Quantum Cryptography

Christian Schaffner

Research Center for Quantum Software

Institute for Logic, Language and Computation (ILLC)
University of Amsterdam

Centrum Wiskunde & Informatica

ICT OPEN 2017

Tuesday, 21 March 2017

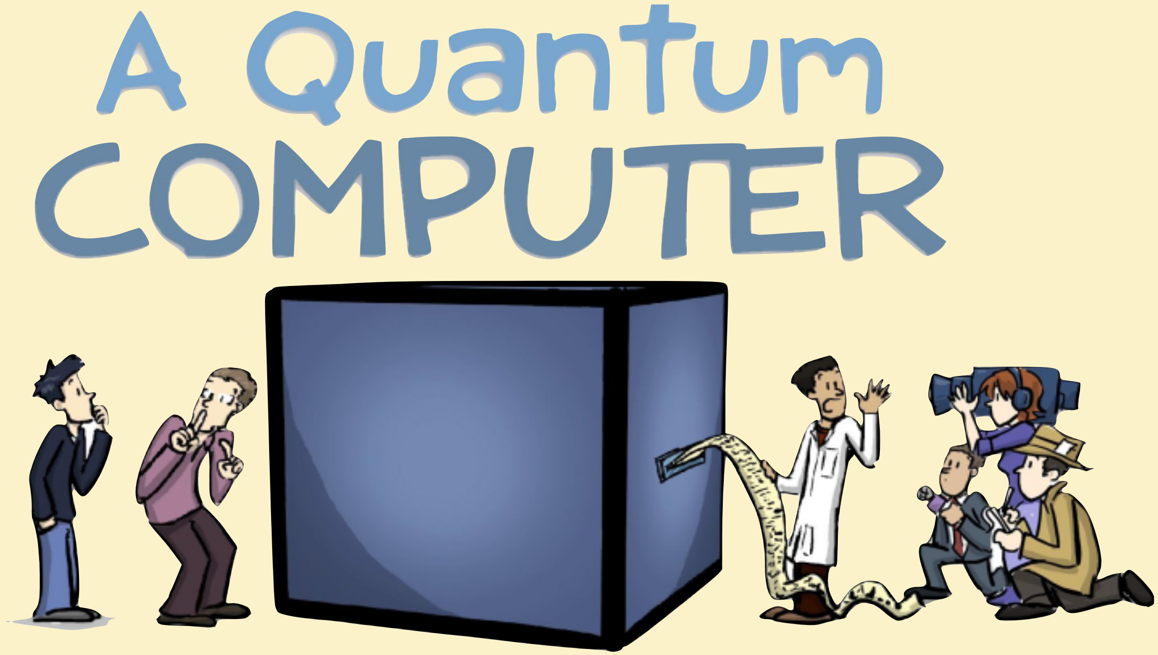
QuSoft

2

Keynote: Quantum Computer

Barbara Terhal

Where we stand with building



This talk:

What are the effects on cryptography?

Talk Outline

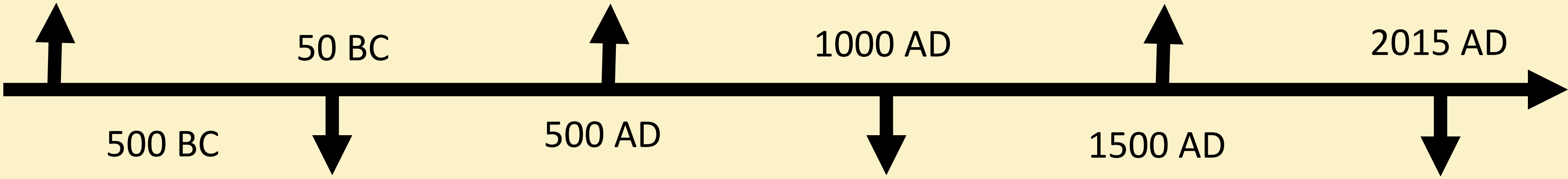
- Classical Cryptography
- Impact of Quantum Computers on Crypto
- When do we need to worry?

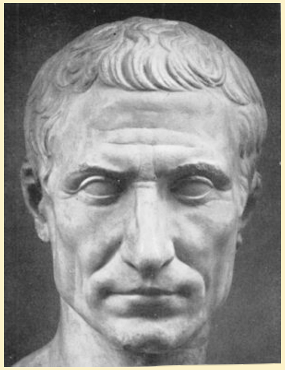
- Solutions
- Quantum Future

Ancient Cryptography

Scytale

Blaise de Vigenère

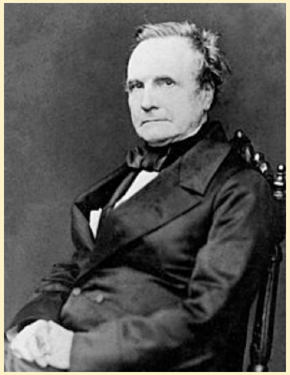




Caesar Cipher (ROT4)

