



black hat[®]
EUROPE 2020

DECEMBER 9-10
BRIEFINGS

Quantum Security and Cryptography: You're (Probably) Doing it Wrong


Tommaso Gagliardini - Kudelski Security (Switzerland)

Who I am at a glance

- Tommaso Gagliardini (Italian, based in Zurich)
- Degree in Mathematics at University of Perugia, Italy
- PhD from Technical University of Darmstadt, Germany
- Dissertation title:
“Quantum Security of Cryptographic Primitives”
- Post-Doc at IBM Research Zurich, Switzerland
- Joined Kudelski Security in January 2019



In This Talk:

- (Minimal) Introduction to Quantum Computing
 - Connections to Cybersecurity
 - “Post-Quantum”: a Bad Name Choice
 - The Magic World of Quantum Cryptography
- 

Quantum Computing



Revolutionary model of computation based on **quantum mechanics**

Can solve **certain problems** much faster than traditional computers

Very challenging to build, currently only exist **prototypes** which are not yet usable

But technology is **improving rapidly** and large investments are pushing R&D

Bits and Qubits

Classical bit: can be either 0 or 1

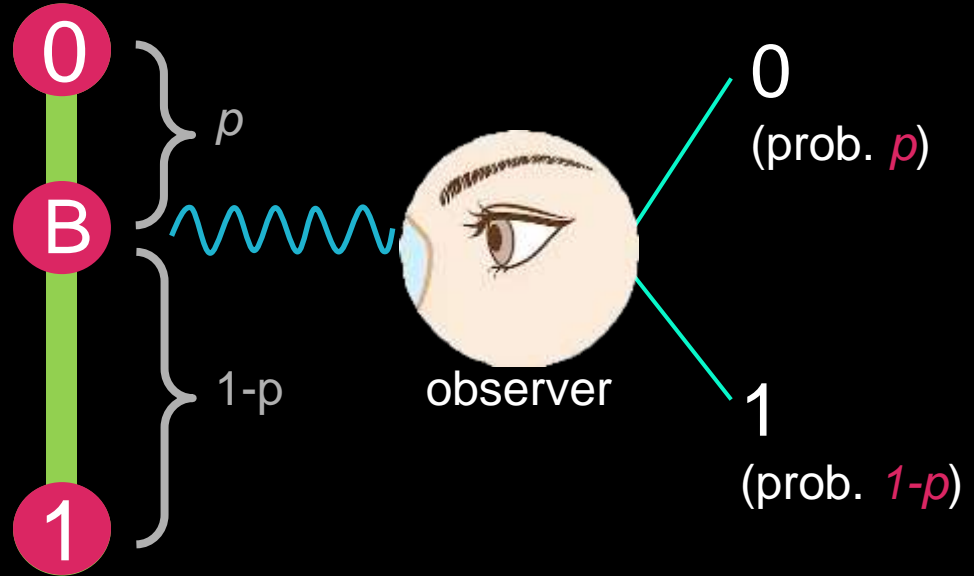
0

1

Bits and Qubits

Probabilistic bit: can be 0, or 1, or 0 with probability p and 1 with probability $(1-p)$

