CWI IN BEDRIJF
Technology for Tomorrow
18 mei 2017

Quantum Cryptography

Christian Schaffner

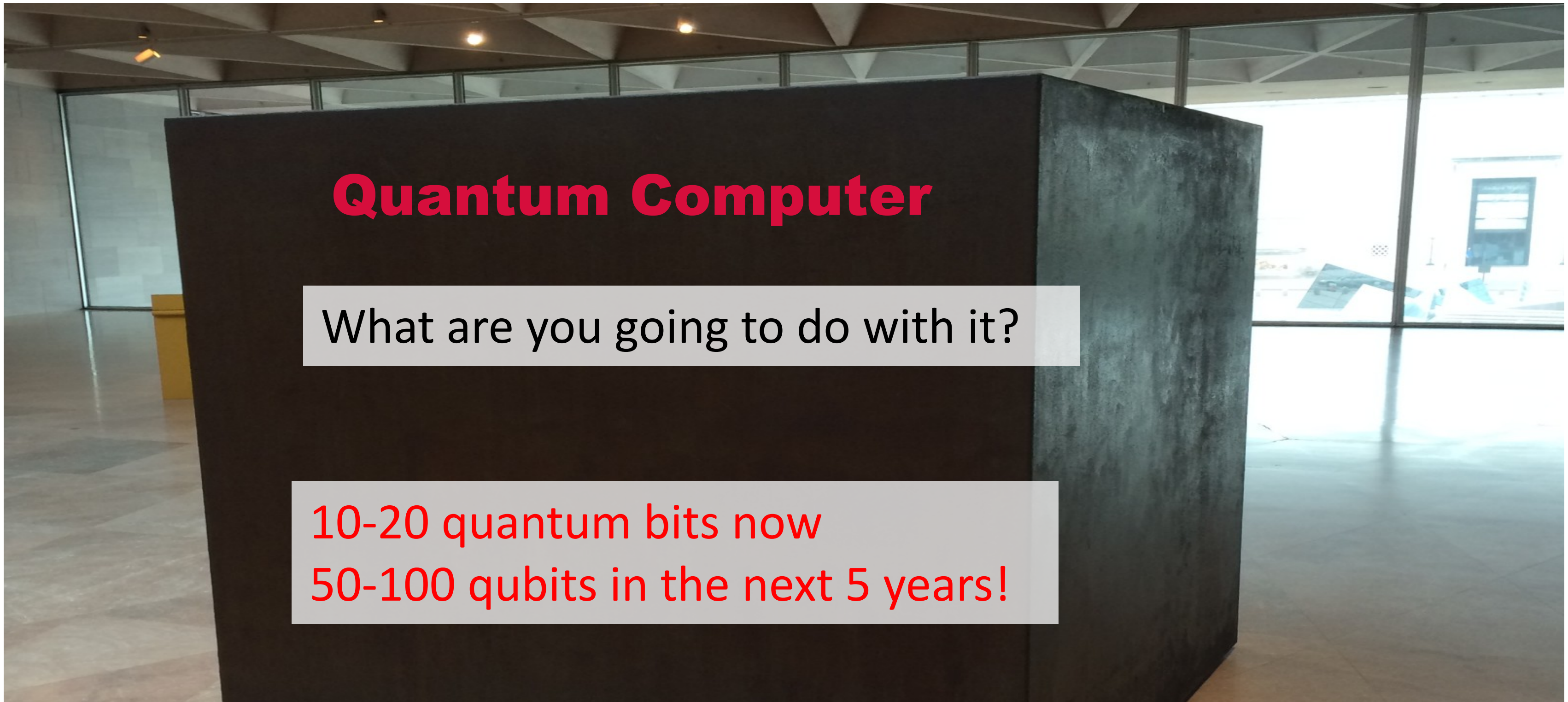
QuSoft Research Center for Quantum Software

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

CWI Centrum Wiskunde & Informatica

NWO Nederlandse Organisatie voor Wetenschappelijk Onderzoek

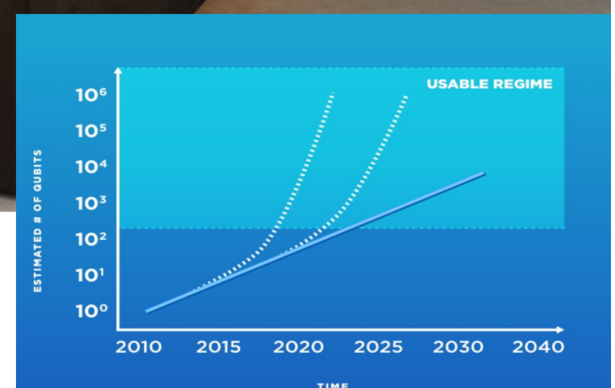
CWI IN BEDRIJF
Technology for Tomorrow
18 mei 2017



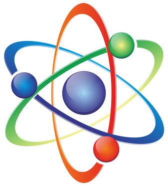
Quantum Computer

What are you going to do with it?

10-20 quantum bits now
50-100 qubits in the next 5 years!

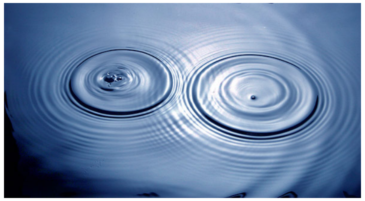


Quantum Software is Fundamentally Different



- Qubit: superposition of 0 and 1
- Massive parallel computation:
  - Each extra qubit doubles number of parameters
  - 300 qubits bigger than number of atoms in universe
  - Exponentially large state space

- How to get the answer out??
  - Measuring destroys computation!!
- Quantum Program
  - Use interference to cancel unwanted computations
  - Counterintuitive, fundamentally different from classical programming



- Does not work for every computational problem!
  - most problems no speed-up!

CWI IN BEDRIJF
Technology for Tomorrow
18 mei 2017

Quantum Software

- Focus mostly on quantum hardware
- Time is now to put more effort into quantum software. It is essential for a successful quantum future.

