

TeleTrust-interner Workshop

Berlin, 28.06.2023

Wann müssen wir unsere IT-Netze quantensicher machen?

Dr. Tobias Fehenberger
Adva Network Security

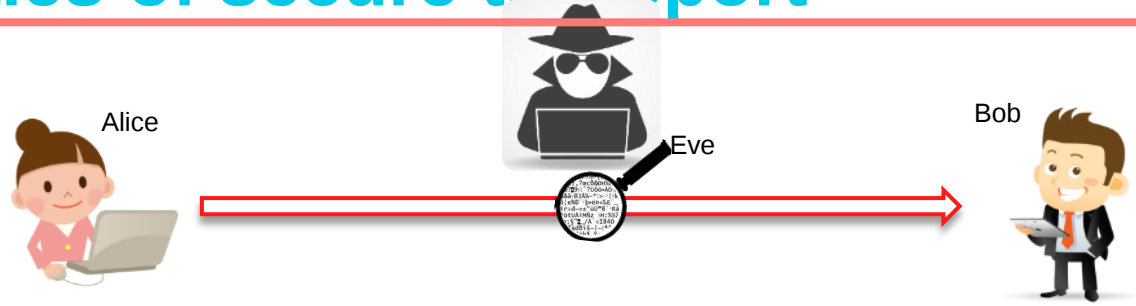
Wann müssen wir unsere IT-Netze quantensicher machen?

