Lattice-Based Cryptography

A Gentle Introduction

Katharina Boudgoust

CNRS, Univ Montpellier, LIRMM, France

Prelude

My academic path:

- **2018** Master in Mathematics, KIT Karlsruhe
- **2021** PhD in Cryptography, Irisa Rennes
- **2022-23** Postdoc in Cryptography, Aarhus University
- **Since February** Chargée de Recherche CNRS, LIRMM

Misc:

- Women in Cryptography
- Climbing and Hiking

Cryptography

👉 The word **cryptography** is composed of the two ancient Greek words *kryptos* (hidden) and *graphein* (to write). Its goal is to provide **secure communication**.

- Encryption
- Digital Signatures

Cryptography

👉 The word **cryptography** is composed of the two ancient Greek words *kryptos* (hidden) and *graphein* (to write). Its goal is to provide **secure communication**.

- Encryption
- Digital Signatures
- Zero-Knowledge Proofs
- Fully-Homomorphic Encryption

5	3			7				
6			1	9	5			
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9

Context

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 $N = p \cdot q$

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

Context

👉 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 $N = p \cdot q$

⚠ $\exists$ 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

Context

👍 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 $N = p \cdot q$

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

Quantum-resistant candidates:

- Codes
- Lattices $\Rightarrow$ my 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: selection of 4 schemes, 3 of them relying on lattice problems

Public Key Encryption:

- Kyber

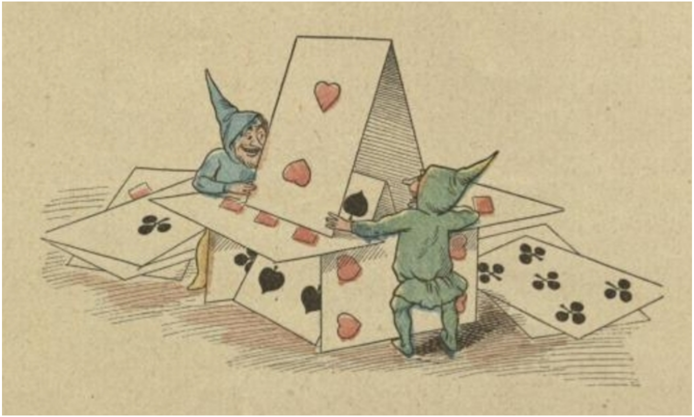
Digital Signature:

- 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

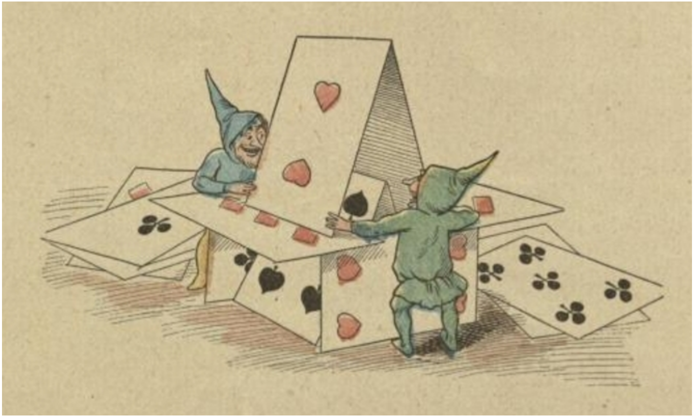
ERROR IN PROOF!

Yilei Chen

April 18, 2024

ia.cr/2024/555

Really Post-Quantum?



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]
- Crash Course Spring 2022 [lecture notes]

Part 1:

What is a lattice?

Euclidean Lattices

An Euclidean lattice Λ is a discrete additive subgroup of $\mathbb{R}^n$.

Euclidean Lattices

An Euclidean lattice Λ is a discrete additive subgroup of $\mathbb{R}^n$.

- additive subgroup: $\mathbf{0} \in \Lambda$, and for all $\mathbf{x}, \mathbf{y} \in \Lambda$ it holds $\mathbf{x} + \mathbf{y}, -\mathbf{x} \in \Lambda$;
- discrete: every $\mathbf{x} \in \Lambda$ has a neighborhood in which $\mathbf{x}$ is the only lattice point.
  $\exists \varepsilon > 0$ such that $\mathcal{B}(\mathbf{x}, \varepsilon) \cap \Lambda = \{\, \mathbf{x} \,\}$

Euclidean Lattices

An Euclidean lattice Λ is a discrete additive subgroup of $\mathbb{R}^n$.