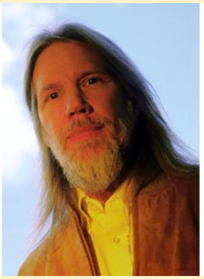
Ancient Cryptography

Charles Babbage



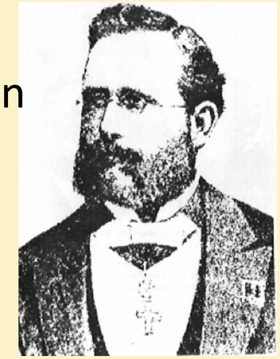
Claude Shannon

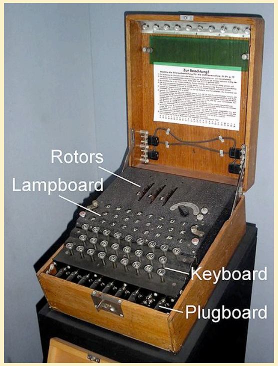
Diffie / Hellman



1800 1850 1900 1950 1976 2015

"A cryptosystem should be secure even if everything about the system, except the key, is public knowledge"





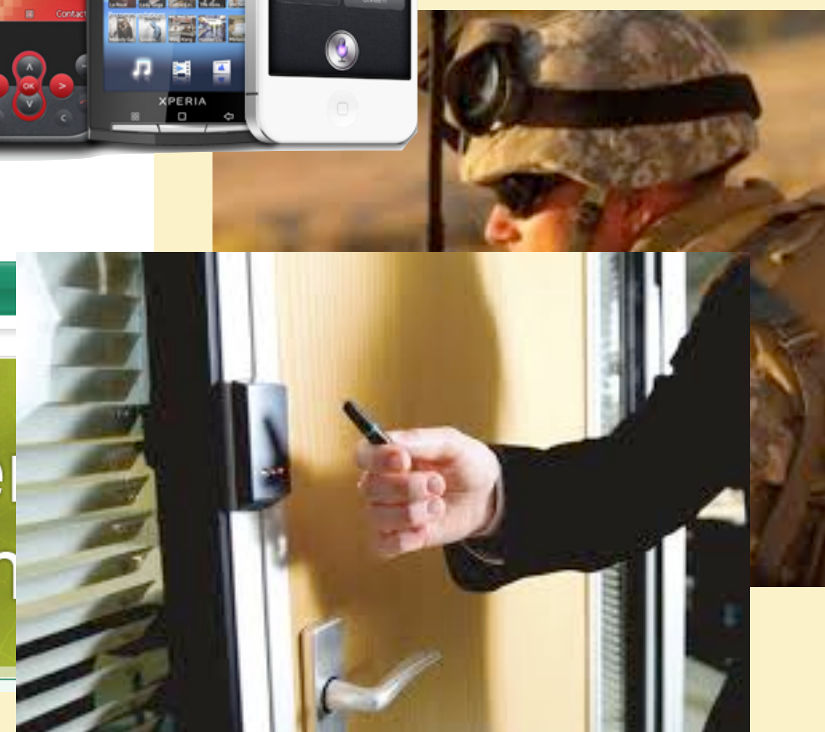
Auguste Kerckhoffs

Enigma

Alan Turing

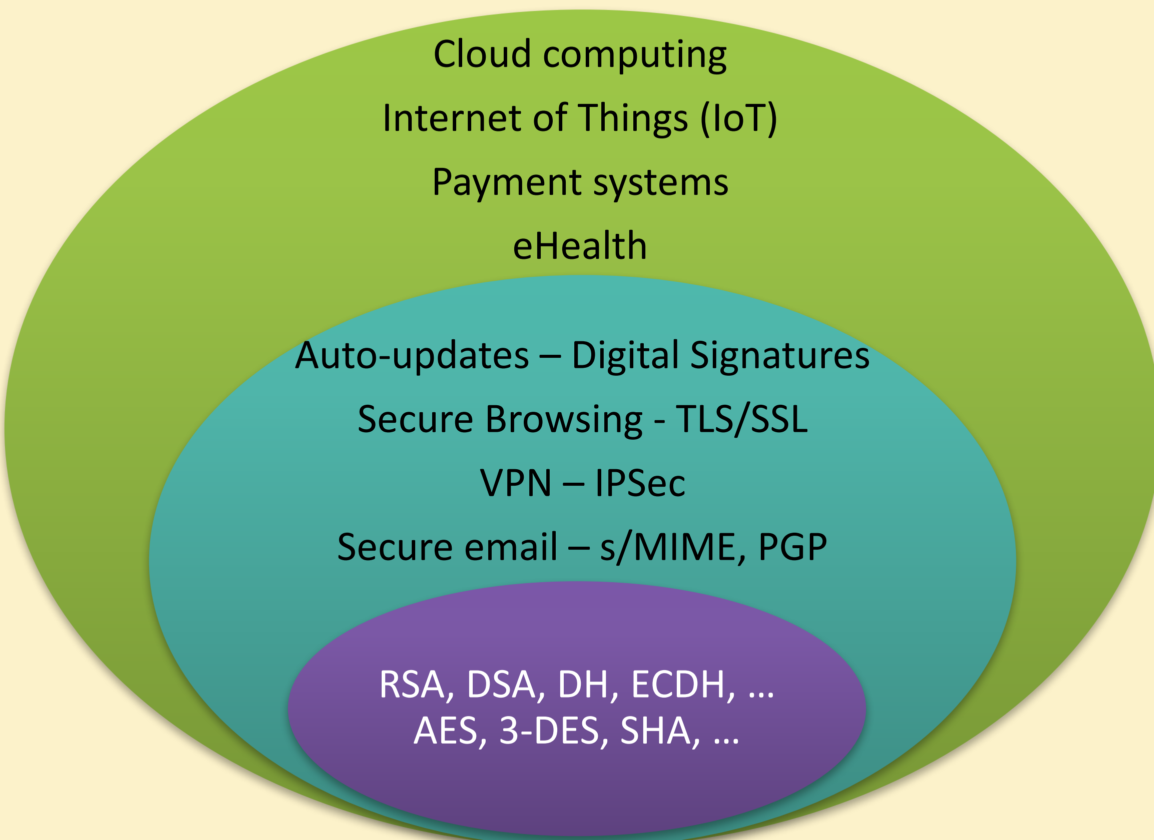
Modern Cryptography

- is everywhere!
- is concerned with all settings where people do not trust each other



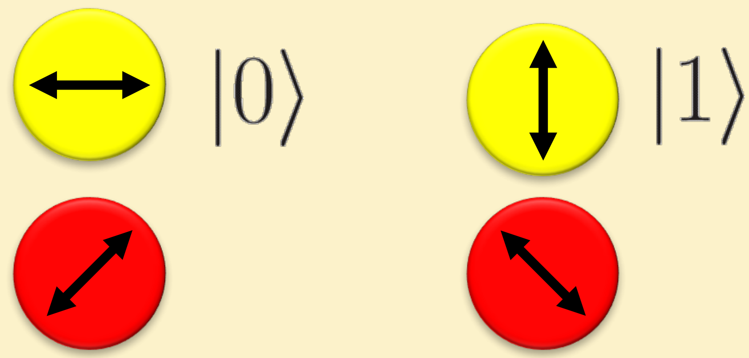
Cyber Security

- “Cyber Security in the Netherlands is an important focal area that provides security, safety and privacy solutions that are vital for our economy including but not limited to critical infrastructures, smart cities, cloud computing, online services and e-government.”



