Cryptography and Quantum Key Distribution for long term secret storage

Thomas Prévost, Bruno Martin, Olivier Alibart, Marc Kaplan, Anne Marin

Agenda

01

LONG TERM SECRET STORAGE?

02

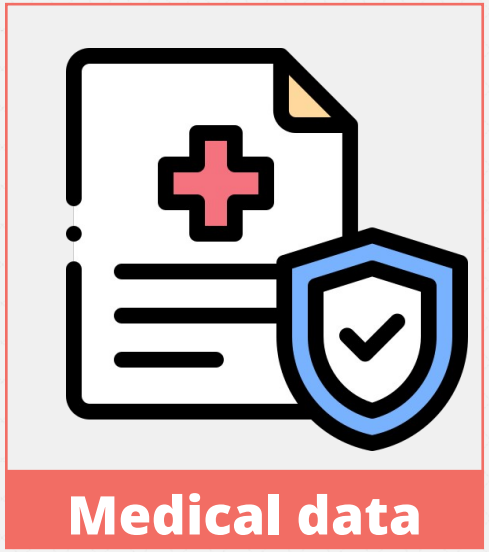
BACKWARD COMPATIBLE EXTENDED QUANTUM TRANSMISSION

03

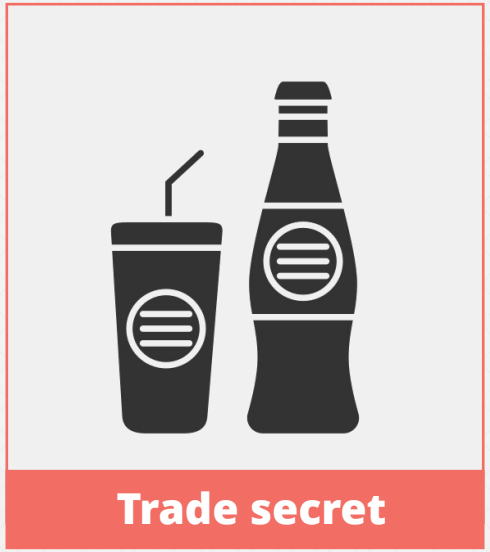
MULTISS: DISTRIBUTED QUANTUM STORAGE

Why long term secret storage?

