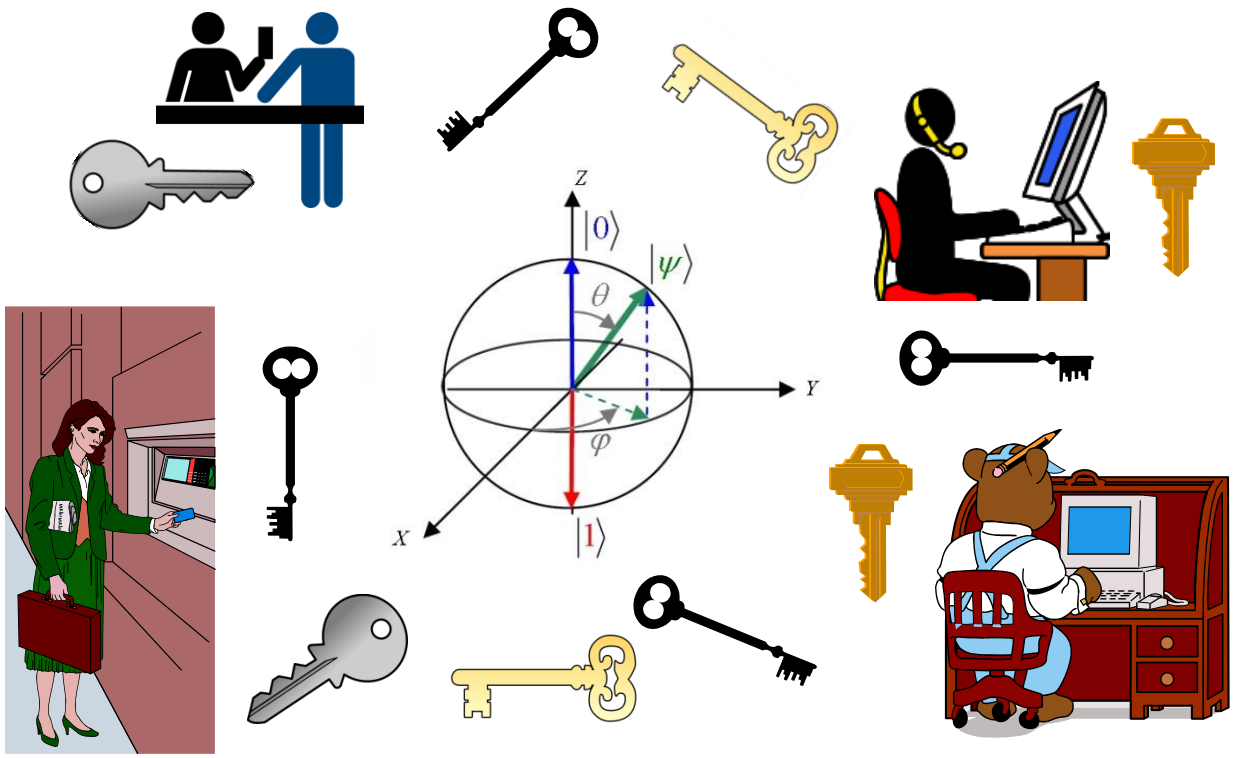
Post-Quantum Crypto Challenges



Prof. Audun Jøsang

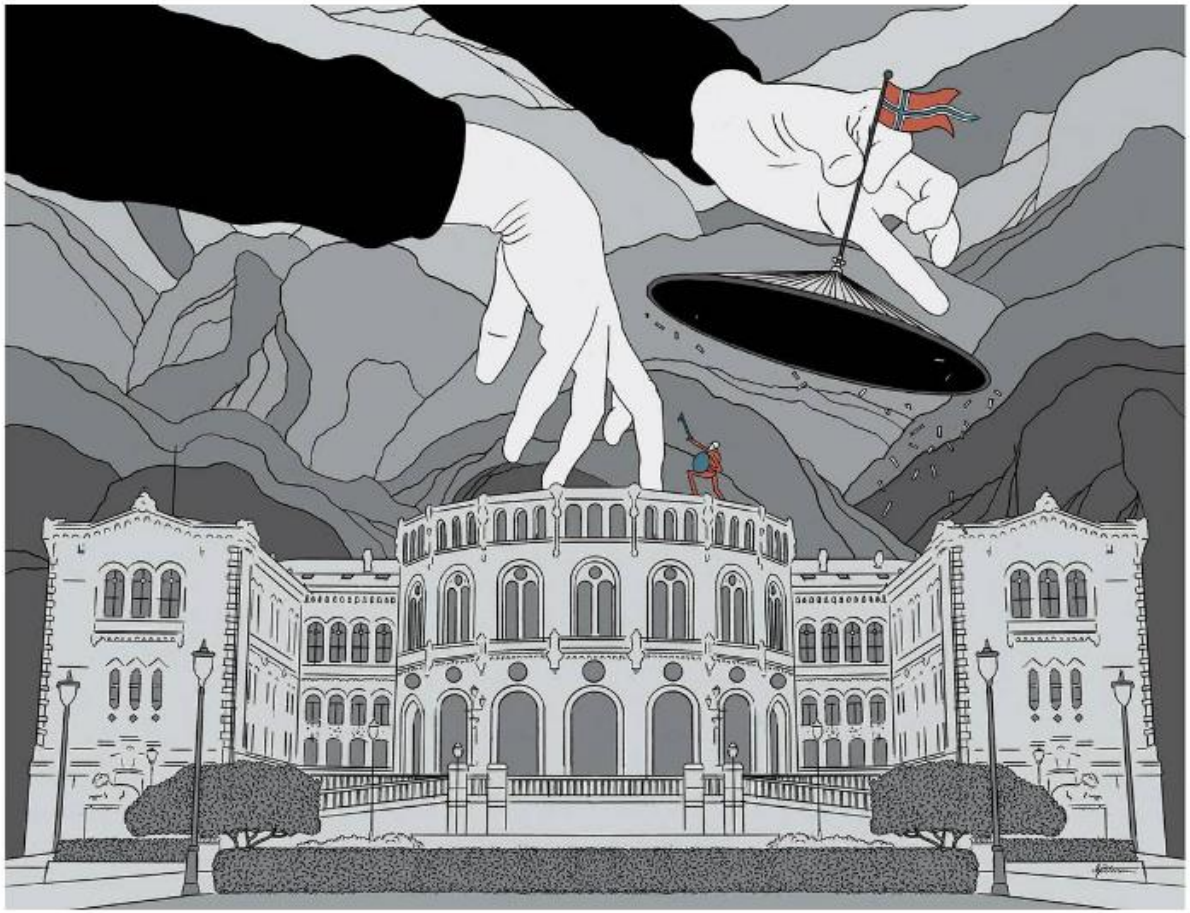
Universitetet i Oslo

SINET ≡ DN.no Logg inn Kunde

Norge kan snart ikke vokte statshemmeligheter lenger

TEKNOLOGI

TEKST Osman Kibar FØLG MEG
FOTO Åge Peterson, Gorm K. Gaare & Helge Skodvin
01 DESEMBER 2017 - KOLSÅS/OSLO



DN.no, 1 December 2017

https://www.aftenposten.no

Aftenposten A-magasinet Osloby Sport Meninger

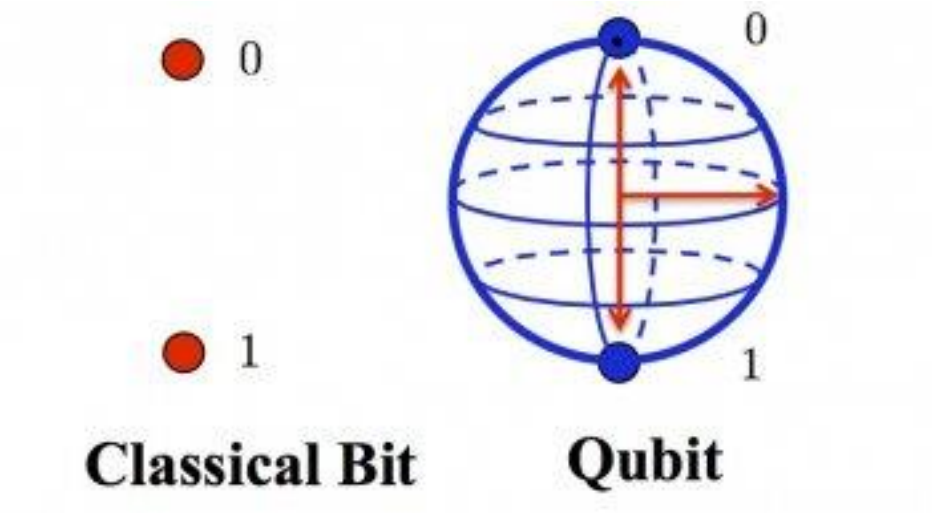
For abonnenter

Norges hemmeligheter skjules bak sterke krypteringer. Om få år vil kodene kanskje kunne knekkes.

