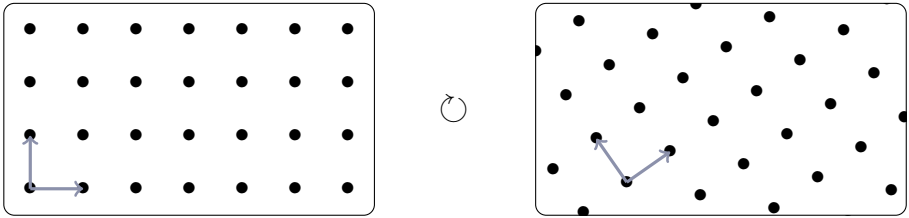
The (Module) Lattice Isomorphism Problem

Alice Pellet-Mary

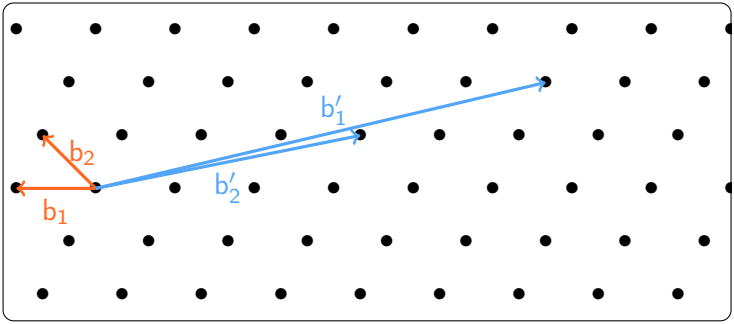
Oberwolfach workshop

January 2025

The lattice isomorphism problem



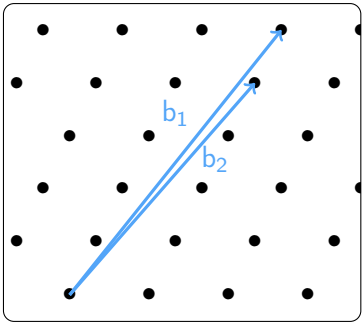
Lattices



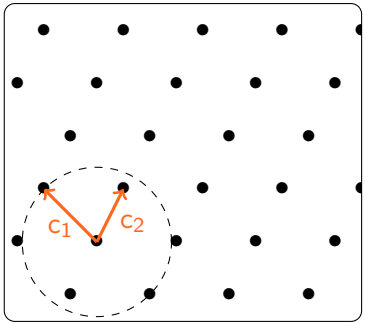
- $\mathcal{L} = \{\sum_{i=1}^{n} x_i \mathbf{b}_i \mid \forall i,\ x_i \in \mathbb{Z}\}$ is a lattice
- $(\mathbf{b}_1, \ldots, \mathbf{b}_n) =: B \in \mathrm{GL}_n(\mathbb{R})$ is a basis (not unique)
- n is the dimension (or rank)

Short basis problem

Input:



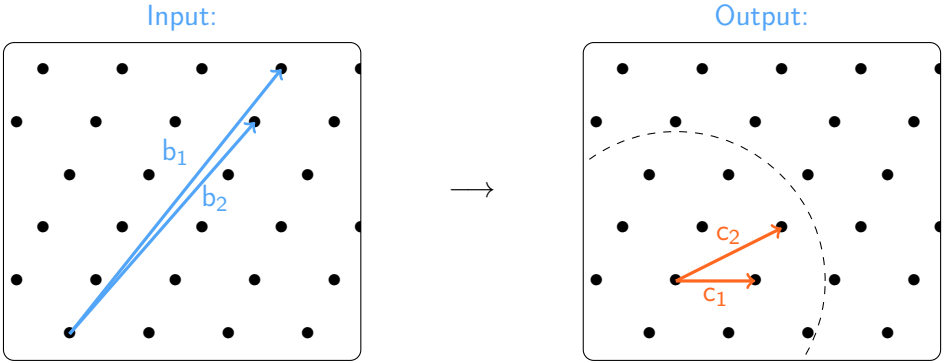
Output:



Shortest basis problem

$$\max_i \|c_i\| \leq \min_{B' \text{ basis of } \mathcal{L}} \left(\max_i \|b'_i\| \right)$$

Short basis problem



Approximate short basis problem

$$\max_i \|c_i\| \leq \gamma \cdot \min_{B' \text{ basis of } \mathcal{L}} \left(\max_i \|b'_i\| \right)$$

Hardness of the short basis problem

The short basis problem is hard

Hardness of the short basis problem

The best known algorithms solving the short basis problem have complexity $\approx \exp(n)$ (for small approximation factors)

Hardness of the short basis problem

The best known algorithms solving the short basis problem have complexity $\approx \exp(n)$ (for small approximation factors)

Consequences

- we can do crypto

Hardness of the short basis problem

The best known algorithms solving the short basis problem have complexity $\approx \exp(n)$ (for small approximation factors)

Consequences

- we can do crypto
- n has to be somewhat large (say 700 for crypto)

Hardness of the short basis problem

The best known algorithms solving the short basis problem have complexity $\approx \exp(n)$ (for small approximation factors)

Consequences

- we can do crypto
- n has to be somewhat large (say 700 for crypto)
- we only know the problem is hard for some lattices

  Analogy with factoring: factoring is hard
  - for some integers $\rightsquigarrow N = pq$ with p, q large primes is hard
  - but not for all integers $\rightsquigarrow N = 2p$ with p prime is easy

Hardness of the short basis problem

The best known algorithms solving the short basis problem have complexity $\approx \exp(n)$ (for small approximation factors)

Consequences

- we can do crypto
- n has to be somewhat large (say 700 for crypto)
- we only know the problem is hard for some lattices

  Analogy with factoring: factoring is hard
  - for some integers $\rightsquigarrow N = pq$ with p, q large primes is hard
  - but not for all integers $\rightsquigarrow N = 2p$ with p prime is easy

How do we generate hard lattices?

The goal of all lattice assumptions

What we want: An algorithm `KeyGen` such that

- `KeyGen` computes
  - a random lattice $\mathcal{L}$
  - a short basis B_s of $\mathcal{L}$ (sk)
  - a long basis B_p of $\mathcal{L}$ (pk)

The goal of all lattice assumptions

What we want: An algorithm `KeyGen` such that

- `KeyGen` computes
  - a random lattice $\mathcal{L}$
  - a short basis B_s of $\mathcal{L}$ (sk)
  - a long basis B_p of $\mathcal{L}$ (pk)
- computing a short basis of $\mathcal{L}$ from B_p is hard (i.e., key recovery is hard)

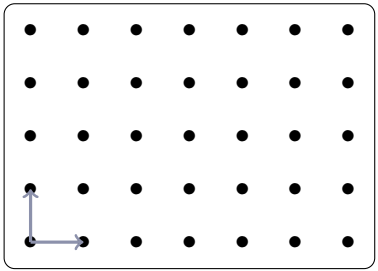
The goal of all lattice assumptions

What we want: An algorithm `KeyGen` such that

- `KeyGen` computes
  - a random lattice $\mathcal{L}$
  - a short basis B_s of $\mathcal{L}$ (sk)
  - a long basis B_p of $\mathcal{L}$ (pk)
- computing a short basis of $\mathcal{L}$ from B_p is hard (i.e., key recovery is hard)

This is the purpose of all usual lattice assumptions:
LWE, SIS, NTRU, the lattice isomorphism problem (LIP), ...

The lattice isomorphism problem [DW22,BGPS23]

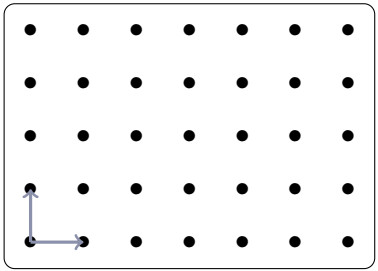


$\mathcal{L}_0 = \mathbb{Z}^n$

[DW22] Ducas and van Woerden. On the lattice isomorphism problem, quadratic forms, remarkable lattices and cryptography. Eurocrypt