Some data may require confidentiality over decades



Medical data



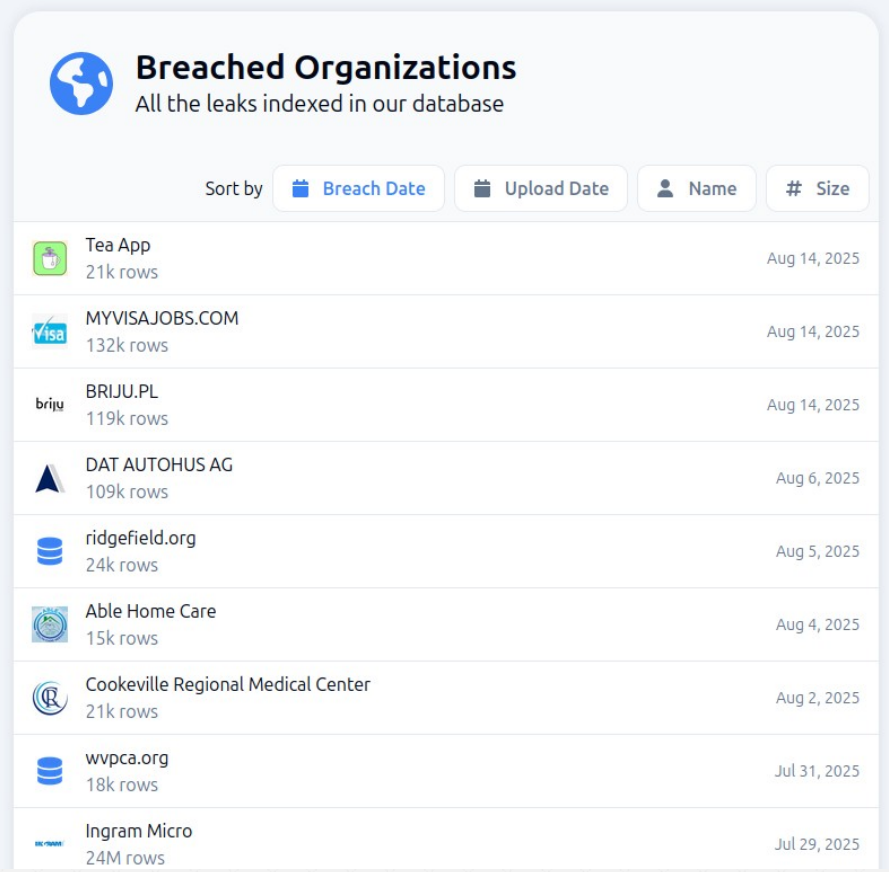
Trade secret

State secret

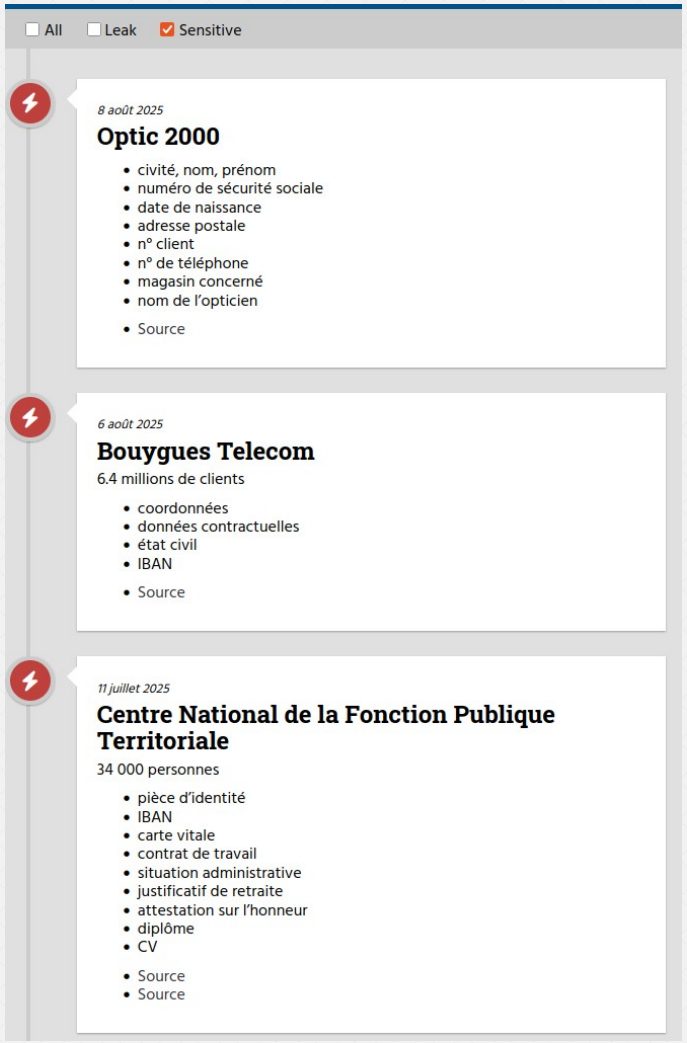
Cloud storage: risky

More and more organisation migrate their data storage on the Cloud for cost and praticity

