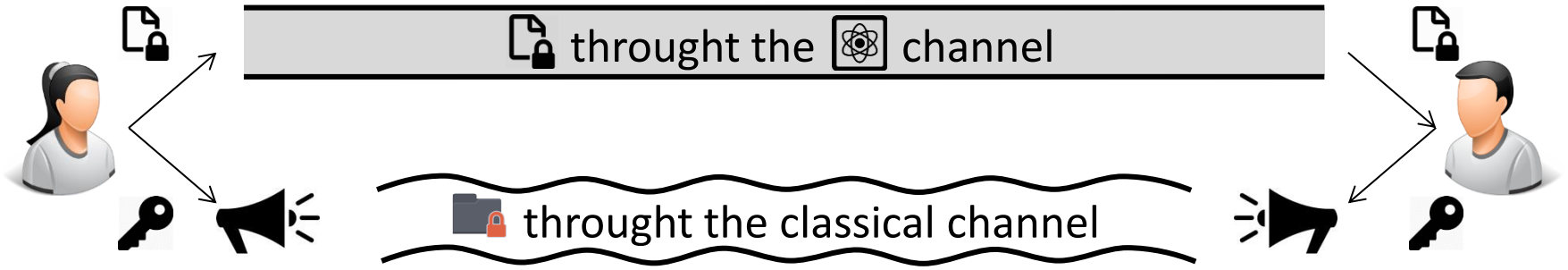
The beam splitter deviates the photon to a 0/1 detector