Aftenposten.no, 10 May 2018

Principle for Quantum Computing

- Quantum Computing (QC) uses quantum superpositions instead of binary bits to perform computations.



- Quantum algorithms, i.e. algorithms for quantum computers, can solve certain problems much faster than classical algorithms.

Quantum Computers

QC Threat to Traditional Cryptography

- Shor's Quantum Algorithm (1994) can factor integers and compute discrete logarithms efficiently. It has also been extended to the crack ECC. Together, these attacks would be devastating to traditional public key crypto algorithms.

- Grover's Quantum Search Algorithm (1996) can be used to brute-force search for a *k*-bit secret key with an effort of only

$$\sqrt{2^k} = 2^{k/2}$$

which effectively doubles the required key sizes for ciphers.

- QC has been dismissed by most cryptographers until recent years. General purpose quantum computers do not currently exist, but are expected to be built in foreseeable future.

Cryptographic Security Services

Symmetric encryption

Confidentiality

Authentcity / Integrity

Hash-functions

Non-repudiation

PKI / Key distribution

Asymmetric encryption & digital signature (Traditional)

Confidentiality

Quantum Threat

Cryptographic Security Services

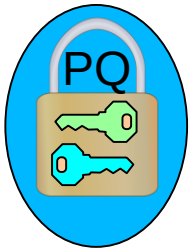
Symmetric encryption

Confidentiality

Authentcity / Integrity

Hash-functions

Non-repudiation
PKI / key distribution

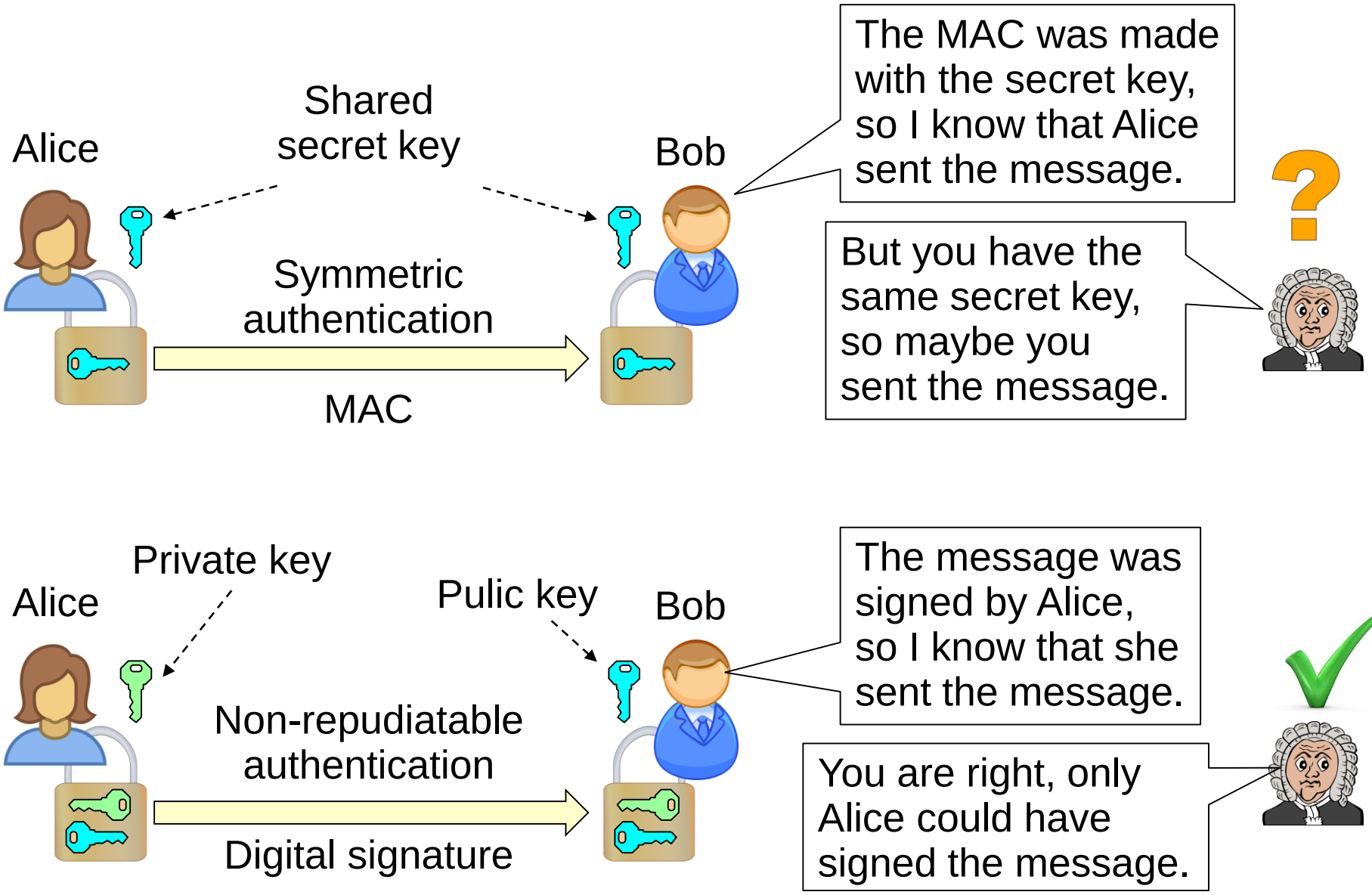


Asymmetric encryption & digital signature (Post-Quantum)

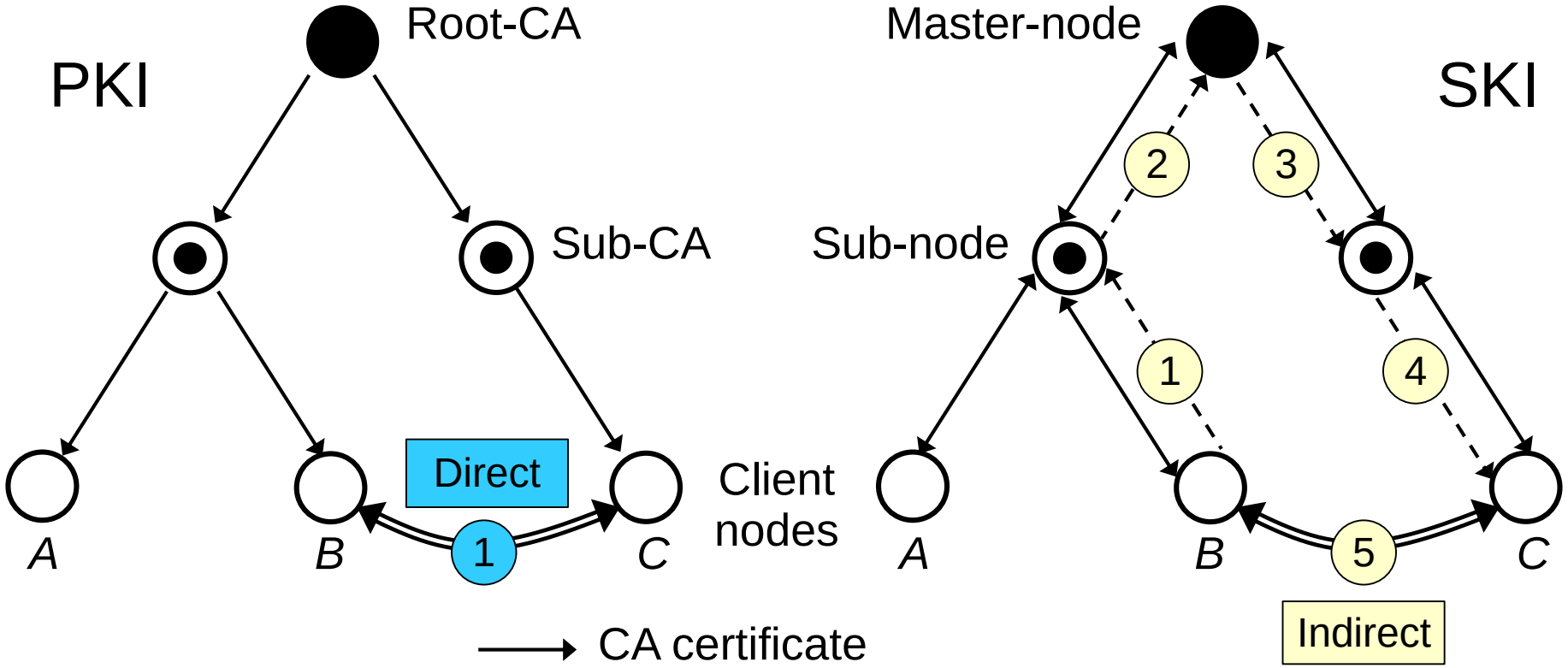
Confidentiality

PKIs can survive

Non-repudiation only possible with PKI



SKI (Symmetric Key Infrastructure) as alternative to PKI



Forklaring:

- CA certificate
- Pre-distributed shared secret keys
- Send encrypted secret session key
- Shared secret session key

Analogy between QC and Nuclear Fusion Research

- The New York Times, August 1975
  - "Major breakthrough in nuclear fusion research‘’
  - "Test reactor could be working as early as the mid-1980's."
  - "Commercial applications to become a reality a decade later.‘’
- The Guardian, March 2018
  - "Nuclear fusion on brink of being realised, say MIT scientists."
  - "Carbon-free fusion power could be 'on the grid in 15 years."