Data leaks

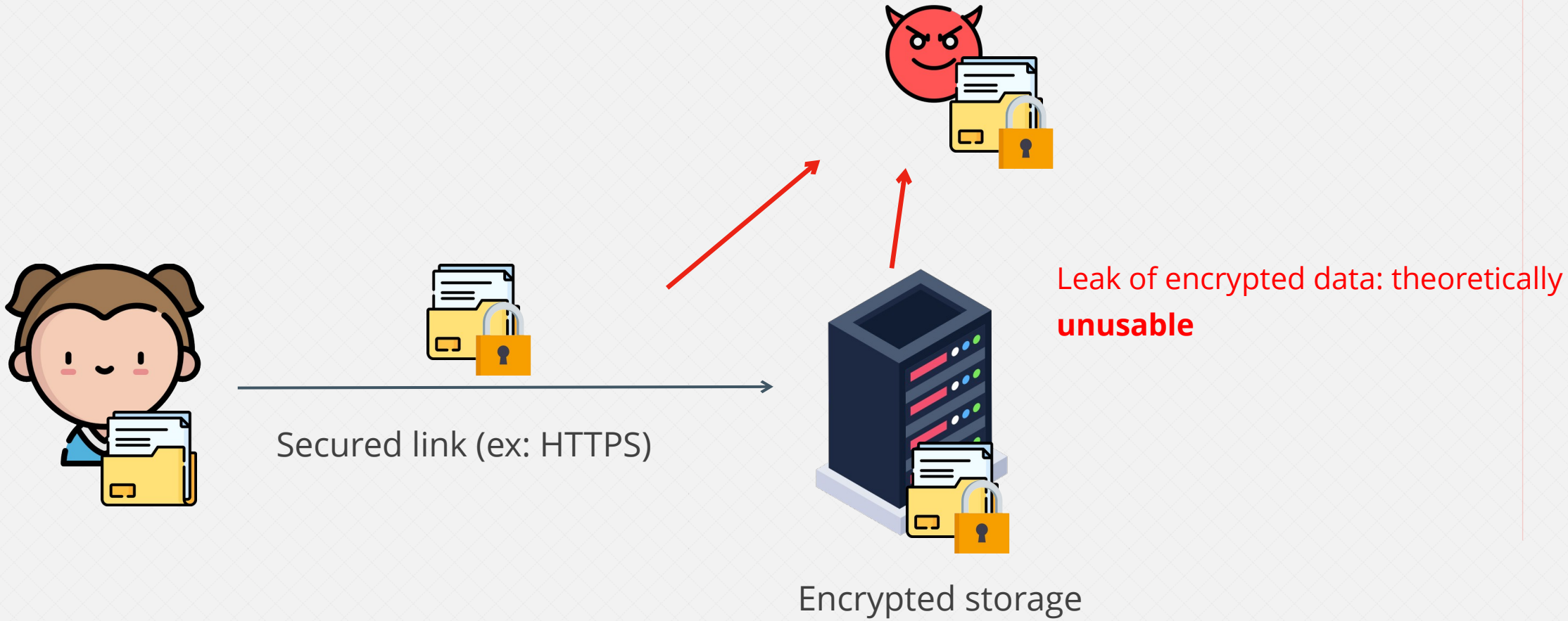


Source: https://databreach.com/breach



Source: https://bonjourlafuite.eu.org/

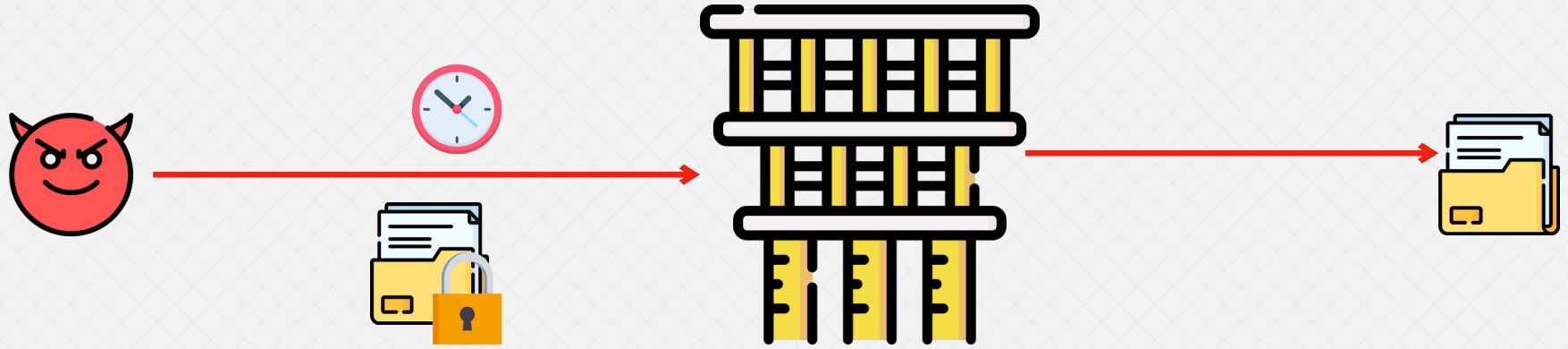
Solution: cryptography



Required for managing credit cards, for example (PCI-DSS)