The photon's choice at beam splitting is **totally random**

Quantum Key Distribution

Transfer **securely** from Alice to Bob

From , produce a **random shared** secret key

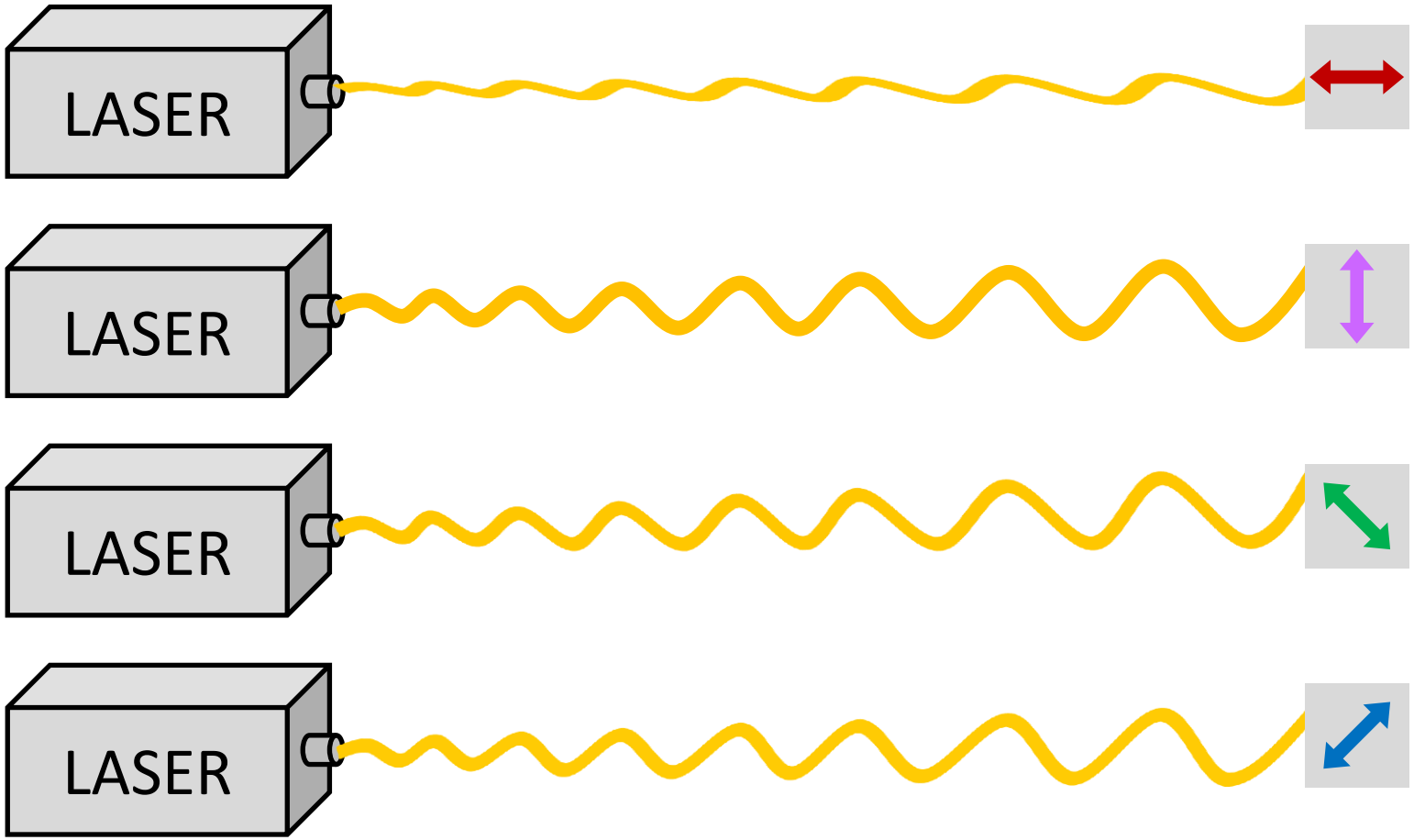


---

qkdsimulator.com

Quantum Key Distribution

Polarization of a photon

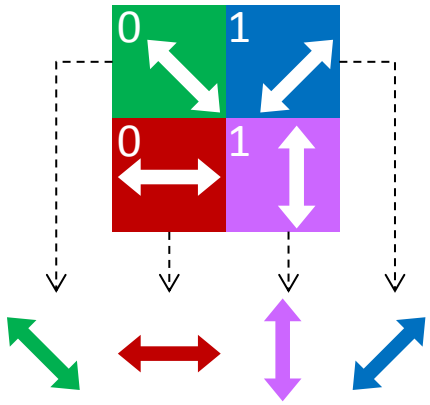


Quantum Key Distribution

Polarization of a photon

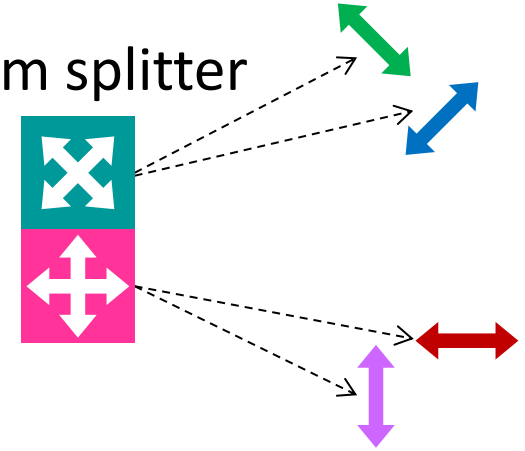
Unpolarized photon

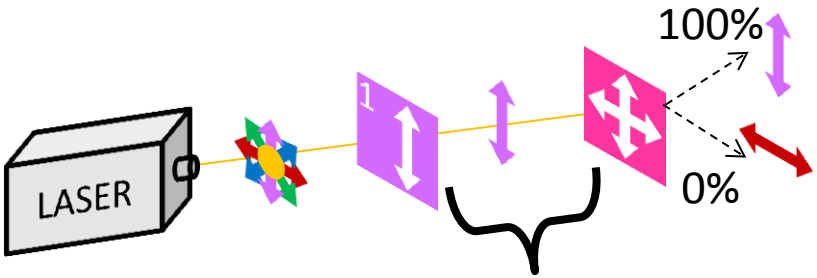
Polarization filter



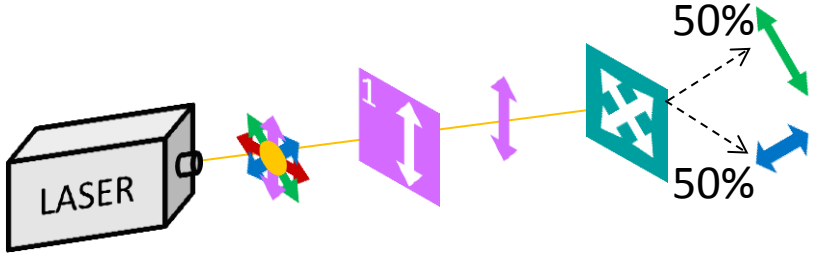
4 polarized photons

Beam splitter



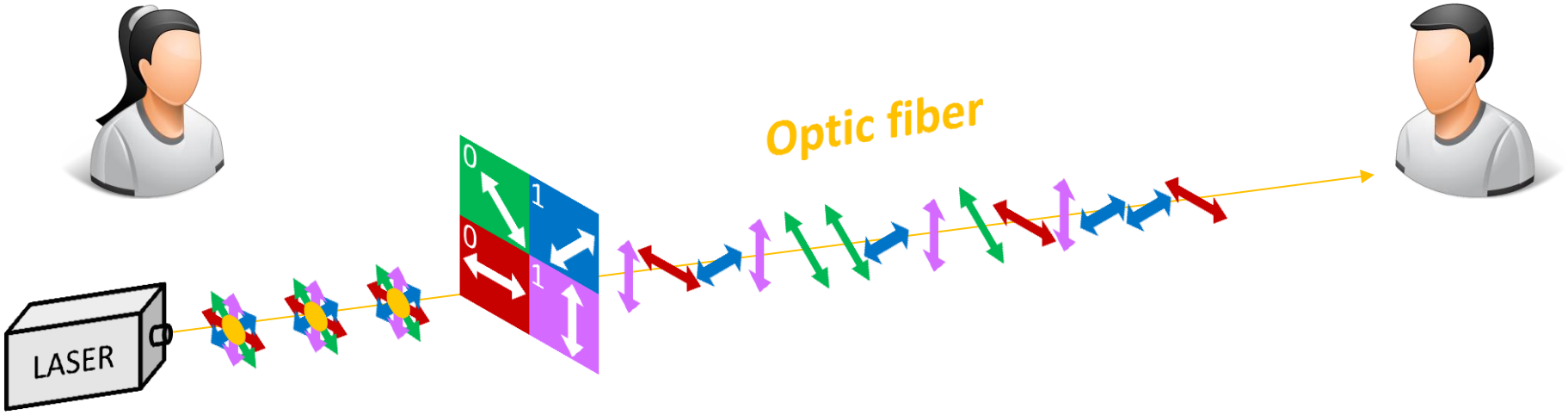


Not readable during transfer
otherwise **qubits are disturb**



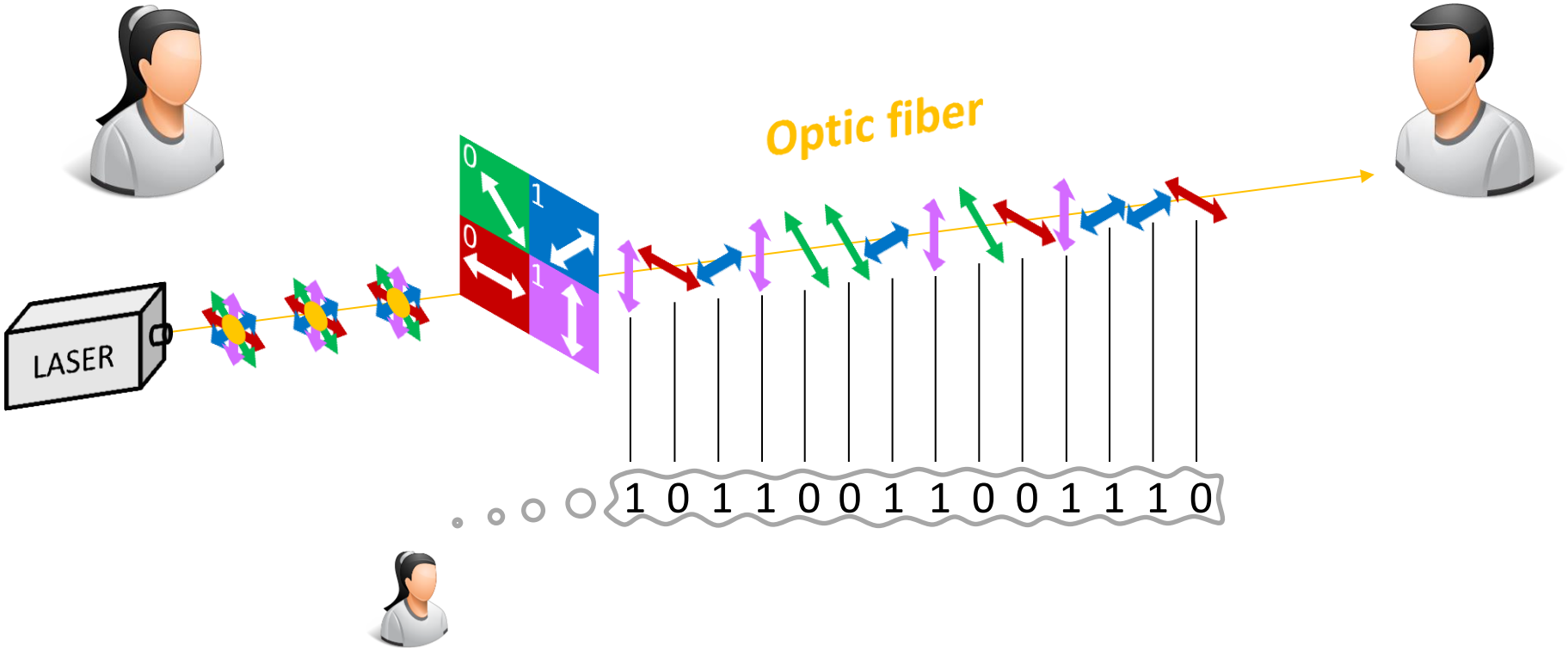
Quantum Key Distribution

The BB84 protocol



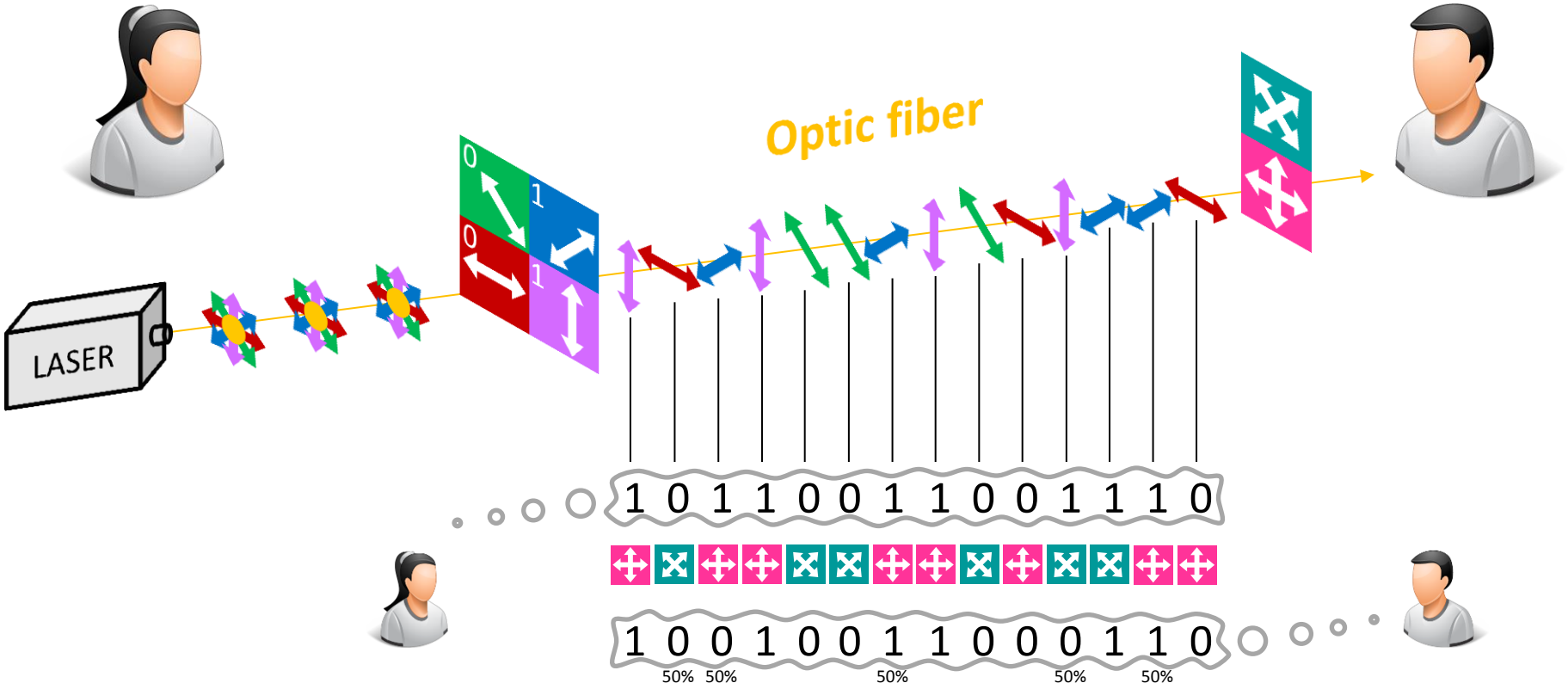
Quantum Key Distribution

The BB84 protocol



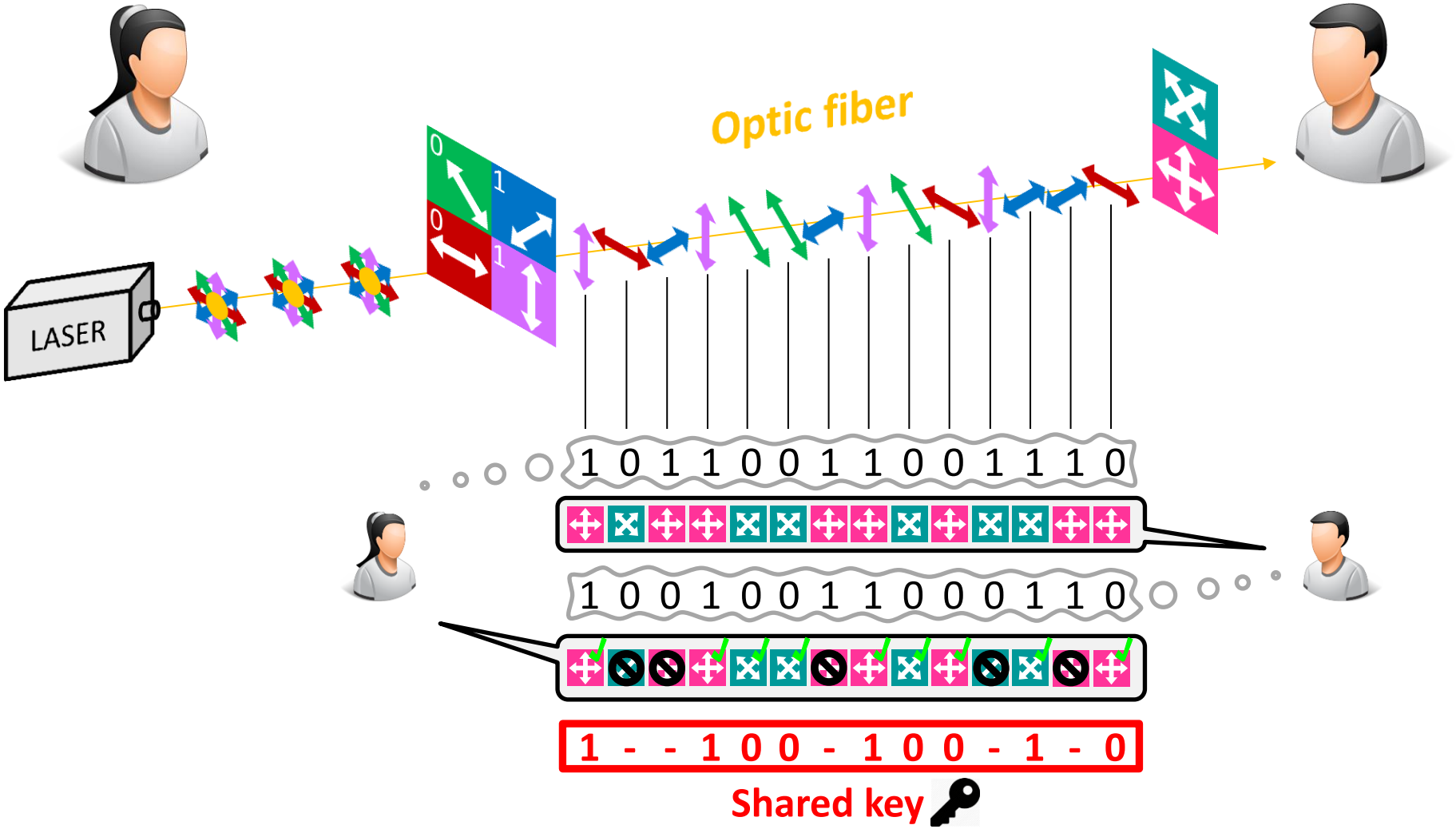
Quantum Key Distribution

The BB84 protocol



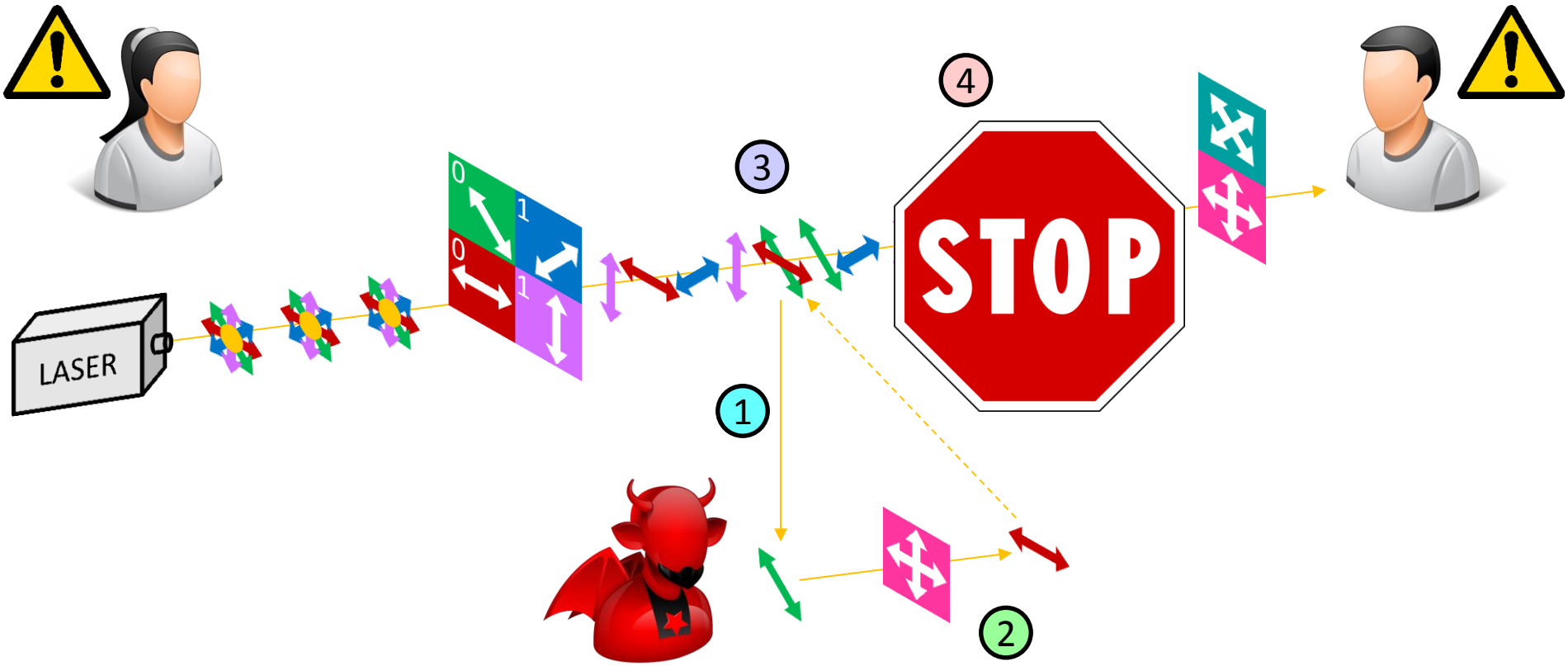
Quantum Key Distribution

The BB84 protocol



Quantum Key Distribution

