Post-quantum cryptography

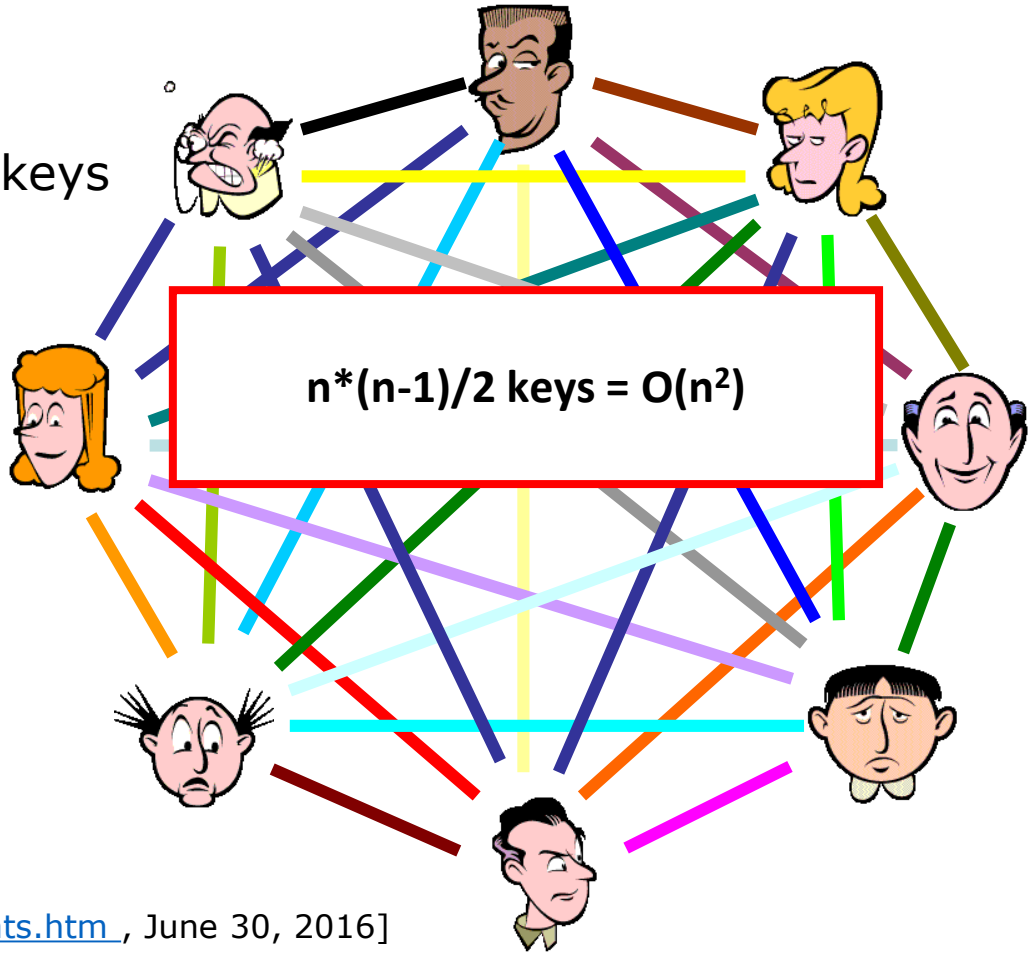
Andreas Hülsing, TU/e

Public-key cryptography (PKC)

