Quantum Apocalypse?

Demystifying the Doomsday of Encryption

Pascal Schärli
BaselOne
2024-10-17

pascscha.ch

ELCASecurity
AN ELCA COMPANY

Breaking News

National Institute of Standards and Technology

NIST NEWS

Working with industry and academia to enhance security

VOL. 1337 | Tuesday, 13. August 2024 | nist.gov

NIST Releases First 3 Finalized Post-Quantum Encryption Standards

NIST is encouraging computer system administrators to begin transitioning to the new standards as soon as possible.

By Chad Boutin

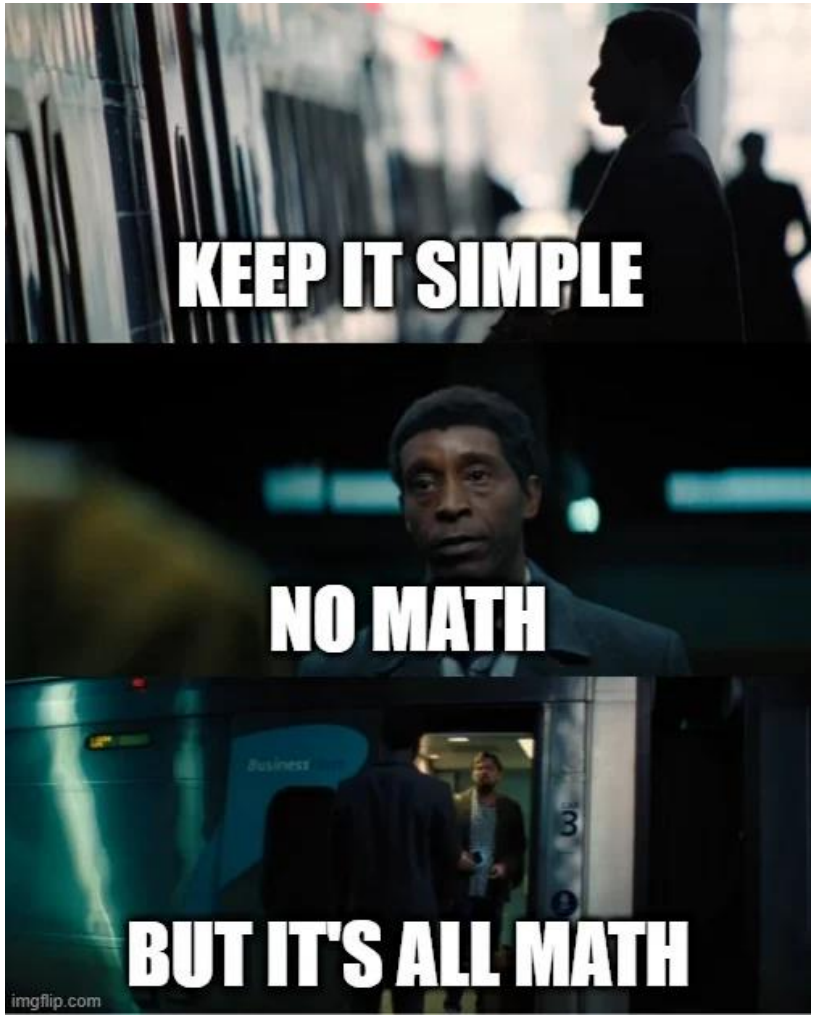
GAITHERSBURG, Md. — The U.S. Department of Commerce's National Institute of Standards and Technology (NIST) has finalized its principal set of encryption algorithms designed to withstand cyberattacks from a quantum

The three new standards are built for the future. Quantum computing technology is developing rapidly, and some experts predict that a device with the capability to break current encryption methods could appear

Article

Overview

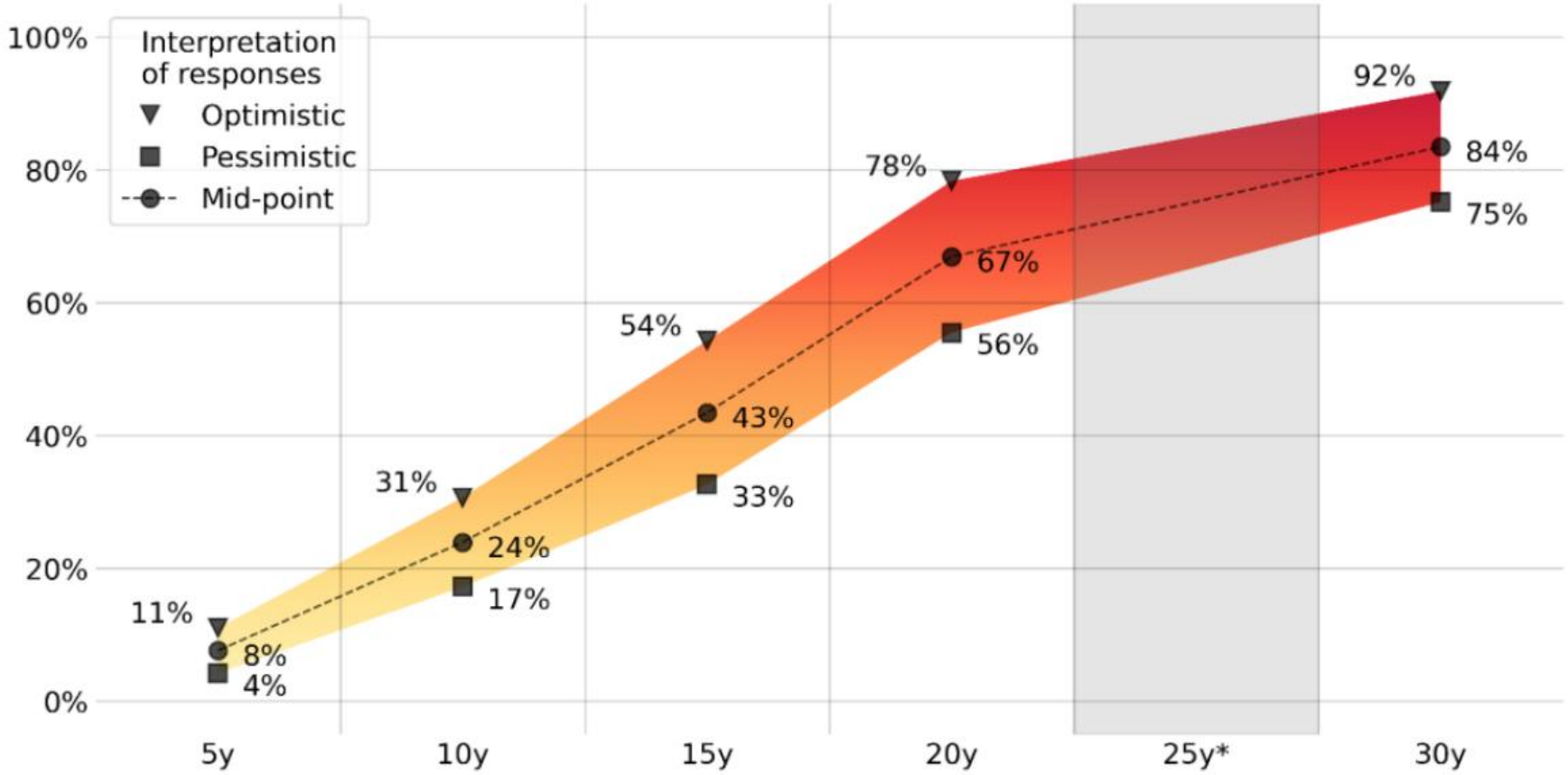
- Why we care today
- Cryptography Crash Course
- Quantum Computers
- Shor’s Algorithms
- Lattice based cryptography
- Way Forward
- Takeaways



