Lattice-Based Cryptography

A Gentle Introduction

Katharina Boudgoust

CNRS, Univ Montpellier, LIRMM, France

Disclaimer

- I come from an academic background.
- Very happy to engage with practitioners.
- Just be patient with me if there are too many math modes.
- Ask as many questions as you want, that's why I'm here.

Security Paradigm

👉 The security in public-key cryptography relies on presumably hard mathematical problems.

"If one can break the security of the cryptographic scheme, then one could also solve the mathematical problem."

Currently used problems:

- Discrete logarithm
- Factoring

  Given N, find p, q such that $N = p \cdot q$

*Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM Journal of Computations 1997

Security Paradigm

👉 The security in public-key cryptography relies on presumably hard mathematical problems.

"If one can break the security of the cryptographic scheme, then one could also solve the mathematical problem."

Currently used problems:

- ~~Discrete logarithm~~
- ~~Factoring~~

  Given N, find p, q such that $N = p \cdot q$

⚠ $\exists$ poly-time quantum algorithm [Sho97]*

Quantum-resistant candidates:

- Codes
- Lattices
- Isogenies
- Multivariate systems
- **?**

*Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM Journal of Computations 1997

Security Paradigm

👉 The security in public-key cryptography relies on presumably hard mathematical problems.

Currently used problems:

- ~~Discrete logarithm~~
- ~~Factoring~~

  Given N, find p, q such that $N = p \cdot q$

⚠ ∃ poly-time quantum algorithm [Sho97]*

Quantum-resistant candidates:

- Codes
- Lattices today's focus
- Isogenies
- Multivariate systems
- **?**

*Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM Journal of Computations 1997

US National Institute of Standards and Technology (NIST) Project

- 2016: start of NIST's post-quantum cryptography project*
- 2022+25: selection of 5 schemes, 3 of them relying on lattice problems

Public Key Encryption:

- Kyber 

- HQC

Digital Signature:

- Dilithium 

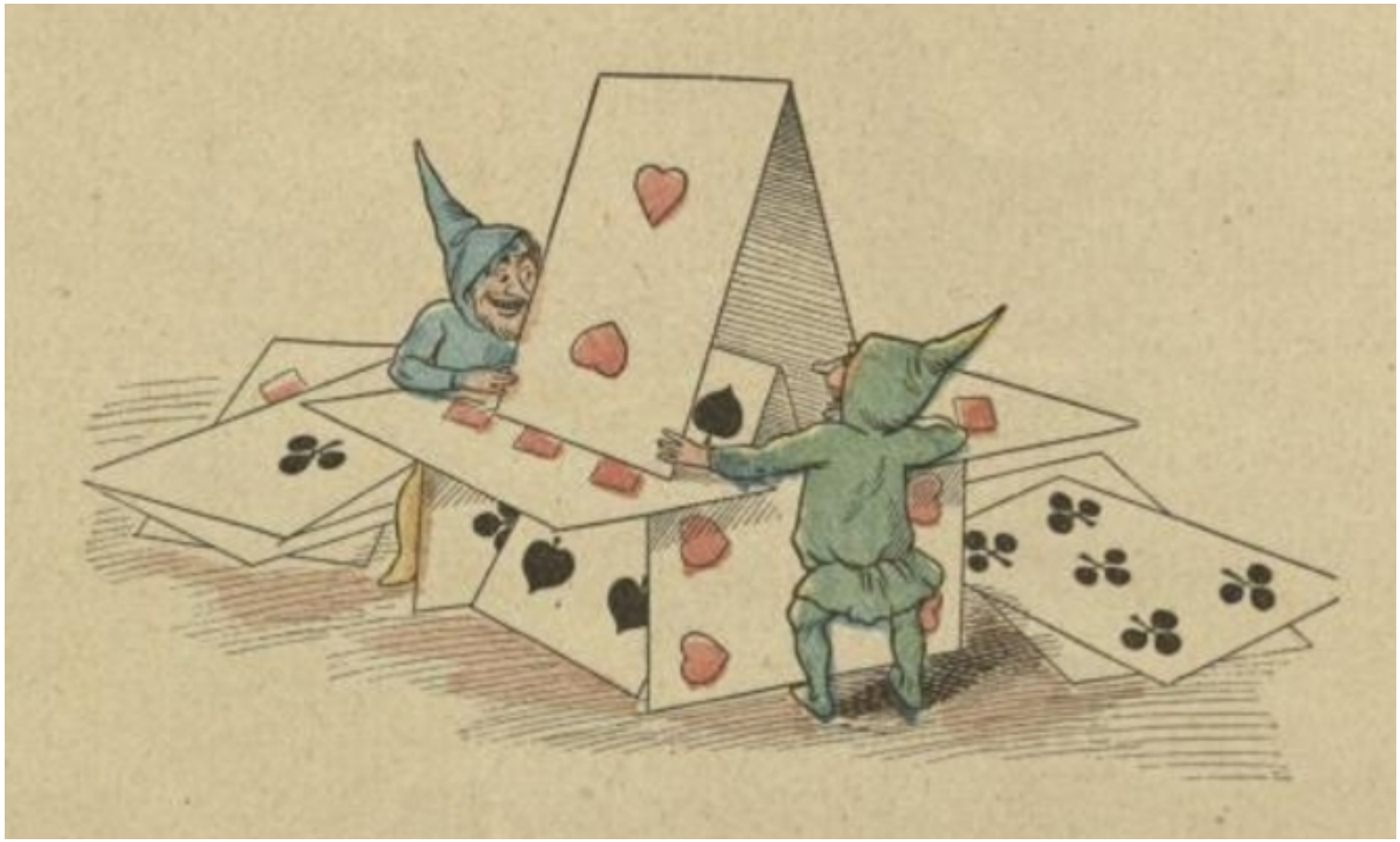
- Falcon 

- SPHINCS+ 

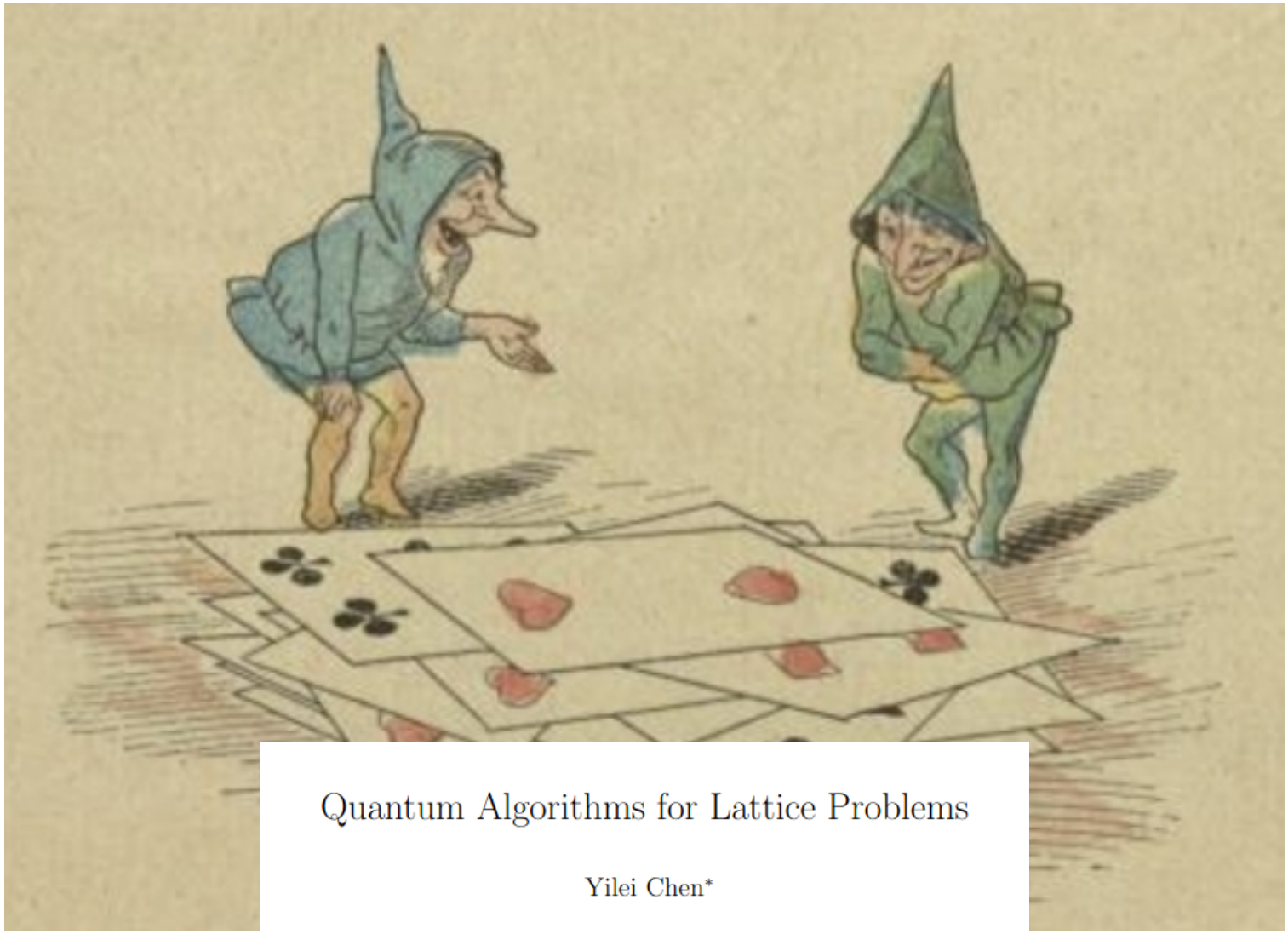
Lattice-based cryptography plays a leading role in designing post-quantum cryptography.