The key exchange problem

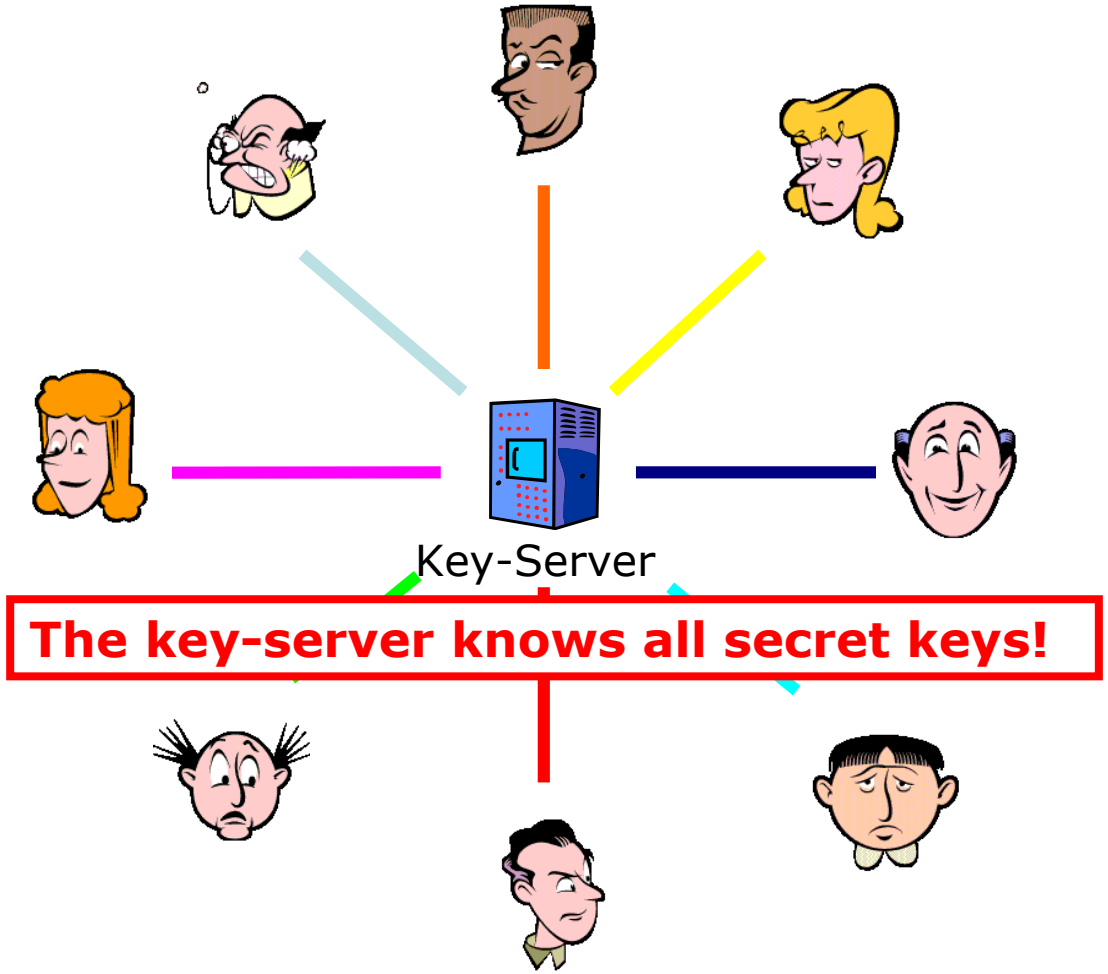
Internet: ~ **3,675,824,813** users

➔6,755,844,026,095,330,078 keys
