



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



Doctolib



Data leaks

 **Breached Organizations**
All the leaks indexed in our database

Sort by Breach Date Upload Date Name # Size

	Tea App 21k rows	Aug 14, 2025
	MYVISAJOBS.COM 132k rows	Aug 14, 2025
	BRIJU.PL 119k rows	Aug 14, 2025
	DAT AUTOHUS AG 109k rows	Aug 6, 2025
	ridgefield.org 24k rows	Aug 5, 2025
	Able Home Care 15k rows	Aug 4, 2025
	Cookeville Regional Medical Center 21k rows	Aug 2, 2025
	wvPCA.org 18k rows	Jul 31, 2025
	Ingram Micro 24M rows	Jul 29, 2025

Source: <https://databreach.com/breach>

All Leak Sensitive

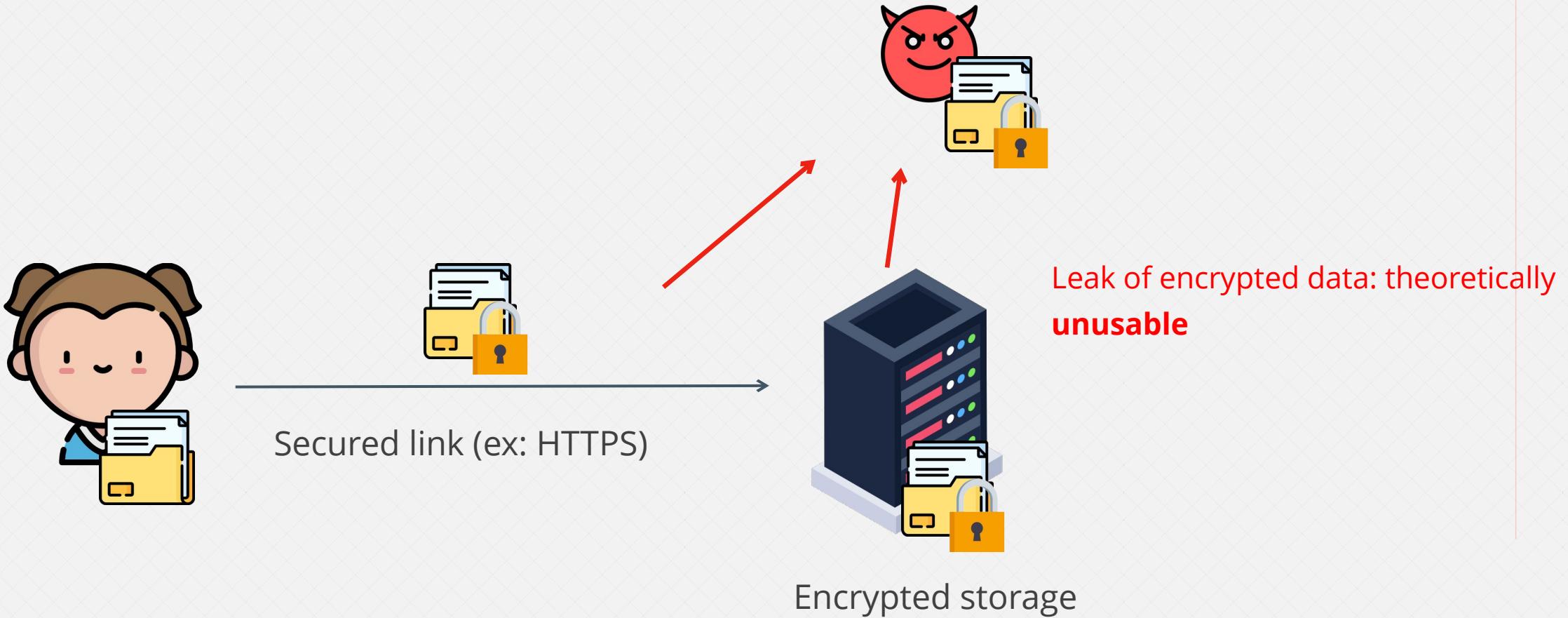
 8 août 2025 **Optic 2000**
• civilité, nom, prénom
• numéro de sécurité sociale
• date de naissance
• adresse postale
• n° client
• n° de téléphone
• magasin concerné
• nom de l'opticien
• Source

 6 août 2025 **Bouygues Telecom**
6.4 millions de clients
• coordonnées
• données contractuelles
• état civil
• IBAN
• Source

