POST-QUANTUM CRYPTOGRAPHY

VIENNA CYBER SECURITY WEEK 2018

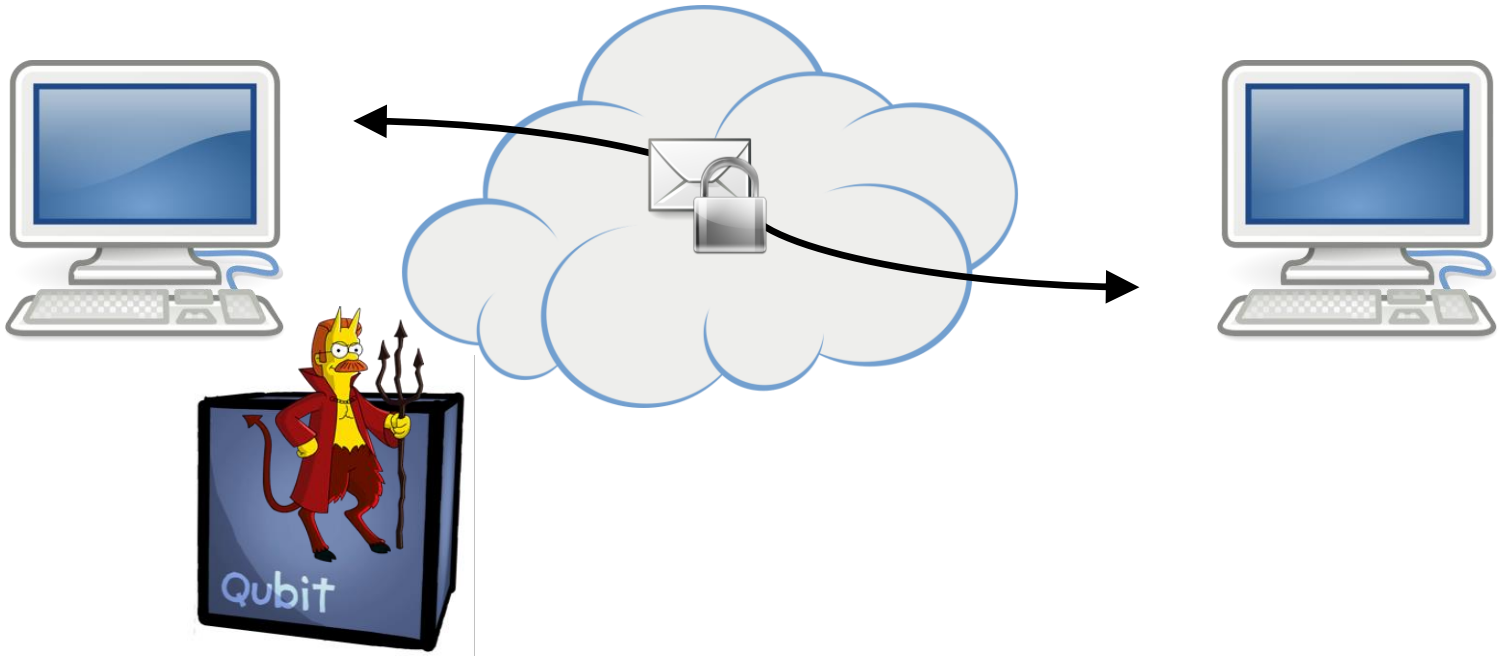
02.02.2018

DR. DANIEL SLAMANIG

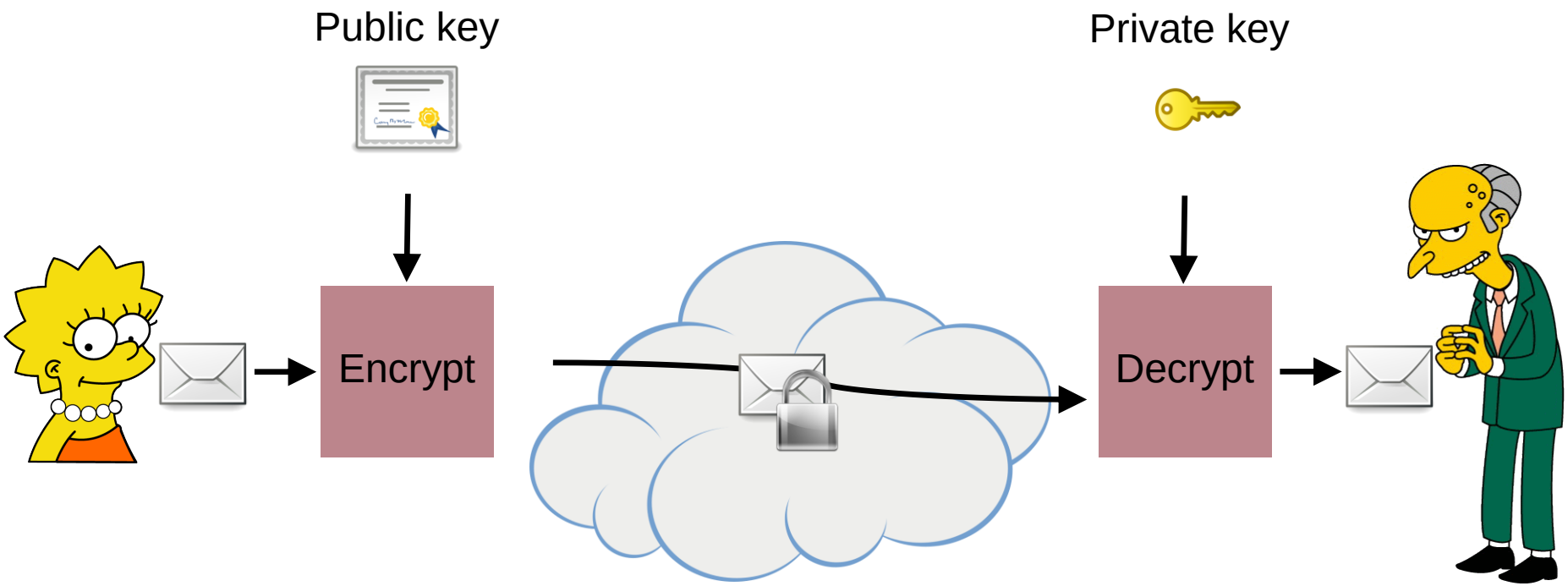
WHAT IS POST-QUANTUM CRYPTOGRAPHY?

