CASA
SECURING THE DIGITAL SOCIETY

Insights into the New Post-Quantum Cryptography Standards

Eike Kiltz | Ruhr-Universität Bochum

RUHR UNIVERSITÄT BOCHUM RUB
Funded by DFG Deutsche Forschungsgemeinschaft German Research Foundation
HGI HORST GÖRTZ INSTITUTE

EIKE KILTZ

CASA
SECURING THE DIGITAL SOCIETY

Professor of computer science at Ruhr University Bochum, Germany

RUHR
UNIVERSITÄT
BOCHUM

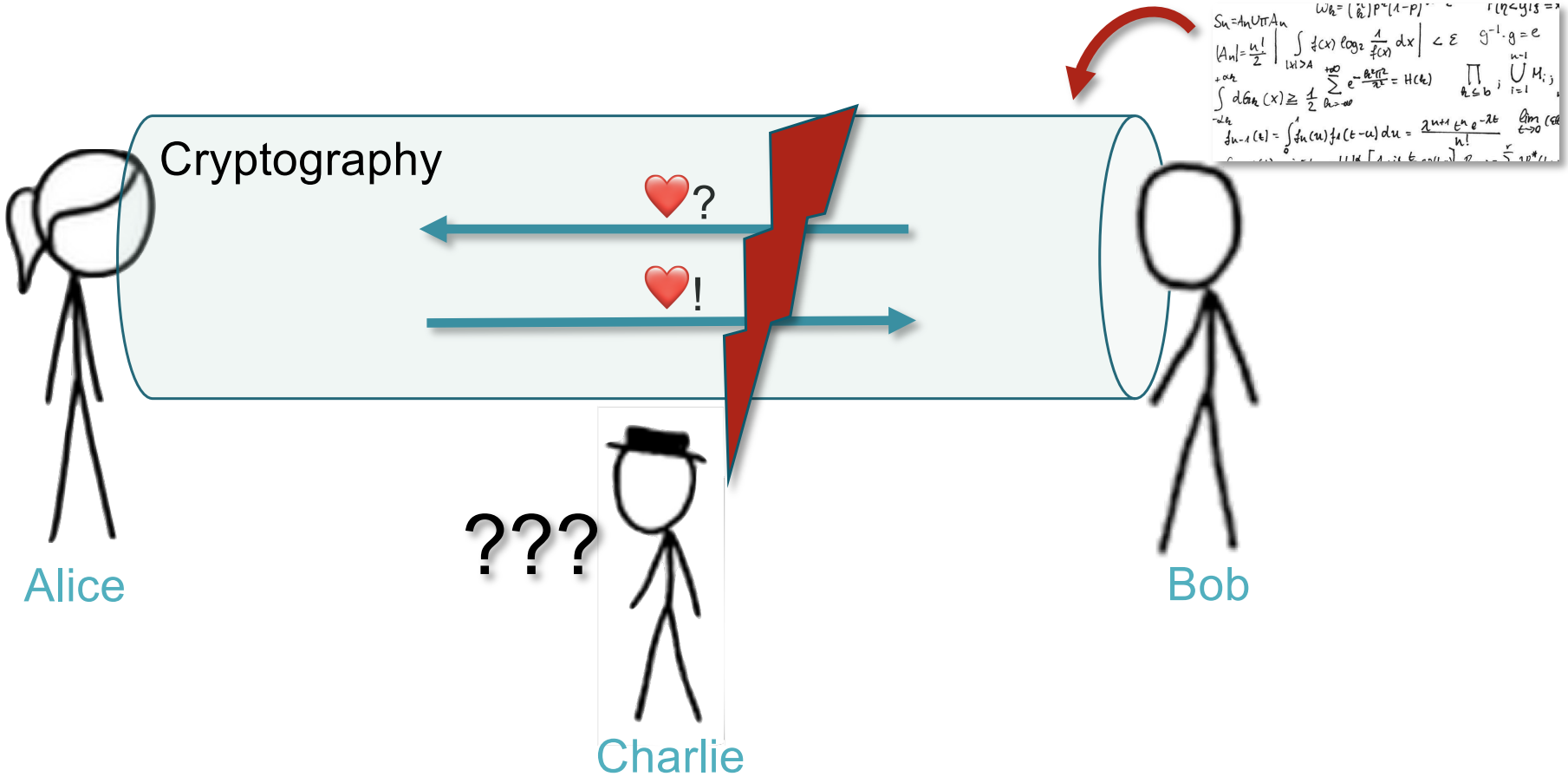
RUB

MAX PLANCK INSTITUTE
FOR SECURITY AND PRIVACY

CRYPTOGRAPHY

CASA
SECURING THE DIGITAL SOCIETY

”Science of secure communication in presence of malicious parties”

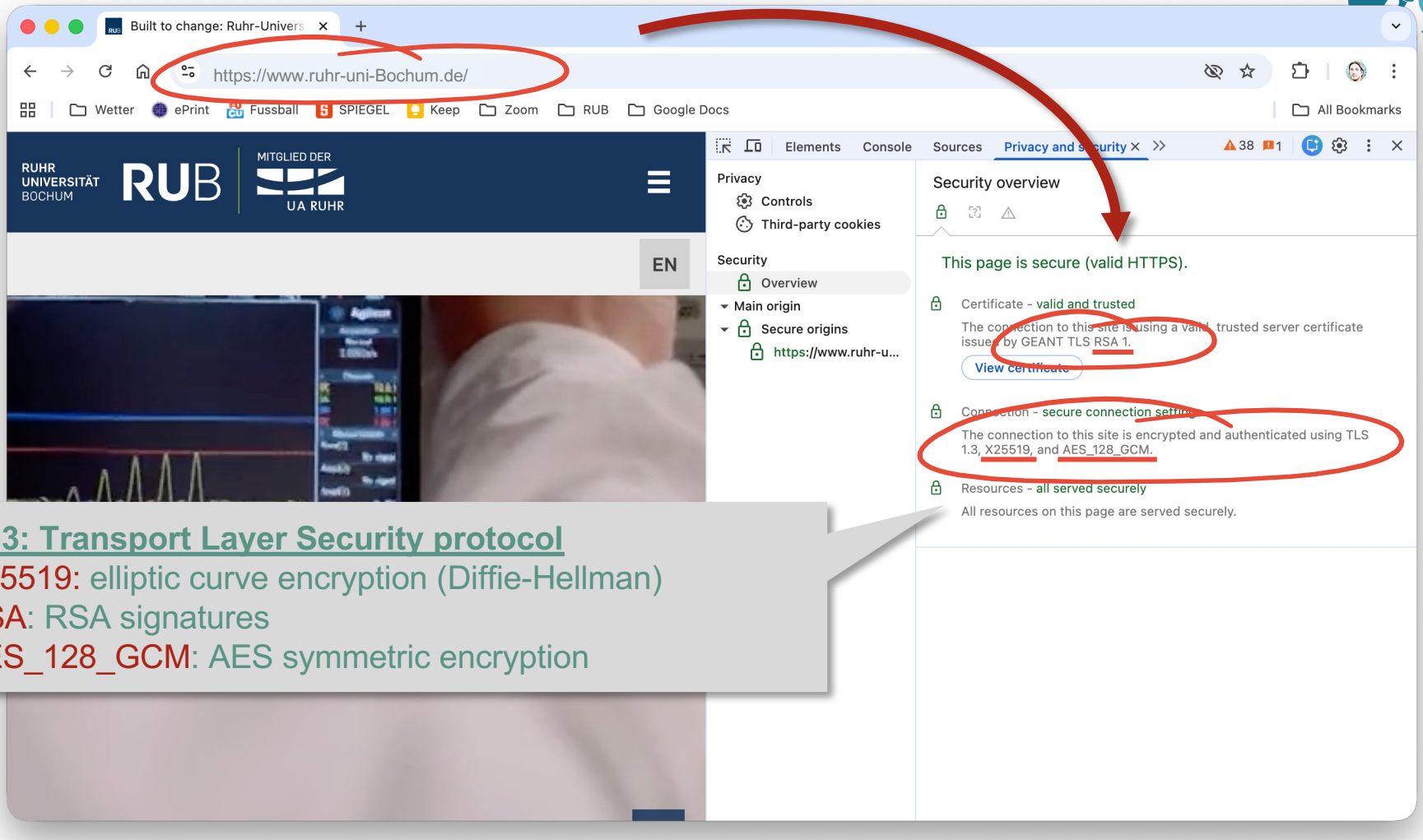


Images: xkcd

MODERN CRYPTOGRAPHY

CASA
SECURING THE DIGITAL SOCIETY

- Digital communication
  - WhatsApp, Signal, iMessage, ...
  - (PGP-) encrypted emails
  - Websites with https://
- Financial
  - Credit and EC cards
  - Secure transactions
  - Cryptocurrencies: Bitcoin, Etherium, ...
- Cars, Medicine, elections, …



TLS 1.3: Transport Layer Security protocol

- X25519: elliptic curve encryption (Diffie-Hellman)
- RSA: RSA signatures
- AES_128_GCM: AES symmetric encryption