 11 juillet 2025 **Centre National de la Fonction Publique Territoriale**
34 000 personnes
• pièce d'identité
• IBAN
• carte vitale
• contrat de travail
• situation administrative
• justificatif de retraite
• attestation sur l'honneur
• diplôme
• CV
• Source
• Source

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

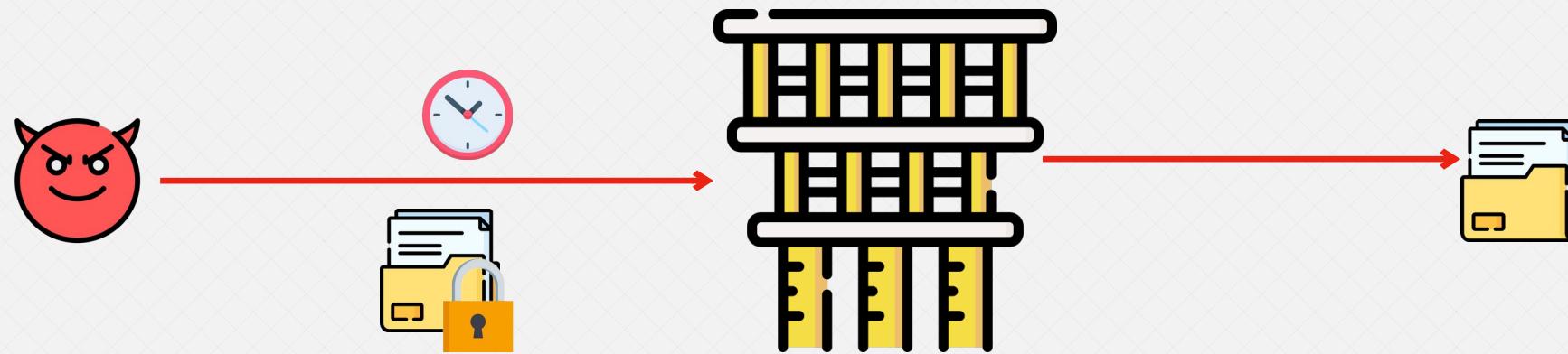
Solution: cryptography



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

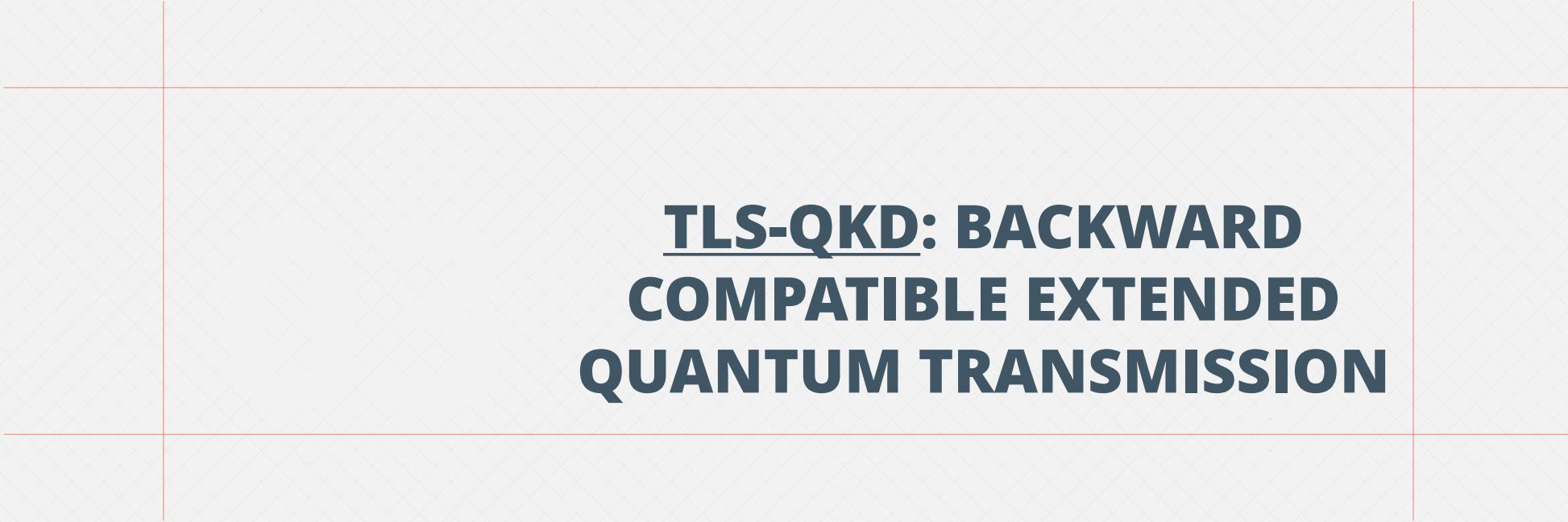


«*Harvest now, decrypt later*» attack

Post-quantum cryptography?