Why we care today

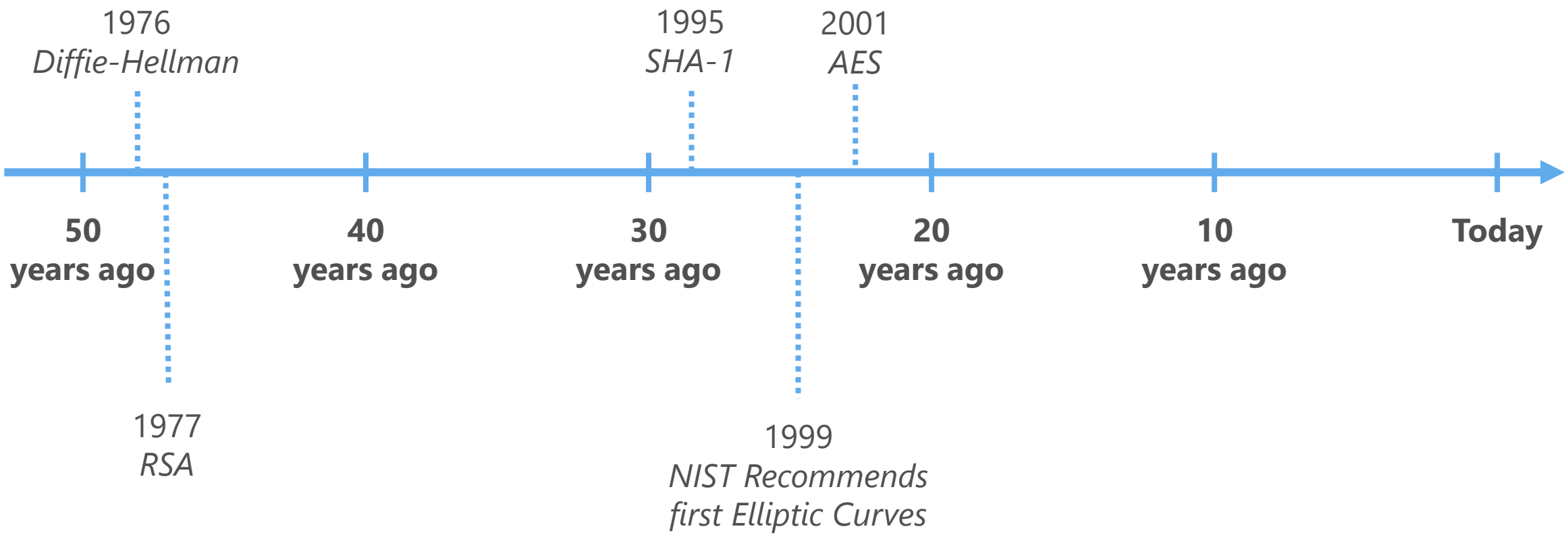
Why we care today

Expert predictions



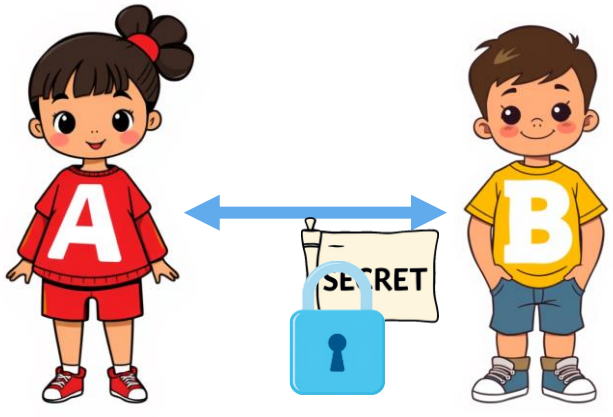
Report

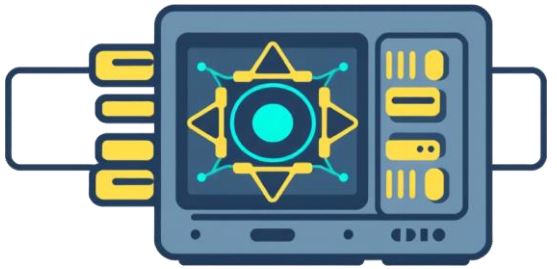
Time Flies

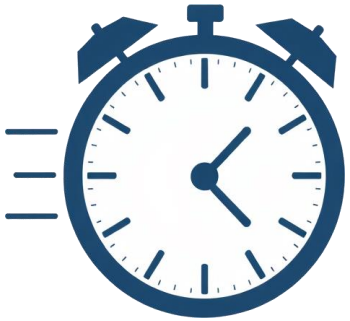


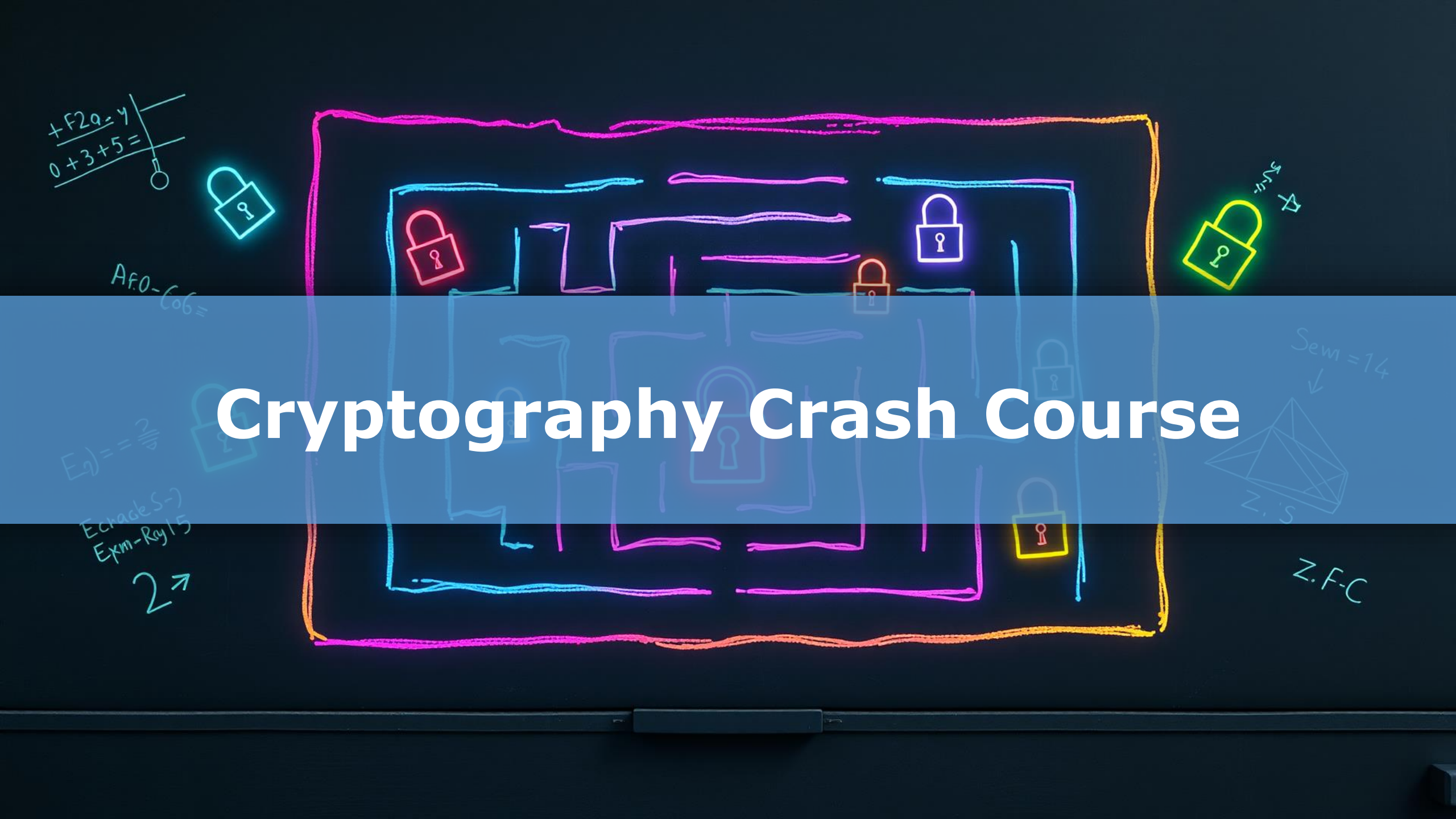
Why we care today

Store now, decrypt later







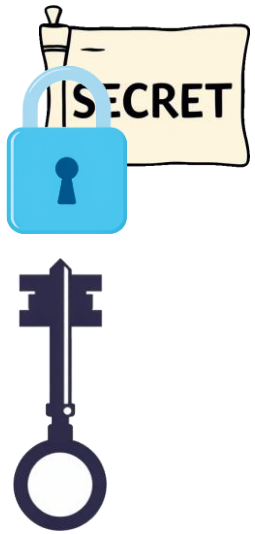

Cryptography Crash Course

Unkeyed

feb6
541d
492a

- MD5
- SHA
- Argon2

Symmetric



- AES
- ChaCha20
- HMAC

Asymmetric

- **RSA**
- **DH**
- **DSA**

Diffie-Hellman Key Exchange

g, p

$g^a \bmod p = A$

$B^a \bmod p = g^{ab} \bmod p = S$

A

B

g, p

$g^b \bmod p = B$

$A^b \bmod p = g^{ab} \bmod p = S$

g, p

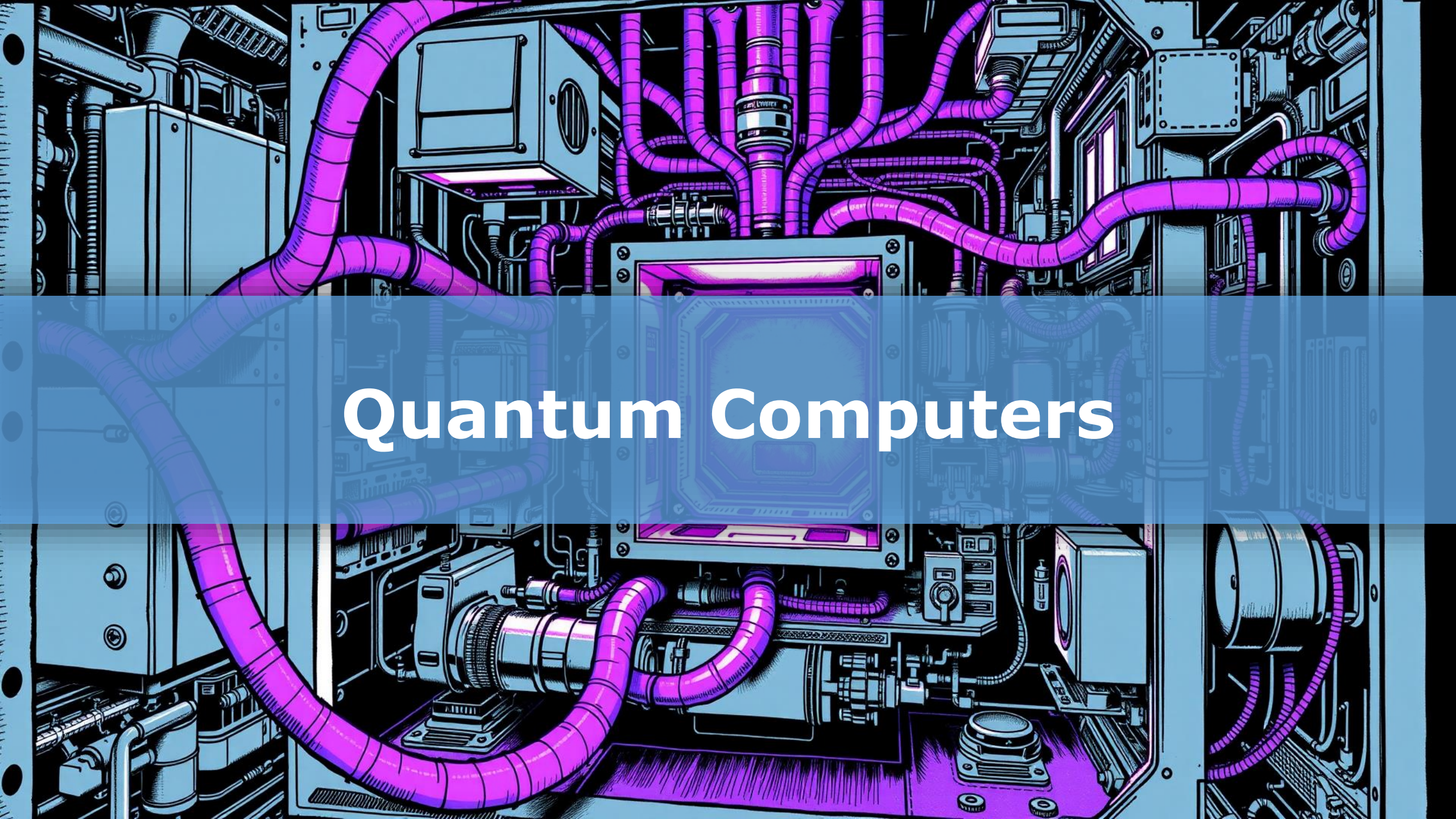
A, B

Discrete Logarithm Problem:

$g^a \bmod p = A \nrightarrow a$

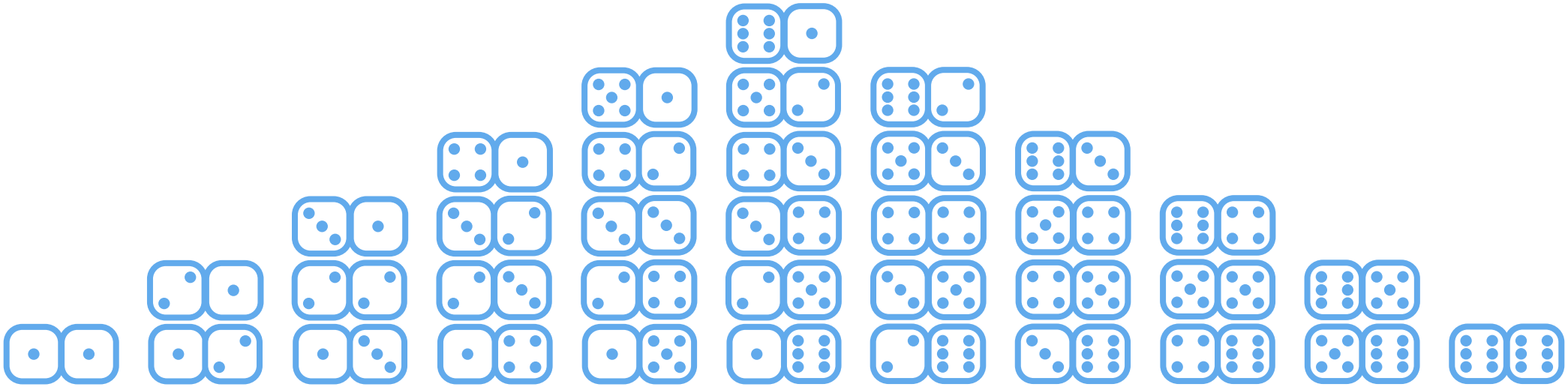
$g^b \bmod p = B \nrightarrow b$

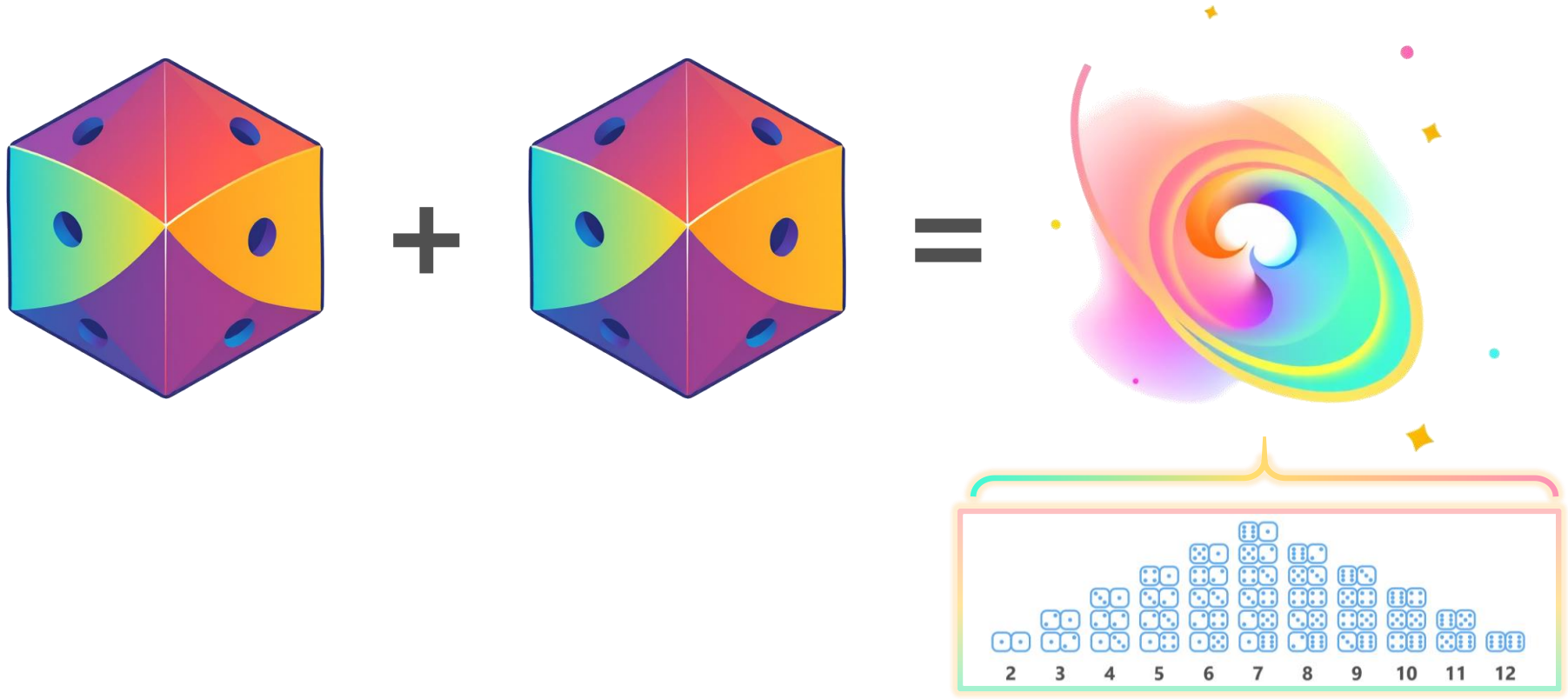
Paper

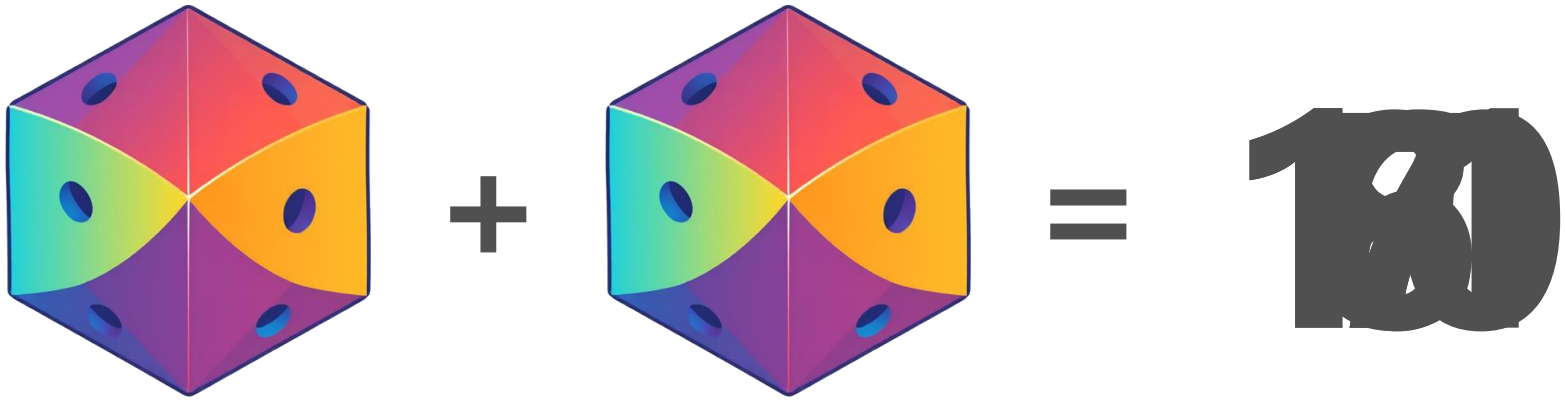


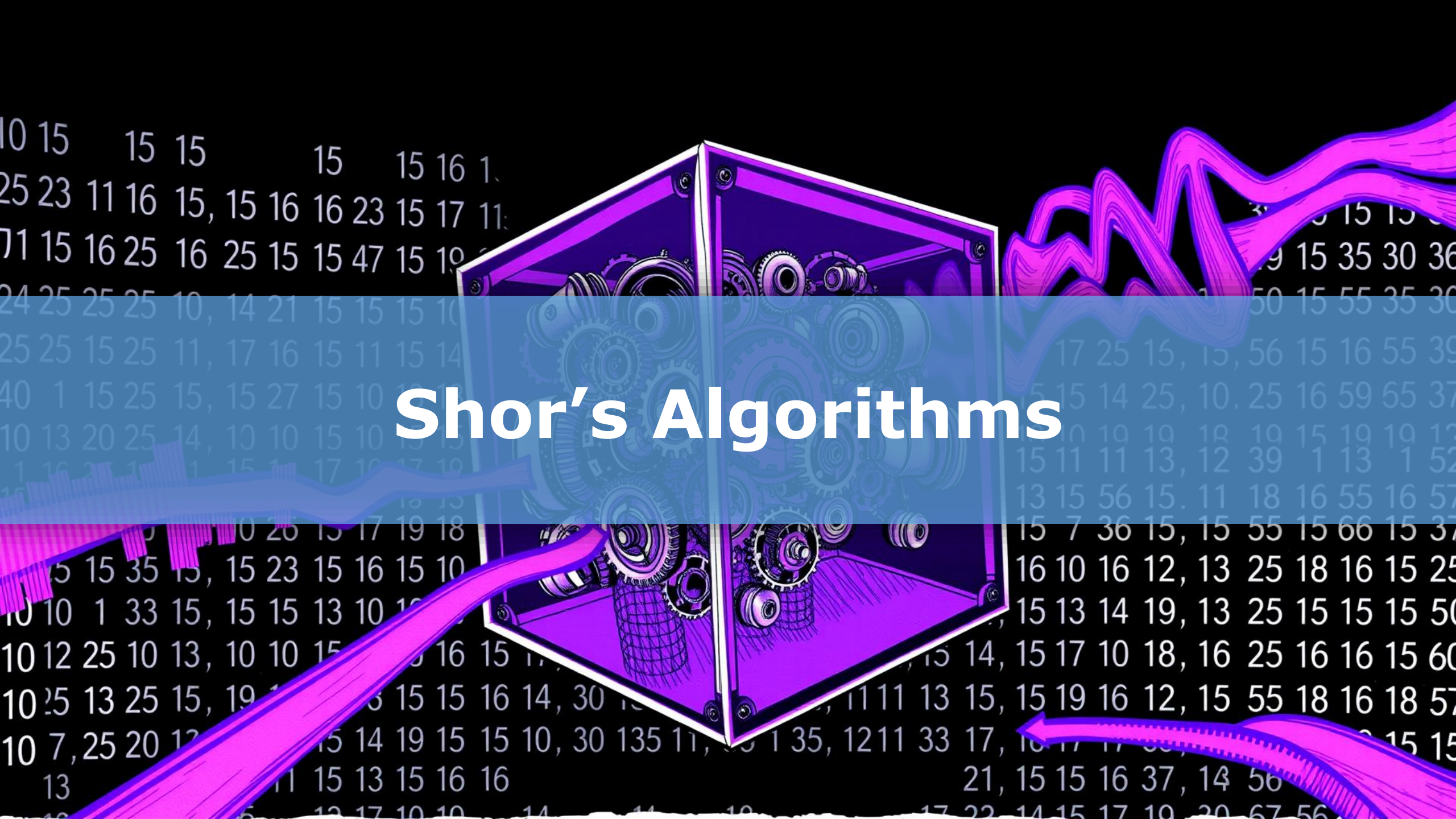
Quantum Computers

Classical Computers are slow









Shor’s Algorithms

$$g^x \bmod N = 1$$

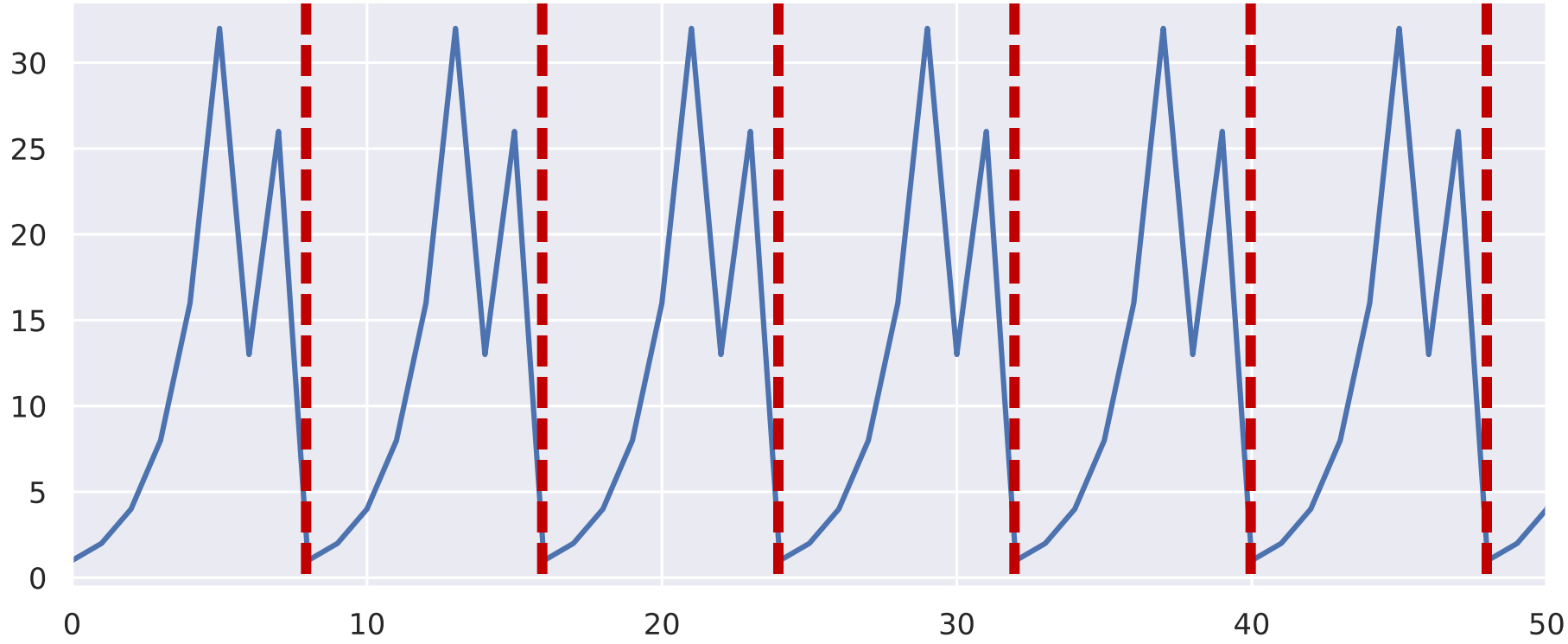
Finding a non-trivial solution.

$2^0 \mod 51 = 1$
$2^1 \mod 51 = 2$
$2^2 \mod 51 = 4$
$2^3 \mod 51 = 8$
$2^4 \mod 51 = 16$
$2^5 \mod 51 = 32$
$2^6 \mod 51 = 13$
$2^7 \mod 51 = 26$

$2^8 \mod 51 = 1$
$2^9 \mod 51 = 2$
$2^{10} \mod 51 = 4$
$2^{11} \mod 51 = 8$
$2^{12} \mod 51 = 16$
$2^{13} \mod 51 = 32$
$2^{14} \mod 51 = 13$
$2^{15} \mod 51 = 26$

