HSLU Hochschule Luzern

Quantum – Threat or Solution?

Prof. Dr. Esther Hänggi,
Dozentin

Smartcardforum Schweiz 08.11.2023

About me

Prof. Dr. Esther Hänggi

Arbeitserfahrung

Hochschule Luzern

- Dozentin und Forscherin (seit 2019): (Quanten-) Kryptographie

Ergon (Airlock) Informatik, Zürich, Schweiz

- Senior Security Engineer (2016 - 2019): IAM Solutions

cnlab security ag, Rapperswil, Schweiz

- Security Analyst (2012 - 2016): Sicherheitsreviews

Center for Quantum Technologies, Singapur

- Senior Research Fellow (2011 - 2012): Forschung in Quanteninformation

Ausbildung

Dr. sc. (Informatik), ETH Zürich, Schweiz (2006-2010)

MSc (Physik) EPF Lausanne (2000-2005)

Agenda

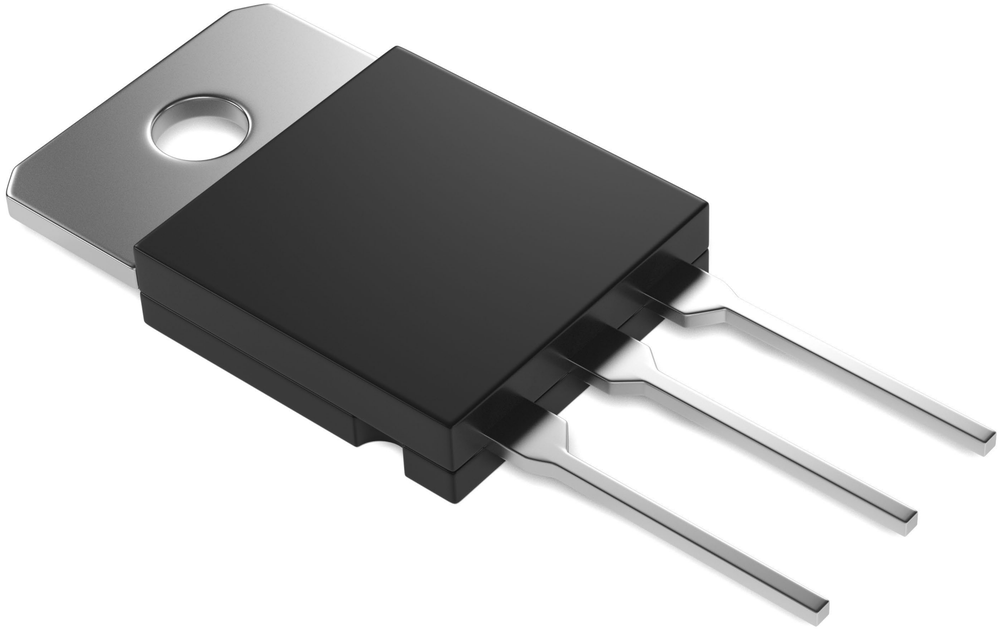
- What are quantum technologies?
- What are the implications of quantum computers on security?
- How can we achieve security against quantum computers?
  - Post-quantum cryptography
  - Quantum cryptography

Agenda

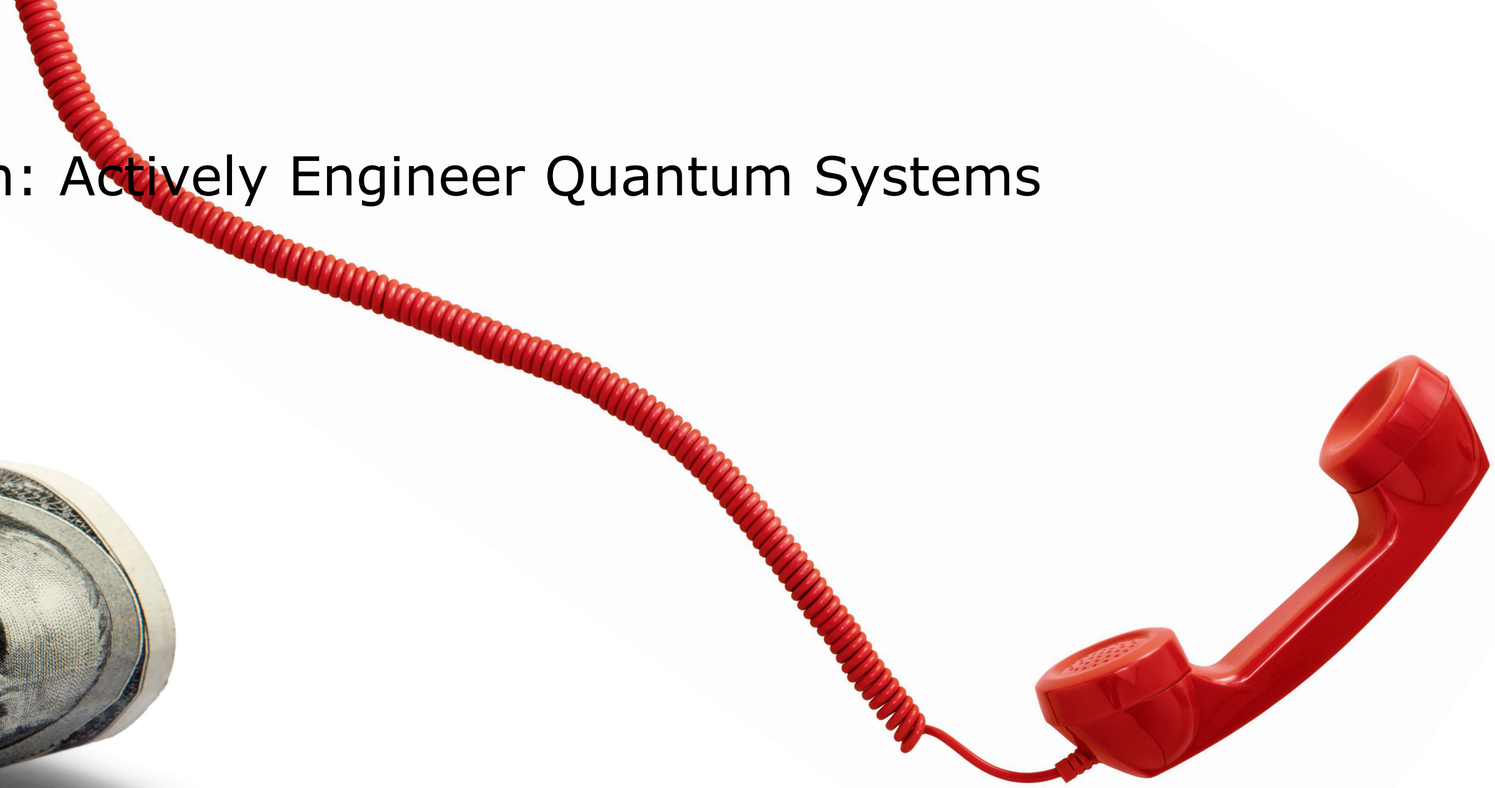
- **What are quantum technologies?**
- What are the implications of quantum computers on security?
- How can we achieve security against quantum computers?
  - Post-quantum cryptography
  - Quantum cryptography

