An overview of post-quantum cryptography

Monika Trimoska

Security in Times of Surveillance 2024
May 31, Eindhoven

TU/e

*Animated version at: https://mtrimoska.com/slides/PQC_May_31/index.html

Post-quantum cryptography

Implemented on a classical, but resistant to attacks on a quantum computer.

- Shor's quantum algorithm: solves integer factorisation and discrete logarithms in abelian groups in polynomial time.
  - All* currently deployed public-key cryptosystems would be broken by an adversary in possession of a large quantum computer.
  - All public-key cryptosystems need to be replaced.

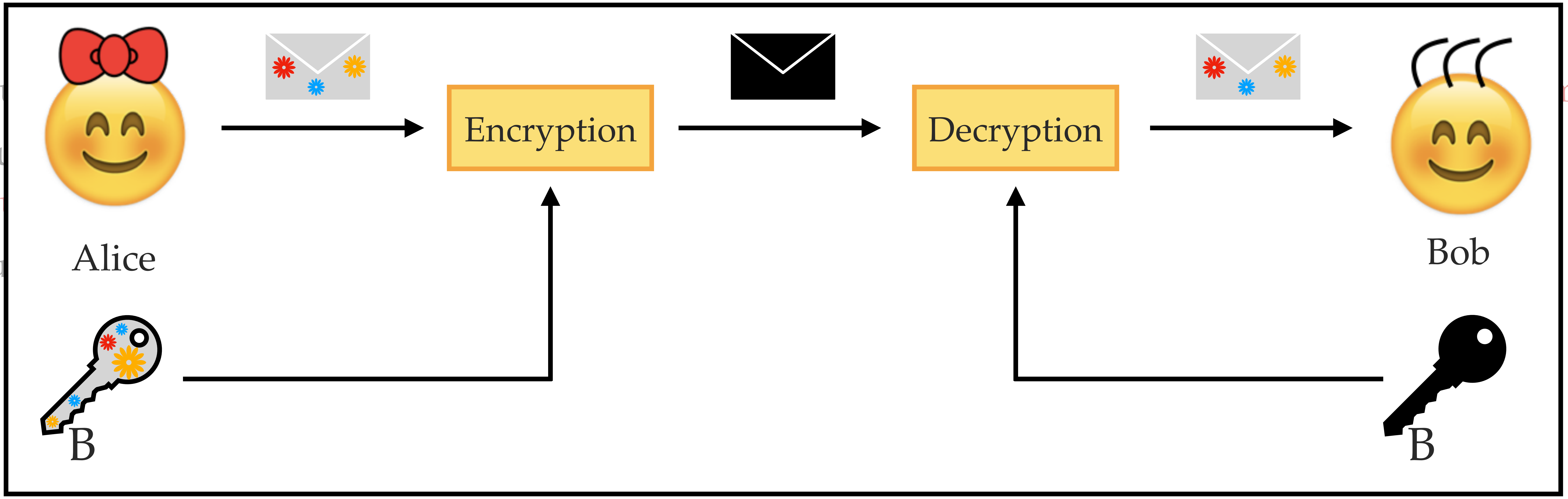
Post-quantum cryptography

Implemented on a classical, but resistant to attacks on a quantum computer.

- Shor's quant
  - All* cu
    quant
  - All pu

nial time.

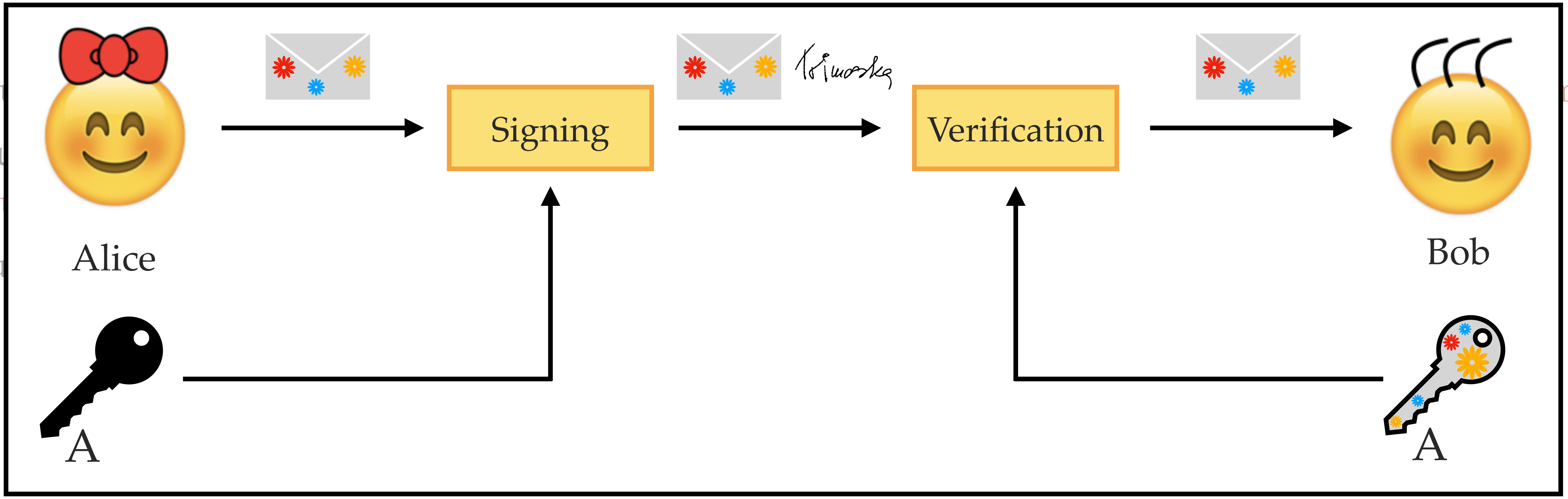
a large



Post-quantum cryptography

Implemented on a classical, but resistant to attacks on a quantum computer.

- Shor's quant… …nial time.
  - All* c… …a large quant…
  - All pu…



Post-quantum cryptography

Implemented on a classical, but resistant to attacks on a quantum computer.

- Shor's quantum algorithm: solves integer factorisation and discrete logarithms in abelian groups in polynomial time.
  - All* currently deployed public-key cryptosystems would be broken by an adversary in possession of a large quantum computer.
  - All public-key cryptosystems need to be replaced.
  - If the public-key cryptography component is broken, the entire infrastructure is broken because the handshake is compromised.
- Grover's quantum algorithm: quadratic speedup of exhaustive search.
  - Impact on symmetric cryptography (as a rule of thumb): double the key sizes.

Computationally hard problems

Discrete log problem

Travelling salesman problem

MQ (multivariate quadratic) problem

Isomorphism of polynomials problem

Boolean satisfiability problem

Code equivalence problem

Integer factorisation problem

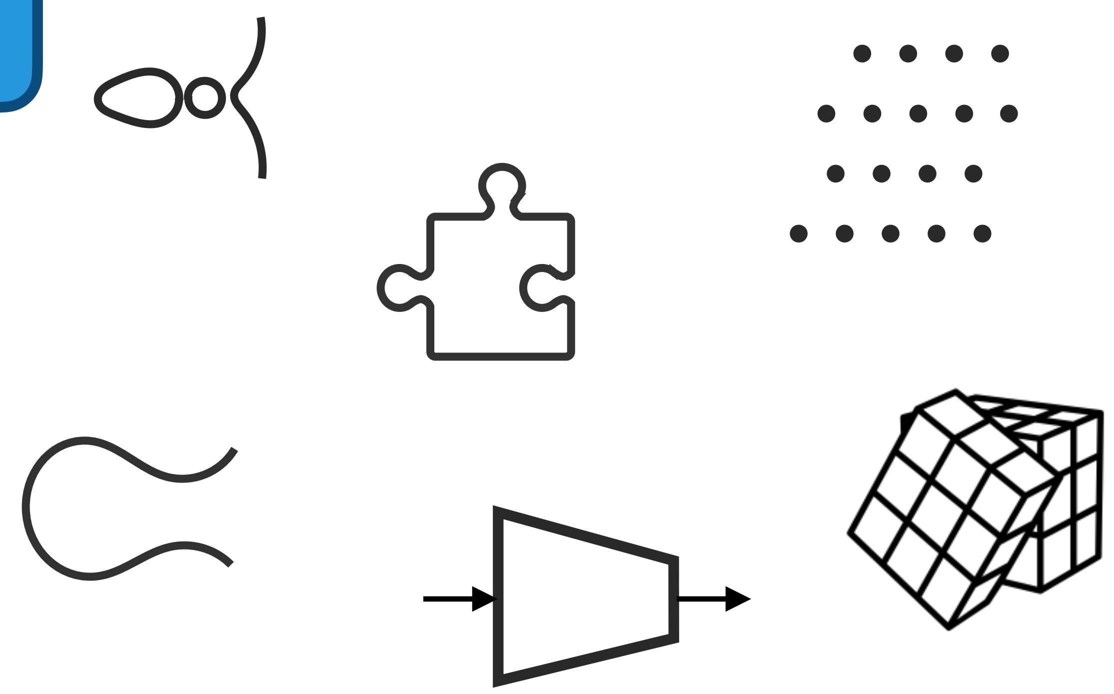
Graph colouring problem

Syndrome decoding problem

Isogeny path problem

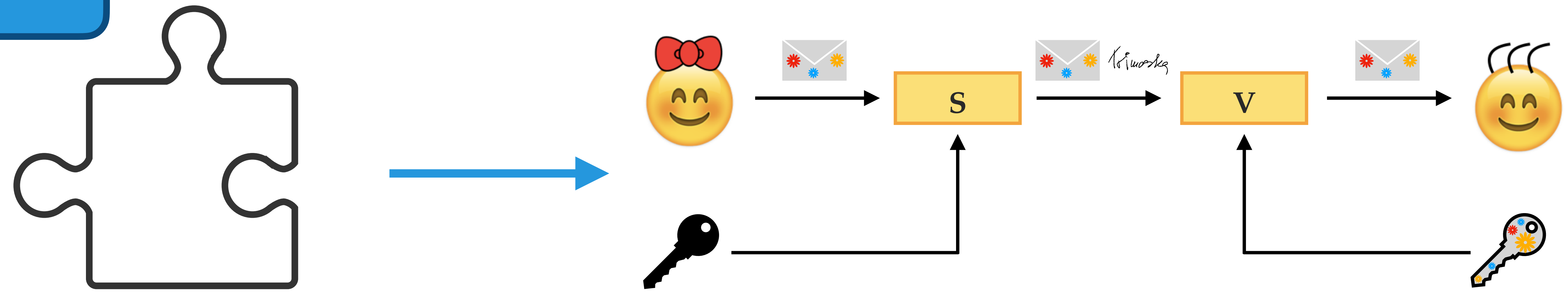
In this talk

1



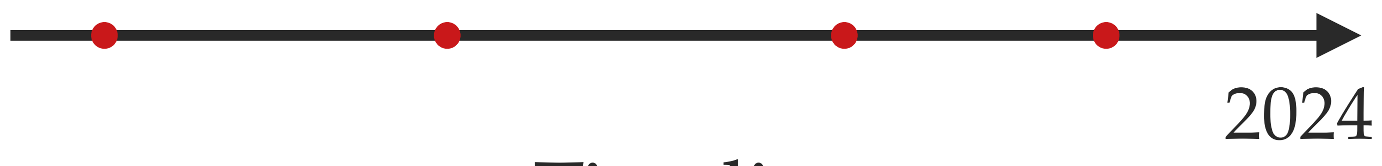
The different flavours of PQC

2



Cryptographic design example

3



Timeline

The different flavours of PQC

PQC families

Hash-based cryptography

Multivariate cryptography

Code-based cryptography

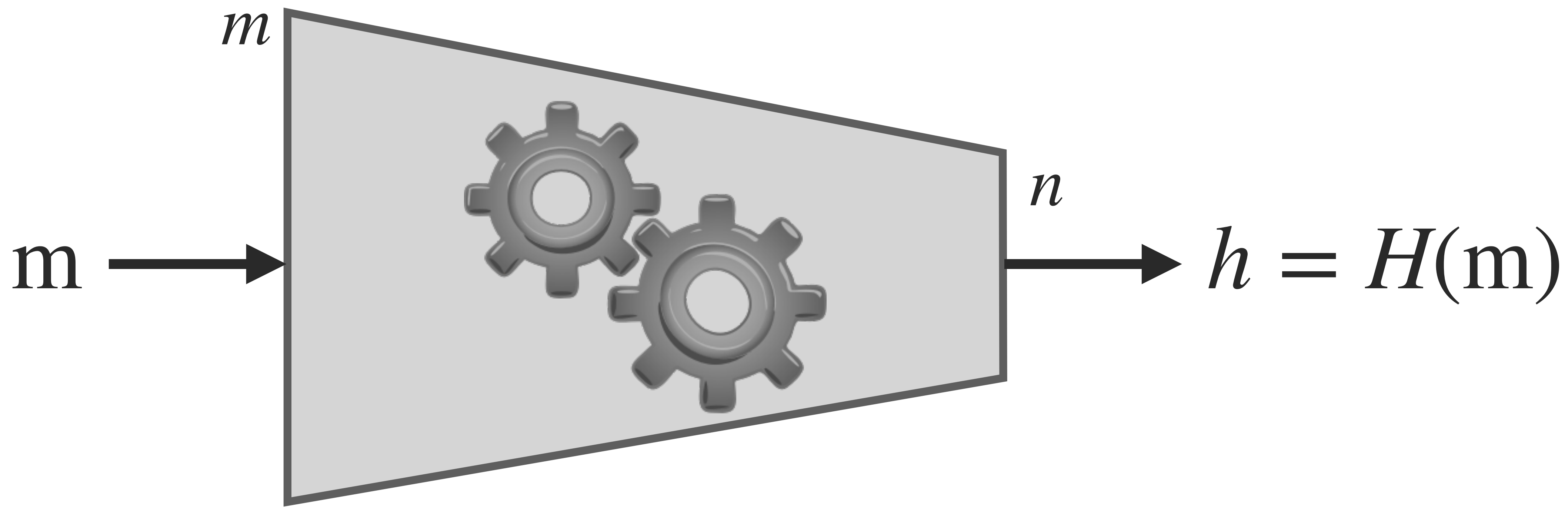
Lattice-based cryptography

Isogeny-based cryptography

Hash-based cryptography

Hash-based cryptography

Worst-case complexity: $\mathcal{O}(2^n)$



Hard problem: find a pre-image of h.

Used to build digital signature schemes with only one security assumption.

Multivariate cryptography

Multivariate cryptography

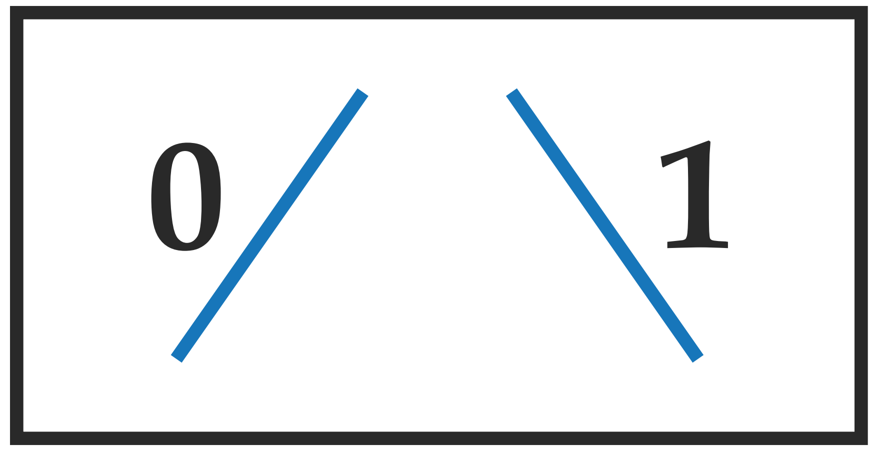
The MQ problem

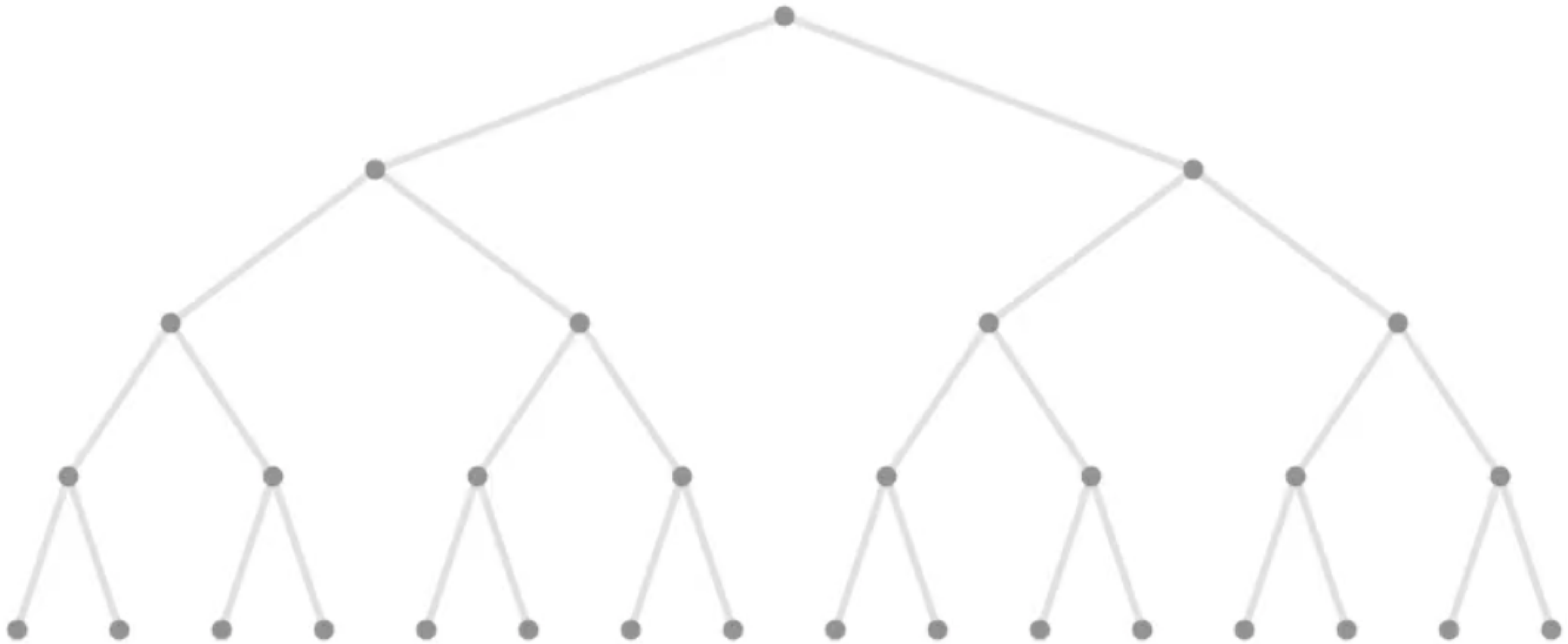
Input: m multivariate quadratic polynomials $f_1, \ldots, f_m$ of n variables over a finite field $\mathbb{F}_q$.
Question: find a tuple $\mathbf{x} = (x_1, \ldots, x_n)$ in $\mathbb{F}_q^n$, such that $f_1(\mathbf{x}) = \ldots = f_m(\mathbf{x}) = 0$.