- Also called **quantum safe/resistant cryptography**
  - **NOT quantum cryptography (= quantum key distribution (QKD), etc.)**

- Cryptosystems which run on classical computers, and are considered to be resistant to quantum attacks (no known exponentional quantum speedup)
  - (Public key) encryption schemes, signature schemes, Key-establishment (like DH), etc.

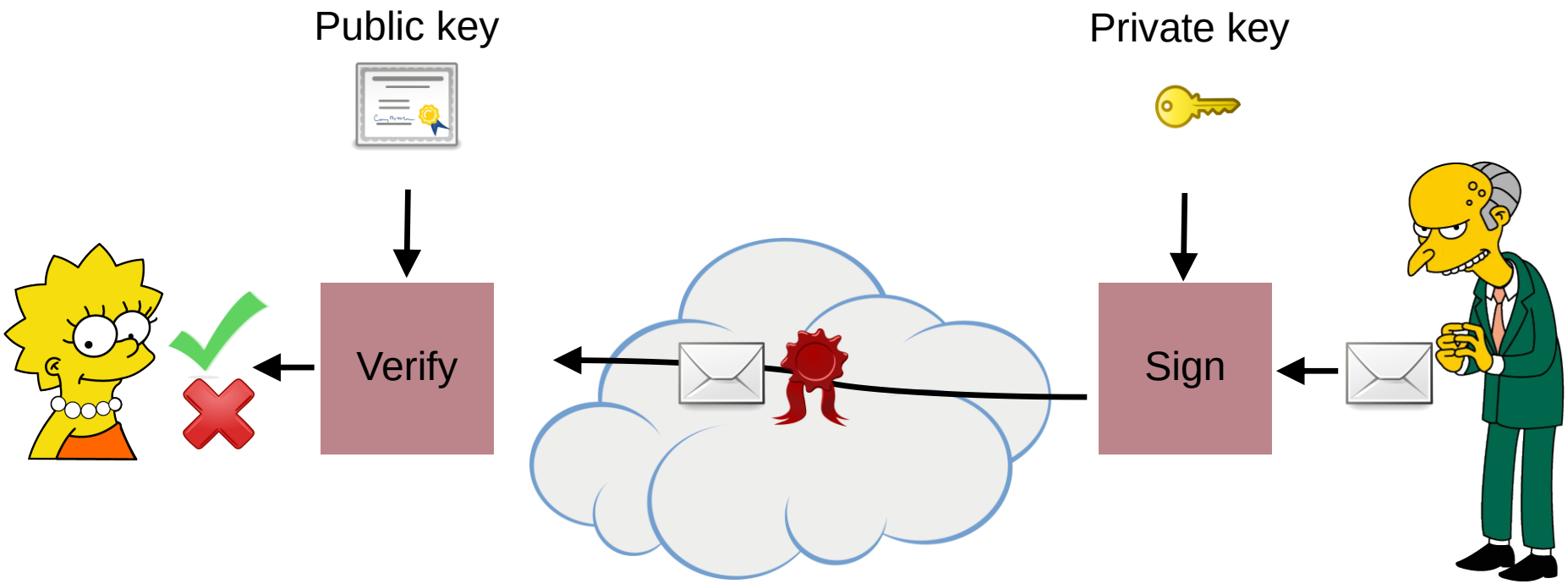


CRYPTOGRAPHY 101: PUBLIC KEY ENCRYPTION*



* = Asymmetric encryption

CRYPTOGRAPHY 101: DIGITAL SIGNATURES



MOTIVATION

Why post-quantum cryptography?

Workshops and Timeline - Post-Quantum Cryptography | CSRC - Mozilla Firefox

Workshops and Timeline - P

https://csrc.nist.gov/projects/post-quantum-cryptography/workshops-and-timeline

NIST

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

PROJECTS | POST-QUANTUM CRYPTOGRAPHY

Post-Quantum Cryptography

Workshops and Timeline

Workshops

April 12-13, 2018 - First PQC Standardization Conference, co-located with PQCrypto 2018

Pier Sixty-Six Hotel and Marina
Fort Lauderdale, FL

Call for Proposals - Submission deadline **November 30, 2017**

April 2-3, 2015 - Workshop on Cybersecurity in a Post-Quantum World NIST, Gaithersburg, MD

Workshops and Timeline - Post-Quantum Cryptography | CSRC - Mozilla Firefox

Workshops and Timeline - P

https://csrc.nist.gov/projects/post-quantum-cryptography/workshops-and-timeline

csrc.nist.gov
Secure Connection

Permissions
You have not granted this site any special permissions.