Quantum Technologies are Already Part of our Everyday L

Quantum Technologies are Already Part of our Everyday Lifes

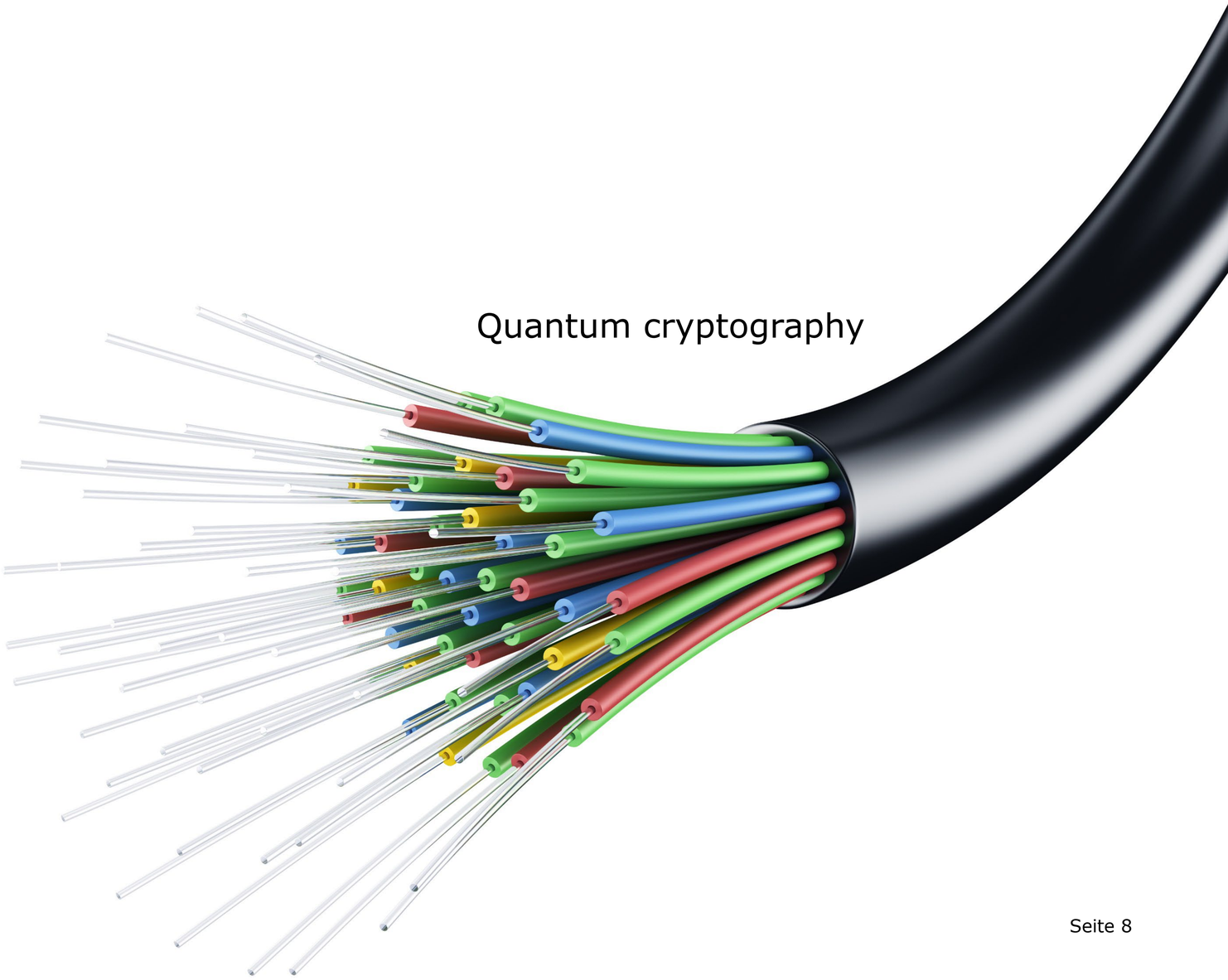


The Second Quantum Revolution: Actively Engineer Quantum Systems



The Second Quantum Revolution: Actively Engineer Quantum Systems

Quantum computer



Quantum cryptography

Why are companies interested in quantum computers?

Quantum computers are really good at solving certain specific problems

What does this mean?

They need less steps to find the solution

What exactly can they do better?

Searching
Find prime factors of a number; logarithms
Solving linear equations
Physical simulation?
Optimization?

What does this mean for security and cryptography?

Agenda

- What are quantum technologies?
- **What are the implications of quantum computers on security?**
- How can we achieve security against quantum computers?
  - Post-quantum cryptography
  - Quantum cryptography

COMPUTING

How a quantum computer could break 2048-bit RSA encryption in 8 hours

A new study shows that quantum technology will catch up with today's encryption standards much sooner than expected. That should worry anybody who needs to store data securely for 25 years or so.

By Emerging Technology from the arXiv — May 30, 2019

Cryptographers Are Racing Against Quantum Computers

Today's security schemes will soon be obsolete.

Tammy Xu — April 30, 2021 · Updated: June 28, 2021

10.06.2021 | **Networks & Platforms** | **Thought Leadership**

Quantum computing will break today's encryption standards - here's what to do about it

By: William F. Copeland

Quantum computing will break the encryption used in e-commerce and VPNs someday. The race is on to develop quantum-safe algorithms and procedures before that happens. The remedy will be found in physics or mathematics.

NSA working on quantum computer to break any encryption

The spy agency is reportedly in a race to build its own quantum computer to stay ahead of others seeking to own the mother of all decryption machines.

Mark Dodds
Jun 30, 2019 · 11 min read ★ · Listen

How Quantum Computers Will Break Your Phone's Encryption

Jatin Mehta
Feb 26, 2020 · 9 min read · Listen

Quantum Computers: Doomsday for Modern Encryption

A look into how quantum computers break RSA encryption by understanding the unique properties of quantum computers and Shor's algorithm.

QUANTUM COMPUTING AND THE END OF ENCRYPTION

by: Maya Posch — 57 Comments

June 11, 2020

SECURITY & PRIVACY

How Quantum Computing Will Affect Computer Security and Passwords

Posted on October 29th, 2020 by Kirk McElhearn

Microsoft Azure Quantum Blog

Cryptography in the era of quantum computers

February 26, 2020 • 5 min read

Home > Security > Encryption

NEWS ANALYSIS

How quantum computers will destroy and (maybe) save cryptography

Quantum computer advances mean we might have only a few years before they can break all public key encryption. The day when every secret is known is near.

The race for quantum-resistant cryptography

By Heidi Vella

Published Thursday, January 20, 2022

That large-scale universal quantum computers could break widely used encryption methods is well known, but what was once seen as a distant, even theoretical, problem is now driving the latest technology race.

THURSDAY, MARCH 31, 2022

On the Radar: Is 2022 the year encryption is doomed?

Future-proofing the internet

Quantum computers will break the encryption that protects the internet

Fixing things will be tricky

IBM warns of instant breaking of encryption by quantum computers: 'Move your data today'

Welcome to the future transparency of today as quantum computers reveal all currently encrypted secrets -- a viable scenario within just a few years.

Quantum computers could crack today's encrypted messages. That's a problem

We'll likely see the top picks for safer, post-quantum encryption technology early in 2022.