CASA
SECURING THE DIGITAL SOCIETY

Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

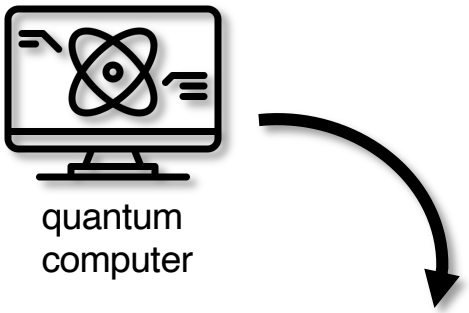
Peter W. Shor†

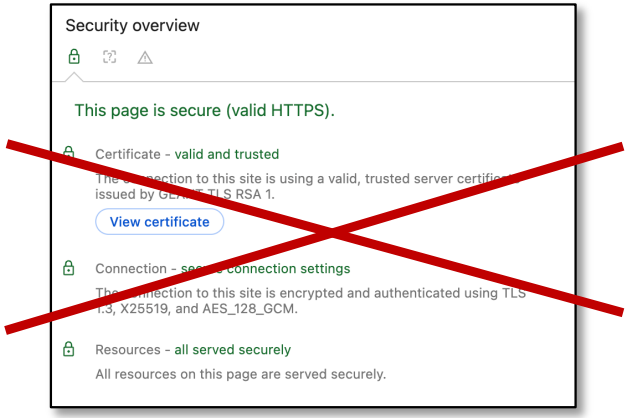
Abstract

A digital computer is generally believed to be an efficient universal computing device; that is, it is believed able to simulate any physical computing device with an increase in computation time by at most a polynomial factor. This may not be true when quantum mechanics is taken into consideration. This paper considers factoring integers and finding discrete logarithms, two problems which are generally thought to be hard on a classical computer and which have been used as the basis of several proposed cryptosystems. Efficient randomized algorithms are given for these two problems on a hypothetical quantum computer. These algorithms take a number of steps polynomial in the input size, e.g., the number of digits of the integer to be factored.

Keywords: algorithmic number theory, prime factorization, discrete logarithms, Church's thesis, quantum computers, foundations of quantum mechanics, spin systems, Fourier transforms

AMS subject classifications: 81P10, 11Y05, 68Q10, 03D10





YEAR 2035: FAR AWAY?

Harvest Now, Decrypt Later (HNDL)

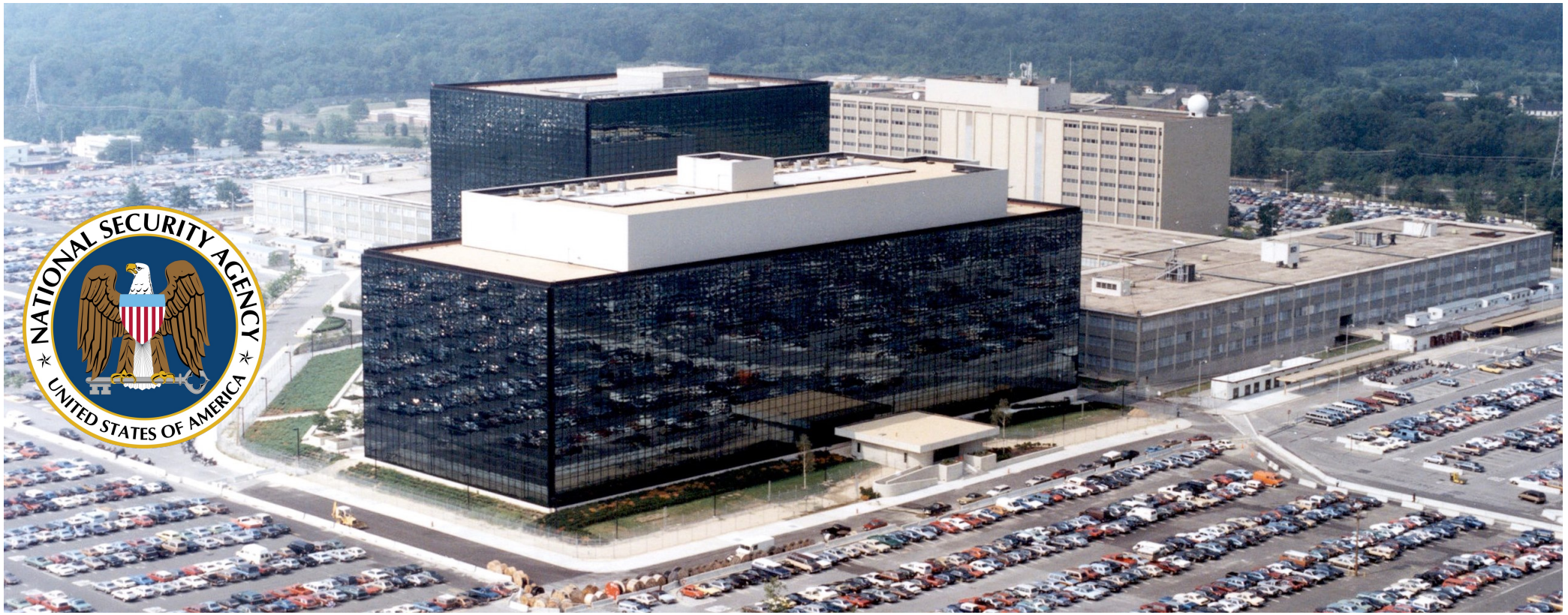


Image: wikipedia

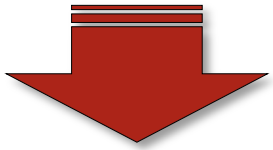
CASA
SECURING THE DIGITAL SOCIETY

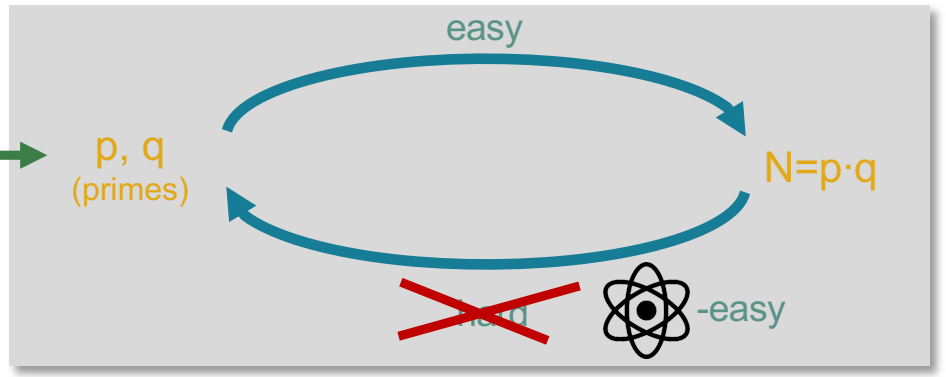
Summary

- Cryptography: protects digital data and is ubiquitous
- Quantum computers: break existing cryptography
- Unclear when (or whether) quantum computers will become available
- Act now: cryptography secure against quantum attackers

POST-QUANTUM CRYPTOGRAPHY

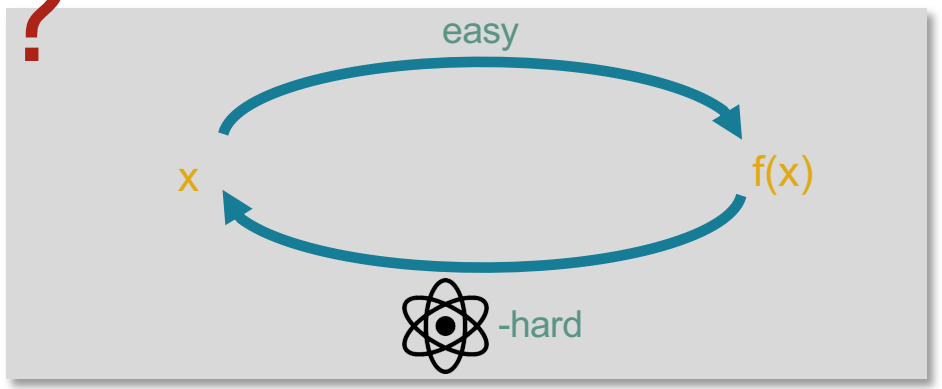
- Existing cryptography
  - ~~RSA~~
  - ~~Elliptic curves~~





- Post-quantum cryptography
  - Coding theory (McEliece)
  - Isogenies between elliptic curves
  - Lattices

??



NIST POST-QUANTUM COMPETITION

CASA
SECURING THE DIGITAL SOCIETY

2016 — Call

2017 — 82 submissions

Discussion with >1000 researchers

2022 — 4 NIST standards

2024

Public-Key Encryption:
- KYBER (ML-KEM)

Digital Signatures:
- DILITHIUM (ML-DSA)
- Falcon (FN-DSA)
- SPHINCS+ (SLH-DSA)

FIPS 203

Federal Information Processing Standards Publication

Module-Lattice-Based Key-Encapsulation Mechanism Standard

Category: Computer Security — Subcategory: Cryptography

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

This publication is available free of charge from:
https://doi.org/10.6028/NIST.FIPS.203

Published August 13, 2024

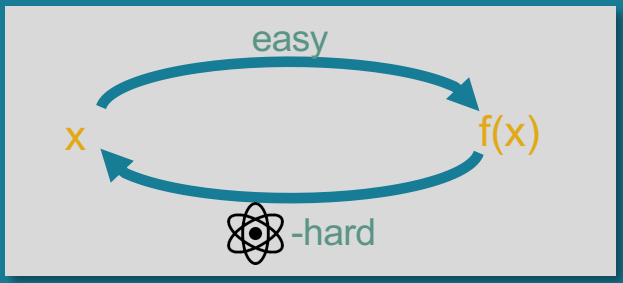
U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