Eavesdropping the BB84 protocol



1. Lecture of the qubit state
2. splitter ⇒ disturbance
3. Qubit modification in the channel
4. Detection (error rate) & abortion

Quantum Key Distribution

In practice

Currently

The highest bit rate for QKD with optical fiber is held by Toshiba with

1 Mbit/s over 50 km

[up to our knowledge]

Limitation on the distance of key exchange

Quantum attacks

Goal

Exploit the  mechanical properties to **crack/solve hard problems**

Shor's algorithm

Grover's algorithm

HHL's algorithm

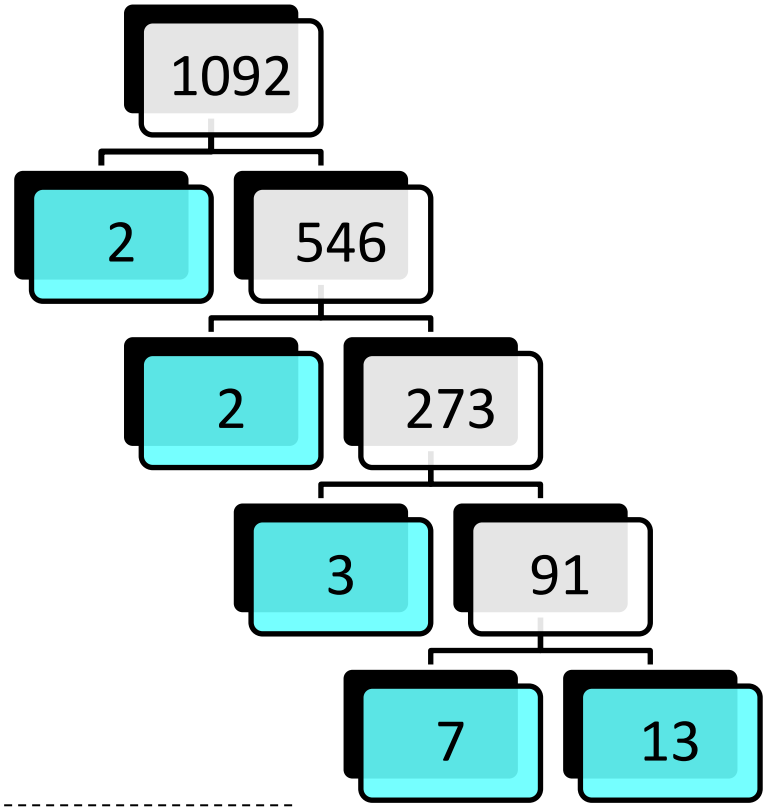
Quantum simulator

Etc…

Shor's algorithm

Created by
Peter Shor (1994)

Solve
prime factorization
in polynomial time



Prime factors:
$2, 2, 3, 7, 13$

$1092 = 2^2 * 3 * 7 * 13$

This is a very simple example

Shor's algorithm

Breaking public-key cryptography

E.g. an RSA number:

$N = p * q$, where (p, q) are prime numbers

Easy to compute N from (p, q)

Hard to recover (p, q) from N with standard methods

RSA-1024 =
135066410865995223349603216278805969
938881475605667027524485143851526510
604859533833940287150571909441798207