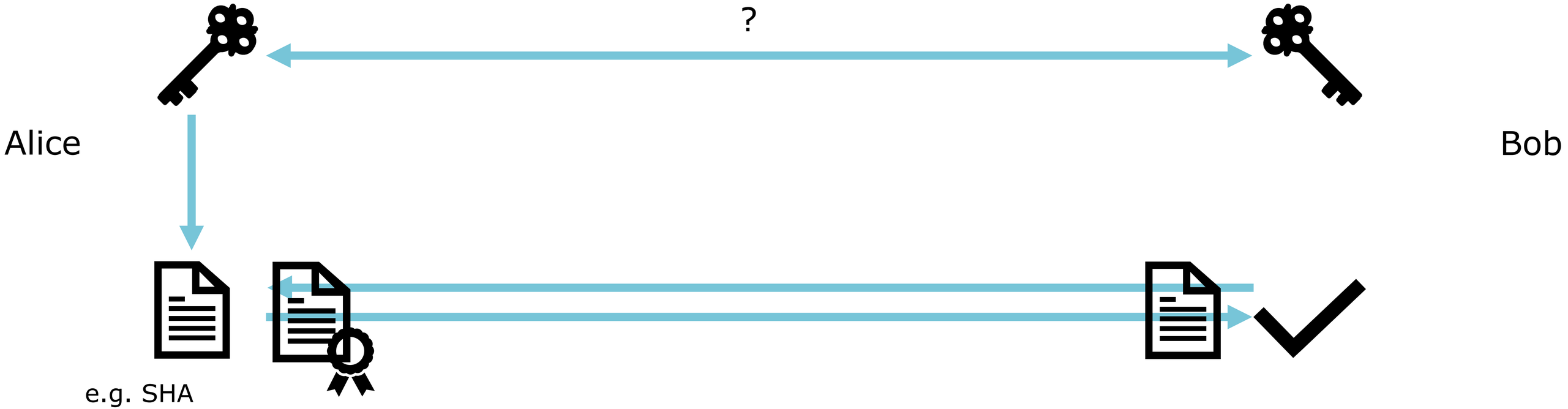
Cryptography is used for: secret communication

A shared key allows to send encrypted messages

Cryptography is used for: secret communication & authentication

A shared key allows to send encrypted messages & authenticate messages or entities

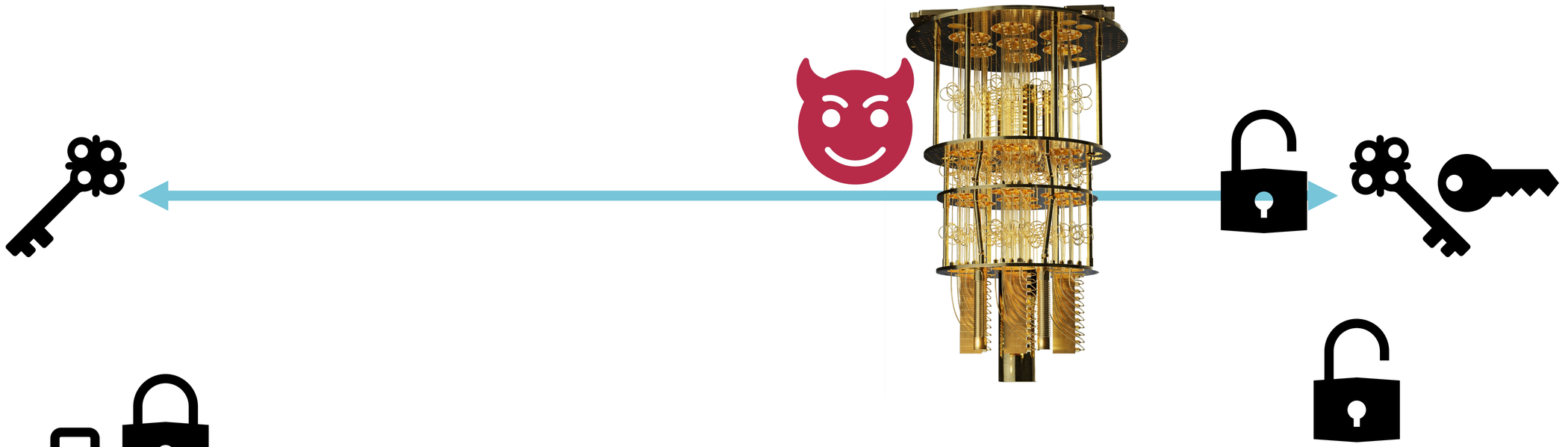
Cryptography is used for: secret communication & authentication



A shared key allows to send encrypted messages & authenticate messages or entities

How can we obtain a shared key?

Key exchange with public key cryptography



RSA, (Elliptic Curve) Diffie-Hellman

Security bases on mathematical problems which are thought to be
- Easy to calculate for the honest parties
- Hard to invert for an adversary

E.g. multiplying vs. factoring

Broken by Quantum Computer!

Public key cryptography is also used for electronic signatures & authentication!

Effects of quantum computers on cryptography

Symmetric cryptography Requires a shared key!

- Encryption with symmetric cipher:
  AES, (DES, 3DES)
- Message authentication with hash function:
  SHA, (MD5)
- Challenge-response authentication with hash function:
  SHA, (MD5)

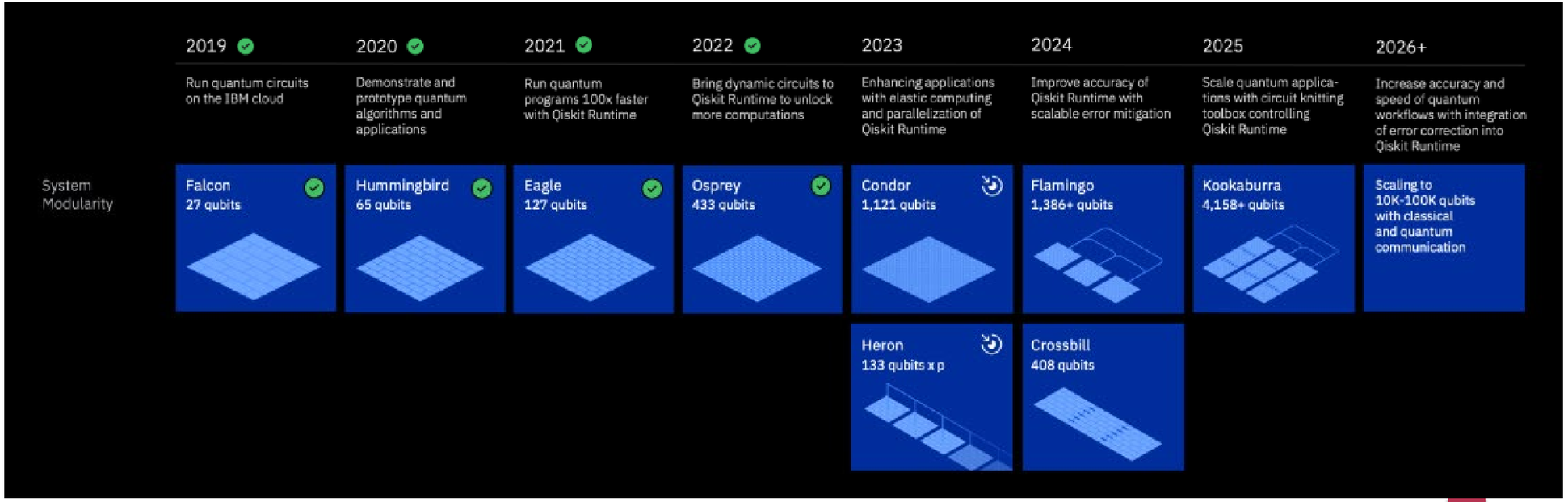
Weakened

Public key cryptography

- Encryption (key exchange) with asymmetric algorithm:
  RSA, DH, ECDH
- Electronic signature:
  RSA, DSA
- Challenge-response authentication with signature:
  RSA, DAS

Broken

How far is the implementation of quantum computers?