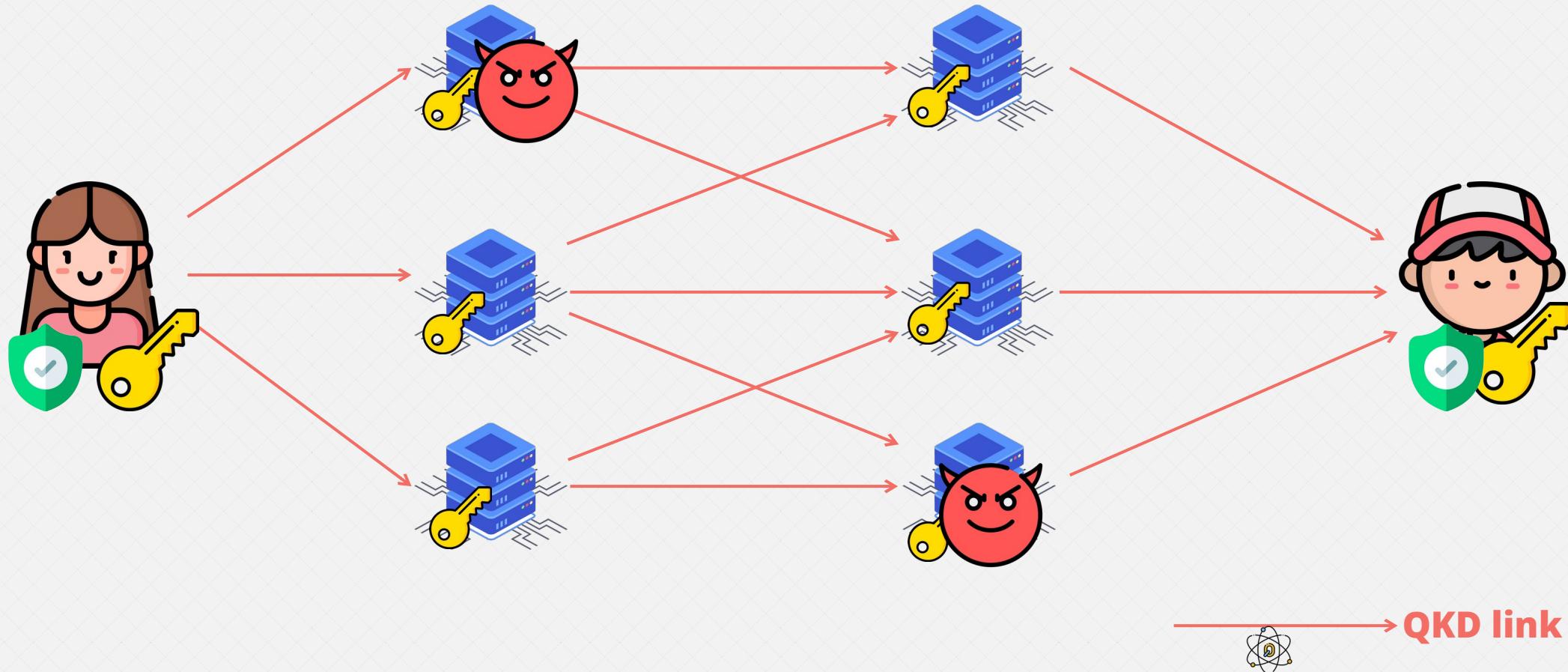


The mathematical foundations are too recent for "long-term security"