E CENTER

PROJECTS | POST-QUANTUM CRYPTOGRAPHY

Post-Quantum Cryptography

Workshops and Timeline

Workshops

April 12-13, 2018 - First PQC Standardization Conference, co-located with PQCrypto 2018

Pier Sixty-Six Hotel and Marina
Fort Lauderdale, FL

Call for Proposals - Submission deadline **November 30, 2017**

April 2-3, 2015 - Workshop on Cybersecurity in a Post-Quantum World NIST, Gaithersburg, MD

Workshops and Timeline - Post-Quantum Cryptography | CSRC - Mozilla Firefox

Workshops and Timeline - P

https://csrc.nist.gov/projects/post-quantum-cryptography/workshops-and-timeline

csrc.nist.gov
Secure Connection

Permissions
You have not gran
permissions.

Page Info - https://csrc.nist.gov/projects/post-quantum-cryptography/workshops-a

General | Media | Permissions | Security

Website Identity

Website: **csrc.nist.gov**
Owner: **This website does not supply ownership information.**
Verified by: **Symantec Corporation**
Expires on: **April 2, 2018**

View Certificate

Privacy & History

Have I visited this website prior to today? **No**
Is this website storing information (cookies) on my computer? **Yes** View Cookies
Have I saved any passwords for this website? **No** View Saved Passwords

Technical Details

Connection Encrypted (TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA, 256 bit keys, TLS 1.2)
The page you are viewing was encrypted before being transmitted over the Internet.
Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

Help

PROJECTS

Post-Qu

Workshop

Workshops

April 12-13, 2018 - F

Pier Sixty-Six H
Fort Lauderdal

Call for Propos

April 2-3, 2015 - Workshop on Cybersecurity in a Post-Quantum World NIST, Gaithersburg, MD

Workshops and Timeline - Post-Quantum Cryptography | CSRC - Mozilla Firefox

Workshops and Timeline - P

https://csrc.nist.gov/projects/post-quantum-cryptography/workshops-and-timeline

Certificate Viewer: "NVD.nist.gov"

General Details

Certificate Hierarchy

- VeriSign Class 3 Public Primary Certification Authority - G5
  - Symantec Class 3 Secure Server CA - G4
    - NVD.nist.gov

Certificate Fields

- Subject
- Subject Public Key Info
  - Subject Public Key Algorithm
  - Subject's Public Key
- Extensions
  - Certificate Subject Alt Name
  - Certificate Basic Constraints
  - Certificate Key Usage
  - Extended Key Usage
  - Certificate Policies
  - Certificate Authority Key Identifier

Field Value

PKCS #1 RSA Encryption

Export...

Close

Page Info - https://csrc.nist.gov/projects/post-quantum-cryptography/workshops-a

Media | Permissions | Security

ntity

csrc.nist.gov

This website does not supply ownership information.

y: Symantec Corporation

n: April 2, 2018

View Certificate

story

ted this website prior to today? No

osite storing information (cookies) nputer? Yes — View Cookies

ed any passwords for this website? No — View Saved Passwords

Technical Details

Connection Encrypted (TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA, 256 bit keys, TLS 1.2)