$2^x \bmod 51$

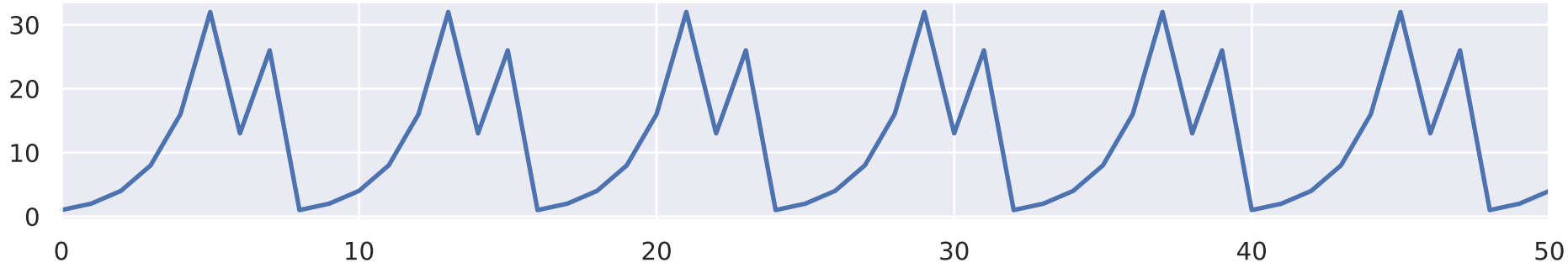
period = 8



Fourier Transform

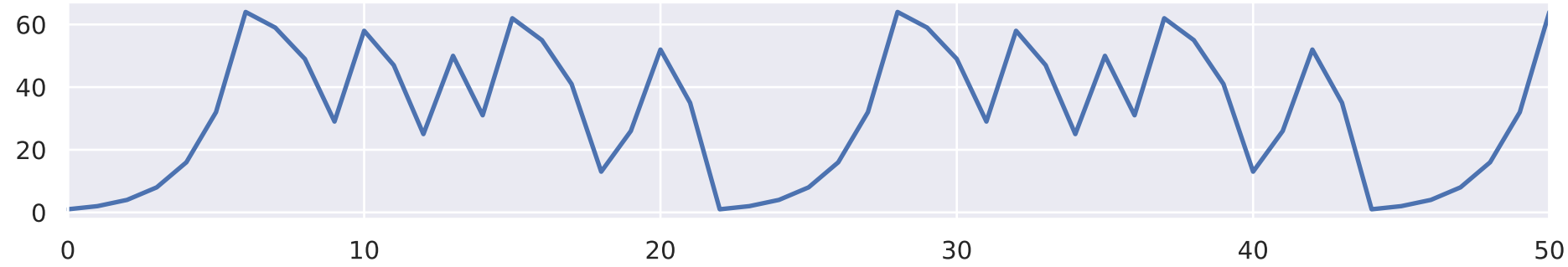
$2^x \bmod 51$

period = 8



$2^x \bmod 69$

period = 22



$2^{x} \bmod 51 =$ 

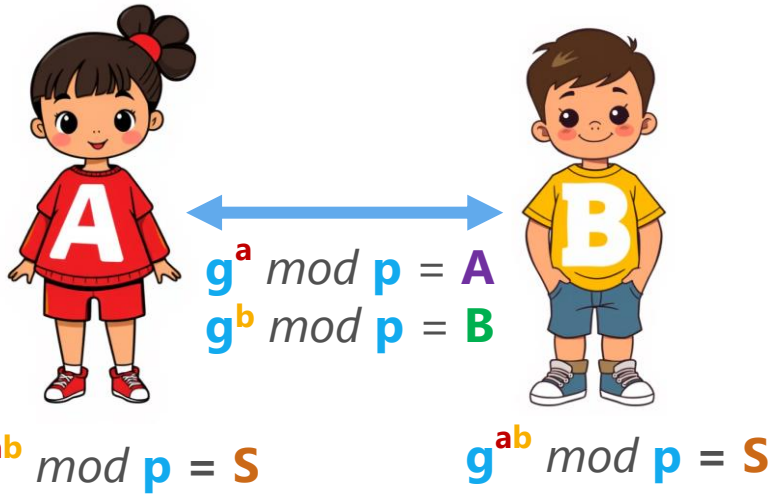
FourierTransform()

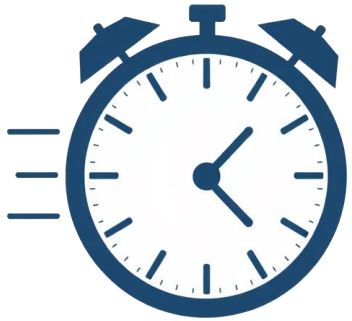
1/8

→ period = 8 → **x = 8**

Fourier

Breaking Diffie-Hellman





$g^{?} \bmod p =$ 

FourierTransform()

→ **a**

→ $B^a \bmod p = S$

Shor DL

Shor's Algorithms

What it can break

Algorithms for quantum computation: discrete logarithms and factoring

Peter W. Shor, 1994

Breaks algorithms relying on discrete logarithms (DH, DSA) and those based on factoring (RSA)

integer to be factored. [...]