Analogy between SHA-1 and QC

- The threat of large-scale quantum computing is weakly analogous to the threat of a break-through in finding SHA-1 collisions.

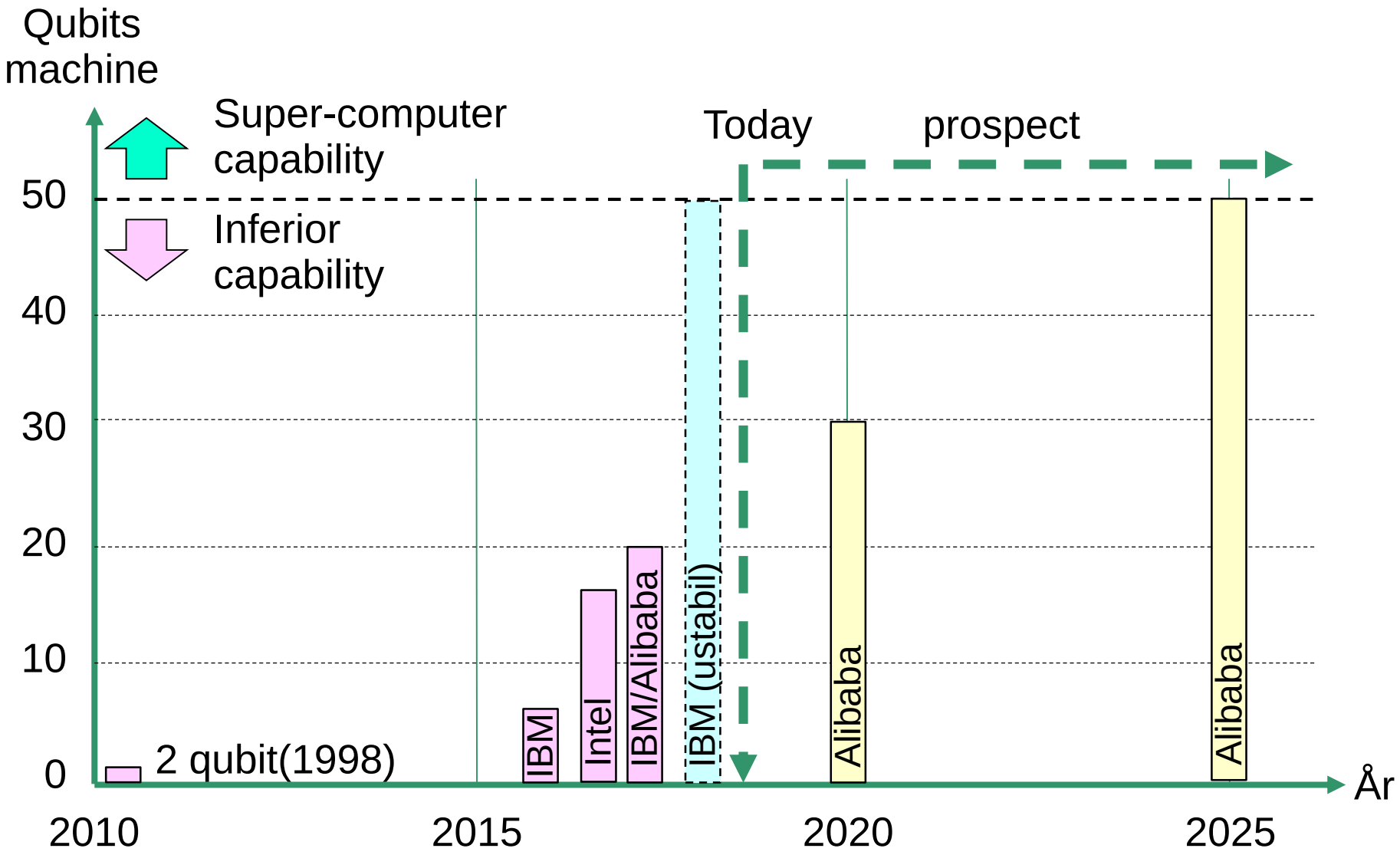
- Breakthrough in finding hash collisions was seen as imminent, but at the same time it was highly uncertain.
- Hard to quantify the risk that a breakthrough would happen, and hard to put time-frame on it.
- Substantial results would have significant impact on the industry.
- Resourceful researchers worked hard on it and received a lot of research funding.
- A breakthrough would bring fame and prestige to the researchers

Progress in Quantum Computing

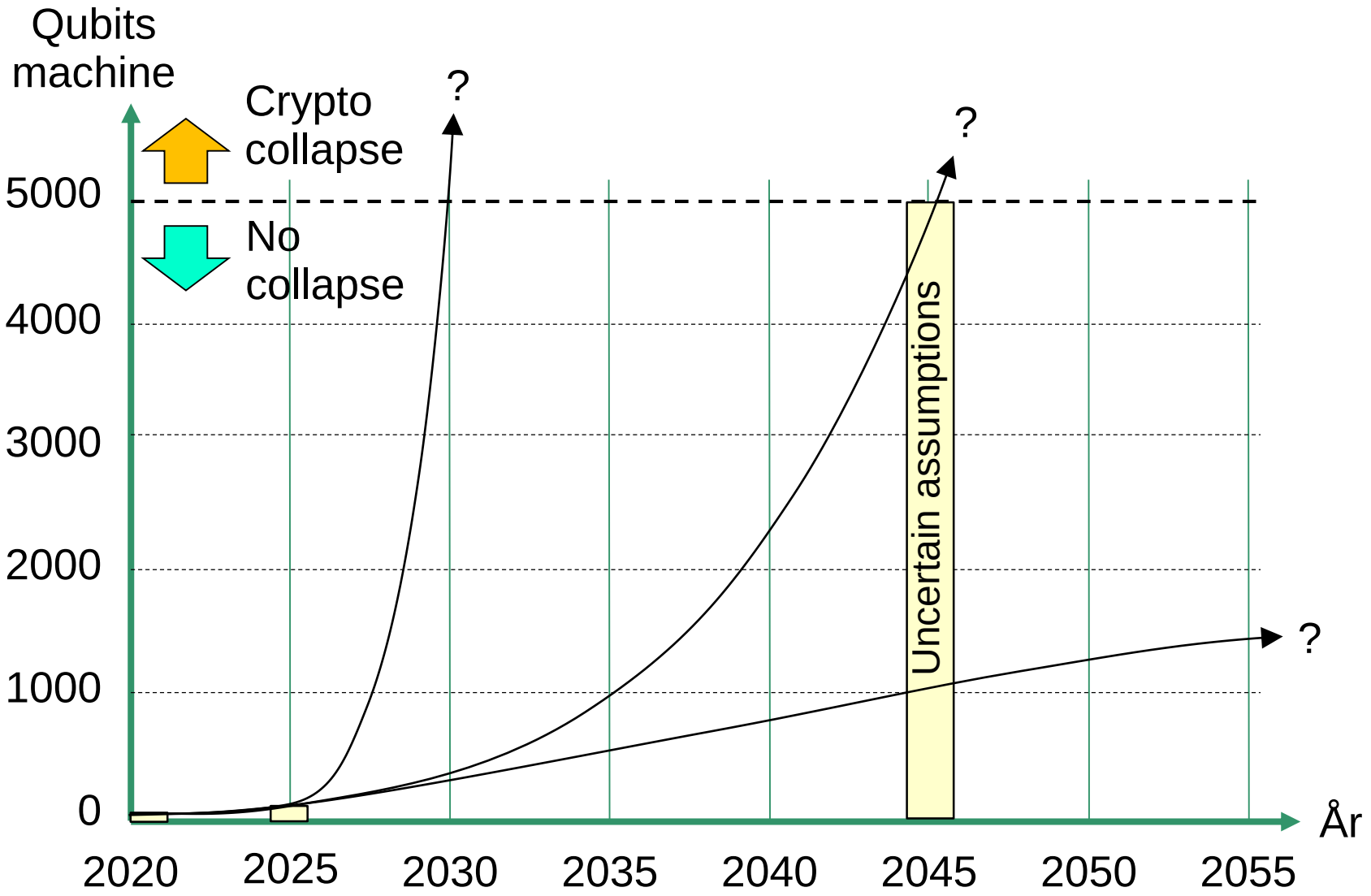
- Pre 1994: isolated contributions by Wiesner, Holevo, Bennett, etc.
- 1994: Shor's algorithm – breaks discrete log and factoring problems
- 1996: Grover's algorithm – quadratic speed-up for search problems,
- 1998: 2-qubit and 3-qubit NMR (Nuclear Magnetic Resonnance)
- 2000: 5-qubit and 7-qubit NMR. 2001: The number 15 is factored!
- 2005: qbyte announced (8 qubits?)
- 2006: 12 qubits.
- 2011: 14 qubits.
- 2012: The number 21 is factored!
- 2017: IBM unveils 20-qubit machine; Google, MSR doing cool stuff
- 2018: IBM and Alibaba announces 50-qubit machine (unstable)