282164471551373680419703964191743046
496589274256239341020864383202110372
958725762358509643110564073501508187
510676594629205563685529475213500852
879416377328533906109750544334999811
150056977236890927563

Shor's algorithm

Breaking public-key cryptography

E.g. an RSA number:

$N = p * q$, where (p, q) are prime numbers

Easy to compute N from (p, q)

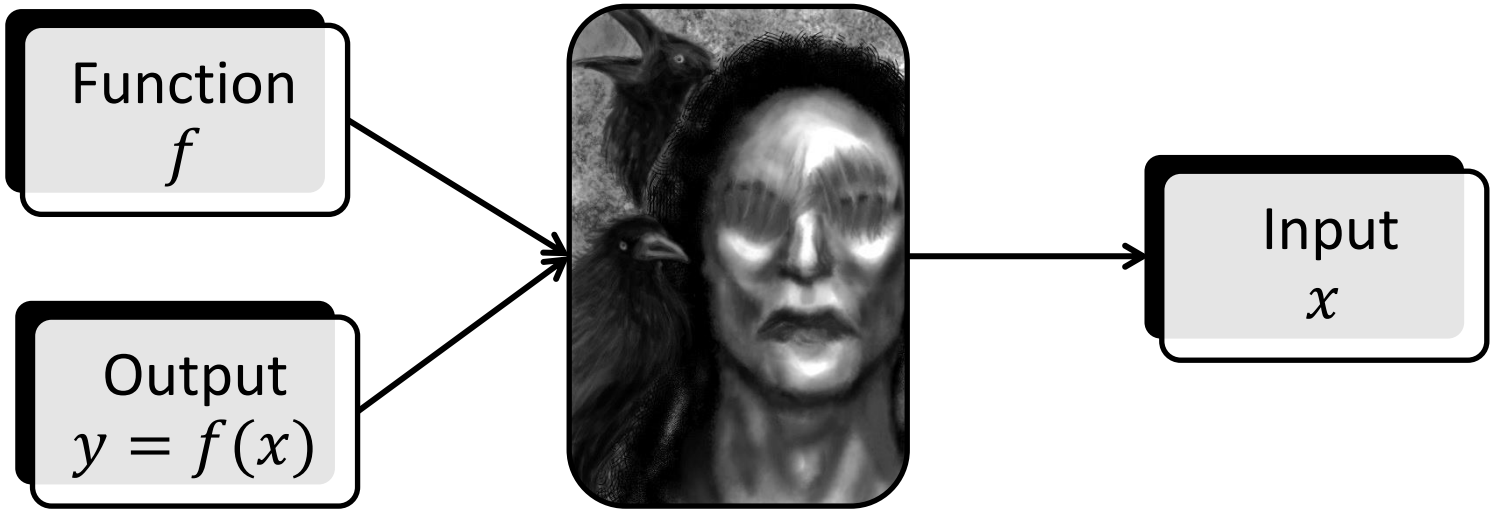
Easy to recover (p, q) from N with Shor's algorithm

RSA-1024 =
135066410865995223349603216278805969
938881475605667027524485143851526510
604859533833940287150571909441798207
282164471551373680419703964191743046
496589274256239341020864383202110372
958725762358509643110564073501508187
510676594629205563685529475213500852
879416377328533906109750544334999811
150056977236890927563

Grover's algorithm

Created by
Lov Grover (1996)

Solve
invertion of function
in sub-linear time



Grover's algorithm

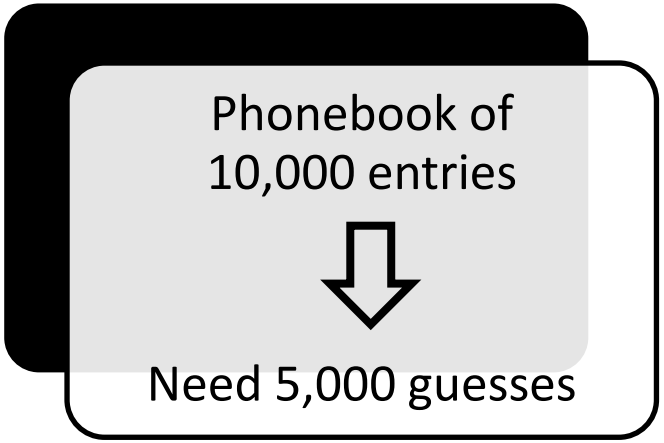
Searching an unstructured DB / an unsorted list

E.g. searching a phonebook where:

- x is a name
- $y = f(x)$ is a phone number

Easy to find y from (f, x)