Long term cryptography?

Increased computing power, advances in cryptanalysis, and the advent of quantum computers will allow an attacker to break current encryption



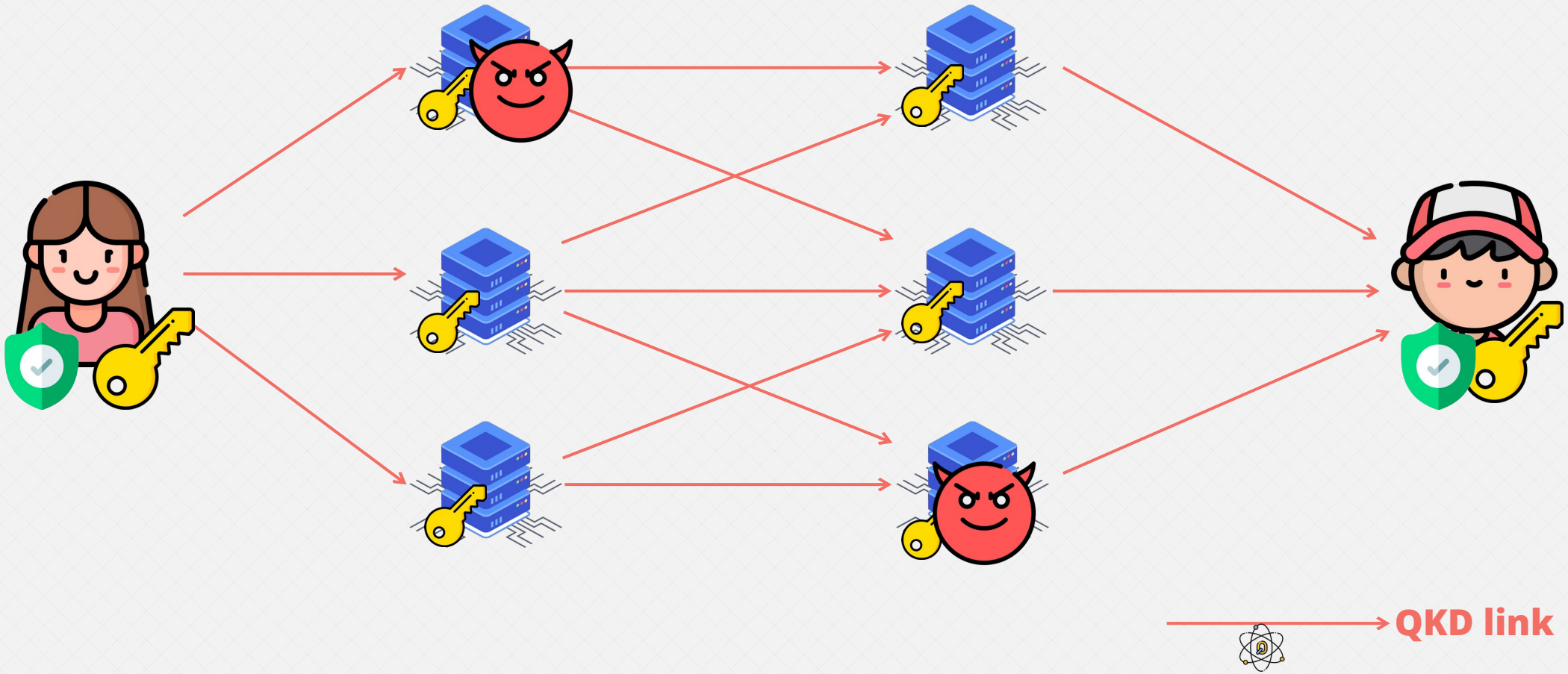
«*Harvest now, decrypt later*» attack

Post-quantum cryptography?