- Billion dollar investment in quantum computing research globally
- Race towards "quantum supremacy"

Towards Quantum Supremacy

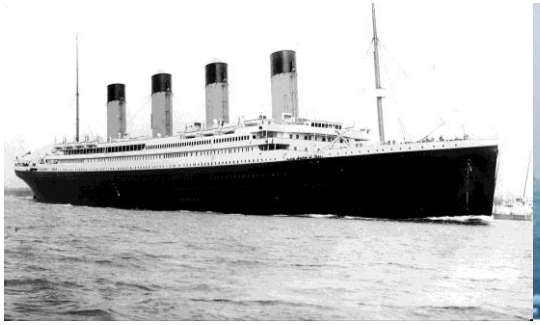


Towards Collapse of Asymmetric Crypto ?



A possible crypto collapse

- We don’t know if there will be a high scale QC breakthrough or not.
- If one comes, it would be fairly catastrophic – a Crypt-Apocalypse.
- Shor’s algorithm imperils all public key crypto deployed on the Internet today.
- ECC is likely to be broken sooner than RSA!
- Attackers can capture interesting DH exchanges now, break them later.
- We would expect some warning of impending disaster.
- But replacing crypto and PKI at scale takes time.
- And traffic captured now could be broken later, so it’s a problem today if you have data that needs to be kept secure for decades.



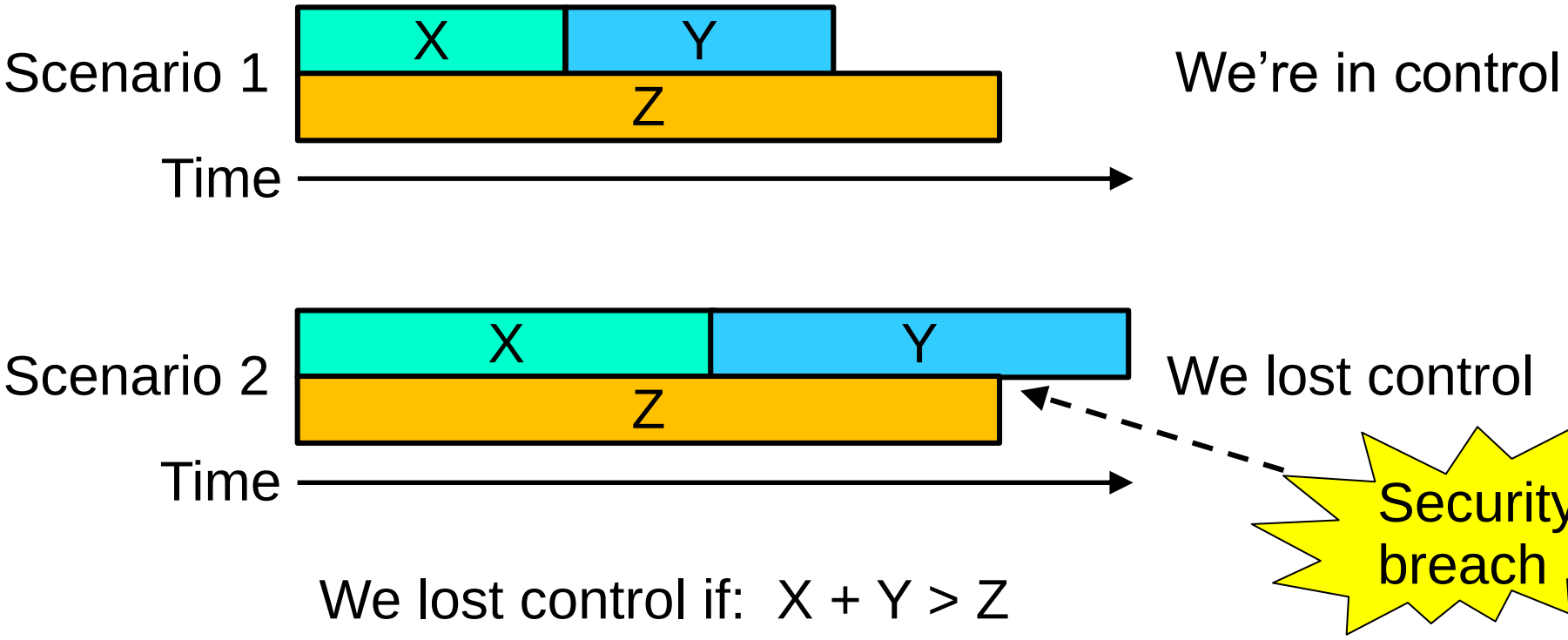
What should be our strategy?