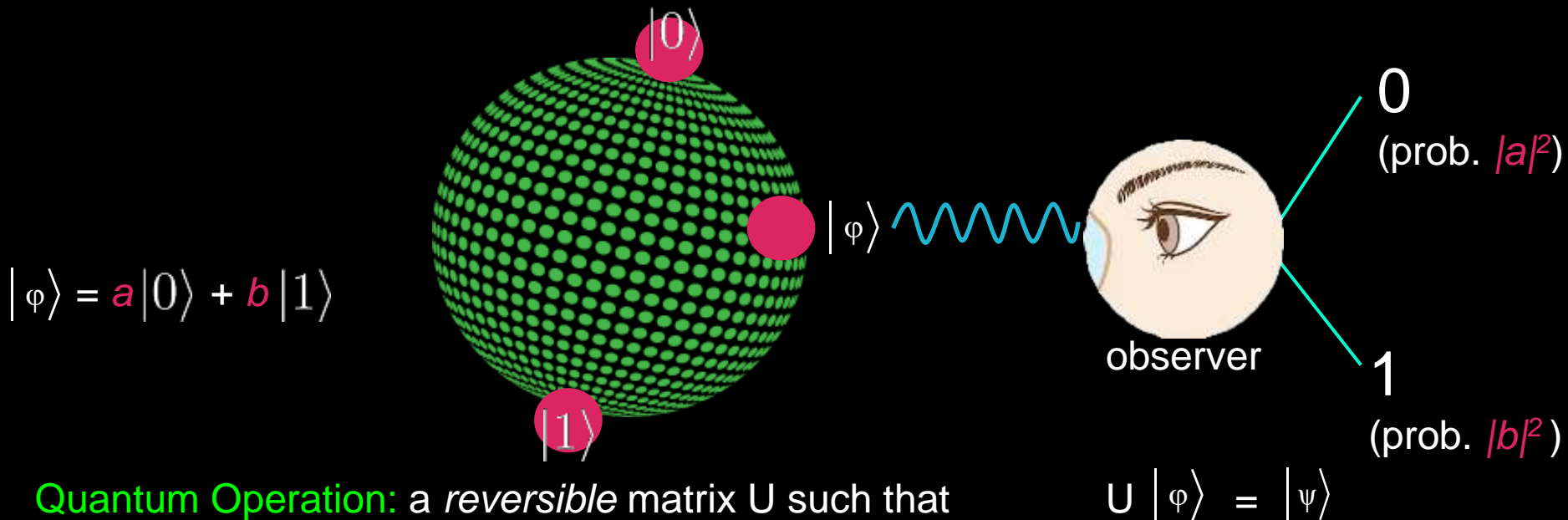
$$B = p \underline{0} + (1-p) \underline{1}$$



Bits and Qubits

Quantum bit (qubit): it's like a probabilistic bit but the probabilities are complex numbers the resulting representation is a sphere

A qubit can be $|0\rangle$, or $|1\rangle$ or a superposition

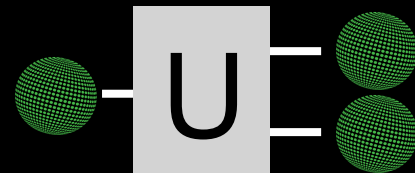


Entanglement, Teleportation, No-Cloning

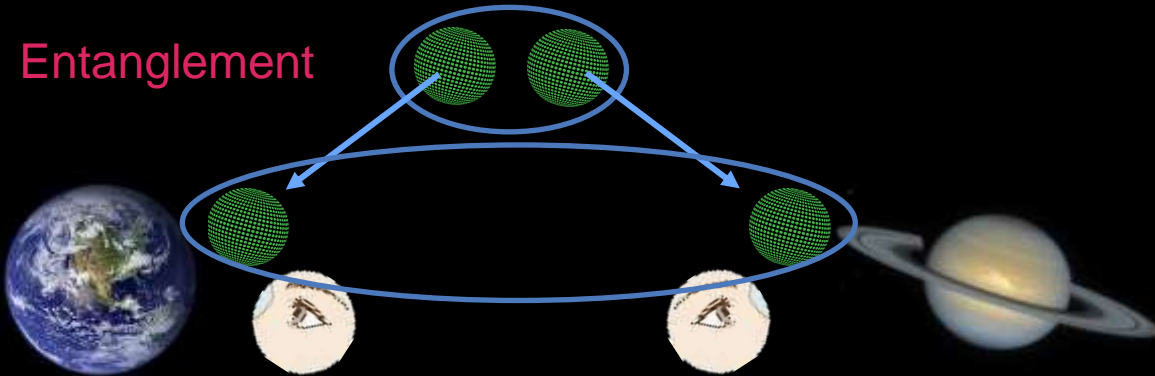


NOPE

No-Cloning Theorem: there is no valid U such that:

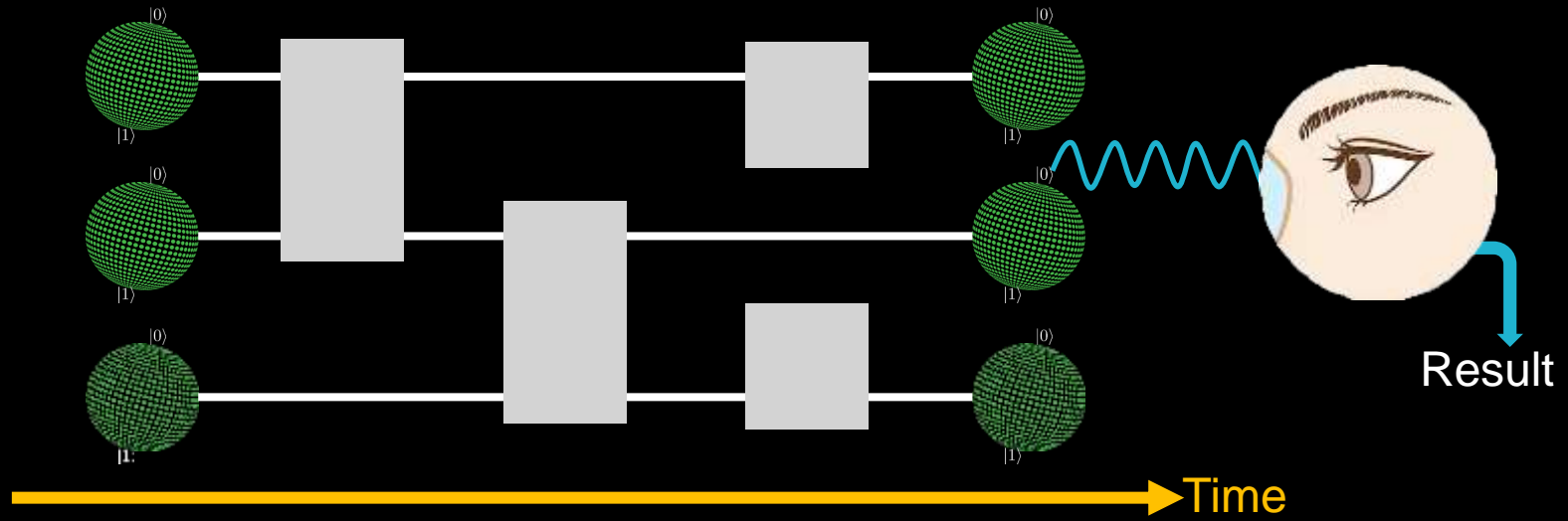


What it means: it is impossible to make a copy of an arbitrary quantum state



Recipe for a Quantum Computer

1. Find a suitable quantum physical system to be your qubit memory register
2. Apply controlled operations through a sequence of physical quantum gates
3. Measure the final state of the register to get the result



Quantum circuit: theoretical model for describing a quantum algorithm

Quantum Computers: Hard Facts

1. Building qubits and manipulating qubits to compute is **difficult** (effort scales exponentially, noise)
2. Current qubits are only stable for a **few milliseconds** (decoherence time)
3. Any computation that runs on a quantum computer can also be **simulated** on a classical computer (with memory and time overhead)
4. There is no proof that a quantum computer can achieve more than a “**modest**” **speedup** over a classical one, and only speculation for **few candidate problems**

So why is all this interesting?

Two Reasons

1. “Modest” speedup in theoretical terms translates to “huge” speedup for many practical problems (Grover’s algorithm et co., quadratic-time speedup)
2. The few candidate problems that are easy to solve on a quantum computer but (believed to be) hard on a classical computer are super important!

Security applications

Shor’s algorithm

can break the security of today’s cryptography

RSA, DLog, elliptic curves...

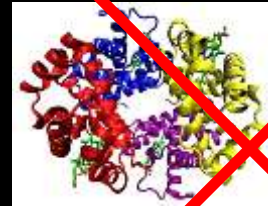


2 possible defenses

1) Quantum cryptography

2) Quantum-resistant (or post-quantum) cryptography

Civilian applications



Chemistry

Optimization & Logistics

AI, finance

and much more...

not in this talk



There is More: Quantum Security Classes

“less”
quantum

classical cryptography RSA, Diffie-Hellmann, Elliptic Curves, etc.

quantum-resistant cryptography Lattice-based, isogenies, NIST, etc.

superposition-resistant cryptography Resistant to attacks with quantum access. Spoiler: many block ciphers insecure in this scenario. Recently introduced model, controversial, very powerful, models hardware attacks.

hybrid cryptography Classical communication but local quantum computing power for honest parties. Surprisingly versatile (one-shot signatures, decentralized money, etc).