Source: IBM https://www.ibm.com/quantum/roadmap

20’000’000 qubits

Needed to break 2048-bit RSA in 8 hours

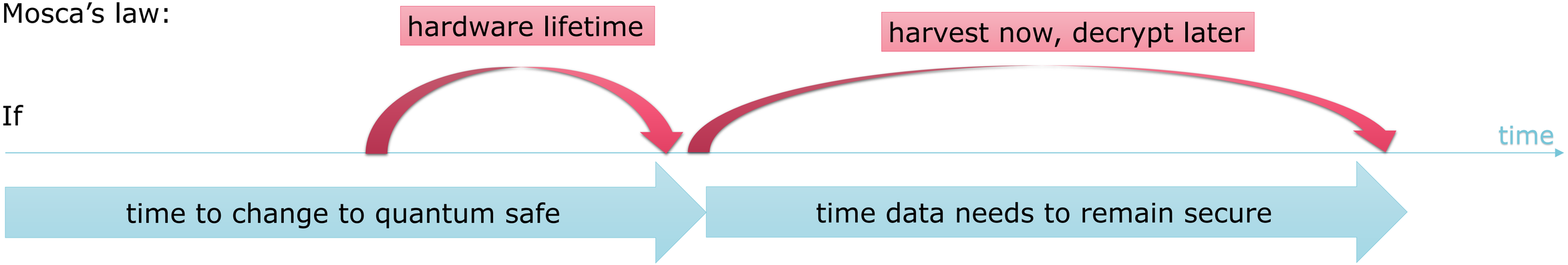
Source: https://quantum-journal.org/papers/q-2021-04-15-433/

When do we need to start worrying about quantum computers?

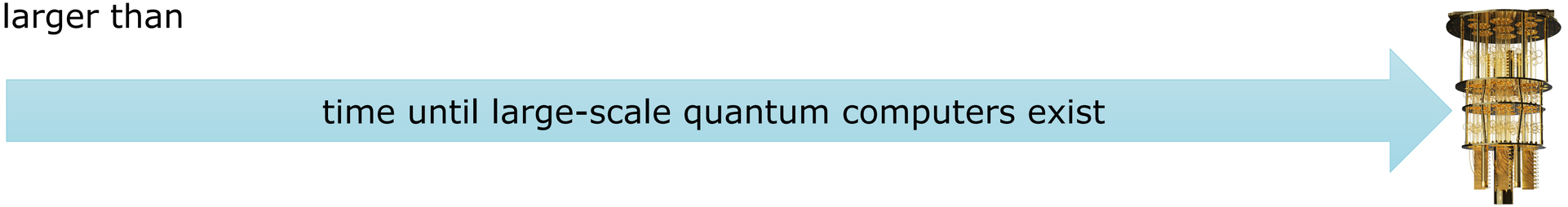
Relevant time depends on application:
- secret message
- authentication for e-banking
- electronic signature of a mortgage

Mosca's law:

If



larger than



then problem!

Agenda

- What are quantum technologies?
- What are the implications of quantum computers on security?
- **How can we achieve security against quantum computers?**
  - Post-quantum cryptography
  - Quantum cryptography

How to do cryptography in the era of quantum computers?

Post-quantum cryptography

Base on different mathematical problems

NIST «competition» to solicit, evaluate, and standardize quantum-resistant public-key cryptographic algorithms

- encryption / key exchange
- Signature

https://csrc.nist.gov/projects/post-quantum-cryptography

Current project at HSLU (joint with industry partner essendi xc)

- Implications of post-quantum cryptography on certificate management
- Benchmarking post-quantum cryptography from NIST competition
- Integrating post-quantum cryptography with current system (change process)

How to do cryptography in the era of quantum computers?

Post-quantum cryptography

Base on different mathematical problems

NIST «competition» to solicit, evaluate, and standardize quantum-resistant public-key cryptographic algorithms

- encryption / key exchange
- Signature

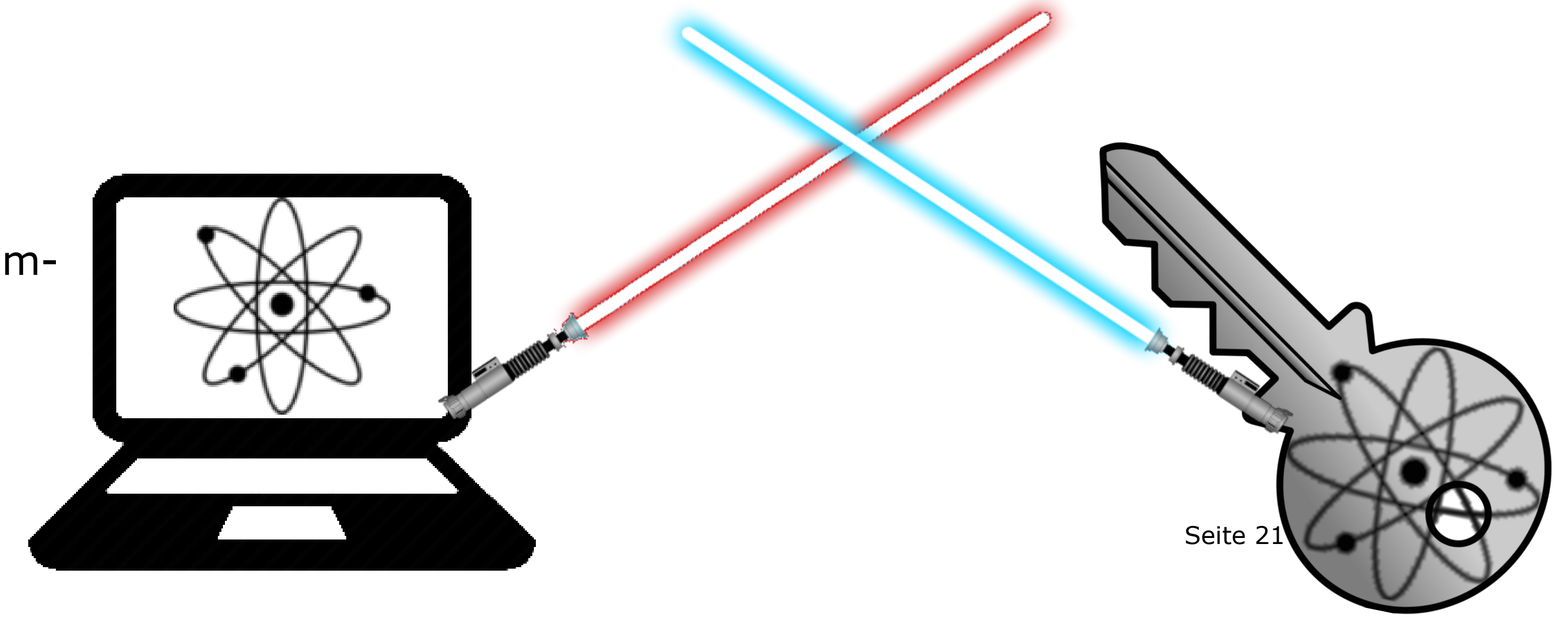
https://csrc.nist.gov/projects/post-quantum-cryptography