Hard to find x from (f, y) with standard methods



Grover's algorithm

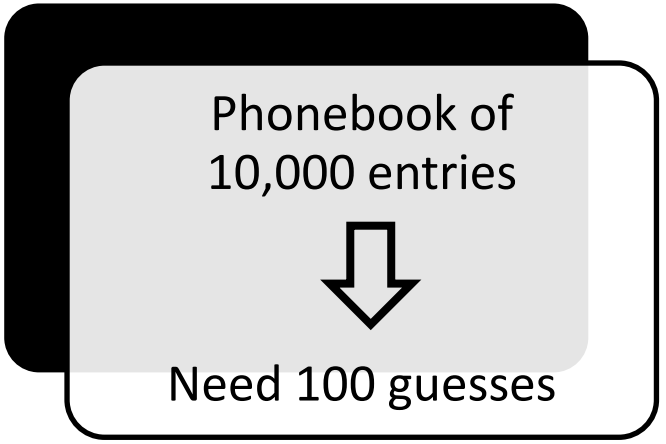
Searching an unstructured DB / an unsorted list

E.g. searching a phonebook where:

- x is a name
- $y = f(x)$ is a phone number

Easy to find y from (f, x)

Easy to find x from (f, y) with Grover's algorithm



Grover's algorithm

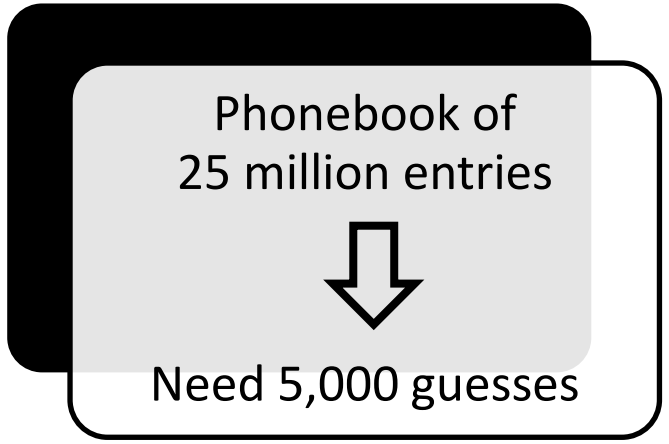
Searching an unstructured DB / an unsorted list

E.g. searching a phonebook where:

- x is a name
- $y = f(x)$ is a phone number

Easy to find y from (f, x)

Easy to find x from (f, y) with Grover's algorithm



Grover's algorithm

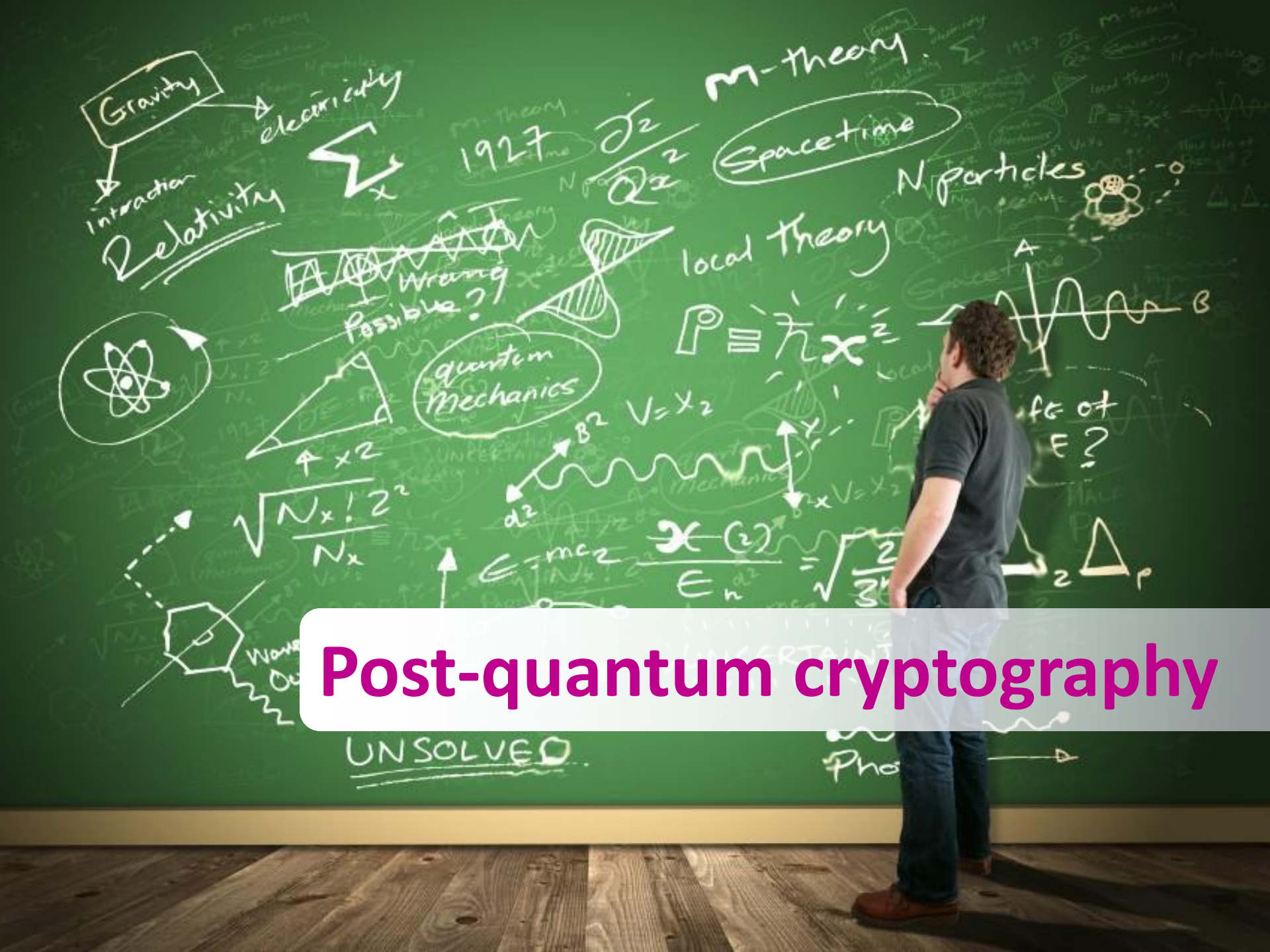
Breaking symmetric-key cryptography

Brute-forcing
a 128-bit key
in $\approx \mathbf{2^{64}}$ iterations

Brute-forcing
a 256-bit key
in $\approx \mathbf{2^{128}}$ iterations

Simple solution

Use **looooooooooooonger** keys!



Post-quantum cryptography

Goal

Cryptographic schemes/algorithms
resistant to  **attacks**

Hash-based crypto

Code-based crypto

Lattice-based crypto

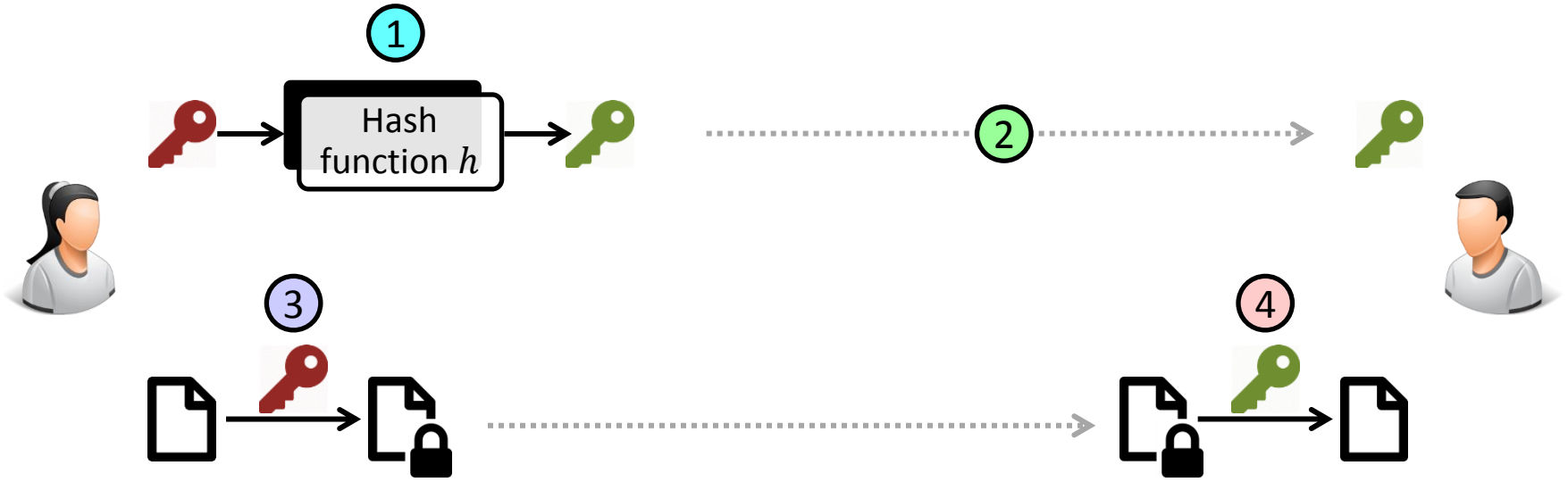
Multivariate crypto

Etc…

Hash-based crypto

Created by
Ralph Merkle (1970)