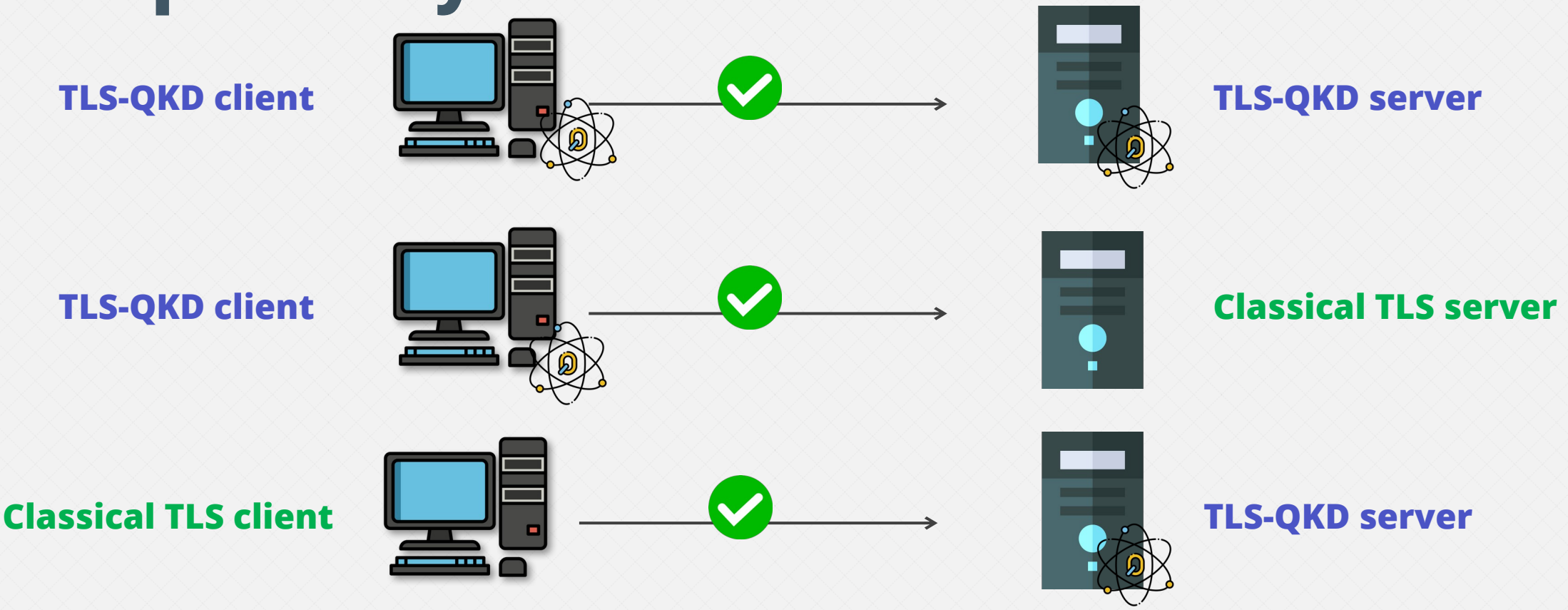
The mathematical foundations are too recent for "long-term security"