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

Help

Workshops

April 12-13, 2018 - F

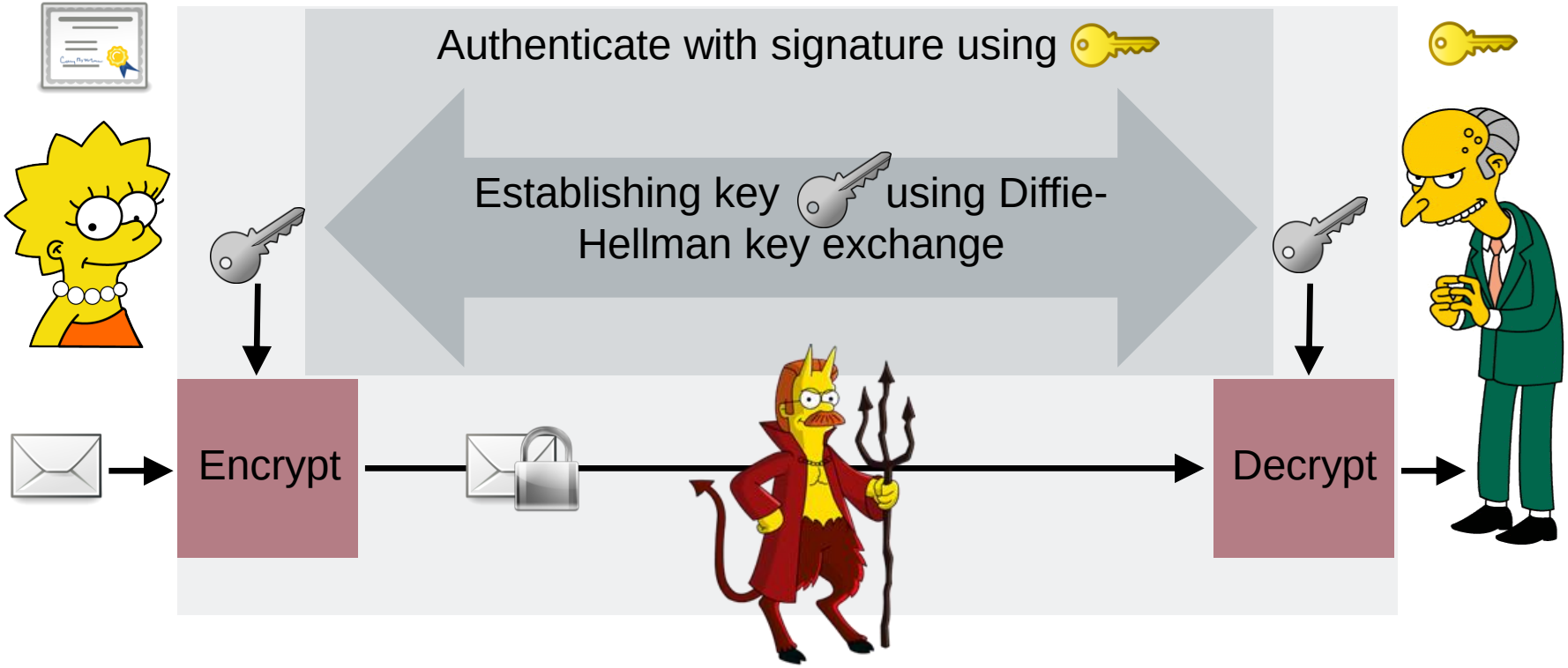
Pier Sixty-Six H

Fort Lauderdal

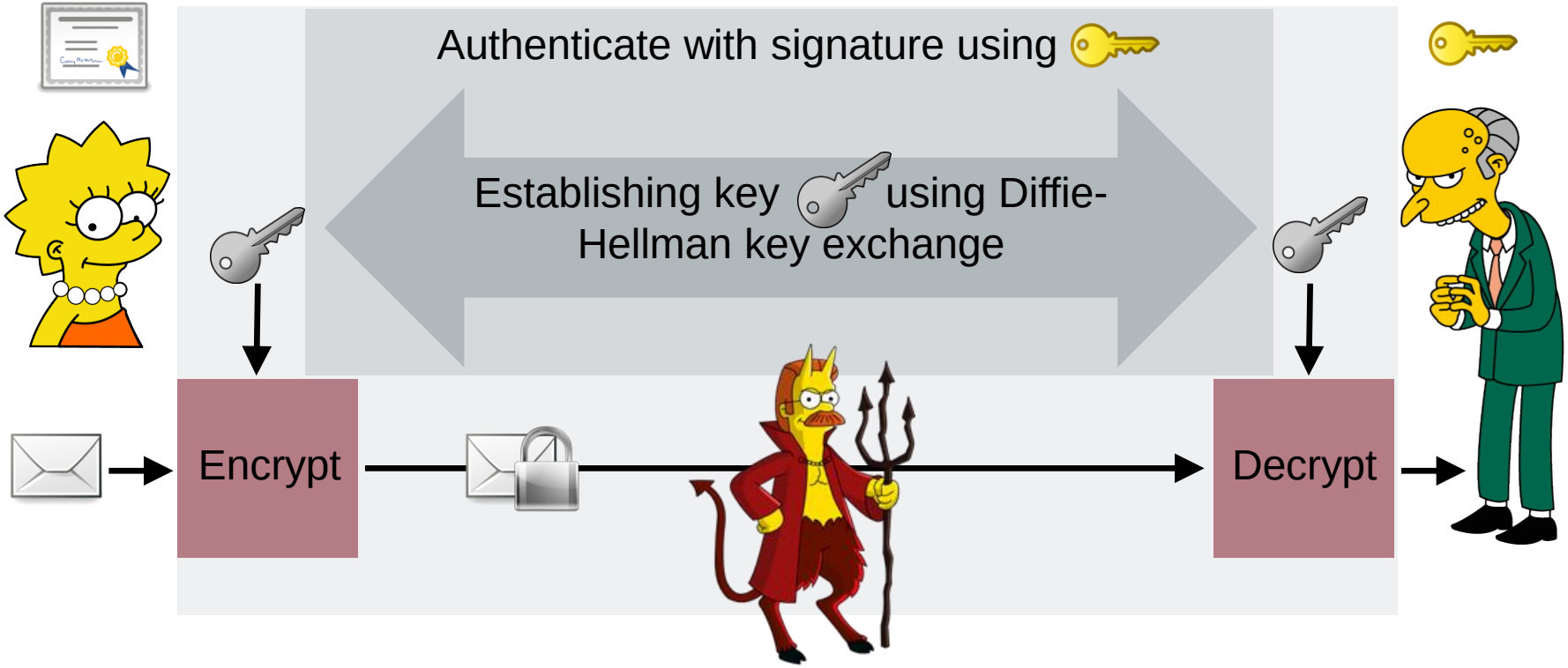
Call for Propos

April 2-3, 2015 - Workshop on Cybersecurity in a Post-Quantum World NIST, Gaithersburg, MD

