



# Quantum threat...and quantum solutions

How can quantum key distribution be integrated into a quantum-safe security infrastructure

Bruno Huttner  
ID Quantique

ICMC 2017

- ❑ Presentation of ID Quantique
- ❑ The Quantum Threat
- ❑ Quantum Solutions (1): QRNGs
- ❑ Quantum Solutions (2): QKD
- ❑ Integration of QKD in optical networks today
- ❑ Towards a world-wide QKD network
- ❑ Conclusion



Founded in 2001



Geneva, Switzerland



Key technology: photon counting

Three business units:

- Photon counting & Instrumentation
- Quantis: Quantum Random Number for Key Generation
- Quantum-Safe Security



Performs R&D, production, professional services, integration, support



Clients : Governments / Banks / Gaming Industry / Universities / IT Security



# The Quantum Threat



The hacker's point of view today...



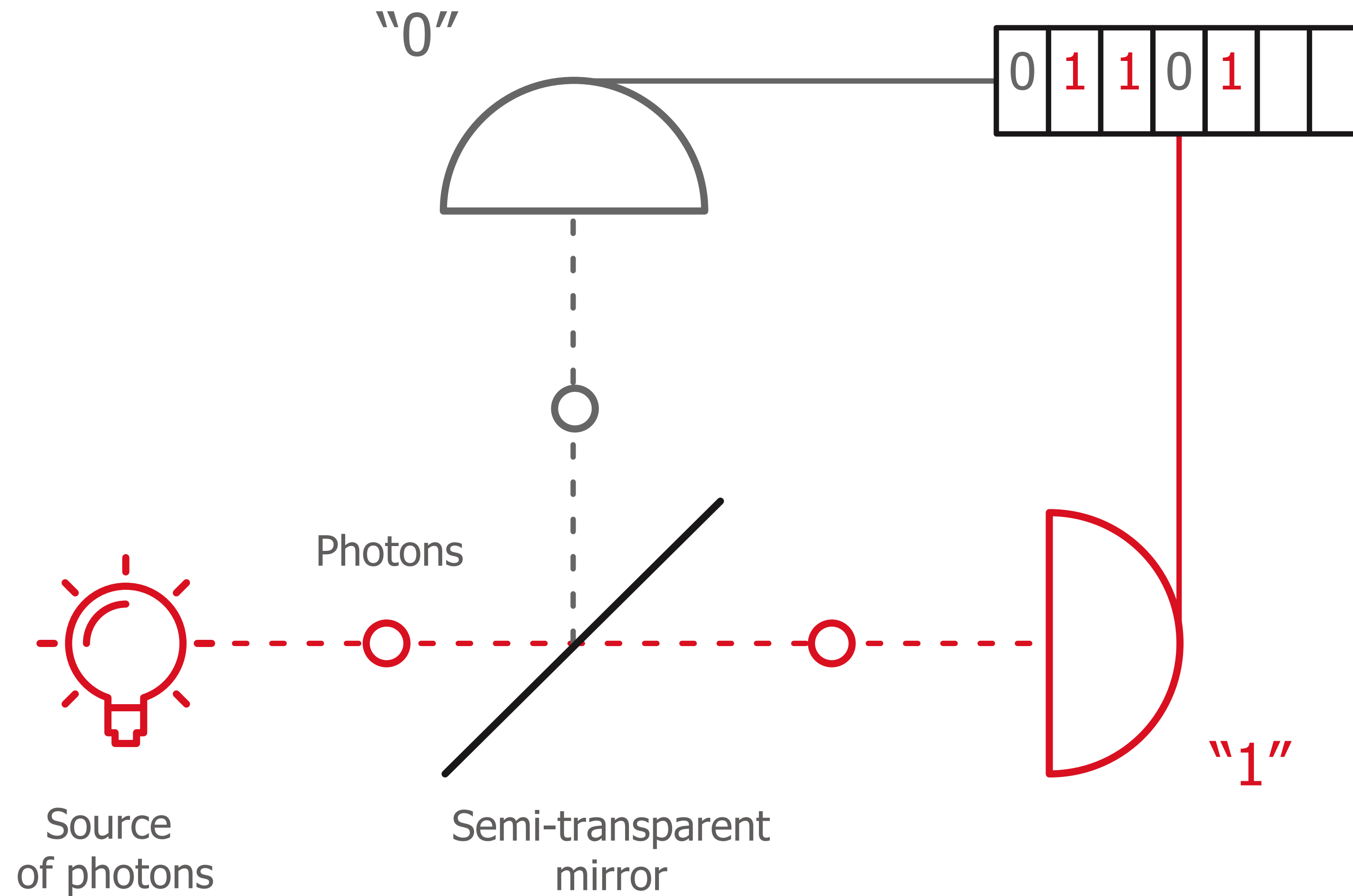
... and after the  
Quantum Computer



# QUANTUM SOLUTION (1): QUANTUM KEY GENERATION



# True Random Number Generator based on Quantum Physics

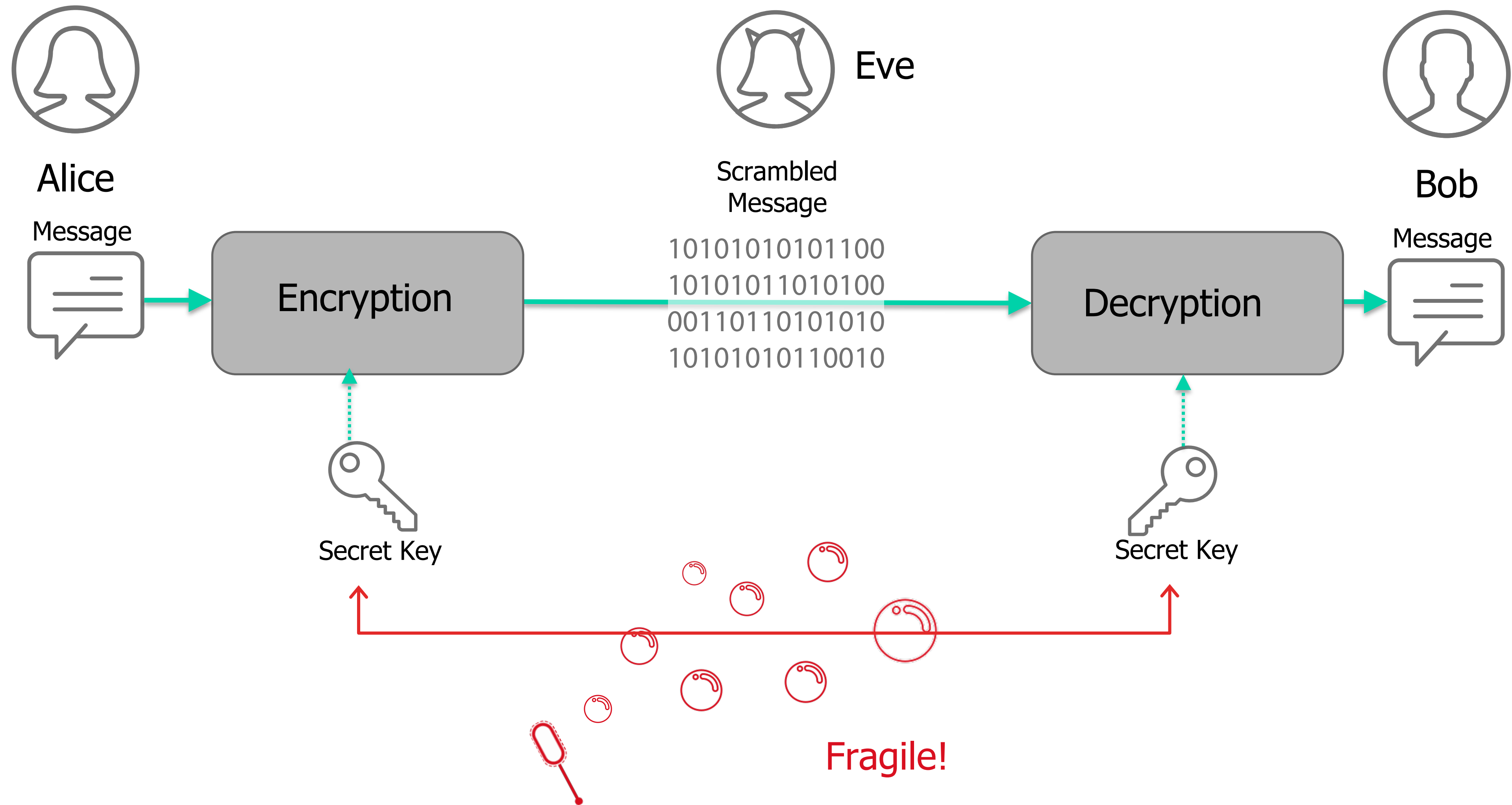




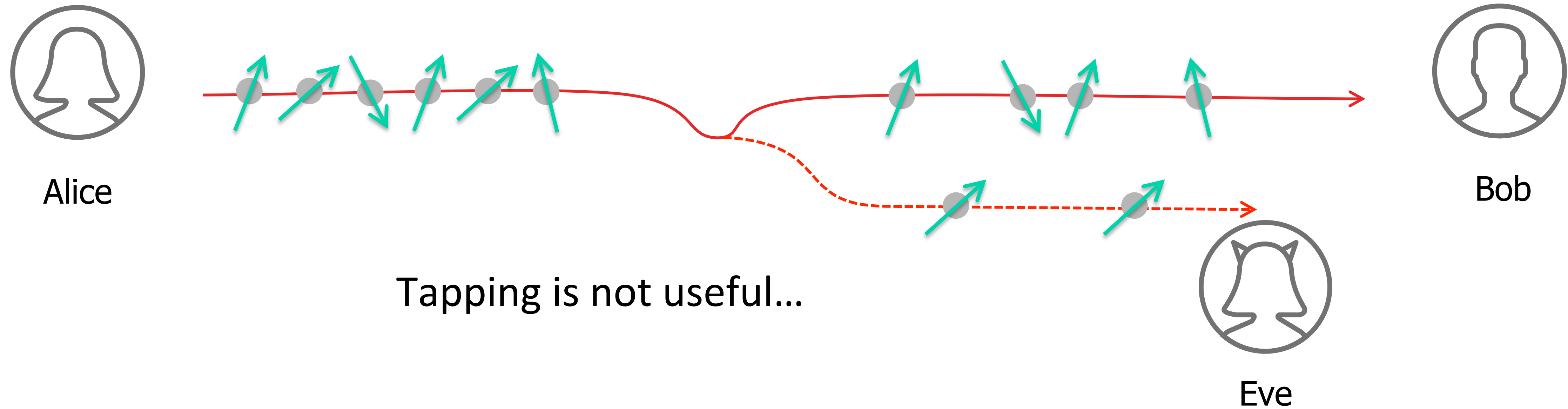
# QUANTUM SOLUTION (2): QUANTUM KEY DISTRIBUTION