Quantum cryptography

Use physical properties to achieve security

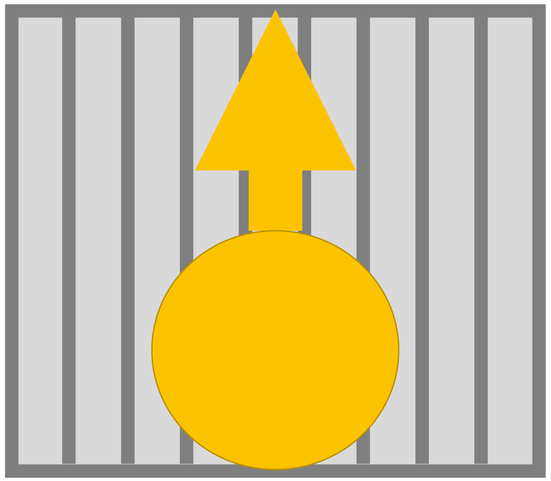
Quantum Key Distribution

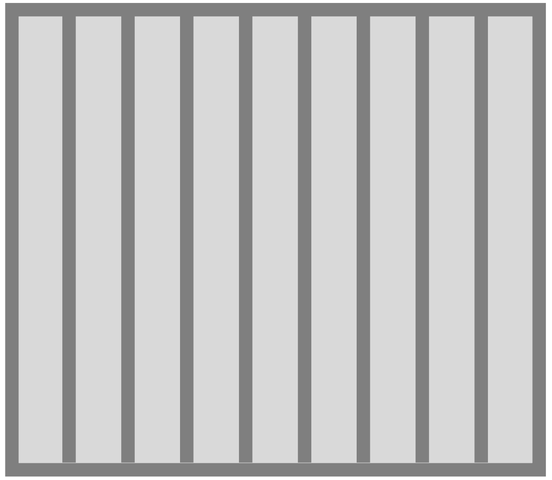
Quantum Random Number Generation



Quantum cryptography uses properties of quantum physics to achieve security

Alice



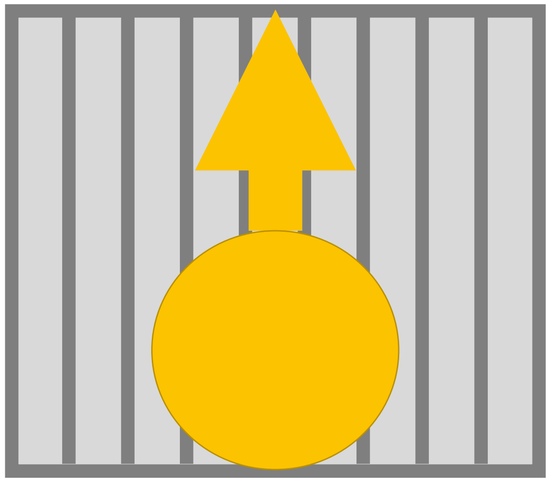


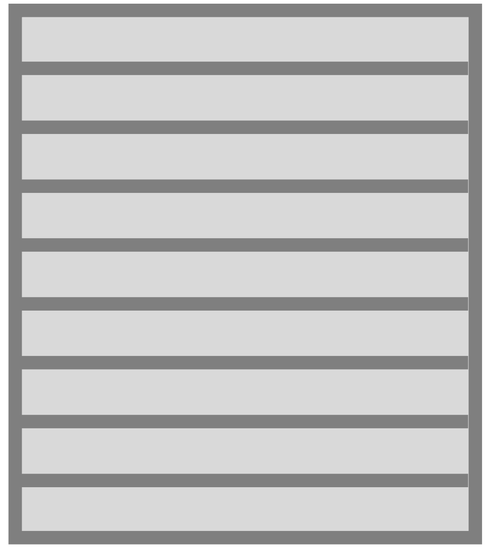
Bob

0° → Photon passes

Quantum cryptography uses properties of quantum physics to achieve security

Alice



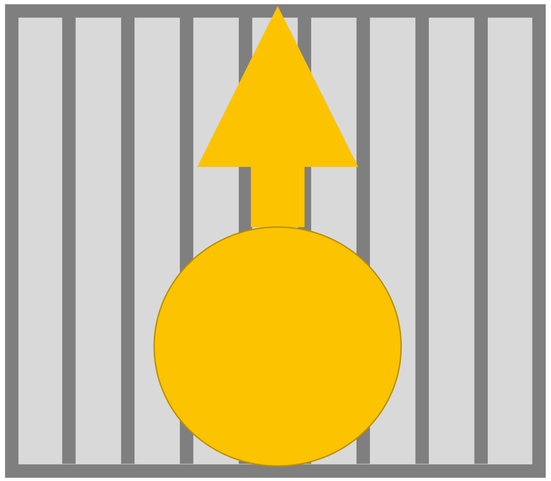


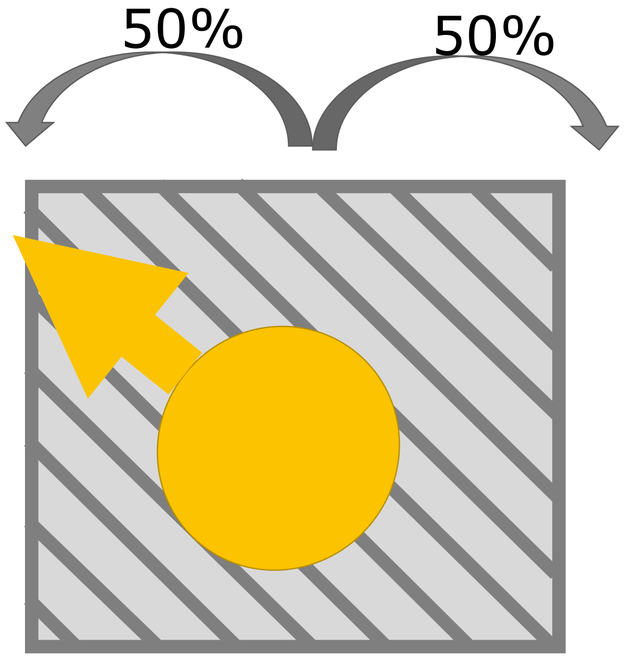
Bob

0° → Photon passes
90° → Photon reflected

Quantum cryptography uses properties of quantum physics to achieve security

Alice



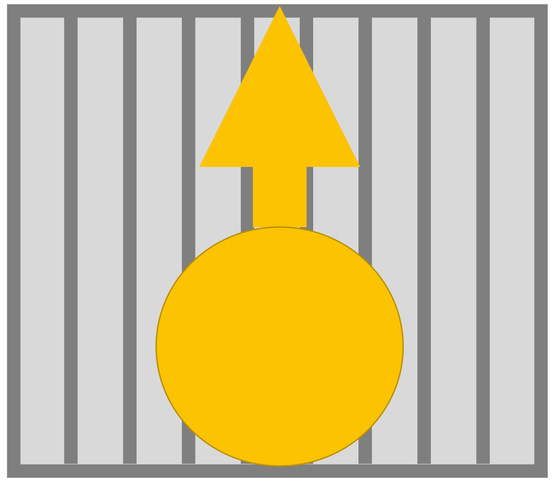


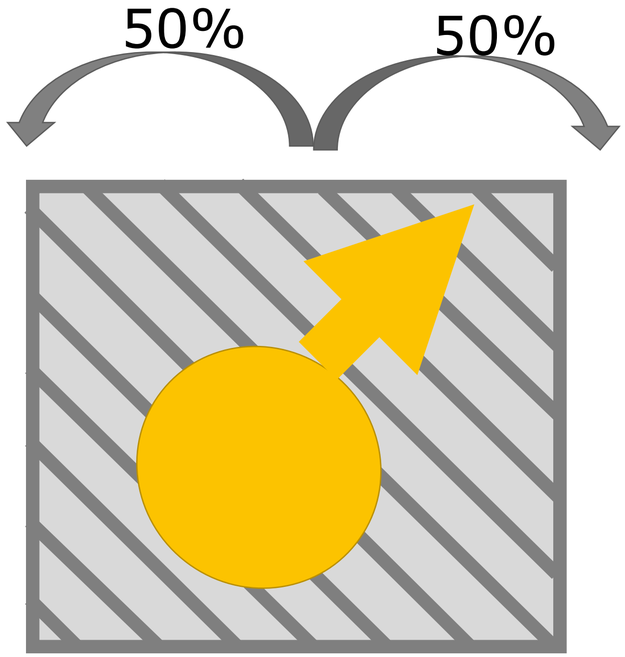
Bob

0° → Photon passes
90° → Photon reflected
45° → 50% probability

Quantum cryptography uses properties of quantum physics to achieve security