[BGPS23] Bennett, Ganju, Peetathawatchai, Stephens-Davidowitz. Just how hard are rotations of $\mathbb{Z}^n$? [...] Eurocrypt

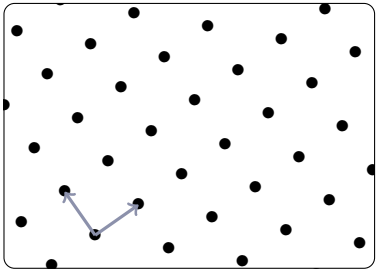
The lattice isomorphism problem [DW22,BGPS23]



$\mathcal{L}_0 = \mathbb{Z}^n$

rotate

(choose O orthogonal matrix)

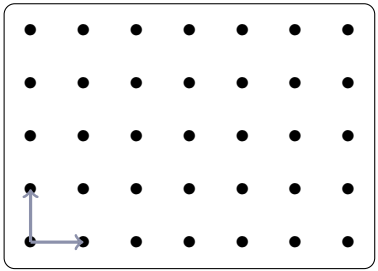


$\mathcal{L} = O \cdot \mathbb{Z}^n$

[DW22] Ducas and van Woerden. On the lattice isomorphism problem, quadratic forms, remarkable lattices and cryptography. Eurocrypt

[BGPS23] Bennett, Ganju, Peetathawatchai, Stephens-Davidowitz. Just how hard are rotations of $\mathbb{Z}^n$? [...] Eurocrypt

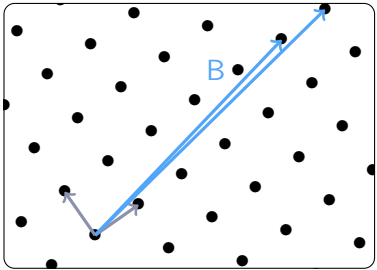
The lattice isomorphism problem [DW22,BGPS23]



$\mathcal{L}_0 = \mathbb{Z}^n$

rotate

(choose O orthogonal matrix)



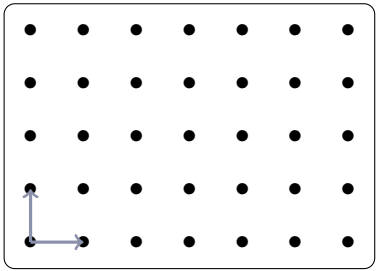
$\mathcal{L} = O \cdot \mathbb{Z}^n$

B long basis of $\mathcal{L}$

[DW22] Ducas and van Woerden. On the lattice isomorphism problem, quadratic forms, remarkable lattices and cryptography. Eurocrypt

[BGPS23] Bennett, Ganju, Peetathawatchai, Stephens-Davidowitz. Just how hard are rotations of $\mathbb{Z}^n$? [...] Eurocrypt

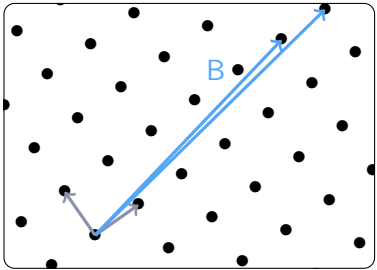
The lattice isomorphism problem [DW22,BGPS23]



$\mathcal{L}_0 = \mathbb{Z}^n$

rotate

(choose O orthogonal matrix)



$\mathcal{L} = O \cdot \mathbb{Z}^n$

B long basis of $\mathcal{L}$

Lattice Isomorphism Problem (LIP) assumption

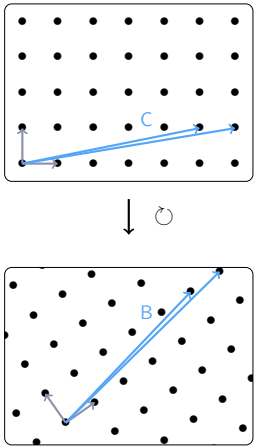
recovering O from B is hard

$\Leftrightarrow$ computing a shortest basis of $\mathcal{L}$ is hard

Equivalent formulation with Gram matrices

Lattice isomorphism problem: Given $B = O \cdot C$ with
- $O \in O_n(\mathbb{R})$ orthogonal
- C a basis of $\mathbb{Z}^n$