≈6,8* $\mathbf{10^{18}}$ keys

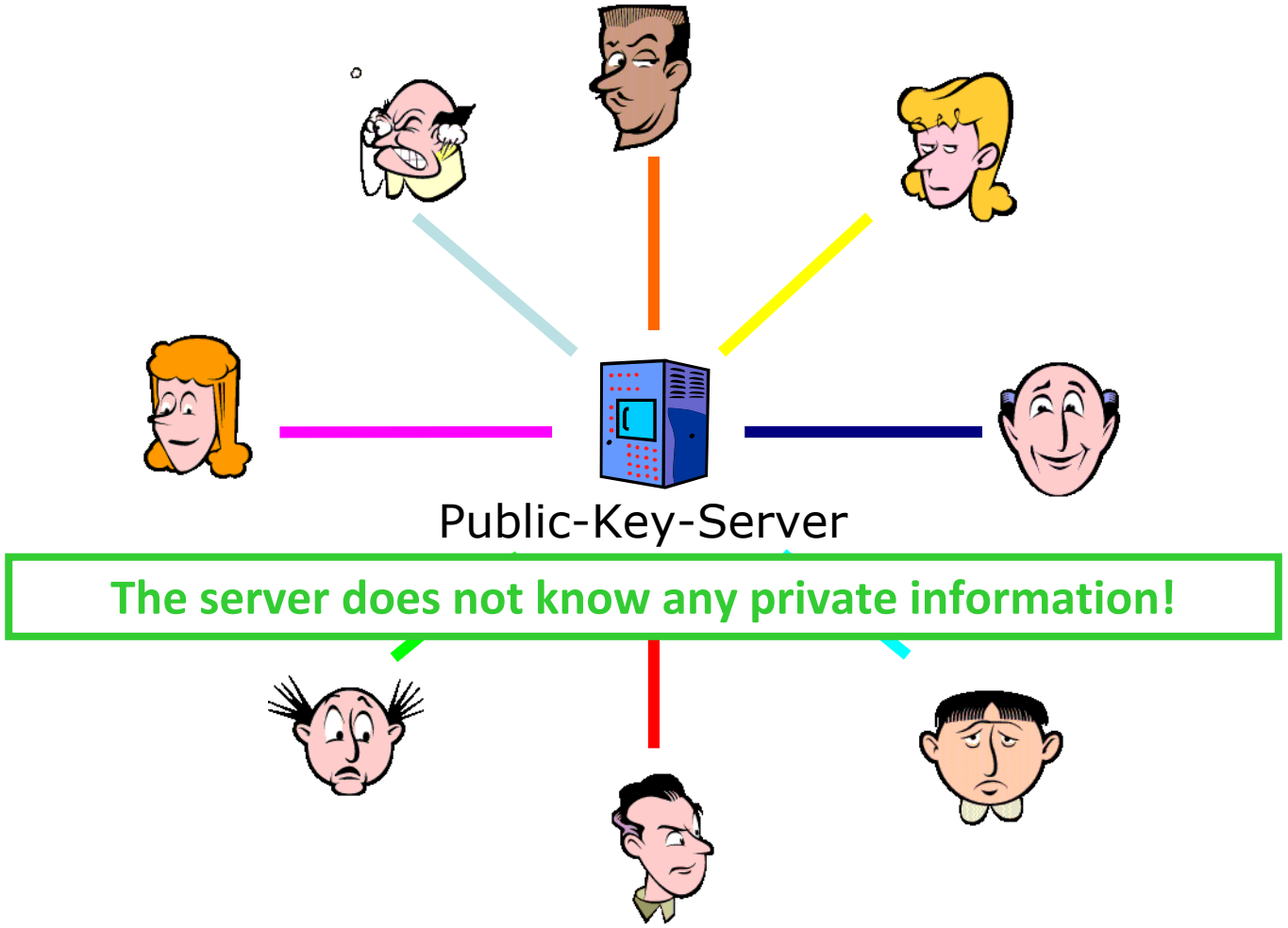


[From: http://www.internetworldstats.com/stats.htm , June 30, 2016]