*https://csrc.nist.gov/projects/post-quantum-cryptography

Really Post-Quantum?



Really Post-Quantum?



Quantum Algorithms for Lattice Problems

Yilei Chen*

April 18, 2024

ia.cr/2024/555

Really Post-Quantum?

Quantum Algorithms for Lattice Problems

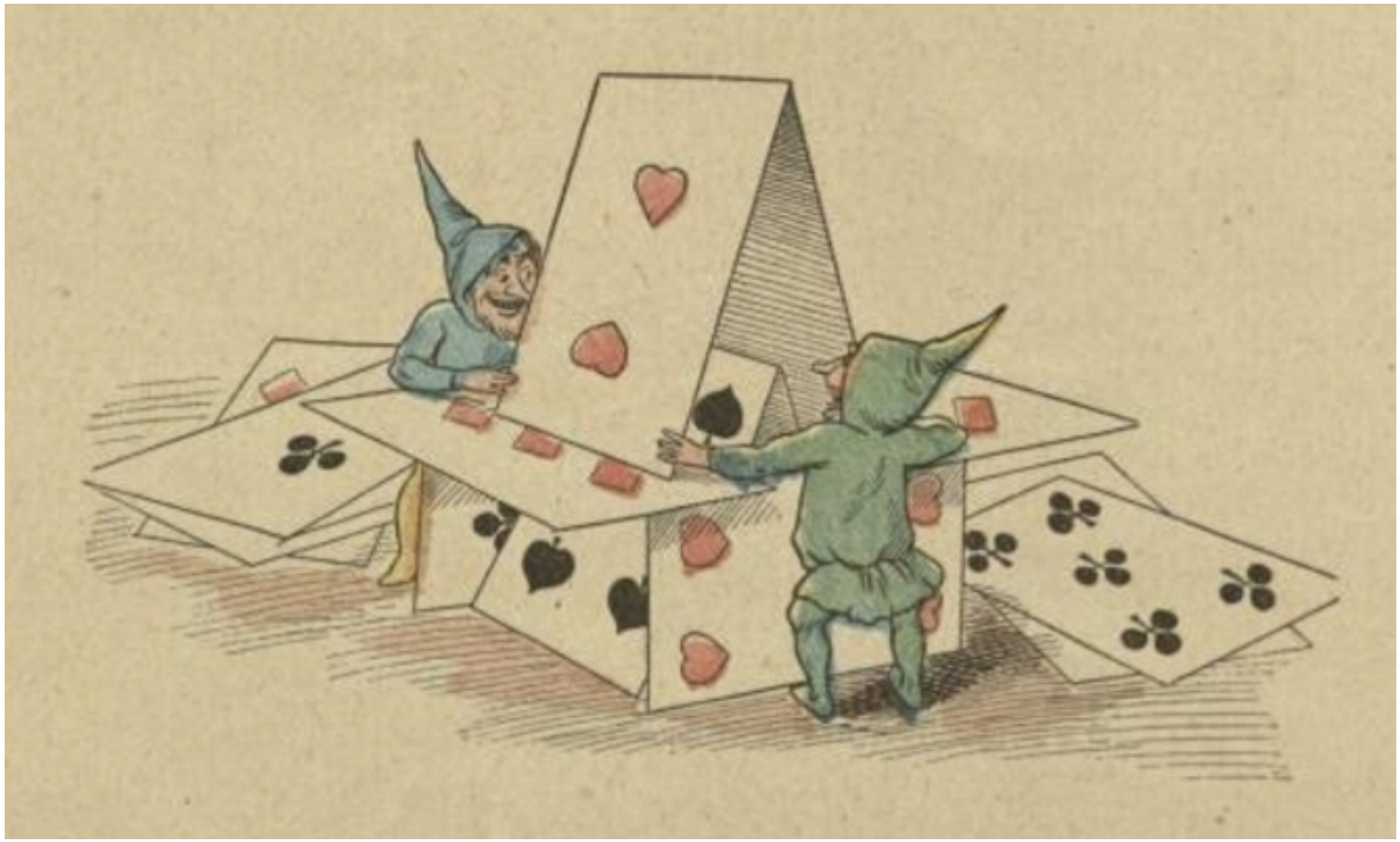
ERROR IN PROOF!

Yilei Chen

April 18, 2024

ia.cr/2024/555

Really Post-Quantum?!



Lattices Can Do Much More!

Fully Homomorphic Encryption

* outsource data and analysis on the data
* threshold variant: multiple parties involved
* very powerful
* only known from lattices so far!

Overview of Today's Presentation

Questions we are trying to answer today:

- Part 1: *What are lattices?*
- Part 2: *What are lattice problems?*
- Part 3: *What is lattice-based cryptography?*
- Part 4: *What are some (of my) current challenges?*

References:

- The Lattice Club [website]
- Vinod Vaikuntanathan's [lecture notes]
- A Crash Course I Gave [lecture notes]

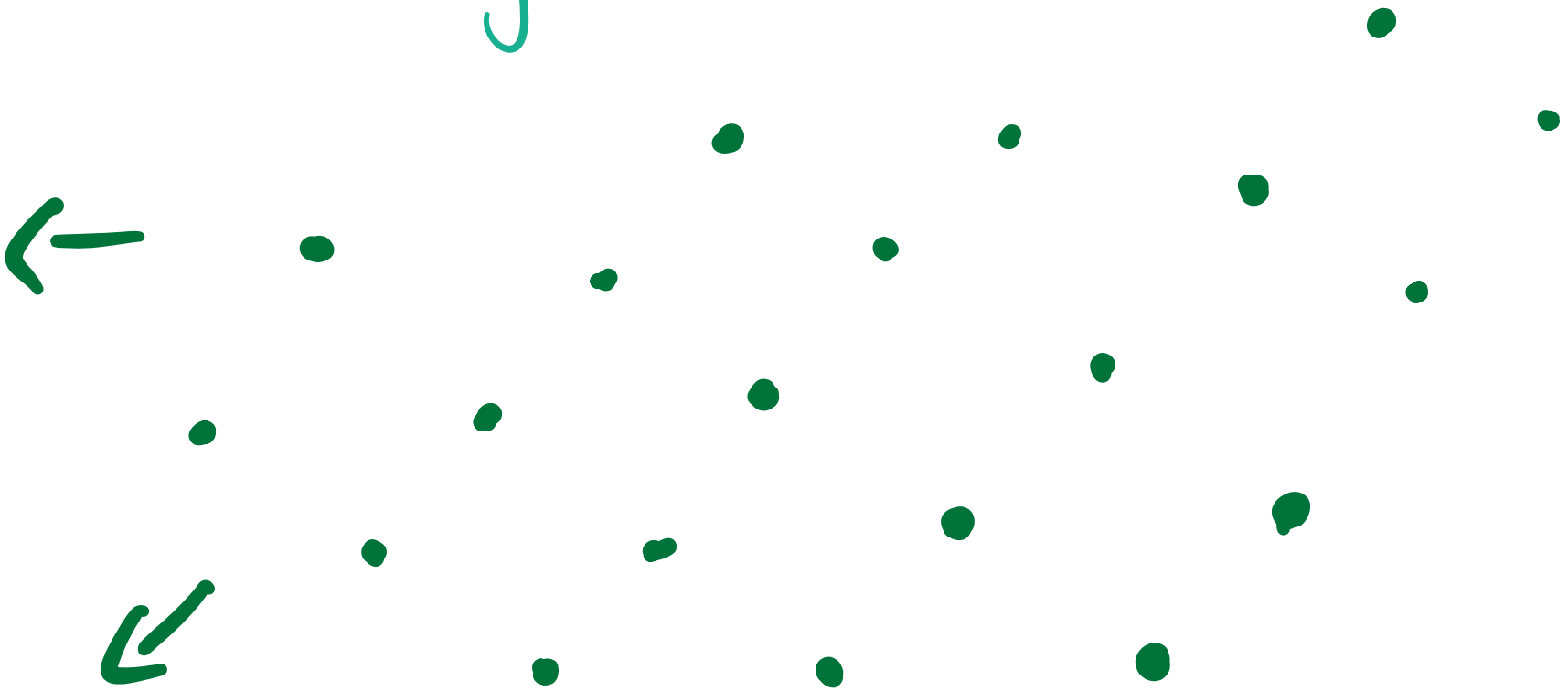
Part 1:

What is a lattice?