- Launch research center for quantum software:

QuSoft

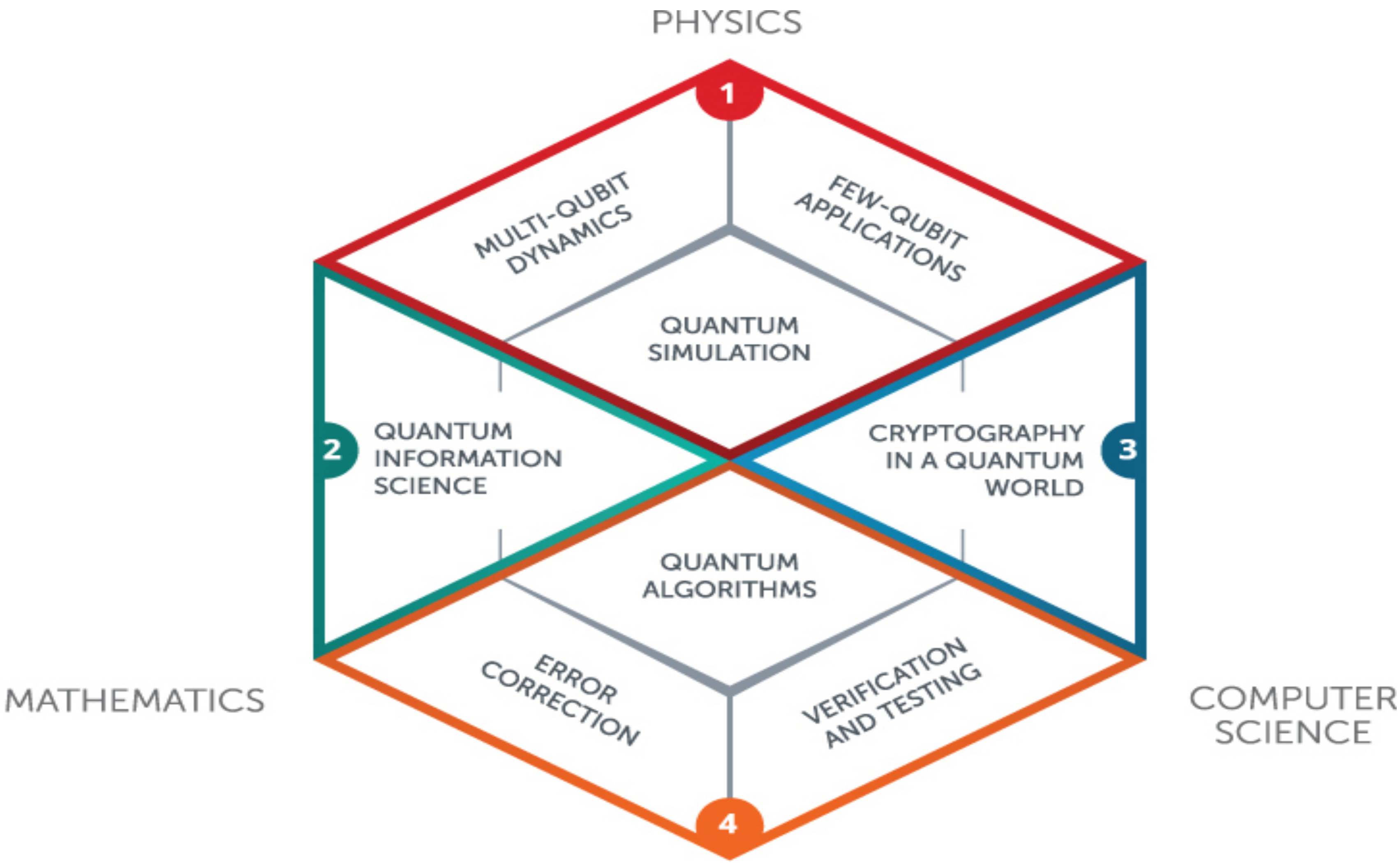
CWI

VU VRIJE UNIVERSITEIT AMSTERDAM

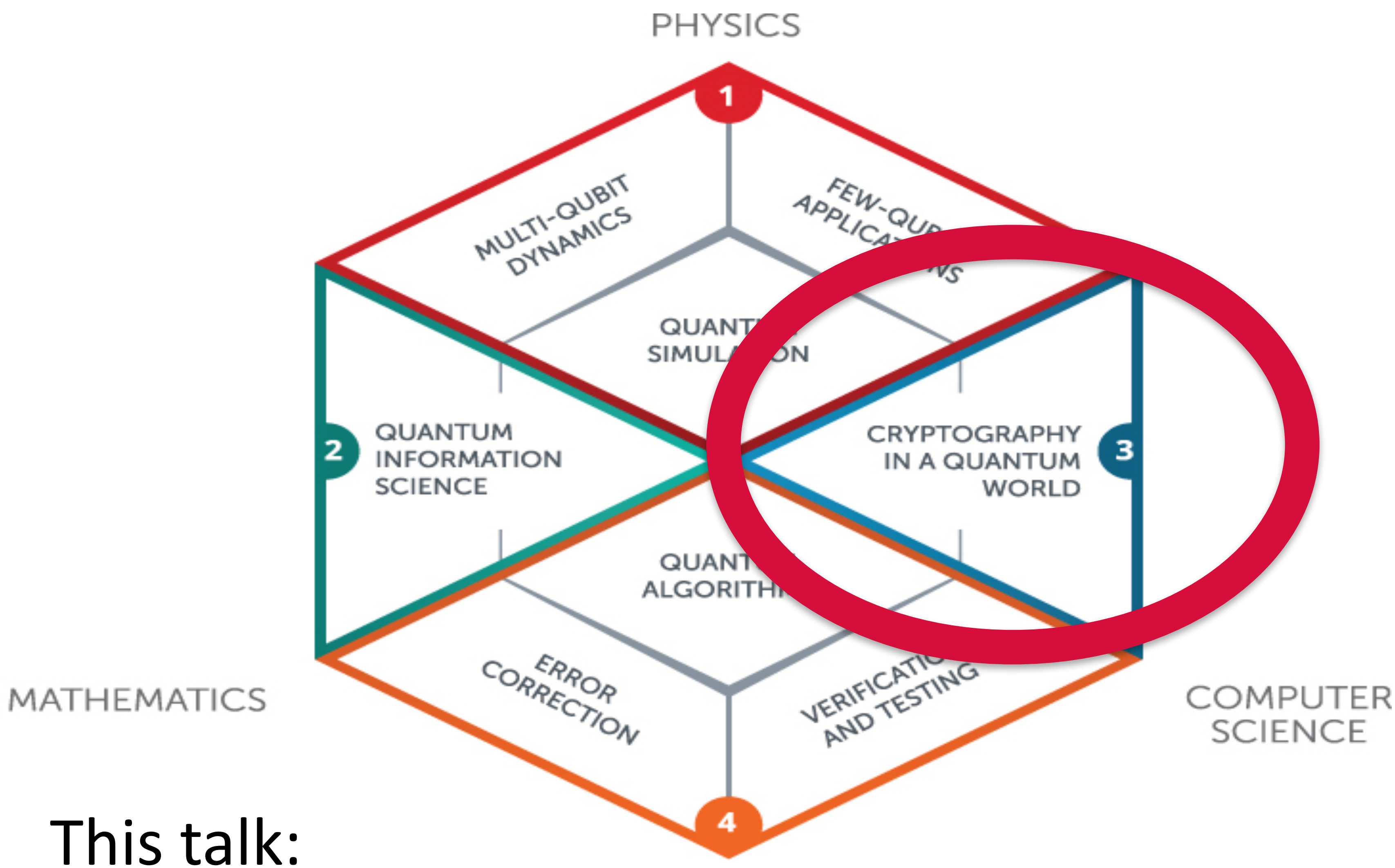
CWI IN BEDRIJF Technology for Tomorrow 18 mei 2017