Alice





Bob

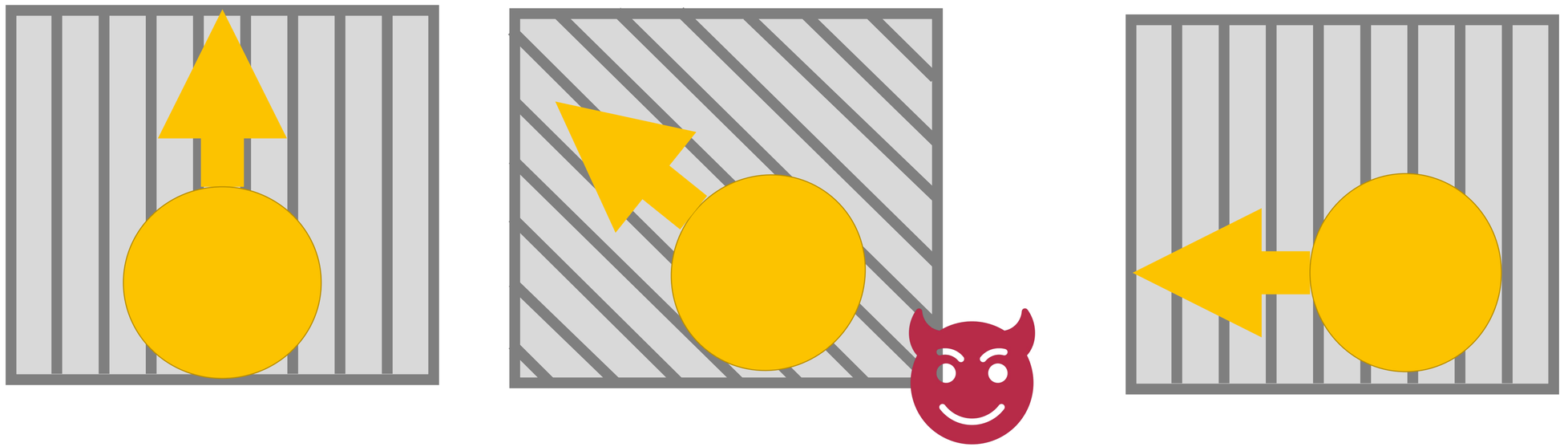
0° → Photon passes
90° → Photon reflected
45° → 50% probability

Quantum Random Number Generator (QRNG)

Changes polarisation direction!

Quantum cryptography uses properties of quantum physics to achieve security

Alice

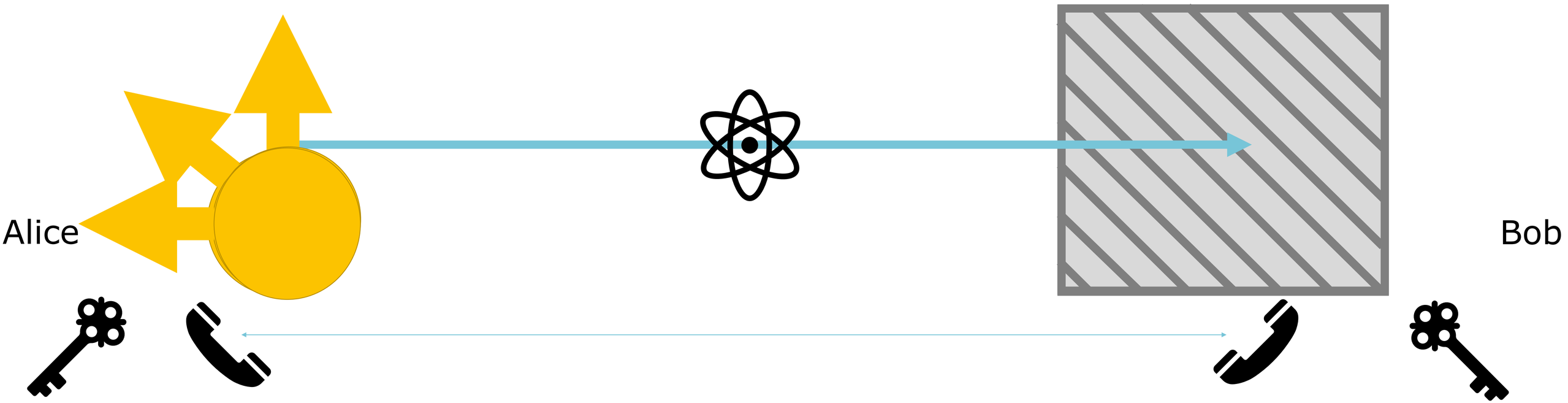


Bob

Observation changes polarization!

Can detect eavesdropper!

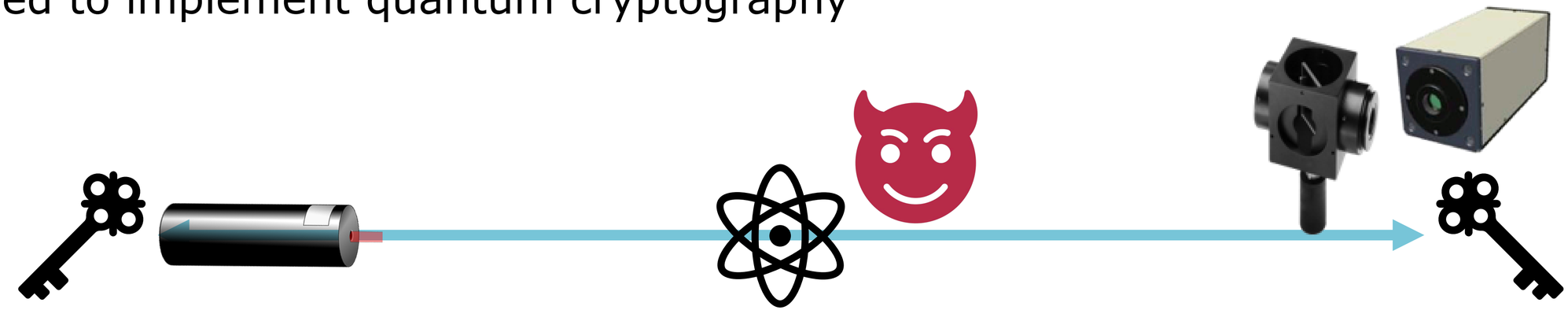
Quantum key distribution (QKD)



1. Send photons in randomized polarization direction -45°, 0°, 45°, 90°
2. Measure with filter randomized either at 0° or 45°
3. Over classical authentic channel
   1. Remove data with non-matching basis
   2. Check if eavesdropper present from small random sample of the data
   3. Create key from remaining data

Different type of security: An eavesdropper will be detected

Needed to implement quantum cryptography



Alice

Bob

Needed

Direct communication line (optical fiber)