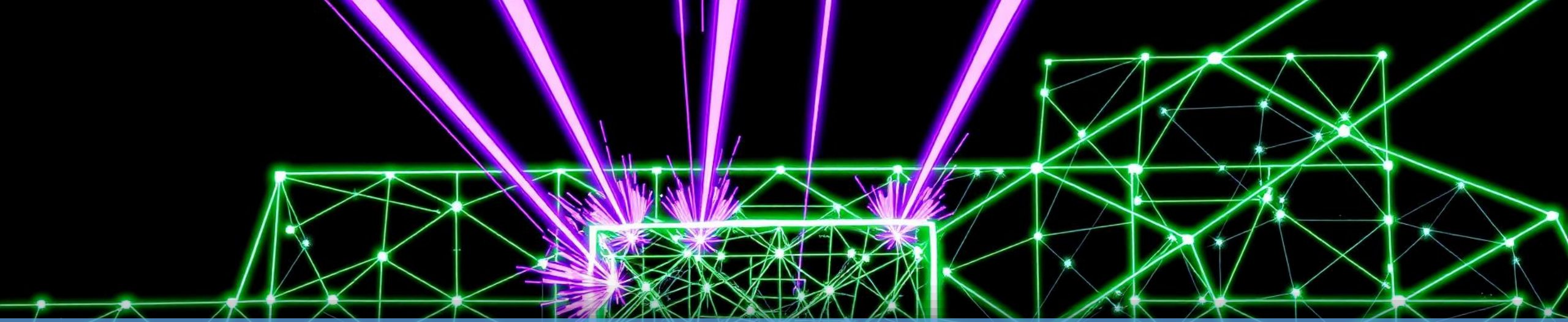
Shor's discrete logarithm quantum algorithm for elliptic curves

John Proos and Christof Zalka, 2003

Extends Shor's algorithm to break Elliptic curve-based cryptography as well (ECDH, ECDSA)