Euclidean Lattices

My personal definition:

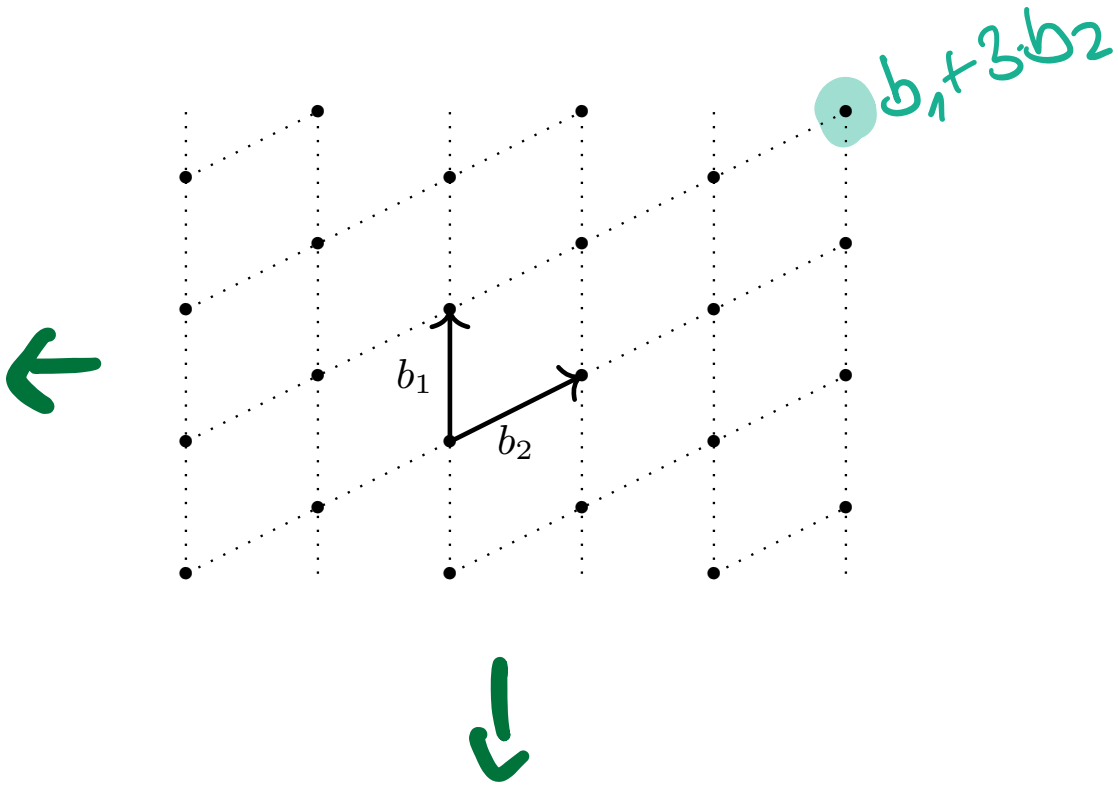
"A lattice is an infinite, regular grid in high dimensions."



Euclidean Lattices

Let $\mathbf{B} = (\mathbf{b}_i)_{i=1,\ldots,n}$ be a set of linearly independent vectors, defining the lattice

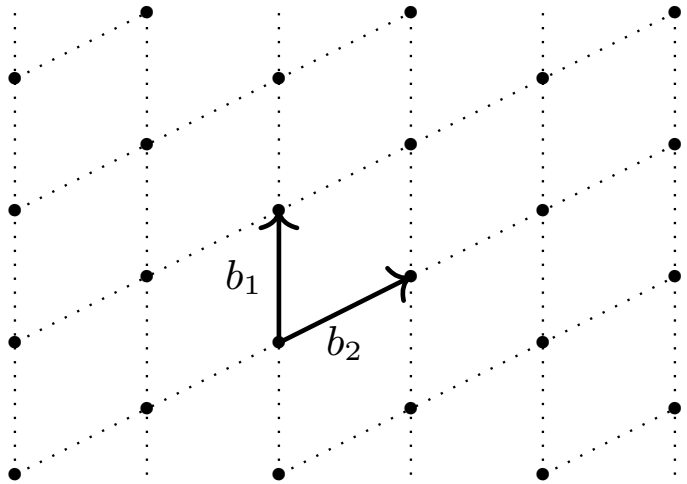
$$\Lambda(\mathbf{B}) = \left\{ \sum_{i=1}^{n} z_i \mathbf{b}_i : z_i \in \mathbb{Z} \right\}.$$

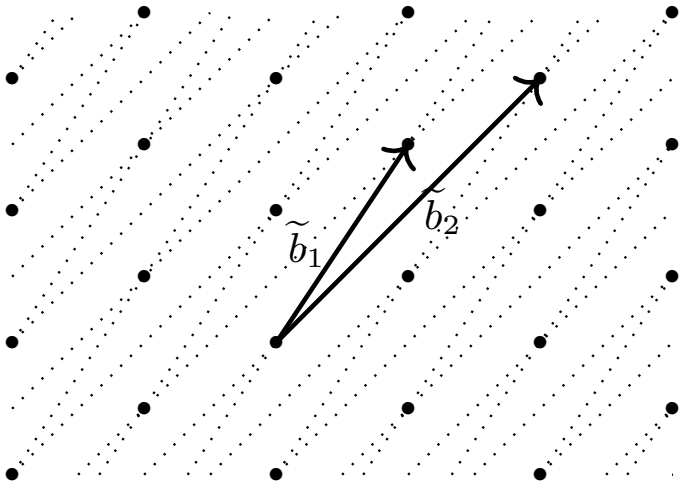


Euclidean Lattices

Let $\mathbf{B} = (\mathbf{b}_i)_{i=1,\dots,n}$ be a set of linearly independent vectors, defining the lattice

$$\Lambda(\mathbf{B}) = \left\{ \sum_{i=1}^{n} z_i \mathbf{b}_i : z_i \in \mathbb{Z} \right\}.$$



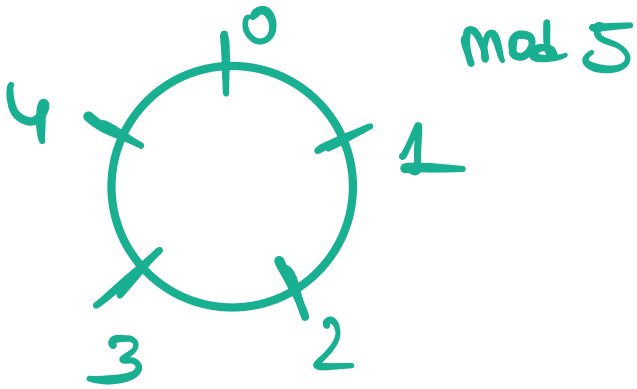


- $\mathbf{B}$ is the description of the lattice Λ, n the dimension
- Λ can have many different descriptions

Special Lattices

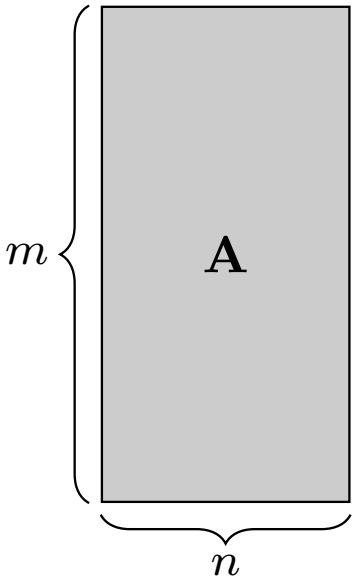
$\mathbb{Z}_q$ = integers $\mathbb{Z}$ modulo q

$\approx \{0, \dots, q-1\}$



Let $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$ for some $n, m, q \in \mathbb{N}$ with $n \leq m$

$$\Lambda_q^{\perp}(\mathbf{A}) = \left\{ \mathbf{y} \in \mathbb{Z}^m : \mathbf{A}^T \mathbf{y} = \mathbf{0} \bmod q \right\}$$



- infinte : y composed of multiples of q is in the lattice
- regular : y, z in the lattice $\Rightarrow A^T(y+z) = A^T y + A^T z = 0$
- dimension : m

Concrete Example

$q = 5$

$A^T = \begin{pmatrix} 1 & 0 & 2 & 3 \\ 0 & 1 & 3 & 1 \end{pmatrix}$

$y = \begin{pmatrix} 3 \\ 2 \\ 1 \\ 0 \end{pmatrix}$

$A^T y = \begin{pmatrix} 3+0+2+0 \\ 0+2+3+0 \end{pmatrix} = \begin{pmatrix} 5 \\ 5 \end{pmatrix}$