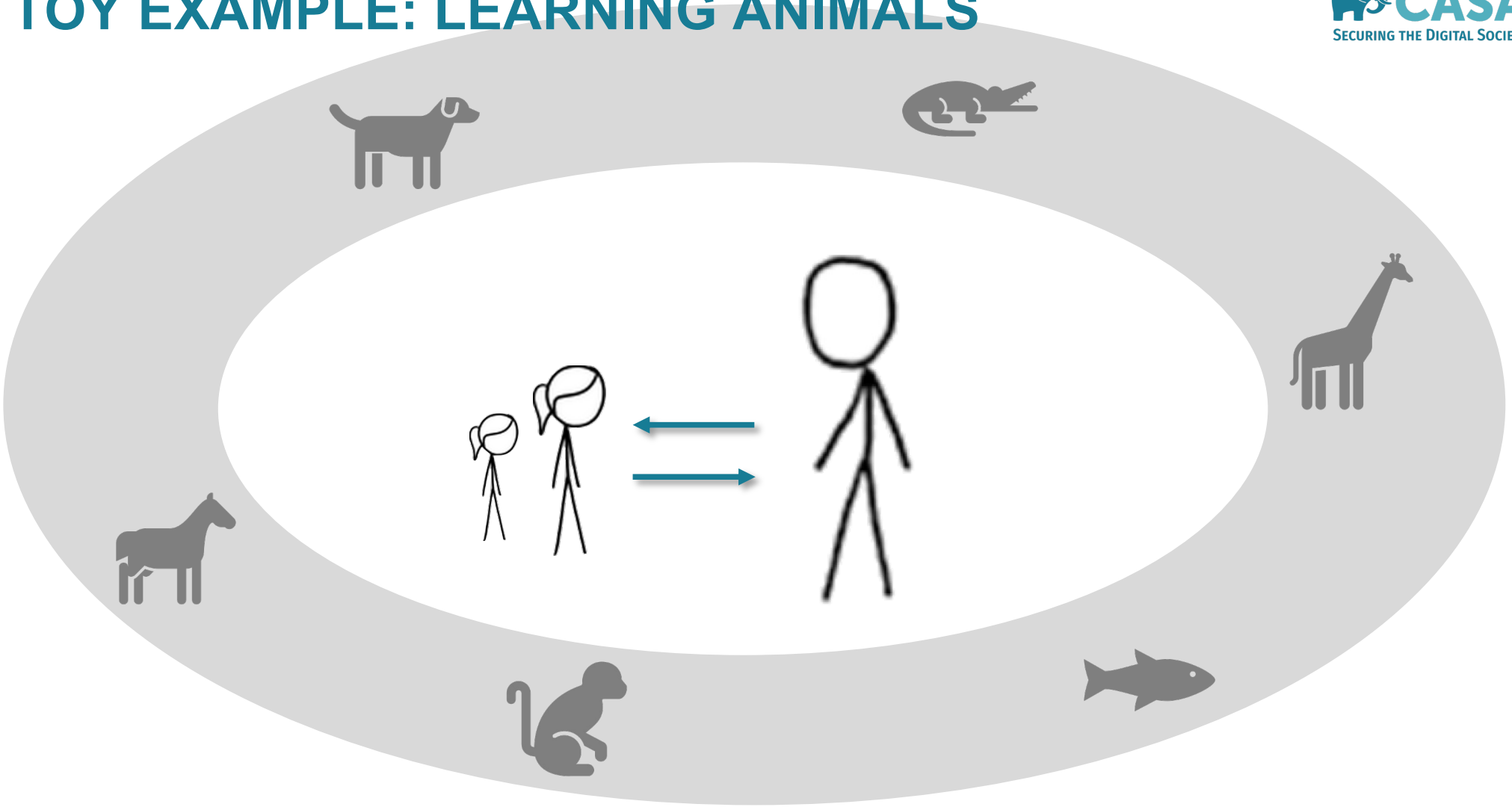
CASA
SECURING THE DIGITAL SOCIETY

Post-quantum cryptography

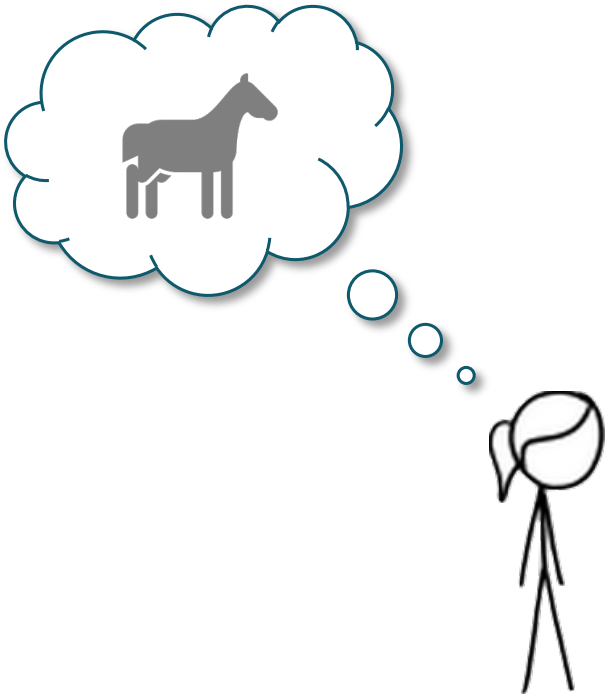
Mathematical foundations



TOY EXAMPLE: LEARNING ANIMALS



LEARNING ANIMALS



living in the water?

no

feathers?

no

mammal?

yes

⋮

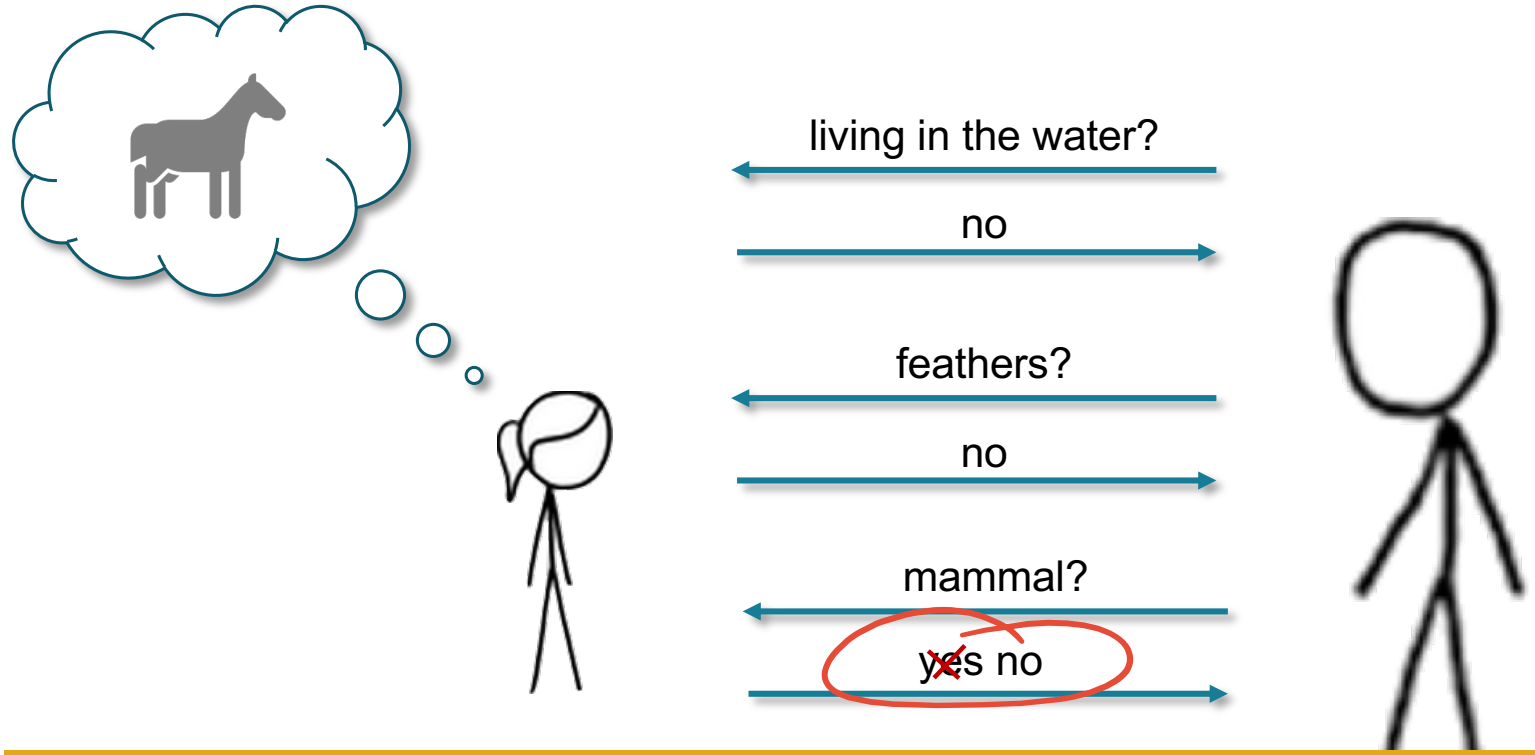
unicorn?

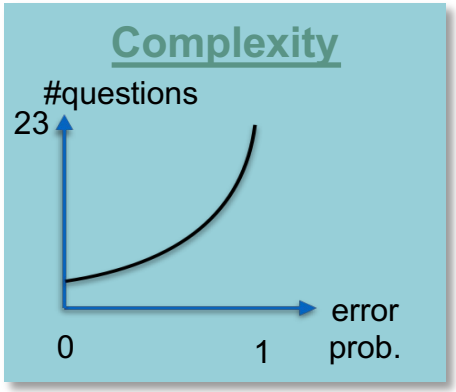
yes!