Warum – Wann – Wie



Three main properties of secure transport

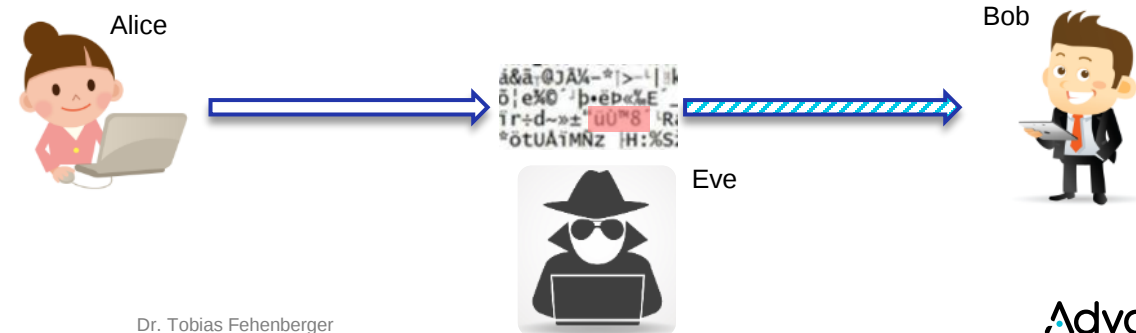
confidentiality



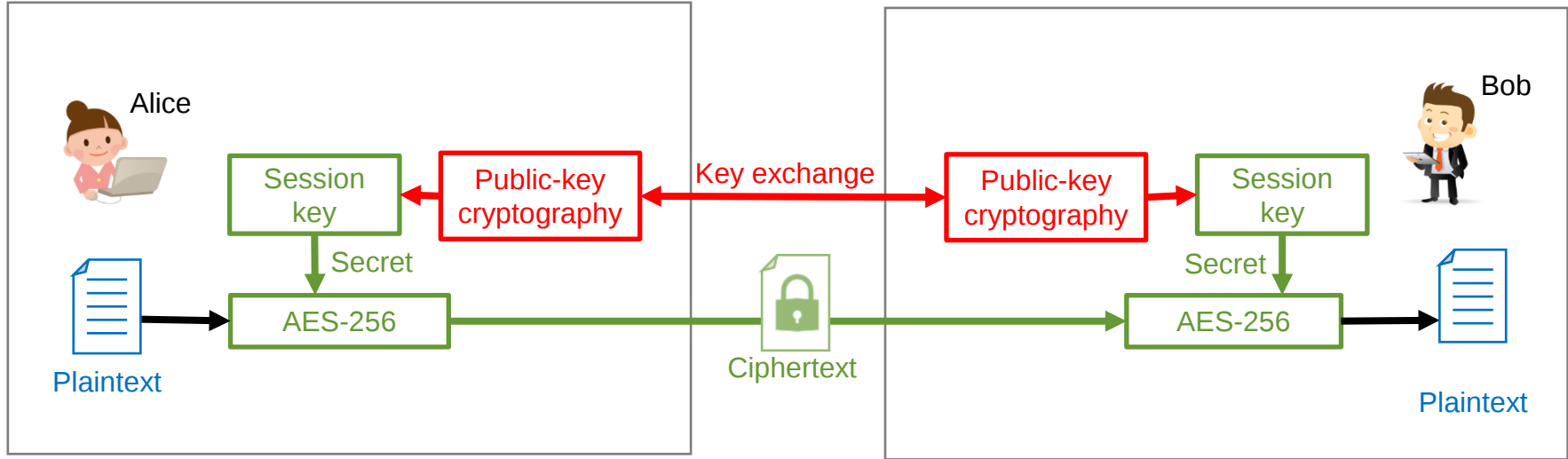
authenticity



data integrity



Confidentiality: Symmetric Cryptography



Problem: How to perform key exchange efficiently?

Public-key cryptography to exchange *secure* key over *insecure* channel

Encryption protects sensitive data ...



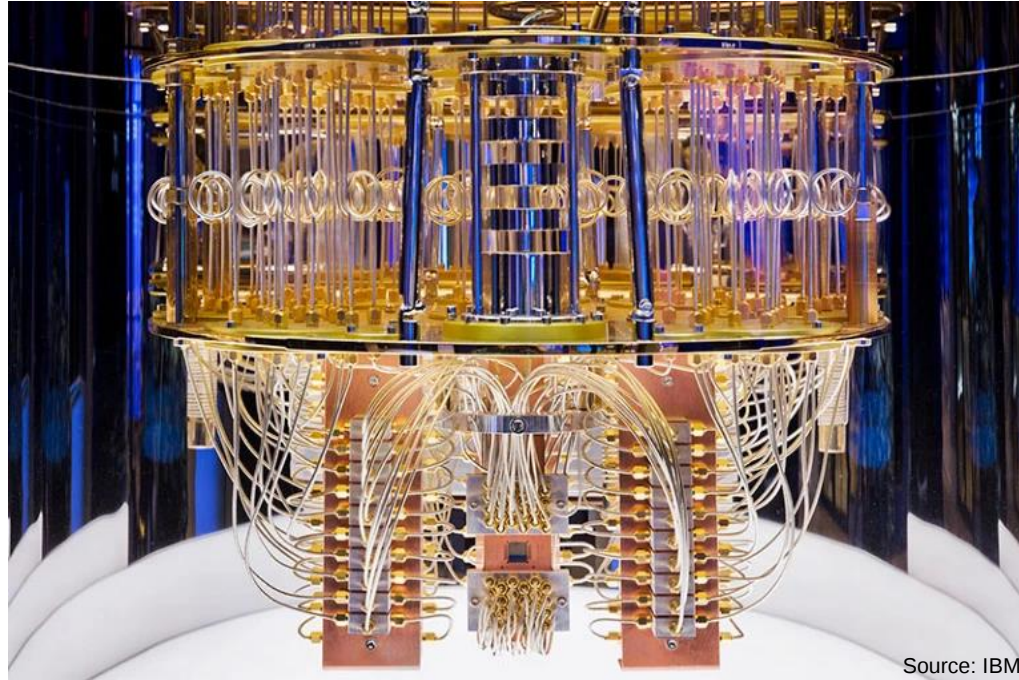
Encryption works.