Laser

Beamsplitter

Single photon detector

Not needed

Quantum Computer

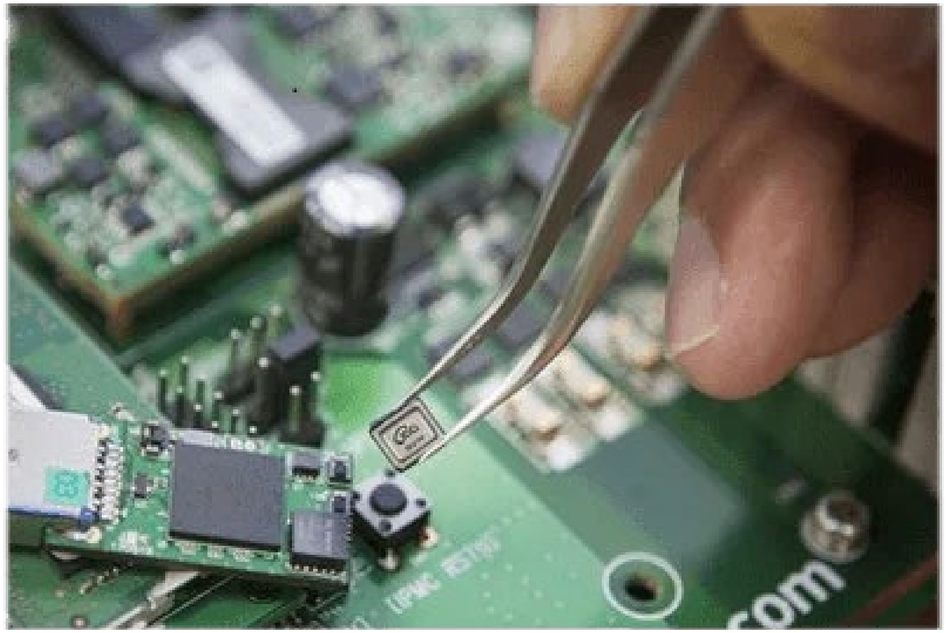
Quantum memory

Complicated particle interactions

But remains secure if adversary has one!

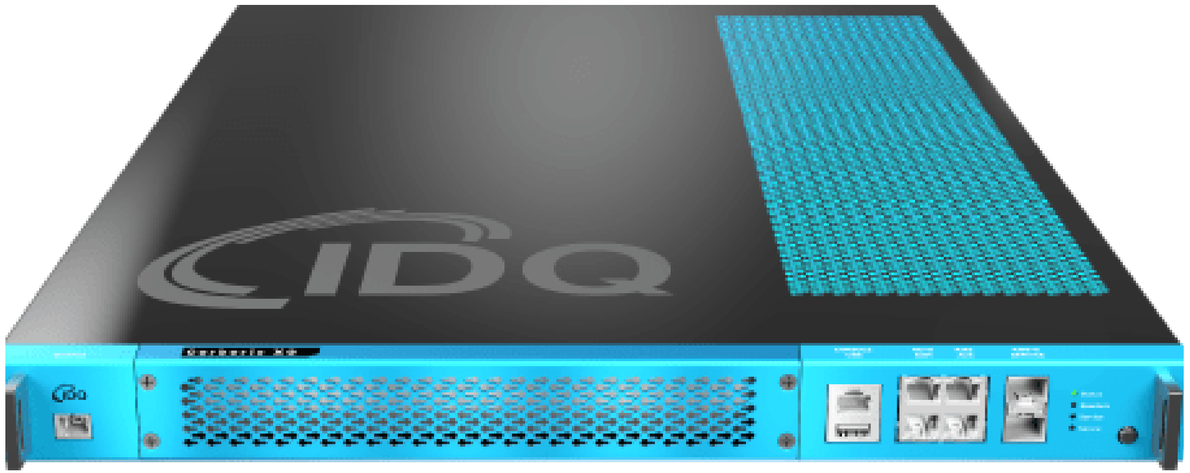
Commercial QRNG and QKD devices are being produced today!

Quantum Random Number Generators



Samsung Galaxy Quantum 4

Quantum Key Distribution Devices



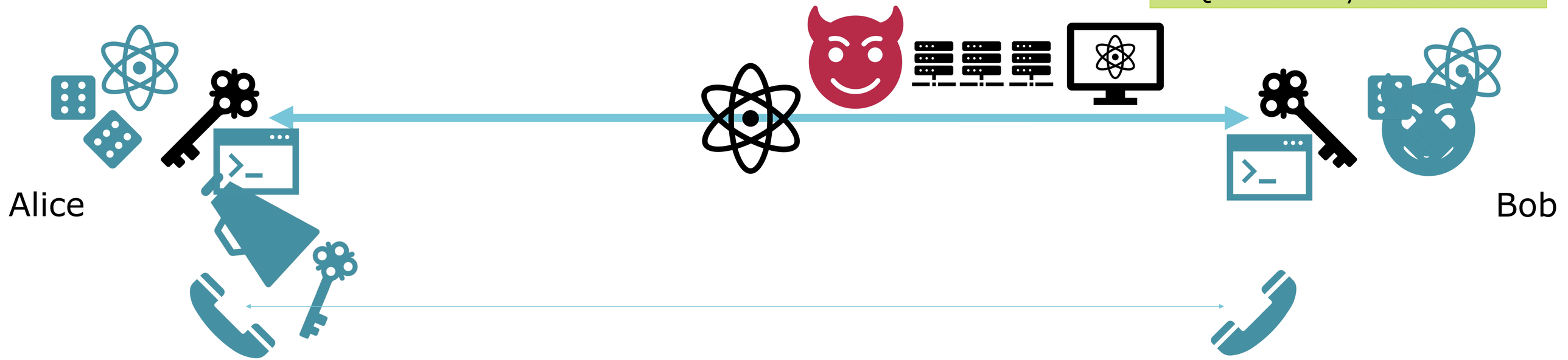
Source: IdQ https://www.idquantique.com/

Prerequisites for quantum key distribution

Also needed for «classical» cryptography!

Transition roadmap:

1. Quantum random numbers
2. Post-quantum algorithms
3. Quantum key distribution



Authentication → start with small key or combine with «classical» (quantum-safe) authentication protocol

Local randomness → use a quantum random number generator

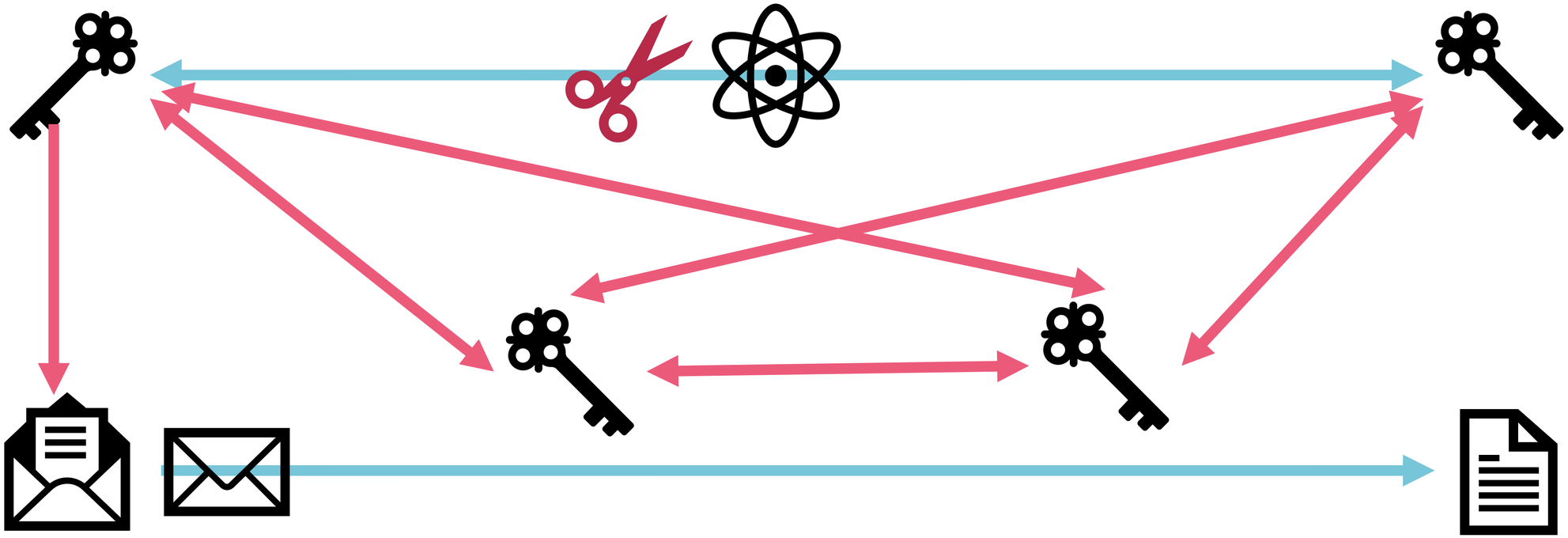
Information leakage → careful integration