Binary search

#questions = $\log_2$(#animals) = 23

LEARNING ANIMALS WITH ERRORS



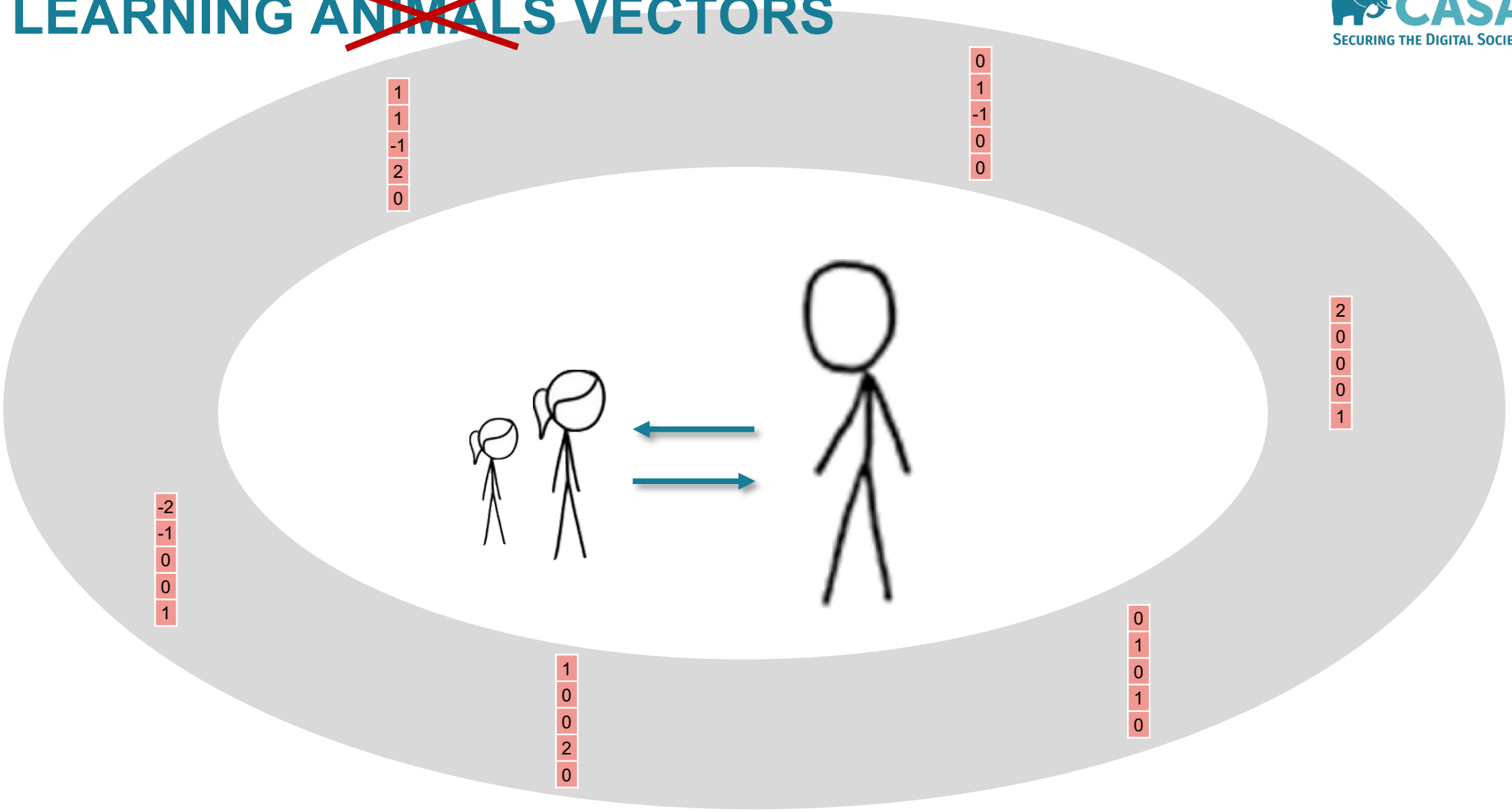


Summary

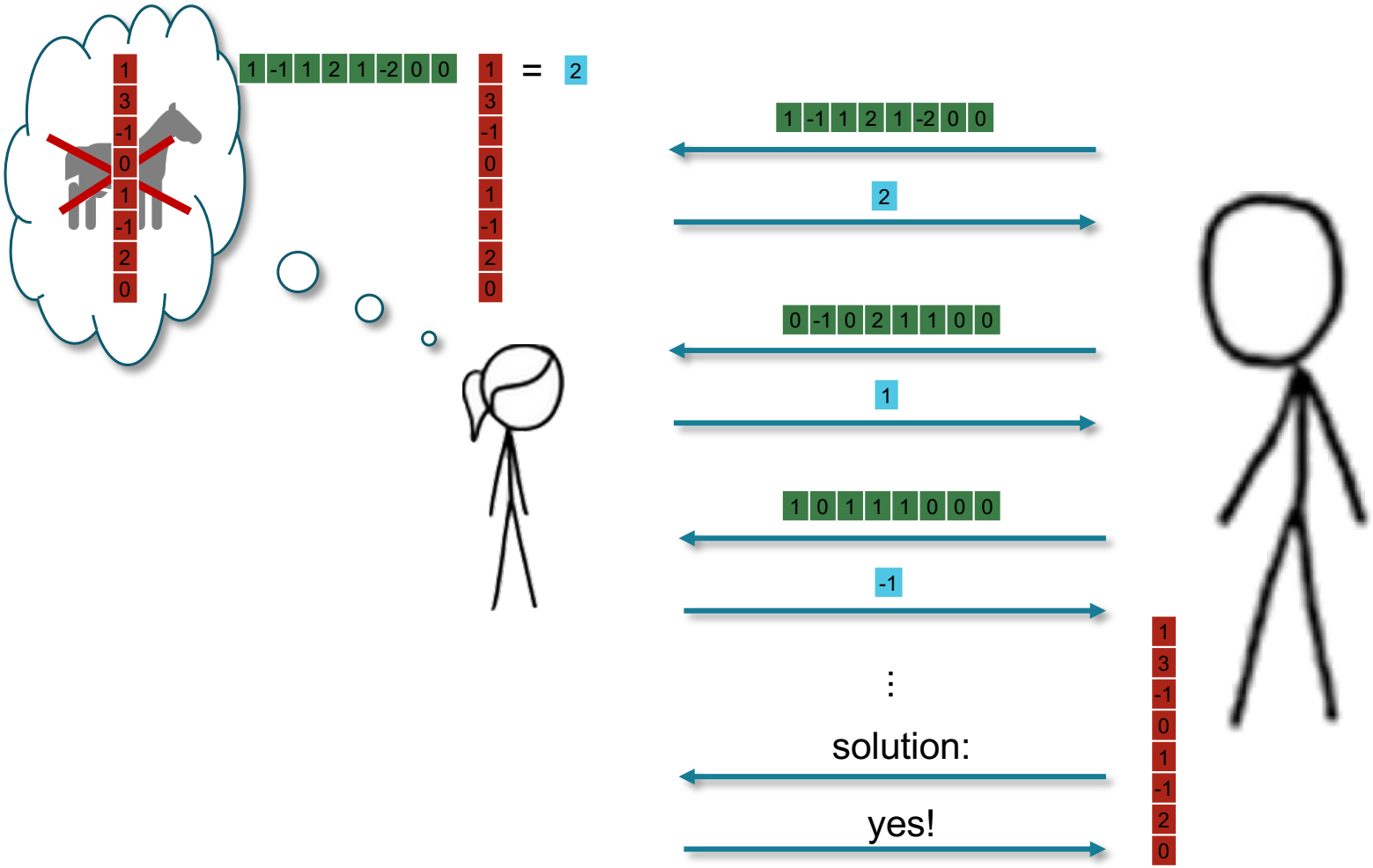
- Learning animals: easy
- Learning animals with errors: difficult