Example.

$$f_1 : x_1x_3 + x_2x_4 + x_1 + x_3 + x_4 = 0$$
$$f_2 : x_2x_3 + x_1x_4 + x_3x_4 + x_1 + x_2 + x_4 = 0$$
$$f_3 : x_2x_4 + x_3x_4 + x_1 + x_3 + 1 = 0$$
$$f_4 : x_1x_2 + x_1x_3 + x_2x_3 + x_3 + x_4 + 1 = 0$$
$$f_5 : x_1x_2 + x_2x_3 + x_1x_4 + x_3 = 0$$
$$f_6 : x_1x_3 + x_1x_4 + x_3x_4 + x_1 + x_2 + x_3 + x_4 = 0$$

Multivariate cryptography





Binary search tree

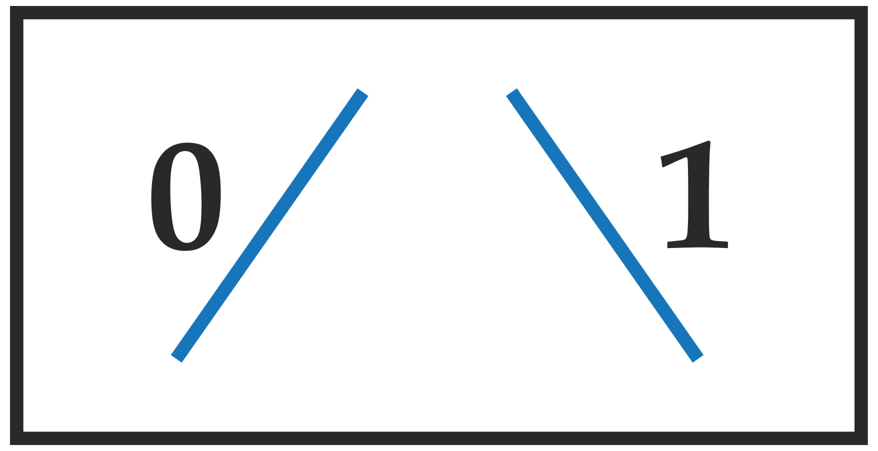
$$x_1 \cdot x_2 + x_1 \cdot x_3 + x_3 \cdot x_4 + x_3 = 0$$

$$x_2 \cdot x_3 + x_2 \cdot x_4 + x_1 + x_2 + 1 = 0$$

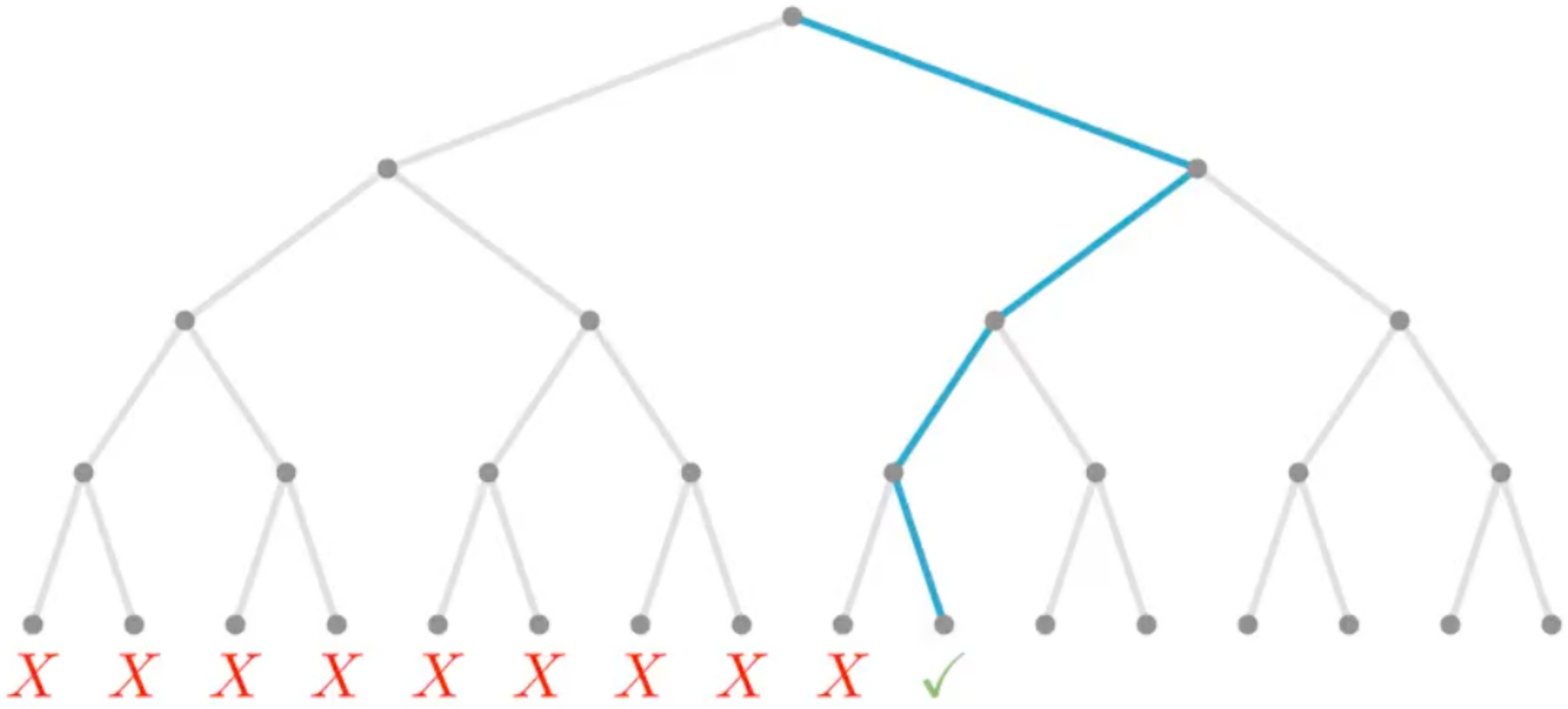
$$x_1 \cdot x_2 + x_2 \cdot x_3 + x_2 \cdot x_4 + x_1 + x_4 = 0$$

$$x_1 \cdot x_4 + x_2 \cdot x_3 + x_2 + x_3 + x_4 = 0$$

Multivariate cryptography



Worst-case complexity: $\mathcal{O}(2^n)$

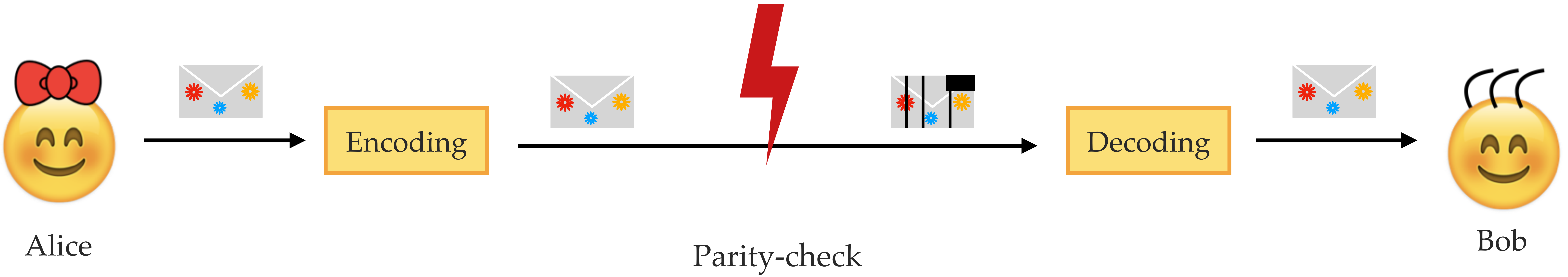


$$1 \cdot 0 + 1 \cdot 0 + 0 \cdot 1 + 0 = 0$$
$$0 \cdot 0 + 0 \cdot 1 + 1 + 0 + 1 = 0$$
$$1 \cdot 0 + 0 \cdot 0 + 0 \cdot 1 + 1 + 1 = 0$$
$$1 \cdot 1 + 0 \cdot 0 + 0 + 0 + 1 = 0$$

Binary search tree

Code-based cryptography

Code-based cryptography



Parity-check matrix

Codeword: it is in the kernel of $\mathbf{H}$

$$\mathbf{Hc} = \mathbf{0}$$

Small error: Hamming weight is t

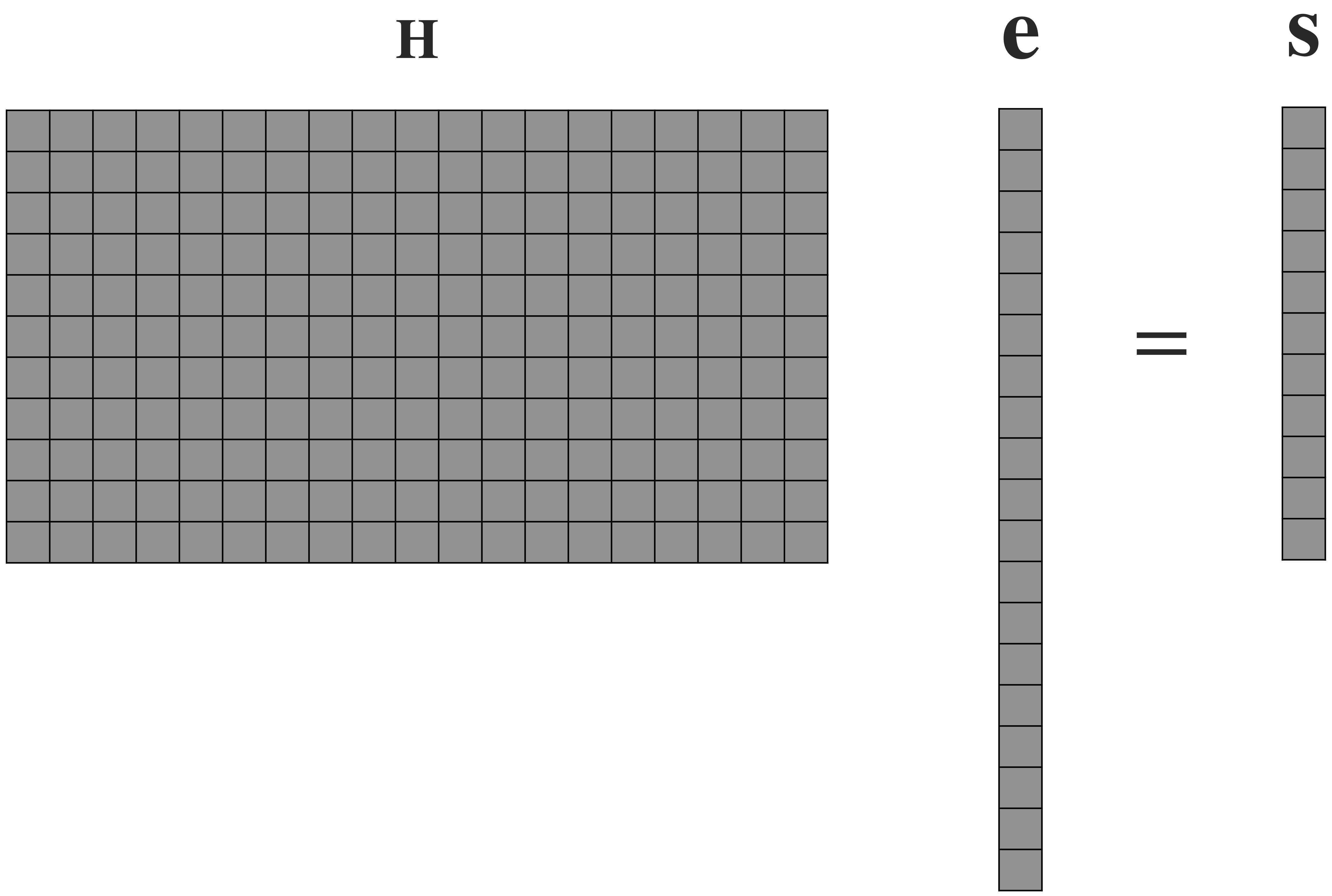
Syndrome: depends only on the error vector.

$$\mathbf{H}(\mathbf{c} + \mathbf{e}) = \mathbf{Hc} + \mathbf{He} = \mathbf{0} + \mathbf{He} = \mathbf{He} = \mathbf{s}$$

The syndrome decoding problem

Given a syndrome $\mathbf{s} = \mathbf{He}$, find $\mathbf{e}$ such that $\mathrm{wt}(\mathbf{e}) = t$.

Code-based cryptography



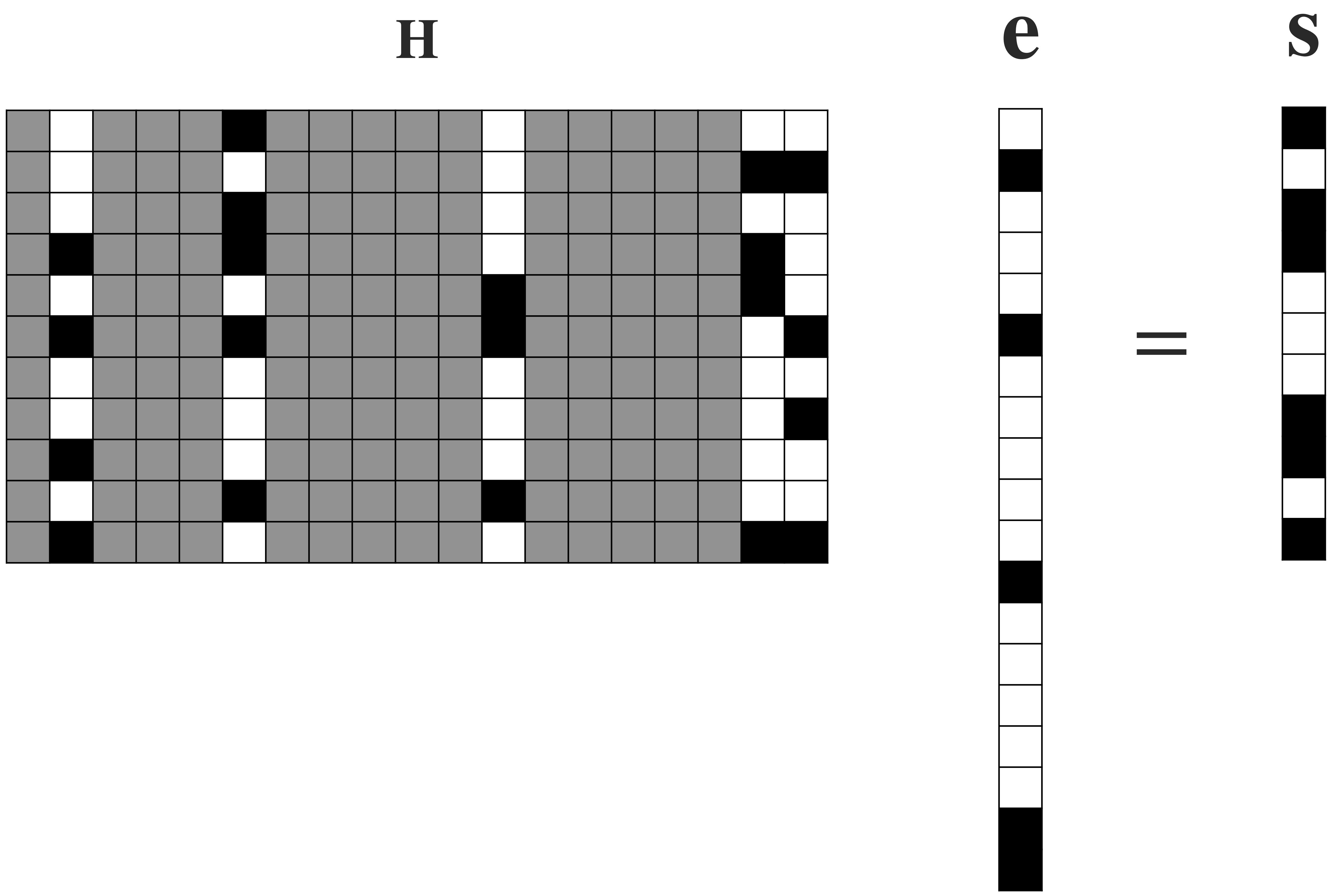
Entry is 0

Entry is 1

Entry is 0 or 1

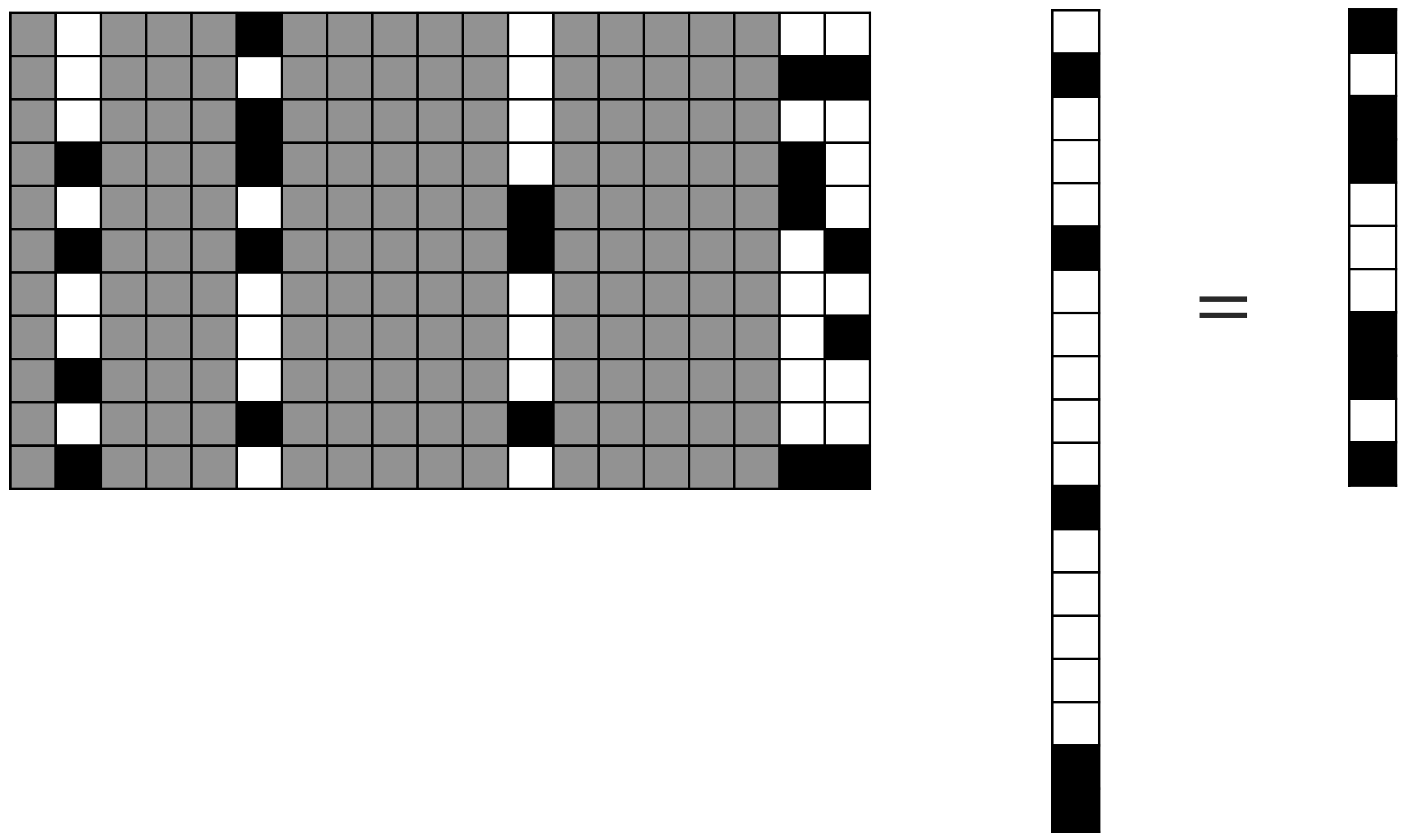
Code-based cryptography

- Entry is 0
- Entry is 1
- Entry is 0 or 1



s is equal to the sum of the columns where e_i is nonzero.