QuSoft
Research Center for Quantum Software

“Enabling the power of quantum computers”



"Enabling the power of quantum computers"



This talk:

What are the effects on cryptography?

Talk Outline

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

CWI IN BEDRIJF Technology for Tomorrow 18 mei 2017

Ancient Cryptography

Scytale

Blaise de Vigenère

500 BC

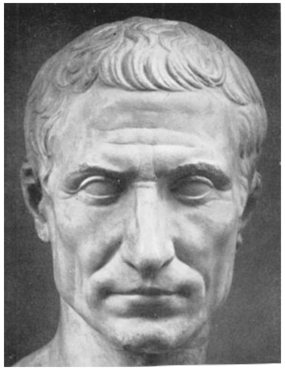
50 BC

500 AD

1000 AD

1500 AD

2015 AD



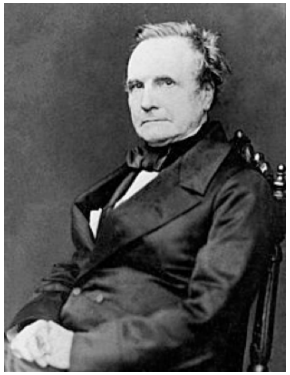
Caesar Cipher (ROT4)

QuSoft

CWI IN BEDRIJF
Technology for Tomorrow
18 mei 2017

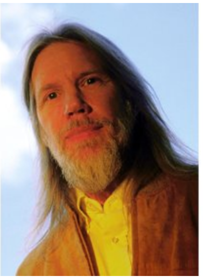
Ancient Cryptography

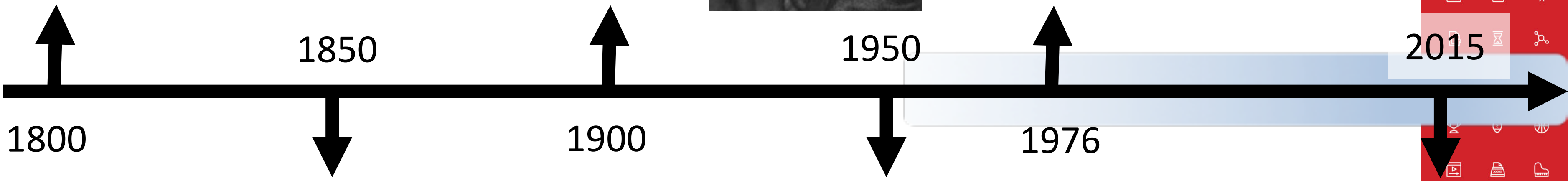
Charles Babbage



Claude Shannon

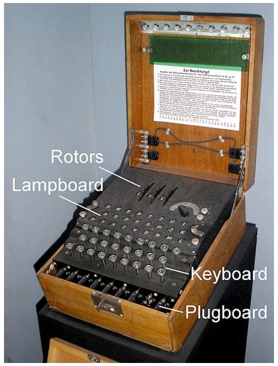
Diffie / Hellman





"een systeem van versleuteling moet even veilig zijn, zelfs als alles behalve de sleutel over het systeem publiek bekend is"