LEARNING ~~ANIMALS~~ VECTORS

CASA
SECURING THE DIGITAL SOCIETY



LEARNING VECTORS

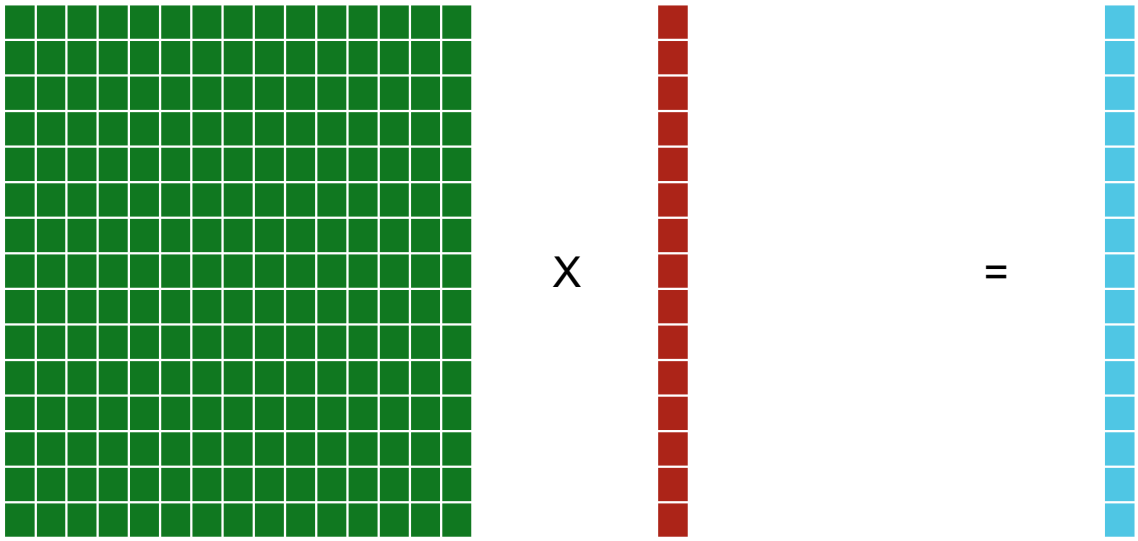


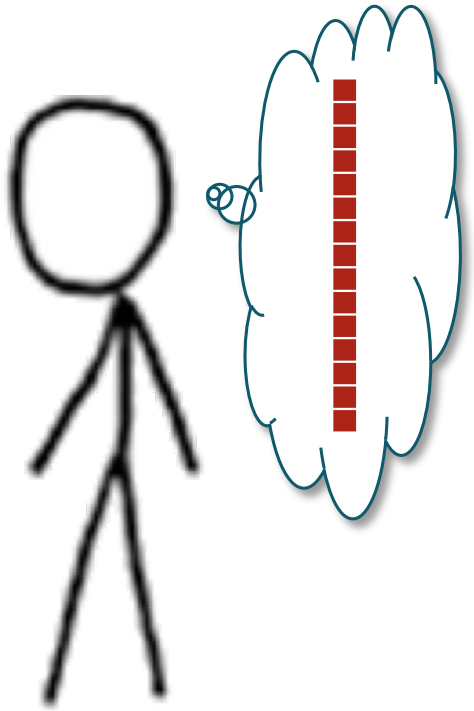
LEARNING VECTORS: MATHEMATICAL

CASA
SECURING THE DIGITAL SOCIETY

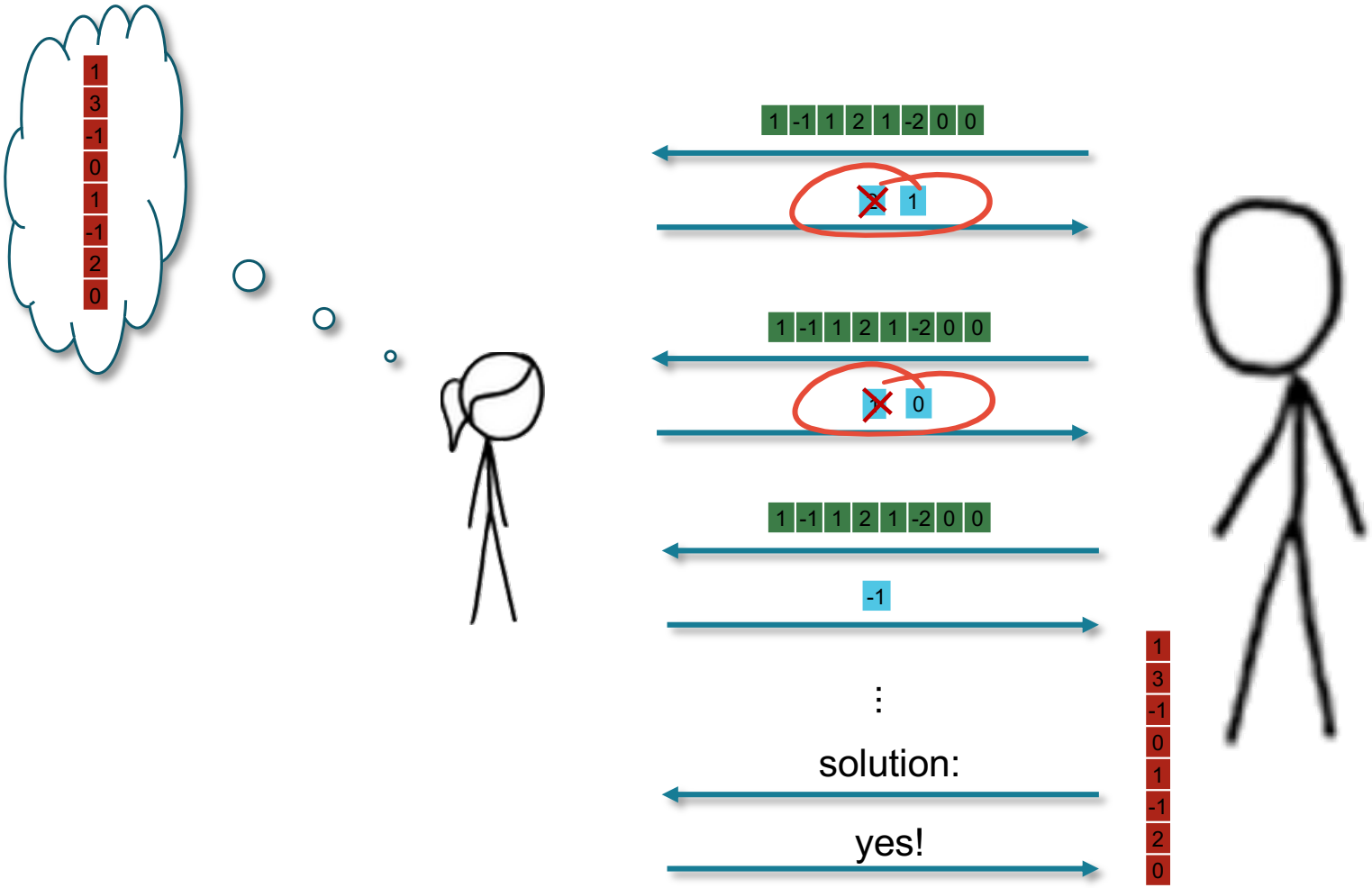
Complexity
#questions = dimension of vector