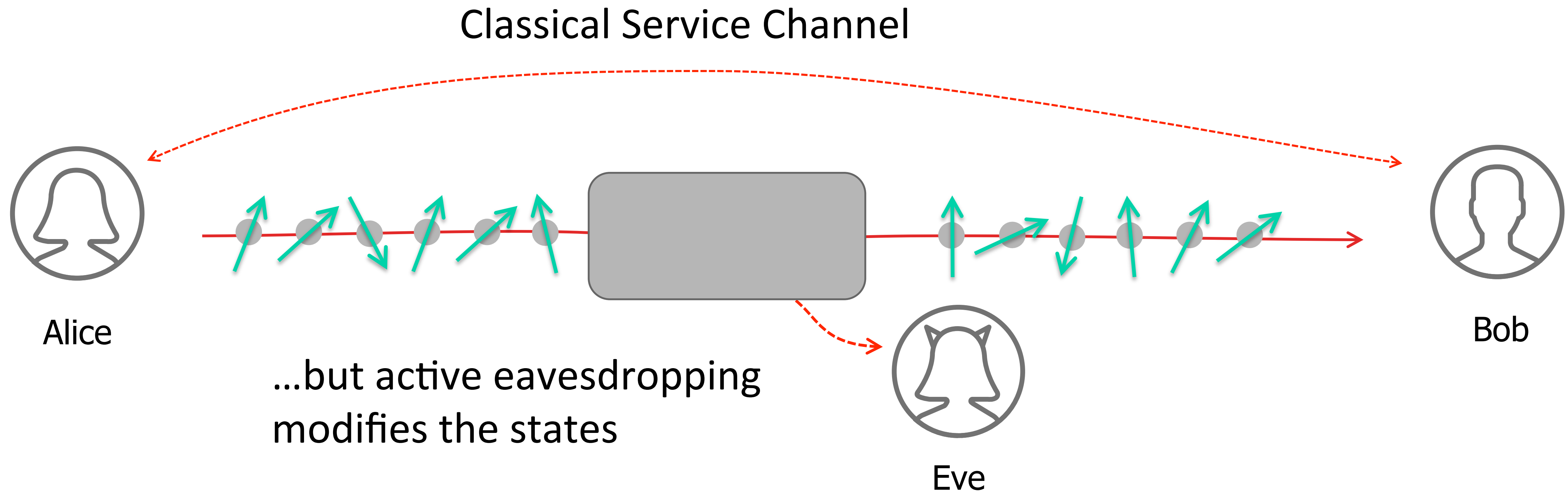


# Quantum Key Distribution (QKD): Basic idea











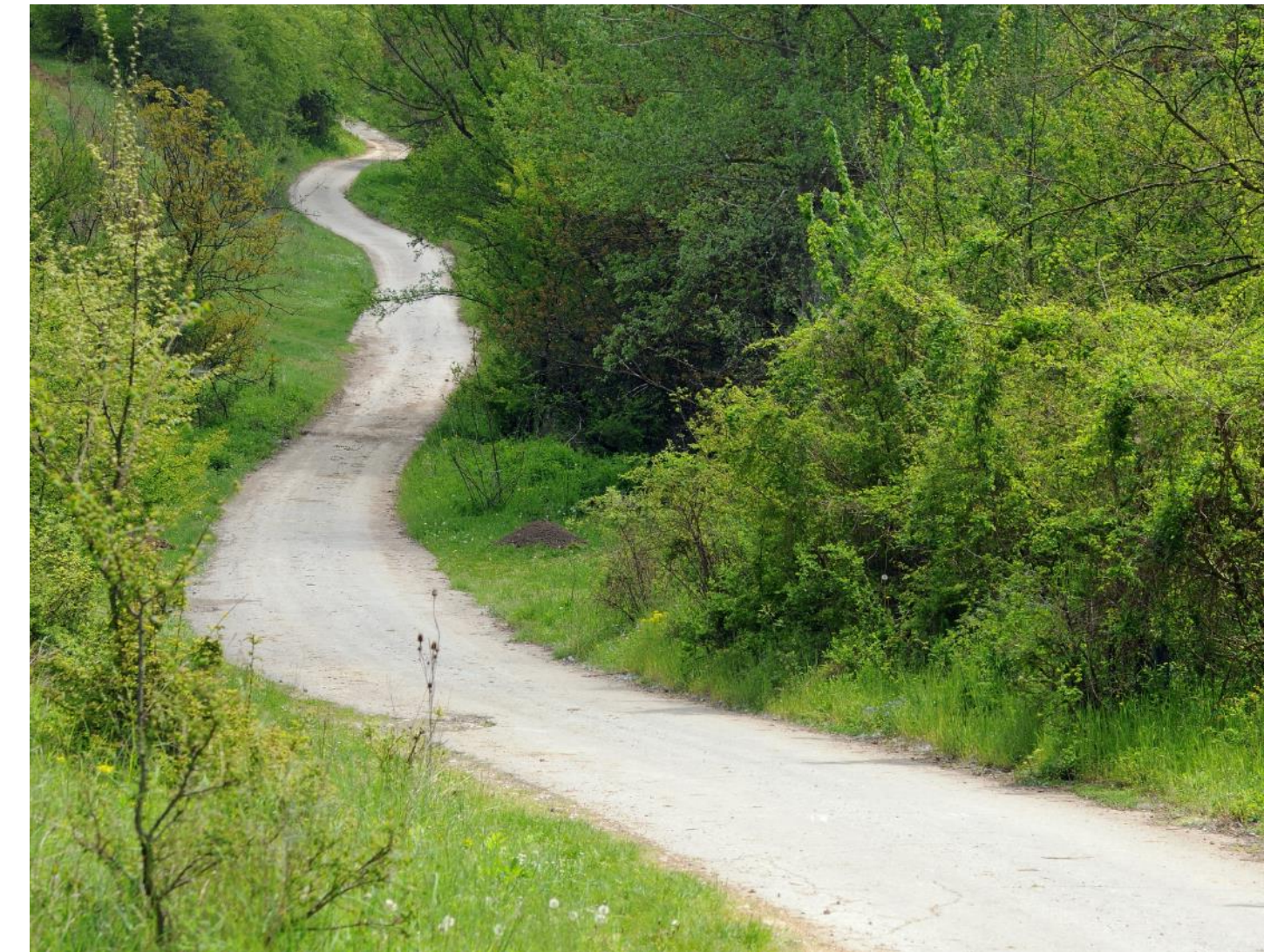
Pros	Cons
Based on different principle (physics)	Need physical infrastructure
Not impacted by QC	Limited distance between nodes (to date)
Provable security of transmission	Only part of the solution: Needs conventional crypto to use the key (e.g. symmetric key encryption); And post-quantum Authentication
Real-time eavesdropping possible only	
Adds one layer of security	