Find O (equivalently: find C)



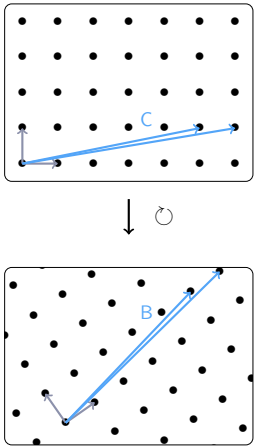
Equivalent formulation with Gram matrices

Lattice isomorphism problem: Given $B = O \cdot C$ with
- $O \in O_n(\mathbb{R})$ orthogonal
- C a basis of $\mathbb{Z}^n$

Find O (equivalently: find C)

Gram matrix associated to B:
$G = B^T B = C^T (O^T O) C = C^T C$

$\Rightarrow$ O has disappeared



Equivalent formulation with Gram matrices

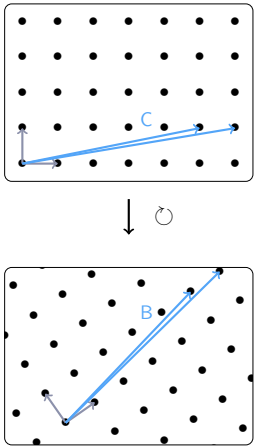
Lattice isomorphism problem: Given $B = O \cdot C$ with
- $O \in O_n(\mathbb{R})$ orthogonal
- C a basis of $\mathbb{Z}^n$

Find O (equivalently: find C)

Gram matrix associated to B:
$G = B^T B = C^T (O^T O) C = C^T C$

$\Rightarrow$ O has disappeared

Lattice isomorphism problem (Gram matrix formulation):
Given $G = C^T C$ with C a (secret) basis of $\mathbb{Z}^n$, find C.



Equivalent formulation with Gram matrices

Lattice isomorphism problem: Given $B = O \cdot C$ with
- $O \in O_n(\mathbb{R})$ orthogonal
- C a basis of $\mathbb{Z}^n$

Find O (equivalently: find C)

Gram matrix associated to B:

$$G = B^T B = C^T (O^T O) C = C^T C$$

$\Rightarrow$ O has disappeared

Lattice isomorphism problem (Gram matrix formulation):
Given $G = C^T C$ with C a (secret) basis of $\mathbb{Z}^n$, find C.

Example:

- $C = \begin{pmatrix} 1 & 1 \\ 4 & 5 \end{pmatrix}$
- $O = \begin{pmatrix} 0.5 & 0.87 \\ 0.87 & -0.5 \end{pmatrix}$
- $B = \begin{pmatrix} 3.96 & 4.83 \\ -1.13 & -1.63 \end{pmatrix}$
- $G = \begin{pmatrix} 17 & 21 \\ 21 & 26 \end{pmatrix}$
  $= C^T C = B^T B$

Given G, recover $C \in \mathbb{Z}^{2\times 2}$ with $\det(C) = \pm 1$ such that $C^T C = G$

Section's conclusion

The lattice isomorphism problem (LIP):

- allows to generate random lattices
- where the short basis problem is believed to be hard to solve
- together with a short secret basis

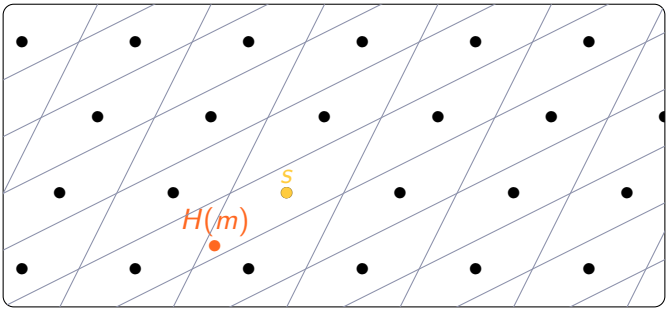
We can use LIP to build crypto [DW22,BGPS23,DPPW23]
(see next section)