Code-based cryptography

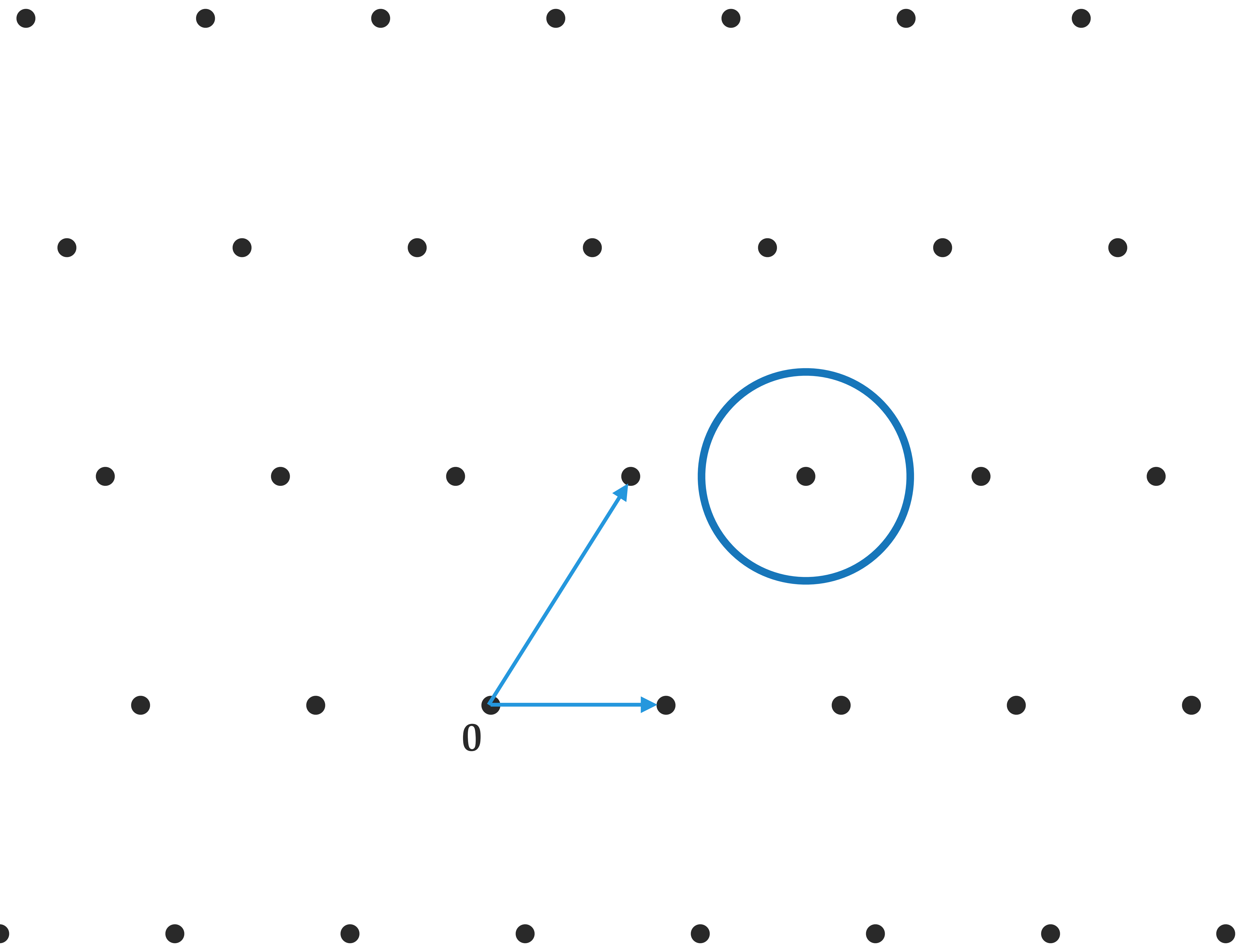


Pick any group of t columns of $\mathbf{H}$, add them and compare with $\mathbf{s}$.

Cost: $\binom{n}{t}$ sums of t columns.

Lattice-based cryptography

Lattice-based cryptography



A lattice $L \subset \mathbb{R}^n$ is a discrete subgroup of $\mathbb{R}^n$.

→ dots: points on the lattice $\mathbf{c} \in L$.

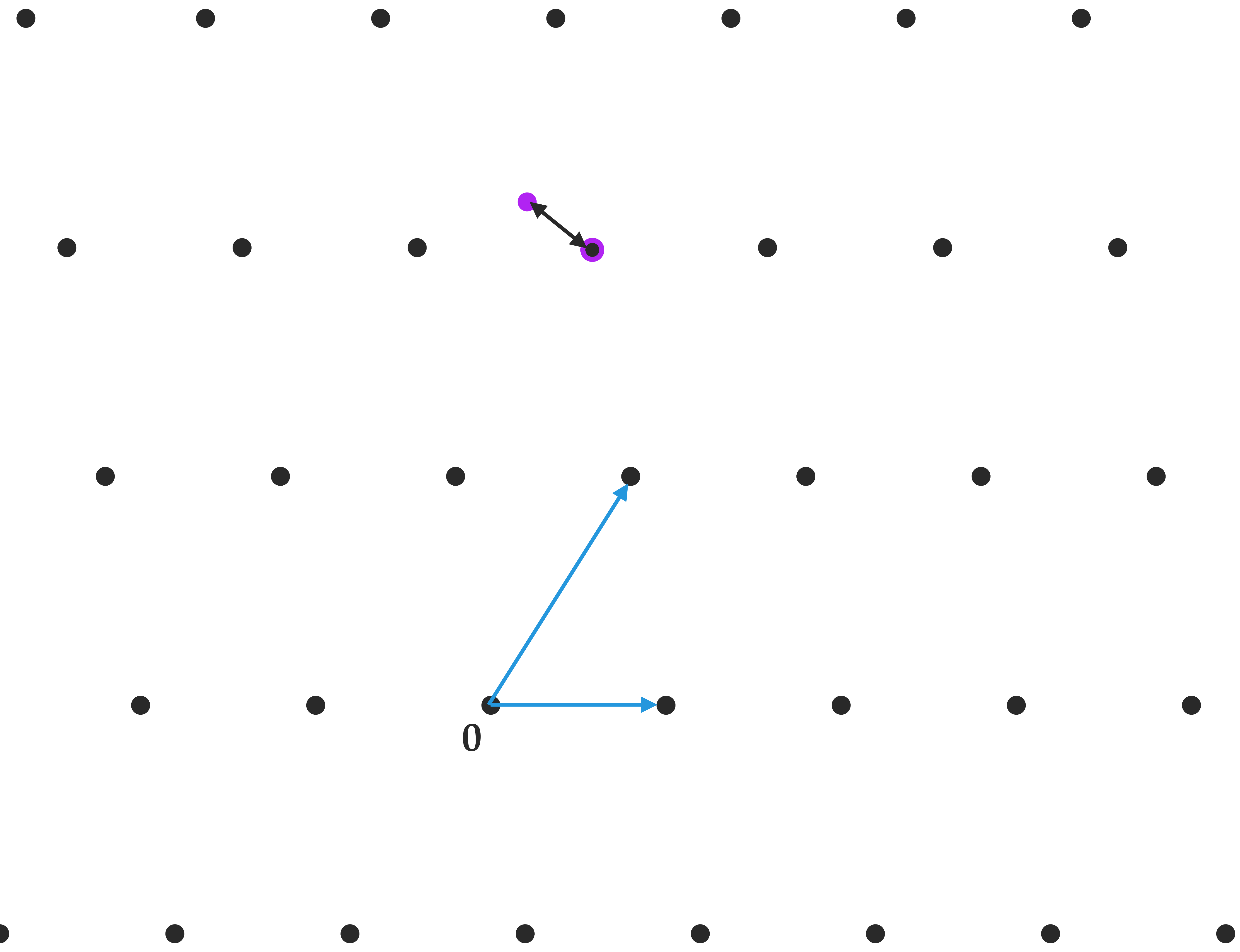
for every $\mathbf{v} \in L$, there exists an open ball around $\mathbf{v}$ that contains no other elements from L.

Lattice basis: n $\mathbb{R}$-linearly independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$

$$L := \{ \sum_{i=1}^{n} a_i \mathbf{b}_i \mid a_i \in \mathbb{Z} \}$$

$$\mathbf{B} = \begin{pmatrix} \mathbf{b}_1 \\ \mathbf{b}_2 \end{pmatrix} = \begin{pmatrix} 4 & 0 \\ 3 & 5 \end{pmatrix}$$

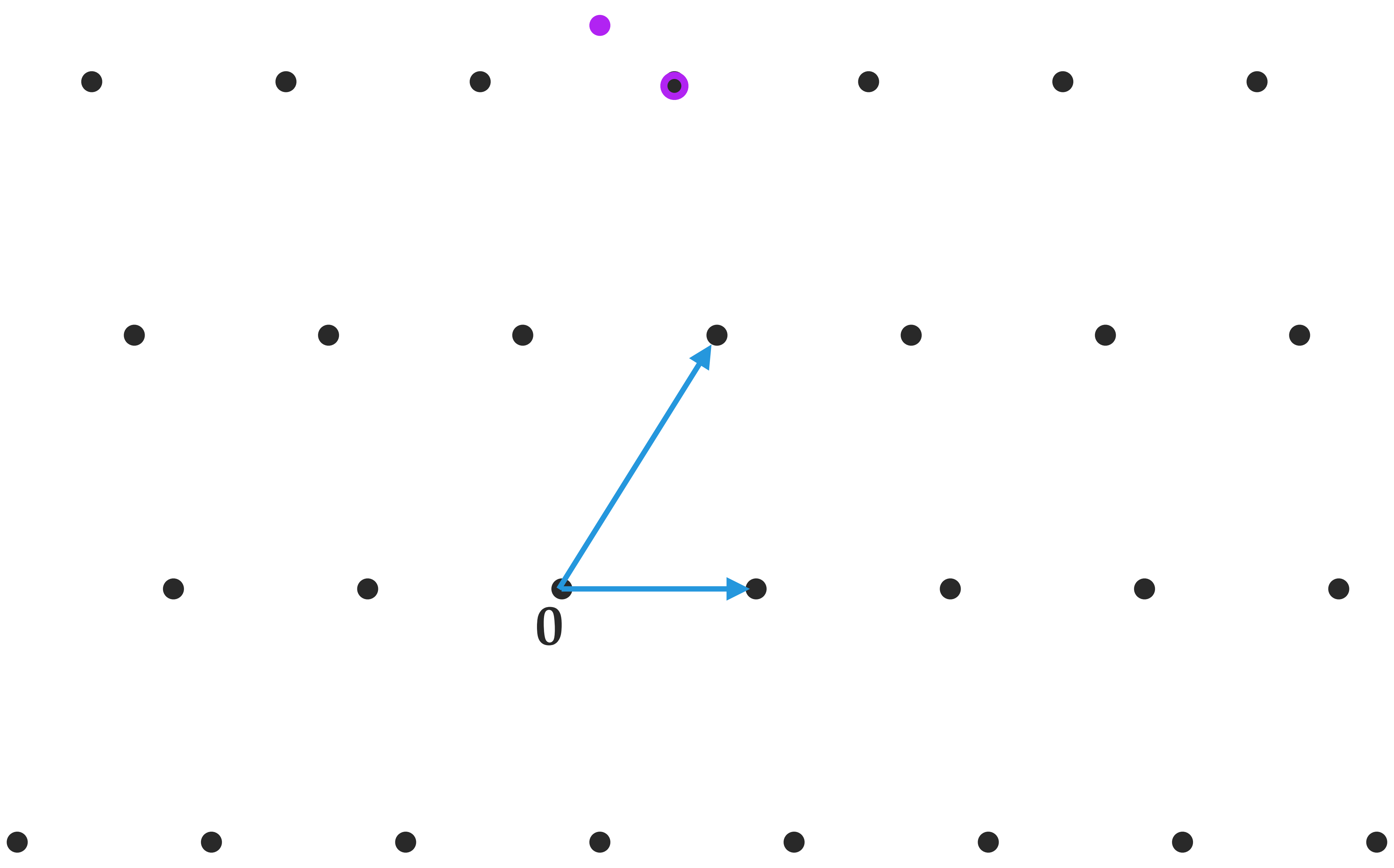
Lattice-based cryptography



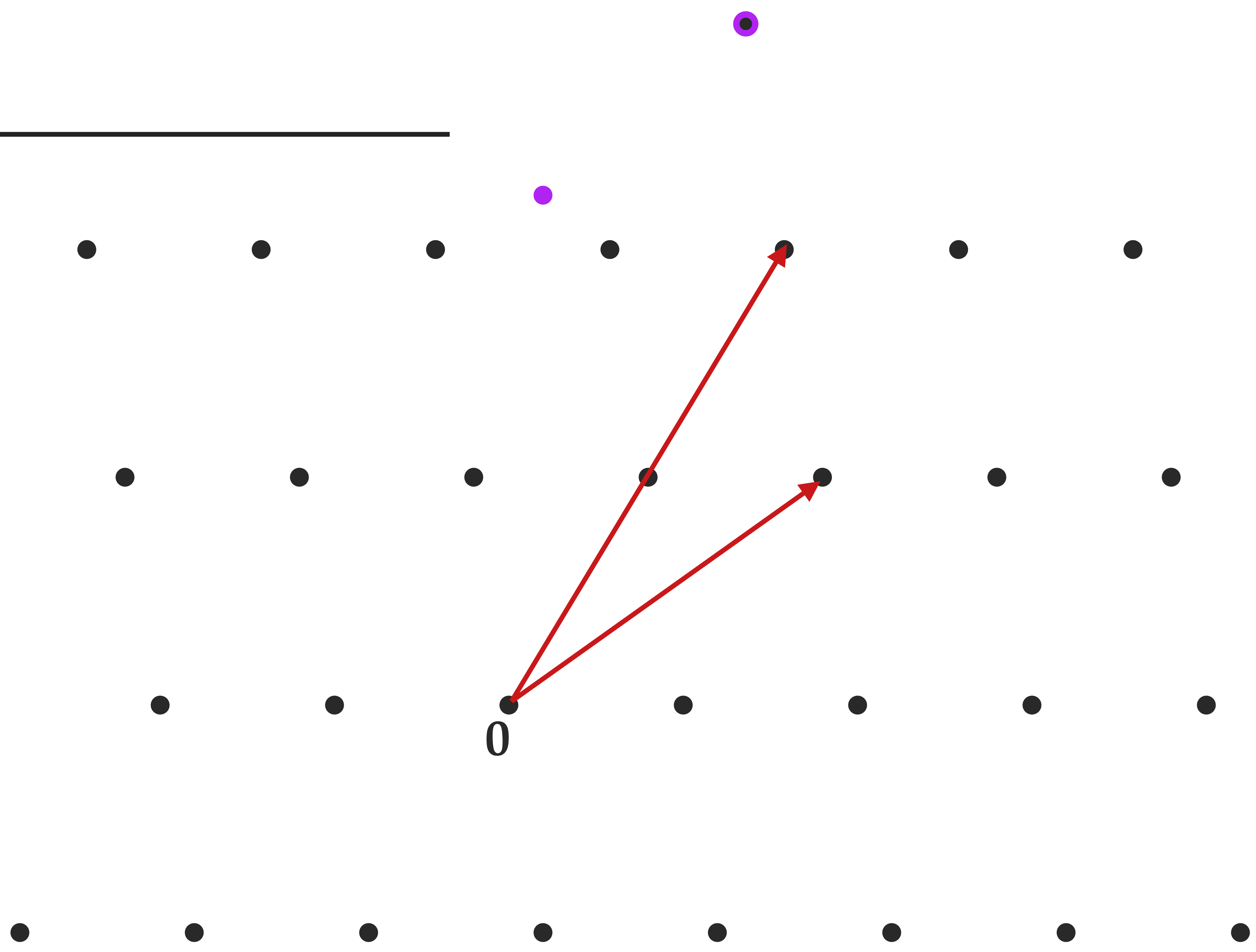
The Closest Vector Problem (CVP)

Input: an arbitrary basis $\mathbf{B}$ of a lattice L and a target vector $\mathbf{t} \in \mathbb{R}^n$.
Question: Find a lattice vector $\mathbf{v} \in L$ that is closest to $\mathbf{t}$.