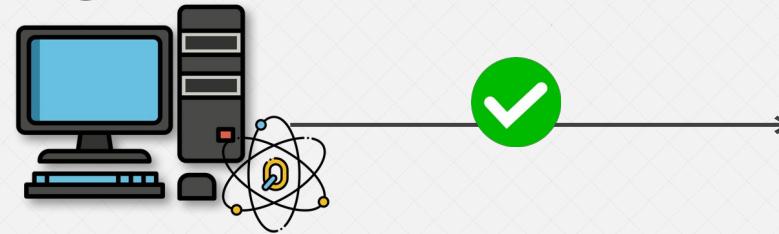
TLS-QKD: BACKWARD **COMPATIBLE EXTENDED** **QUANTUM TRANSMISSION**

Extended transmission



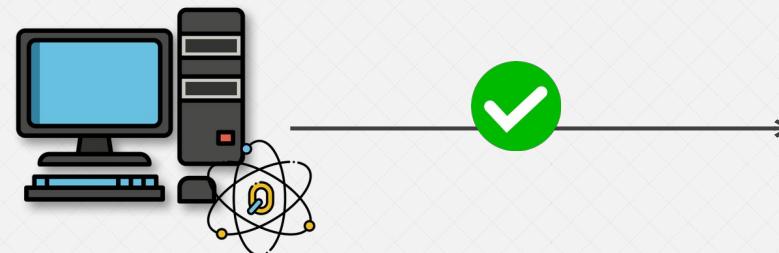
TLS (HTTPS) backward compatibility

TLS-QKD client



TLS-QKD server