[DW22] Ducas and van Woerden. On the lattice isomorphism problem, quadratic forms, remarkable lattices and cryptography. Eurocrypt

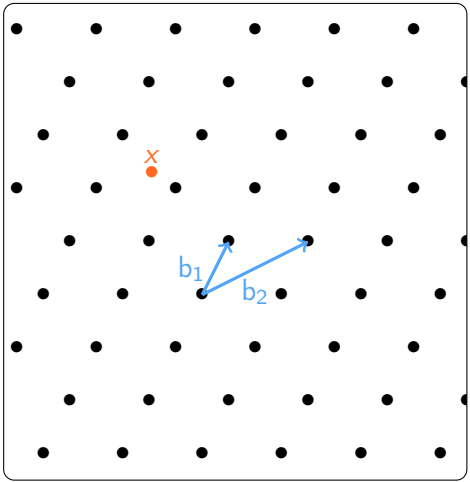
[BGPS23] Bennett, Ganju, Peetathawatchai, Stephens-Davidowitz. Just how hard are rotations of $\mathbb{Z}^n$? [...] Eurocrypt

[DPPW23] Ducas, Postlethwaite, Pulles, van Woerden. Hawk: Module LIP makes lattice signatures Fast, Compact and Simple. Asiacrypt

Hawk signature



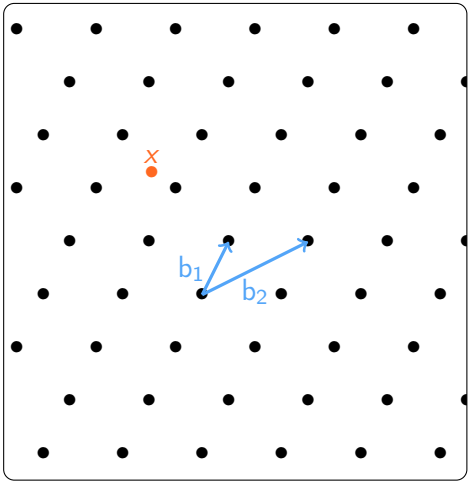
Finding a close vector using a short basis



Input: $x = 3.7 \cdot \mathbf{b}_1 - 1.4 \cdot \mathbf{b}_2$

Objective: find $s \in \mathcal{L}$ close to x

Finding a close vector using a short basis

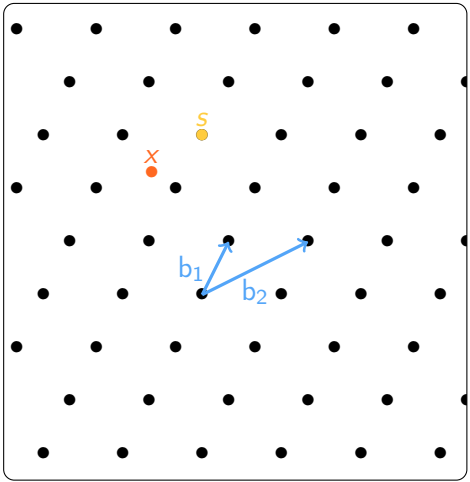


Input: $x = 3.7 \cdot \mathbf{b}_1 - 1.4 \cdot \mathbf{b}_2$

Objective: find $s \in \mathcal{L}$ close to x

Algo: round each coordinate

Finding a close vector using a short basis



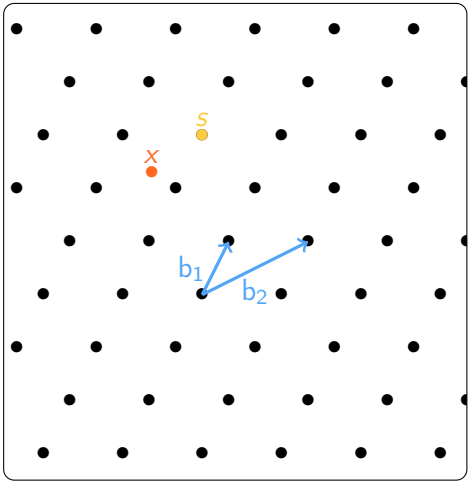
Input: $x = 3.7 \cdot \mathbf{b}_1 - 1.4 \cdot \mathbf{b}_2$