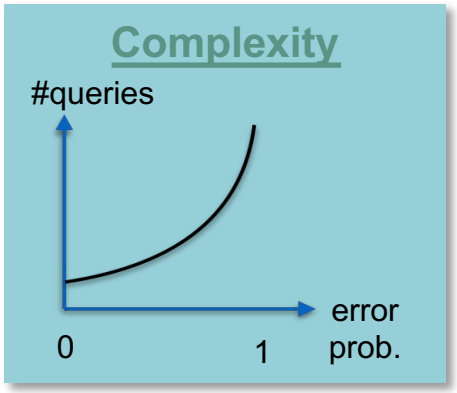
matrix (queries) secret vector answers



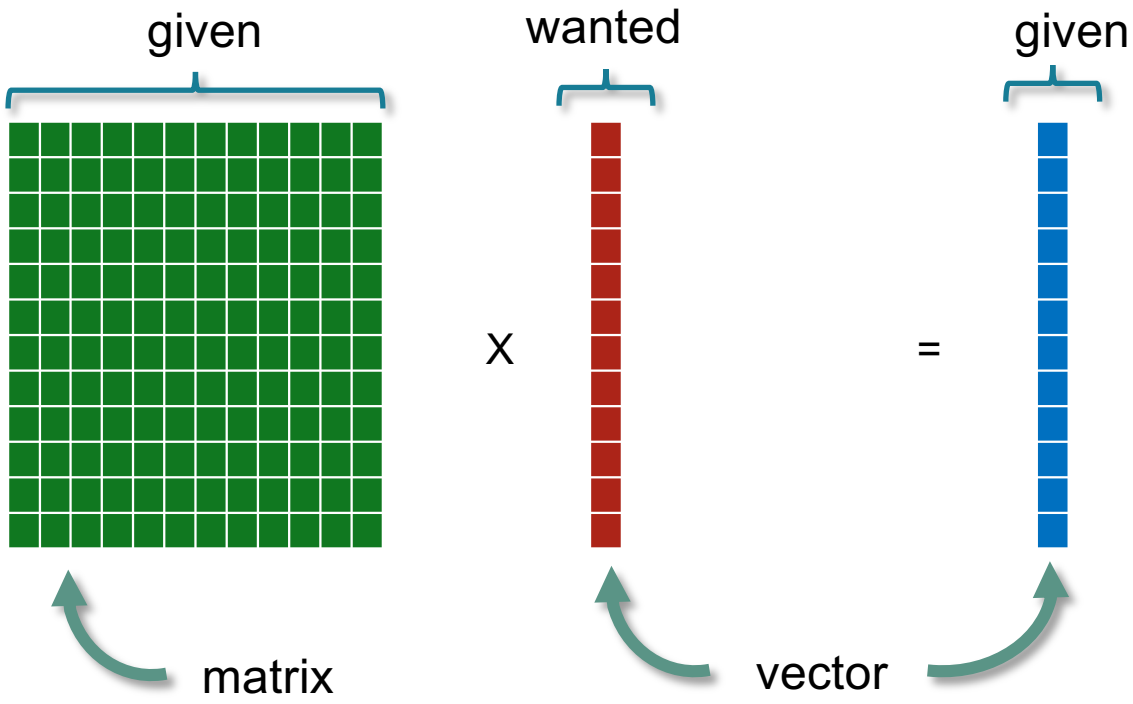


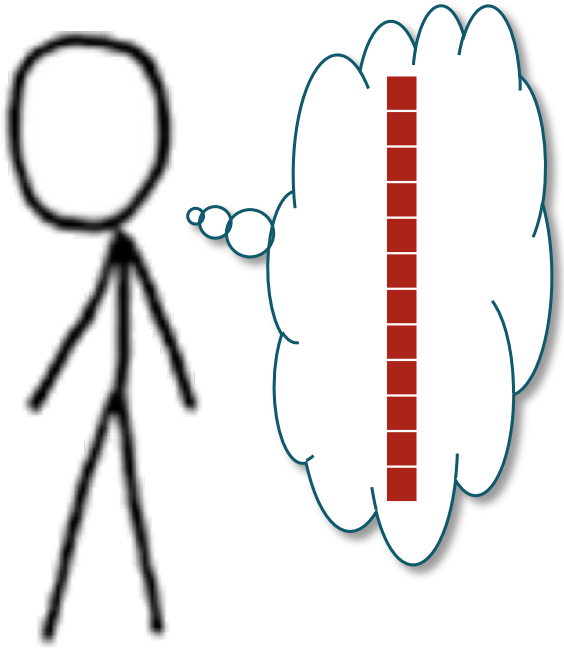
LEARNING VECTORS WITH ERRORS



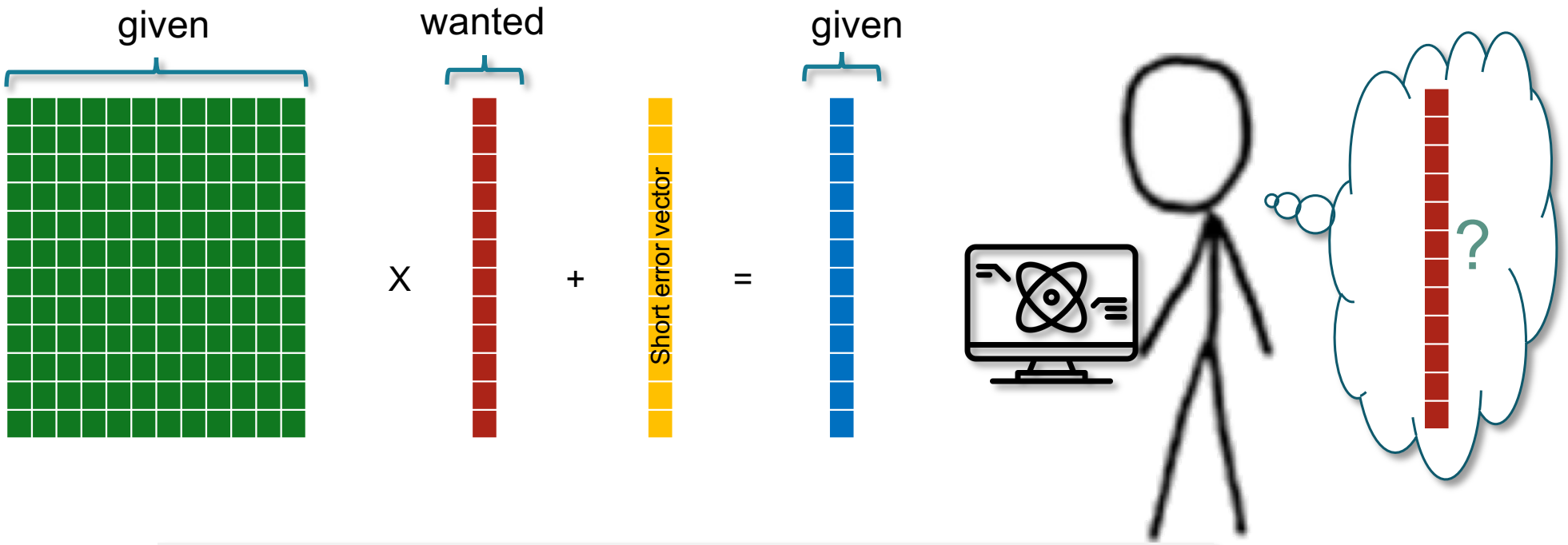


LEARNING VECTORS (LW)





LEARNING VECTORS WITH ERRORS (LWE)



LEARNING VECTORS WITH ERRORS (LWE)

CASA
SECURING THE DIGITAL SOCIETY

Summary

- Learning animals: easy
- Learning animals with errors: hard
- Learning vectors: easy
- Learning vectors with errors: hard

Post-quantum cryptography

Encrypyion from lattices

LATTICES

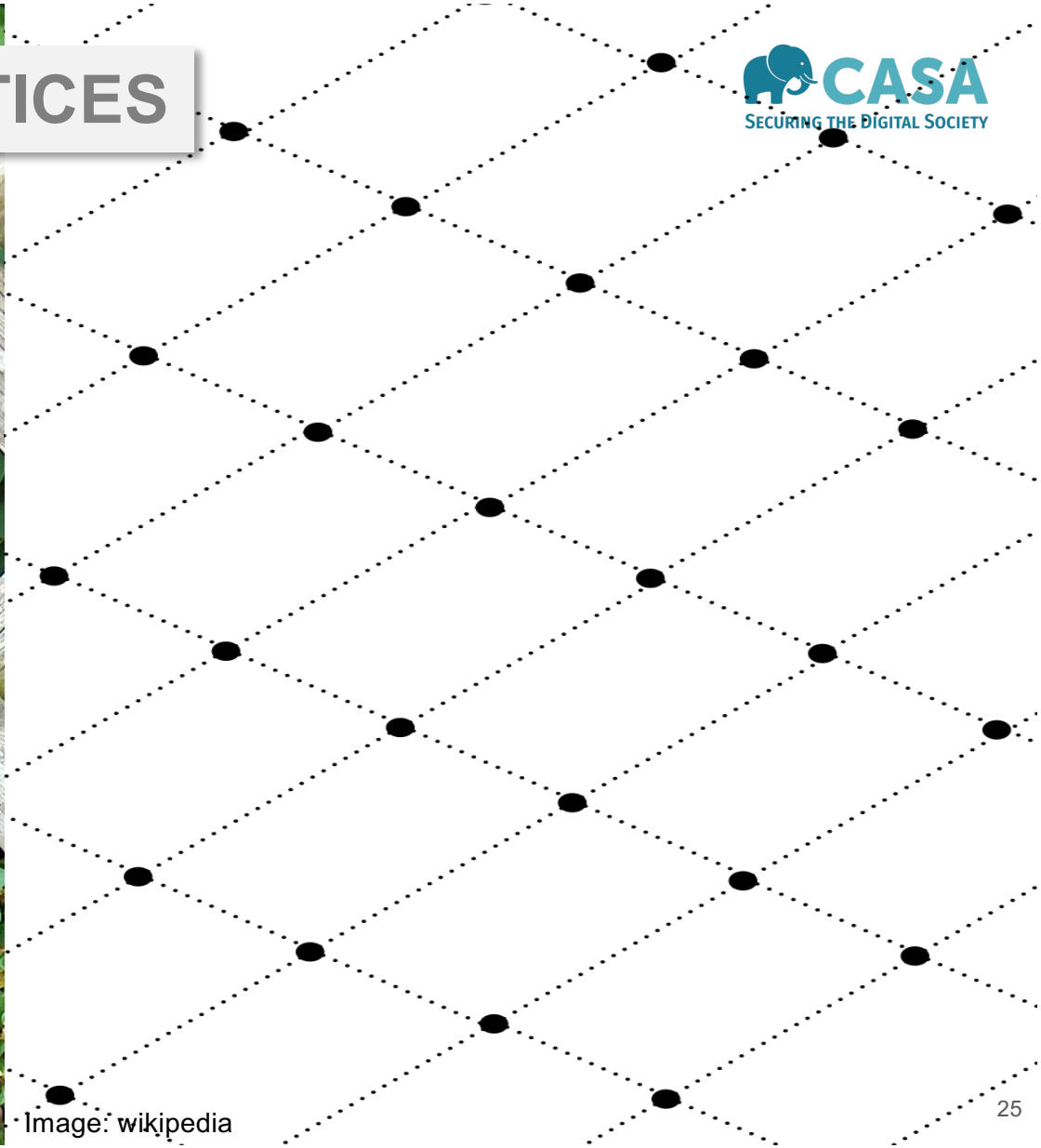
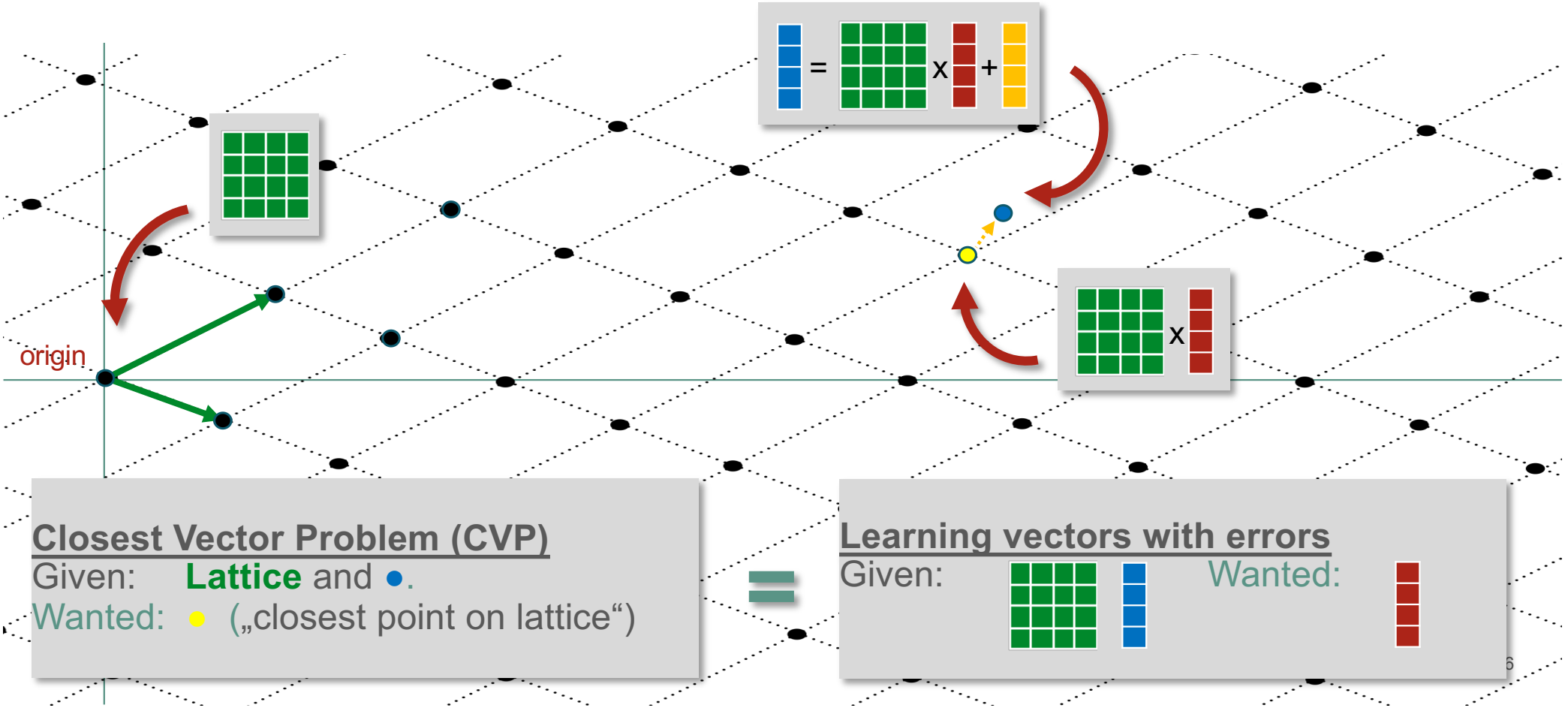