Time Perspective on Quantum Threat

X: Time it takes to implement secure post-quantum crypto

Y: Required time that traditional crypto must remain secure

Z: Time it takes to develop a 5000-qubits quantum computer

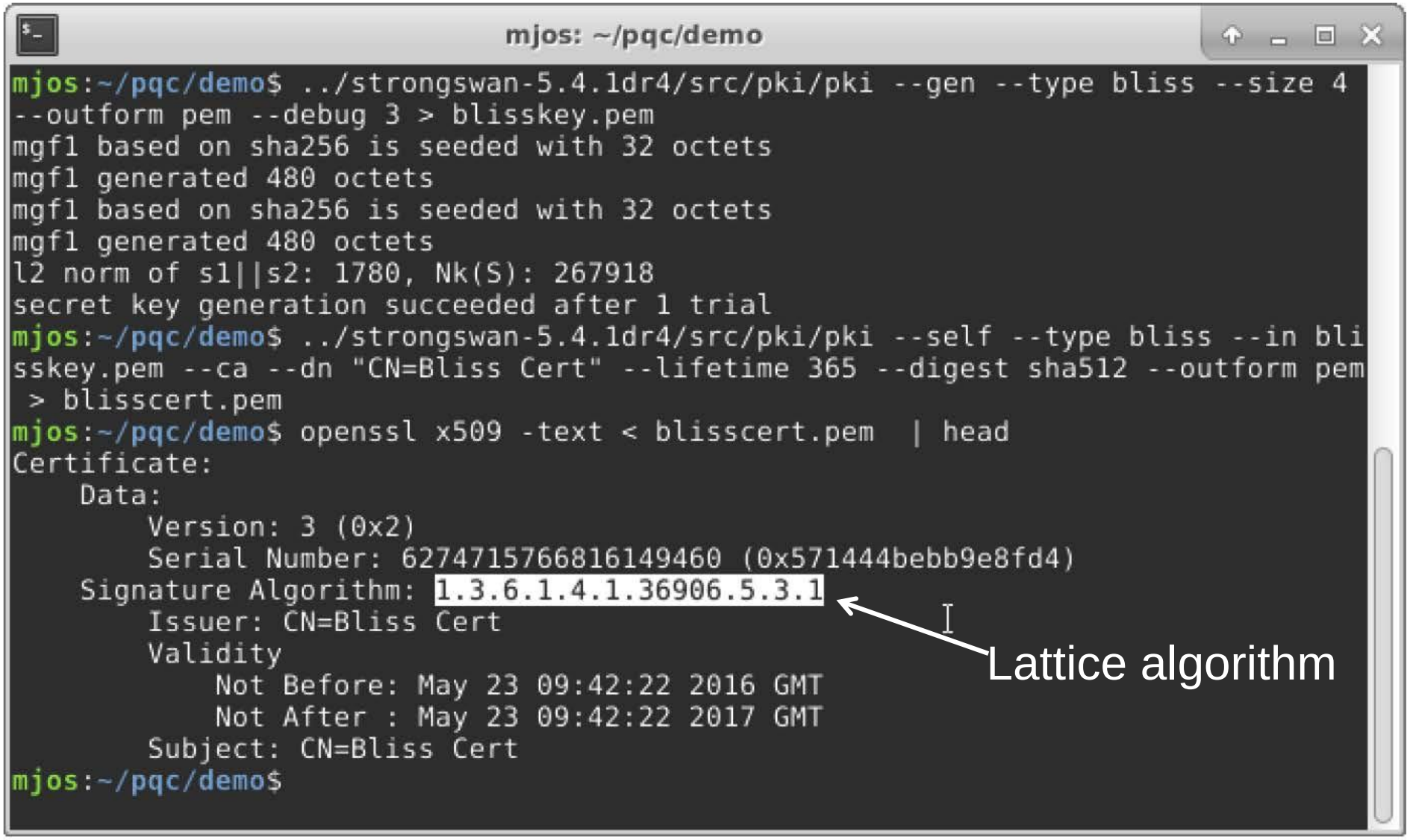


We lost control if: X + Y > Z

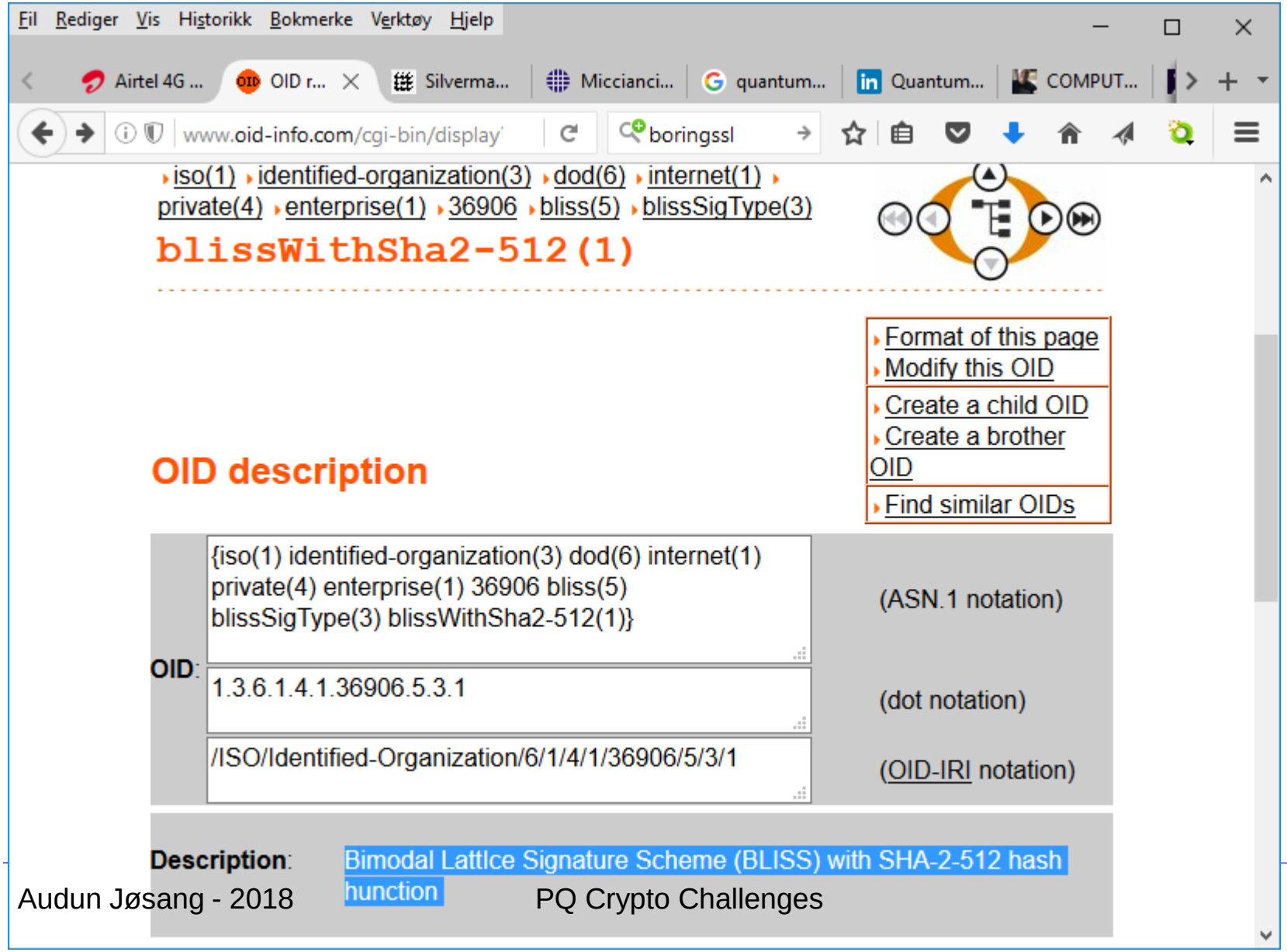
Full steam forward for PQC

- PQC (Post Quantum Cryptography) denotes public-key cryptosystems that resist attacks by known quantum algorithms.
- Main candidates are
  - Lattice-based cryptography based on lattice problems.
  - Code-based cryptography based on coding theory.
  - Multivariate polynomial cryptography based on solving systems of multivariate polynomials.
  - Hash-based signatures based on cryptographic hash functions
  - Others: There exist a variety of proposals based on various NP-hard problems
- These are possibly vulnerable to further advances in quantum algorithms.
- Even conventional security is not yet well understood in all cases.
- Notable exception: hash-based signatures schemes are particularly mature and well understood:
  - XMSS (eXtended Merkle Signature Scheme) (2011)
  - SPHINCS (2015)

StrongSwan OpenSSL with Lattice Algorithm



Lattice Algorithm in StrongSwan OpenSSL



BoringSSL: The Google fork of OpenSSL

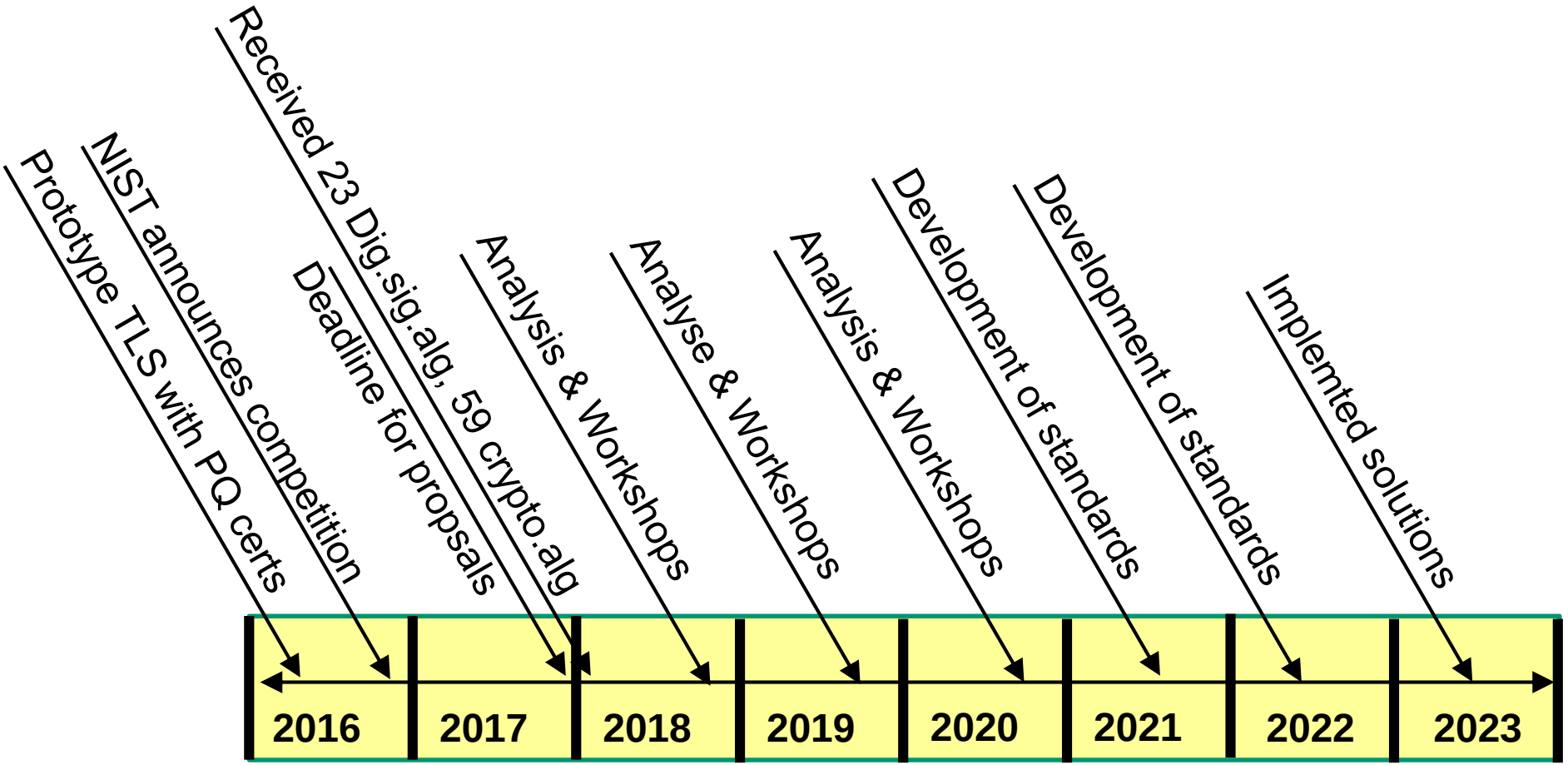
- BoringSSL provides a TLS stack for Google projects such as Android, Chrome Browser, Gmail, Google Search. It has been largely written from scratch.