Based on slides by Michele Mosca

Quantum Effects



- Classical bit: 0 or 1
- Quantum bit: can be in superposition of 0 and 1
- Yields a more powerful computational model:
  - 1. Shor’s algorithm allows to efficiently factor integers
  - 2. Grover’s algorithm allows to search faster

Current Crypto under Quantum Attacks

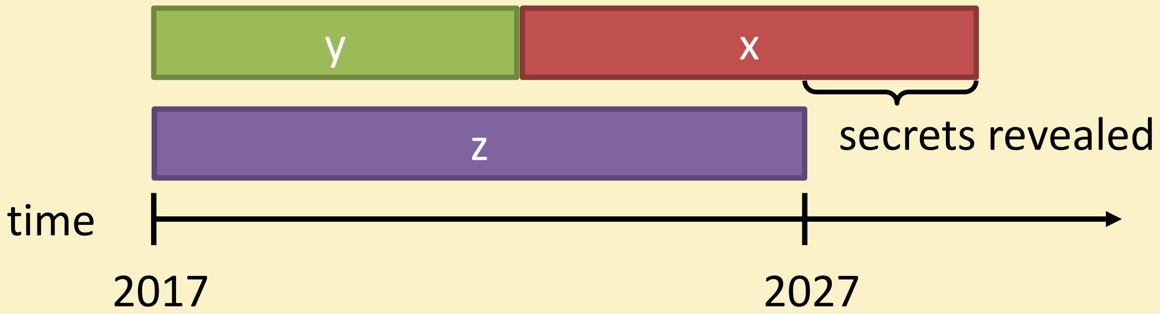
Security level systems	Conventional attacks	Quantum attacks
Symmetric-key encryption (AES-256)	256 bits	128 bits
Hash functions (SHA3-256)	128 bits	85 bits
Public-key crypto (key exchange, digital signatures, encryption) (RSA-2048)	112 bits	~ 0 bits
Public-key crypto (ECC-256)	128 bits	~ 0 bits

- Products, services, businesses relying on security either stop functioning or do not provide expected levels of security

When do we need to worry?