$= \begin{pmatrix} 0 \\ 0 \end{pmatrix} \mod 5$

$\Rightarrow y \in \Lambda_q^{\perp}(A)$

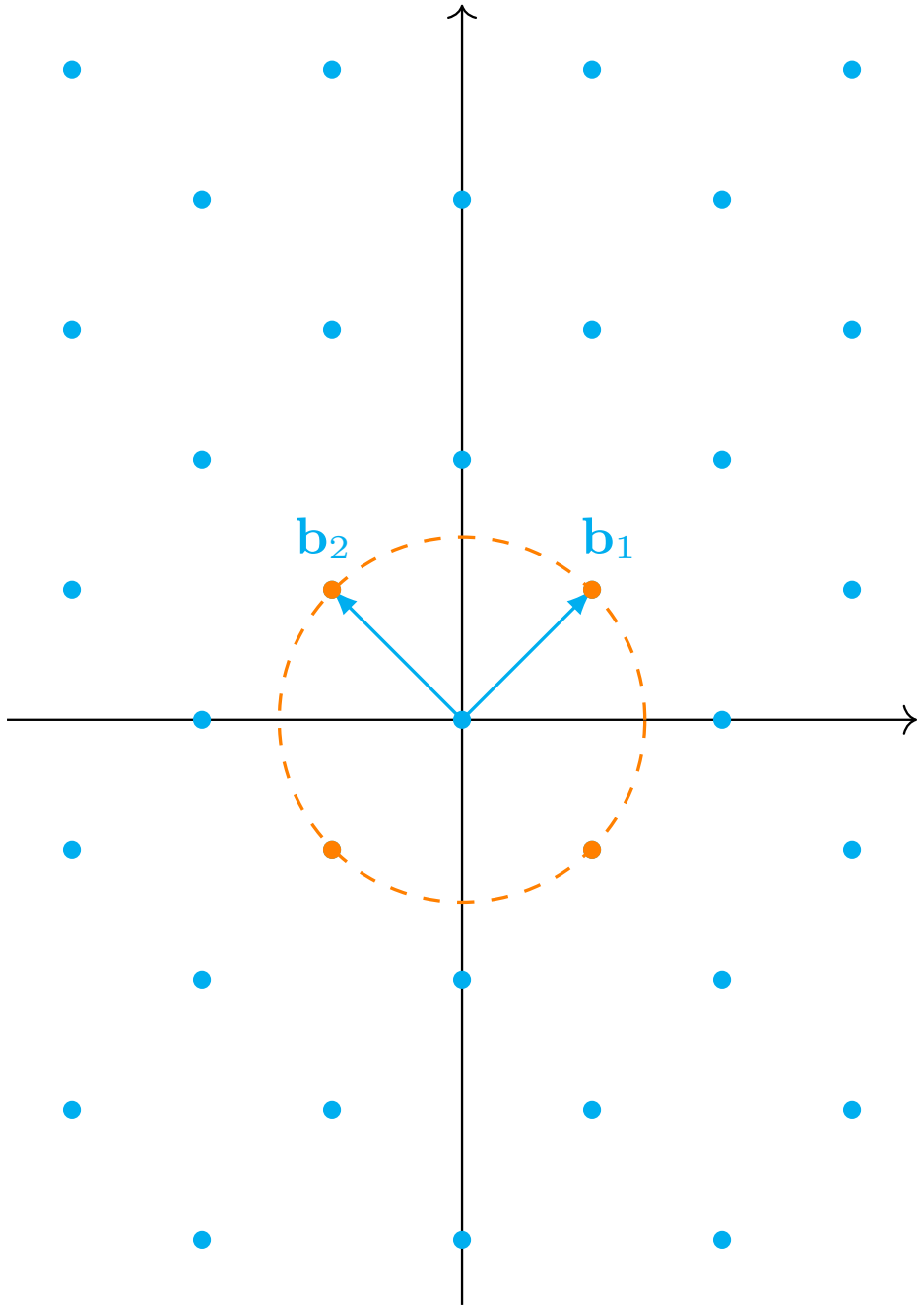
Part 2:

What are lattice problems?

Shortest Vector Problem

Given a lattice Λ.

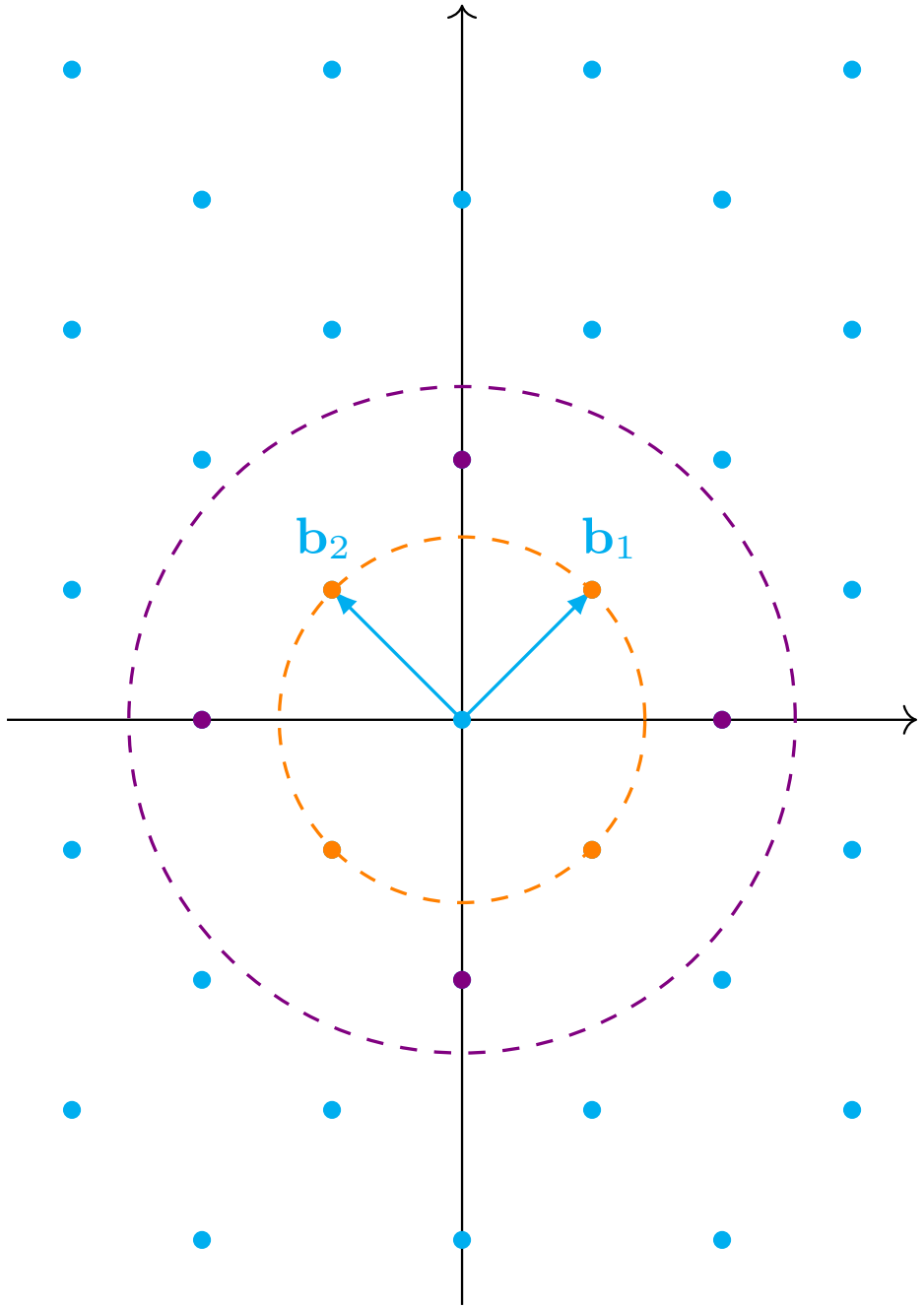
The **shortest vector problem** (SVP) asks to find a non-zero vector in Λ of shortest norm.



Shortest Vector Problem

Given a lattice Λ.

The **approximate shortest vector problem** (approx-SVP) asks to find a non-zero vector in Λ of approximately shortest norm.



Shortest Vector Problem

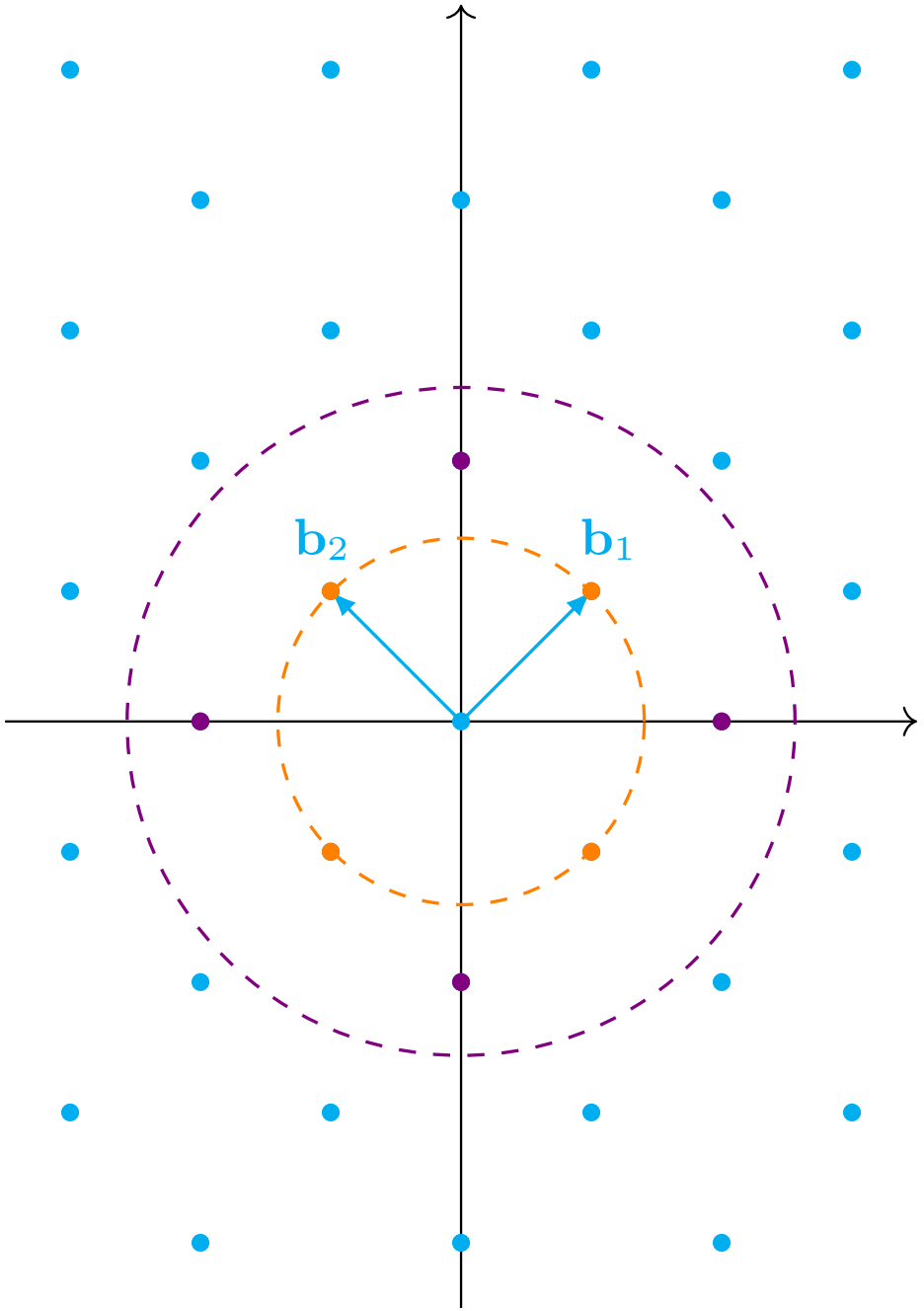
Given a lattice Λ.