AUTHENTICATED KEY EXCHANGE AND SYMMETRIC ENCRYPTION

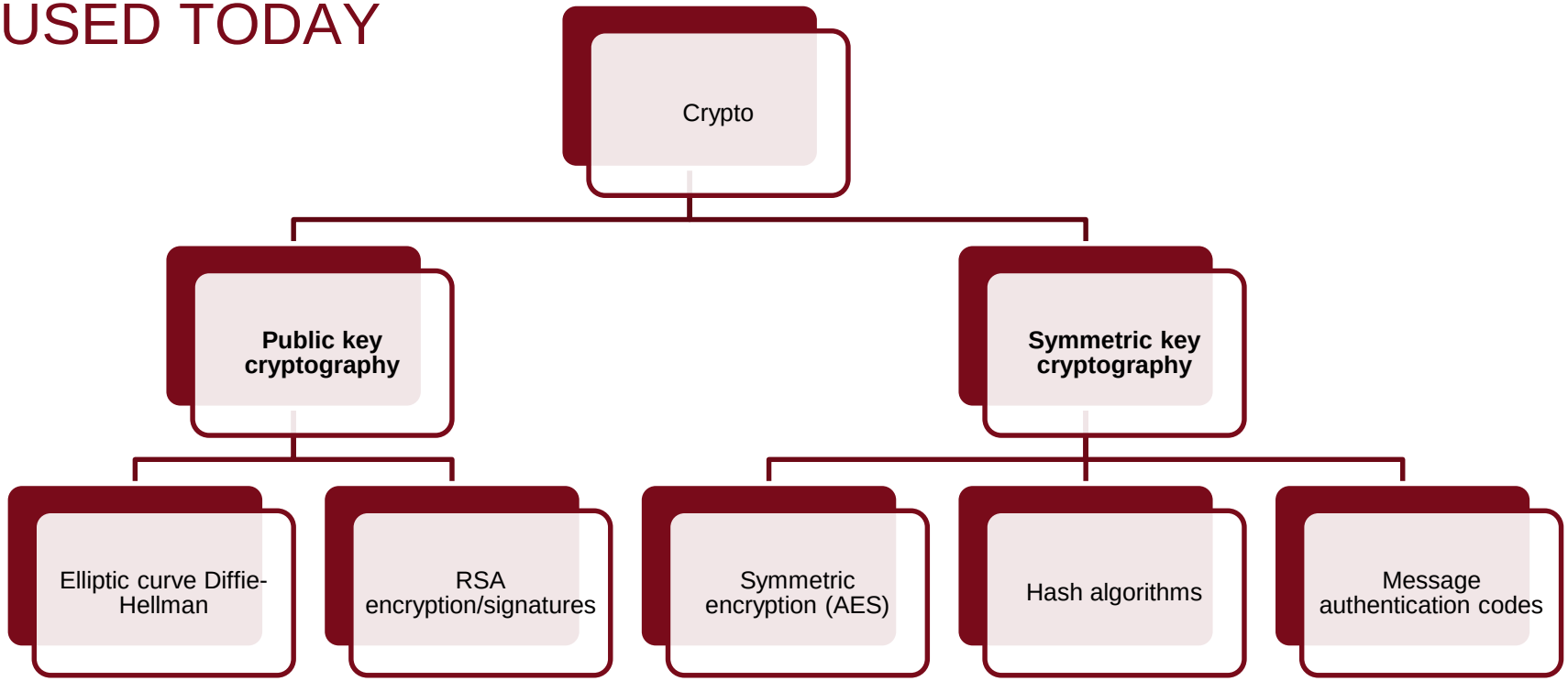


AUTHENTICATED KEY EXCHANGE AND SYMMETRIC ENCRYPTION

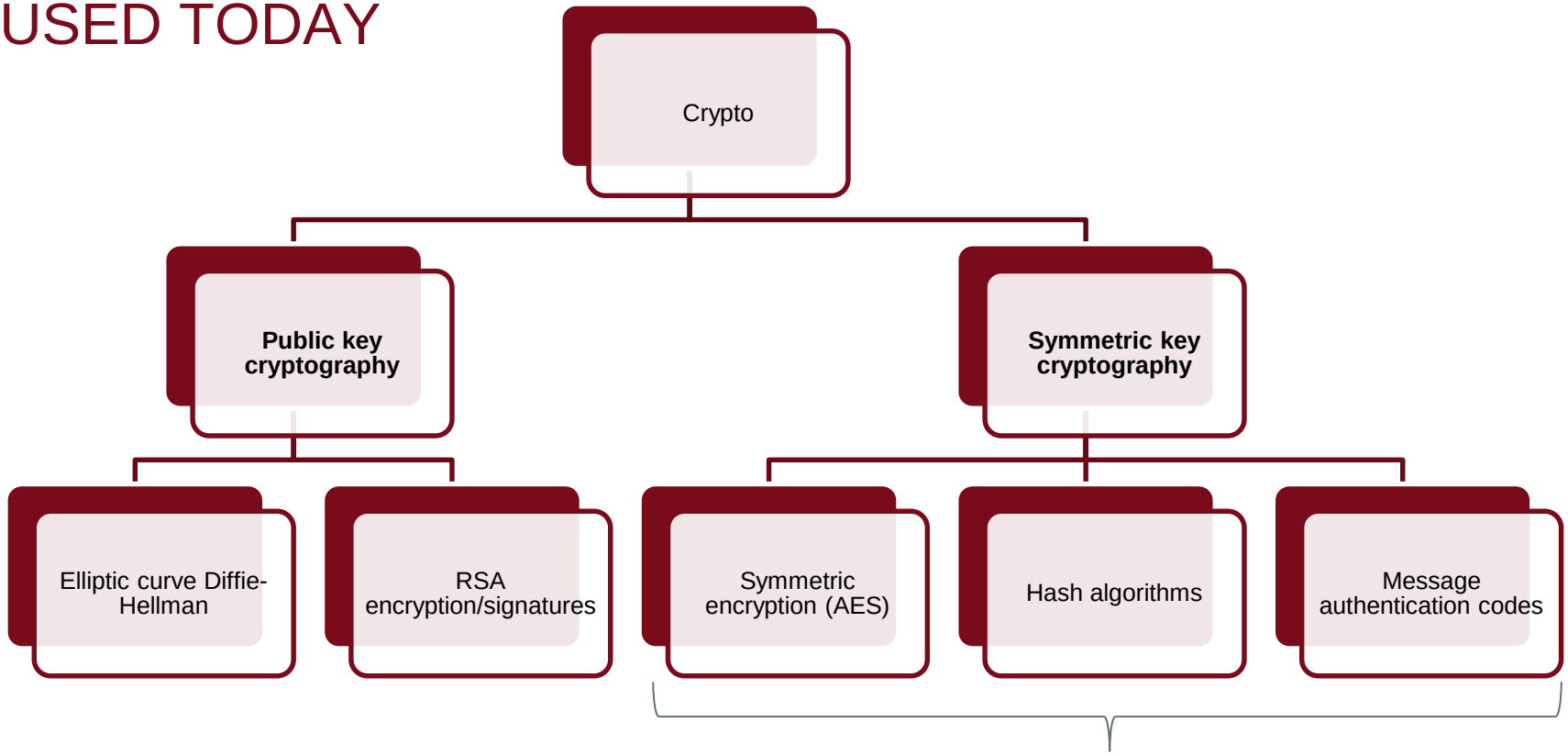


- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
  - **Elliptic curve Diffie-Hellman** with ephemeral keys (forward secrecy)
  - Authenticate DH parameters with **RSA signatures**
  - **AES** with 256 bit keys in CBC mode as **encryption** algorithm
  - **HMAC-SHA1** as **message authentication code** (MAC)