Lattice-based cryptography



Hard problem



Good basis

CVP input $\mathbf{t} = (1,11)$

Bad basis

$$(\lambda_1, \lambda_2)\begin{pmatrix} 4 & 0 \\ 3 & 5 \end{pmatrix} = (1,11)$$

$$\mathbf{t} = -1.4\,\mathbf{b}_1 + 2.2\,\mathbf{b}_2$$

$$\Big\downarrow \text{rounding}$$

$$\mathbf{c} = -1\mathbf{b}_1 + 2\mathbf{b}_2 \quad ✓$$

$$(\lambda_1, \lambda_2)\begin{pmatrix} 7 & 5 \\ 6 & 10 \end{pmatrix} = (1,11)$$

$$\mathbf{t} = -1.4\,\mathbf{b}_1' + 1.8\,\mathbf{b}_2'$$

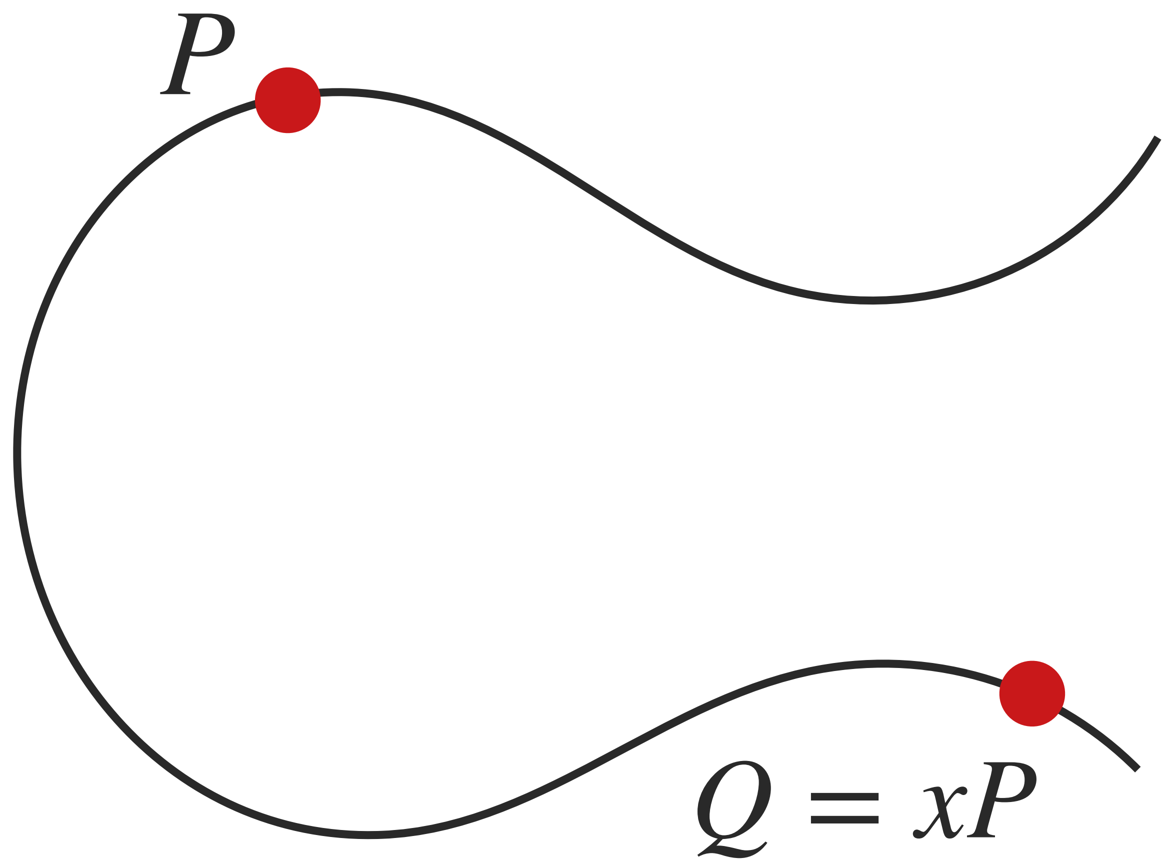
$$\Big\downarrow \text{rounding}$$

$$\mathbf{c} = -1\mathbf{b}_1' + 2\mathbf{b}_2' \quad ✗$$

Isogeny-based cryptography

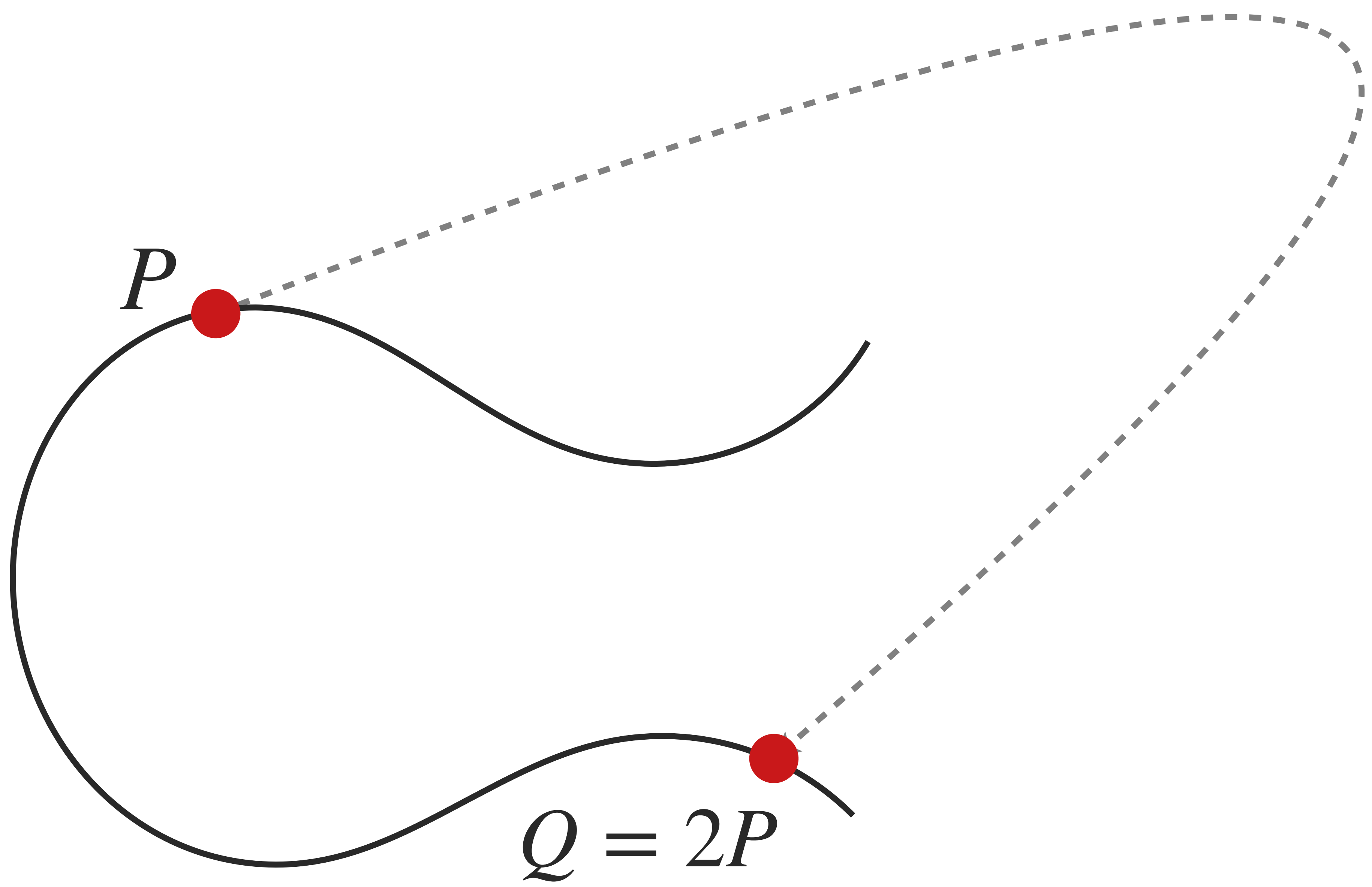
Isogeny-based cryptography

→ Elliptic curves



Isogeny-based cryptography

Elliptic curves

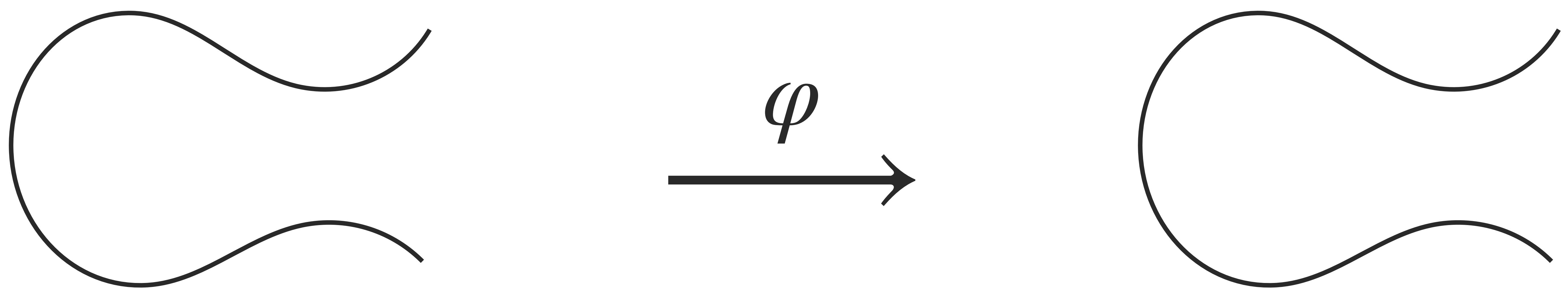


$$(x, y) \mapsto (\lambda^2 - 2x, \lambda x + y),$$

$$\lambda = \frac{3x^2 + a}{2y}$$

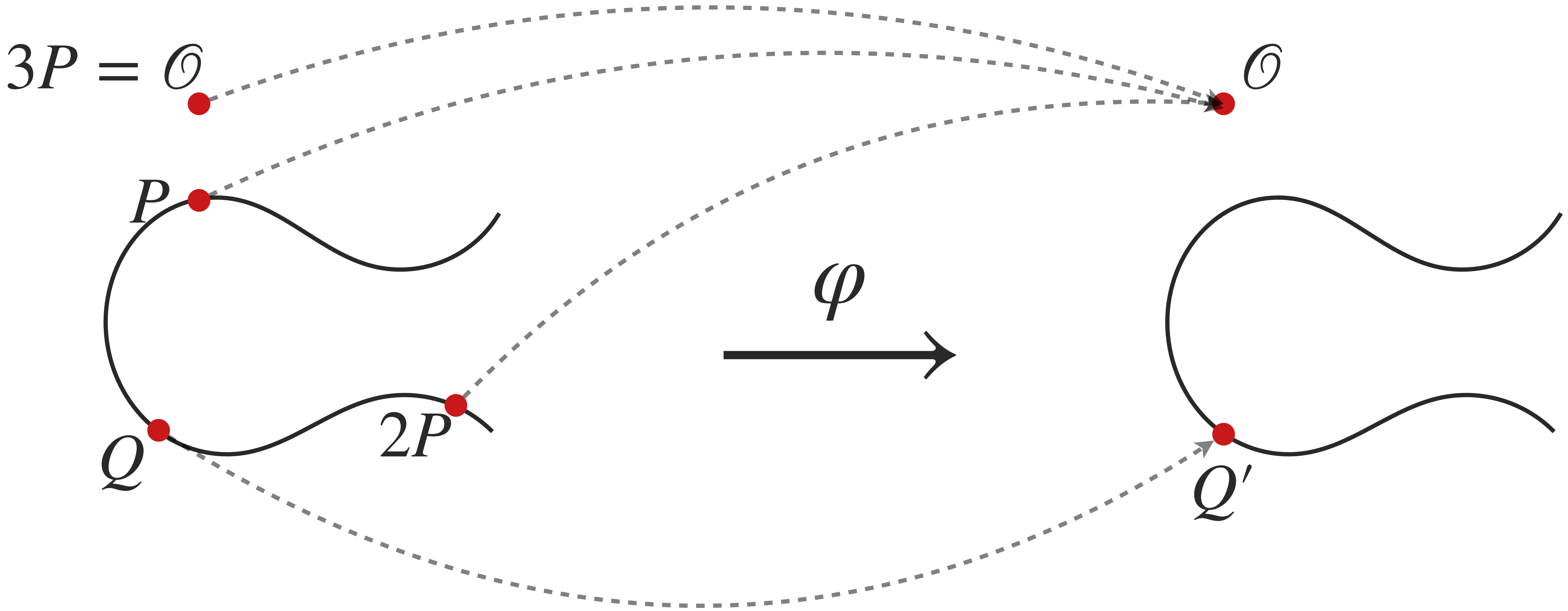
Isogeny-based cryptography

Isogenies: maps between elliptic curves



Isogeny-based cryptography

Isogenies: maps between elliptic curves



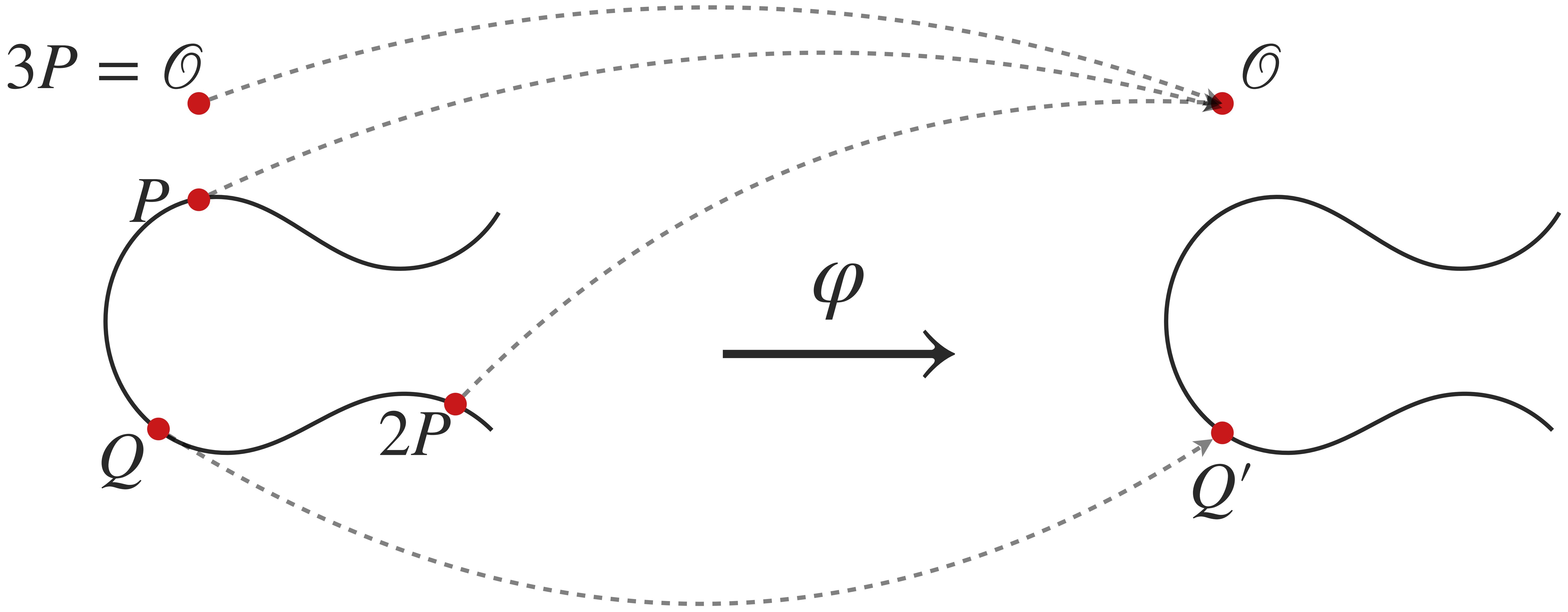
$$(x, y) \mapsto \left(\frac{x^3 - 4x^2 + 30x - 12}{(x-2)^2}, \frac{x^3 - 6x^2 - 14x + 35}{(x-2)^3} \cdot y\right)$$

Isogeny-based cryptography

The isogeny path problem

Input: Two supersingular curves E and E'.
Question: Find an isogeny φ from E to E'.

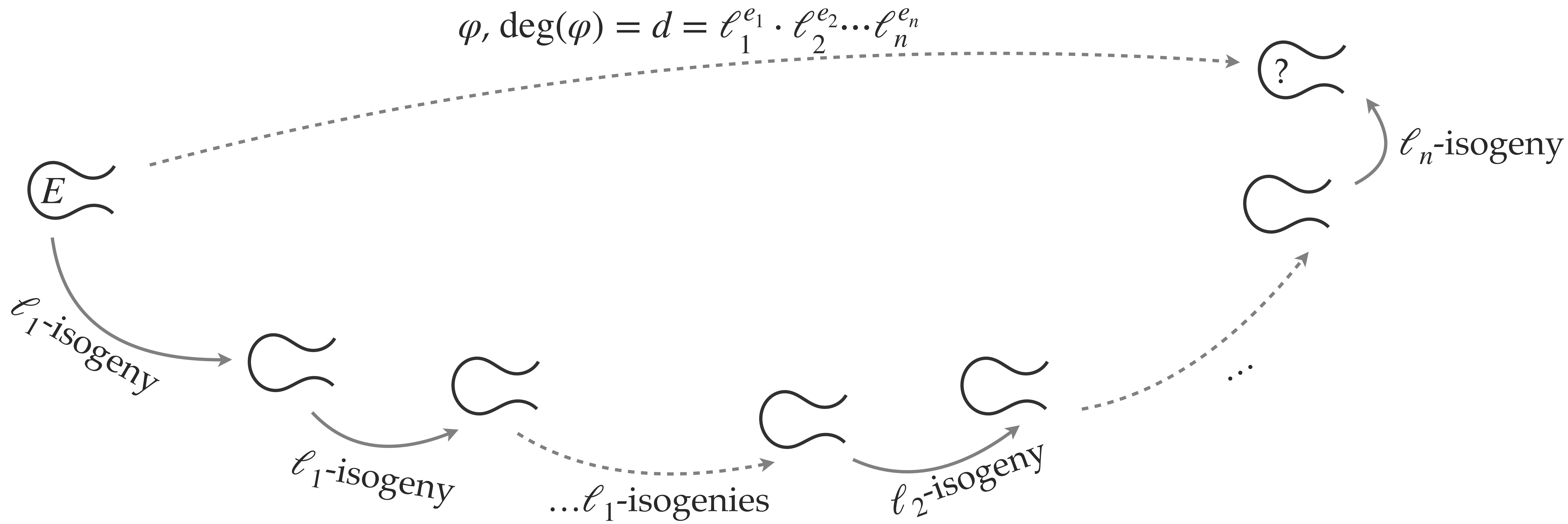
Isogenies: maps between elliptic curves



$$(x, y) \mapsto \left(\frac{x^3 - 4x^2 + 30x - 12}{(x-2)^2}, \frac{x^3 - 6x^2 - 14x + 35}{(x-2)^3} \cdot y\right)$$