- additive subgroup: $\mathbf{0} \in \Lambda$, and for all $\mathbf{x}, \mathbf{y} \in \Lambda$ it holds $\mathbf{x} + \mathbf{y}, -\mathbf{x} \in \Lambda$;
- discrete: every $\mathbf{x} \in \Lambda$ has a neighborhood in which $\mathbf{x}$ is the only lattice point.
  $\exists \varepsilon > 0$ such that $\mathcal{B}(\mathbf{x}, \varepsilon) \cap \Lambda = \{ \mathbf{x} \}$

There exists a finite basis $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_n) \subset \mathbb{R}^n$ such that

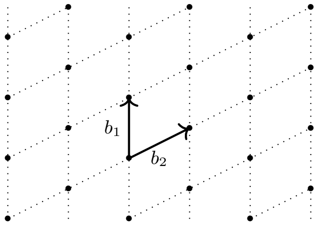
$$\Lambda(\mathbf{B}) = \left\{ \sum_{i=1}^{n} z_i \mathbf{b}_i : z_i \in \mathbb{Z} \right\}.$$

- n is the dimension of Λ

Euclidean Lattices

Let $\mathbf{B} \in \mathbb{R}^{n \times n}$ be a basis for Λ, i.e.,

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

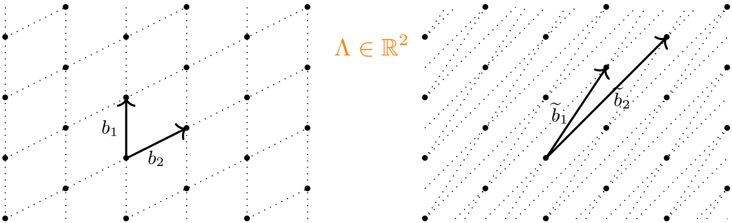


$\Lambda \in \mathbb{R}^2$

Euclidean Lattices

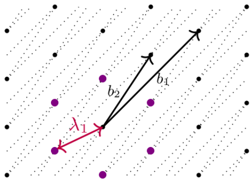
Let $\mathbf{B} \in \mathbb{R}^{n \times n}$ be a basis for Λ, i.e.,

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



- $\mathbf{U} \in \mathbb{Z}^{n \times n}$ unimodular, then $\widetilde{\mathbf{B}} = \mathbf{B} \cdot \mathbf{U}$ also a basis of Λ $\quad$ $\det(\mathbf{U}) = \pm 1$
- $\det(\Lambda) := |\det(\mathbf{B})|$

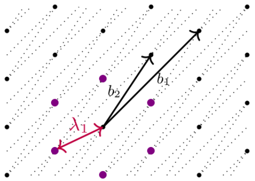
Lattice Minimum & Special Lattices



The **minimum** of a lattice $\Lambda \subset \mathbb{R}^n$ is defined as

$$\lambda_1(\Lambda) = \min_{\mathbf{x} \in \Lambda \setminus \{\mathbf{0}\}} \|\mathbf{x}\|_2.$$

Lattice Minimum & Special Lattices



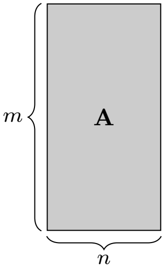
The **minimum** of a lattice $\Lambda \subset \mathbb{R}^n$ is defined as

$$\lambda_1(\Lambda) = \min_{\mathbf{x} \in \Lambda \setminus \{\mathbf{0}\}} \|\mathbf{x}\|_2.$$

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

$\mathbb{Z}_q$ integers modulo q

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



Part 2:

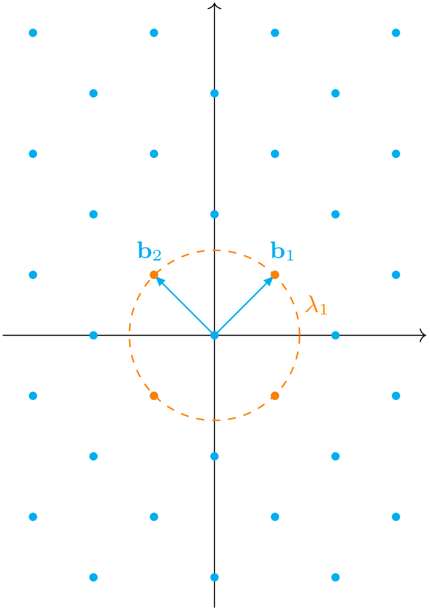
What are lattice problems?