TLS-QKD client



Classical TLS server

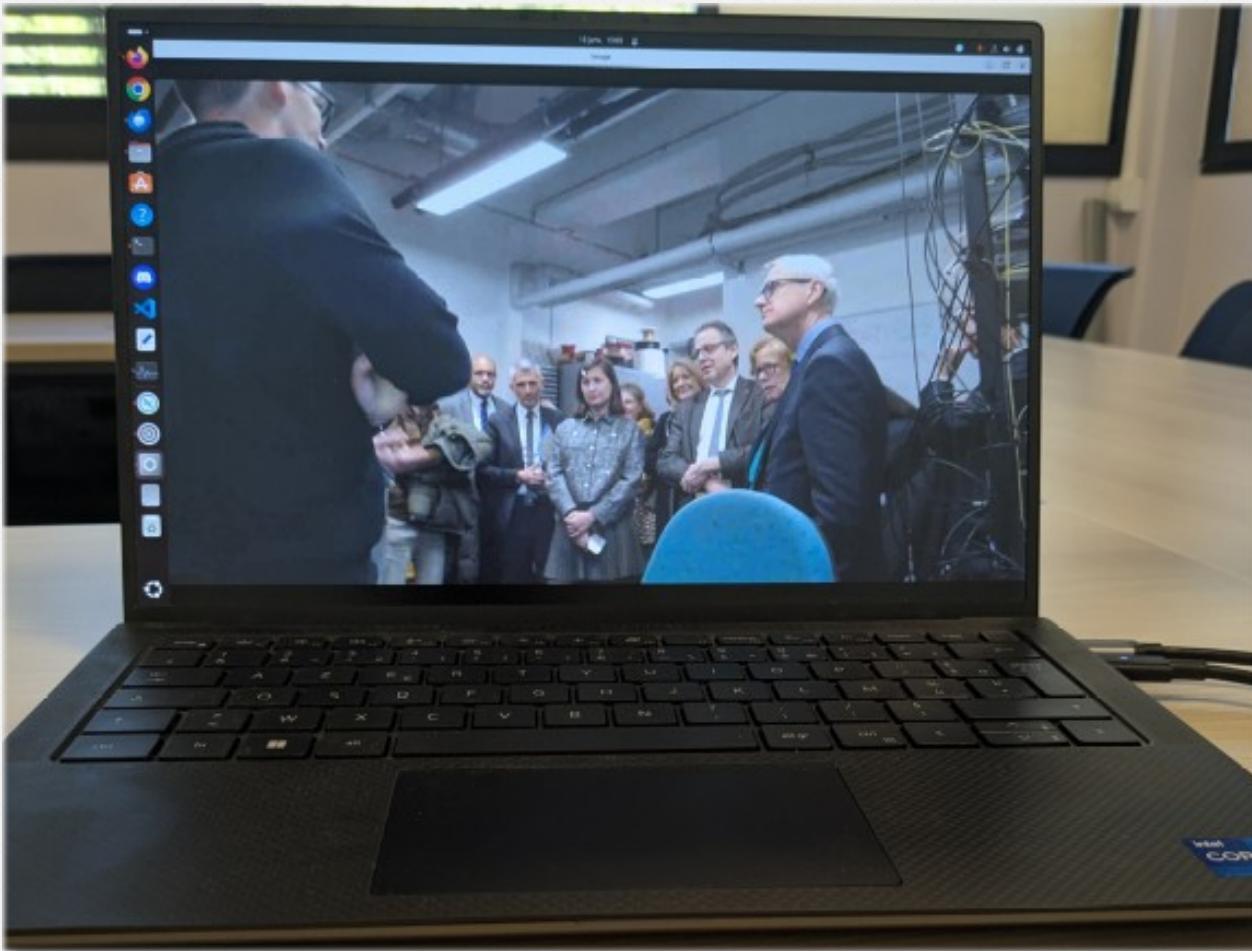
Classical TLS client



TLS-QKD server

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



MULTISS: DISTRIBUTED QUANTUM STORAGE

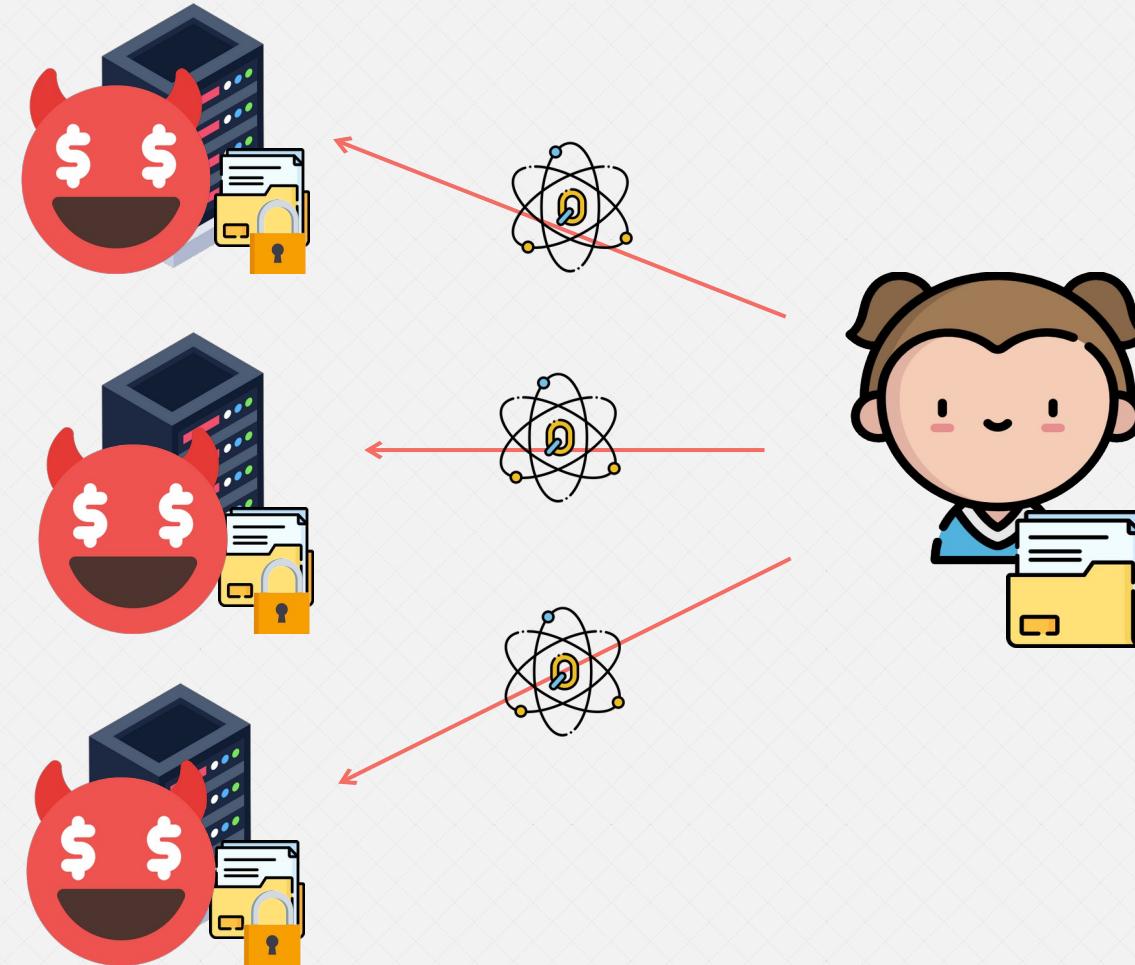