Auguste Kerckhoffs



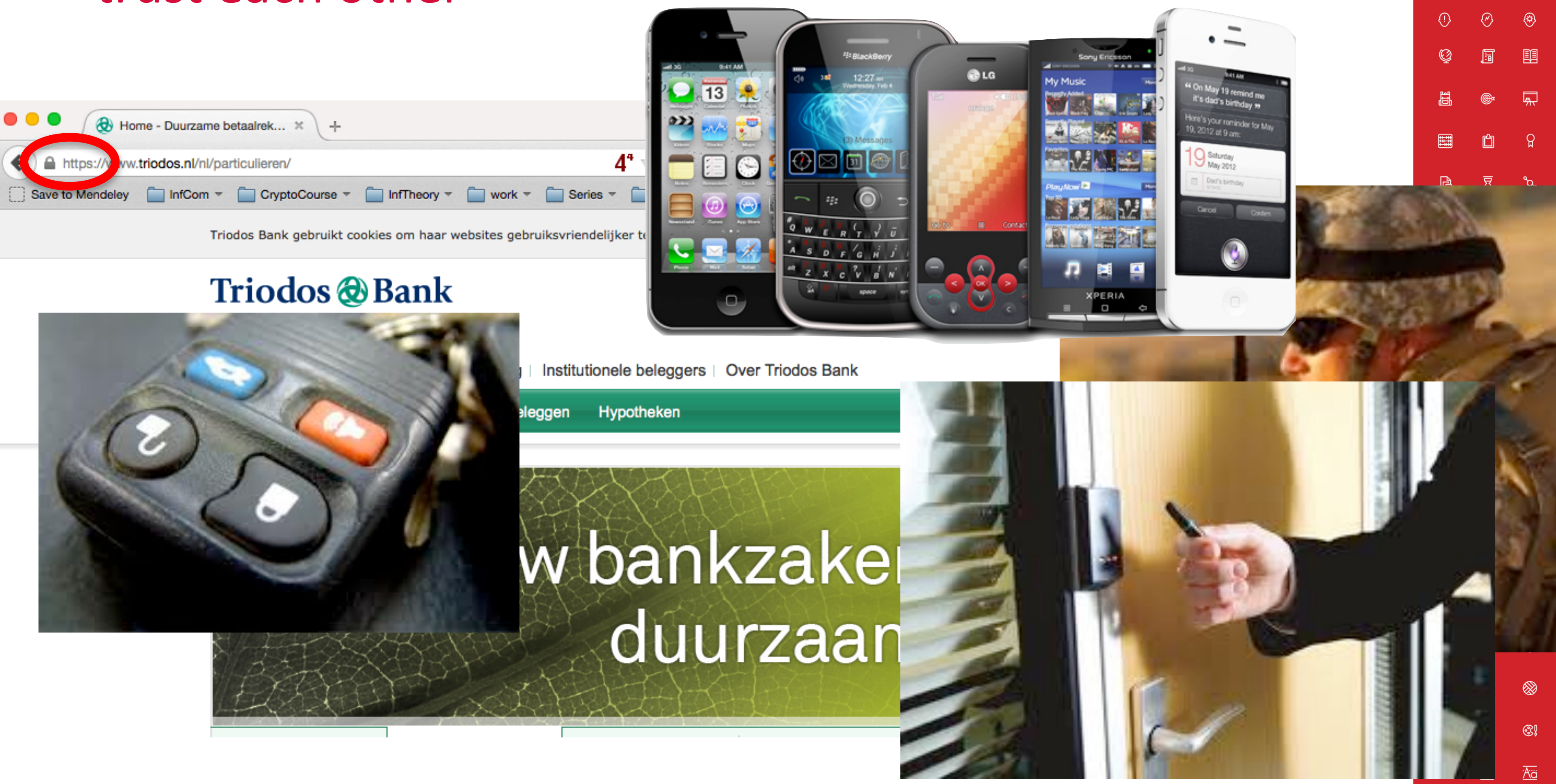
Enigma

Alan Turing

QuSoft

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.”

Cloud computing
Internet of Things (IoT)
Payment systems
eHealth

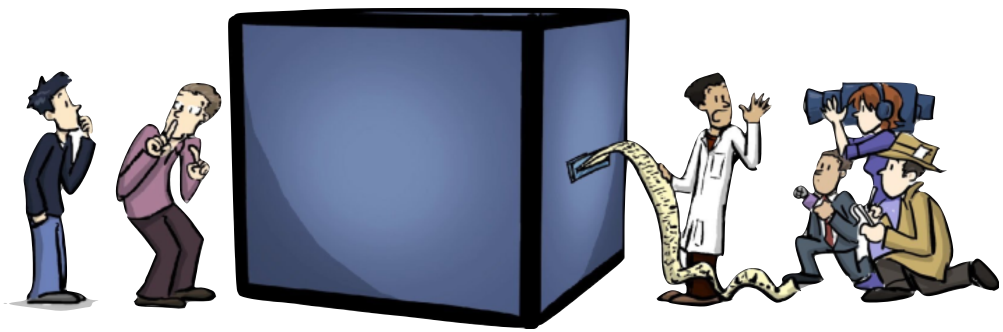
Auto-updates – Digital Signatures
Secure Browsing - TLS/SSL
VPN – IPSec
Secure email – s/MIME, PGP

RSA, DSA, DH,
ECDH, …
AES, 3-DES, SHA, …

Based on slides by Michele Mosca

CWI IN BEDRIJF Technology for Tomorrow 18 mei 2017

Quantum Effects



A Quantum COMPUTER

- Classical bit: 0 or 1
- Quantum bit: can be in superposition of 0 and 1

- Yields a more powerful computational model:
  - Shor's algorithm allows to factor numbers
  - Grover's algorithm allows to search faster

CWI IN BEDRIJF
Technology for Tomorrow
18 mei 2017

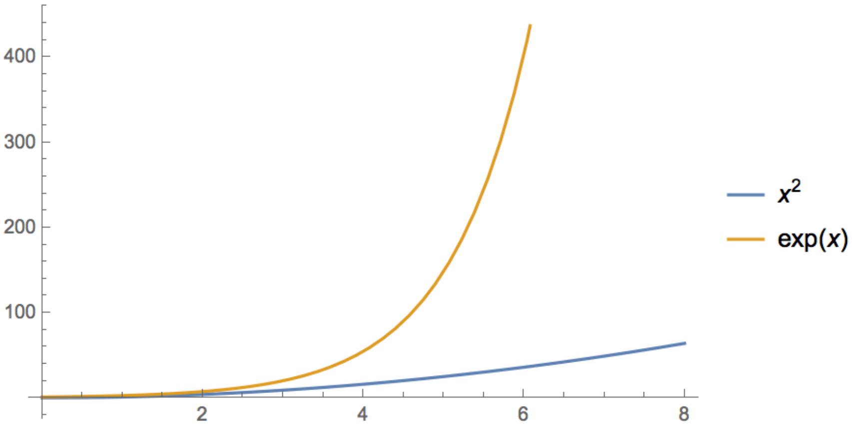
Quantum Algorithms: Factoring

- [Shor ’94] Polynomial-time quantum algorithm for factoring integer numbers
- 15 = 3 * 5
- 27 =
- 31 =
- 57 =
- 91 =
- 173 =
- RSA-100 = 152260502792253336053561837813263742971806811496138068 8657908494580122963258952897654000350692006139 =