Objective: find $s \in \mathcal{L}$ close to x

Algo: round each coordinate

Output: $s = 4 \cdot \mathbf{b}_1 - 1 \cdot \mathbf{b}_2$

Finding a close vector using a short basis



Input: $x = 3.7 \cdot \mathbf{b}_1 - 1.4 \cdot \mathbf{b}_2$

Objective: find $s \in \mathcal{L}$ close to x

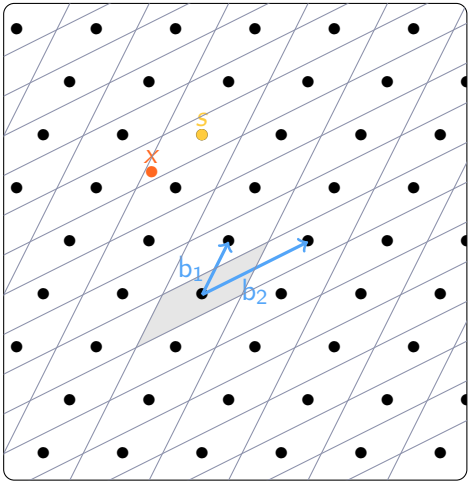
Algo: round each coordinate

Output: $s = 4 \cdot \mathbf{b}_1 - 1 \cdot \mathbf{b}_2$

The smaller the basis, the closer the solution

(called Babai's round-off algorithm)

Finding a close vector using a short basis



Input: $x = 3.7 \cdot \mathbf{b}_1 - 1.4 \cdot \mathbf{b}_2$

Objective: find $s \in \mathcal{L}$ close to x

Algo: round each coordinate

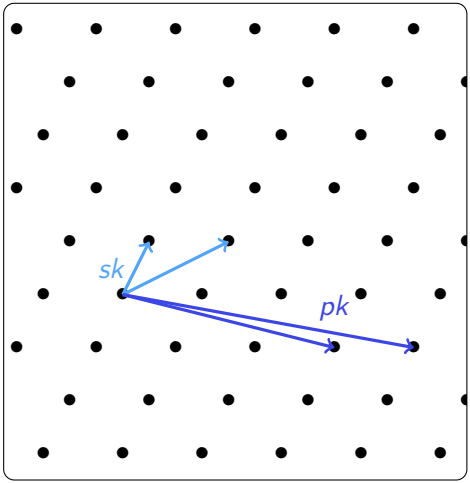
Output: $s = 4 \cdot \mathbf{b}_1 - 1 \cdot \mathbf{b}_2$

The smaller the basis, the closer the solution

(called Babai's round-off algorithm)

$$= \left\{ x_1\mathbf{b}_1 + x_2\mathbf{b}_2 \;\middle|\; |x_i| \leq \tfrac{1}{2} \right\}$$

Hash-and-sign framework [GGH97]

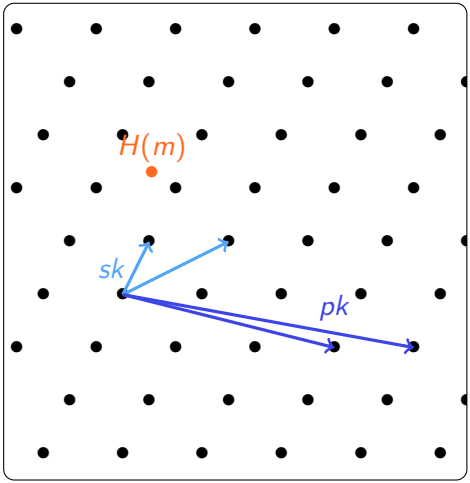


KeyGen:

- pk = long basis of $\mathcal{L}$
- sk = short basis of $\mathcal{L}$

[GGH97] Goldreich, Goldwasser, and Halevi. Public-key cryptosystems from lattice reduction problems. Crypto