**Properly implemented strong crypto systems are
one of the few things that you can rely on.**

Edward Snowden

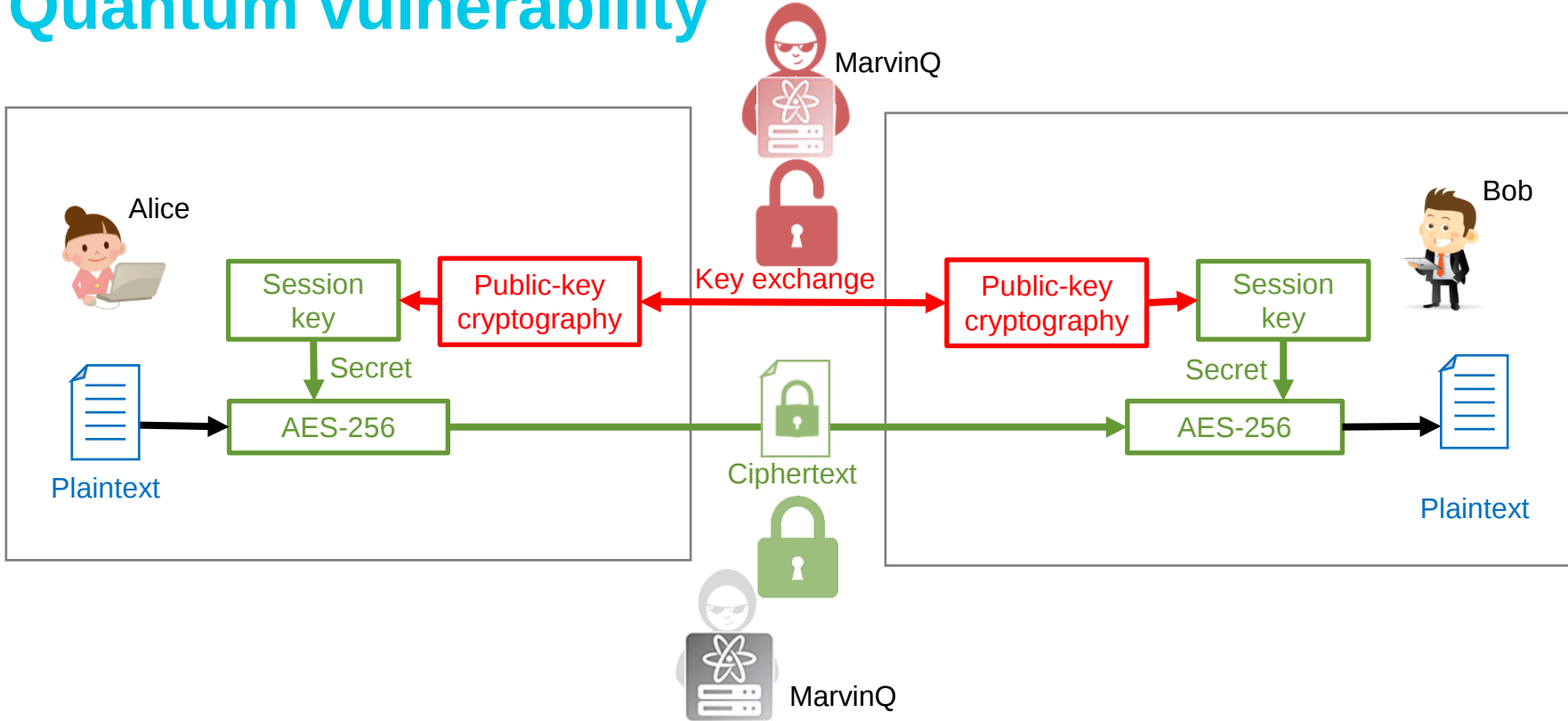
Freedom of the Press Foundation, Edward-Snowden-FOPF-2014, CC BY 4.0