The **approximate shortest vector problem** (approx-SVP) asks to find a non-zero vector in Λ of approximately shortest norm.

The complexity of approx-SVP increases with the dimension of Λ, but decreases with the approximation factor.

Conjecture:

There is no polynomial-time classical or quantum algorithm that solves approx-SVP **for all** lattices to within polynomial factors.

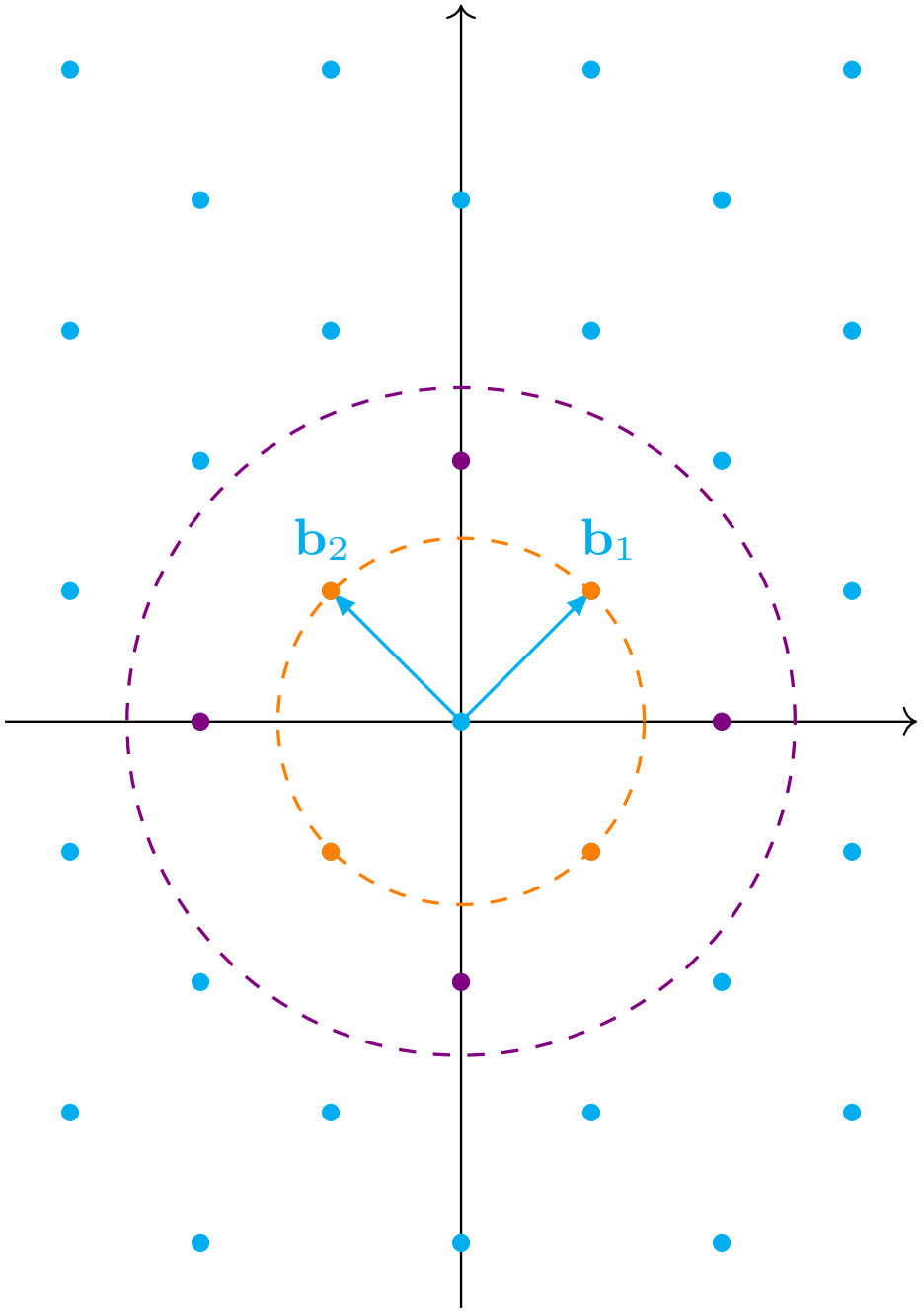


Shortest Vector Problem

But approx-SVP might be easy for some lattices !

For instance $\mathbb{Z}^n$ ⇝ unit vector

How do we generate "hard" instanes of SVP?

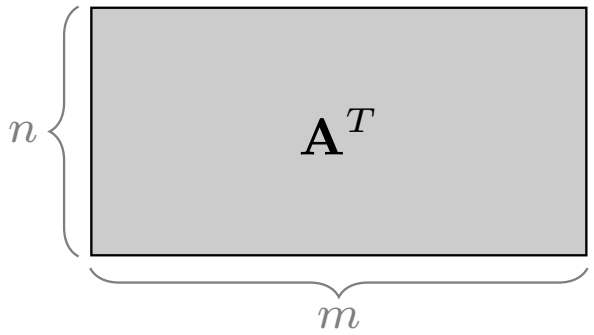


Conjecture:

There is no polynomial-time classical or quantum algorithm that solves approx-SVP **for all** lattices to within polynomial factors.

Short Integer Solution [Ajt96]*

Given a matrix $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$ sampled uniformly at random and bound $\beta > 0$.



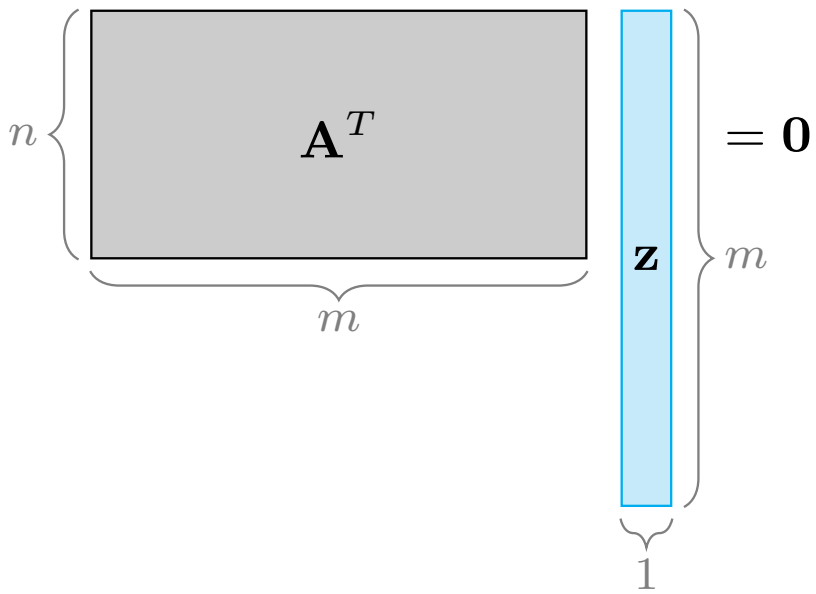
*Ajtai, *Generating hard instances of lattice problems*, STOC'96

Short Integer Solution [Ajt96]*

Given a matrix $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$ sampled uniformly at random and bound $\beta > 0$.

The **short integer solution** (SIS_β) problem asks to find a vector $\mathbf{z} \in \mathbb{Z}^m$ of norm $0 < \|\mathbf{z}\|_2 \leq \beta$ such that

$$\mathbf{A}^T \mathbf{z} = \mathbf{0} \bmod q.$$



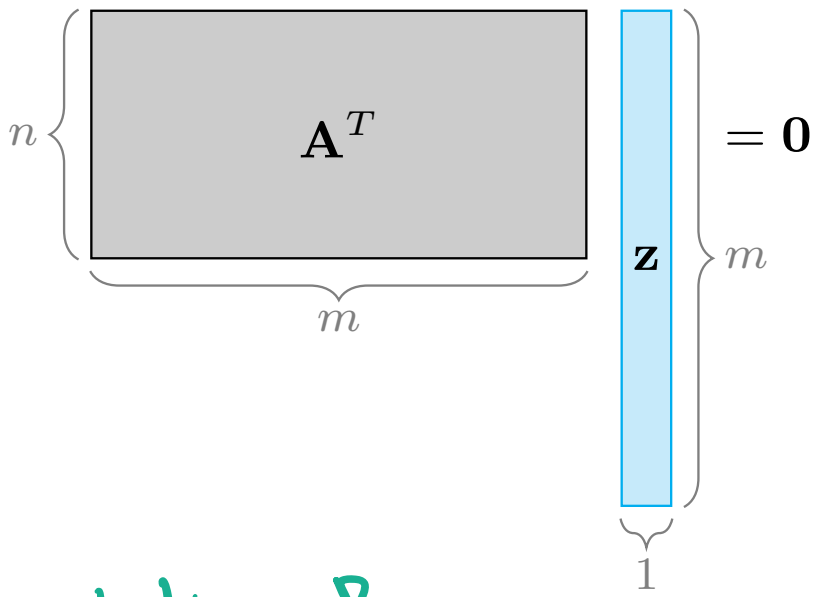
*Ajtai, *Generating hard instances of lattice problems*, STOC'96

Short Integer Solution [Ajt96]*

Given a matrix $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$ sampled uniformly at random and bound $\beta > 0$.