- Latest development version implements key agreement with the New Hope lattice algorithm.

Call for Post-Quantum Crypto Algorithms

- 2016: NIST (US National Institute of Standards and Technology) called for *post-quantum* (quantum-resistant) cryptographic algorithms to become new public-key crypto standards
  - Digital signatures
  - Encryption/key-establishment
- NIST sees its role as managing a process of achieving community consensus in a transparent and timely manner
- No planned single “winner”, in contrast to AES and SHA3
  - Ideally, several algorithms will emerge as ‘good choices’
- Multiple algorithms will be promoted for standardization
  - Only algorithms received through the public call will be considered

Towards Standardized PQC



Difference with AES and SHA-3 Calls

- Standardising PQC algorithms is more complicated than standardising AES and SHA-3.,
  - No silver bullet - each candidate has some disadvantage
  - Currently not enough research on PQC algorithms to ensure adequate confidence in any existing schemes
- The aim is to standardise multiple PQC algorithms, not just one
- Unpredictable development in the research field
  - Focus may become more narrow at some point
  - Requirements/timeline could potentially change based on news developments in the field

PQC characteristics

- Current PQC schemes are generally not as performant as pre-quantum schemes.
- Typically larger public keys, larger key exchange messages/ciphertexts.
- Particularly challenging to deploy in low-power/wireless/IoT.
- Often faster cryptographic operations – just matrix multiplication plus noise in some cases.
- Performance may suffer even more as we refine our understanding of how to choose parameters for security.
- Better attacks implies larger parameters are needed.
- Or, eventually, abandonment of a particular approach.
- Parameter selection is a more complex question than for RSA/ECC.
  - Or: we are where we were for RSA in about 1982.

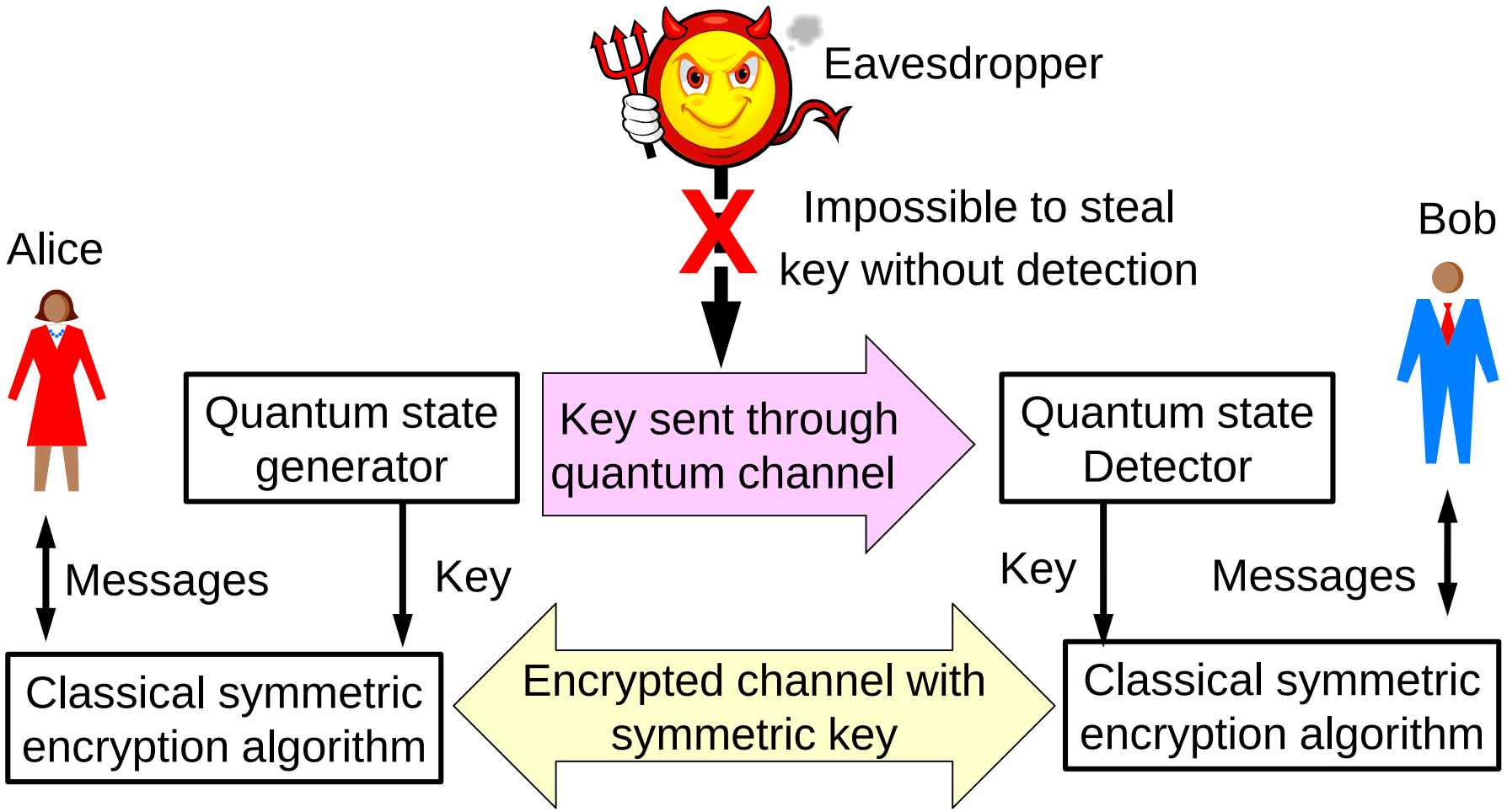
Standardisation of PQC

- Within IRTF (Internet Research Task Force) the working group CFRG (Crypto Forum Research Group) has worked on hash-based signatures.
  - Mature, well-understood area, less risky in security terms.
- Other PQ schemes are still not sufficiently studied and analsed.
- NIST's process is where the PQC action will be for the next 6 years.
- IETF should standardise only after NIST's process has run its course.
- Be ready to roll-over to new algorithms once they are standardised.
- Avoid building new systems with algorithm constraints, either explicitly or implicitly (e.g. via maximum key/field sizes).
- When designing protocols, be aware of key exchange flow characteristics and understand implications for protocol latency/round trips.
- Understand how to combine pre- and post-quantum elements to make hybrid schemes.
- Resist efforts to bypass the NIST and IETF process with ad-hoc solutions.

It takes time to build robust crypto

- Many stages of research from cryptographic design to deployment:
  - Explore space of cryptosystems.
  - Study attack models and identify points of vulnerability.
  - Propose fixes and improvements
  - Study implementations on real hardware.
  - Study side-channel attacks, fault attacks, etc.
  - Test that implementations meet performance requirements.
  - Integrate securely into real-world applications.
- Example: ECC introduced 1985; with significant advantages over RSA. Robust ECC started to take over the Internet in 2015.
- Risky to wait for quantum computers before starting to develop a solution!

Quantum Key Distribution



- Quantum key distribution is **not** a solution for PQ crypto

Quantum Key Distribution

GHz-rate prototype, H. Zbinden, University of Geneva.

QKD is NOT the Solution !

Summary

National Cyber Security Centre

a part of GCHQ

QKD:

- has fundamental practical limitations
- does not address large parts of the security problem
- is poorly understood in terms of potential attacks

By contrast, post-quantum public key cryptography appears to offer much more effective mitigations for real-world communications systems from the threat of future quantum computers.

While we're waiting for PQC

- Get an overview of critical affected systems
  - which use traditional asymmetric crypto
  - Which require long-term confidentiality
- Make impact assessment
  - Security risk
  - Privacy risk
- Identify systems where risk is unacceptable and assess measures to reduce risk
  - Alternative crypto solutions (eg SKI)
  - Ad-hoc PQ crypto (without standards and thorough analysis)
  - Change practice in business processes

Concern for Long-Term Confidetiality

- Today's encrypted communication is being stored by attackers and will be decrypted years later with quantum computers. Danger for human-rights workers, medical records, journalists, security research, legal proceedings, state secrets, . . .