“more”
quantum

quantum cryptography The cool stuff.

Quantum Cryptography

A form of cryptography that protects information using quantum effects

“General” Quantum Cryptography

Used to protect quantum or classical data

Can only be used on a quantum computer

Not yet realizable

But will be useful one day for a quantum Internet

Allows exotic uses (uncloneable data, quantum money, etc)



Quantum Key Distribution (QKD)

Used to securely exchange classical keys

Can be used today

Requires special hardware

Implementation security must be assessed carefully



not in this talk

Quantum-Resistant Cryptography

Often called “post-quantum”

Cryptography in the traditional sense, but based on **harder mathematical problems**, resistant to quantum attacks

Can be used today on classical computers

Not as efficient as old-style cryptography

Very hard to evaluate security, scientific studies ongoing

NIST post-quantum competition: 2016-ongoing

Still a few years before final standard, but round-3 candidates already very good

Unclear when QC can break today’s cryptography, but for some data **it is already too late**

Very important to **act now** and transition to this form of cryptography as soon as possible



Post-what?

A = time necessary to research and standardize new quantum-resistant cryptography

B = time necessary to deploy the new cryptography to products on the field

C = time that today's products (or information processed therein) are required to remain secure

D = time before a scalable quantum computer is built



If $A + B + C > D$ then *you're already in trouble now!*

You should see quantum-resistant cryptography as insurance for current assets against future threats.

Post-quantum cryptography is actually pre-quantum!

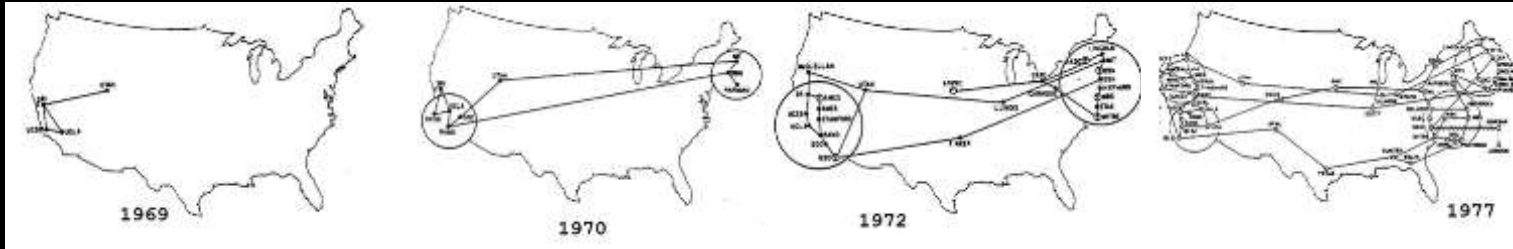
What about *future* assets?

Quantum-resistant cryptography only works on digital data. Ones and zeroes.

What if I want to protect quantum data instead?

Quantum Networks

Remember ARPANET?



When a new computing technology arises, networks soon follow

	You are here	Applications
Stage 1: point-to-point direct link		Quantum key distribution
Stage 2: entanglement-based links		Anonymous transmission, certified randomness
Stage 3: corrected memory channels		Quantum coins, accurate clock synchronization
Stage 4: quantum routing (Internet)		Distributed computing, quantum ML

Doing it wrong!

Question: do you believe that powerful quantum computers will *ever* be built?

If **NO:** then you should not worry about NIST and post-quantum. Stick to RSA and YOLO!

(also: you have quite a bold opinion. Prove that you're right and you win a 100k USD bet by Prof. Scott Aaronson, UT Austin)



If **YES:** then accept that quantum-resistant cryptography is only **part of the solution**

Not because of **security** but for **functionality** (cannot protect quantum states, only classical digital information: ones and zeroes, not qubits)

Quantum networks: expect only a short time span between “NSA has a QC” and “big banks run a QC network” ~~and “my cousin plays Quantum Fortnite with friends”~~

Welcome to the world of Quantum Cryptography!