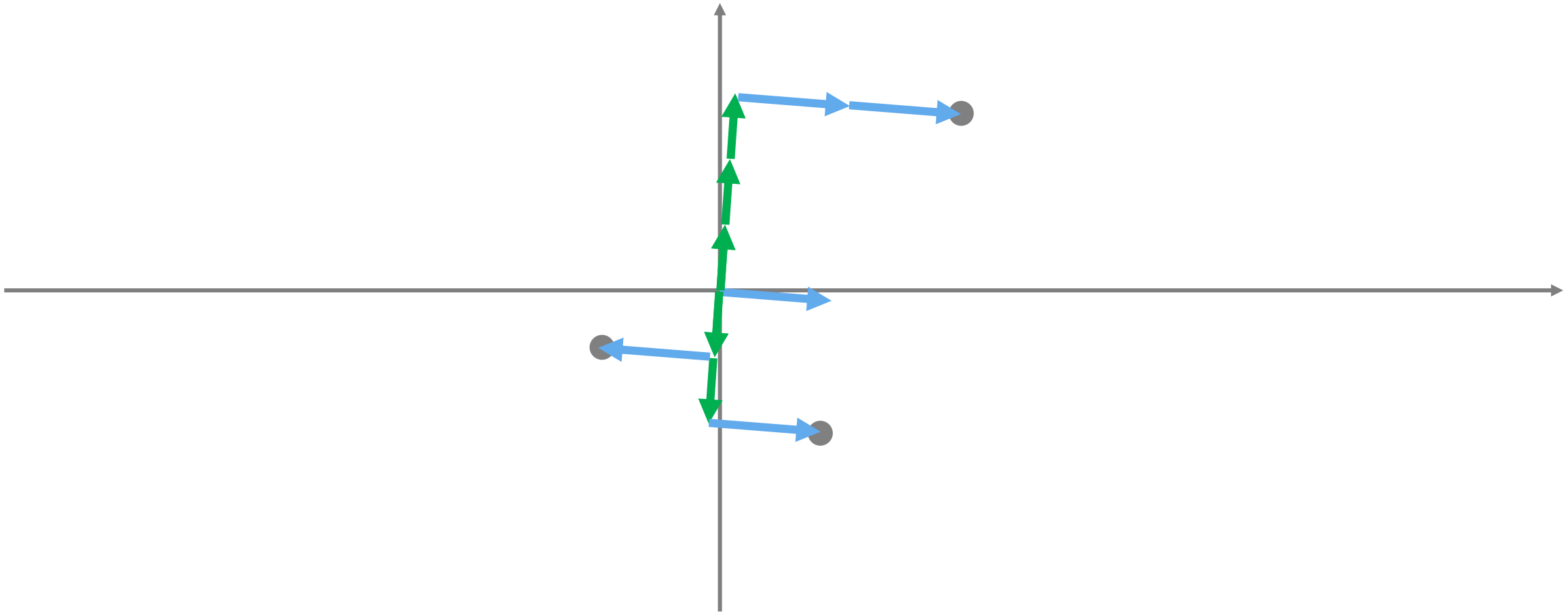
Proos

Shor

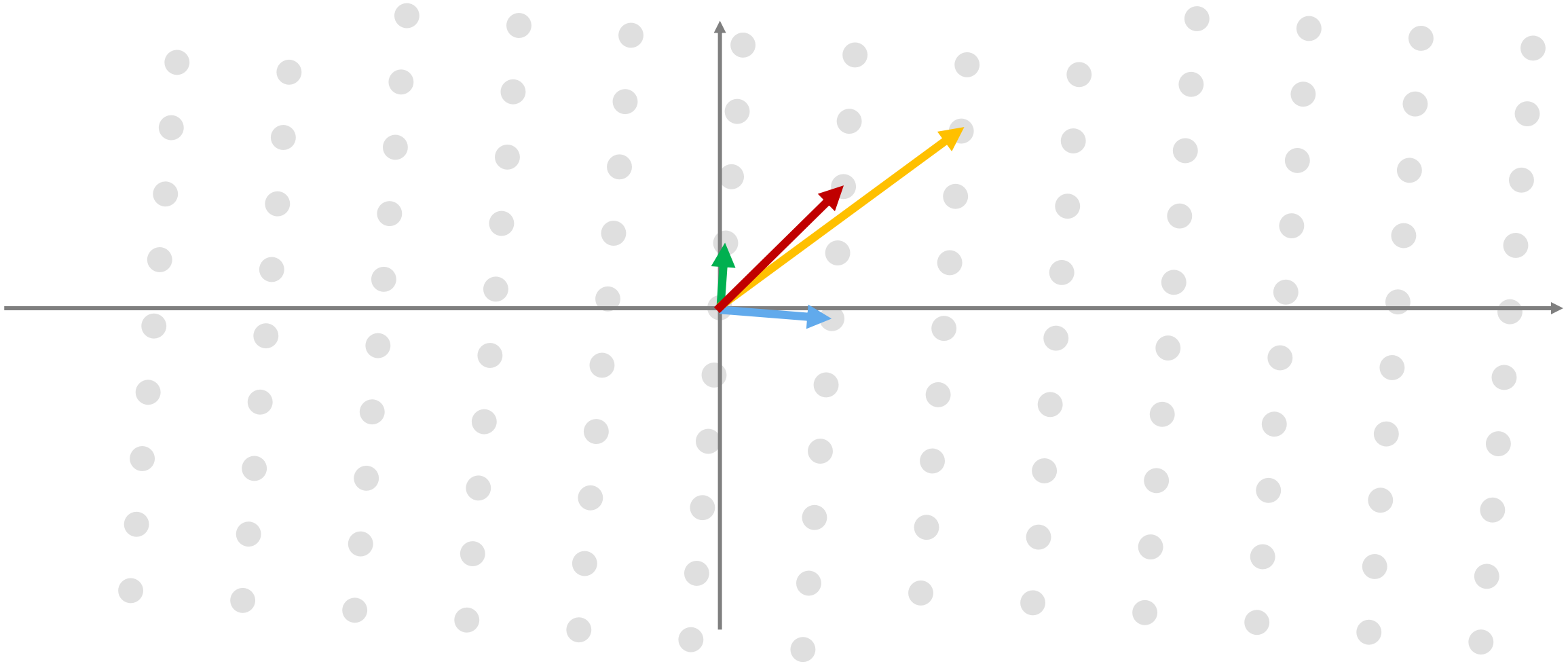


Lattice Based Cryptography

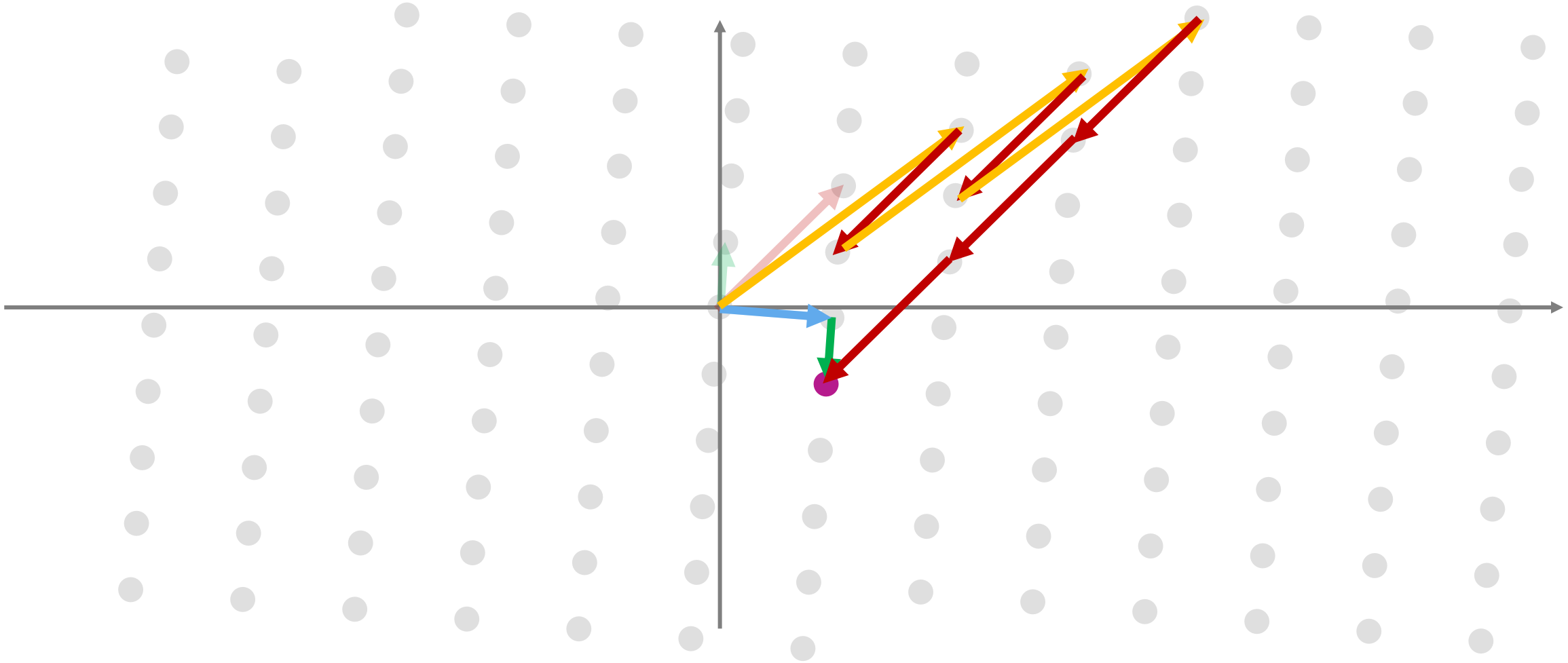
Creating a Lattice from basis vectors



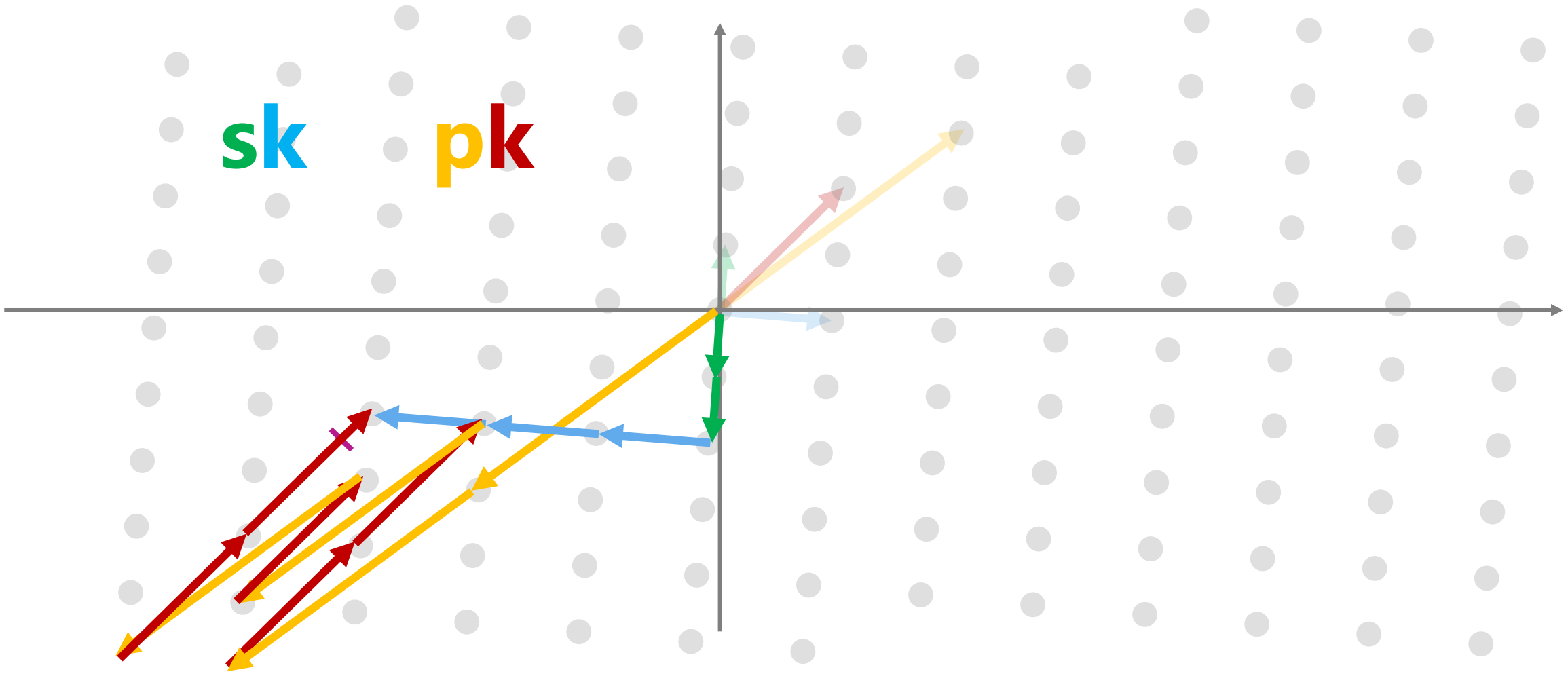
Creating a lattice from basis vectors



Not all basis vectors are nice



Closest vector problem



Way forward

Finalized Asymmetric Algorithms

ML-KEM
(CRYSTALS-Kyber)

ML-DSA
(CRYSTALS-Dilithium)

SLH-DSA
(Sphincs+)

Quantum Algorithms for Lattice Problems

Yilei Chen, April 10, 2024

The attack algorithm contains a bug and does not work. Close call!

KyberSlash: Exploiting secret-dependent division timings in Kyber implementations

Bernstein et al., June 28, 2024

Algorithm itself is not vulnerable, but most implementations were. Can and has been fixed in many libraries.