Post-quantum RSA

Daniel J. Bernstein[1,2], Nadia Heninger[3], Paul Lou[3], and Luke Valenta[3]

[1] Department of Computer Science
University of Illinois at Chicago
Chicago, IL 60607–7045, USA
djb@cr.yp.to
[2] Department of Mathematics and Computer Science
Technische Universiteit Eindhoven
P.O. Box 513, 5600 MB Eindhoven, The Netherlands
[3] Computer and Information Science Department
University of Pennsylvania
Philadelphia, PA 19103, USA nadiah,plou,lukev@seas.upenn.edu

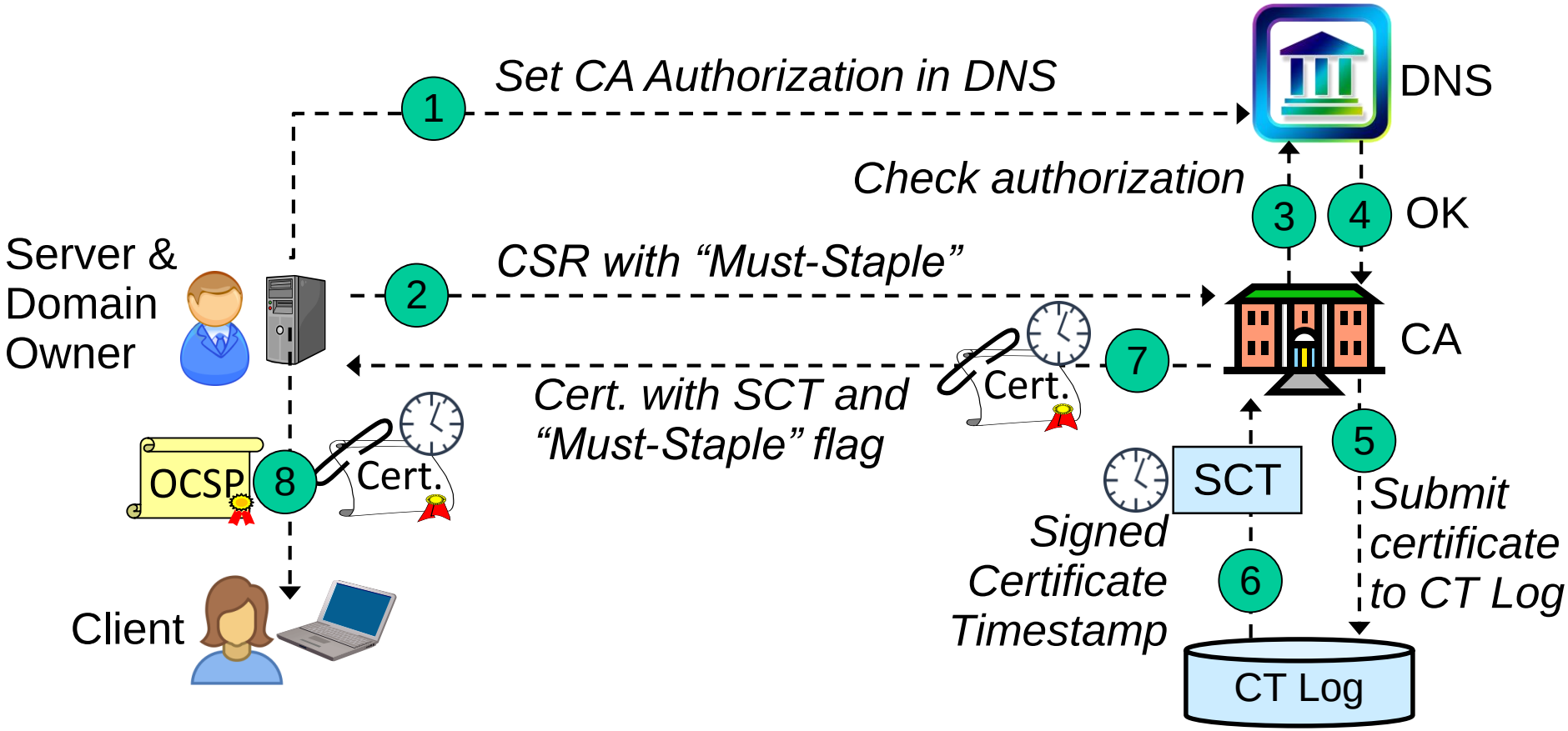
https://eprint.iacr.org/2017/351

Date: 2017.04.19

Post-Quantum RSA

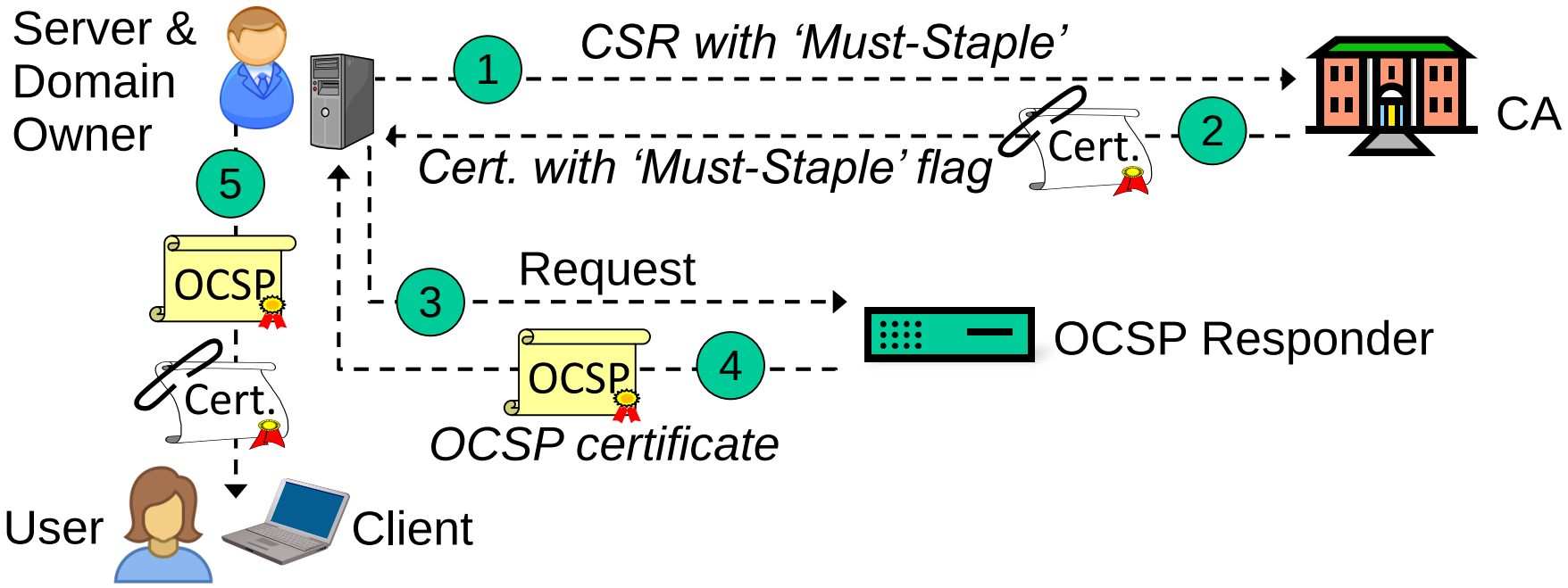
- Main idea: Use extremely large RSA parameters
- Modulus: 1 Terrabyte
- … consisting of 2^{31} 4096-bit primes
- 1 Terrabyte public key
- Relatively small private key
- Platform:
  - Ubuntu with 24 cores at 3:40 GHz
  - 3 terabytes of DRAM, 4.9 terabytes of swap memory
- Encryption time: 100 hours
- … cost in electricity: US$ 1
- Decryption: not completed (weeks to months)

Complexity of modern PKIs



- Enforcement of CA Authorization is by logging every certificate
- Client must reject certificates that have not been logged