TLS-QKD: BACKWARD COMPATIBLE EXTENDED QUANTUM TRANSMISSION

Extended transmission

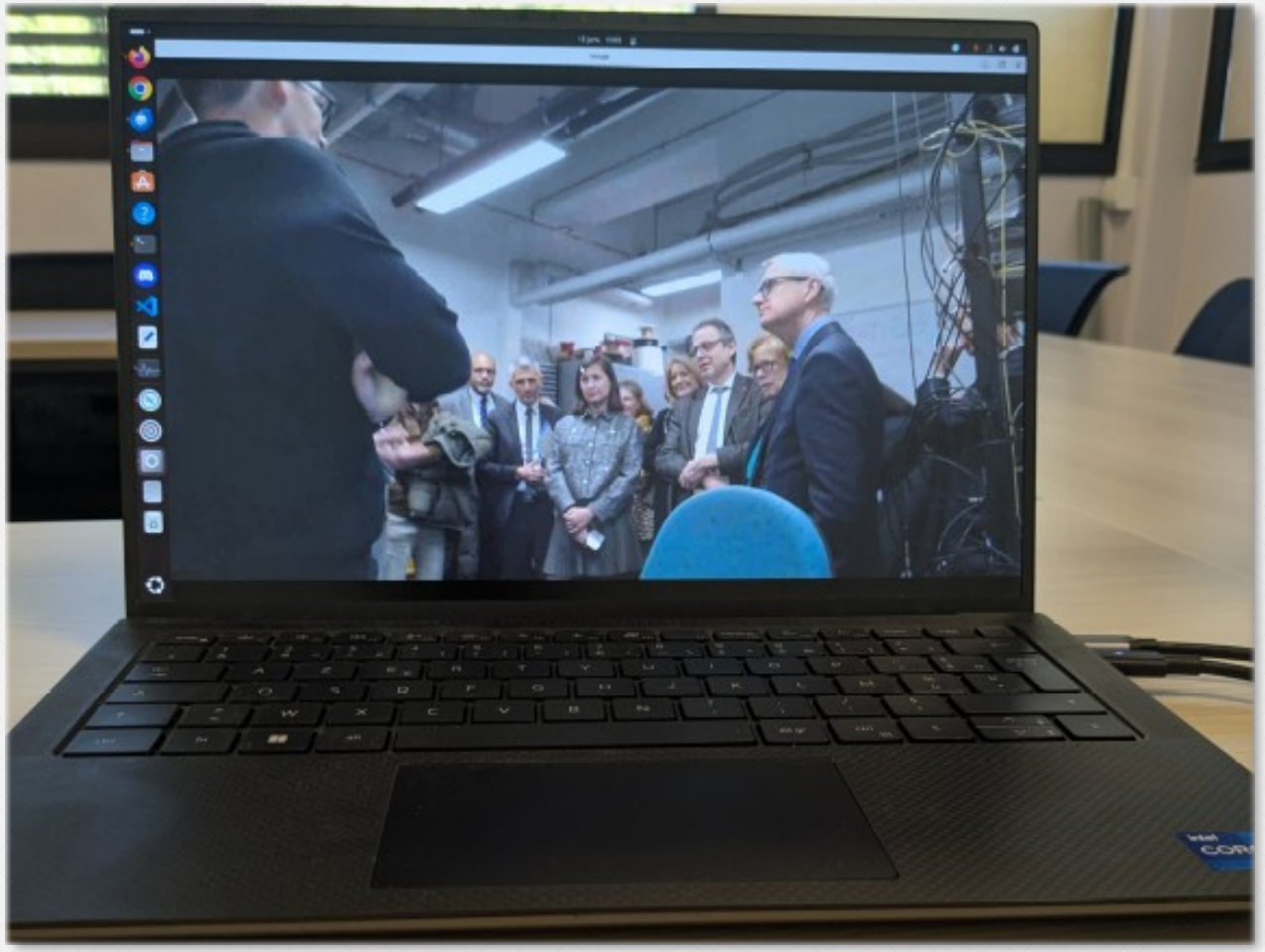


TLS (HTTPS) backward compatibility



Two-way backward compatibility facilitates the gradual migration of existing systems