With



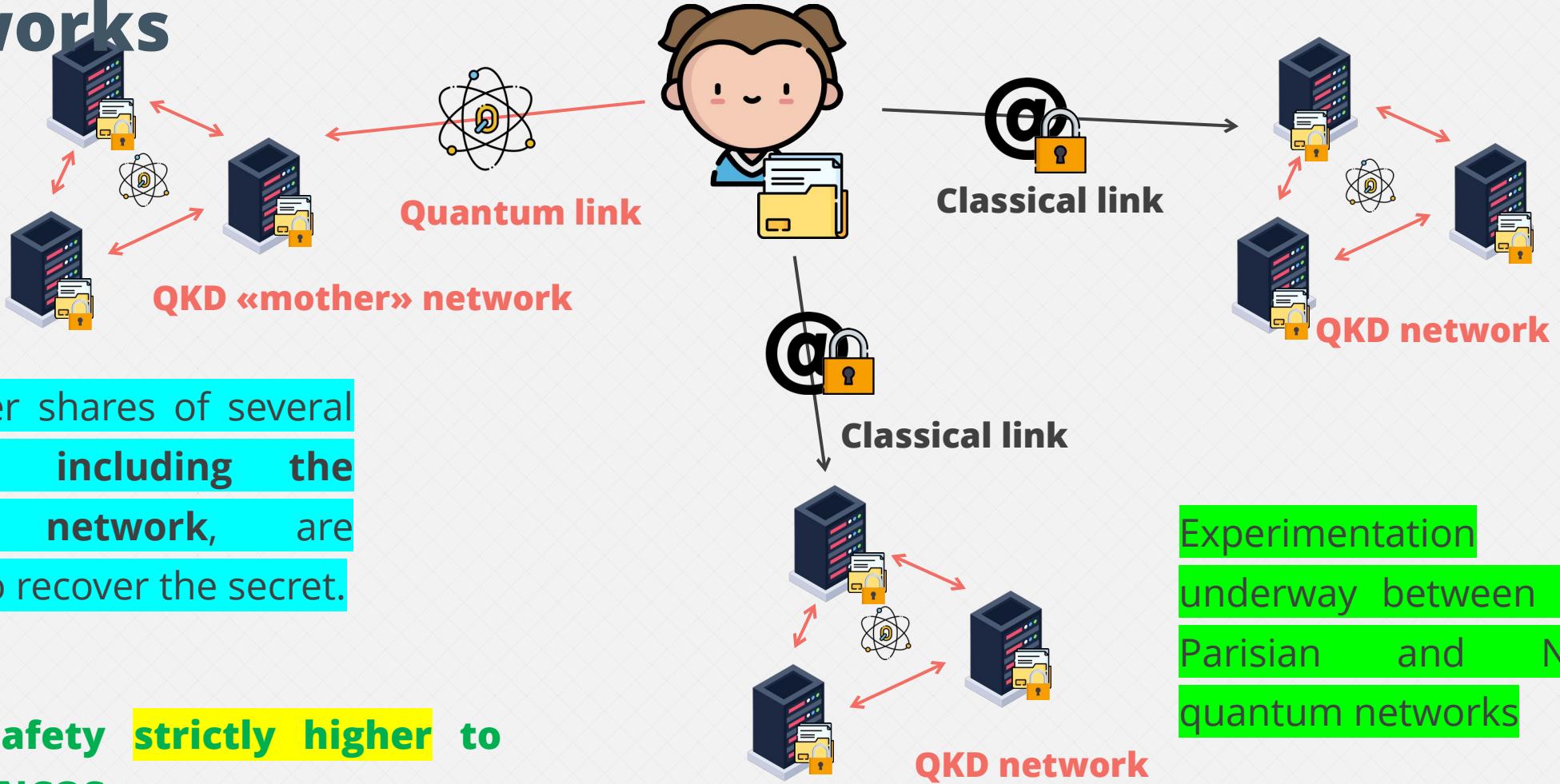
LINCOS: Confidential secret storage on a single QKD network

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



MULTIIS: Confidential secret storage on multiple QKD networks



Thank you!

Questions ?