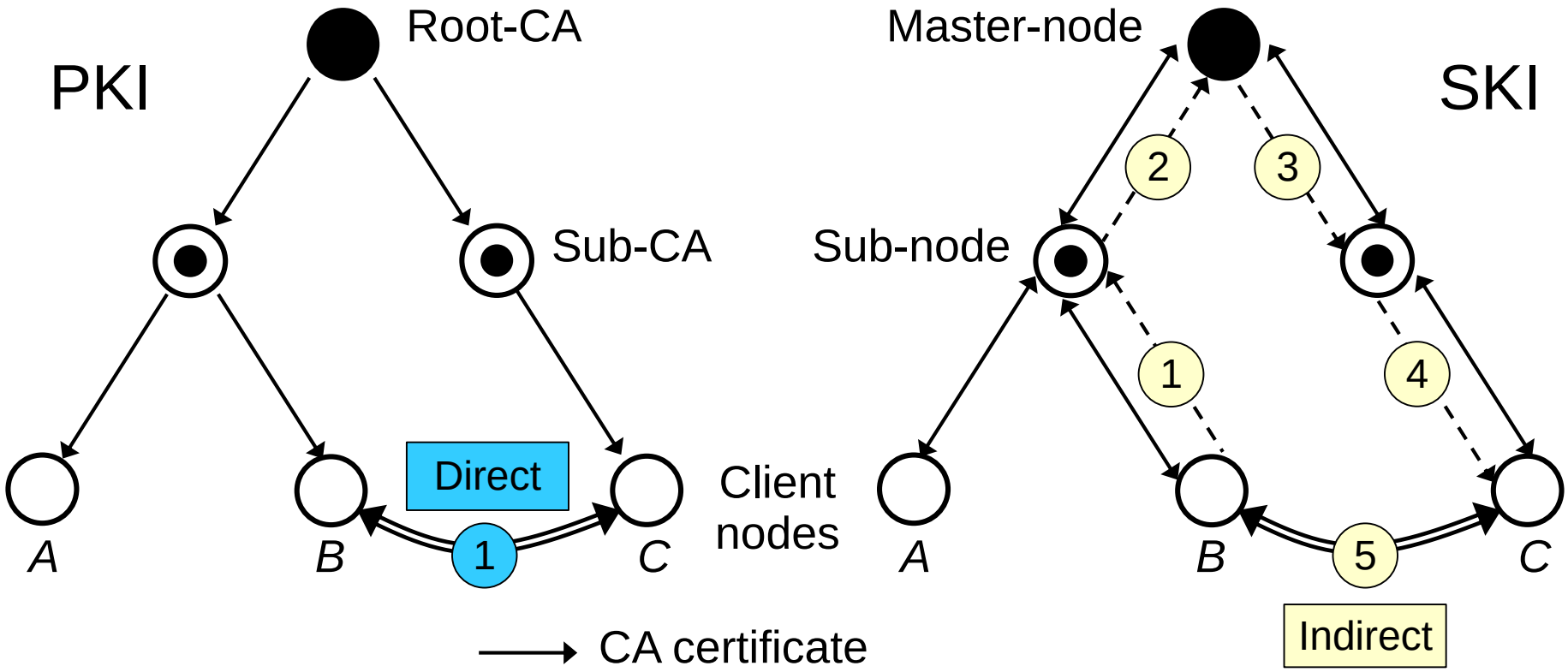
OCSP Must-Staple Protocol



OCSP-Must-Staple protocol necessary for certificate revocation

- CSR (Certificate Signature Request) with 'Must-Staple' flag
  - The 'Must-Staple' flag means that the server *must always* provide an OCSP certificate together with the server certificate

SKI (Symmetric Key Infrastructure) as alternative to PKI for confidentiality

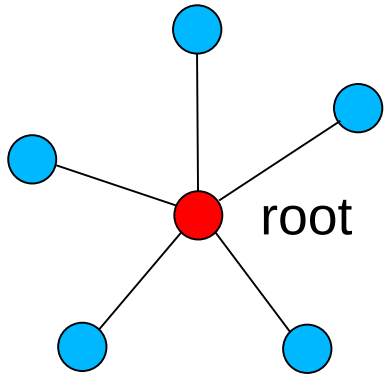


Forklaring:

- CA certificate
- Pre-distributed shared secret keys
- Send encrypted secret session key
- Shared secret session key

Key Distribution Complexity of PKI

- Asymmetric public keys with PKI:
  - 1 root public key distributed to n parties
  - linear growth
  - Scale if distribution problem reduces to N
  - **Authenticity** required,
  - … more difficult than we thought when PKI was invented in 1978



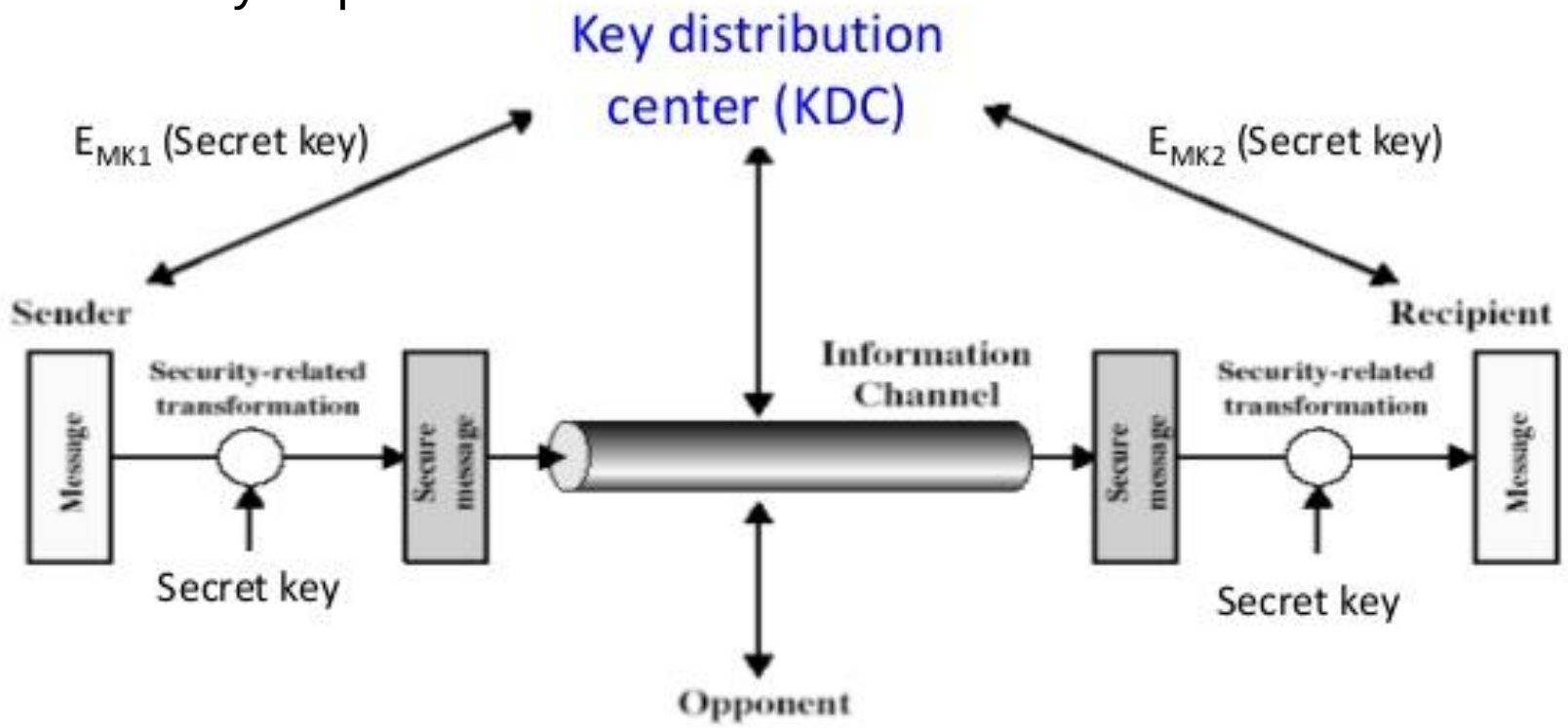
N nodes
N edges

Key distribution center (KDC)

KDC shares a unique key (master key) with each user to distribute secret key (session key) between a pair of users:

scale of key distribution problem reduces to N

Confidentiality required



Symmetric Key Infrastructures and Key DistributionCenters

- Security systems using KDCs include **Kerberos**.
- This structure has some challenges
  1. Single KDC Trusted by all.
  2. Key distribution between KDC and clients
  3. It should have all user information
  4. Scalability issues, recovery, registration
  5. KDC has to be online, which can cause bottle neck as all clients must first connect to it to get the session key.

Concluding Remarks

- The Crypt-Apocalypse might be coming… or it might not be.
- PQC could be a massive misdirection and misconception, designed to distract cryptographers from things that really matter… or it might not be.
- We can hope that the NIST process will proceed in an orderly fashion and produce a sensible and conservative portfolio of options for PQC.
- IETF standardization necessary to make the transition as smooth as possible.

- My personal opinion:
  - Reconsider KDCs and Symmetric Key Infrastructures for confidentiality
  - Use hash-based signatures for non-repudiation