Demonstration



Demonstration of a video conference call encrypted with quantum keys during the inauguration of the INPHYNI laboratory, on January 15, 2025, between Nice and Sophia-Antipolis

i3S sophia antipolis

INPHYNI INSTITUT DE PHYSIQUE DE NICE

cnrs

Inria

UNIVERSITÉ CÔTE D'AZUR

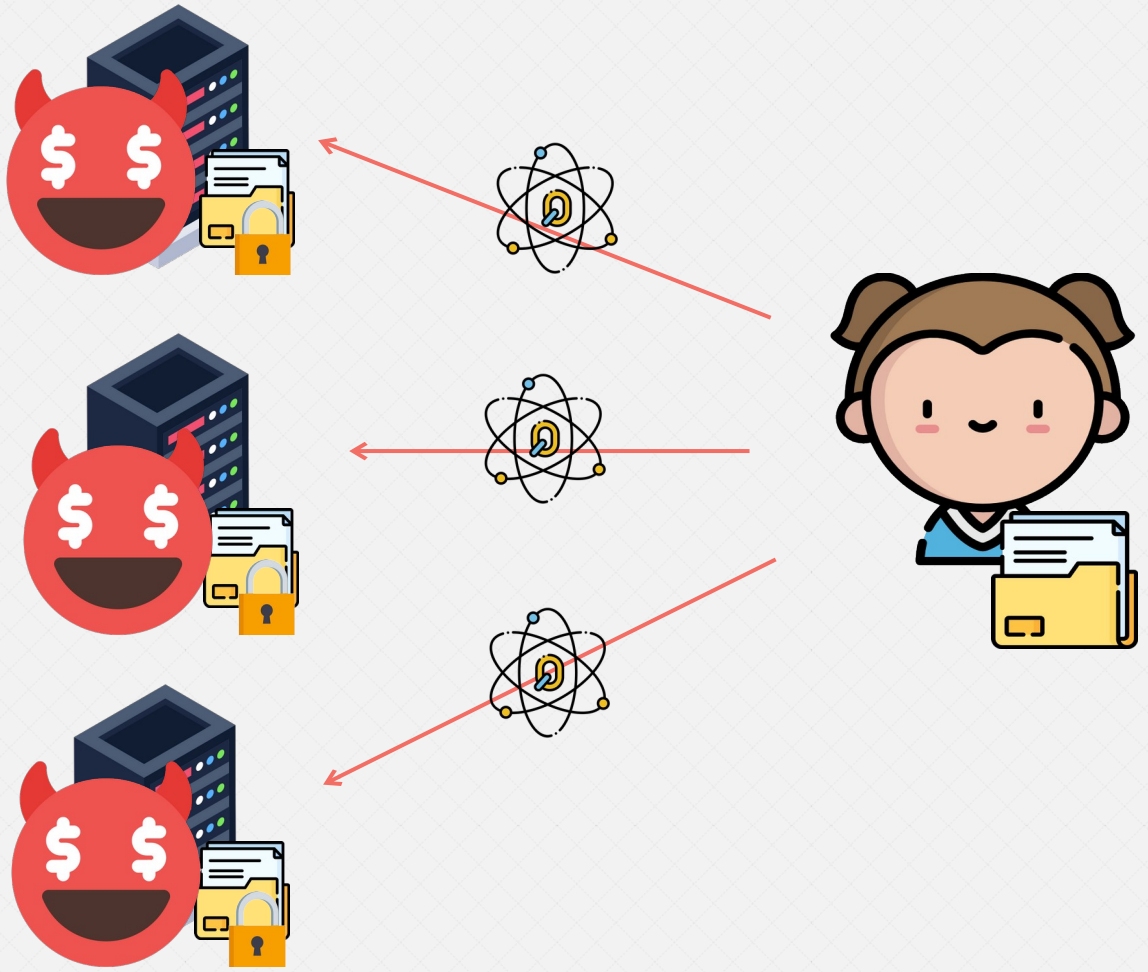
MULTISS: DISTRIBUTED QUANTUM STORAGE

With 

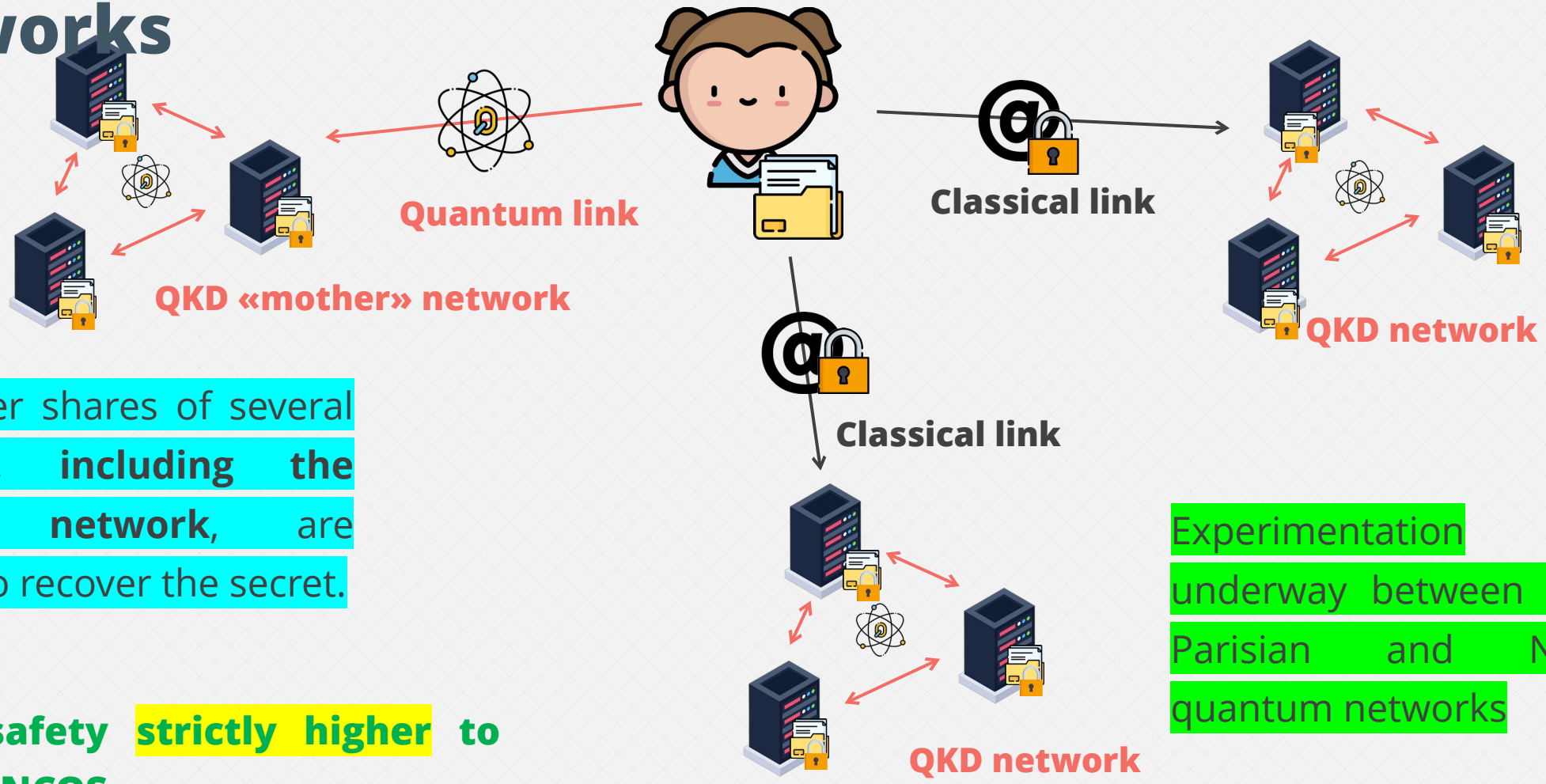
LINCOS: Confidential secret storage on a single QKD network

The shares of a majority of nodes on the local QKD network are needed to recover the secret

The assumption that an attacker could not take control of all servers is dangerous



MULTISS: Confidential secret storage on multiple QKD networks



The server shares of several networks, **including the mother network**, are needed to recover the secret.

Proven safety strictly higher to that of LINCOS

Experimentation underway between the Parisian and Nice quantum networks

Thank you!

Questions ?