Shortest Vector Problem

Given a lattice $\Lambda \in \mathbb{R}^n$ of dimension n.

The **shortest vector problem** (SVP) asks to find a vector $\mathbf{w} \in \Lambda$ such that

$$\|\mathbf{w}\|_2 = \lambda_1(\Lambda).$$

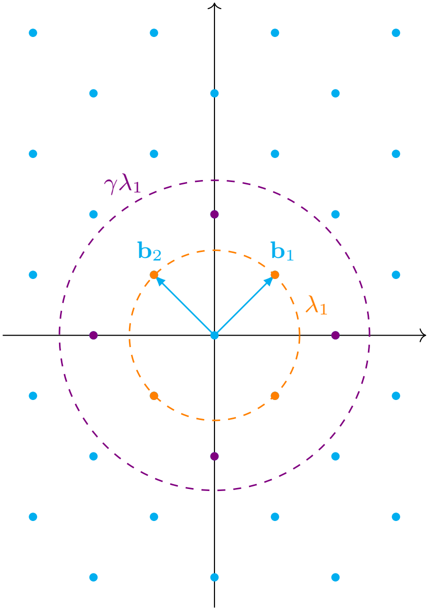


Shortest Vector Problem

Given a lattice $\Lambda \in \mathbb{R}^n$ of dimension n.

The **approximate shortest vector problem** (SVP$_\gamma$) for $\gamma \geq 1$ asks to find a vector $\mathbf{w} \in \Lambda$ such that

$$\|\mathbf{w}\|_2 \leq \gamma\lambda_1(\Lambda).$$



Shortest Vector Problem

Given a lattice $\Lambda \in \mathbb{R}^n$ of dimension n.

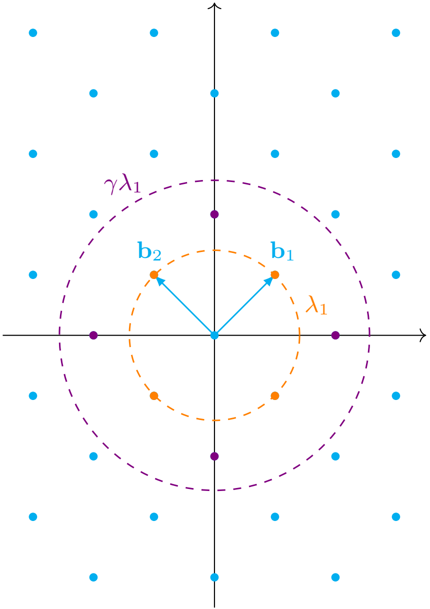
The **approximate shortest vector problem** (SVP$_\gamma$) for $\gamma \geq 1$ asks to find a vector $\mathbf{w} \in \Lambda$ such that

$$\|\mathbf{w}\|_2 \leq \gamma\lambda_1(\Lambda).$$

The complexity of SVP$_\gamma$ increases with n, but decreases with γ.

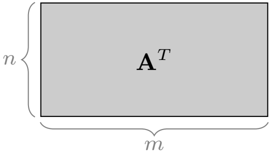
Conjecture:

There is no polynomial-time classical or quantum algorithm that solves SVP$_\gamma$ for any lattice 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 $\beta > 0$.



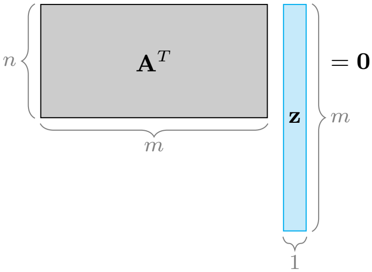
* Ajtai, *Generating hard instances of lattice problems*, STOC'96

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$_\beta$) problem asks to find a vector $\mathbf{z} \in \mathbb{Z}^m$ of norm $0 < \|\mathbf{z}\|_2 \leq \beta$ such that

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



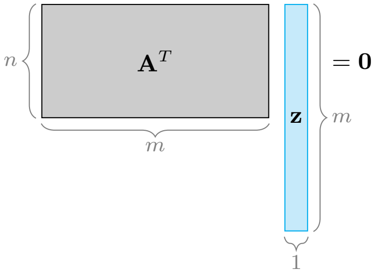
*Ajtai, *Generating hard instances of lattice problems*, STOC'96

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!