Precise devices → post-processing (integrated in commercial device)

Current projects at HSLU

- Integration of QRNG
- Fast and verifiable post-processing algorithms

Practical challenges



Optical fibre: point-to-point connection → secure network, key management?

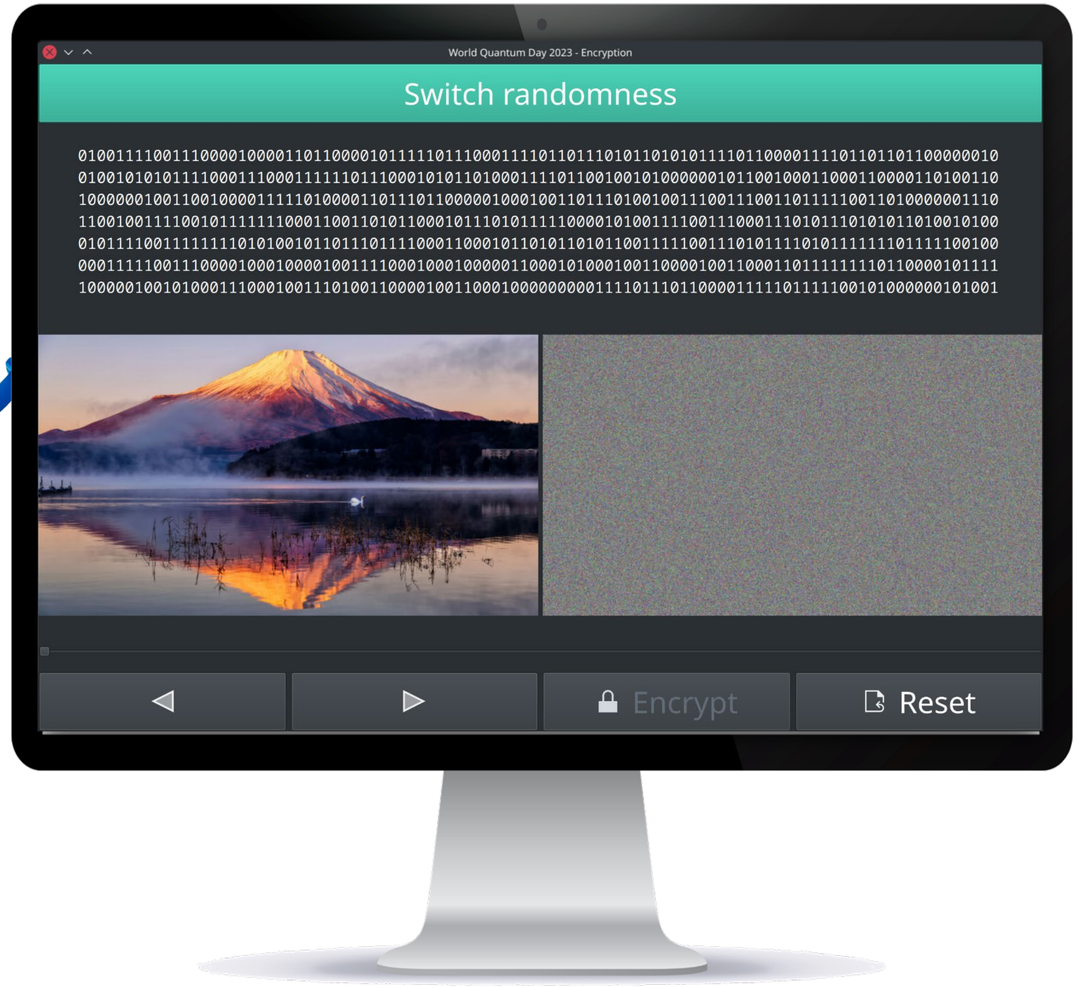
Denial of service → fallback mechanisms

Fully secure system → integration into encryption protocol

Current projects at HSLU

- Combination of quantum with additional mechanisms s.t. the system is secure if either condition holds

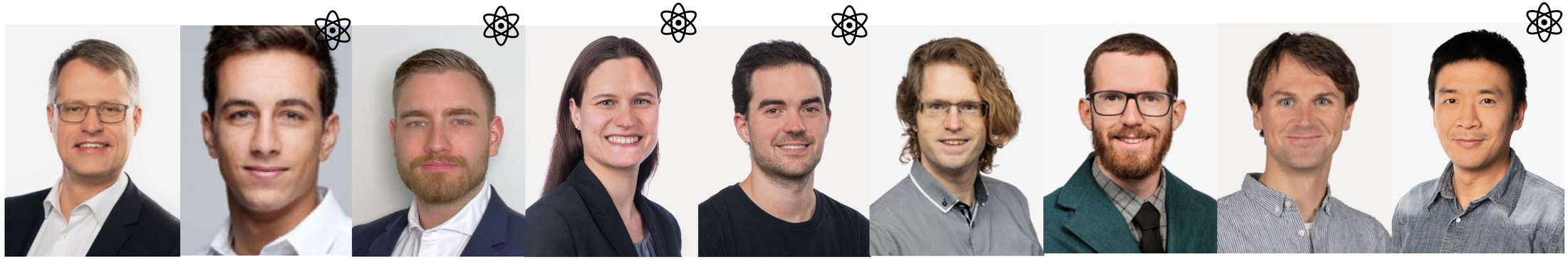

OptiPlex 7050
Quantique
Quantum Random Number Generator
Made in Switzerland
www.idquantique.com


World Quantum Day 2023 - Encryption
Switch randomness
Encrypt
Reset

QUANTUMLAB

Come and talk to us if you are interested in the following questions:

- Where can we apply quantum / post-quantum cryptography in our company?
- What would this change mean for us from an operational and security perspective?
- How can the change process be done?
- Can we devise a «hybrid» setup?
- How can we integrate quantum cryptography into our system? (PoCs for QRNG and/or QKD)
- Or any other questions related to security or cryptography ;-)



HSLU Applied Cyber Security Research Lab: https://www.hslu.ch/en/lucerne-school-of-information-technology/research/applied-cyber-security/

HSLU Lucerne University of Applied Sciences and Arts

School of Computer Science and Information Technology
Research
Prof. Dr. Esther Hänggi
Lecturer

esther.haenggi@hslu.ch