Alternative to
signature schemes
like RSA/DSA/ECDSA

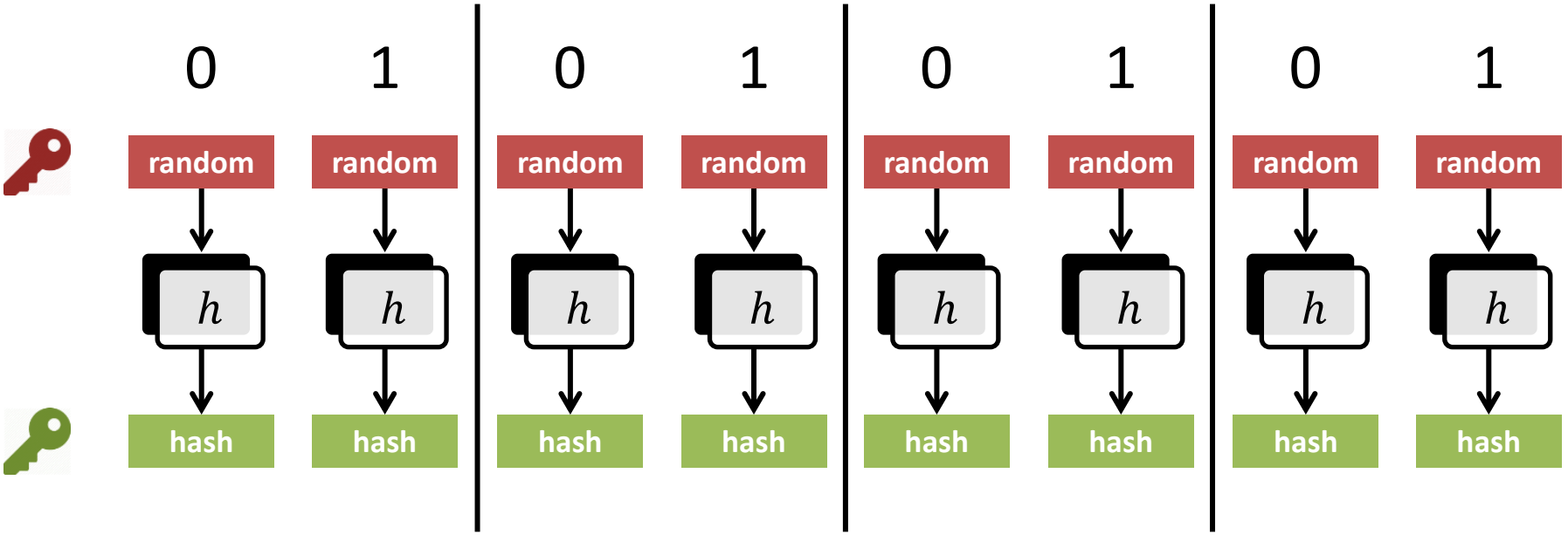


1. Create private key and public key
2. Distribute
3. Sign data with
4. Verify signature with

Hash-based crypto

The Lamport signature scheme

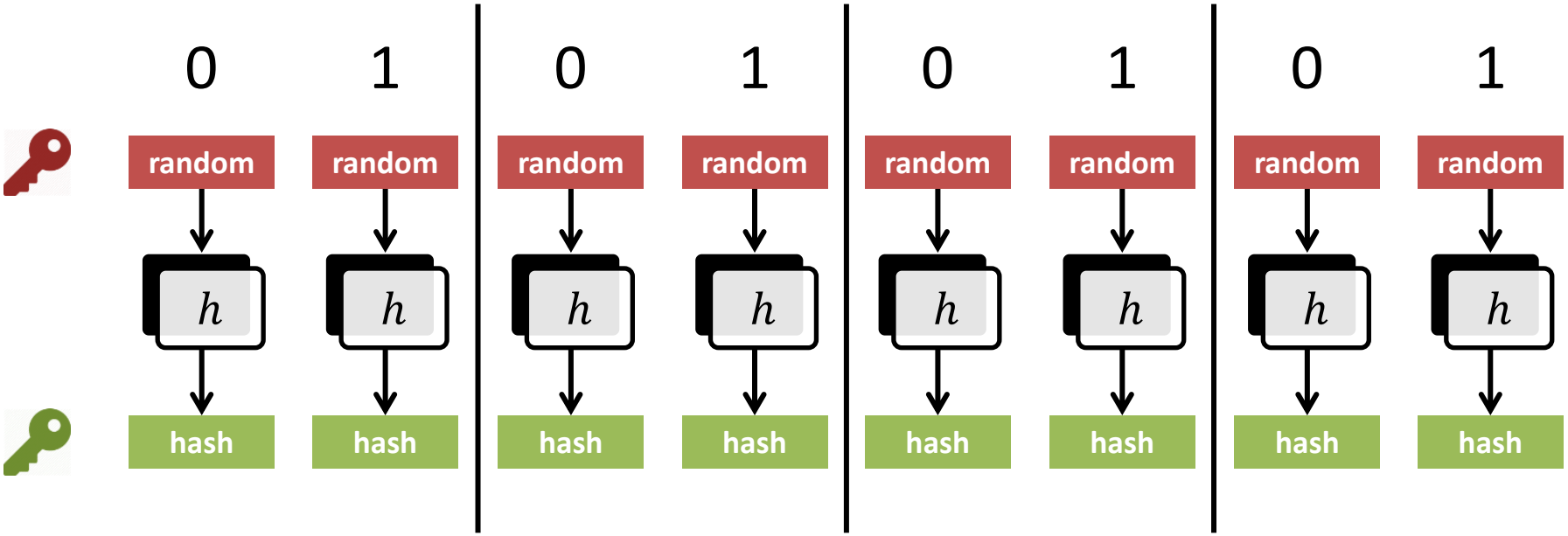
🔑 and 🔑 must be used only **once**



1 Create private key 🔑 and public key 🔑

Hash-based crypto

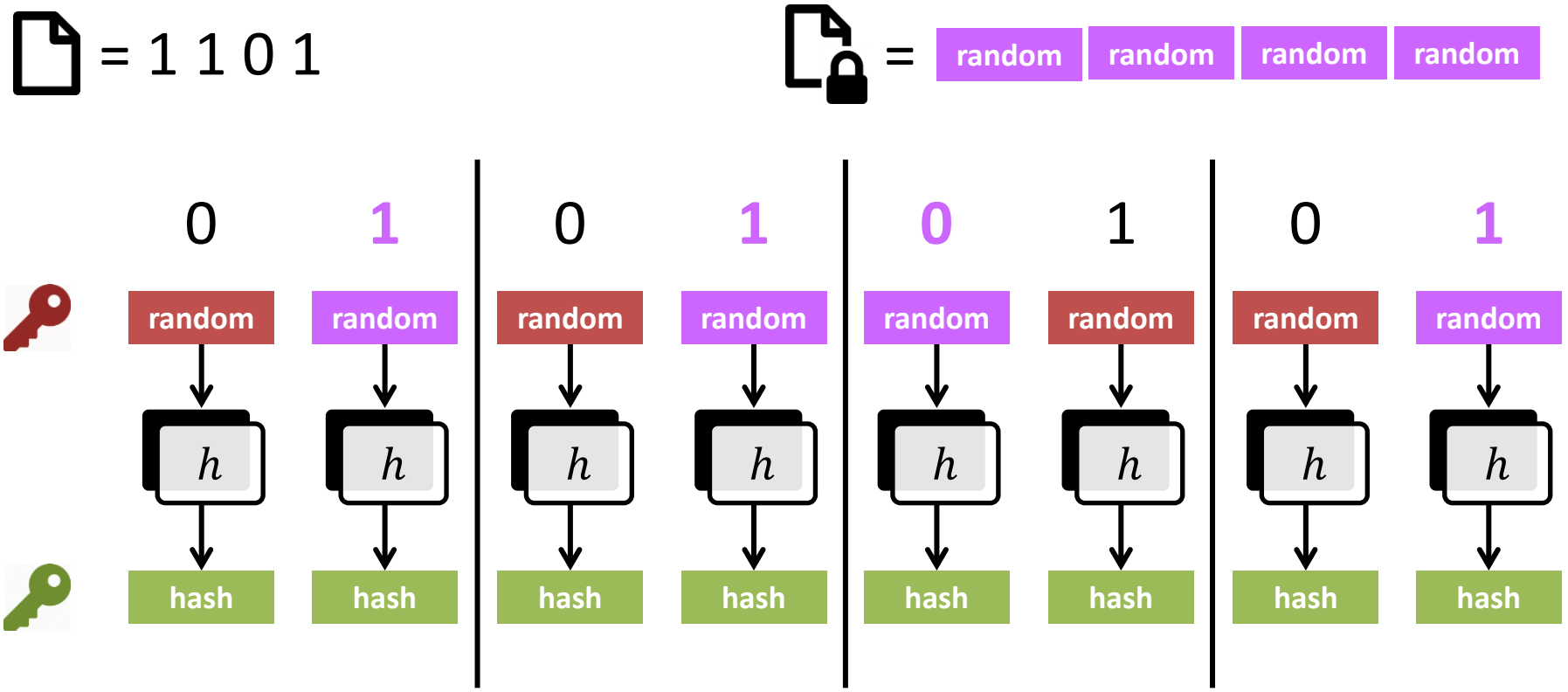
The Lamport signature scheme



1. Create private key and public key
2. Distribute

Hash-based crypto

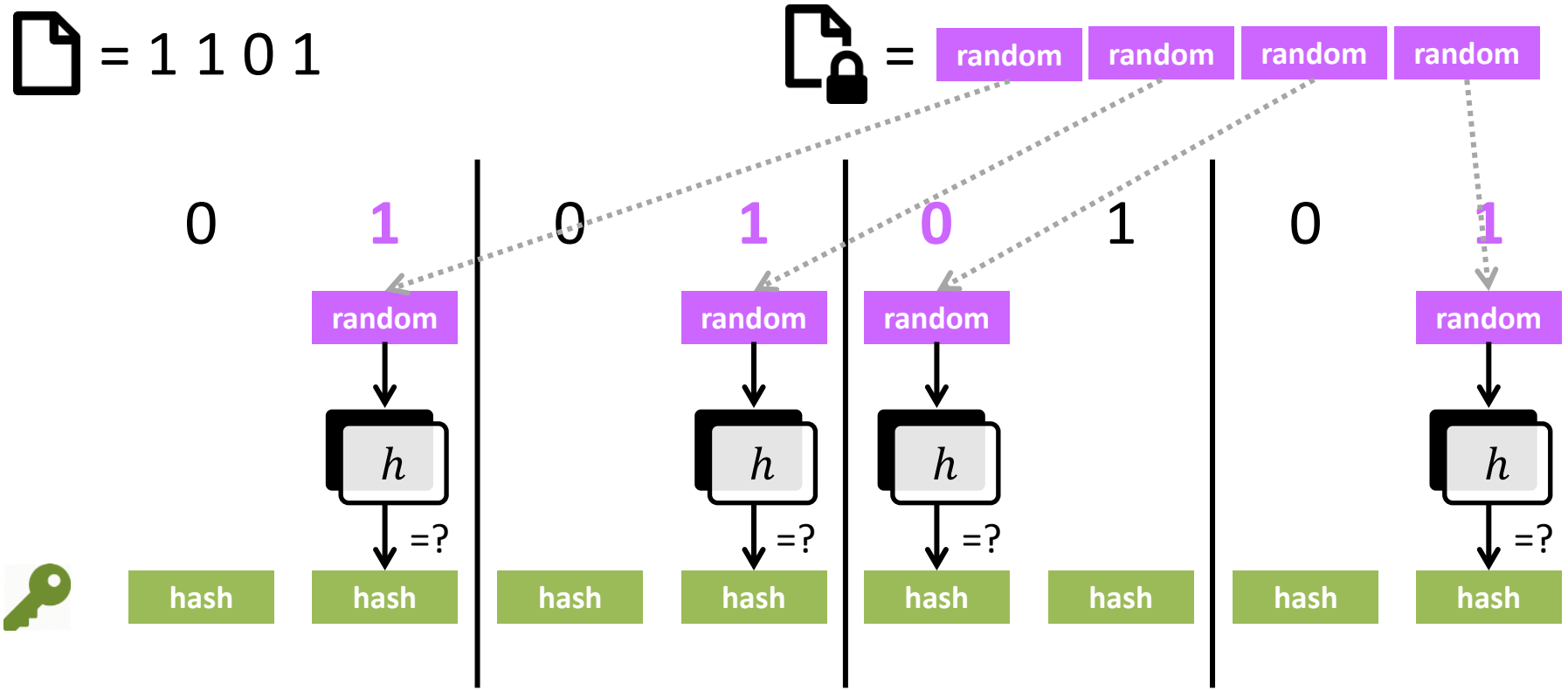
The Lamport signature scheme



1. Create private key and public key
2. Distribute
3. Sign data with

Hash-based crypto

The Lamport signature scheme



1. Create private key and public key
2. Distribute
3. Sign data with
4. Verify signature with

Hash-based crypto

The Lamport signature scheme

To be quantum-resistant

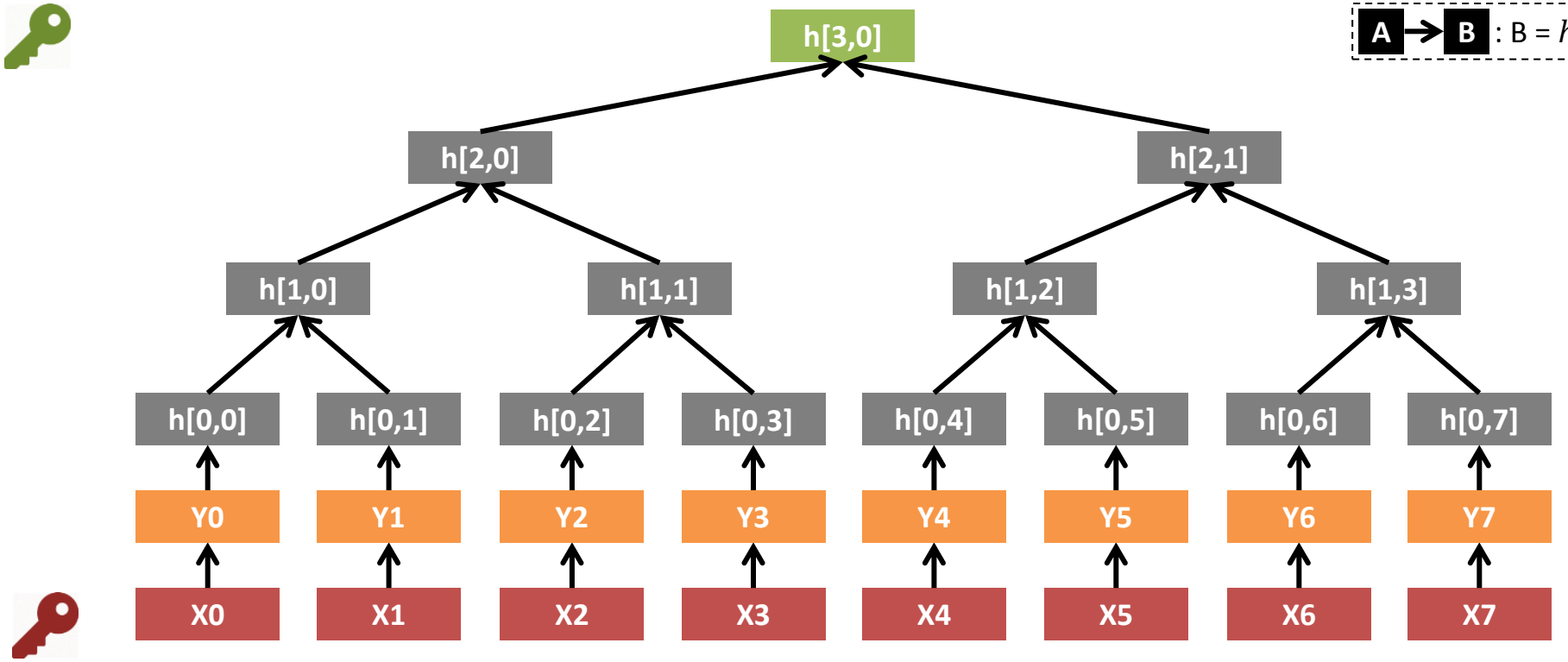
The lengths of random , hash and random
must be **> x2 larger** than the security parameter