Image: wikipedia

LEARNING VECTORS GEOMETRICALLY: LATTICES



Closest Vector Problem (CVP)

Given: **Lattice** and ●.

Wanted: ● („closest point on lattice“)

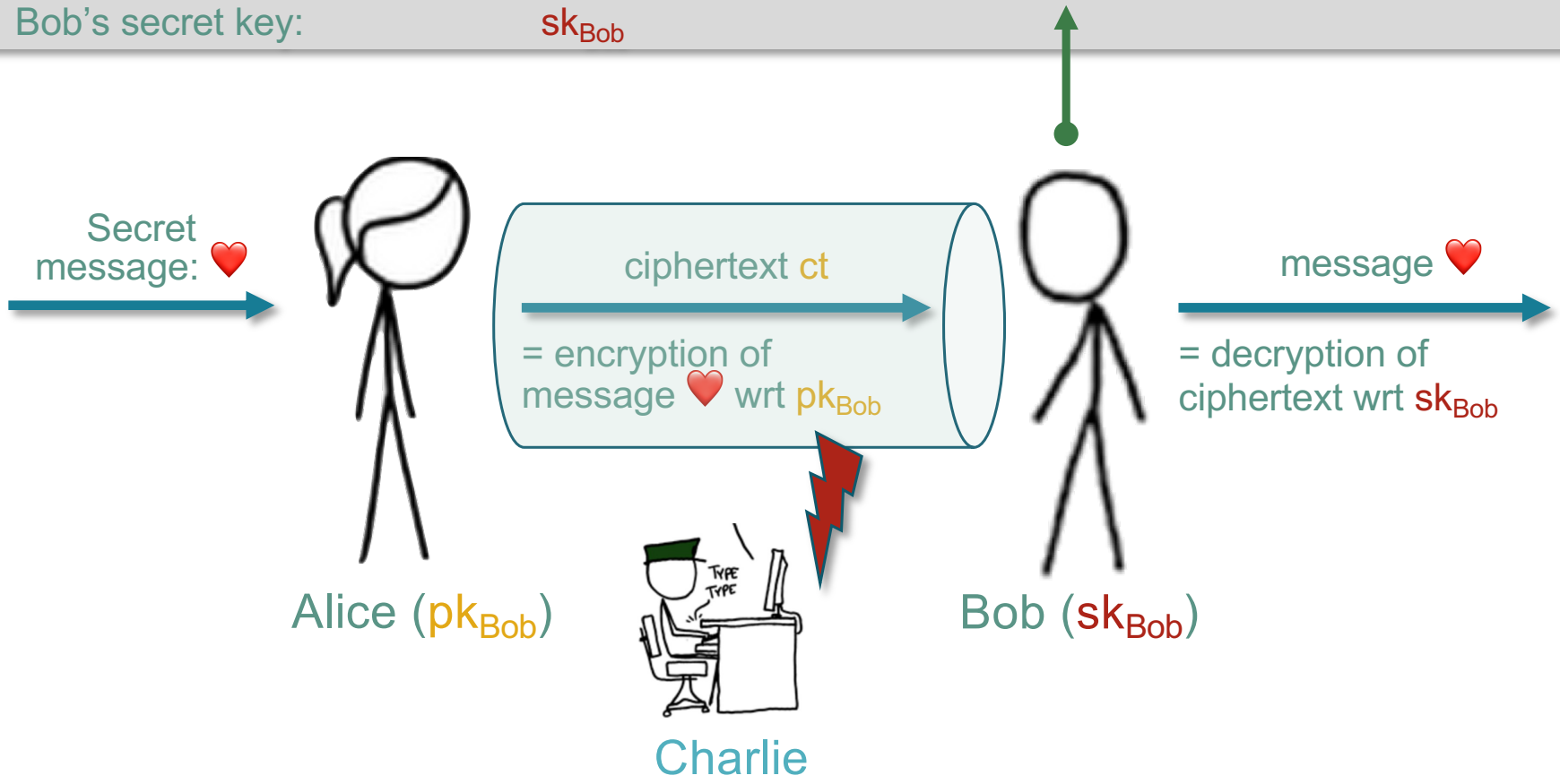
=

Learning vectors with errors

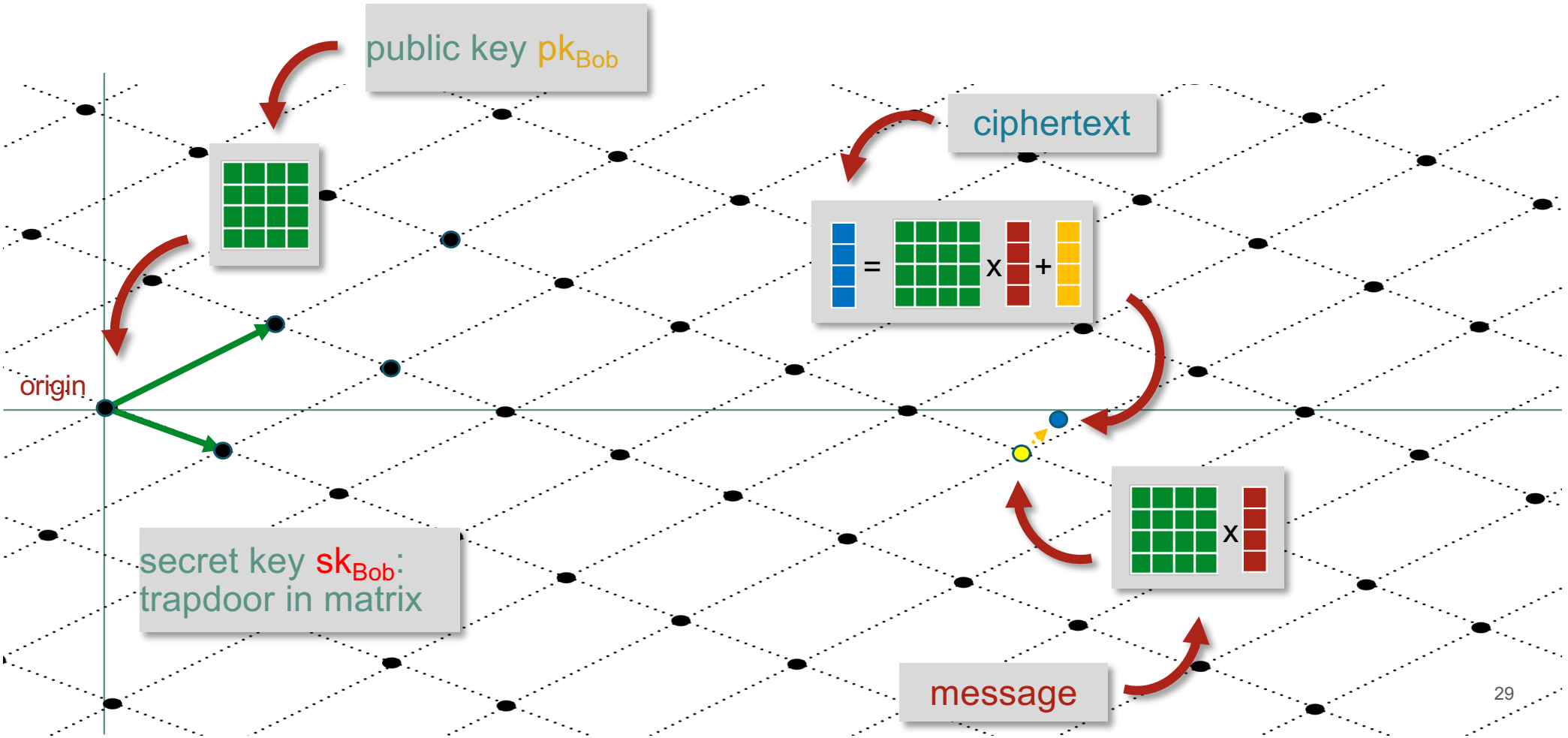
Given: Wanted:

PUBLIC-KEY ENCRYPTION

- Bob's public key: pk_{Bob}
- Bob's secret key: sk_{Bob}



ENCRYPTION FROM LATTICES: BLUEPRINT



ML-KEM (KYBER)

- “Encryption from lattices” blueprint (roughly) + …
- Efficient + security + patent free
- Provably as secure as ”learning vectors with errors” (LWE)
- Encryption and decryption: 2-3x faster
- Public key and ciphertext: 20-30x larger

Check for updates

FIPS 203

Federal Information Processing Standards Publication

Module-Lattice-Based Key-Encapsulation Mechanism Standard

Category: Computer Security **Subcategory: Cryptography**

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

This publication is available free of charge from:
https://doi.org/10.6028/NIST.FIPS.203

Published August 13, 2024

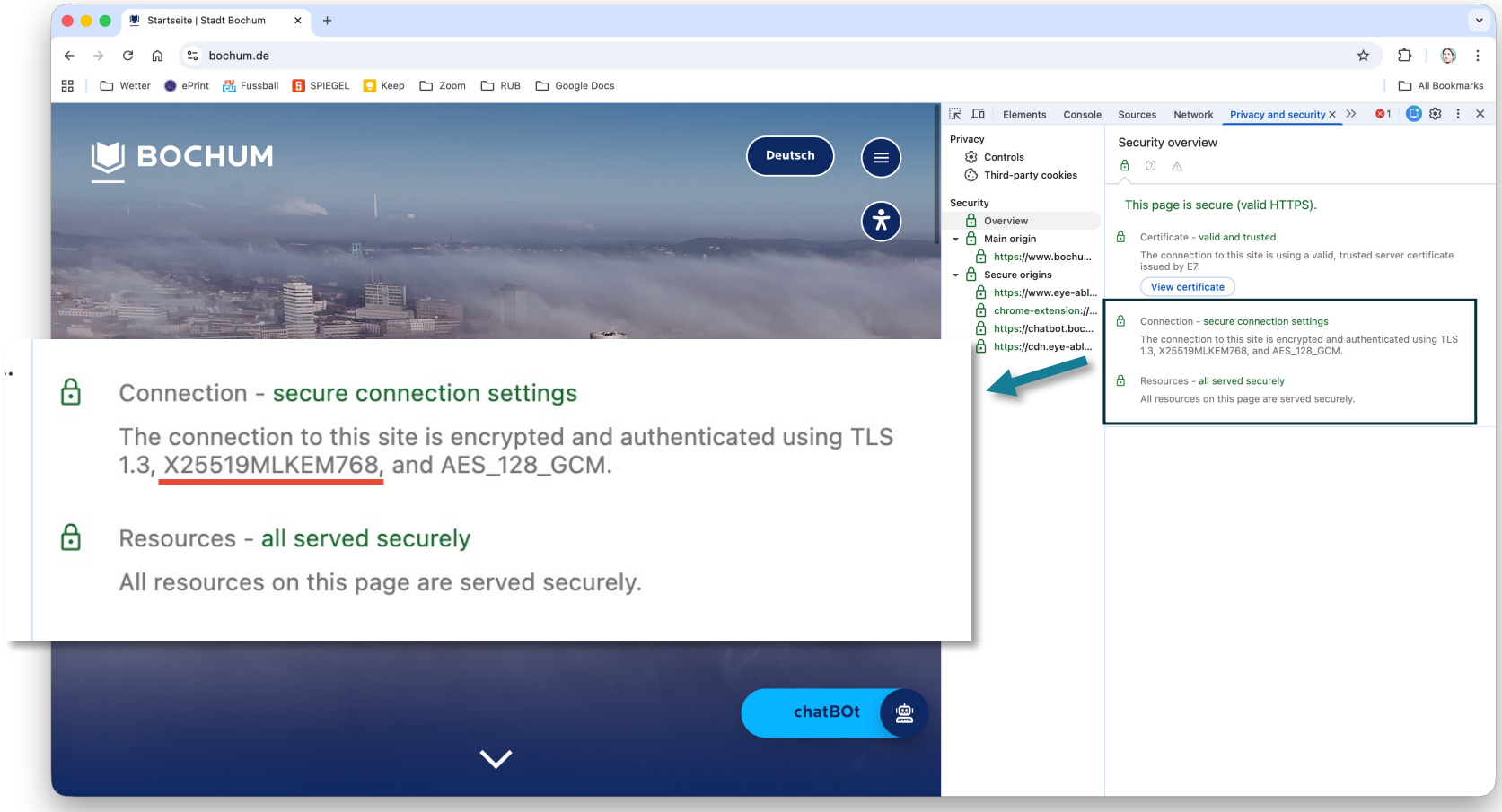
Are we done?

- Post quantum rollout!
- KYBER is not Diffie-Hellman key exchange!
- Implementation security (SCA, microarchitectural attacks)
- Diversity

https://pq-crystals.org/kyber

POST QUANTUM SECURITY 2026

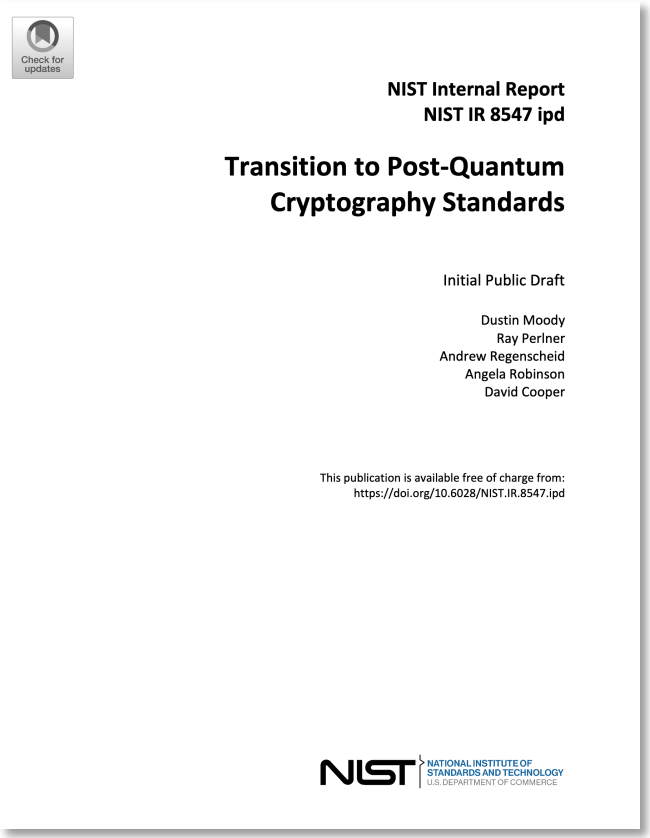
41% of Top 1M servers support post quantum security!

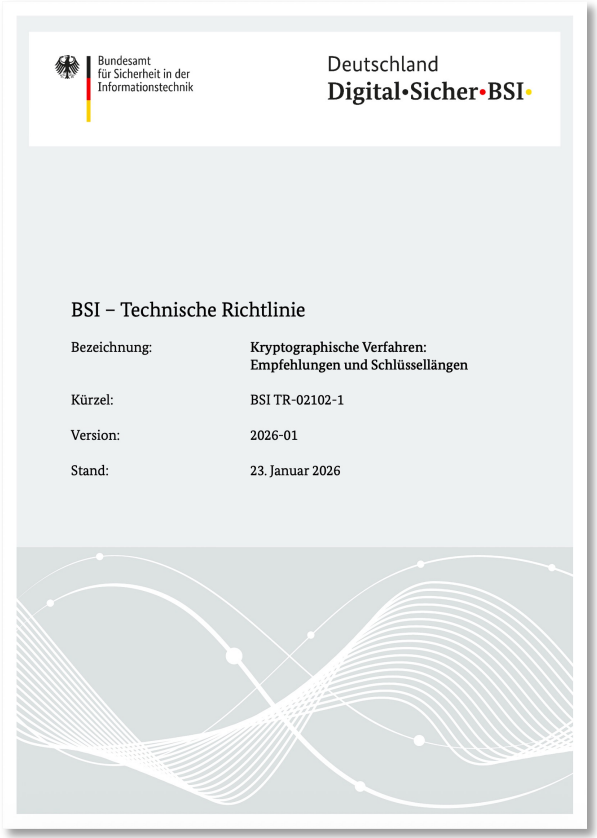


https://www.netmeister.org/blog/pqc-use-2026-02.html

NIST/BSI DOCUMENTS

From 2030-2035 on: only post quantum secure cryptography





- https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html
- https://csrc.nist.gov/pubs/ir/8547/ipd

CASA
SECURING THE DIGITAL SOCIETY

Summary

- **Quantum computers:** break existing cryptography
- **Post-quantum cryptography:** security against future quantum computers
- **July 2022:** 4 algorithms selected as the NIST Post-Quantum Cryptography Standards
- **New cryptographic technology:** lattices