Classic



+



OTP



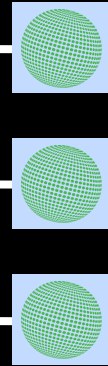
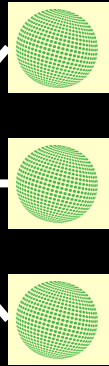
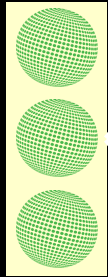
1 bit of message

=

1 bit of key

Quantum One-Time Pad

Quantum message



Quantum ciphertext



1 bit of message

=

2 bits of key

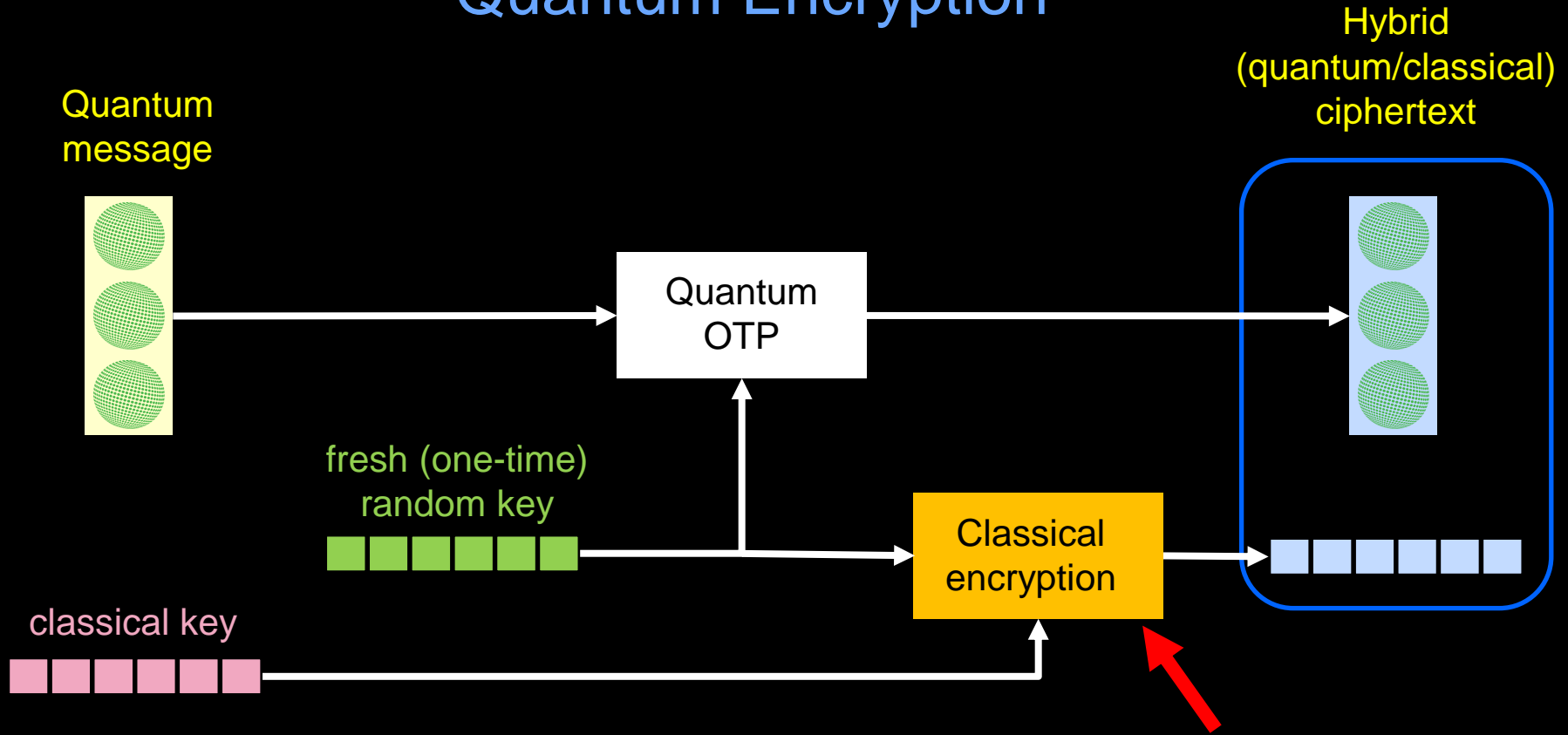
classical key



4 elementary gates:



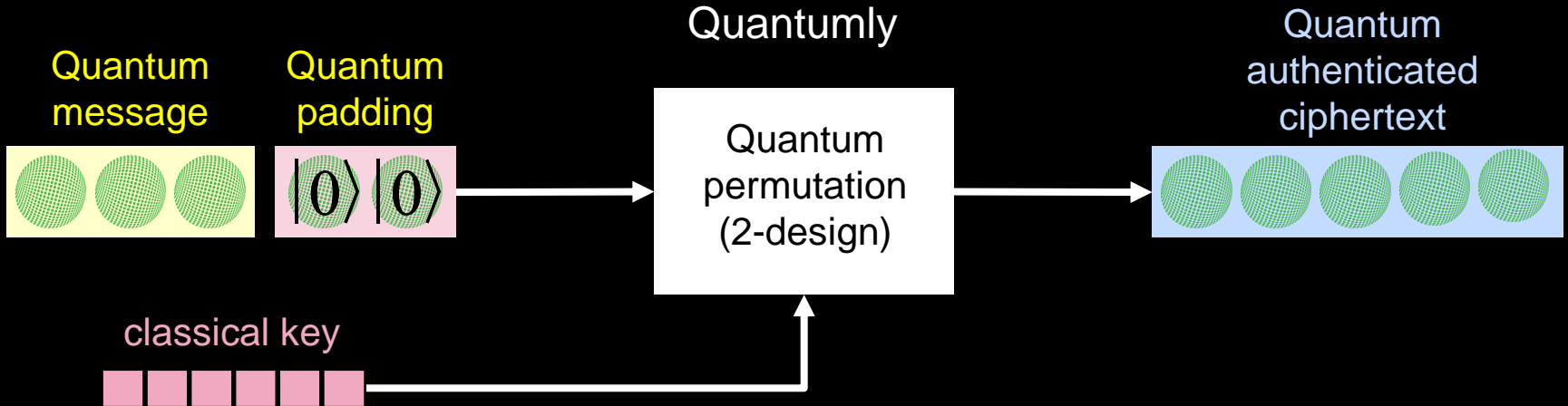
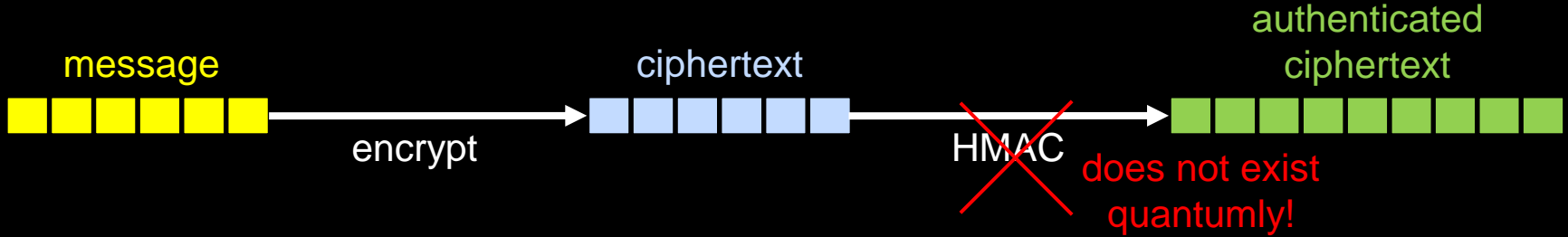
Quantum Encryption



Can be either symmetric-key (e.g. AES) or public-key (e.g. Frodo, Kyber)