Isogeny-based cryptography

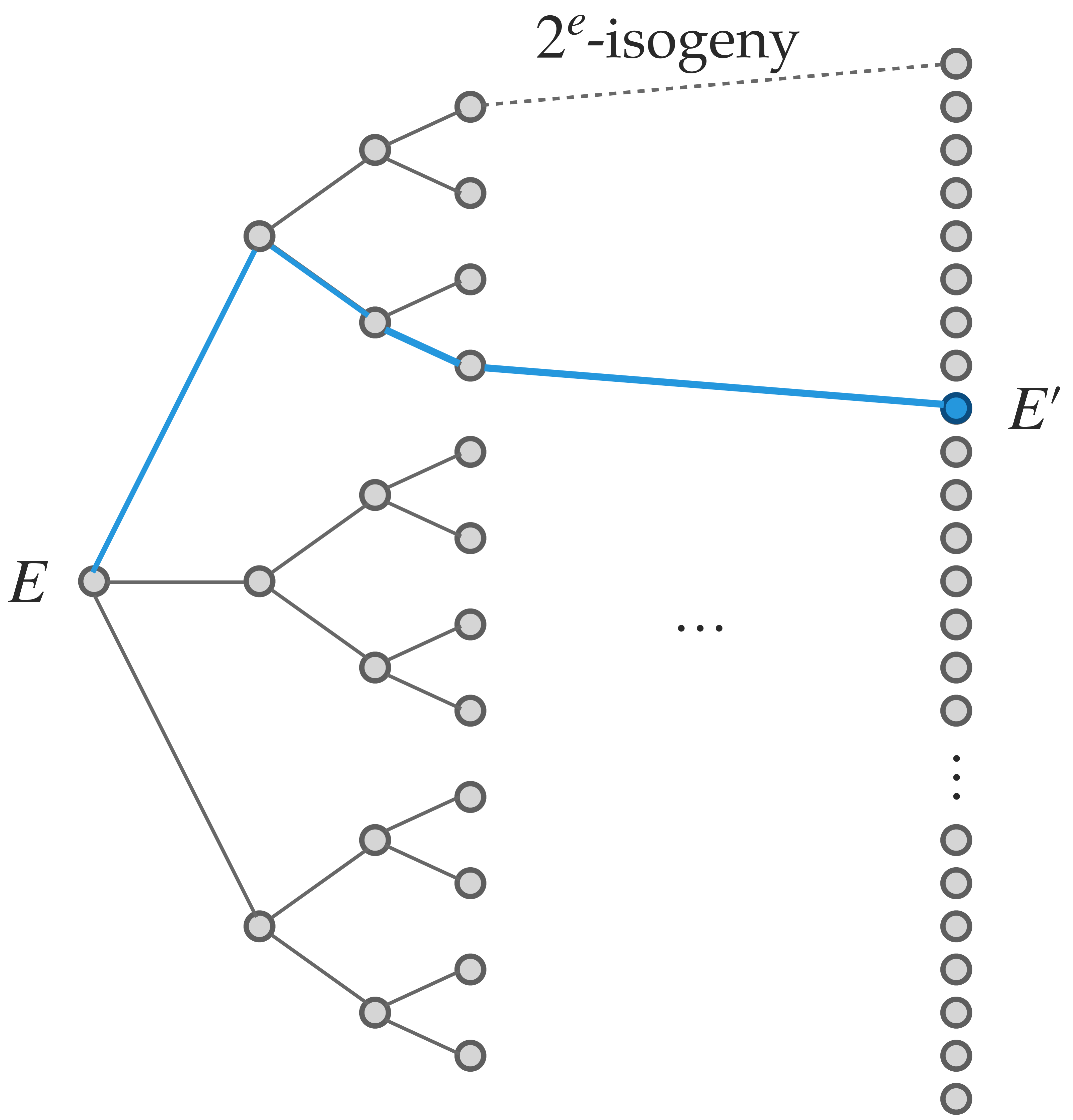
- Degree of an isogeny: how 'big' the isogeny is
  - Complexity of computing an isogeny: linear in the degree.
  - Composing isogenies: the degrees multiply: $\deg(\varphi \circ \psi) = \deg(\varphi) \cdot \deg(\psi)$.



- From a curve E, there are $(\ell + 1)$ isogenies of degree ℓ.

Isogeny-based cryptography

Brute-forcing the (fixed-degree) isogeny path problem.

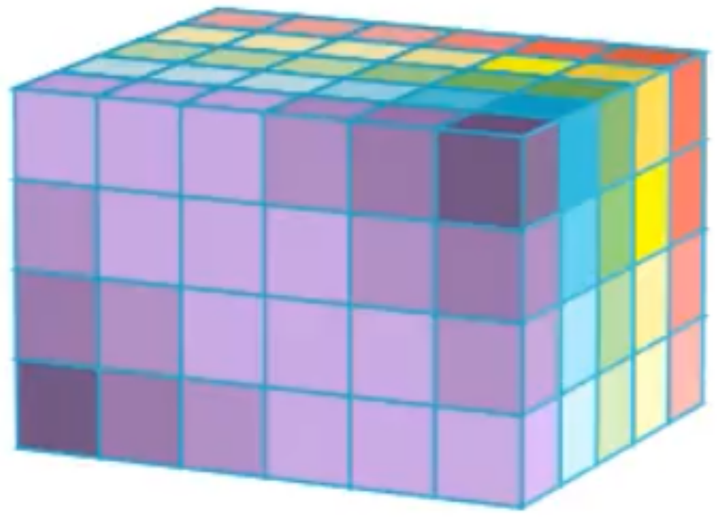


The Fiat-Shamir construction

Pick a hard problem

3-Tensor Isomorphism

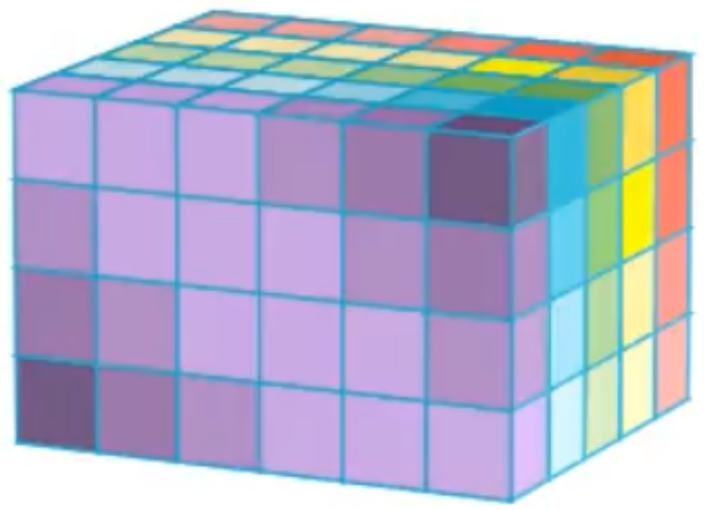
$\mathcal{C} \subseteq \mathbb{F}_q^{m \times n \times k}$



Pick a hard problem

3-Tensor Isomorphism

$\mathbf{T} \in \mathrm{GL}_k(q)$



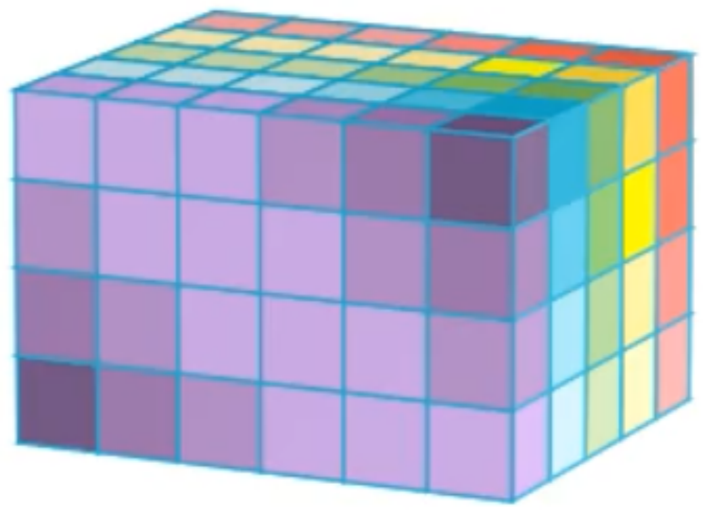
$\mathbf{A} \in \mathrm{GL}_m(q)$

$\mathbf{B} \in \mathrm{GL}_n(q)$

Pick a hard problem

→ 3-Tensor Isomorphism

$\mathbf{T} \in \mathrm{GL}_k(q)$



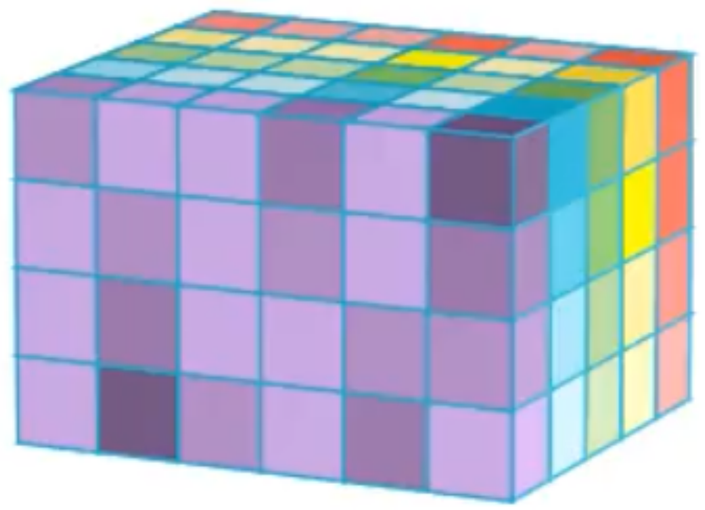
$\mathbf{A} \in \mathrm{GL}_m(q)$

$\mathbf{B} \in \mathrm{GL}_n(q)$

Pick a hard problem

3-Tensor Isomorphism

$\mathbf{T} \in \mathrm{GL}_k(q)$



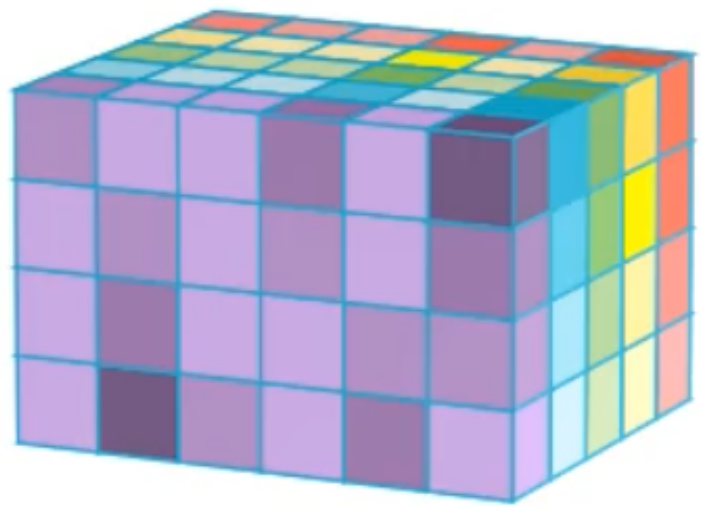
$\mathbf{A} \in \mathrm{GL}_m(q)$

$\mathbf{B} \in \mathrm{GL}_n(q)$

Pick a hard problem

3-Tensor Isomorphism

$\mathbf{T} \in \mathrm{GL}_k(q)$



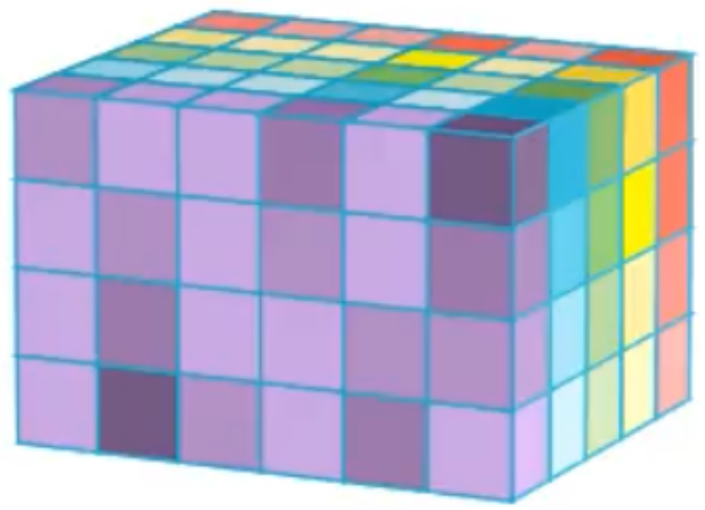
$\mathbf{A} \in \mathrm{GL}_m(q)$

$\mathbf{B} \in \mathrm{GL}_n(q)$

Pick a hard problem

3-Tensor Isomorphism

$\mathbf{T} \in \mathrm{GL}_k(q)$



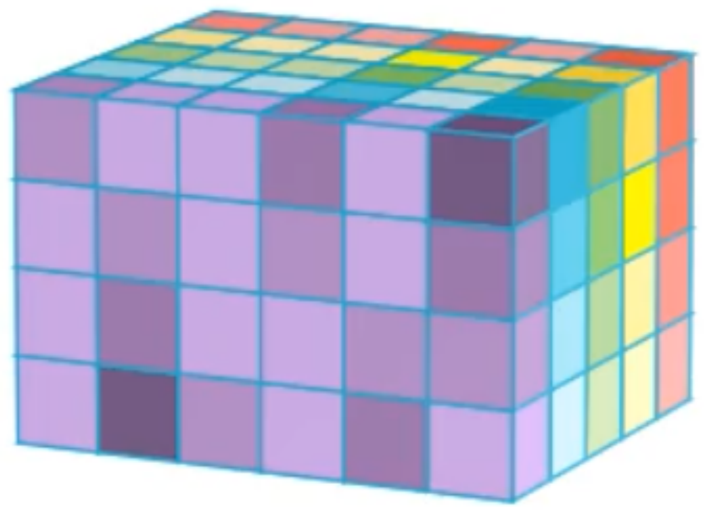
$\mathbf{A} \in \mathrm{GL}_m(q)$

$\mathbf{B} \in \mathrm{GL}_n(q)$

Pick a hard problem

→ 3-Tensor Isomorphism

$\mathbf{T} \in \mathrm{GL}_k(q)$



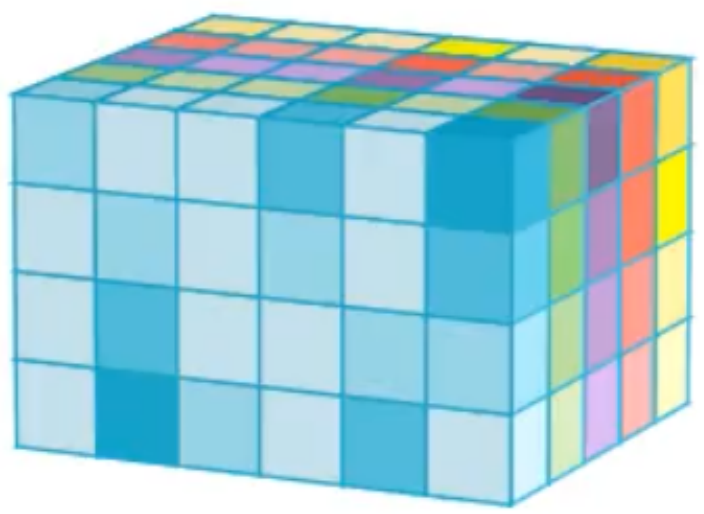
$\mathbf{A} \in \mathrm{GL}_m(q)$

$\mathbf{B} \in \mathrm{GL}_n(q)$

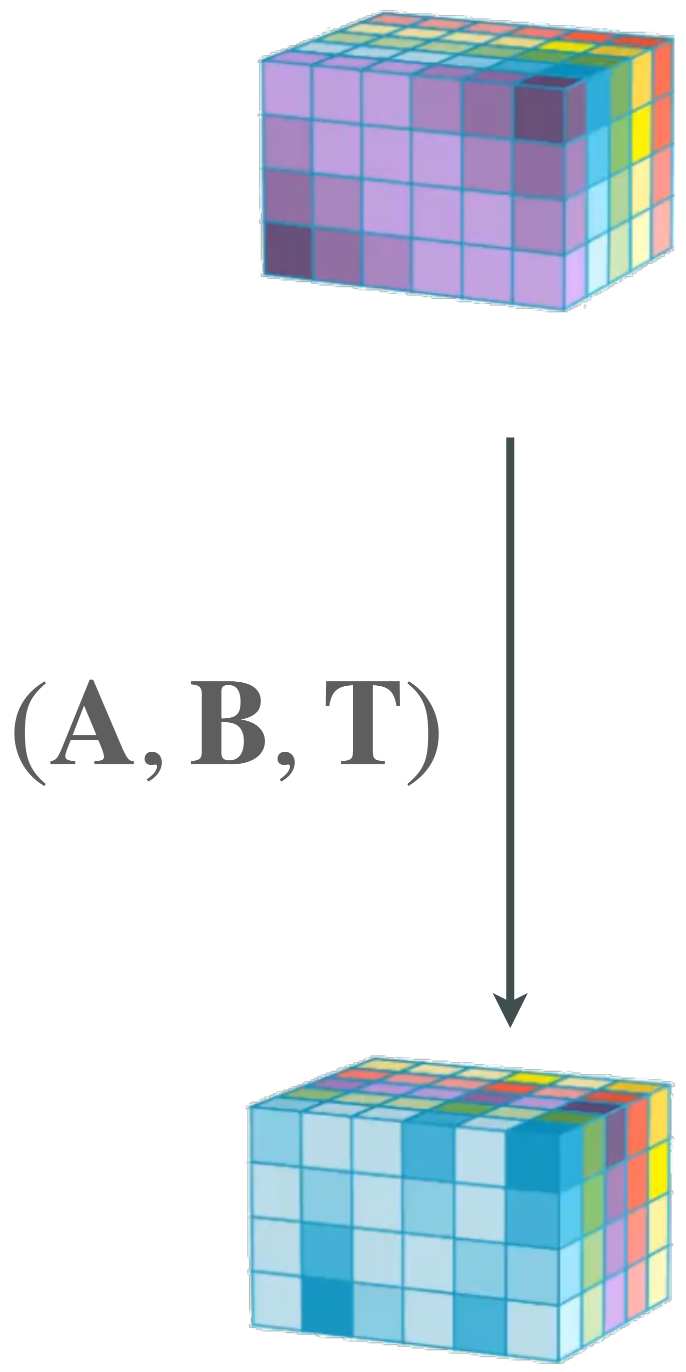
Pick a hard problem

→ 3-Tensor Isomorphism

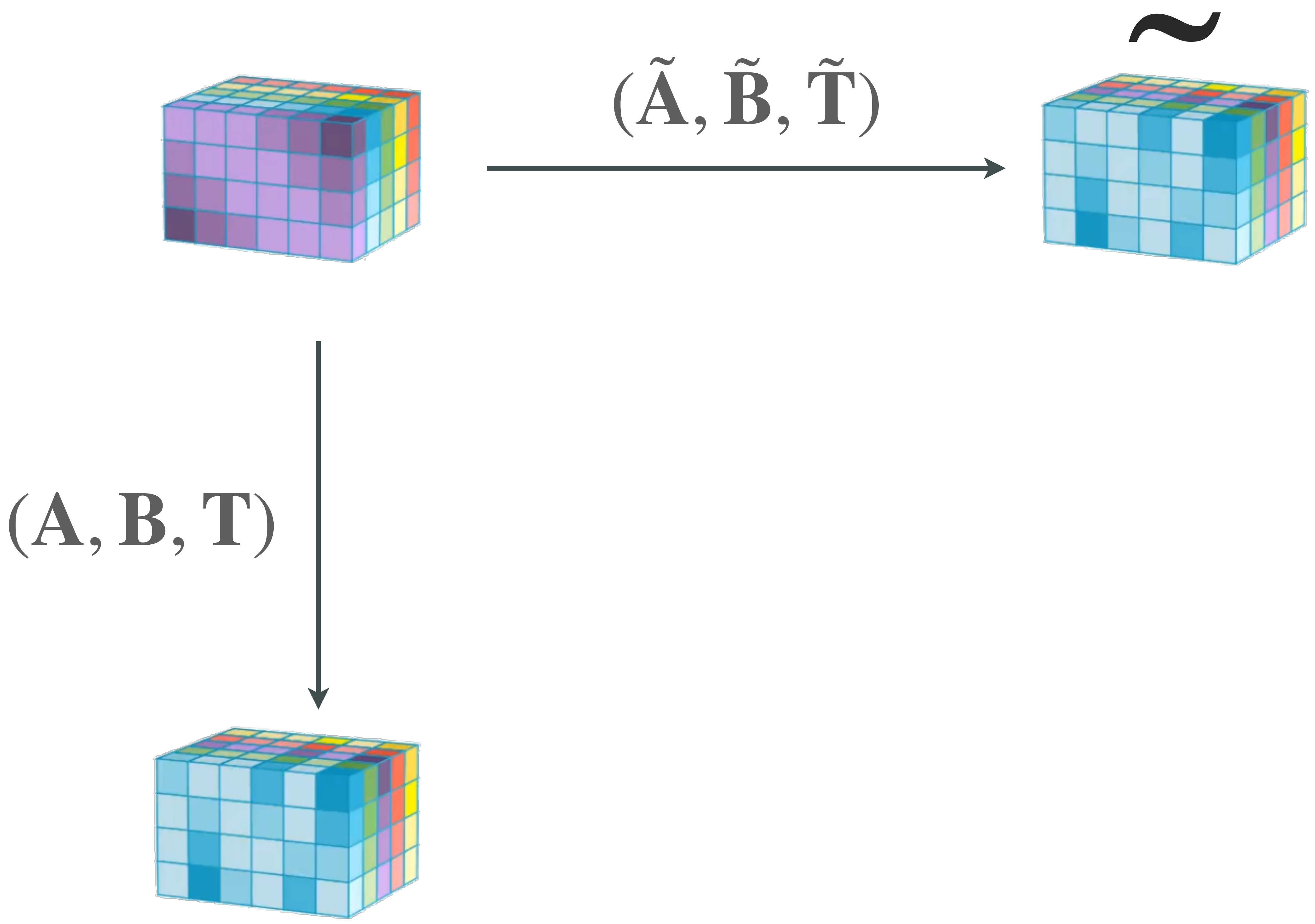
$$\mathcal{D} \subseteq \mathbb{F}_q^{m\times n\times k}$$