Hash-and-sign framework [GGH97]



KeyGen:

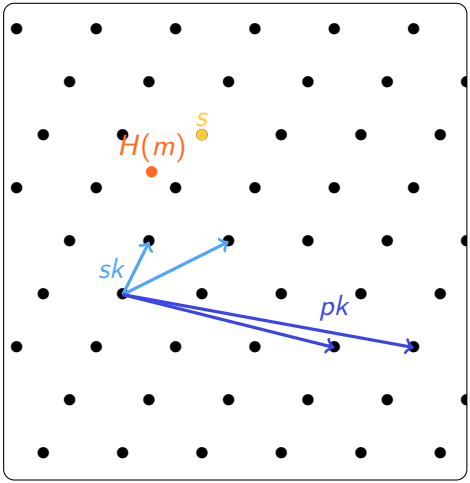
- pk = long basis of $\mathcal{L}$
- sk = short basis of $\mathcal{L}$

Sign(m, sk):

- $x = H(m)$ (hash the message)

[GGH97] Goldreich, Goldwasser, and Halevi. Public-key cryptosystems from lattice reduction problems. Crypto

Hash-and-sign framework [GGH97]



KeyGen:

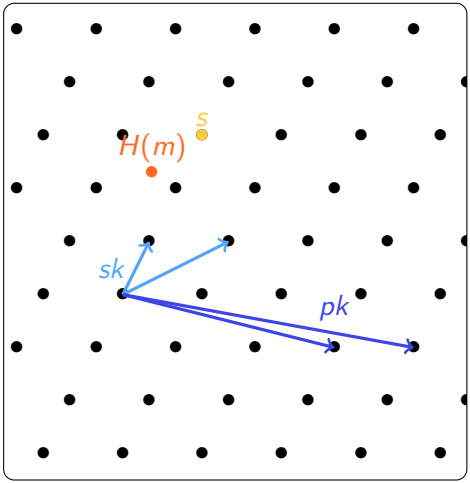
- pk = long basis of $\mathcal{L}$
- sk = short basis of $\mathcal{L}$

Sign(m, sk):

- $x = H(m)$ (hash the message)
- output $s \in \mathcal{L}$ close to $H(m)$

[GGH97] Goldreich, Goldwasser, and Halevi. Public-key cryptosystems from lattice reduction problems. Crypto

Hash-and-sign framework [GGH97]



KeyGen:

- pk = long basis of $\mathcal{L}$
- sk = short basis of $\mathcal{L}$

Sign(m, sk):

- $x = H(m)$ (hash the message)
- output $s \in \mathcal{L}$ close to $H(m)$

Verify(m, s, pk):

- check that $s \in \mathcal{L}$
- check that $H(m) - s$ is small

[GGH97] Goldreich, Goldwasser, and Halevi. Public-key cryptosystems from lattice reduction problems. Crypto

Hawk signature

Warning: The scheme from previous slide is insecure [NR06] but can be fixed [GPV08]

[NR06] Nguyen and Regev. Learning a parallelepiped: Cryptanalysis of GGH and NTRU signatures. J. Cryptology

[GPV08] Gentry, Peikert, and Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. STOC.

Hawk signature

Warning: The scheme from previous slide is insecure [NR06] but can be fixed [GPV08]

Hash-and-sign framework:

- requires a lattice $\mathcal{L}$ + a short basis B_s + a long basis B_p
- provably secure if recovering a short basis from B_p is hard

[NR06] Nguyen and Regev. Learning a parallelepiped: Cryptanalysis of GGH and NTRU signatures. J. Cryptology

[GPV08] Gentry, Peikert, and Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. STOC.

Hawk signature

Warning: The scheme from previous slide is insecure [NR06] but can be fixed [GPV08]

Hash-and-sign framework:

- requires a lattice $\mathcal{L}$ + a short basis B_s + a long basis B_p
- provably secure if recovering a short basis from B_p is hard

Hawk signature (NIST submission)

Hash-and-sign framework
+
hard lattice from lattice isomorphism problem

[NR06] Nguyen and Regev. Learning a parallelepiped: Cryptanalysis of GGH and NTRU signatures. J. Cryptology
[GPV08] Gentry, Peikert, and Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. STOC.