Depends on:

- How long do you need to keep your secrets secure? (x years)
- How much time will it take to re-tool the existing infrastructure? (y years)
- How long will it take for a large-scale quantum computer to be built? (z years)
- Theorem (Mosca): If x + y > z, then worry.



- Corollary: If x > z or y > z, you are in big trouble!

Slide by Michele Mosca

11

Talk Outline

- ✓ Classical Cryptography
- ✓ Impact of Quantum Computers on Crypto
- ✓ When do we need to worry?

- Solutions
- Quantum Future

Solution: Quantum-Safe Cryptography

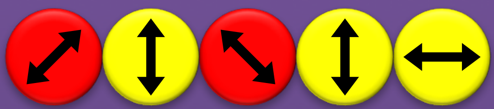
Conventional quantum-safe cryptography (post-quantum crypto)

- Can be deployed without quantum technologies
- Believed to be secure against quantum attacks of the future

+

Quantum Cryptography

- Requires some quantum technology (but no large-scale quantum computer)
- Typically no computational assumptions



Slide by Michele Mosca

Quantum Cryptography Landscape

technical difficulty (€)

Security level / systems	Conventional attacks	Quantum attacks
Symmetric-key encryption (AES-256)	256 bits	128 bits
Hash functions (SHA3-256)	128 bits	85 bits
Public-key crypto (key exchange, digital signatures, encryption) (RSA-2048)	112 bits	~ 0 bits
Hash-based signatures	probably	probably
McEliece	probably	probably
Lattice-based	probably	probably
Quantum Key Distribution (QKD)	provable	provable

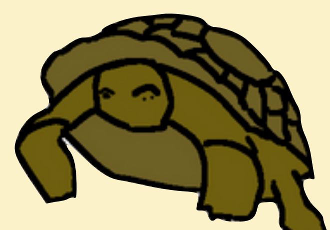
Qantum-safe Crypto

Conventional Quantum-Safe Crypto

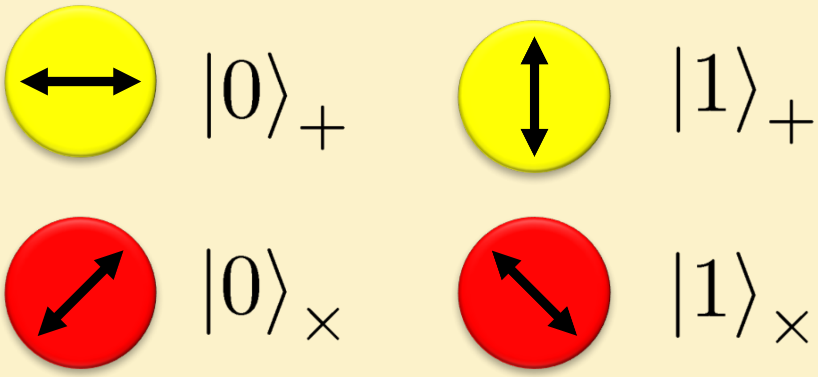
- **Wanted**: new assumptions to replace factoring and discrete logarithms in order to build conventional public-key cryptography