PUBLIC KEY / SYMMETRIC CRYPTO AS USED TODAY



PUBLIC KEY / SYMMETRIC CRYPTO AS USED TODAY

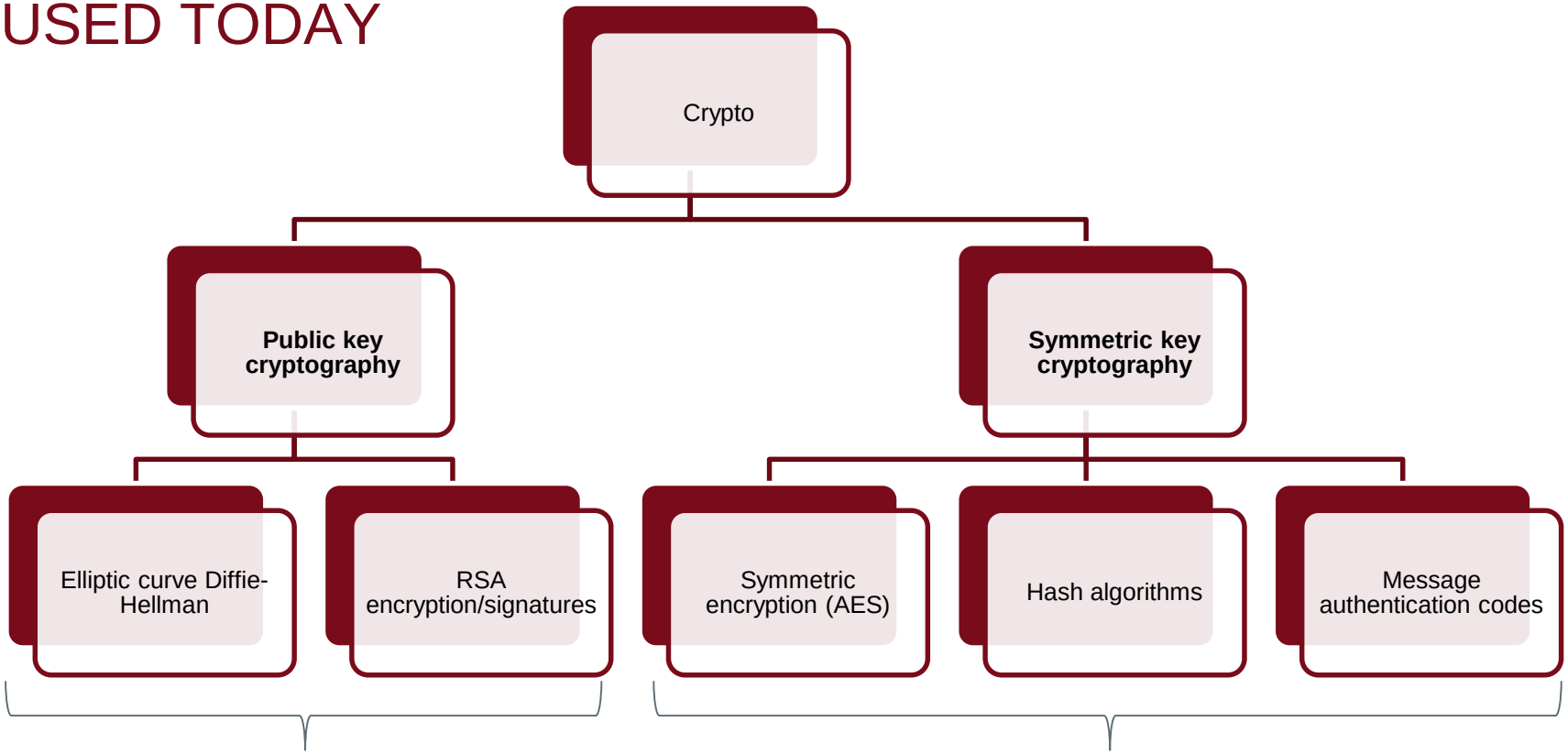


Grover's algorithm: square-root speedup

- double key size (symmetric encryption)
- double output size (hash functions)