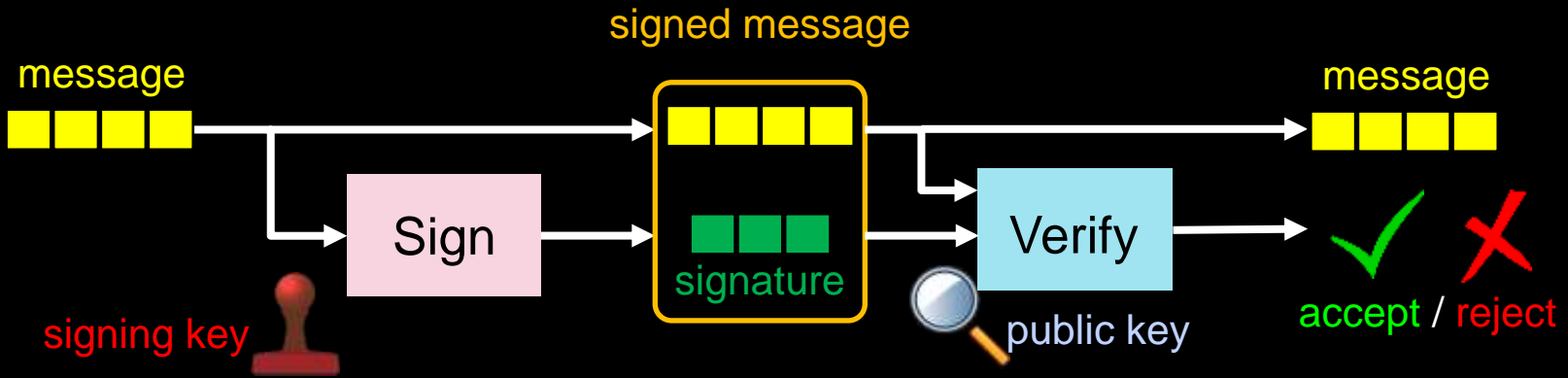
Quantum Authentication

Classically (e.g., AES-GCM)



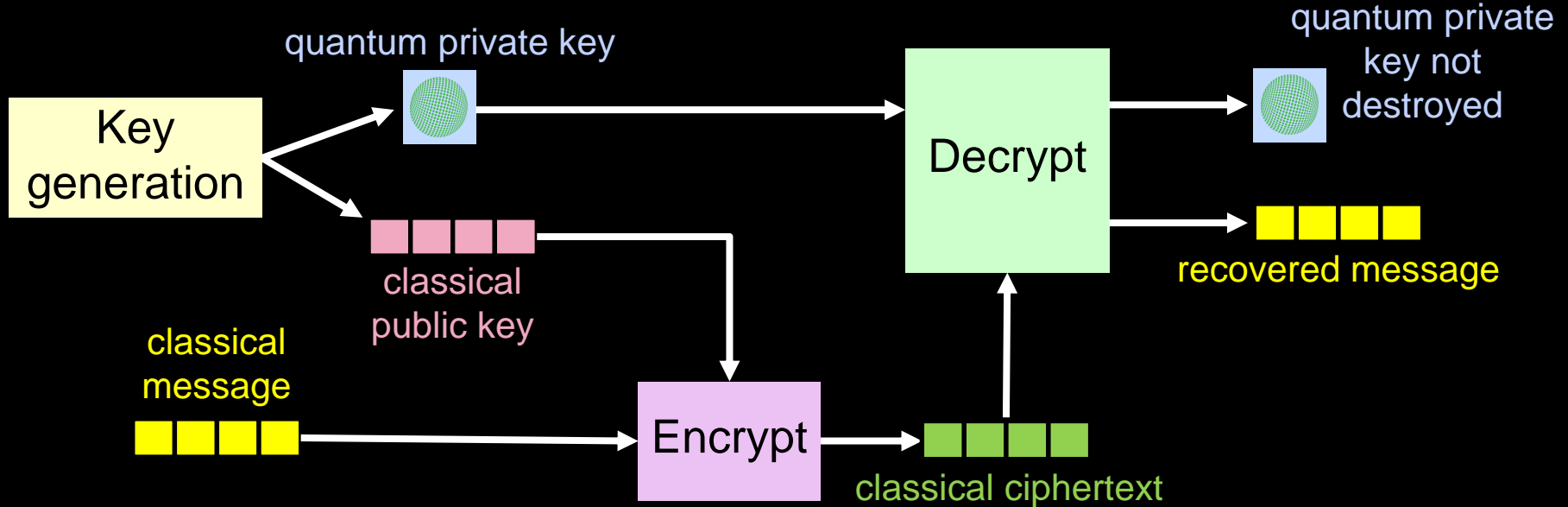
Quantum Signatures

Classically (e.g., RSA, ECDSA, Dilithium, Sphincs+)