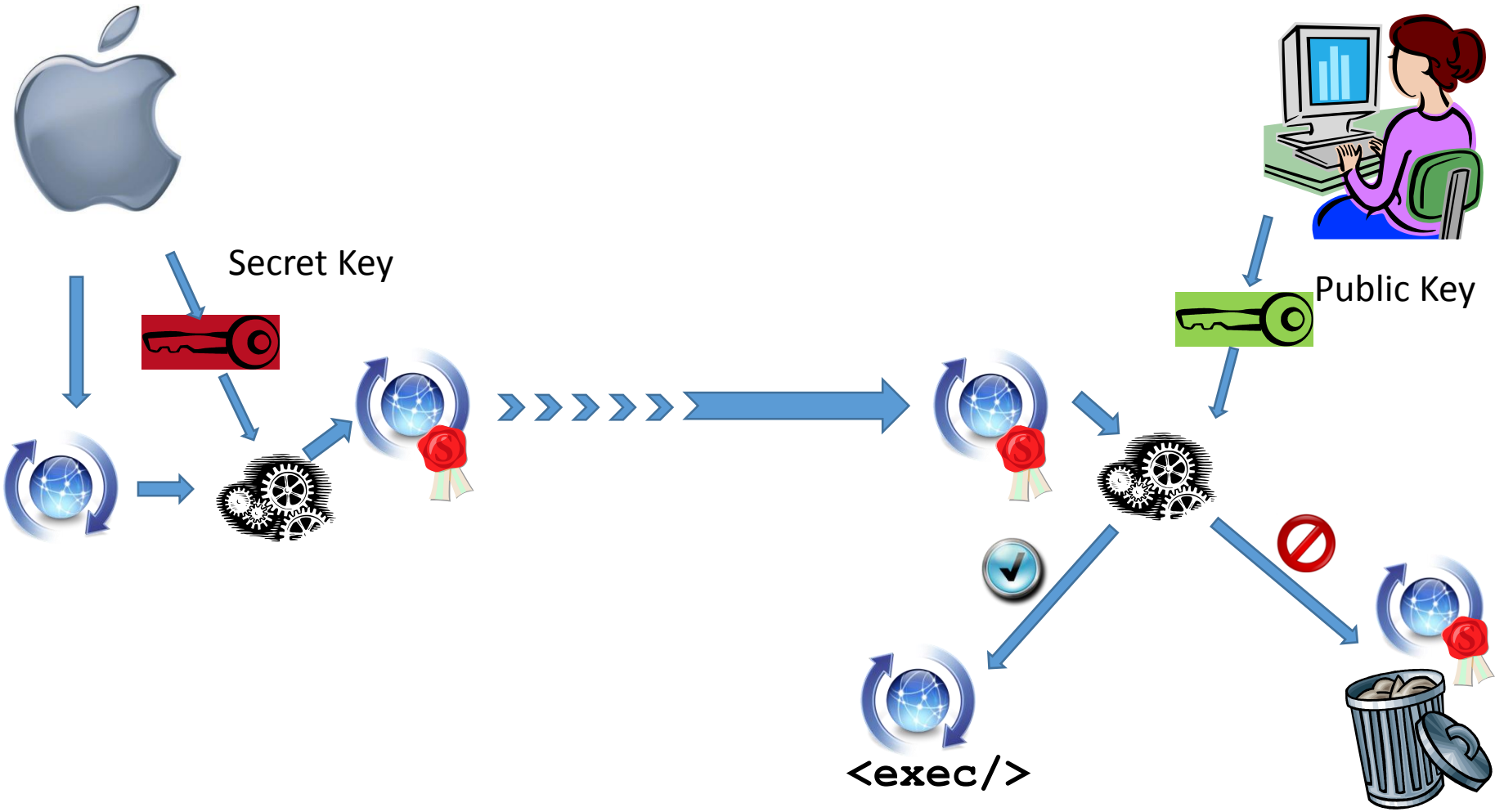
(Secret-)key server



Public key cryptography



Code signing



Code signing



Software distribution and update



Operating system updates


Mobile Code

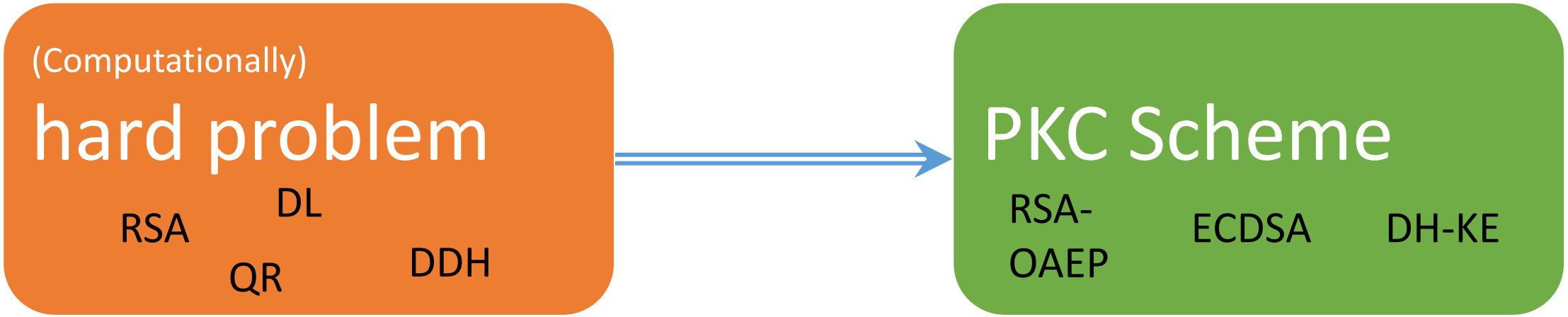
Microsoft Silverlight

Google play

Apps

Communication security

How to build PKC



We need symmetric and asymmetric crypto to achieve security!

Quantum computing

Quantum computing

"Quantum computing studies theoretical computation systems (quantum computers) that make direct use of quantum-mechanical phenomena, such as superposition and entanglement, to perform operations on data."