N bit → 2N bit

PUBLIC KEY / SYMMETRIC CRYPTO AS USED TODAY



Shors's algorithm

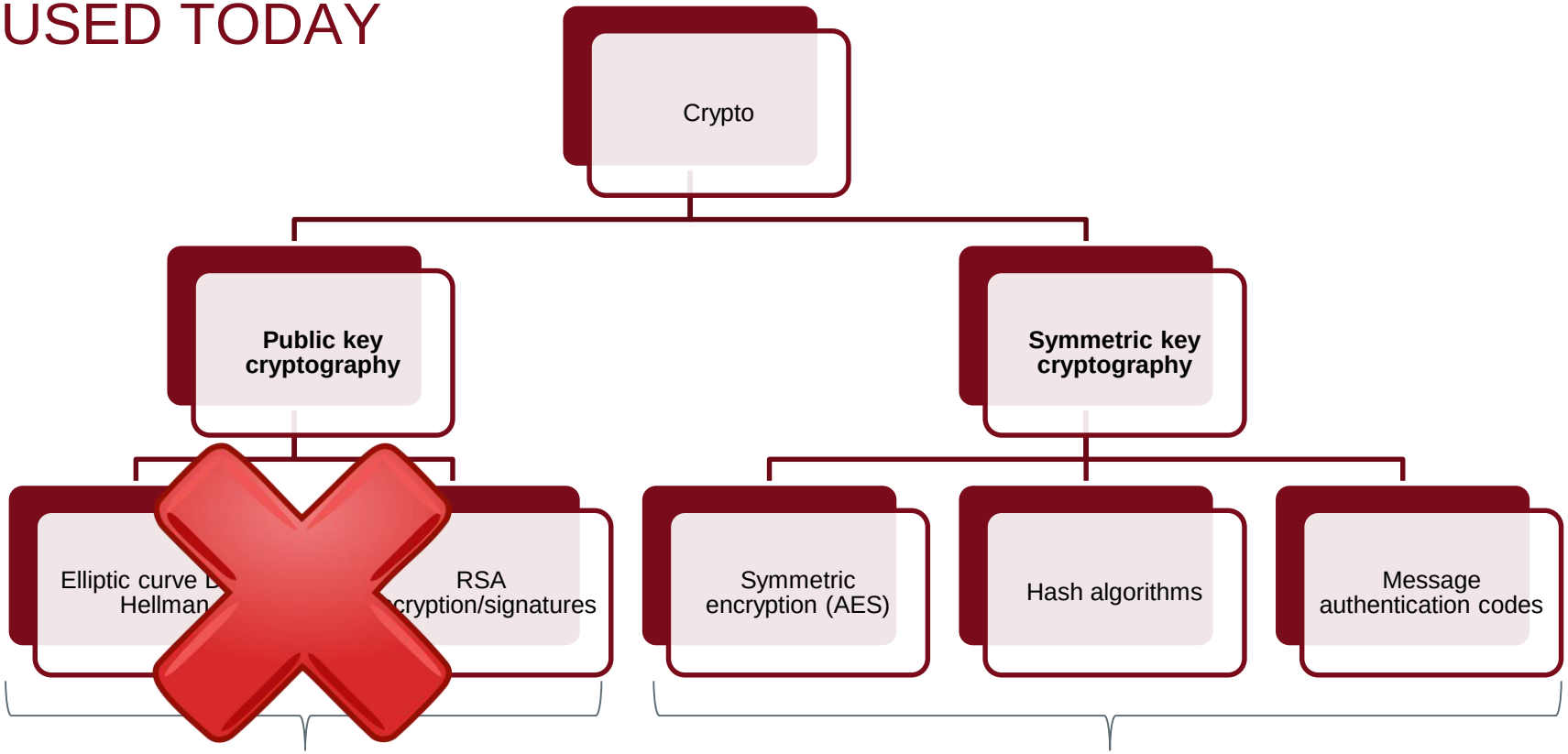
- Factoring and discrete logarithms in polynomial time (= efficient) !

Grover's algorithm: square-root speedup

- double key size (symmetric encryption)
- double output size (hash functions)

N bit → 2N bit

PUBLIC KEY / SYMMETRIC CRYPTO AS USED TODAY



Shors's algorithm

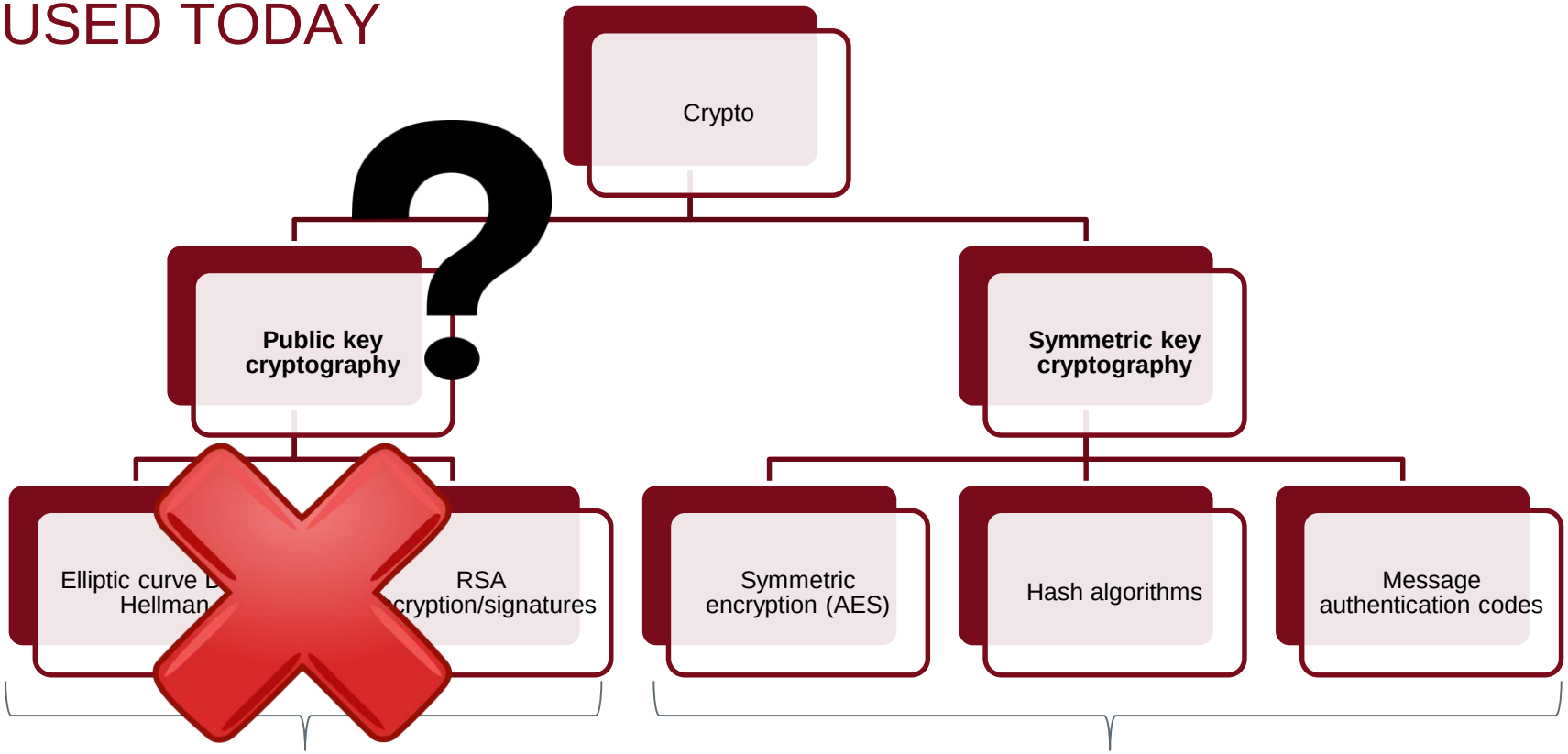
- Factoring and discrete logarithms in polynomial time (= efficient) !