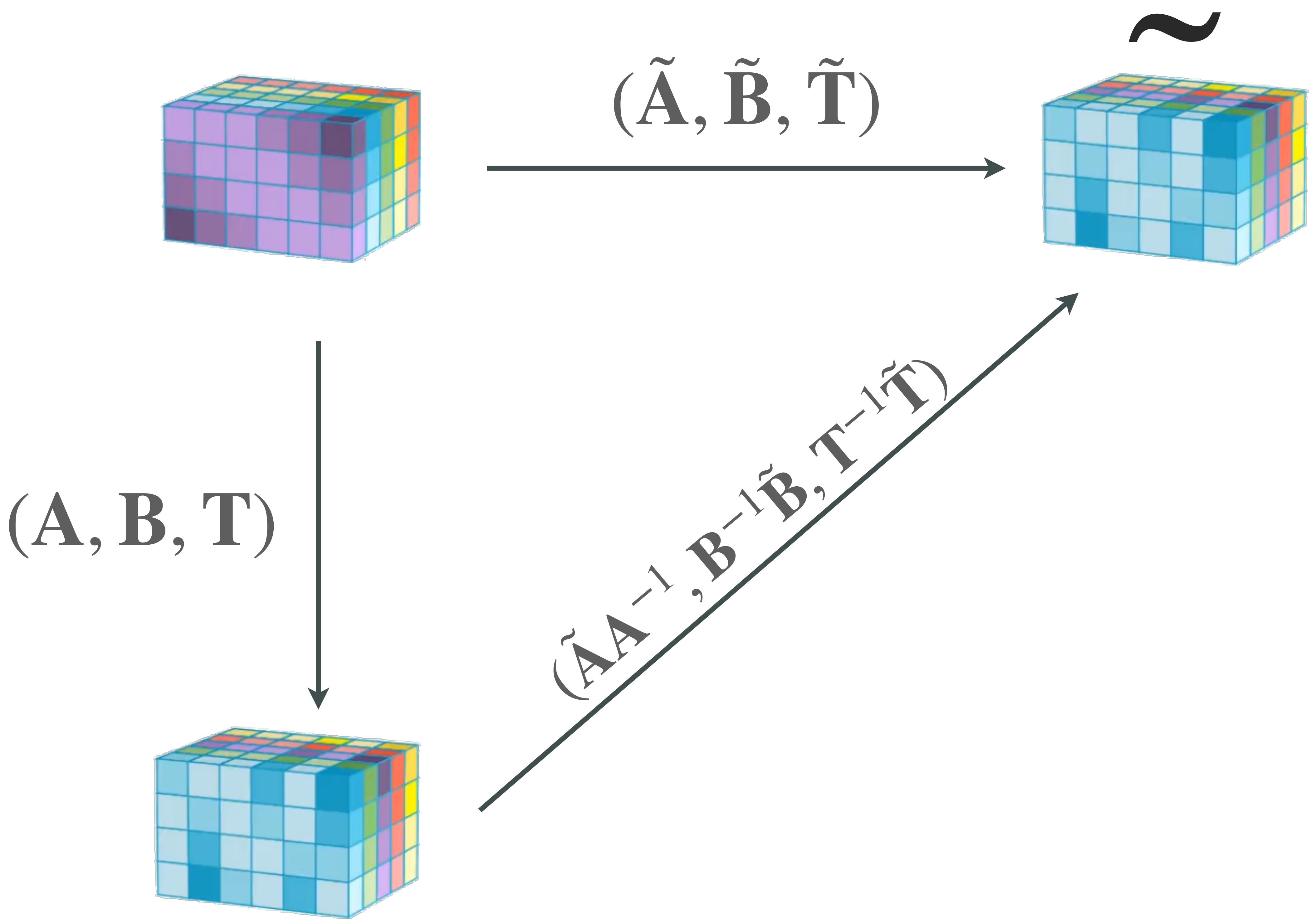
ZK identification scheme



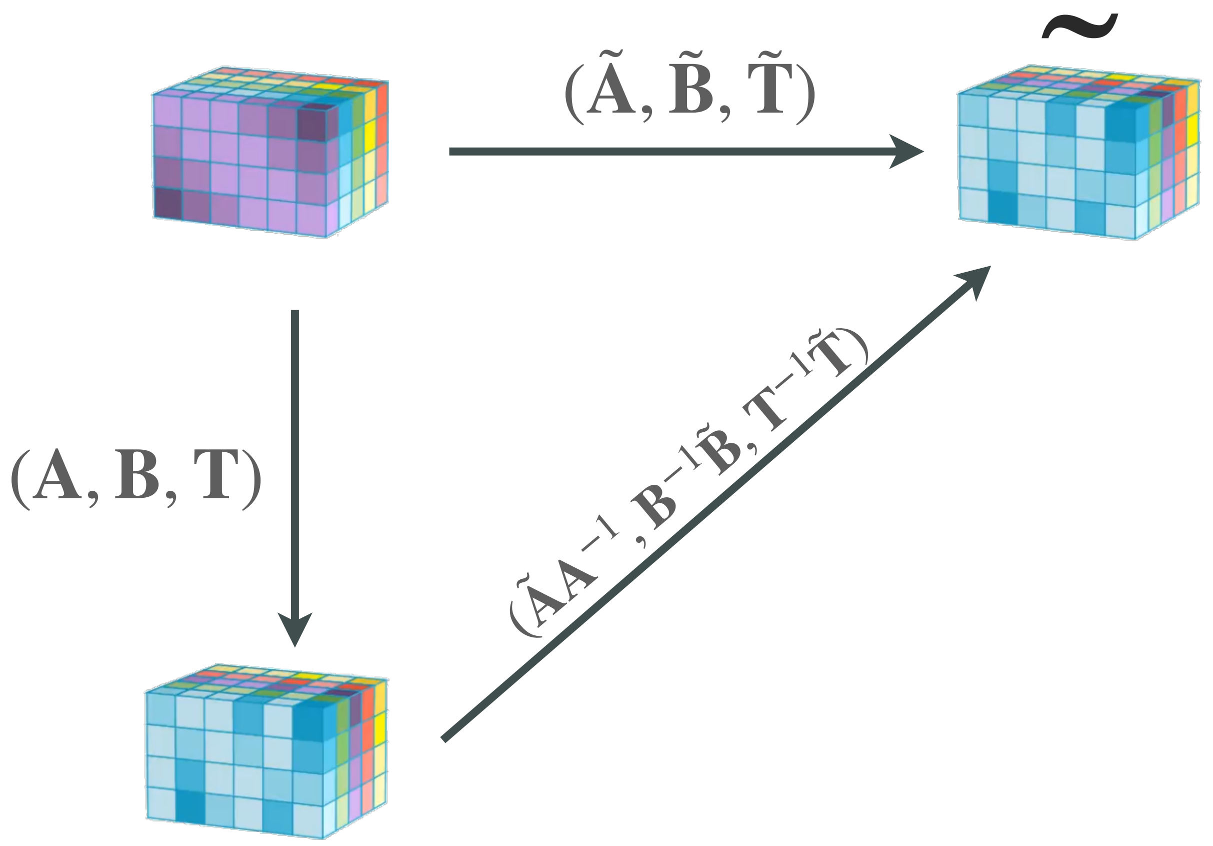
ZK identification scheme



ZK identification scheme



ZK identification scheme



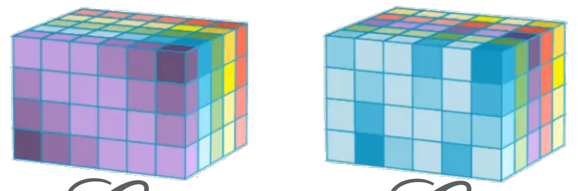
Prover

A

$(\mathbf{A}, \mathbf{B}, \mathbf{T})$

Verifier

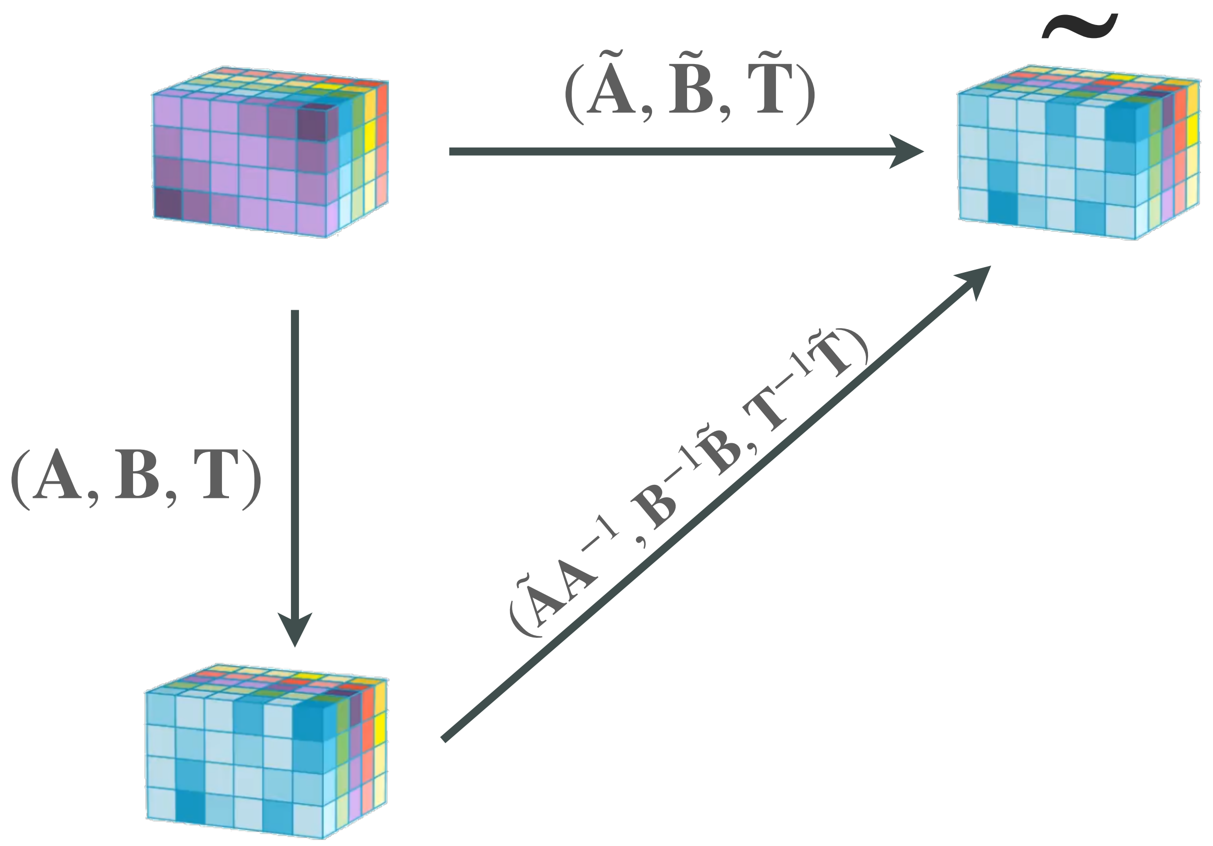
A

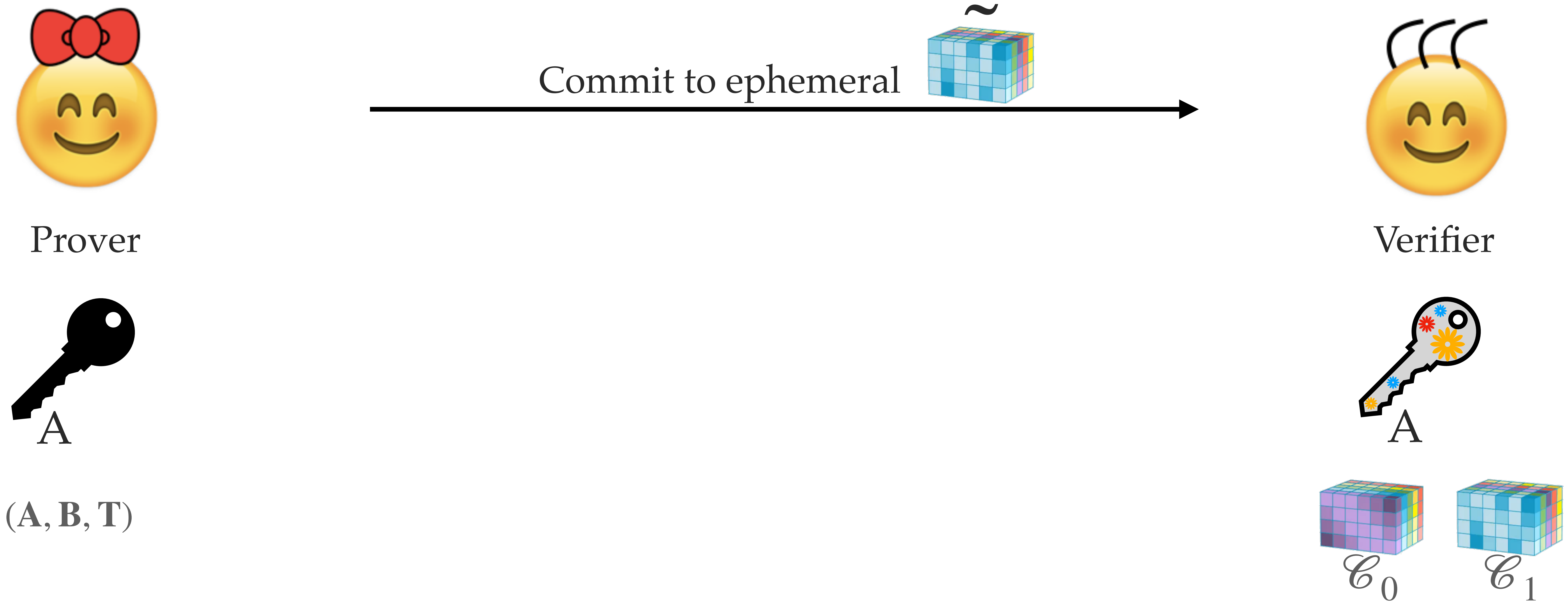


$\mathscr{C}_0$ $\mathscr{C}_1$

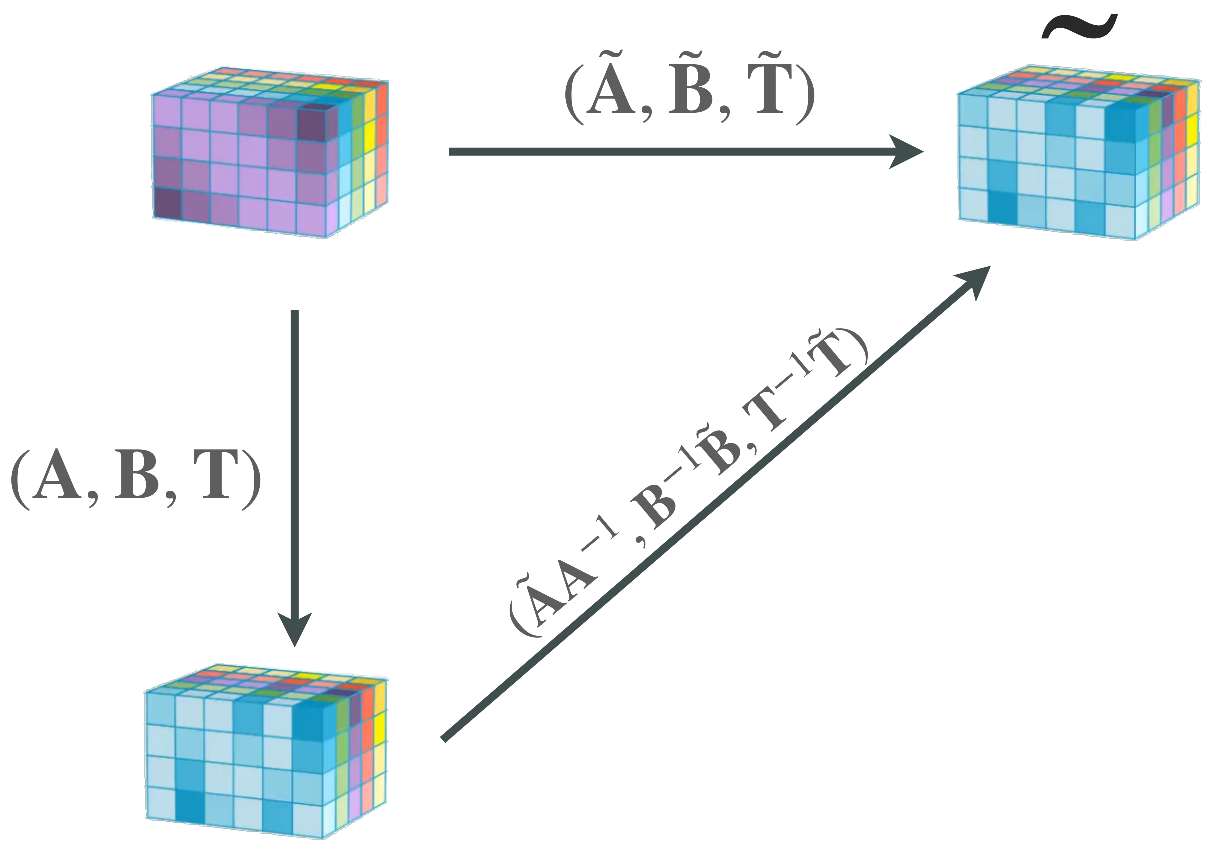
MEDS

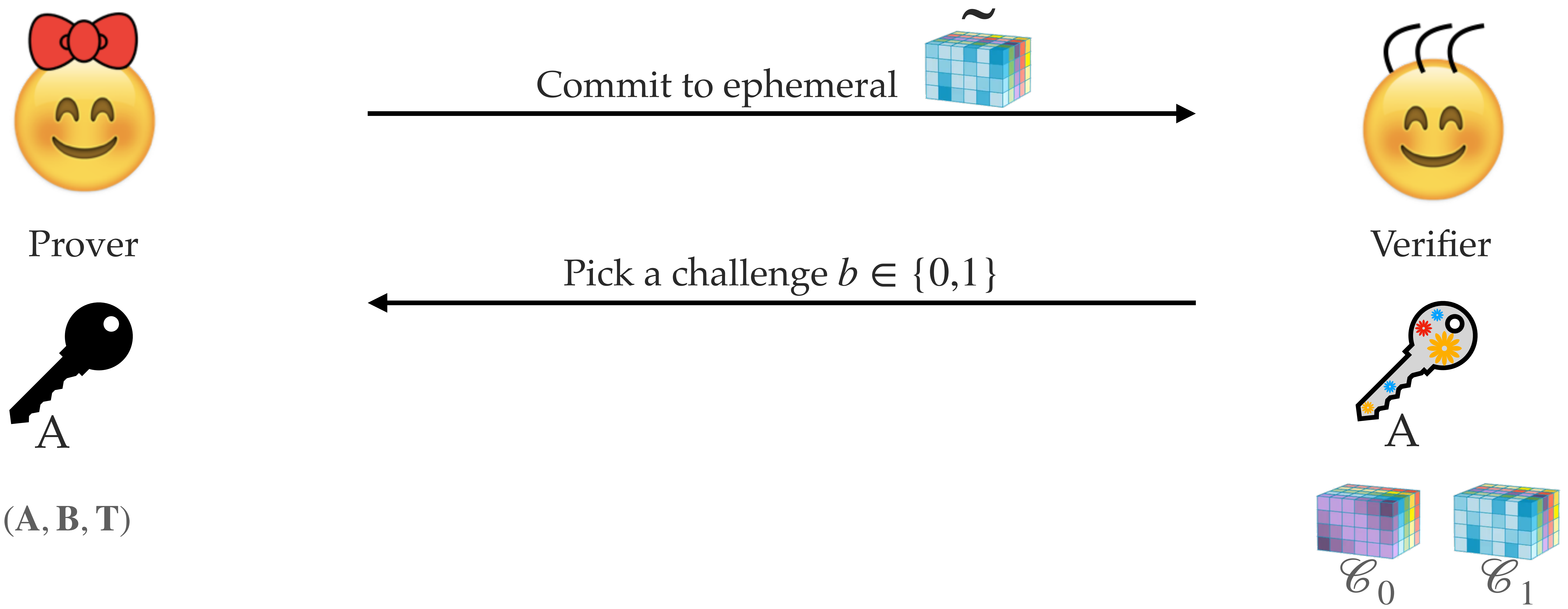
ZK identification scheme



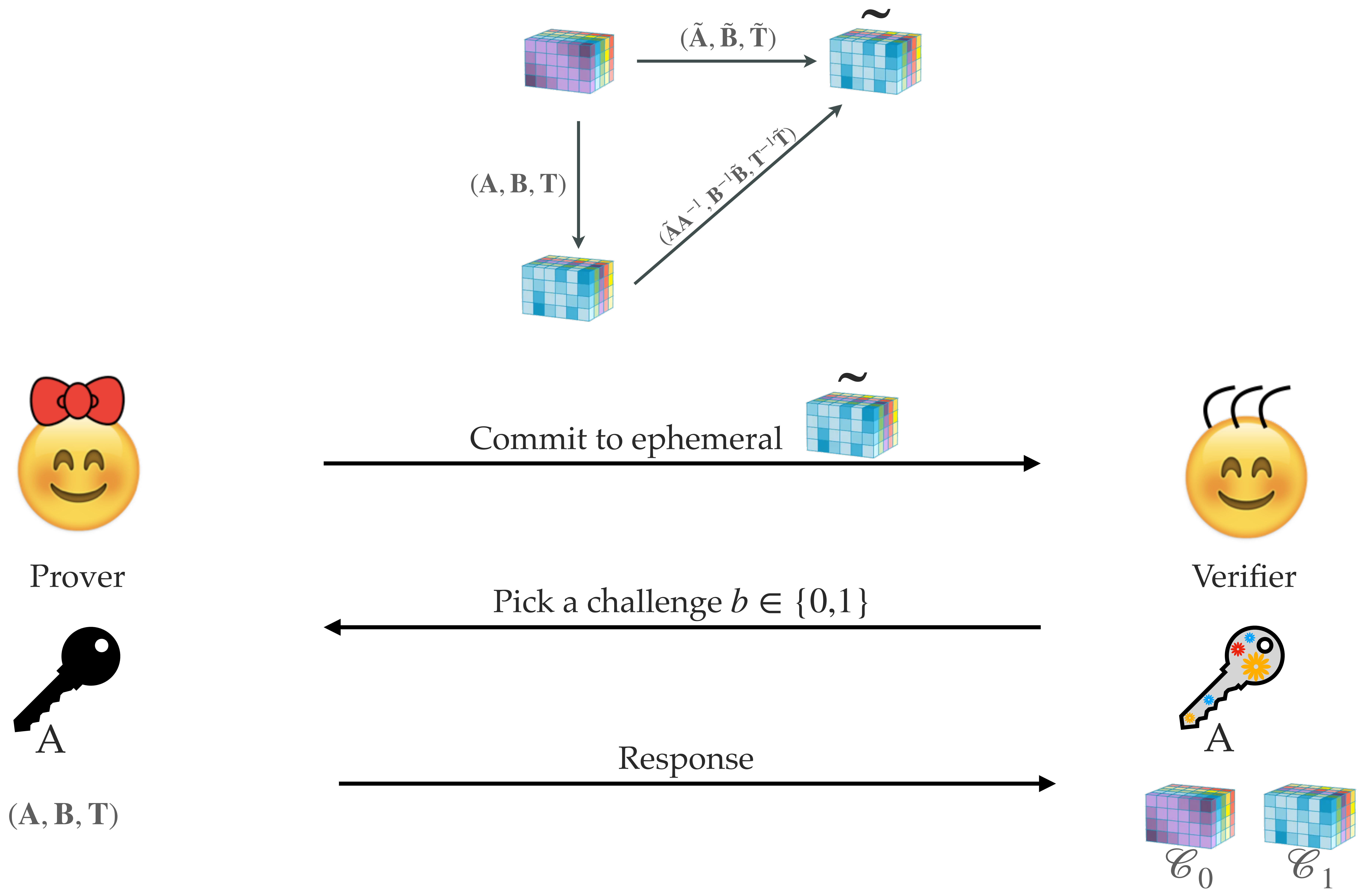