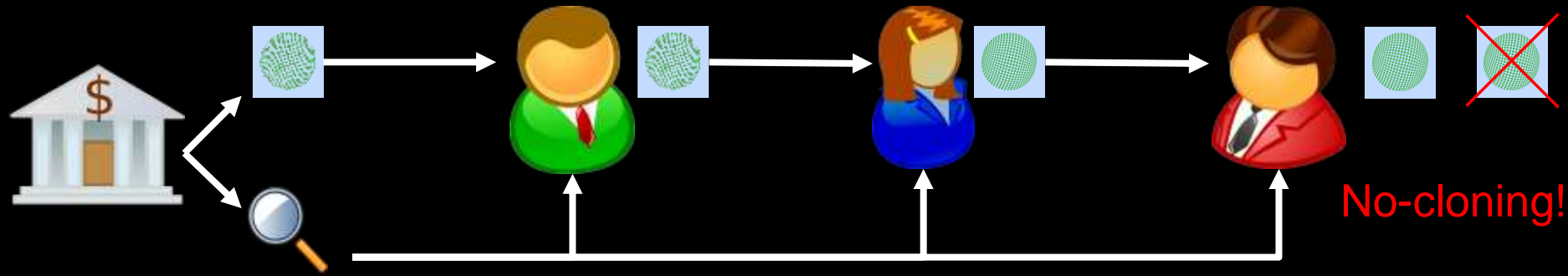
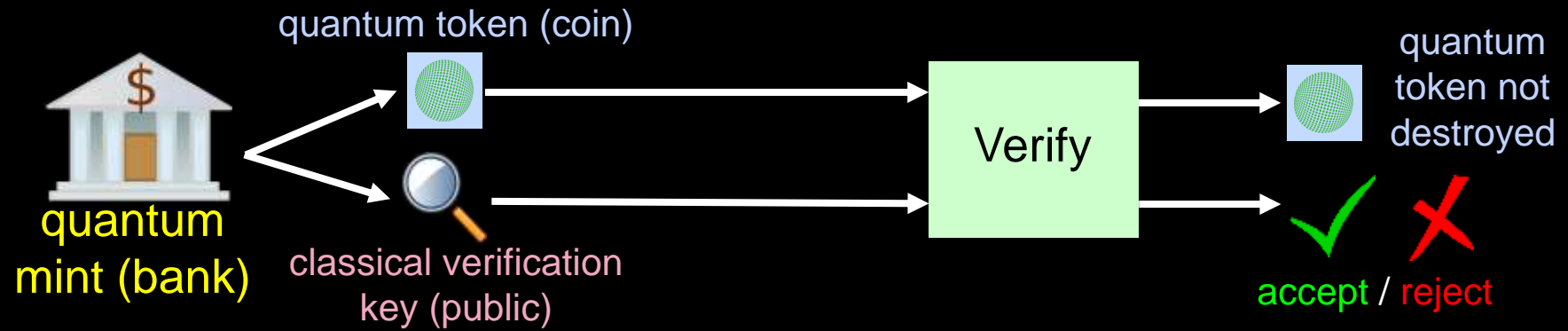
- quantum message (three green circles) + classical signature (three green squares) **IMPOSSIBLE!**
- quantum message (three green circles) + quantum signature (two purple circles) **IMPOSSIBLE!**
- classical message (four yellow squares) + quantum signature (two purple circles) **POSSIBLE**
- quantum message (three green circles) + Sign + public-key encrypt (quantum) **POSSIBLE** but without non-repudiation

Unclonable Decryption Keys



- Anybody can encrypt many times using only classical hardware
- Secret key owner can decrypt many times with local QC
- Secret keys cannot be copied!

Quantum Money



Much more...

- Quantum FHE
- Proofs of quantumness
- One-shot signatures
- Proofs of deletion
- Quantum copy-protection
- Quantum Lightning
- Byzantine agreement
- ...



Summary

Quantum computers impact many areas, in particular **security and cryptography**

“Post-Quantum” is a bad name: it is useful *today*

For **future quantum networks**: need to protect quantum data

Quantum cryptography is not only QKD

Many **exotic applications** possible

Thanks for your attention!

tommaso.gagliardoni@kudelskisecurity.com