QuSoft

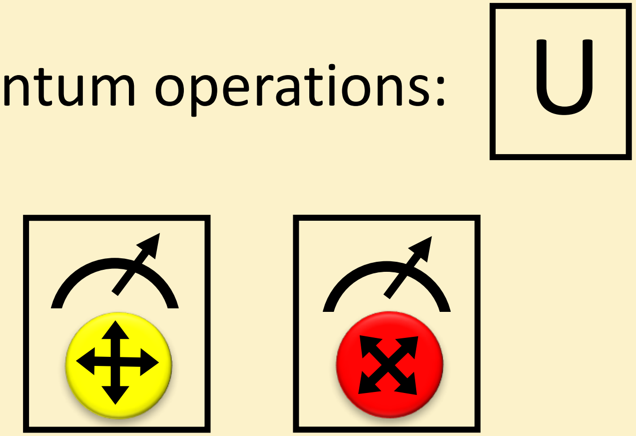
PQCRYPTO
ICT-645622

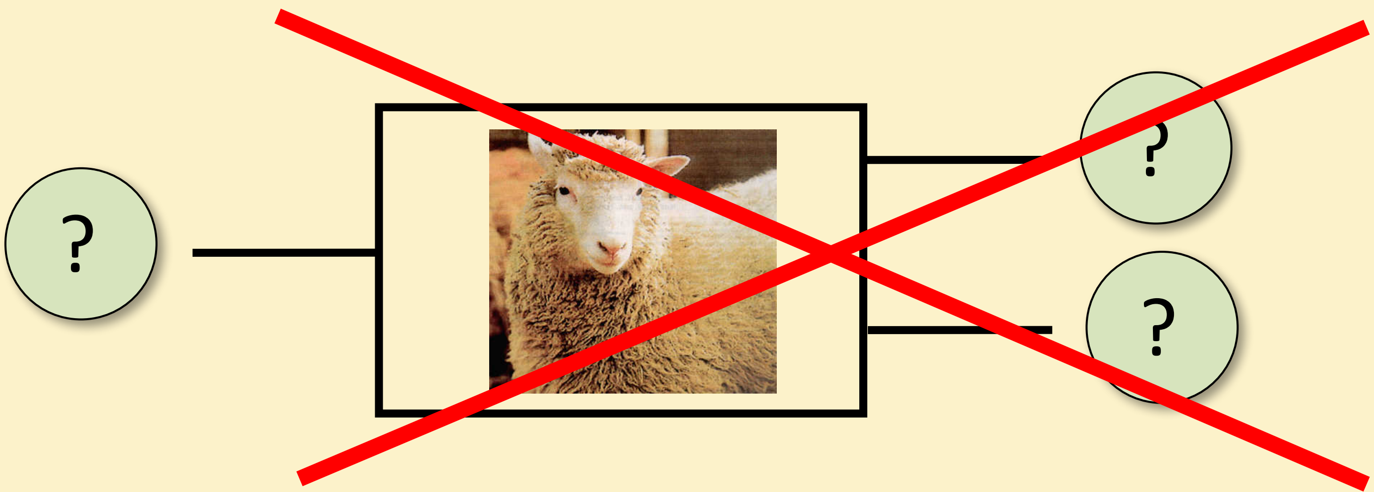


No-Cloning Theorem



Quantum operations:

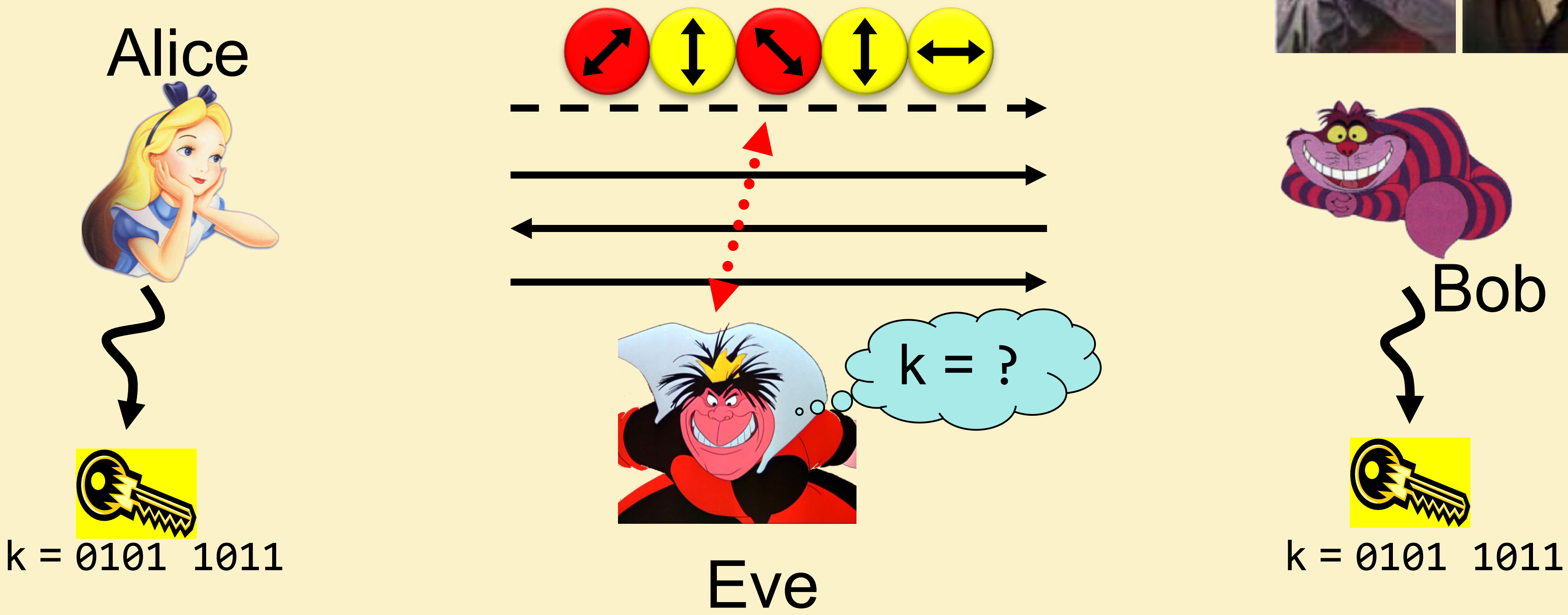




Proof: copying is a non-linear operation

Quantum Key Distribution (QKD)