- ➔ More complicated and costly to implement
- ➔ Useful for high-level and long-term security

# INTEGRATING QKD IN QUANTUM-SAFE SECURITY INFRASTRUCTURE



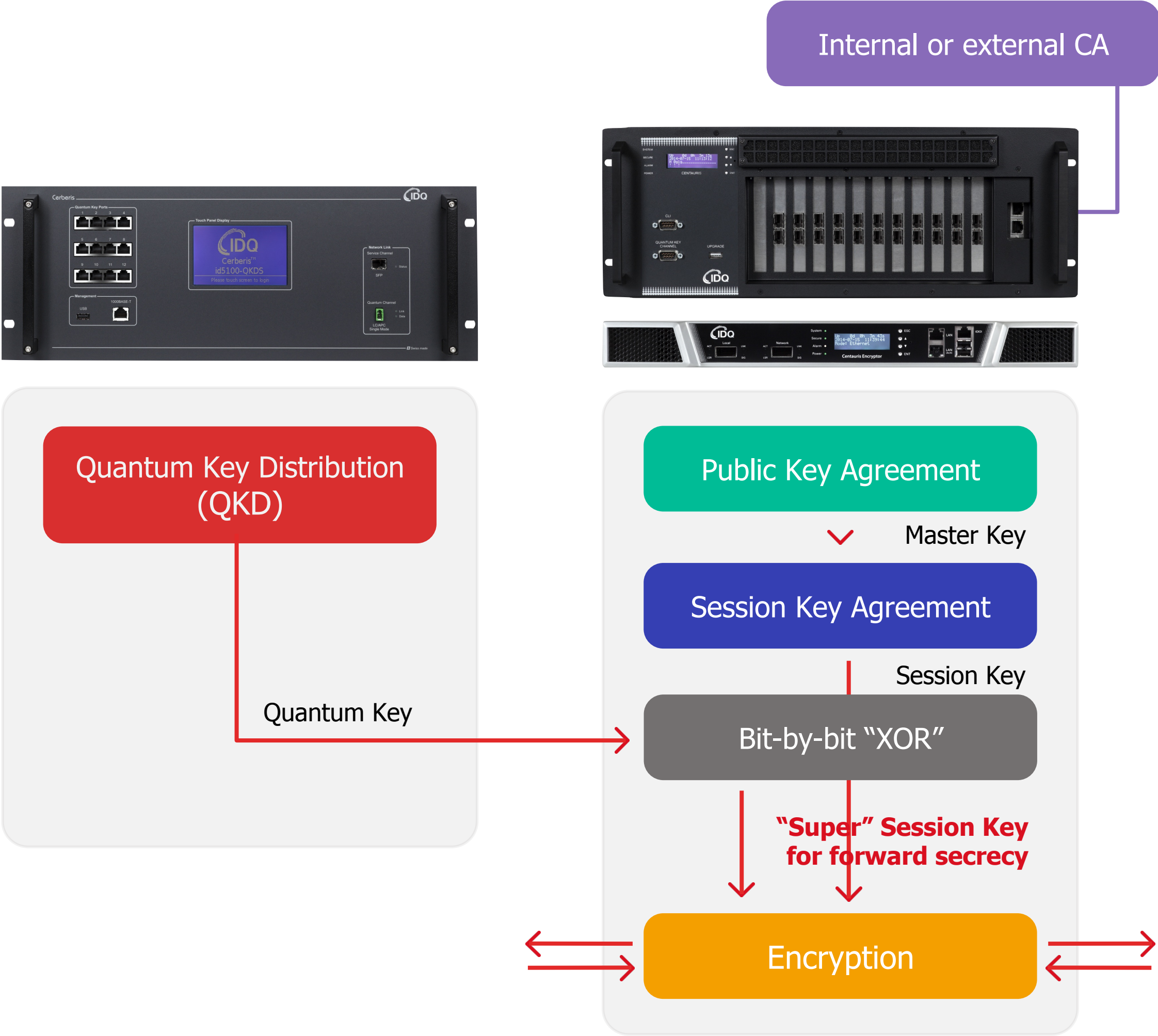
# All links are NOT born equal!



Safety has to be adapted to the communication links.