Quantum Algorithms: Factoring

- [Shor '94] Polynomial-time quantum algorithm for factoring integer numbers

- Classical Computer : Exponential time
- Quantum Computer : Poly-time: n^2
- For a 600-digit number (RSA-2048)
  - Classical: age of universe
  - Quantum: few minutes



CWI IN BEDRIJF
Technology for Tomorrow
18 mei 2017

Current Cryptography under Quantum Attacks

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

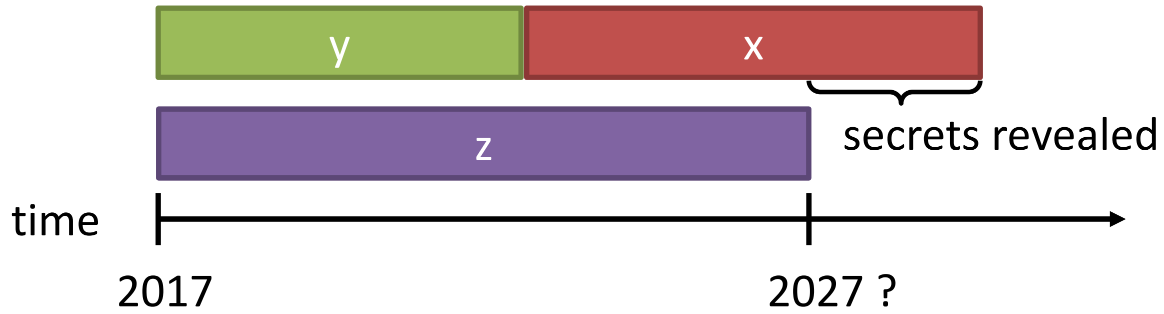
- Products, services, businesses relying on security either stop functioning or do not provide expected levels of security (like last week's ransomware events)

CWI IN BEDRIJF
Technology for Tomorrow
18 mei 2017

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

Talk Outline

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

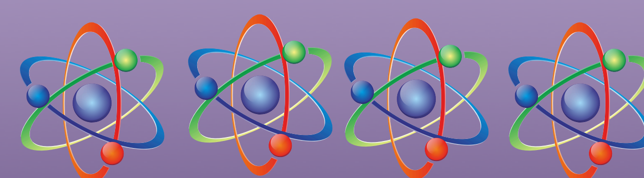
CWI IN BEDRIJF
Technology for Tomorrow
18 mei 2017

Solution: Quantum-Safe Cryptography

Classical quantum-safe cryptography (post-quantum crypto)

+

Quantum Cryptography



Slide by Michele Mosca

CWI IN BEDRIJF
Technology for Tomorrow
18 mei 2017

Quantum Crypto Landscape

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

technical difficulty (€)

Qantum-safe Crypto

Conventional Quantum-Safe Crypto

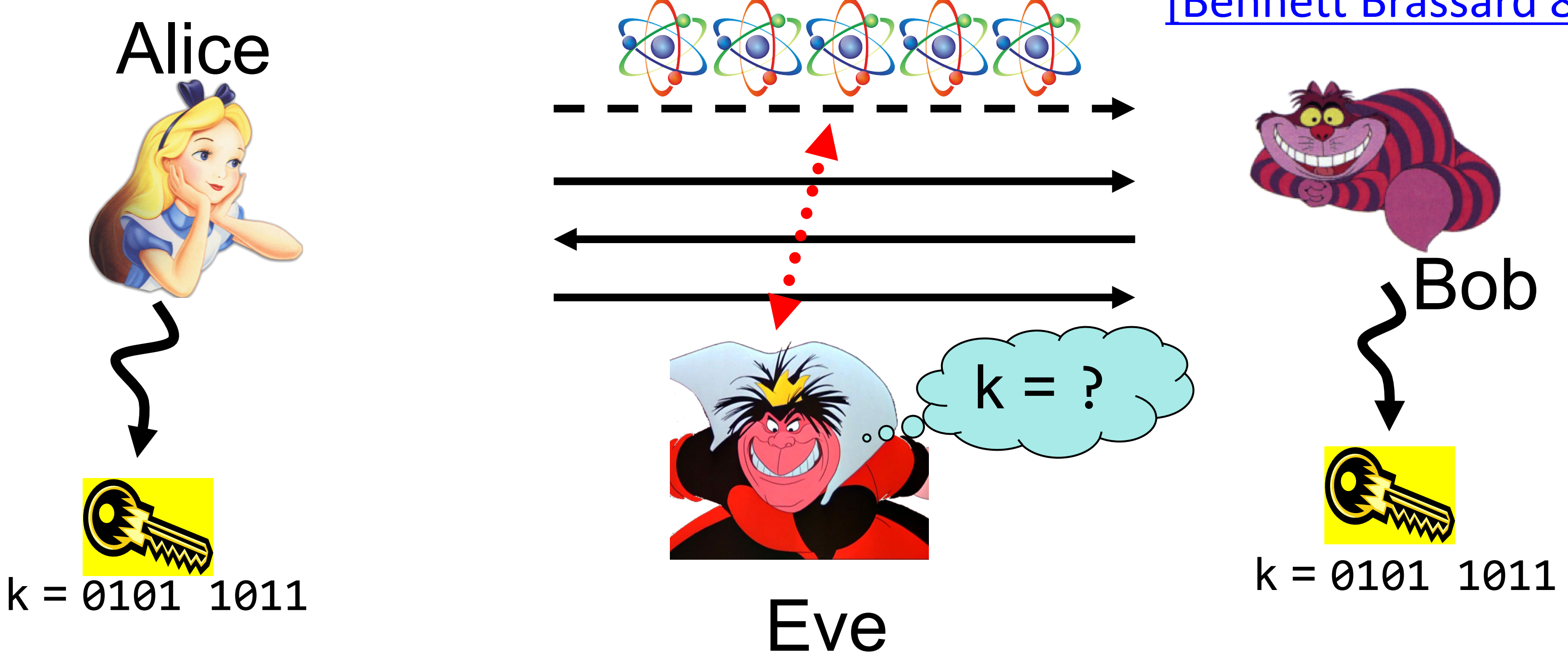
- **Wanted**: new assumptions to replace factoring and discrete logarithms in order to build conventional public-key cryptography