[Bennett Brassard 84]

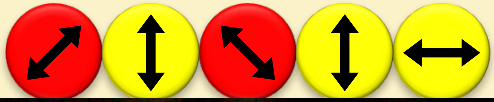


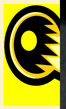
- Offers an quantum solution to the key-exchange problem which does not rely on computational assumptions (such as factoring, discrete logarithms, security of AES, SHA-3 etc.)
- Puts the players into the starting position to use symmetric-key cryptography (encryption, authentication etc.).

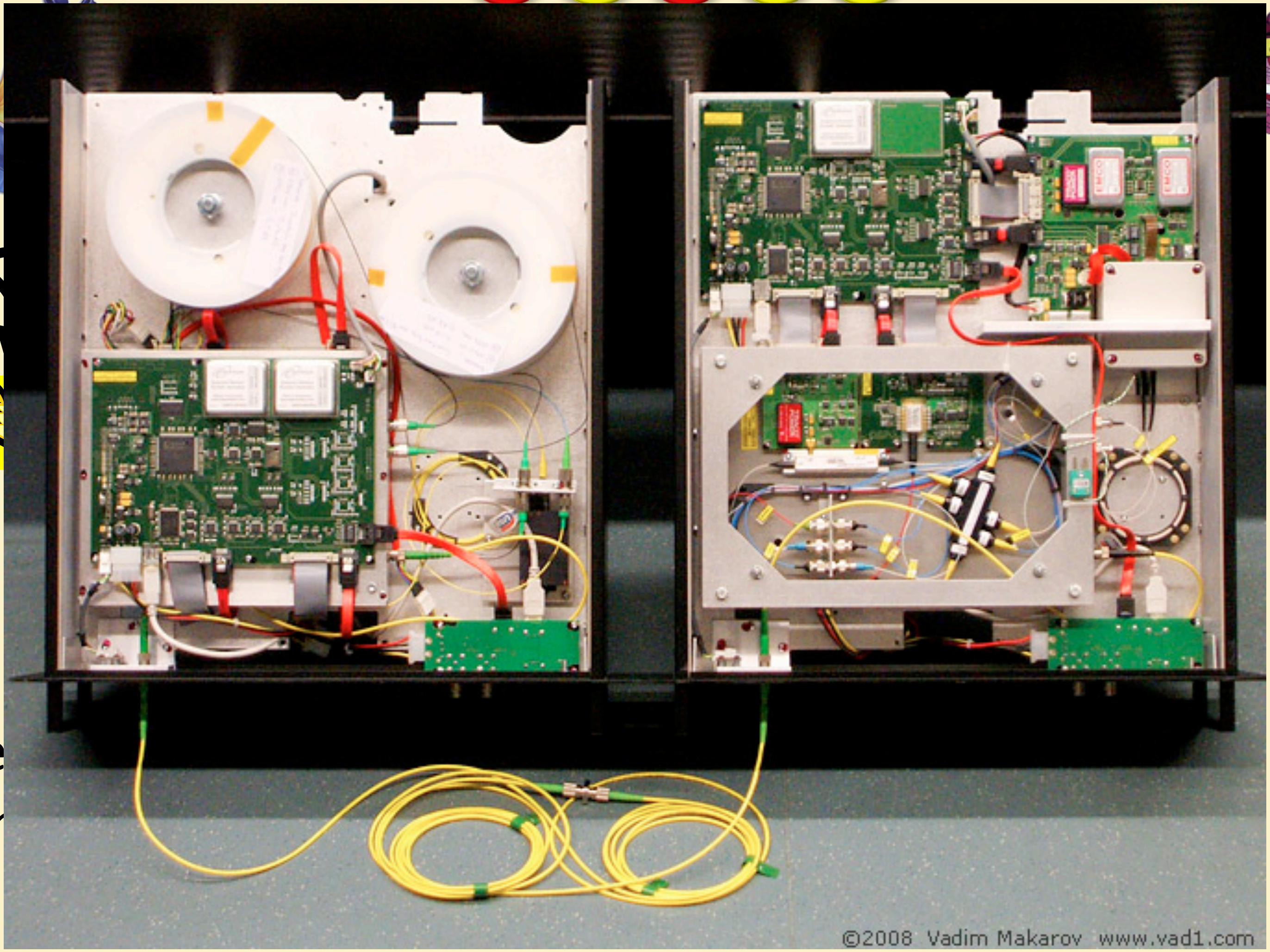
Quantum Key Distribution (QKD)

[Bennett Brassard 84]