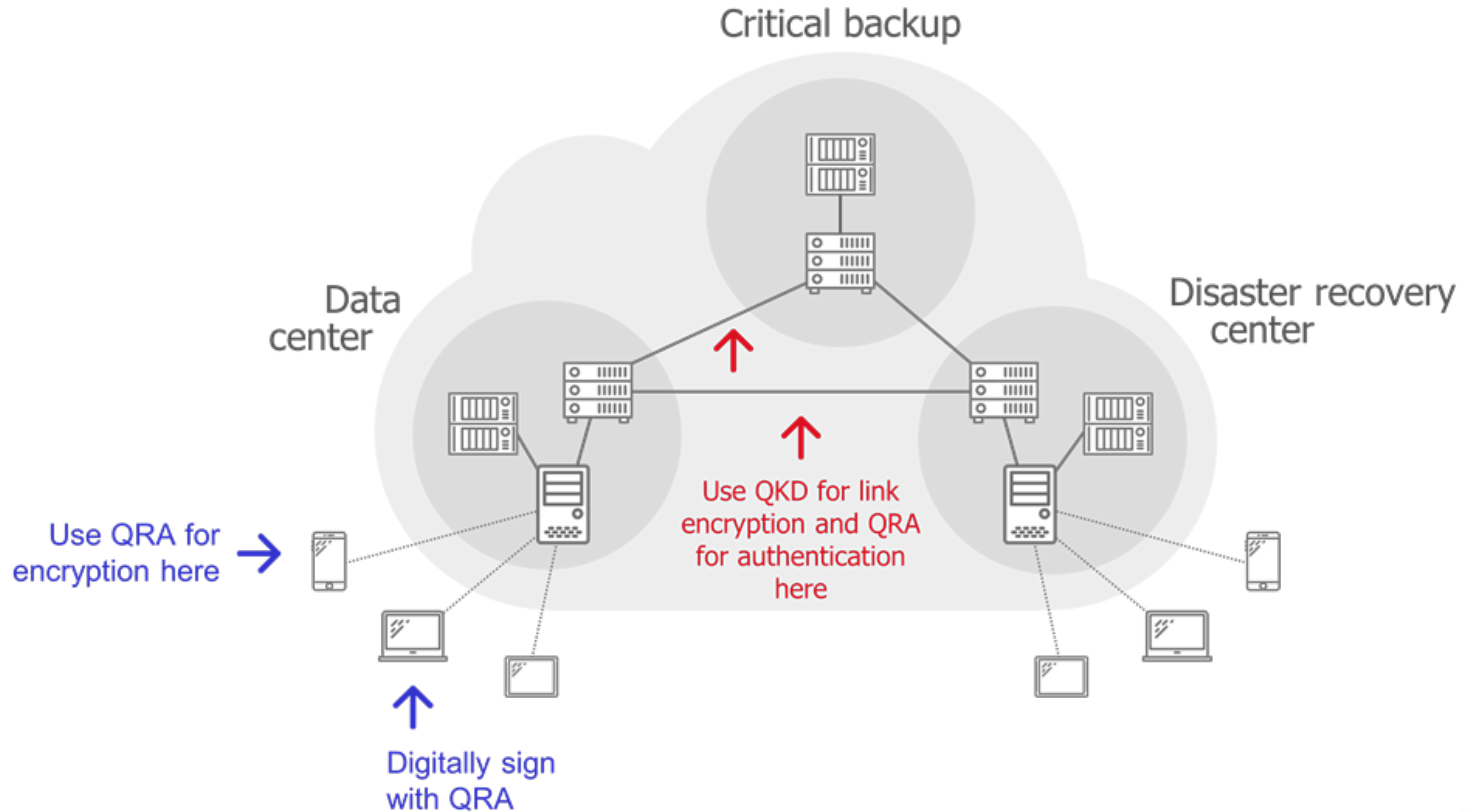


# Use QKD today as an add-on to current encryption systems





# Use QKD today for Critical Links



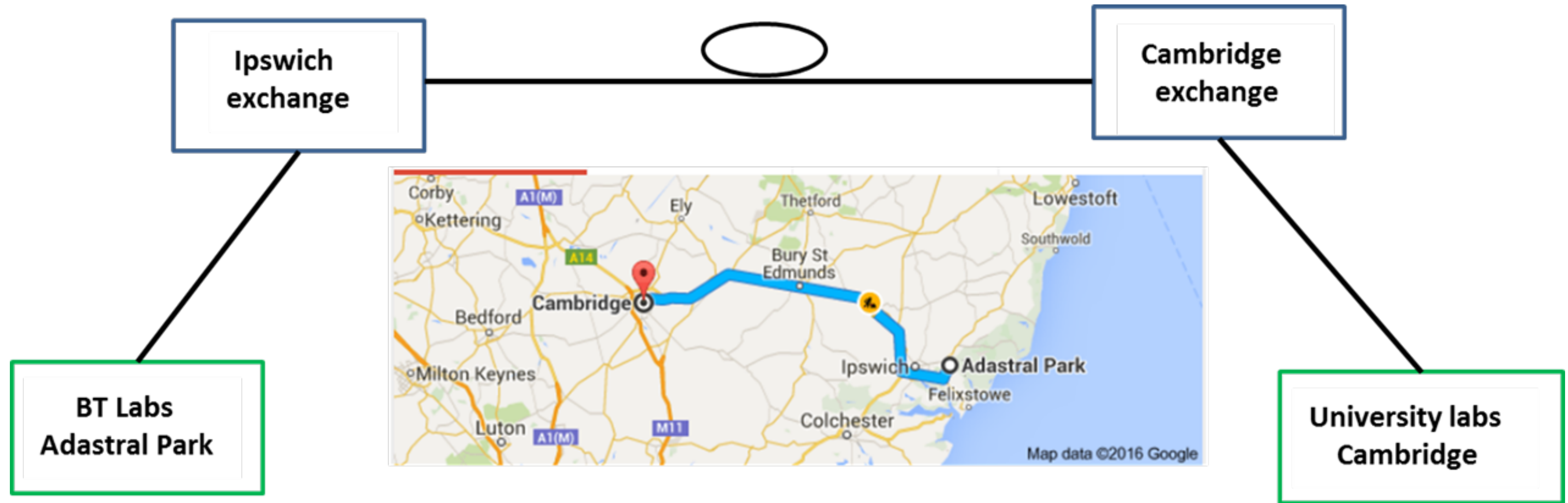


## ROADMAP FOR QKD

- ❑ Trusted Nodes for long-distance QKD
- ❑ Free Space QKD with satellites
- ❑ Global QKD Network based on Quantum Memories