The **short integer solution** (SIS_β) problem asks to find a vector $\mathbf{z} \in \mathbb{Z}^m$ of norm $0 < \|\mathbf{z}\|_2 \leq \beta$ such that

$$\mathbf{A}^T \mathbf{z} = \mathbf{0} \bmod q.$$



⚠ The norm restriction makes it a hard problem!

else $z = \begin{pmatrix} q \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ is a solution !

$\beta \geq q$

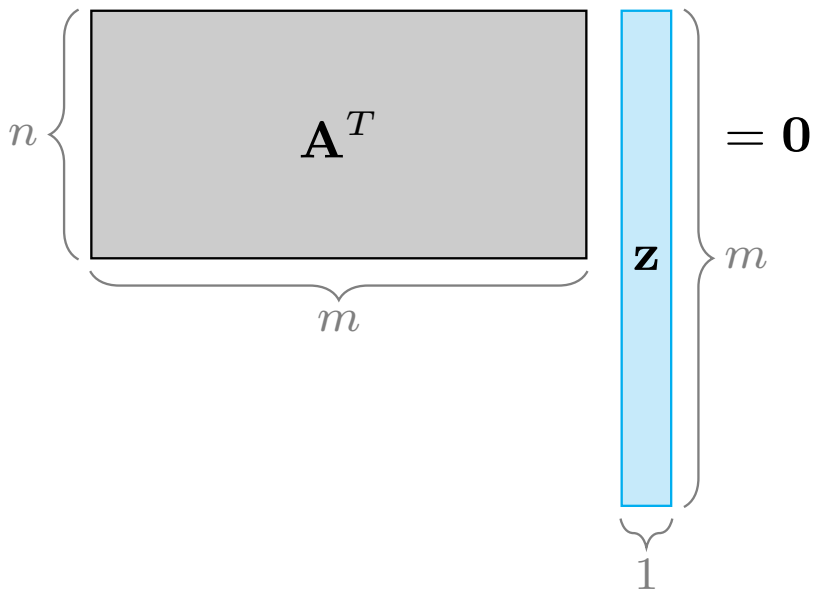
*Ajtai, *Generating hard instances of lattice problems*, STOC'96

Short Integer Solution [Ajt96]*

Given a matrix $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$ sampled uniformly at random and bound $\beta > 0$.

The **short integer solution** (SIS_β) problem asks to find a vector $\mathbf{z} \in \mathbb{Z}^m$ of norm $0 < \|\mathbf{z}\|_2 \leq \beta$ such that

$$\mathbf{A}^T \mathbf{z} = \mathbf{0} \bmod q.$$



⚠ The norm restriction makes it a hard problem!

Recall:

$$\Lambda_q^\perp(\mathbf{A}) = \left\{ \mathbf{y} \in \mathbb{Z}^m : \mathbf{A}^T \mathbf{y} = \mathbf{0} \bmod q \right\}$$

👉 Solving SIS_β equals finding a short vector in the special & random lattice $\Lambda_q^\perp(\mathbf{A})$

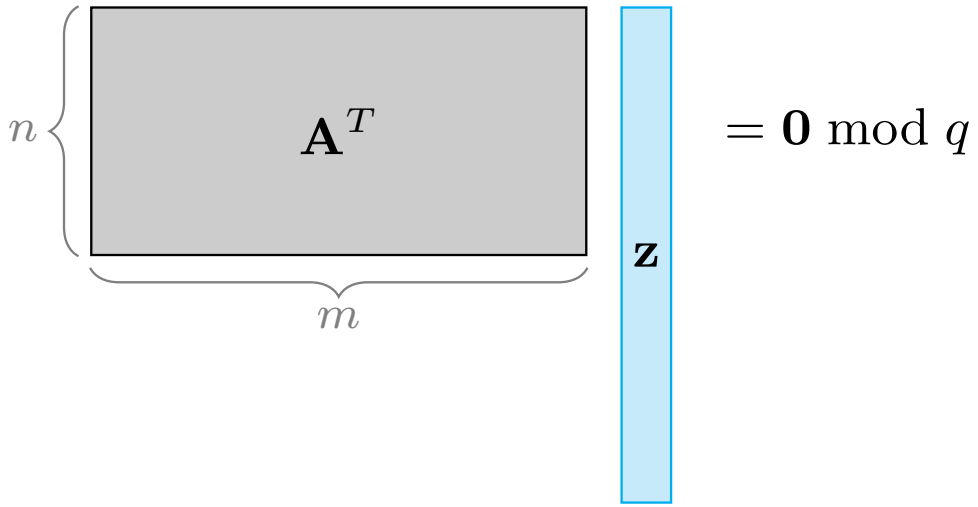
"hard instanes"

*Ajtai, *Generating hard instances of lattice problems*, STOC'96

Example Parameters for Short Integer Solution

Parameters:

- $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and $\|\mathbf{z}\|_2 \leq \beta$
- $m = ?$
- $n = ?$
- $q = ?$
- $\beta = ?$



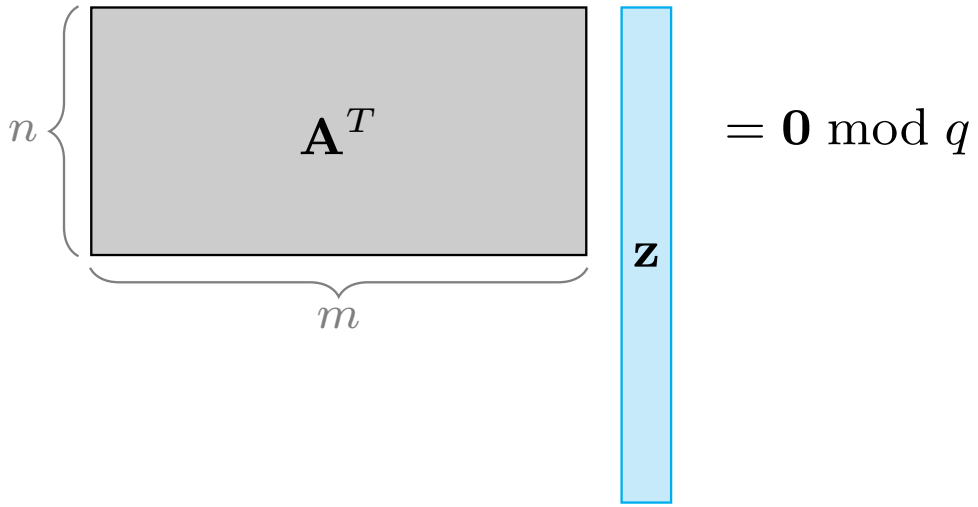
👉 Use the lattice estimator*

*https://github.com/malb/lattice-estimator

Example Parameters for Short Integer Solution

Parameters:

- $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and $\|\mathbf{z}\|_2 \leq \beta$
- m is a function in n
- $n = ?$
- $q = ?$
- $\beta = ?$



n	q	β	security bits
50	2^5	30	39
50	2^{10}	30	62
50	2^{10}	50	47
200	2^{10}	50	212
200	2^{10}	200	107
500	2^{10}	500	213

some days on your own

millions of years all humans together

[⋆] https://github.com/malb/lattice-estimator

Part 3:

What is lattice-based cryptography?

Collision-Resistant Hash Function from SIS [Ajt96]*

A function f : Domain $\to$ Range is called **collision-resistant** if it is hard to output two elements $\mathbf{x}, \mathbf{x}' \in$ Domain such that

$$f(\mathbf{x}) = f(\mathbf{x}') \text{ and } \mathbf{x} \neq \mathbf{x}'.$$

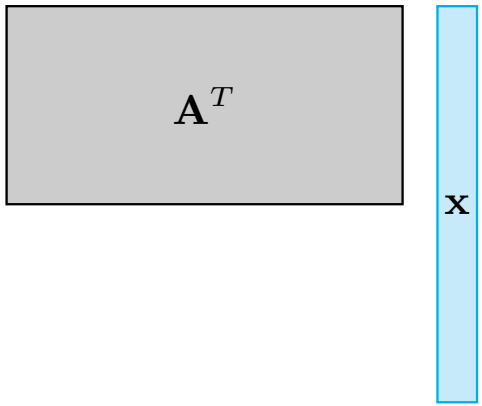
*Ajtai, *Generating hard instances of lattice problems*, STOC'96

Collision-Resistant Hash Function from SIS [Ajt96]*

A function f : Domain $\to$ Range is called **collision-resistant** if it is hard to output two elements $\mathbf{x}, \mathbf{x}' \in$ Domain such that

$$f(\mathbf{x}) = f(\mathbf{x}') \text{ and } \mathbf{x} \neq \mathbf{x}'.$$

Set $f_{\mathbf{A}} : \{0,1\}^m \to \mathbb{Z}_q^n$ with $f_{\mathbf{A}}(\mathbf{x}) = \mathbf{A}^T\mathbf{x} \bmod q$ for $\mathbf{A} \leftarrow \text{Unif}(\mathbb{Z}_q^{m \times n})$.