-- Wikipedia

Qubits

- Qubit state:

$$\alpha_0|0\rangle + \alpha_1|1\rangle$$

Computing with 0 and 1 at the same time!

with $\alpha_i \in \mathbb{C}$ such that $|\alpha_0|^2 + |\alpha_1|^2 = 1$

- Qubit can be in state $\frac{|0\rangle+|1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$

Quantum computers are not almighty

- To learn outcome one has to measure.
  - Collapses state
  - 1 qubit leads 1 classical bit of information
  - Randomized process
- Only invertible computation.
- Impossible to clone (copy) quantum state.

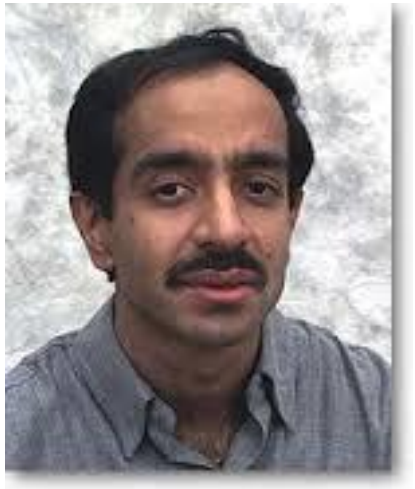
The quantum threat

Shor‘s algorithm (1994)

- Quantum computers can do FFT very efficiently
- Can be used to find period of a function
- **This can be exploited to factor efficiently (RSA)**
- **Shor also shows how to solve discrete log efficiently (DSA, DH, ECDSA, ECDH)**

Grover‘s algorithm (1996)

- Quantum computers can search N entry DB in $\Theta(\sqrt{N})$
- Application to symmetric crypto
- Nice: Grover is provably optimal (For random function)
- **Implication: Double security parameter.**



To sum up

- All asymmetric crypto is broken by QC
  - No more digital signatures
  - No more public key encryption
  - No more key exchange

- Symmetric crypto survives
  (with doubled key / digest size)
  - NOT ENOUGH!

Why care today?

Quantum computing

"Quantum computing studies theoretical computation systems (quantum computers) that make direct use of quantum-mechanical phenomena, such as superposition and entanglement, to perform operations on data."

-- Wikipedia

Bad news

I will not tell you when a quantum computer will be built!

nature
International weekly journal of science

NATURE | NEWS

Europe plans giant billion-euro quantum technologies project

Third European Union flagship will be similar in size and ambition to graphene and human brain initiatives.

Elizabeth Gibney

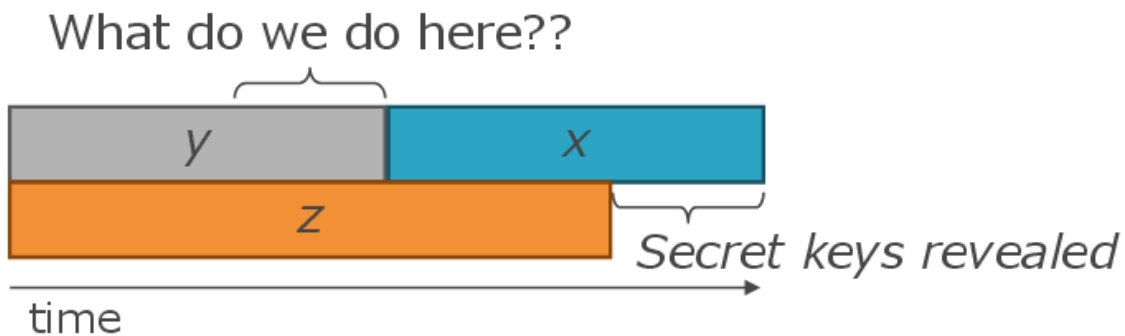
It‘s a question of risk assessment

How soon do we need to worry?