ZK identification scheme

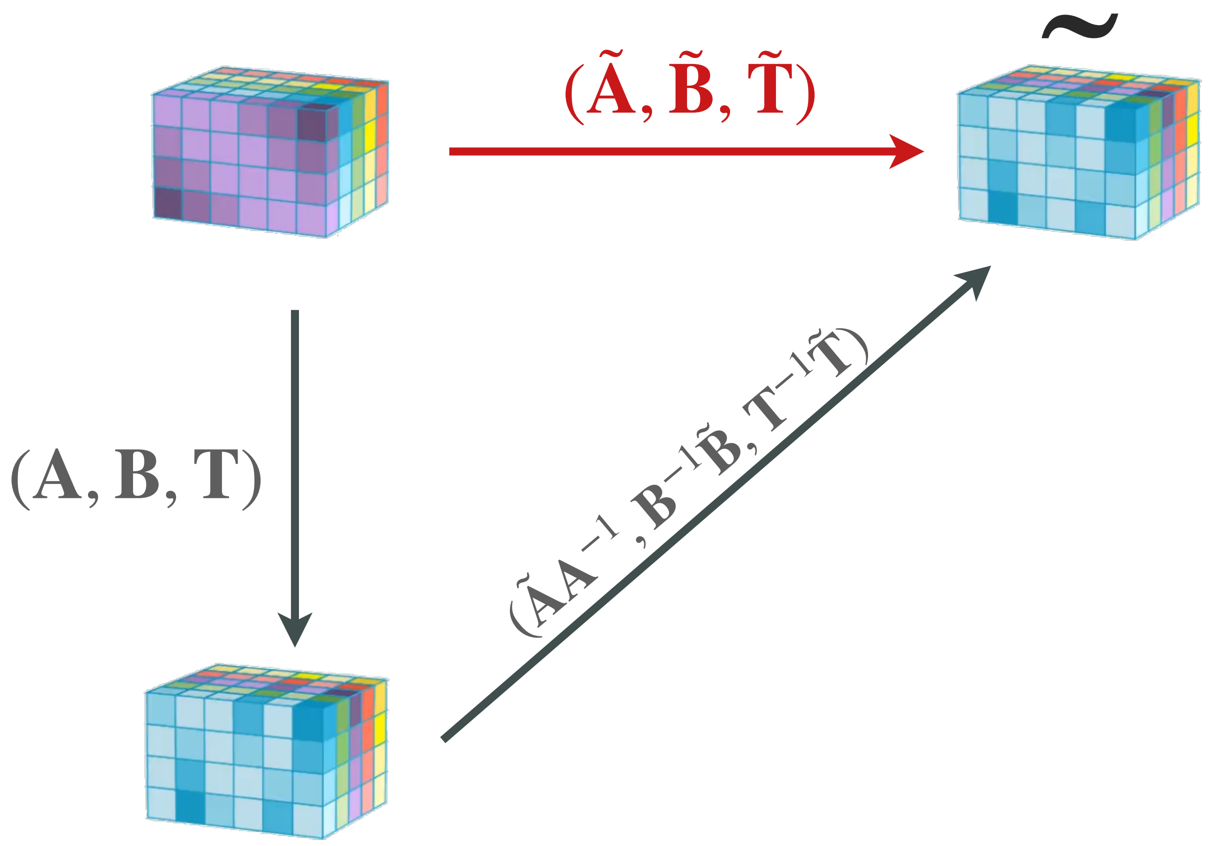


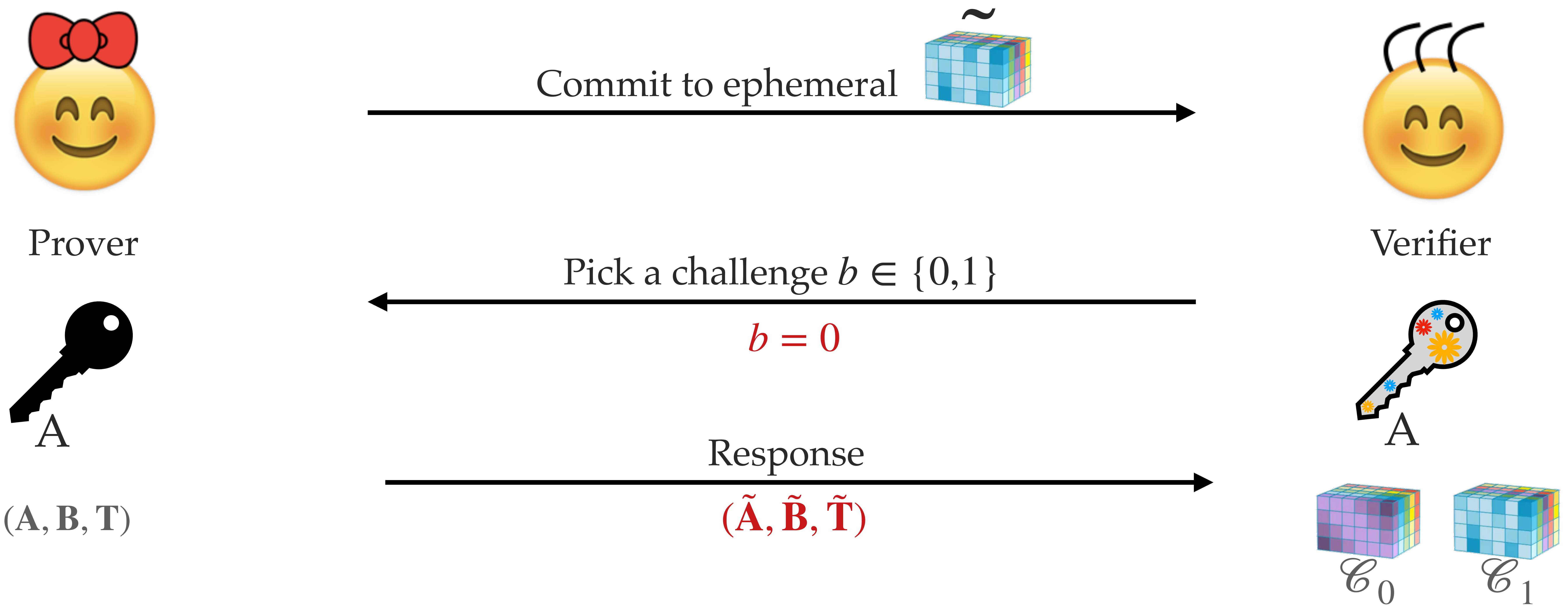


ZK identification scheme

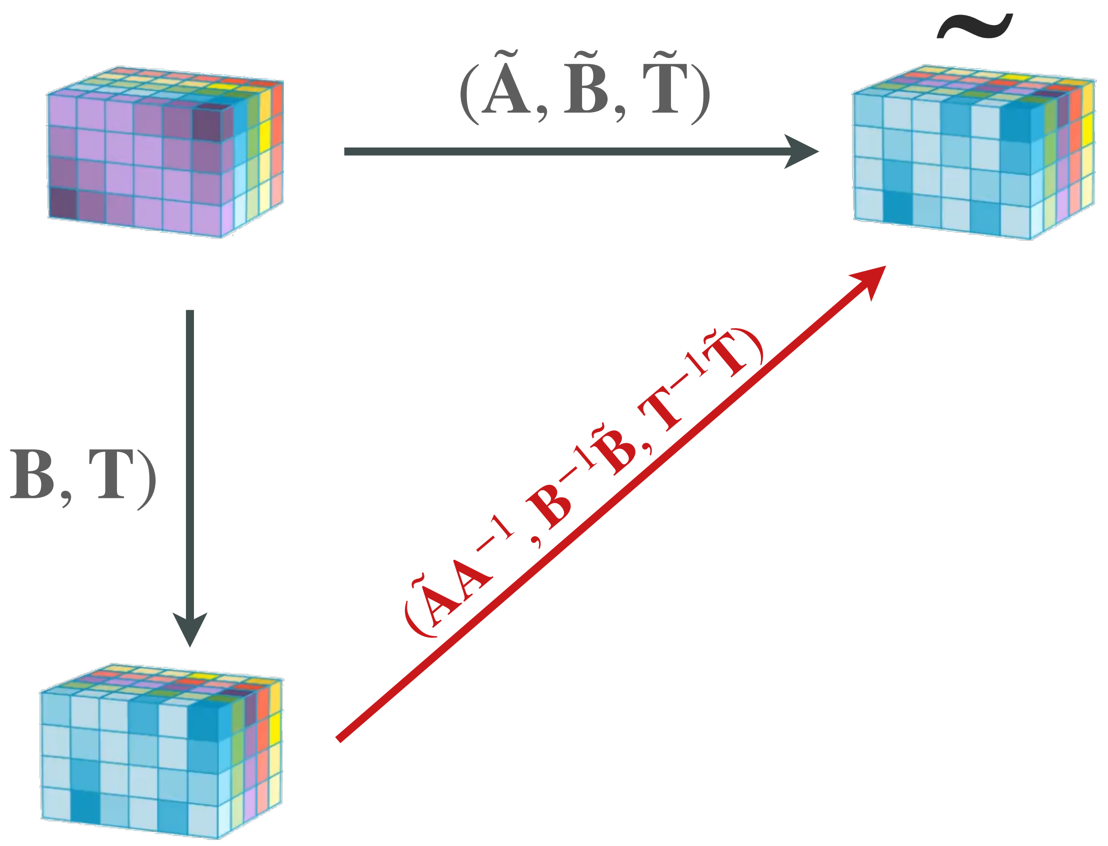


ZK identification scheme





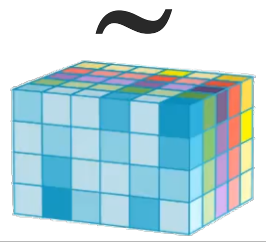
ZK identification scheme



Prover

A

$(\mathbf{A}, \mathbf{B}, \mathbf{T})$

Commit to ephemeral 

Pick a challenge $b \in \{0,1\}$

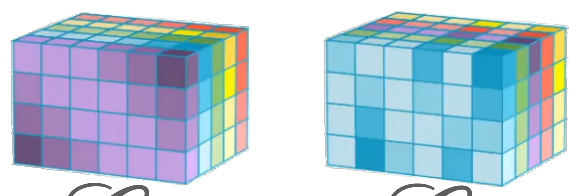
$b = 1$

Response

$(\tilde{\mathbf{A}}\mathbf{A}^{-1}, \mathbf{B}^{-1}\tilde{\mathbf{B}}, \mathbf{T}^{-1}\tilde{\mathbf{T}})$