# Step 1: Long distance QKD with Trusted Nodes





# What about longer links: The Chinese Quantum Backbone

- **Total Length 2000 km**
- **2013.6-2016.12**
- **32 trustable relay nodes**  
**31 fiber links**
- **Metropolitan networks**  
**Existing: Hefei, Jinan**  
**New: Beijing, Shanghai**
- **Customer: China Industrial & Commercial Bank; Xinhua News Agency; CBRC**





## Step 2: A Global Network Based on Free Space QKD



- ▶ Free Space QKD
  - QKD links with LEO satellites
  - LEO acts as a **trusted node** to transport the key to the necessary location.
- ▶ Free space QKD is moving out of the lab & into industry
  - Chinese have launched a QKD satellite in August 2016 and QKD system in space station in September.
  - Worldwide interest at the academic/government level
  - IDQ has started feasibility studies for practical systems (Eurostars and Swiss Space Office)



## Step 3 : A world-wide QKD infrastructure



- ❑ Build a QKD infrastructure based on Quantum Memories (QM)
- ❑ Each node exchanges QMs with the others
- ❑ Customers come to any node to recharge their QMs (similar to bank notes and ATM infrastructure)
- ❑ Nodes need not be trusted anymore



What the Quantum has taken away...

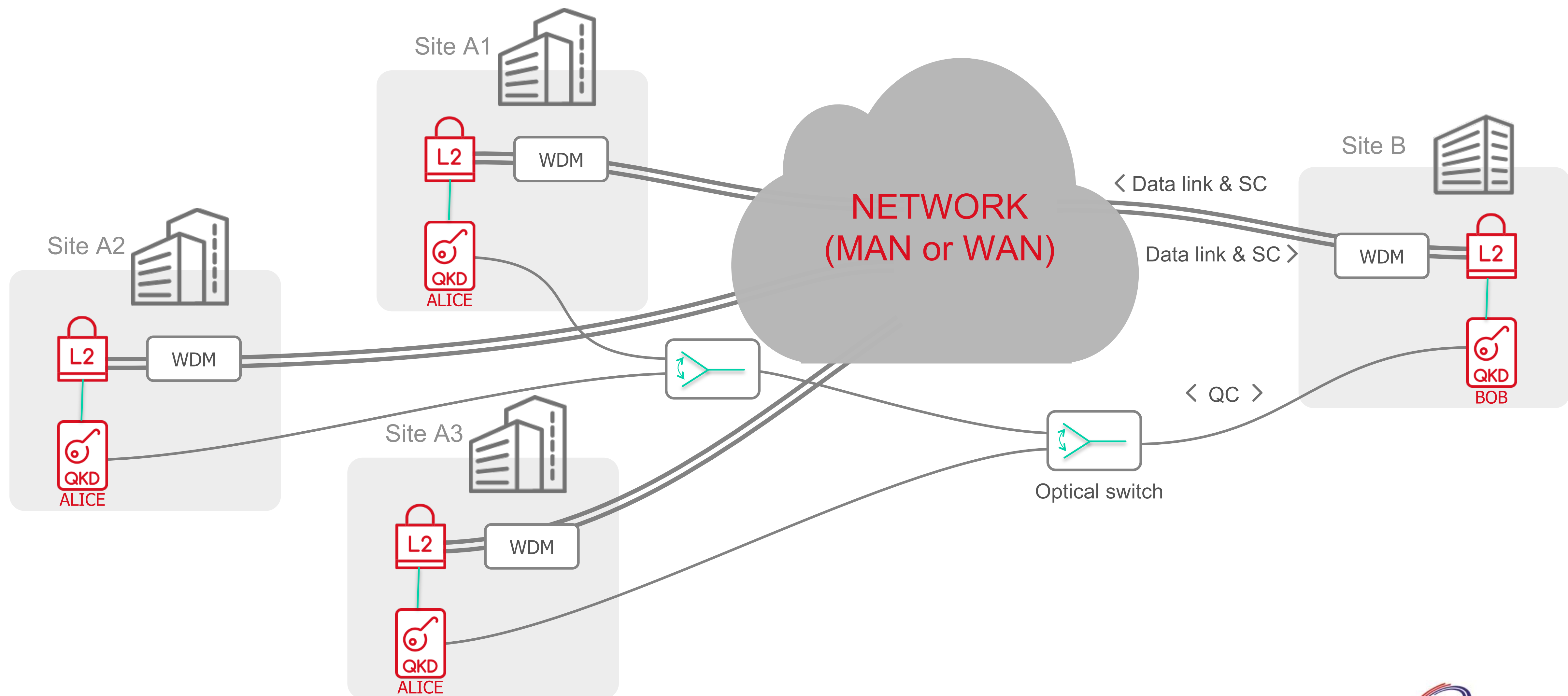
...the Quantum can give back!