EX

A 128-bit security requires
lengths > 256 bits

Hash-based crypto

The Merkle signature scheme

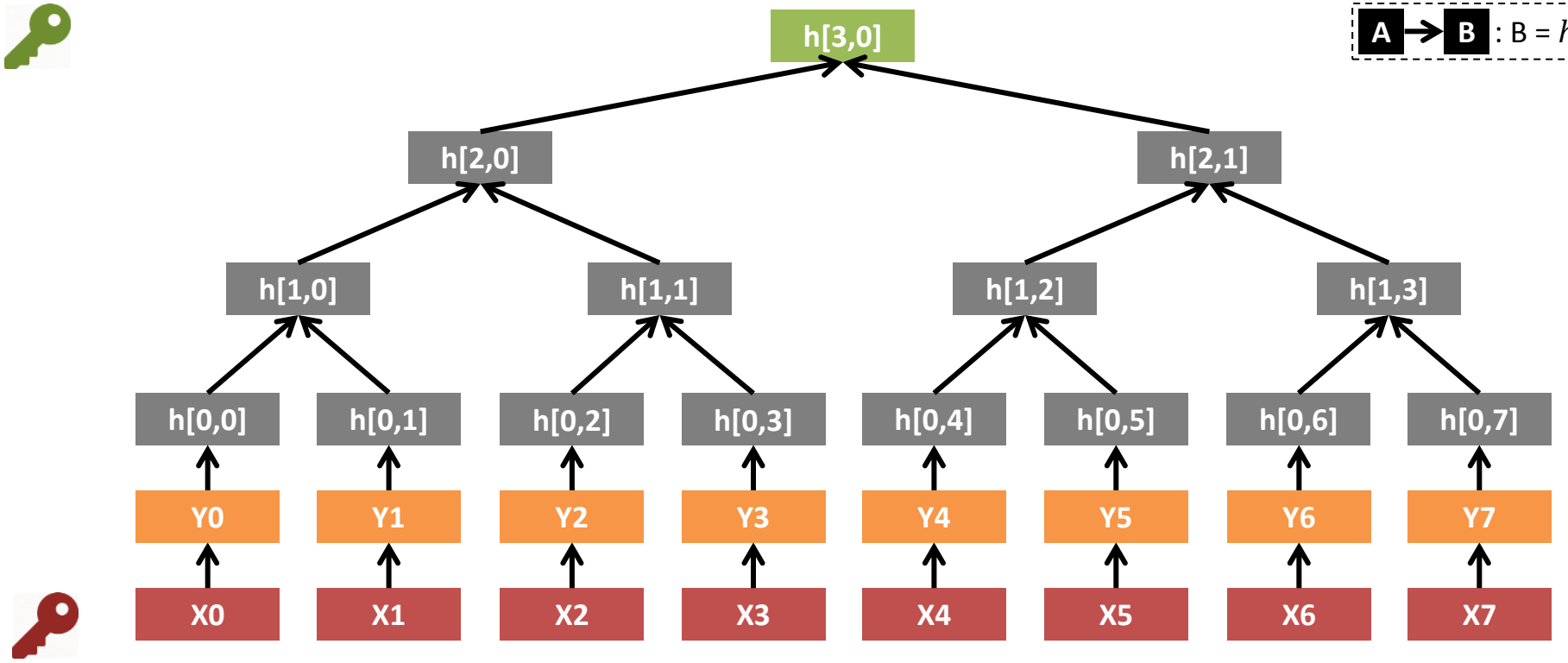


(Xi , Yi) must be used only **once**

1. Create private key and public key

Hash-based crypto

The Merkle signature scheme

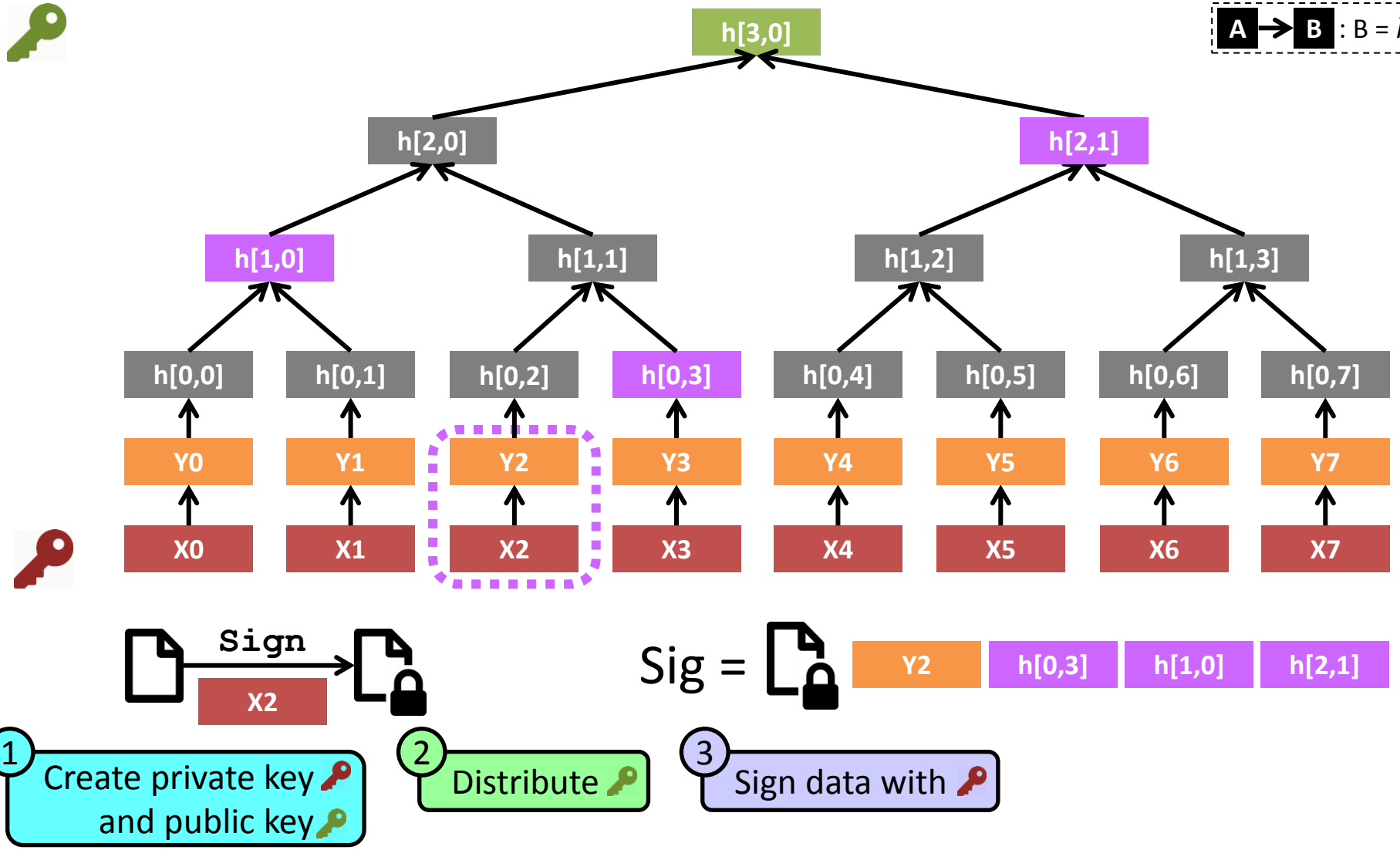


1. Create private key and public key

2. Distribute

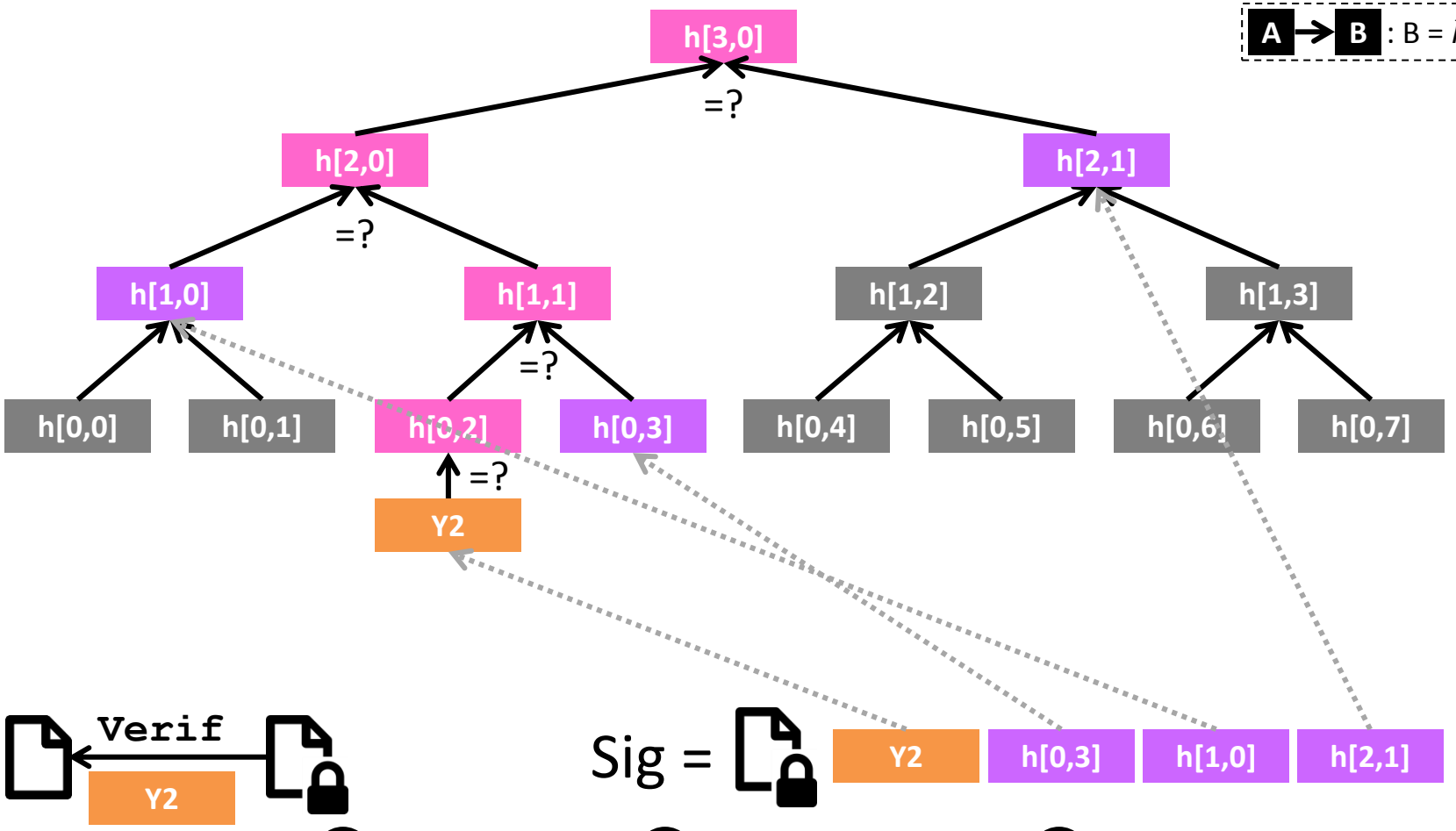
Hash-based crypto

The Merkle signature scheme



Hash-based crypto

The Merkle signature scheme



1. Create private key and public key
2. Distribute
3. Sign data with
4. Verify signature with

Code-based crypto

Created by
Robert McEliece(1978)

Alternative to
PK encryption
like RSA/ECC

Based on error-correcting code

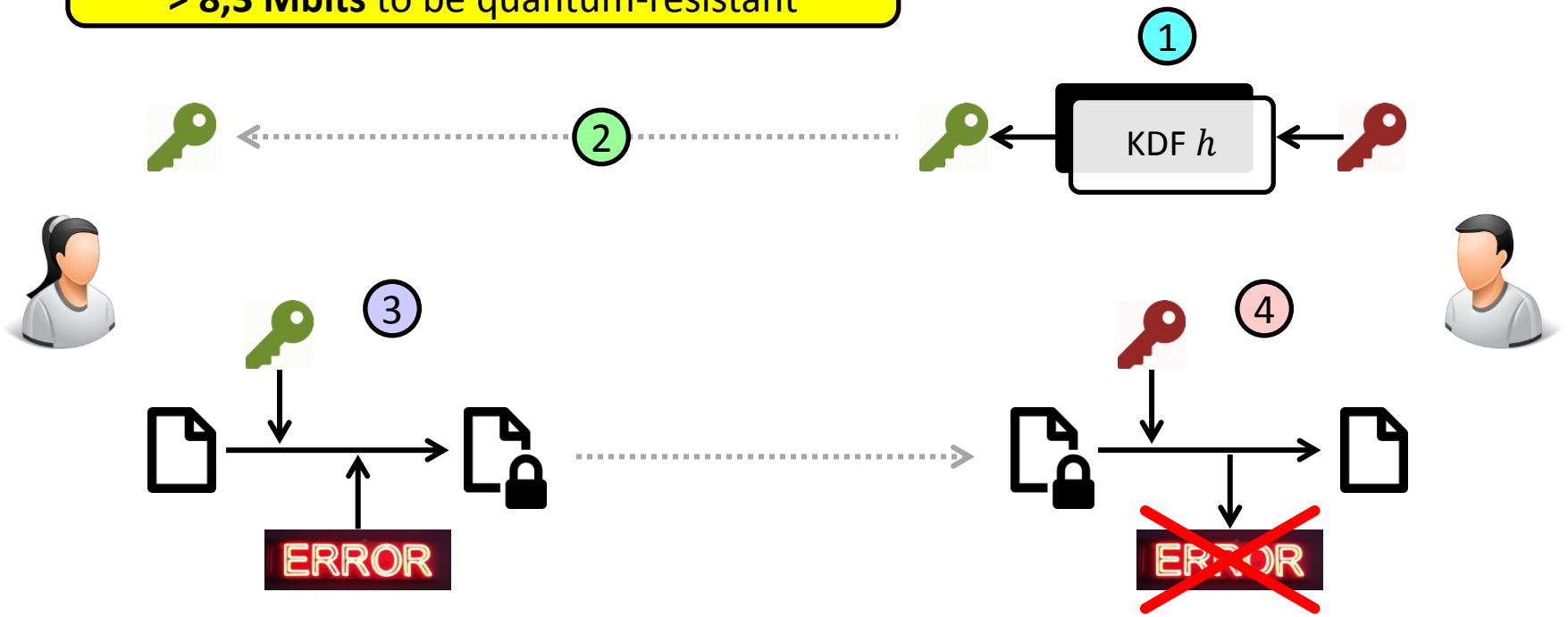
Most well-known

- the McEliece cryptosystem
- the Niederreiter cryptosystem
- the Courtois-Finiasz-Sendrier signature scheme

Code-based crypto

The principles

The size of 🔑 is extremely large:
> 8,3 Mbits to be quantum-resistant



1 Create private key 🔑 and public key 🔑

2 Distribute 🔑

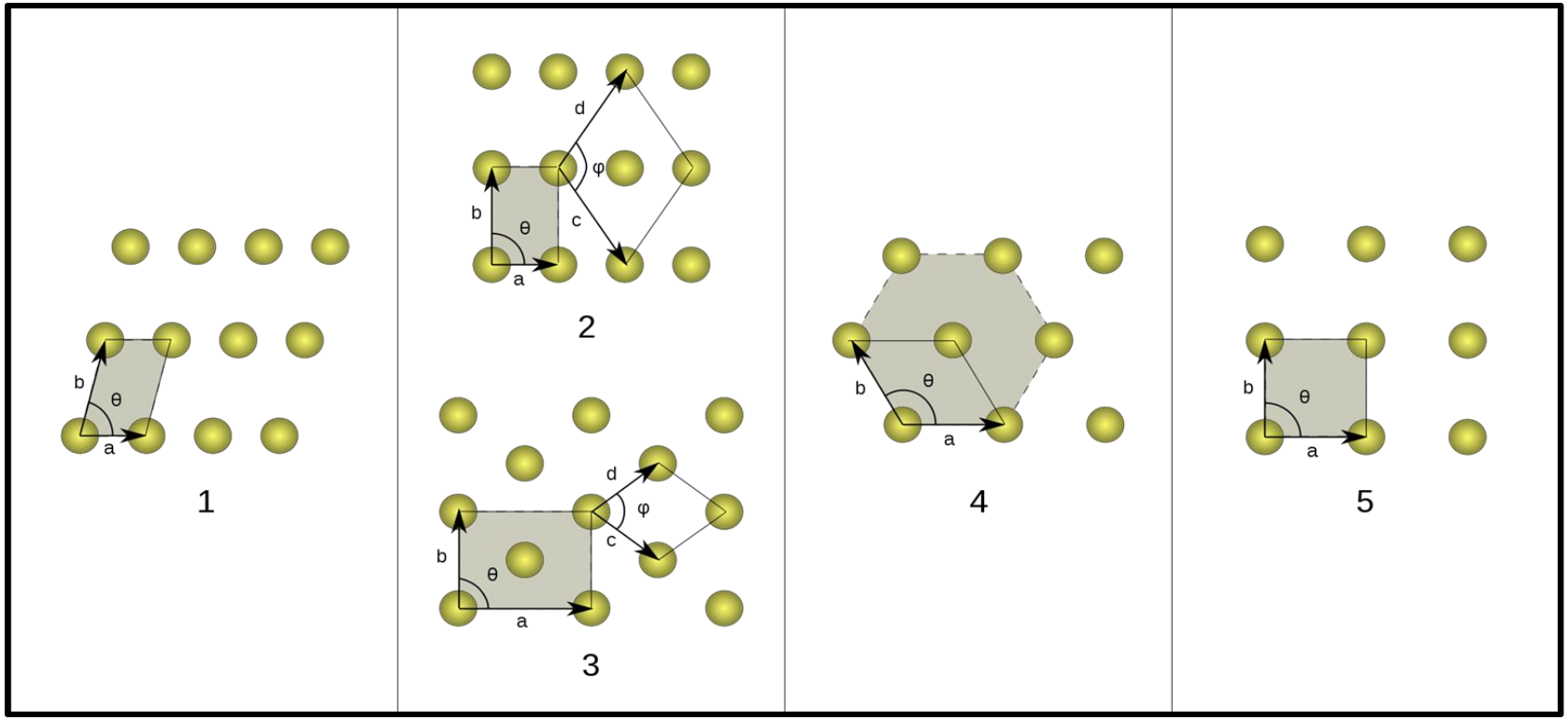
3 Encrypt data with 🔑 and add ERROR

4 Decrypt with 🔑

Lattice-based crypto

Lattices first studied by Lagrange & Gauss (18^{th} century)