Verifier

A



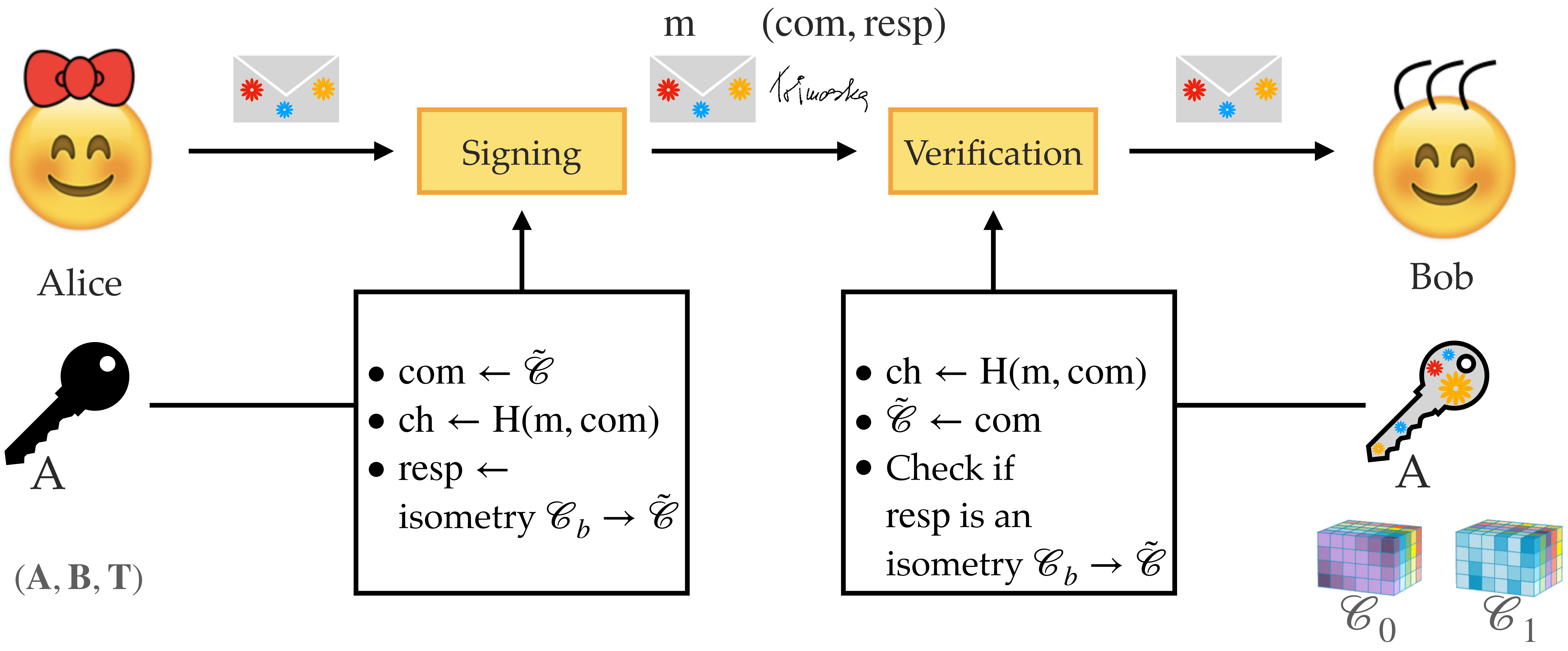
$\mathscr{C}_0$ $\mathscr{C}_1$

MEDS

The Fiat-Shamir transform

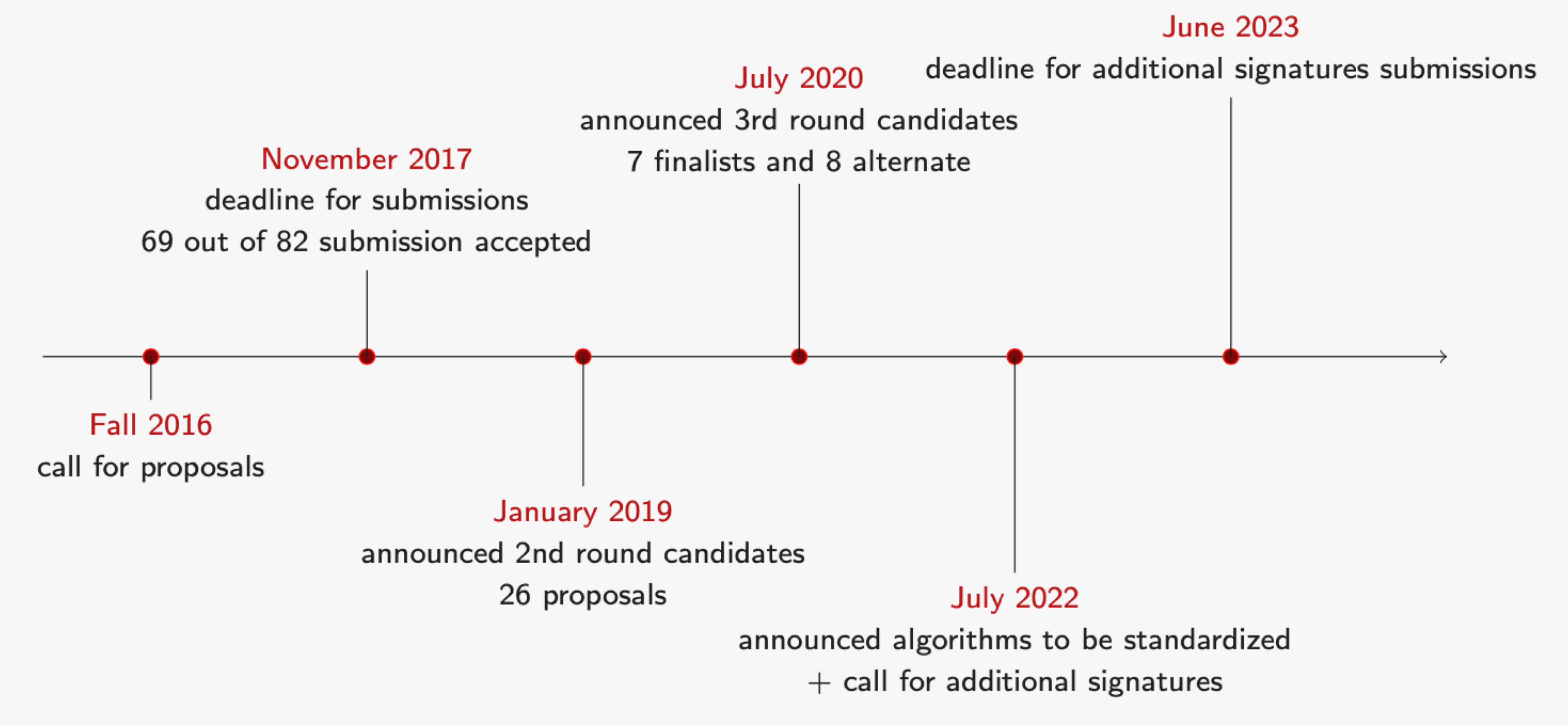
The goal is to transform an interactive identification scheme into a digital signature scheme.

Instead of the prover choosing a challenge, the challenge is determined by the hash of the message and commitments.

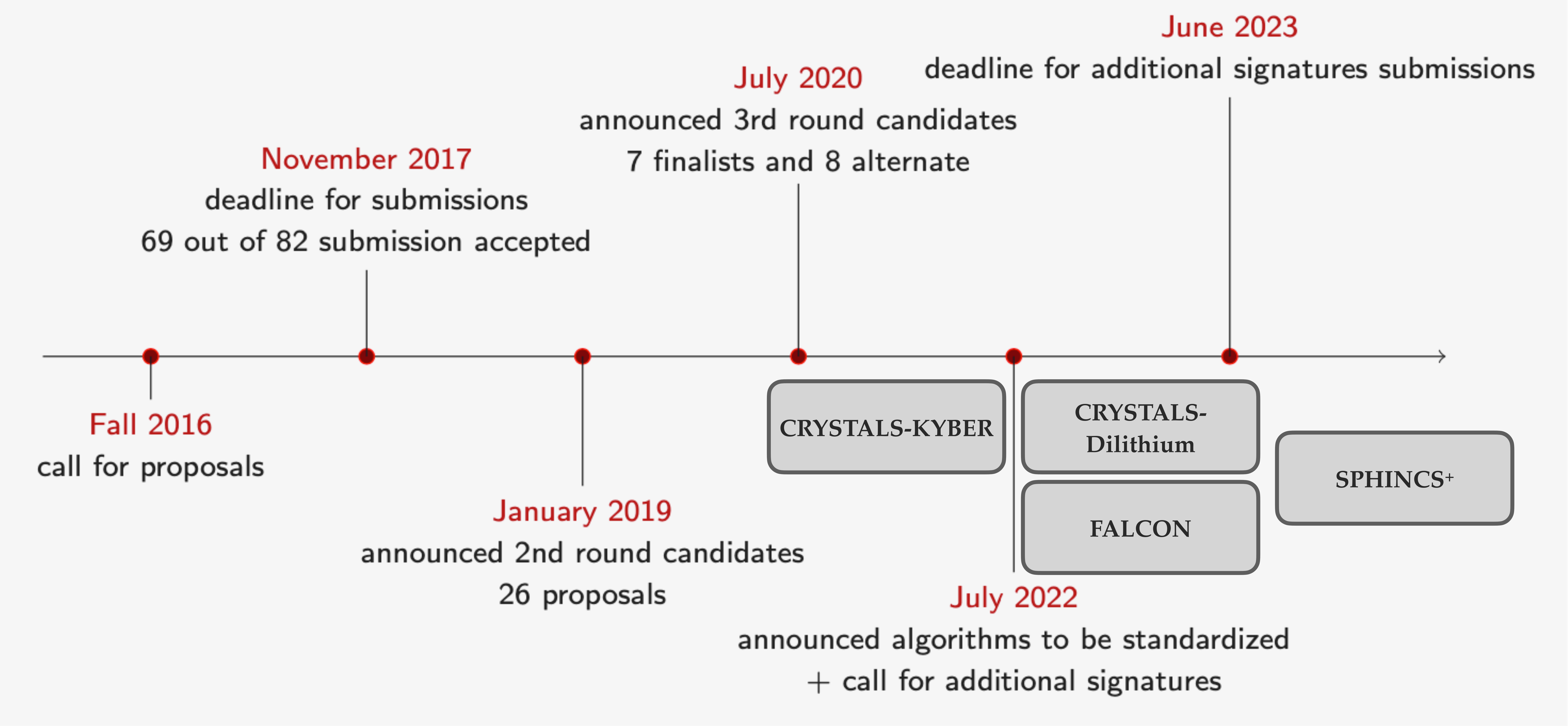


Timeline and challenges

NIST standardisation timeline



NIST standardisation timeline

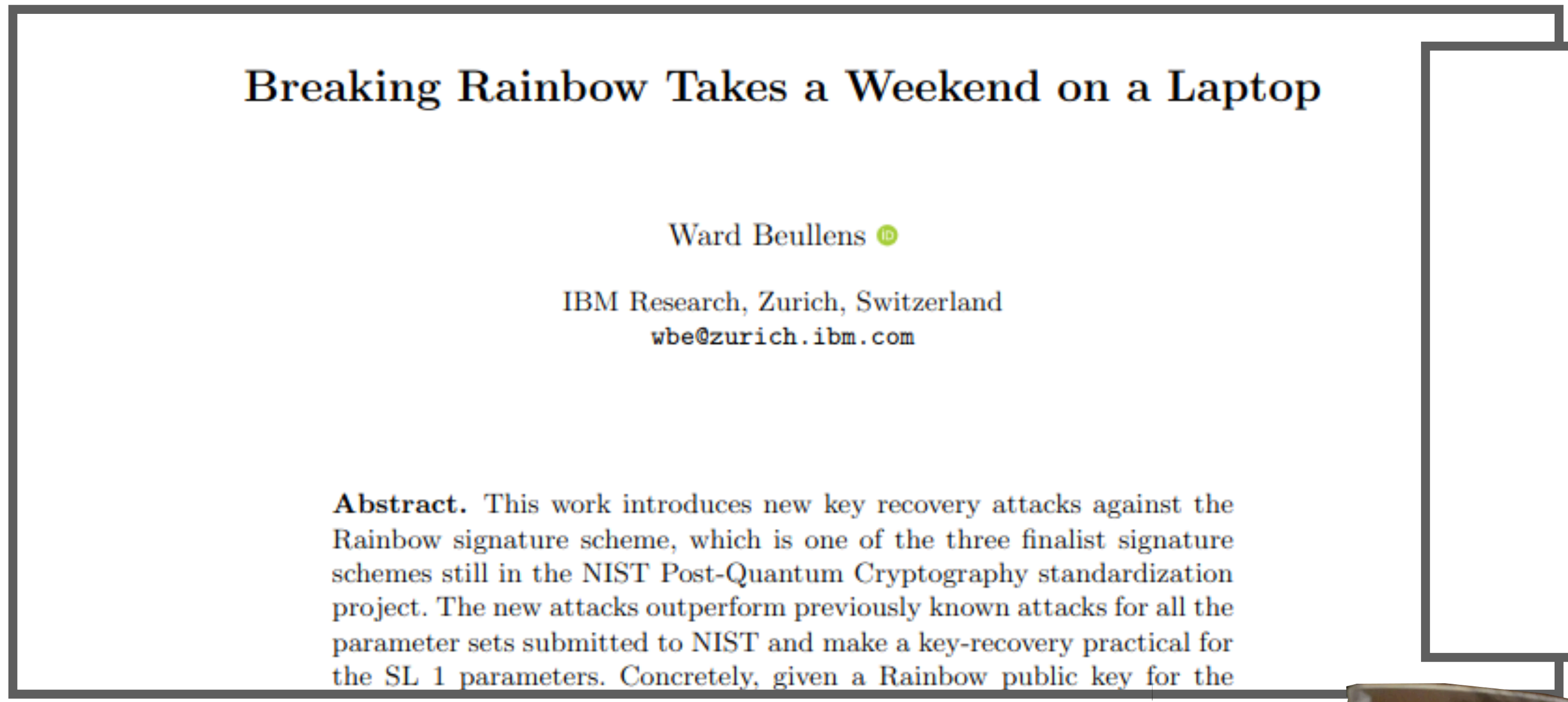


NIST standardisation timeline

		$x_1x_2 + x_3 = 0$ $x_1^2x_3 + x_2 = 0$			
EagleSign	CROSS	Biscuit	SQIsign	AIMer	MIRA
EHTv3/4	Enh. pqsigRM	MQOM		Ascon-Sign	MiRitH
HAETAE	FuLeeca	3WISE		FAEST	PERK
HAWK	LESS	DME-Sign		SPHINCS-α	ALTEQ
HuFu	MEDS	HPPC			eMLE-Sig 2.0
Raccoon	Wave	SNOVA			KAZ-SIGN
SQUIRRELS	RYDE	TUOV			Preon
	SDitH	MAYO			Xifrat1-Sign.I
		PROV			
		QR-UOV			
		UOV			
		VOX			

Challenges in PQC

- Security assessment

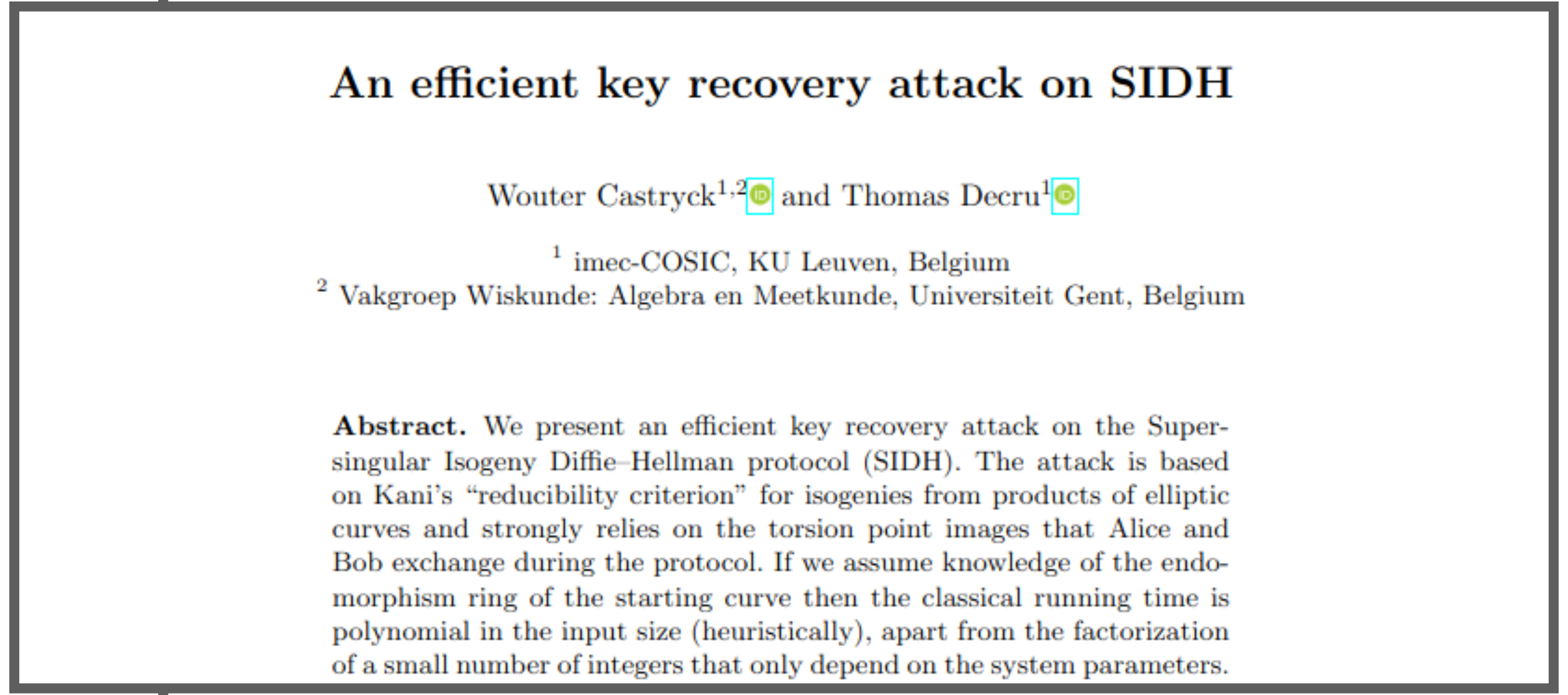


Breaking Rainbow Takes a Weekend on a Laptop

Ward Beullens

IBM Research, Zurich, Switzerland
wbe@zurich.ibm.com

Abstract. This work introduces new key recovery attacks against the Rainbow signature scheme, which is one of the three finalist signature schemes still in the NIST Post-Quantum Cryptography standardization project. The new attacks outperform previously known attacks for all the parameter sets submitted to NIST and make a key-recovery practical for the SL 1 parameters. Concretely, given a Rainbow public key for the



An efficient key recovery attack on SIDH

Wouter Castryck[1,2] and Thomas Decru[1]

[1] imec-COSIC, KU Leuven, Belgium
[2] Vakgroep Wiskunde: Algebra en Meetkunde, Universiteit Gent, Belgium

Abstract. We present an efficient key recovery attack on the Supersingular Isogeny Diffie–Hellman protocol (SIDH). The attack is based on Kani's "reducibility criterion" for isogenies from products of elliptic curves and strongly relies on the torsion point images that Alice and Bob exchange during the protocol. If we assume knowledge of the endomorphism ring of the starting curve then the classical running time is polynomial in the input size (heuristically), apart from the factorization of a small number of integers that only depend on the system parameters.

- Key/ciphertext/signature sizes and computational costs

- Physical security assessment

- Building advanced constructions

Thank you!

Q?