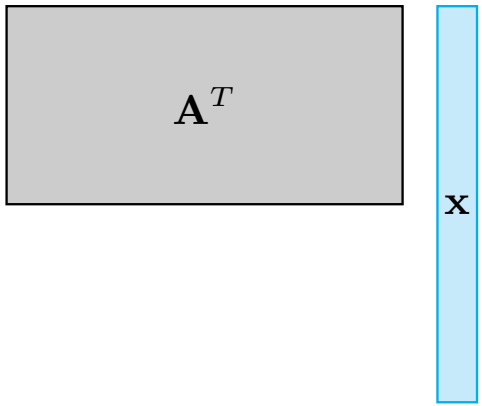
*Ajtai, *Generating hard instances of lattice problems*, STOC'96

Collision-Resistant Hash Function from SIS [Ajt96]*

A function f : Domain $\to$ Range is called **collision-resistant** if it is hard to output two elements $\mathbf{x}, \mathbf{x}' \in$ Domain such that

$$f(\mathbf{x}) = f(\mathbf{x}') \text{ and } \mathbf{x} \neq \mathbf{x}'.$$

Set $f_{\mathbf{A}} : \{0,1\}^m \to \mathbb{Z}_q^n$ with $f_{\mathbf{A}}(\mathbf{x}) = \mathbf{A}^T\mathbf{x} \bmod q$ for $\mathbf{A} \leftarrow \text{Unif}(\mathbb{Z}_q^{m \times n})$.



⚙ Exercise: Assuming SIS is hard to solve for $\beta = \sqrt{m}$, then $f_{\mathbf{A}}$ is collision-resistant

sketch: let $x \neq x' \in \{0,1\}^m$ st $A^T x = A^T x'$

$\Leftrightarrow$ $z = x - x' \in \{-1,0,1\}^m$ $A^T z = A^T x - A^T x' = 0$

$\|z\| \leq \sqrt{m}$

*Ajtai, *Generating hard instances of lattice problems*, STOC'96

Digital Signatures [DH76]*

*Diffie and Hellman, *New directions in cryptography*, IEEE Trans.Inf.Theory 1976

Digital Signatures from Lattices [GPV08]*

$f_A : x \mapsto A^T x$

- collision-resistant
- easy to compute
- hard to invert *

*unless:

$\longrightarrow (A, \text{PreSampler})$

$\forall y$: $x \leftarrow \text{PreSampler}(y)$

* $A^T x = y \bmod q$
* $\|x\|$ small

*Gentry, Peikert, Vaikuntanathan, *Trapdoors for hard lattices and new cryptographic constructions*, STOC'08

Digital Signatures from Lattices [GPV08]*

$f_A : x \mapsto A^T x$

- collision-resistant
- easy to compute
- hard to invert *

*unless:

$\longrightarrow (A, \text{PreSampler})$

$\forall y$: $x \leftarrow \text{PreSampler}(y)$

* $A^T x = y \bmod q$
* $\|x\|$ small

Signatures:

$pk = A$ $sk = \text{PreSampler}$

sign: $\text{Hash}(\text{📄}) =: y$

$\text{PreSampler}(y) \to x$

✏ $= x$

$x =$ ✏

Verify: 👁 $\|x\|$ small

$A^T x = \text{Hash}(\text{📄})$

*Gentry, Peikert, Vaikuntanathan, *Trapdoors for hard lattices and new cryptographic constructions*, STOC'08

Part 4:

What are (my) current challenges?

Digital Signatures [DH76]*

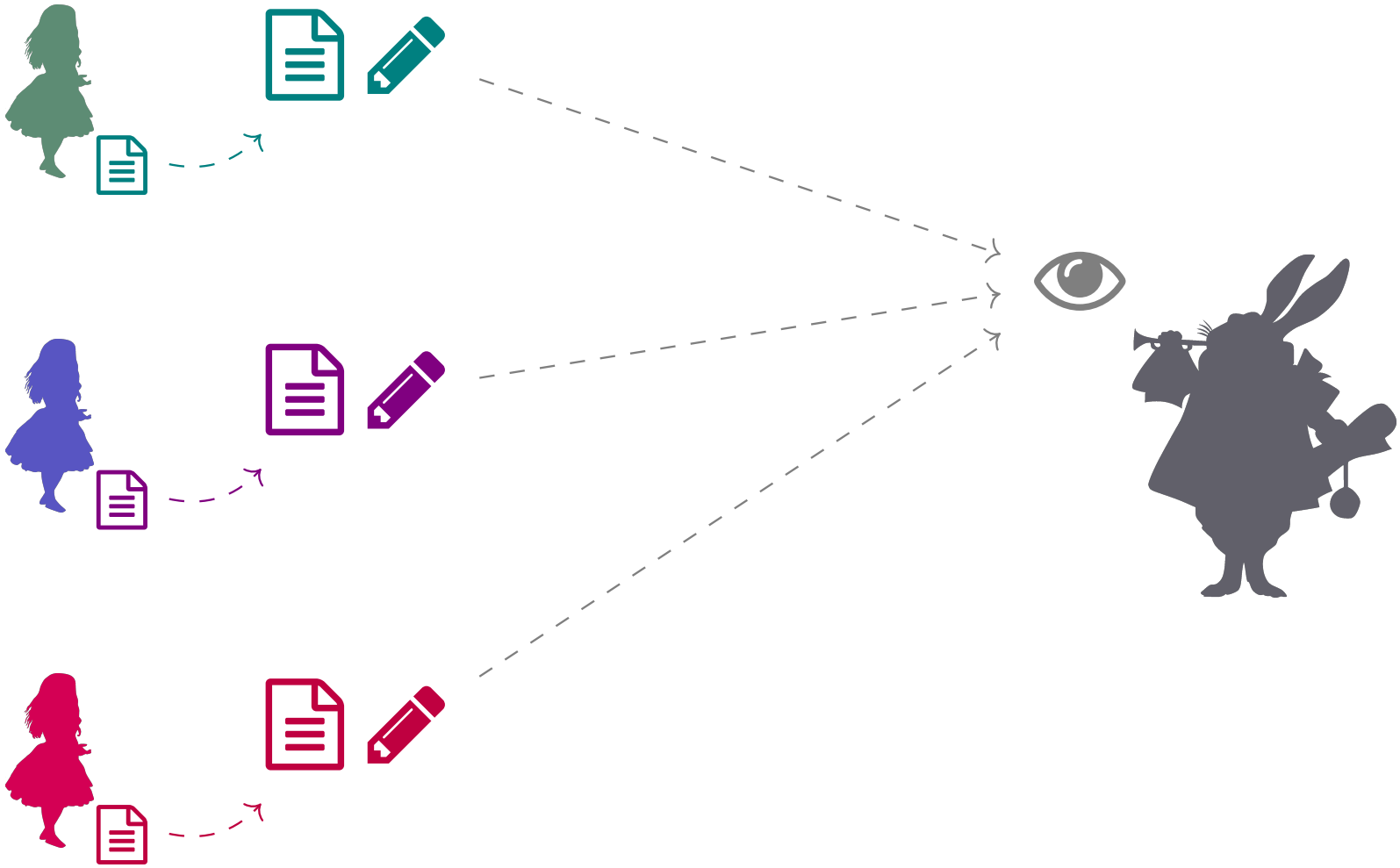
Motivation:

- Digital analogue of handprint signature
- Even more secure?
- Even more functionalities? $\Rightarrow$ my focus