QuSoft

PQCRYPTO
ICT-645622

Quantum Key Distribution (QKD)

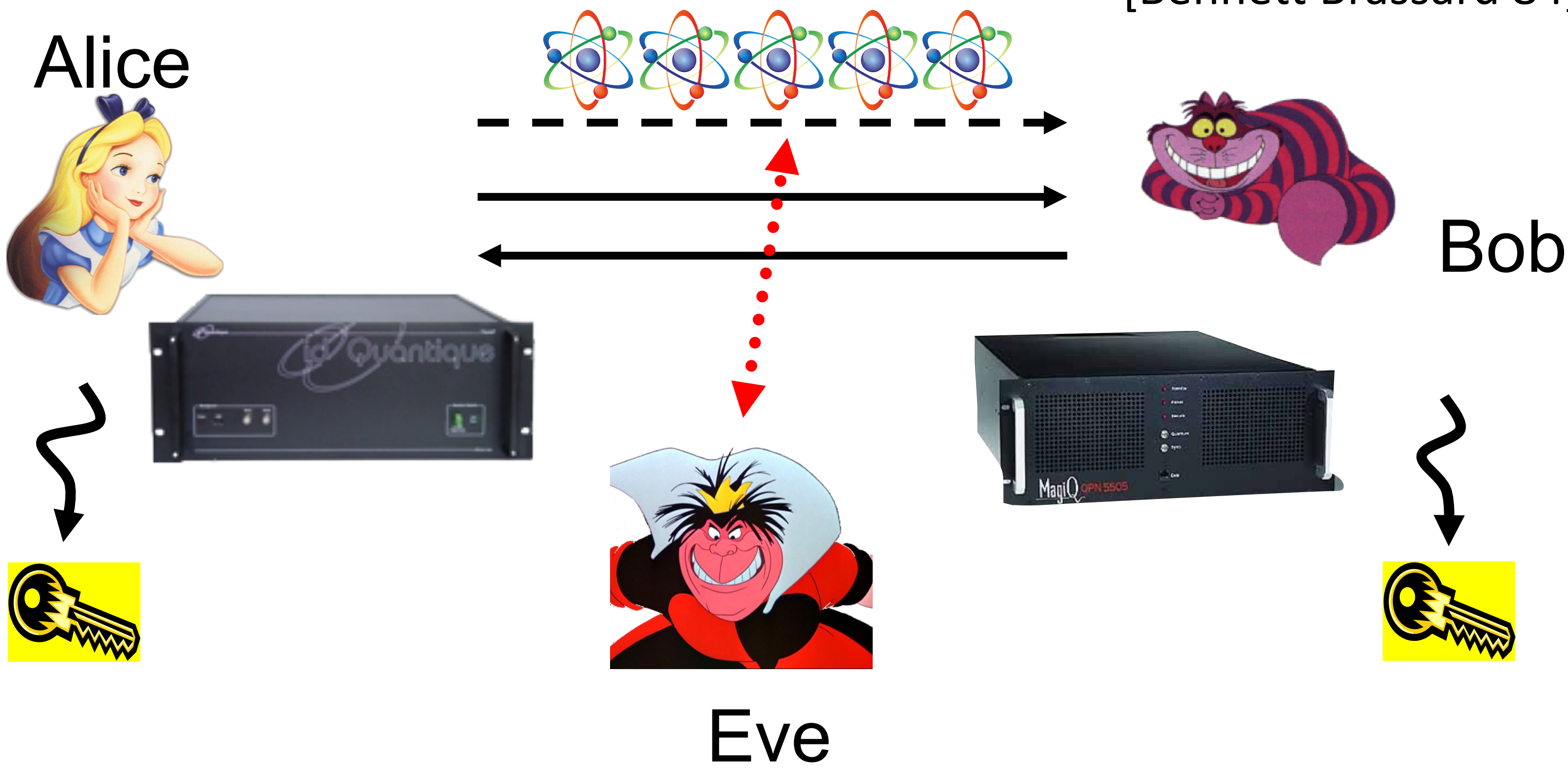
[Bennett Brassard 84]



- Offers an quantum solution to the key-exchange problem which does not rely on computational assumptions

Quantum Key Distribution (QKD)

[Bennett Brassard 84]