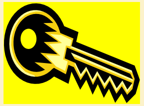
Alice







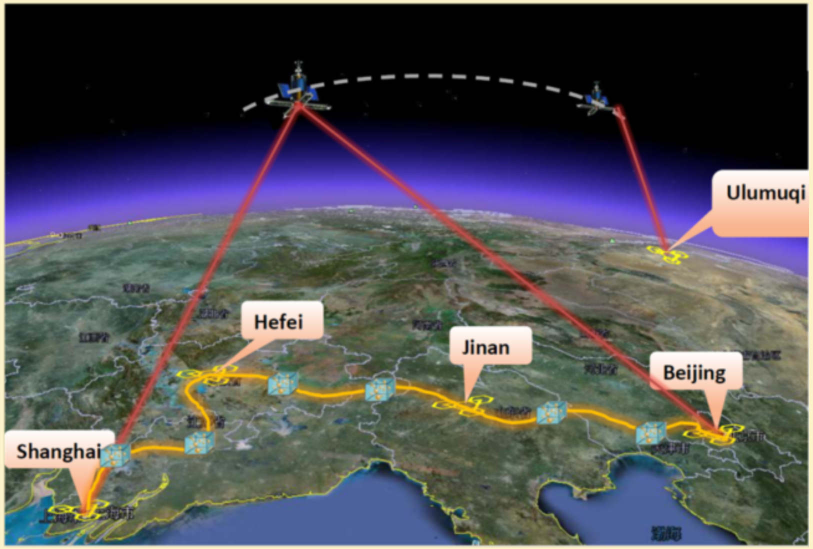
Bob

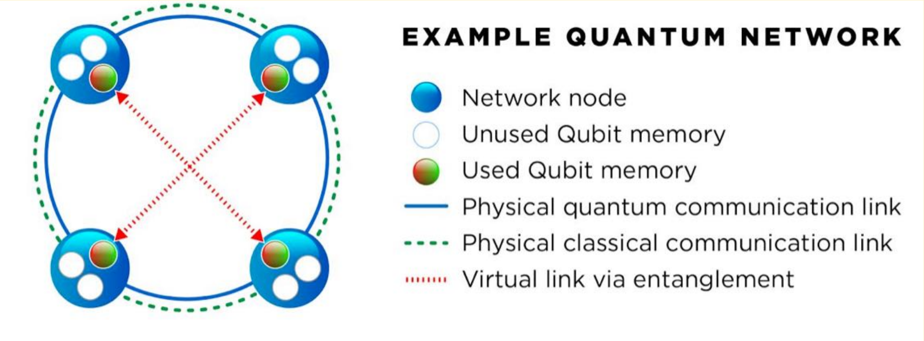


- te
  or

Quantum Networks

- 2000km QKD backbone network between Beijing and Shanghai
- first QKD satellite launched in 2016 from China
- Applied for funding to build the first quantum network in NL
- Quantum entanglement allows to generate secure keys (like QKD)