Alternative to **PK encryption** like RSA/ECC



Lattice-based crypto

The most well-known schemes

Encryption

- the Peikert ring-LWE key exchange
- the Goldreich-Goldwasser-Halevi encryption scheme
- NTRUEncrypt

Signature

- the Gunesyu-Lyubashevsky-Poppleman ring-LWE scheme
- the Goldreich-Goldwasser-Halevi signature scheme
- NTRUSign

Hash

- SWIFFT (based on Fast Fourier Transform)
- LASH (LAttice based haSH function)

LWE = Learning With Errors

Lattice-based crypto

Security assumptions

Learning With Errors (LWE)

Find x from (f, y) when y contains errors

Shortest Vector Problem (SVP)

Find the shortest vector in a lattice

[and its sub-problem]

Short Integer Solution (SIS)

Find the shortest vector in specific lattices

Post-quantum actors

PQCRYPTO
ICT-645622

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

ETSI
World Class Standards

IETF®

Google

The helper: evolution

Michele Mosca

Co-Founder, President and CEO of evolution
Co-founder of IQC Institute for Quantum Computing at University of Waterloo
Project leader of OPEN QUANTUM SAFE

Quantum risk assessment

Quantum safe hardware & software

Roadmap design & implementation

Education service

The integrator: OPEN QUANTUM SAFE

1

Open source C library

liboqs

for quantum-resistant cryptographic algorithms

2

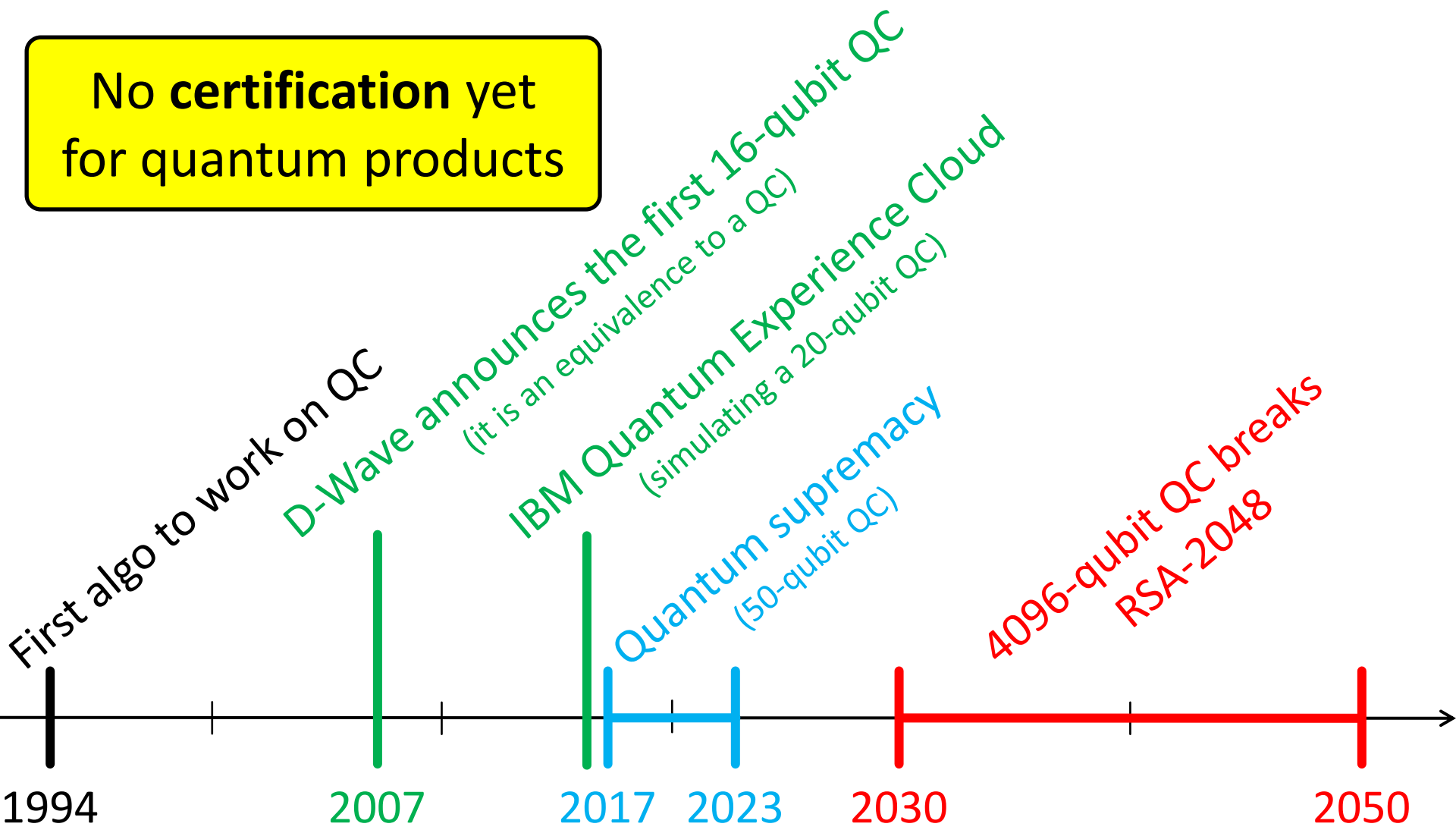
Prototype integrations into protocols/applications such as **OpenSSL**

Some performance results can be found at https://eprint.iacr.org/2016/1017.pdf

Recommandations

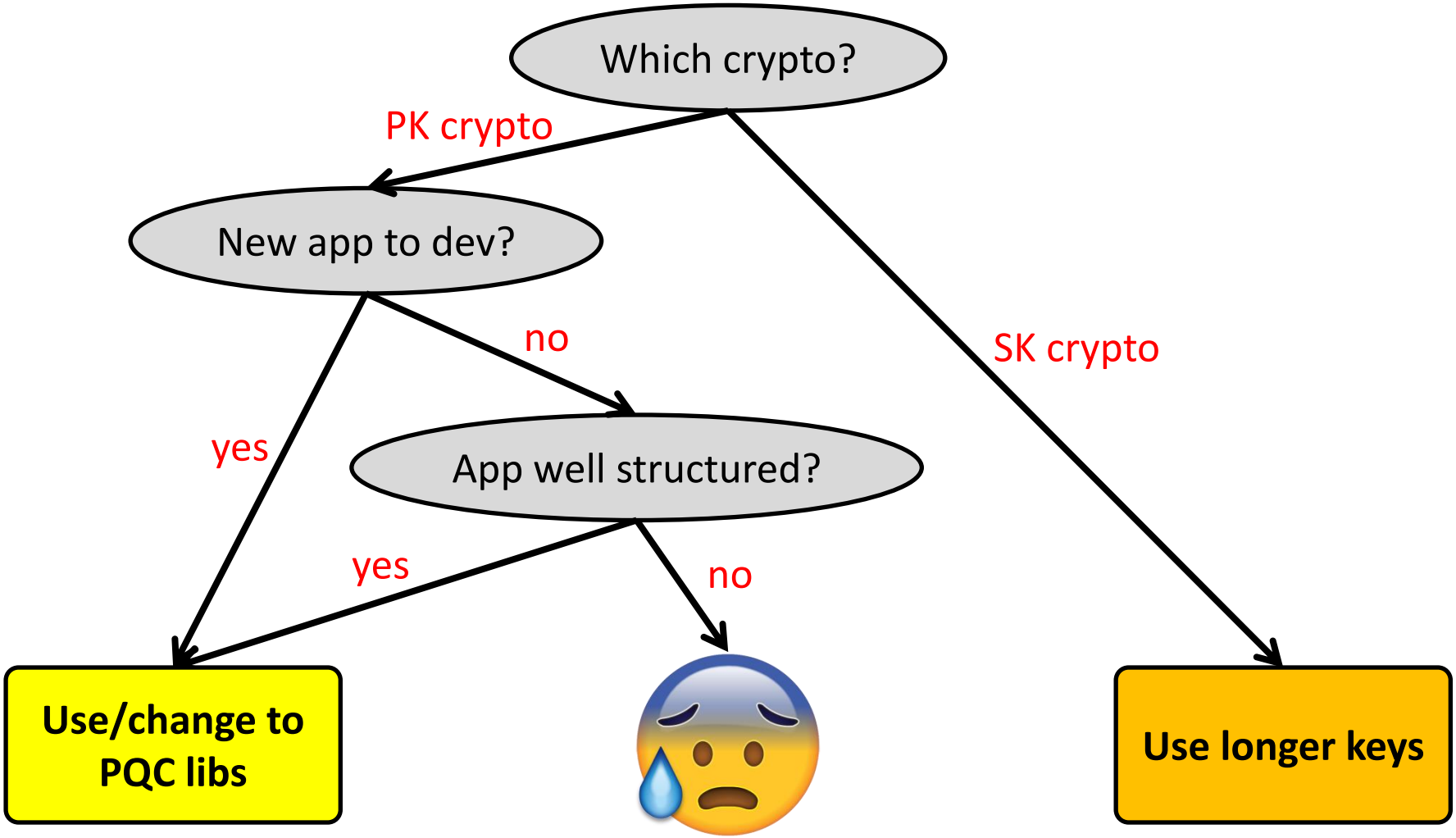
Quantum tech is not a dream

No **certification** yet
for quantum products



QC = Quantum Computer

How to be quantum-resistant



PK = Public Key | SK= Symmetric Key | PQC = Post Quantum Cryptography

Be careful with PQC

Hash-based crypto

- Keys must be **used once**
- Lengths of variables and keys must be **long enough** (> x2) to be quantum-resistant

Code-based crypto

- Size of public key is **extremely large** (> 8,3 Mbits) to be quantum-resistant

Lattice-based crypto

- Not **mature** yet

PQC = Post Quantum Cryptography

Tania Martin

☎ 02 787 56 05

✉ tania.martin@smals.be

Smals

www.smals.be

@Smals_ICT

www.smalsresearch.be

@SmalsResearch