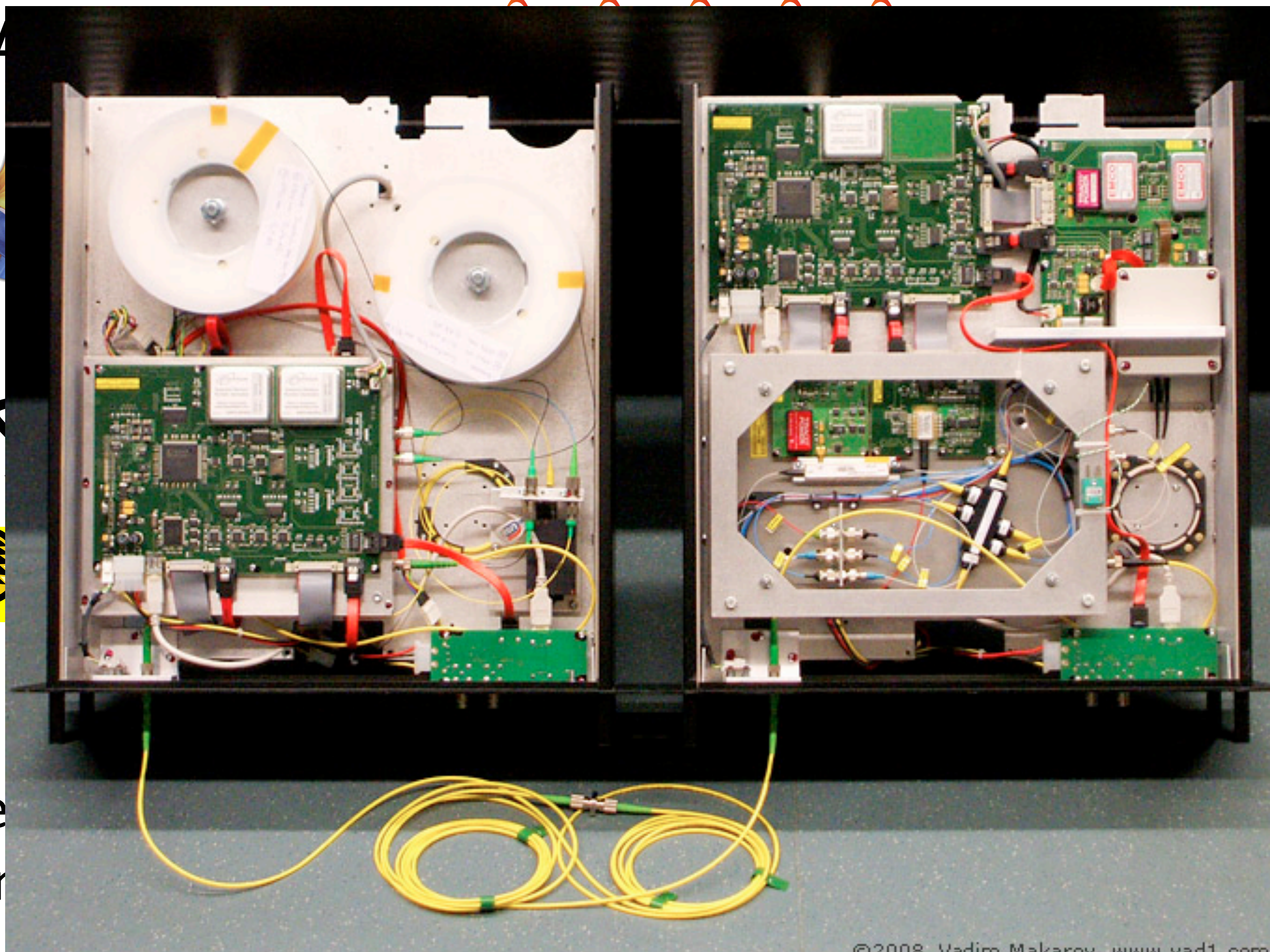
- technically feasible: no quantum computer required, only quantum communication

Quantum Key Distribution (QKD)

[Bennett Brassard 84]

A

Bob



- te
  or

Solution:
Quantum-Safe Cryptography

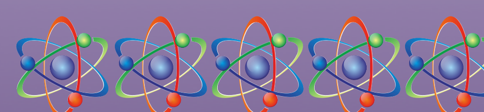
Conventional quantum-safe cryptography (post-quantum crypto)

- 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

Talk Outline

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

Quantum Research in NL

QuSoft
Research Center for Quantum Software

intel

QUTech

Universiteit Leiden

Microsoft

TNO

TU/e Technische Universiteit Eindhoven University of Technology

QuTech: 135 mln € , 50 mln $ Intel

May 2017: NWO Zwaartekracht: 18.8 mln € for 10 years

CWI IN BEDRIJF
Technology for Tomorrow
18 mei 2017

Quantum Research in EU

17 May 2016: 1 mld € flagship program on Q technologies

CWI IN BEDRIJF Technology for Tomorrow 18 mei 2017

Quantum Research Worldwide

Google

IBM

intel

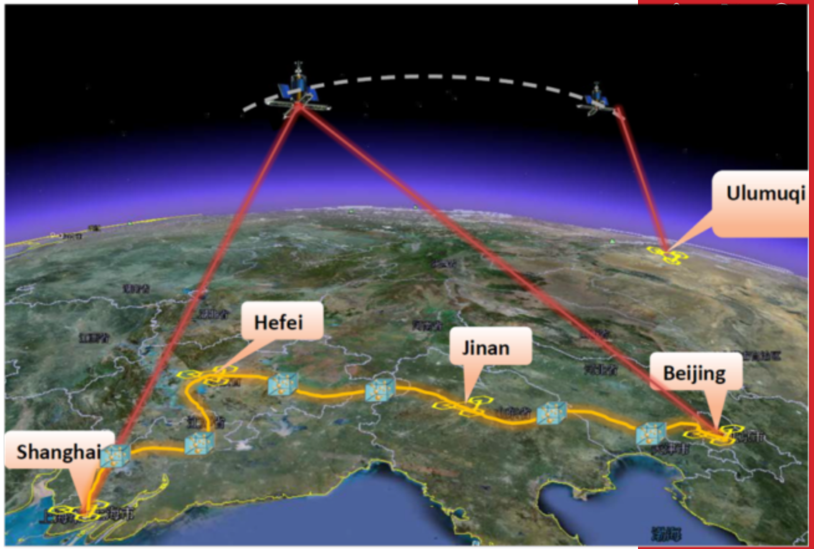
Microsoft

Waterloo, Singapore, Santa Barbara, China, …

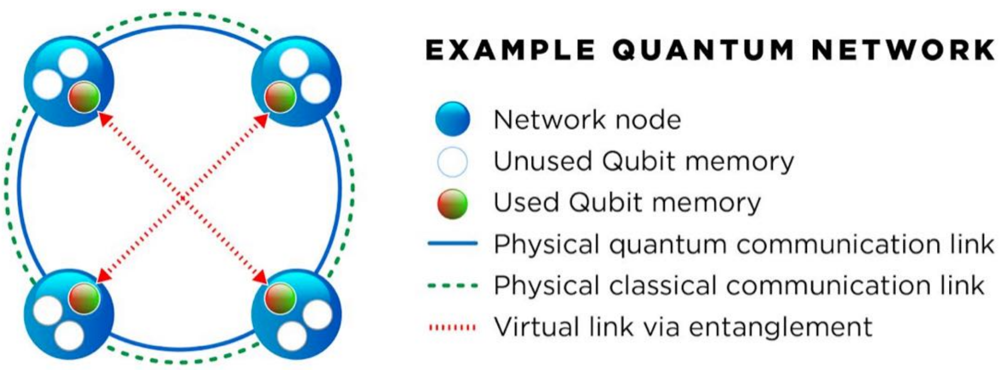
CWI IN BEDRIJF Technology for Tomorrow 18 mei 2017