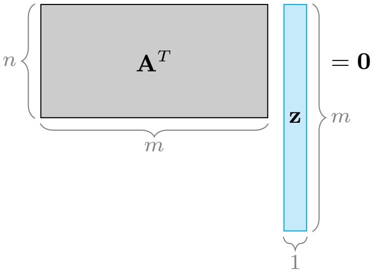
* Ajtai, *Generating hard instances of lattice problems*, STOC'96

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$_\beta$) 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:

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

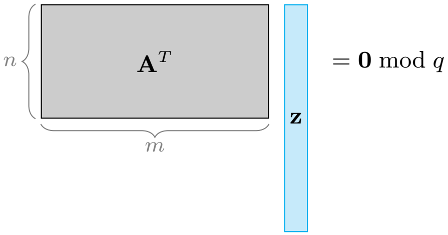
👍 SIS$_\beta$ equals SVP$_\gamma$ in the special lattice $\Lambda_q^\perp(\mathbf{A})$ for $\beta = \gamma \cdot \lambda_1(\Lambda_q^\perp(\mathbf{A}))$

* 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 $\|\mathbf{z}\|_2 \leq \beta$
- $m = ?$
- $n = ?$
- $q = ?$
- $\beta = ?$



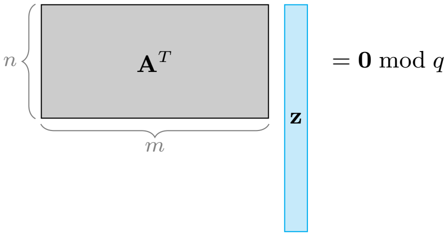
👍 Use the lattice estimator*

* 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

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

Part 3:

What is lattice-based cryptography?

Collision-Resistant Hash Function from SIS [Ajt96]*

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

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

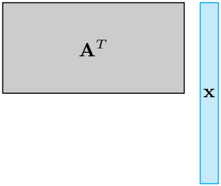
* Ajtai, *Generating hard instances of lattice problems*, STOC'96

Collision-Resistant Hash Function from SIS [Ajt96]*

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



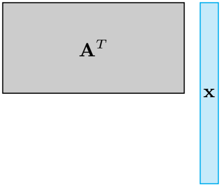
* Ajtai, *Generating hard instances of lattice problems*, STOC'96

Collision-Resistant Hash Function from SIS [Ajt96]*

A function $f\colon$ 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 $f_{\mathbf{A}}\colon \{0,1\}^m \to \mathbb{Z}_q^n$ 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

Hint: $\mathbf{x} \neq \mathbf{x}' \in \{0,1\}^m \Leftrightarrow \mathbf{0} \neq \mathbf{x} - \mathbf{x}' \in \{-1,0,1\}^m$

$$\mathbf{A}^T\mathbf{x} = \mathbf{A}^T\mathbf{x}' \Leftrightarrow \mathbf{A}^T(\mathbf{x} - \mathbf{x}') = 0$$

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

More lattice problems and constructions

at the ICO meeting this Friday :-)

https://www.ico-occitanie.fr

Part 4:

What are (my) current challenges?

Digital Signatures [DH76]*

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

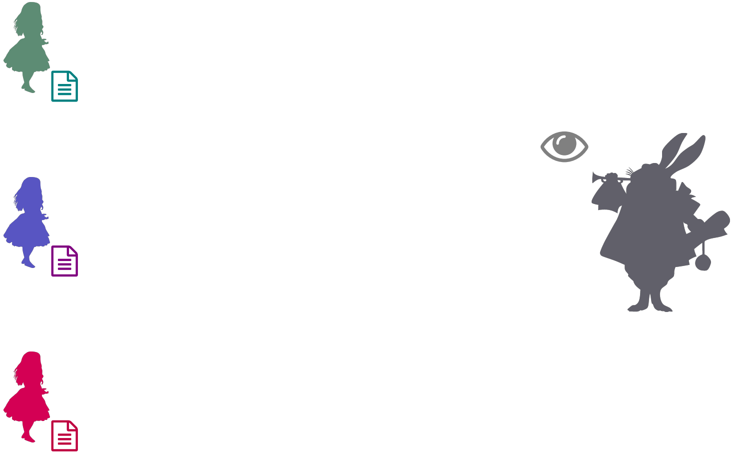
Digital Signatures [DH76]*

Motivation:

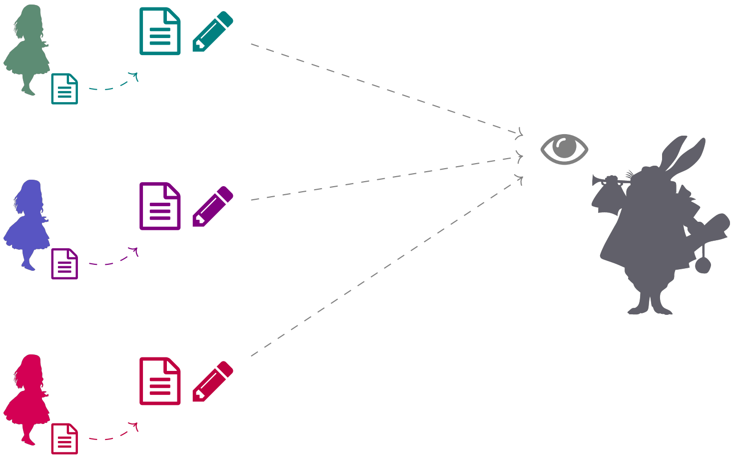
- Digital analogue of handprint signature
- Even more secure?
- Even more functionalities? ⇒ my focus

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

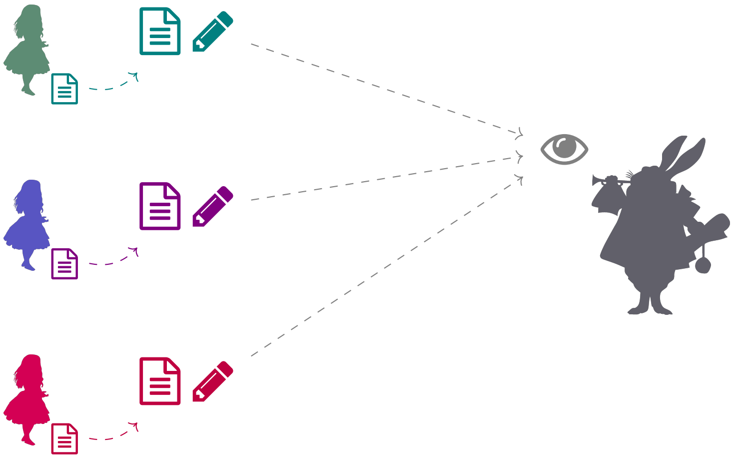
Multiple Signers and Messages, but Same Verifier



Multiple Signers and Messages, but Same Verifier



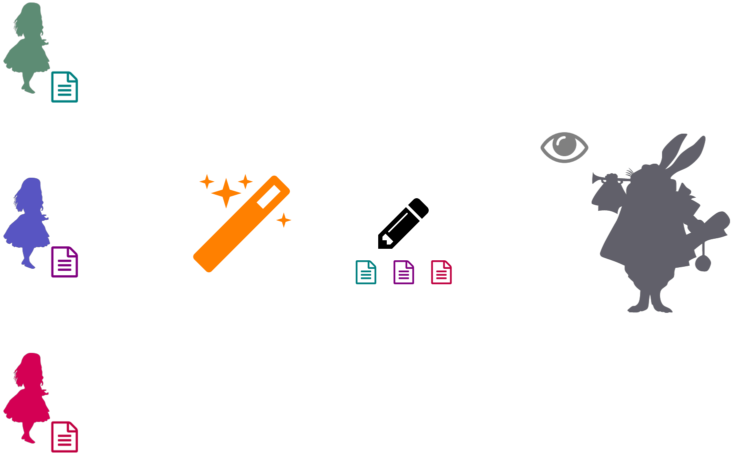
Multiple Signers and Messages, but Same Verifier



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

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

Aggregate Signatures [BGLS03]*

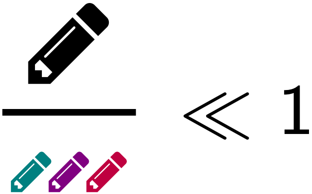


---

*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 $\rightarrow 0.06$
Falcon
ia.cr/2024/311
CRYPTO'24
with M. Aardal, D. Aranha
S. Kolby, A. Takahashi

Bonus:

A little Quiz :-)

When poll is active respond at **PollEv.com/katharinaboudgoust042**

Little Quiz after the gentle introduction to lattice-based cryptography (CIEL)

Win up to 1,000 points per answer

Powered by **Poll Everywhere**

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?

- Reach out to me (in my office E2.14)
- 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!*

Merci !

Any questions or interested in my research?

- Reach out to me (in my office E2.14)
- Write me an e-mail

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.

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