... but can be broken by large quantum computers



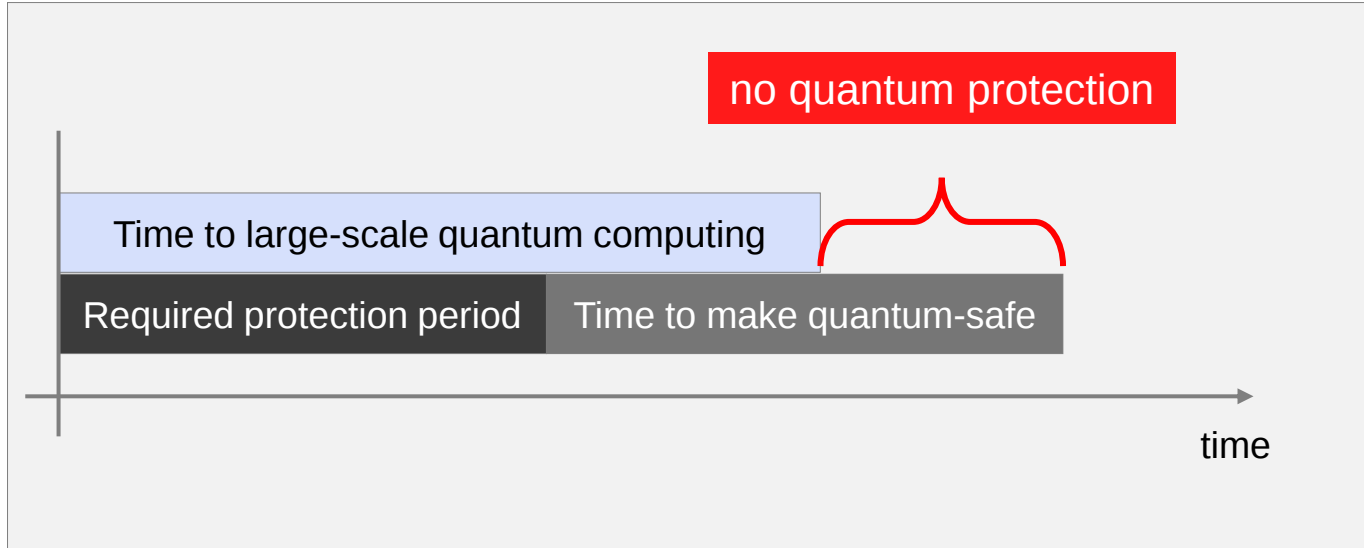
One of the few undisputed applications of quantum computers

Quantum vulnerability



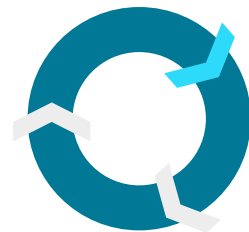
Public-key cryptography is compromised by powerful quantum computers

Is there a quantum-risk today?



Attack scenario: store now – decrypt later

Quantum-safe security controls



Post-quantum cryptography (PQC)

- New, quantum-safe math problems
- Higher requirements: longer keys, complex algorithms
- Ongoing security evaluation
- Risk of future quantum attack

Quantum key distribution (QKD)

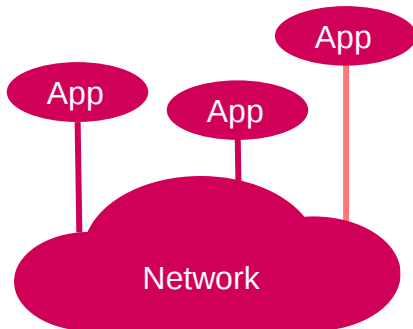
- Uses principles of quantum physics
- Requires optical channel (fiber networks or free-space links)
- Complex and costly infrastructure
- Early stage of commercialization

Complementary techniques – PQC (baseline) & QKD (add-on)

Restoring information security



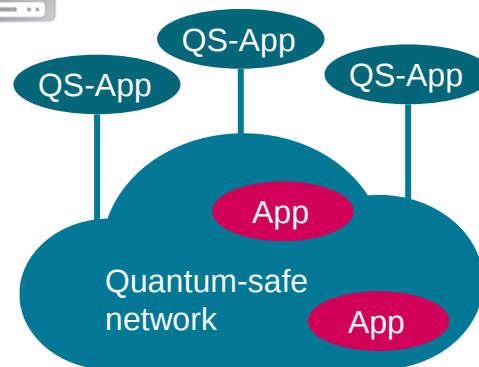
Successful
QAttacker



Quantum vulnerable network
and applications



Frustrated
QAttacker



Quantum-resistant network is foundation of quantum security

Key take-aways



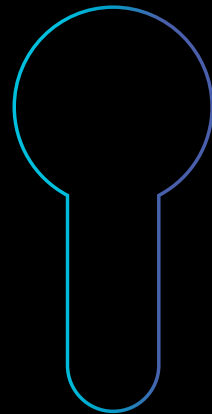
Quantum computers will compromise classical encryption