Quantum Networks

- 2000km QKD backbone network between Beijing and Shanghai
- first QKD satellite launched in 2016 from China



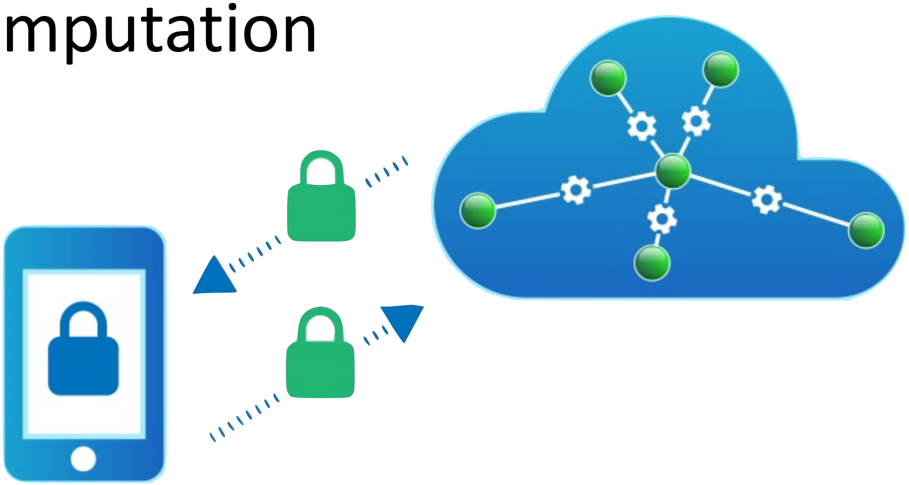
- Quantum entanglement allows to generate secure keys (like QKD)



Secure Computing in Quantum Cloud

- Distributed quantum computing

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

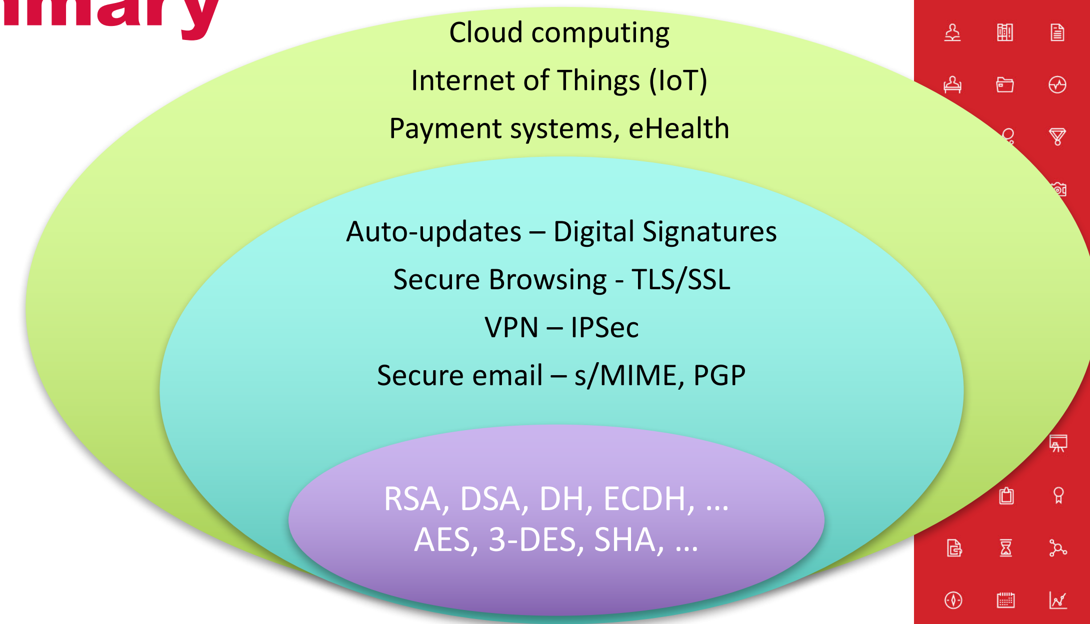


Y. Dulek, C. Schaffner, and F. Speelman, arXiv:1603.09717 *Quantum homomorphic encryption for polynomial-sized circuits*, in CRYPTO 2016, QIP 2017

CWI IN BEDRIJF
Technology for Tomorrow
18 mei 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!

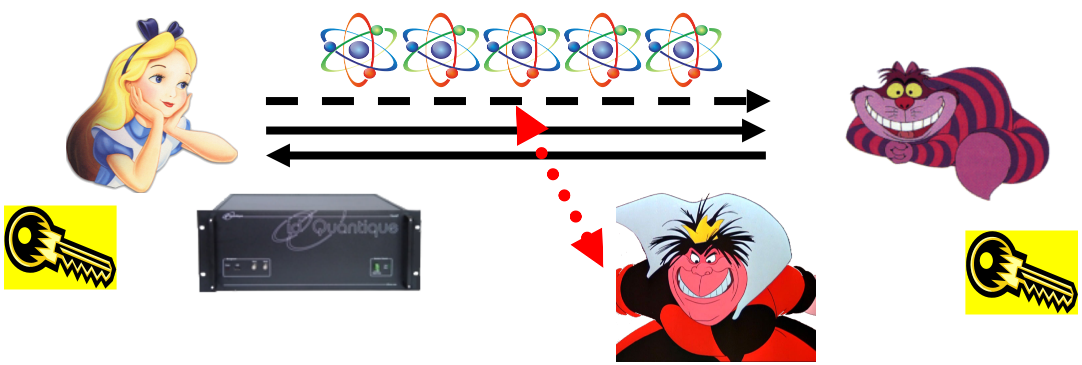
Thm: If x + y > z, then worry

Summary

✓ Quantum-safe crypto:

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

✓ Quantum Key Distribution, Quantum Cloud



CWI IN BEDRIJF
Technology for Tomorrow
18 mei 2017

Thank you for your attention!

Questions

Get in touch: schaffner@qusoft.org

QuSoft

CWI

NWO
Nederlandse Organisatie voor Wetenschappelijk Onderzoek