For more information  
<http://www.idquantique.com>



# QKD for Access Network: one Bob, many Alices...

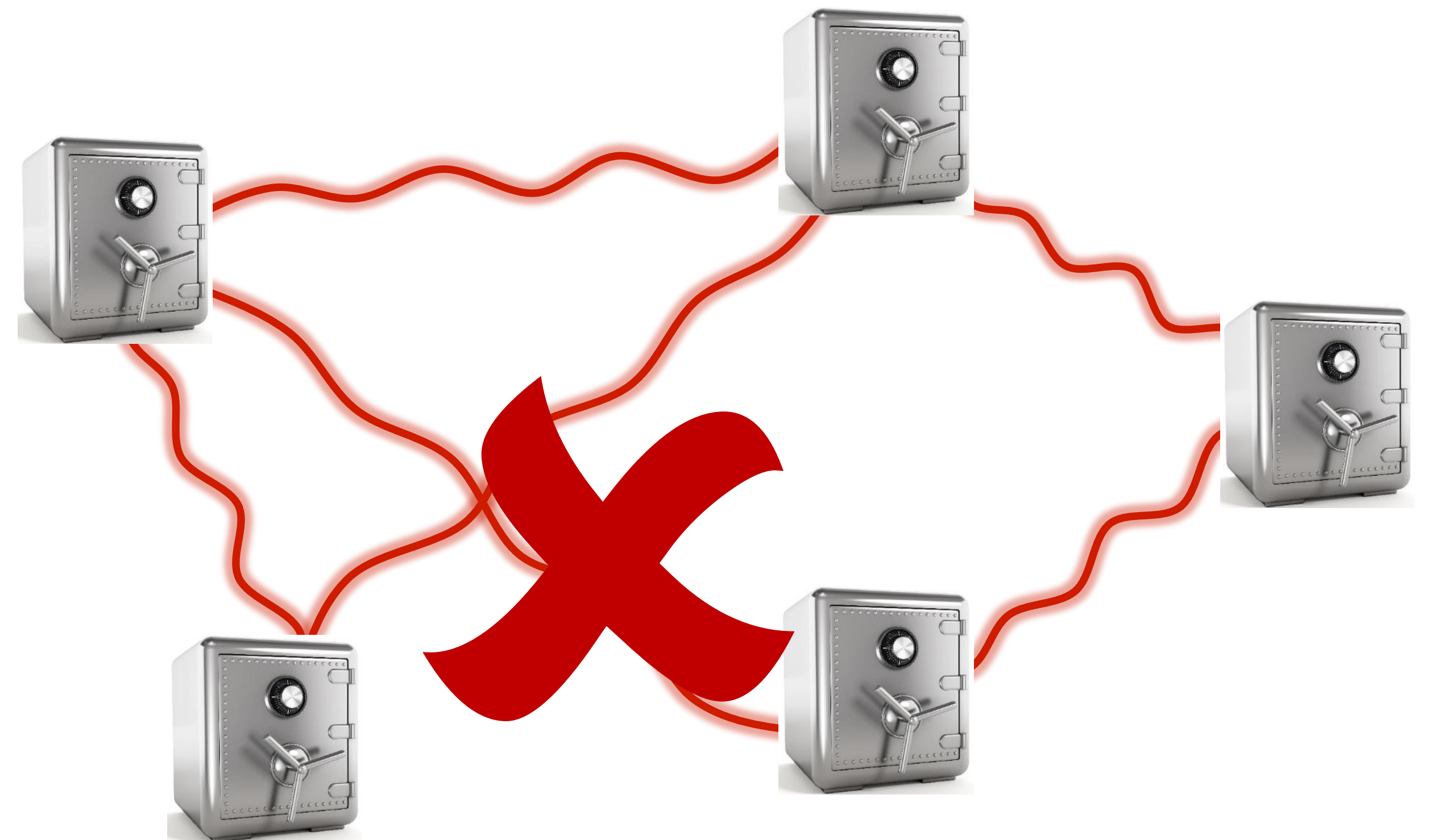


# What is at risk?

Data at rest

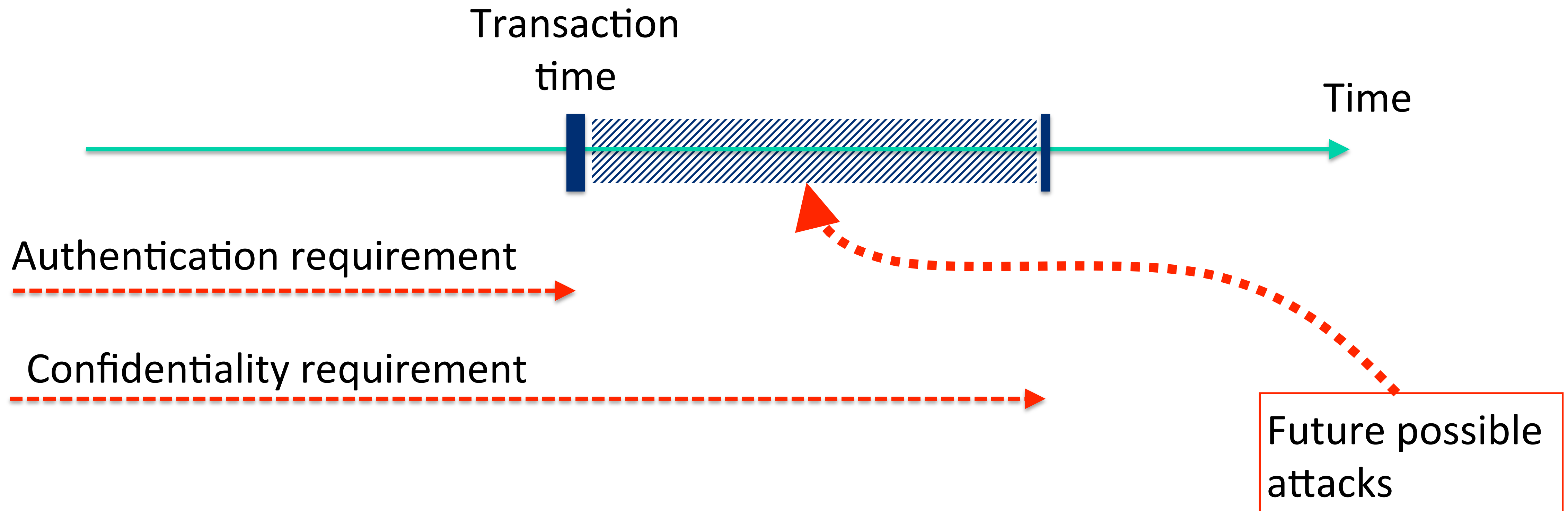


Data in transit



Two requirements:

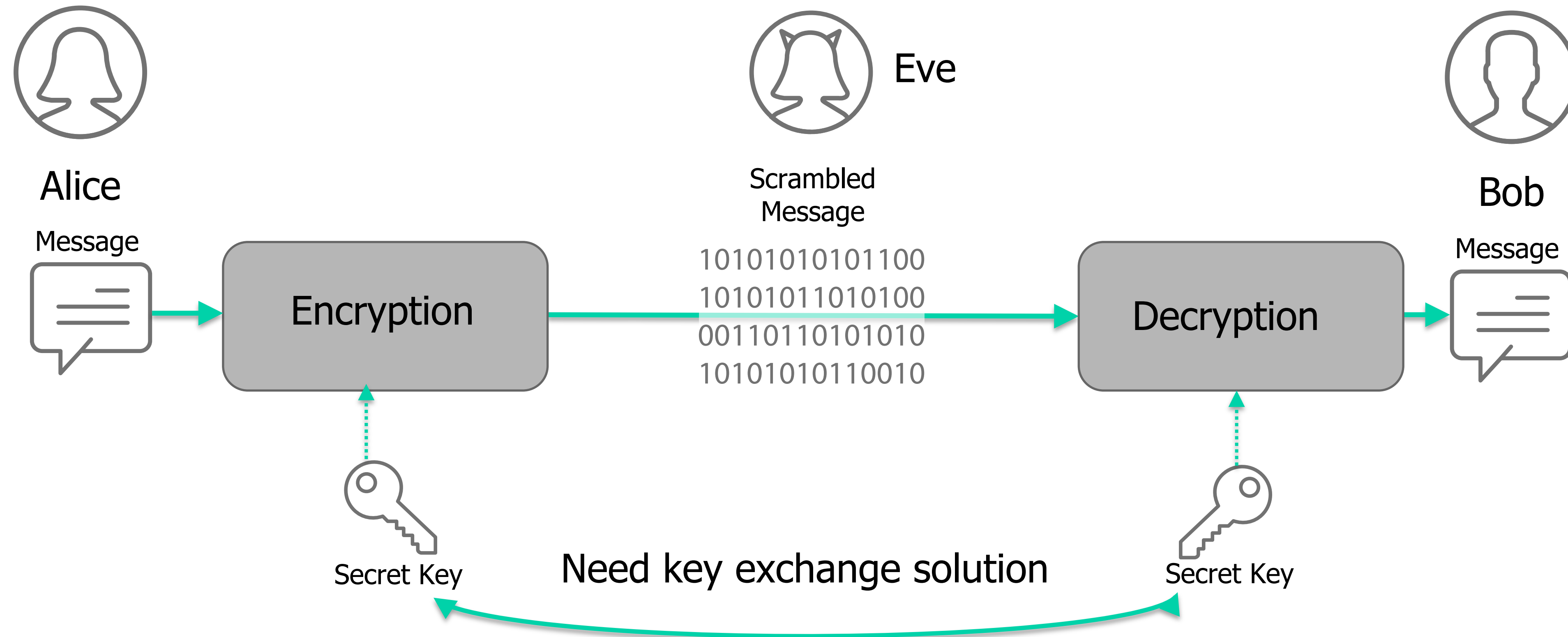
- Authentication
- Confidentiality



Cybersecurity systems should guarantee confidentiality for a long time



# The path to confidentiality: symmetric key crypto



Possible methods:

- ☐ Trusted courier (☹️)
- ☐ Public key cryptography (not quantum-safe today...)
- ☐ Quantum key distribution

# THE TOOLS QUANTUM RESISTANT ALGORITHMS



Name of method	Application	Resilience against Quantum Computer
DH	Key exchange	No
RSA	Key exchange, signature	No
ECC	Key exchange, signature	No
AES	Encryption	Widely believed
Hash-based	Authentication	Widely believed
Lattice-based (NTRU, New Hope)	Key exchange; signature	Believed
Code-based (Mc Eliece)	Key exchange	Believed
Multivariate polynomials	Key exchange; signature	Uncertain so far
...		

High level of confidence

Under investigation

Pros	Cons
<ul style="list-style-type: none"><li>• Direct replacement of current PKs</li></ul>	<ul style="list-style-type: none"><li>• No proof of security</li></ul>
<ul style="list-style-type: none"><li>• Keep all infrastructure</li></ul>	<ul style="list-style-type: none"><li>• Not yet well-studied</li></ul>
<ul style="list-style-type: none"><li>• May be easily adapted to security protocols</li></ul>	<ul style="list-style-type: none"><li>• Resilience against QC not proven</li></ul>
<ul style="list-style-type: none"><li>• Interesting approach: hybrid systems, e.g. RSA + Lattice</li></ul>	<ul style="list-style-type: none"><li>• Might be only a temporary solution...</li></ul>

➔ Probably the easiest to implement and most appealing solution...

➔ But concerns about **long-term security**