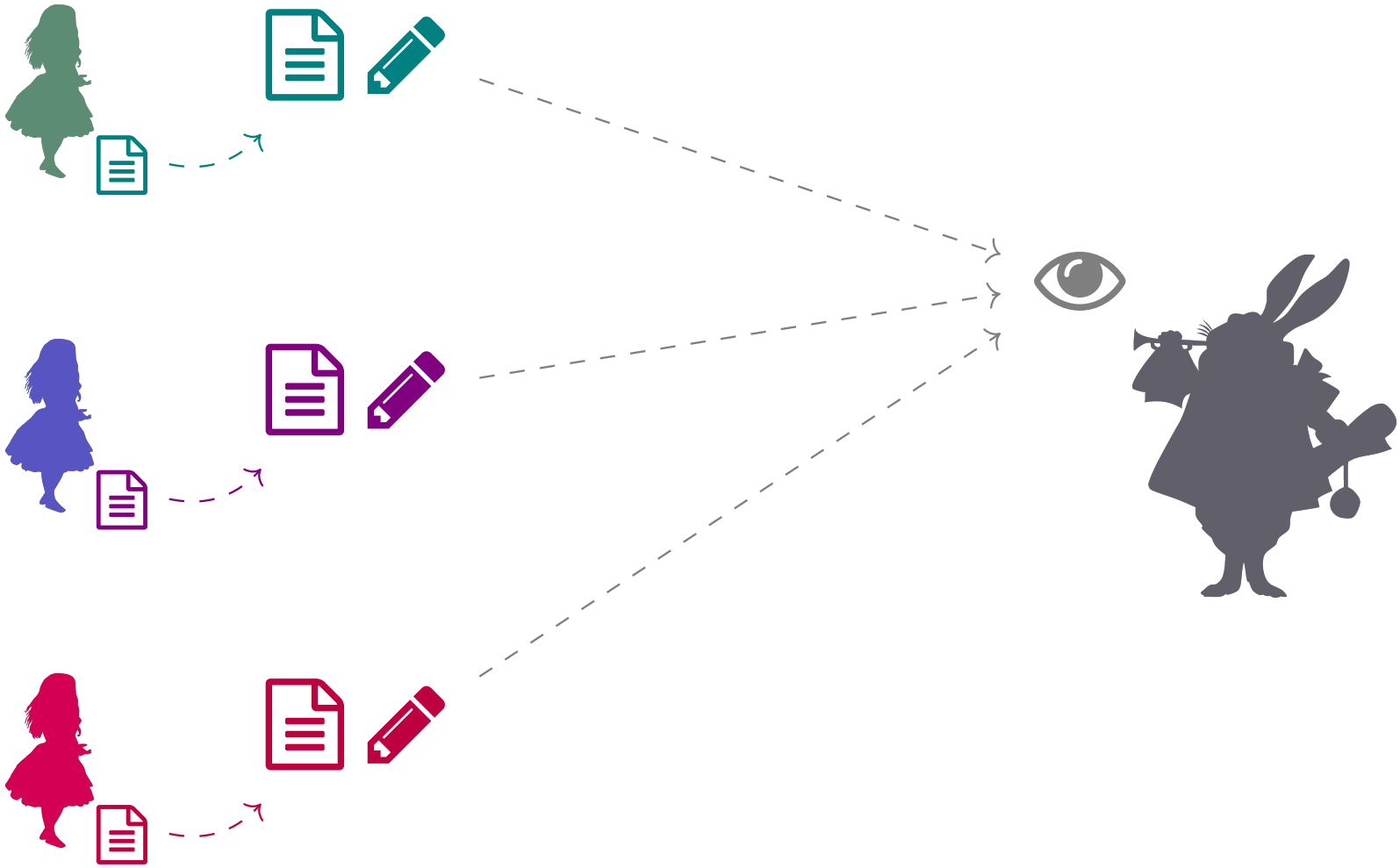
*Diffie and Hellman, *New directions in cryptography*, IEEE Trans.Inf.Theory 1976

Multiple Signers and Messages, but Same Verifier

Multiple Signers and Messages, but Same Verifier



Multiple Signers and Messages, but Same Verifier



Q: Can we combine ✎, ✎ and ✎ into a single compact signature?

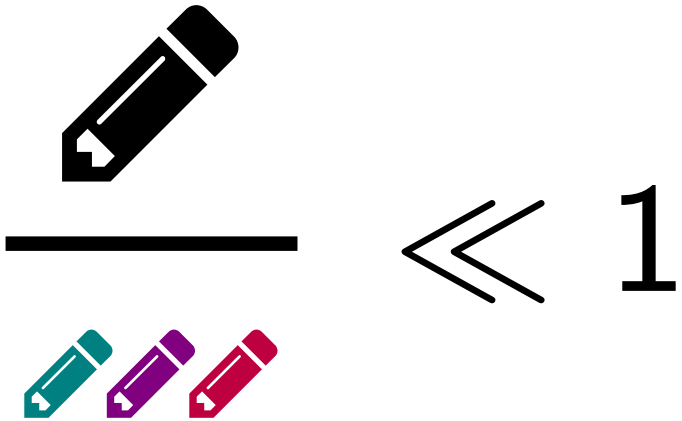
And more generally for $N \gg 3$ many signatures?

Aggregate Signatures [BGLS03]*

*Boneh, Gentry, Lynn and Shacham, *Aggregate and Verifiably Encrypted Signatures from Bilinear Maps*, EUROCRYPT'03

Objectives

Compression Rate:



Preferable Goals:

- As low compression rates as possible
- Presumed post-quantum security
- Compatible with international standards (Dilithium and Falcon)
- As fast signing, aggregation and verification as possible

Research Question:

Can we construct an

aggregate signature scheme

based on **Euclidean lattices?**

Research Question:

Can we construct an

aggregate signature scheme

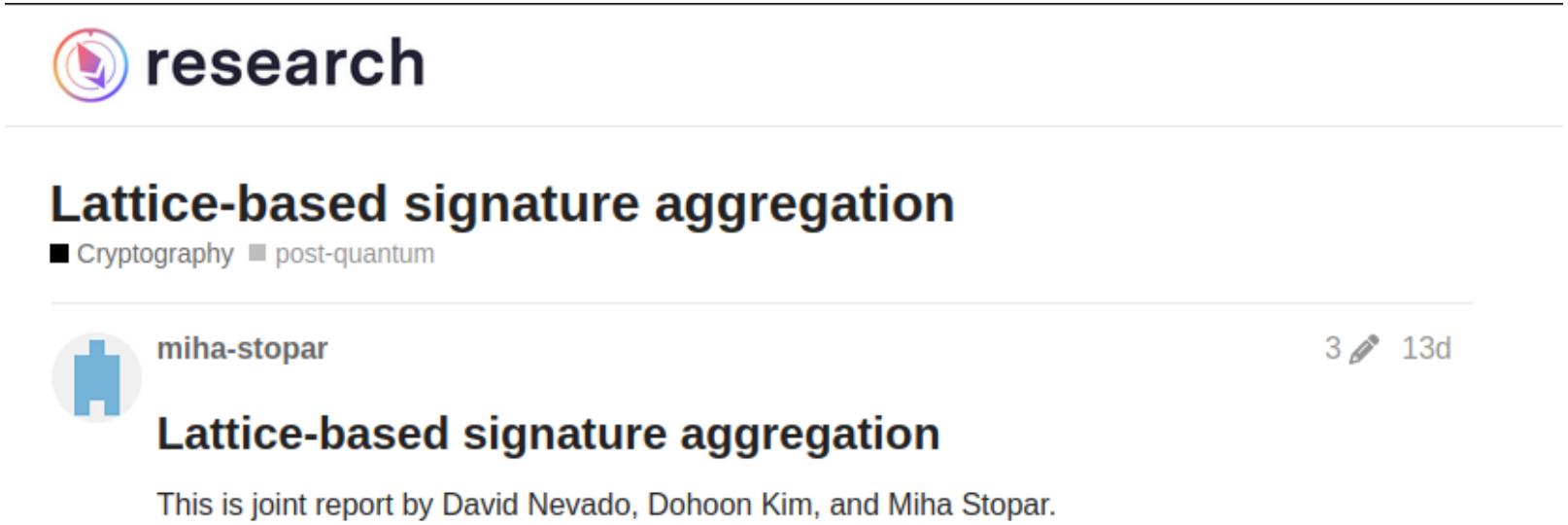
based on **Euclidean lattices?**

Failure:
compression rate > 1
Dilithium-type
ia.cr/2021/263
CFAIL'22
with A. Roux-Langlois

Semi-Success:
$1 >$ compression rate > 0.99
Dilithium-type
ia.cr/2023/159
ESORICS'23
with A. Takahashi

Success:
compression rate $\to 0.06$
Falcon
ia.cr/2024/311
CRYPTO'24
with M. Aardal, D. Aranha
S. Kolby, A. Takahashi

Relevant for Ethereum?*



*https://ethresear.ch/t/lattice-based-signature-aggregation/22282

Relevant for Ethereum?*

Summary

The two approaches for signature aggregation—the one from the paper Aggregating Falcon Signatures with LaBRADOR 26 and the Lazer approach—are quite similar, so we believe our

Share

(based on the Lazer code) are relevant for both.

The most compelling feature of the benchmarked lattice-based signature aggregation scheme is its proof size, while the biggest obstacle to adoption may be the verification time. Verification performance could likely be improved using multi-threading techniques, though this requires further investigation. That said, improvements to both the LaBRADOR protocol and its C implementation are already underway by the LaBRADOR authors, and these are expected to speed up verification—though it's currently difficult to quantify by how much.

*https://ethresear.ch/t/lattice-based-signature-aggregation/22282

Wrap-Up

🏁 Hopefully you have now a rough idea:

- Part 1: *What lattices are!*
- Part 2: *What lattice problems are!*
- Part 3: *What lattice-based cryptography is!*
- Part 4: *What (my) particular challenges are!*

Any questions or interested in my research?

- ✉ Write me an e-mail

Wrap-Up

🏁 Hopefully you have now a rough idea:

- Part 1: *What lattices are!*
- Part 2: *What lattice problems are!*
- Part 3: *What lattice-based cryptography is!*
- Part 4: *What (my) particular challenges are!*

Any questions or interested in my research?

- ✉ Write me an e-mail

Thanks!


Miklós Ajtai.
Generating hard instances of lattice problems (extended abstract).
In *STOC*, pages 99–108. ACM, 1996.


Dan Boneh, Craig Gentry, Ben Lynn, and Hovav Shacham.
Aggregate and verifiably encrypted signatures from bilinear maps.
In *EUROCRYPT*, volume 2656 of *Lecture Notes in Computer Science*, pages 416–432. Springer, 2003.


Whitfield Diffie and Martin E. Hellman.
New directions in cryptography.
IEEE Trans. Inf. Theory, 22(6):644–654, 1976.


Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan.
Trapdoors for hard lattices and new cryptographic constructions.
In *STOC*, pages 197–206. ACM, 2008.


Peter W. Shor.
Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer.
SIAM J. Comput., 26(5):1484–1509, 1997.