KyberSlash

Preprint

Hybrid Mode

S_{DH}

$S_{ML\text{-}KEM}$

DH

ML-KEM

S_{DH}

$S_{ML\text{-}KEM}$

S_{DH} $S_{ML\text{-}KEM}$

Secret

S_{DH} $S_{ML\text{-}KEM}$

Secret

Hybrid Mode in Signal Protocol

S_{DH}

$S_{ML\text{-}KEM}$

DH

ML-KEM

S_{DH}

$S_{ML\text{-}KEM}$

S_{DH} $S_{ML\text{-}KEM}$

Secret

S_{DH} $S_{ML\text{-}KEM}$

Secret

Signal

Symmetric Cryptography

AES-256 ***SHA3***

Argon2 ***ChaCha20***

Asymmetric Encryption

RSA, DH

hybrid

ML-KEM

Digital Signatures

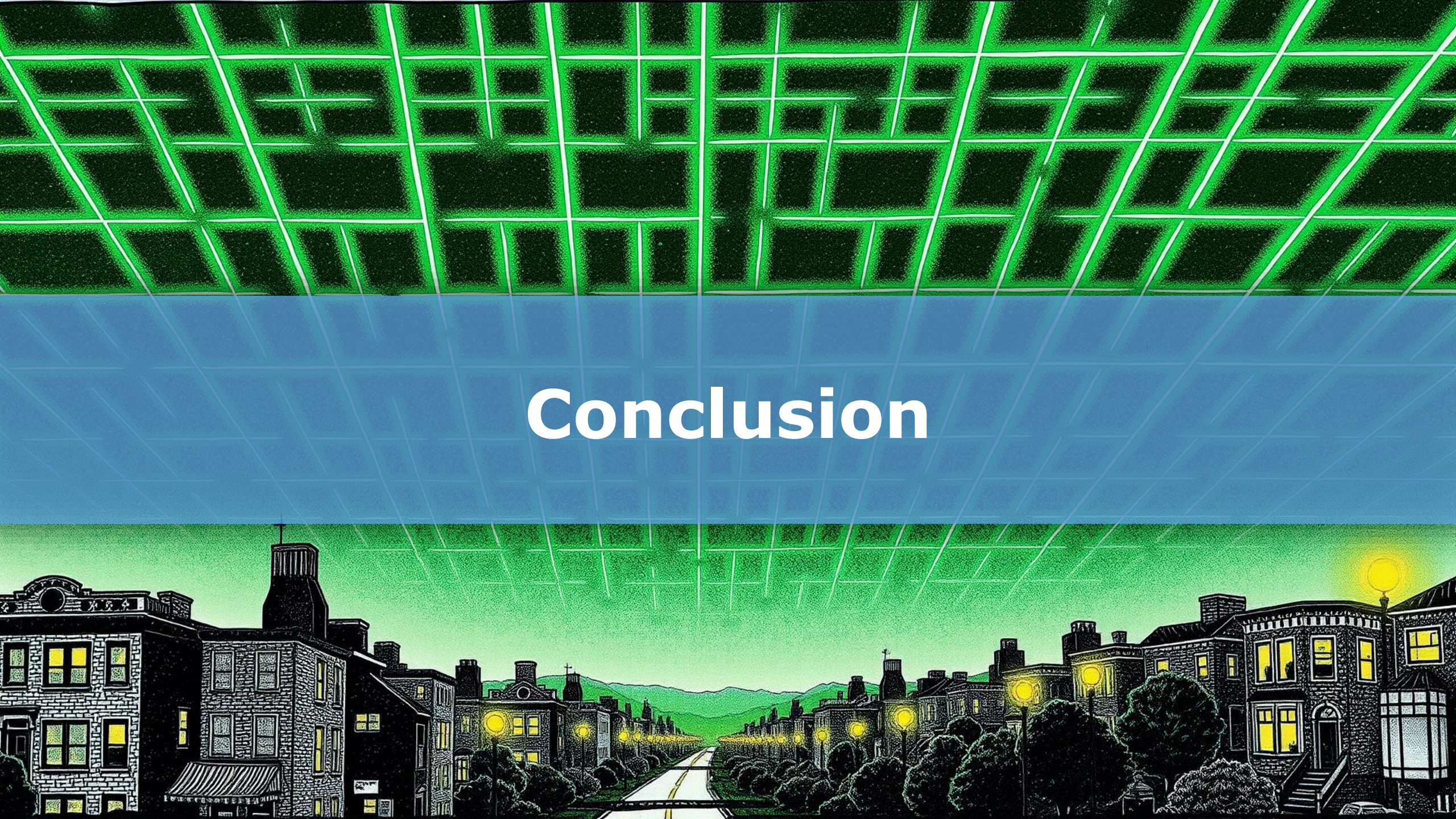
DSA

hybrid

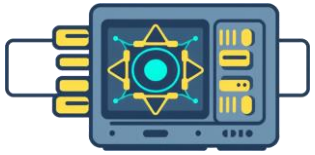
ML-DSA, SLH-DSA

2000 2010 2020 2030 2040 2050

Conclusion

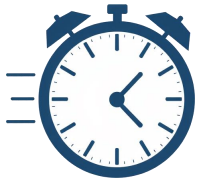


Takeaways



Quantum Computers are not magically fast at everything

Mostly asymmetric cryptographic algorithms are affected.

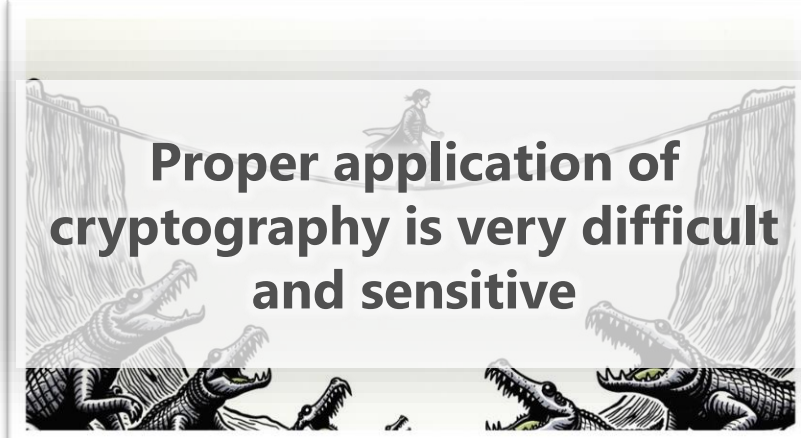


Start migration now because of “store now decrypt later” and long software lifecycles

Use new algorithms in hybrid mode with classical scheme for now

General Remarks

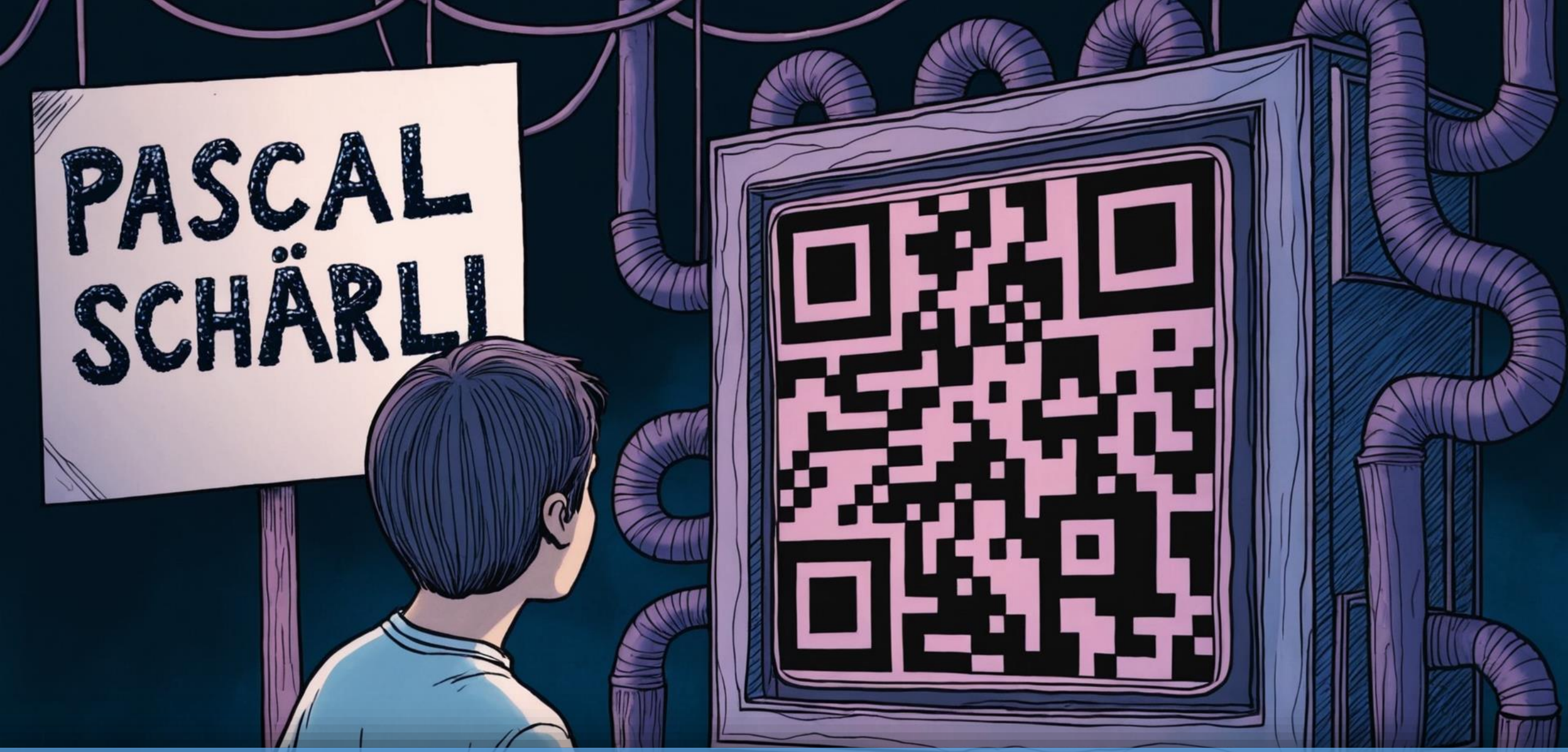
Proper application of cryptography is very difficult and sensitive



Consult with experts when working with cryptography

Secure Algorithms don’t make a secure protocol

Don’t rely on security through obscurity



Thank You!