Grover's algorithm: square-root speedup

- double key size (symmetric encryption)
- double output size (hash functions)

N bit → 2N bit

PUBLIC KEY / SYMMETRIC CRYPTO AS USED TODAY



Shors's algorithm

- Factoring and discrete logarithms in polynomial time (= efficient) !

Grover's algorithm: square-root speedup

- double key size (symmetric encryption)
- double output size (hash functions)

N bit → 2N bit

WHEN ARE QUANTUM COMPUTERS POWERFUL ENOUGH?

“There is a 1 in 7 chance that some fundamental public-key crypto will be broken by quantum by 2026, and a 1 in 2 chance of the same by 2031.”
– Michele Mosca, U. of Waterloo

- Far from certain when we have to be ready
- But
  - History tells us that it takes time to change deployed crypto
    - It is dangerous to end up in a rush
  - Important to have well studied and secure cryptosystems and standards available when required
  - Intensify the research to be ready!

SOLUTION

Realizing post-quantum cryptography

OVERVIEW OF DIFFERENT APPROACHES TO PQC

Signatures only

Hash-based
- Merkle signatures
- SPHINCS

Symmetric-key-based
- Picnic

Symmetric primitives

Signatures + Encryption

Lattice-based
- NTRU
- (Ring-) Learning with Errors

Code-based
- McEliece

Multivariate
- Multivariate polynomials

Isogenies
- Supersingular elliptic curve isogenies

Structured hardness assumptions

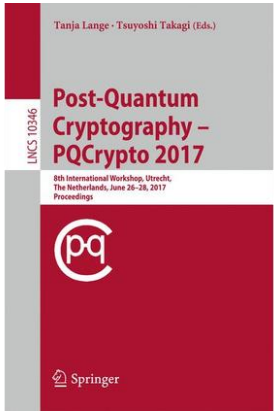
OVERVIEW OF DIFFERENT APPROACHES TO PQC

- Quite a diverse zoo
  - Assumptions (well studied vs. very recent)
  - Computational efficiency
  - Private and public key sizes
  - Ciphertext and signature sizes
  - Inherent protection against side-channel attacks

Much more diversity than with the schemes we have today!

Different schemes (underlying problems) for different settings?

ACADEMIC AND INDUSTRIAL INITIATIVES



- Int. Conference on Post-Quantum Cryptography (PQCrypto)
  - Since 2006
  - PQCrypto 2018 upcoming (co located with NIST PQ Conference)
  - Flagship crypto conferences CRYPTO, Eurocrypt, Asiacrypt, PKC more and more interested in PQC

- EU has announced a one billion € flagship project

- H2020 projects on quantum safe crypto (SAFEcrypto, PQCRYPTO)
  - More to come from last crypto call (FutureTPM, PROMETHEUS)

- ETSI established quantum safe crypto (QSC) group

- NIST started post-quantum cryptography standardization

NIST PQ CRYPTO STANDARDIZATION

- Important competitions for cryptographic schemes in the past
  - AES, SHA-1, SHA-3

- Now running a project for Post-Quantum Cryptography Standardization
  - Signatures, Encryption and Key-establishment

- Timeline

Nov 30, 2017	Deadline for submissions	
Early 2018	Workshop - Submitter's Presentations	**April 12-13, 2018** - First PQC Standardization Conference, co-located with PQCrypto 2018
3-5 years	Analysis Phase - NIST will report findings *1-2 workshops during this phase*	
2 years later	Draft Standards ready (2023-2025)	

"**Our intention is to select a couple of options** for more immediate standardization, as well as to eliminate some submissions as unsuitable. ... The goal of the process is **not primarily to pick a winner**, but to document the strengths and weaknesses of the different options, and to analyze the possible tradeoffs among them."

AIT AND POST-QUANTUM CRYPTOGRAPHY

- New approach for designing post-quantum signature schemes
- Does not require structured hardness assumptions (lattices, codes, etc.)
  - Only symmetric-key primitives: relatively well understood post-quantum security
- Submitted to NIST competition
- Open source reference and optimized implementations available
  - Integrated into Open Quantum Safe (OQS) project

PICNIC https://microsoft.github.io/Picnic/

A Family of Post-Quantum Secure Digital Signature Algorithms

THANK YOU!

daniel.slamanig@ait.ac.at
https://drl3c7er.github.io/
@drl3c7er