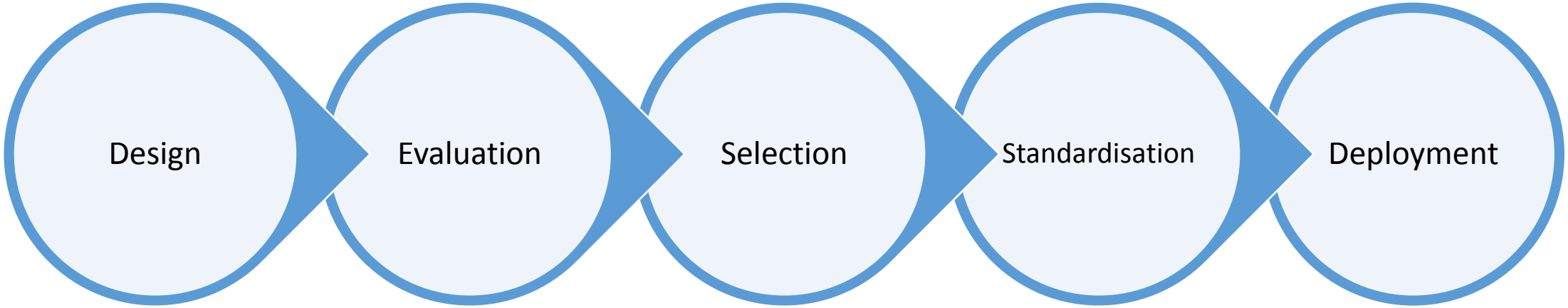
Depends on:

- How long do you need your keys to be secure? (*x* years)
- How much time will it take to re-tool the existing infrastructure with large-scale quantum-safe solution? (*y* years)
- How long will it take for a large-scale quantum computer to be built (or for any other relevant advance? (*z* years)

Theorem 1: If $x + y > z$, then worry.



Time to deployment



- Theoretical design

- Cryptanalysis
- PoC Implementations
- Practical Security Analysis (SCA)

- Competition (Broader evaluation)

- Commerical Implementation
- Integration & Certification
- Role-out

Example: SHA1 →SHA2

- 2005**:** First weakness
  - SHA2 already available! (Standardized)
- 2008: SHA2 availability in Windows (XP, Service pack 3)

- 2016: 2.6 % of TLS servers use certificates signed using XXX-SHA1 (https://www.trustworthyinternet.org/ssl-pulse/)

PQCRYPTO to the rescue

Initial recommendations

- **Symmetric encryption** Thoroughly analyzed, 256-bit keys:
  - AES-256
  - Salsa20 with a 256-bit key

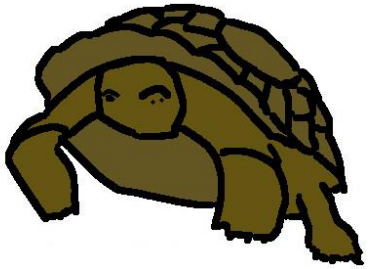
  Evaluating: Serpent-256, ...
- **Symmetric authentication** Informati… …etic MACs:
  - GCM using a 96-bit nonce and … …bit authenticator
  - Poly1305
- **Public-key encrypti…** …Eliece with binary Goppa codes:
  - length $n = …$, …mension $k = 5413$, $t = 119$ errors

  Evaluatin… …DPC, Stehlé-Steinfeld NTRU, ...
- **Pu… …y signatures** Hash-based (minimal assumptions):
  - XMSS with any of the parameters specified in CFRG draft
  - SPHINCS-256

  Evaluating: HFEv-, ...

Confidence inspiring solutions are slow, too big, ...

PQCRYPTO
ICT-645622



PQCrypto

„Official“ developments

- Feb `13: First PQC draft in **IRTF´s CFRG**
- Sep `13: **ETSI** holds first PQC WS (afterwards annually)
- April `15: **NIST** holds conference on PQC
- Aug `15: **NSA** announces transition to PQC
- Feb `16: NIST announces `PQC competition‘

Scheduled:

- Nov `16: NIST opens call for proposals
- 2024: „Draft standards ready“ (NIST, Feb `16)

PQCrypto 2017, June 26-28

- Conference location Utrecht,
  now looking for bigger venue ;-)
- **Dates:**
  - School: June 19-23,
  - Executive school: June 22-23,
  - Conference: June 26-28.
- AMS airport Schiphol is 30 min by train (4 $\times$ per hour)
- Other airports: Rotterdam, Eindhoven, Düsseldorf.
- Direct ICEs from FRA.
- School location will be Eindhoven.
  Travel time Eindhoven–Utrecht: 50 min.

Thank you!
Questions?