“Store now – decrypt later” attacks create a significant security risk **today**

Quantum-safe transport networks are a strong foundation available **today**

Thank you

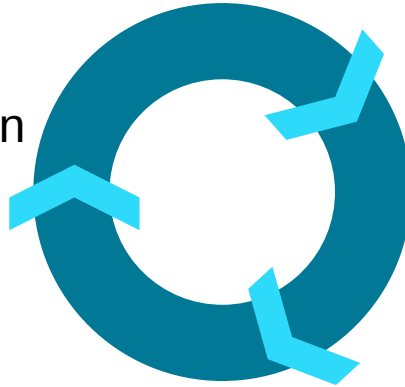
www.advasecurity.com | info@advasecurity.com



Backup

The quantum security migration circle

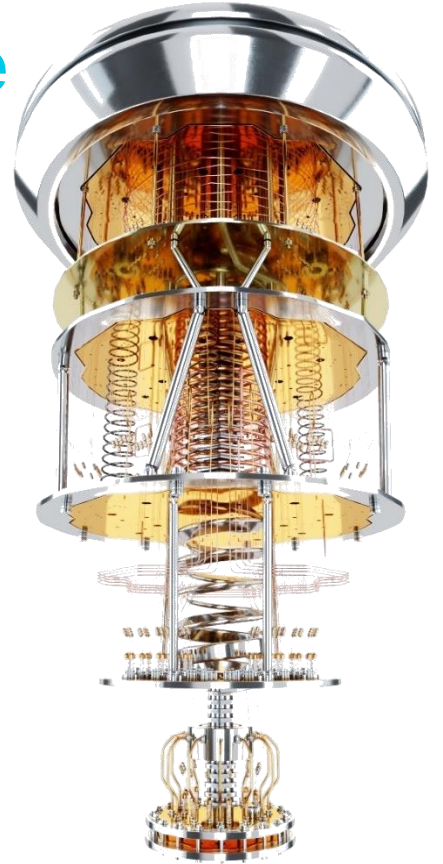
Start: Identify quantum risk and initiate mitigation



Quantum-safe algorithms
and deployment strategy

Execution, restoring
information security

Urgent. Complex. Time-consuming.



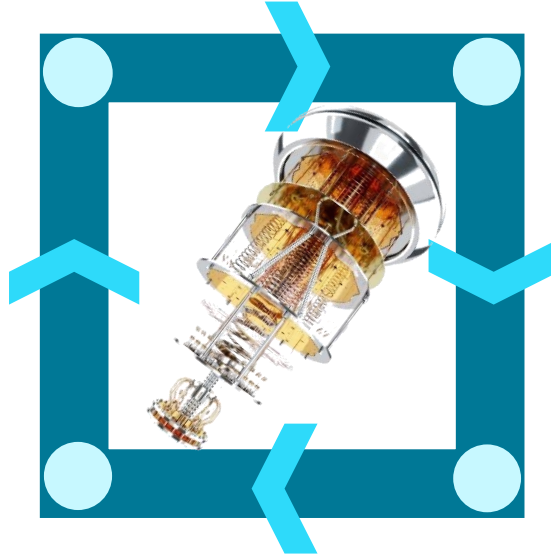
Summary: robust mitigation of quantum risk

2

Evaluating quantum-safe security controls and analyzing the applicability

1

Comprehensive analysis, identifying quantum risk, and starting mitigation



3
Selecting security strategy, establishing execution framework

3

4
Establishing resilient and robust quantum-safe security

4

Maximizing long-term security