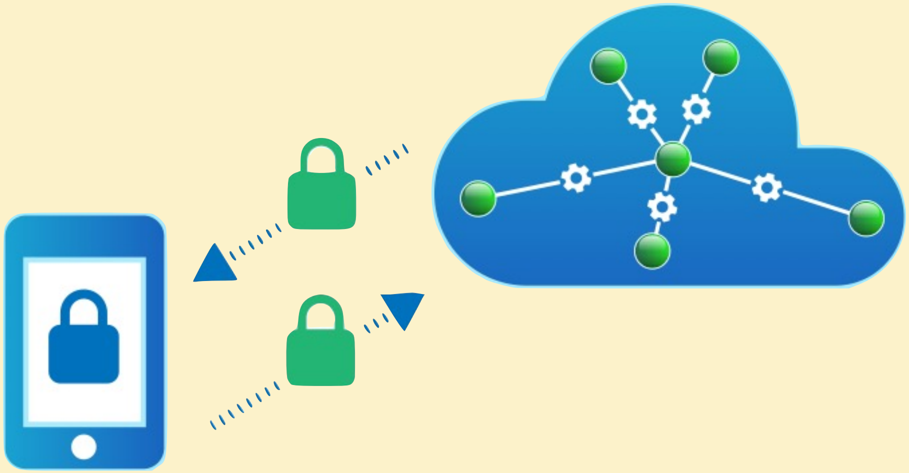




Secure Computing in Quantum Cloud

- Distributed quantum computing

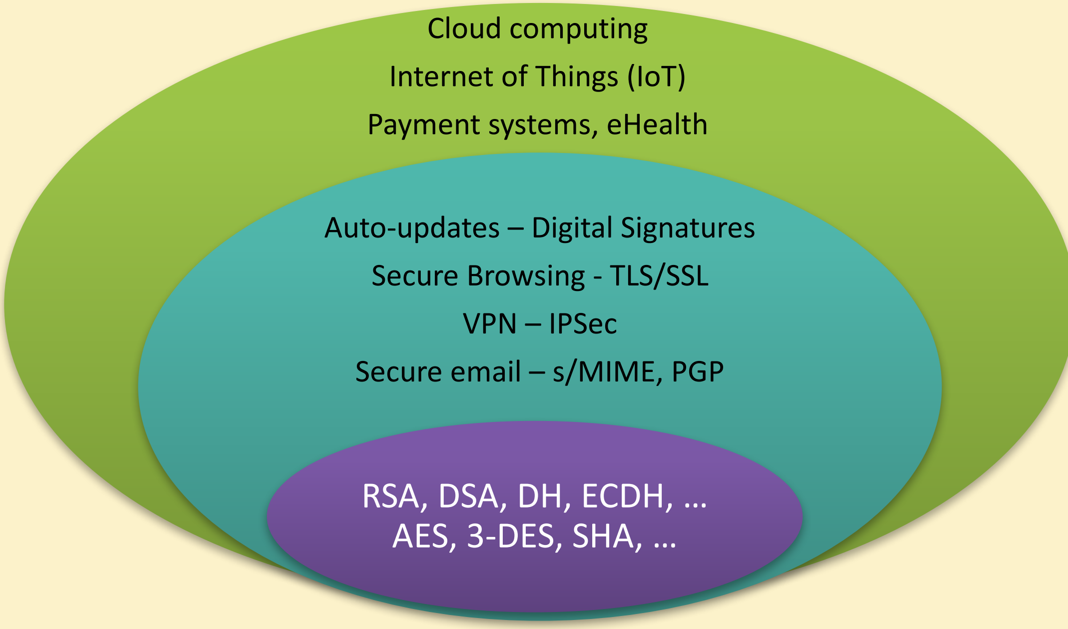
- Recent result: quantum homomorphic encryption allows for secure delegated quantum computation



Y. Dulek, C. Schaffner, and F. Speelman, arXiv:1603.09717
Quantum homomorphic encryption for polynomial-sized circuits, in CRYPTO 2016, QIP 2017

Summary

✓ Cyber Security



✓ Impact of Quantum Computing on crypto

Security level / systems	Conventional attacks	Quantum attacks
Symmetric-key crypto	128 bits	reduced
Public-key crypto	112 bits	broken!

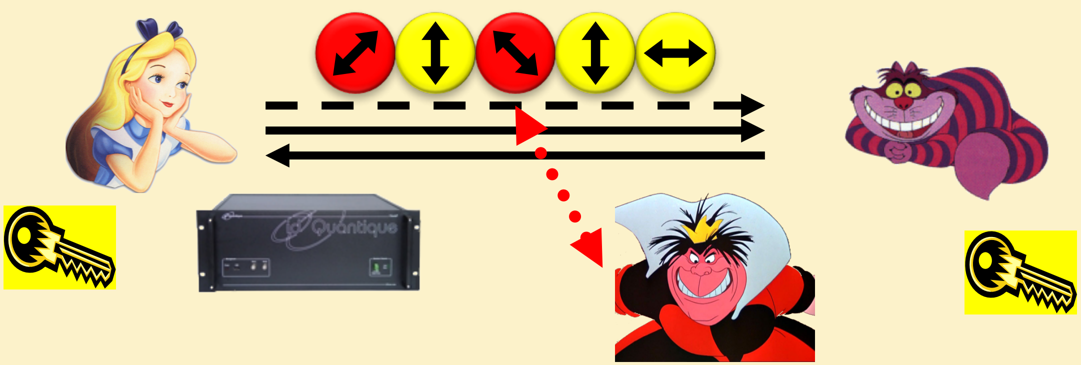
Thm: If x + y > z, then worry

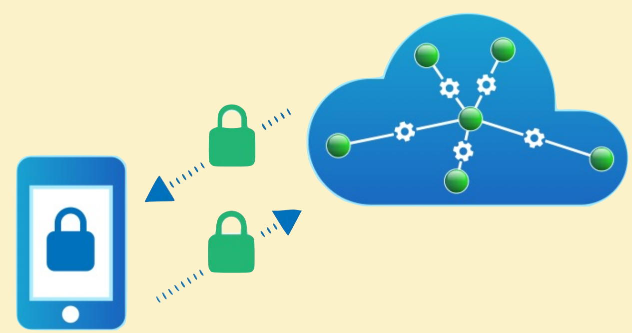
Summary

✓ Quantum-safe crypto:

Conventional quantum-safe cryptography (post-quantum crypto) + Quantum Cryptography

✓ Quantum Key Distribution, Quantum Cloud





Thank you for your attention!

Questions

check http://arxiv.org/abs/1510.06120 for a recent survey on quantum cryptography beyond key distribution