Advantages of Hawk

Hash-and-sign framework can be instantiated with other assumptions

Assumption	LIP (lattice isomorphism problem)		
Construction's name	Hawk		

[DW22] Ducas and van Woerden. On the lattice isomorphism problem, quadratic forms [...]. Eurocrypt

[DPPW23] Ducas, Postlethwaite, Pulles, van Woerden. Hawk: Module LIP makes lattice signatures [...]. Asiacrypt

Advantages of Hawk

Hash-and-sign framework can be instantiated with other assumptions

Assumption	LIP (lattice isomorphism problem)	SIS (short integer solution)	
Construction's name	Hawk	GPV	

Hash-and-sign framework

[Ajt96] Ajtai. Generating hard instances of lattice problems. STOC.

[GPV08] Gentry, Peikert, Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. STOC

Advantages of Hawk

Hash-and-sign framework can be instantiated with other assumptions

Assumption	LIP (lattice isomorphism problem)	SIS (short integer solution)	NTRU
Construction's name	Hawk	GPV	Falcon

Hash-and-sign framework

[HPS98] Hoffstein, Pipher, and Silverman. NTRU: a ring based public key cryptosystem. ANTS.

[Falcon] Fouque, Hoffstein, Kirchner, Lyubashevsky, Pornin, Prest, Ricosset, Seiler, Whyte, Zhang. NIST standard

Advantages of Hawk

Hash-and-sign framework can be instantiated with other assumptions

Assumption	LIP (lattice isomorphism problem)	SIS (short integer solution)	NTRU
Construction's name	Hawk	GPV	Falcon

Hash-and-sign framework

Why do we like Hawk?

- relies on a new fun math assumption (increase diversity of assumptions)

[HPS98] Hoffstein, Pipher, and Silverman. NTRU: a ring based public key cryptosystem. ANTS.

[Falcon] Fouque, Hoffstein, Kirchner, Lyubashevsky, Pornin, Prest, Ricosset, Seiler, Whyte, Zhang. NIST standard

Advantages of Hawk

Hash-and-sign framework can be instantiated with other assumptions

Assumption	LIP (lattice isomorphism problem)	SIS (short integer solution)	NTRU
Construction's name	Hawk	GPV	Falcon

Hash-and-sign framework

Why do we like Hawk?

- relies on a new fun math assumption (increase diversity of assumptions)
- efficient (comparable to Falcon for size and timings)

Nice comparison of many (post-quantum) signatures: https://blog.cloudflare.com/another-look-at-pq-signatures/

Advantages of Hawk

Hash-and-sign framework can be instantiated with other assumptions

Assumption	LIP (lattice isomorphism problem)	SIS (short integer solution)	NTRU
Construction's name	Hawk	GPV	Falcon

Hash-and-sign framework

Why do we like Hawk?

- relies on a new fun math assumption (increase diversity of assumptions)
- efficient (comparable to Falcon for size and timings)
- simple to implement (no floating points → big advantage on Falcon)

Nice comparison of many (post-quantum) signatures: https://blog.cloudflare.com/another-look-at-pq-signatures/

Section's conclusion

Hawk

- post-quantum signature scheme (second round of NIST additional call)

Section's conclusion

Hawk

- post-quantum signature scheme (second round of NIST additional call)
- simple and efficient (comparable to Falcon, but simpler to implement)

Section's conclusion

Hawk

- post-quantum signature scheme (second round of NIST additional call)
- simple and efficient (comparable to Falcon, but simpler to implement)
- relies on the lattice isomorphism problem
  - how hard is this problem?

Section's conclusion

Hawk

- post-quantum signature scheme (second round of NIST additional call)
- simple and efficient (comparable to Falcon, but simpler to implement)
- relies on the lattice isomorphism problem
  - how hard is this problem?

Other constructions from lattice isomorphism problem

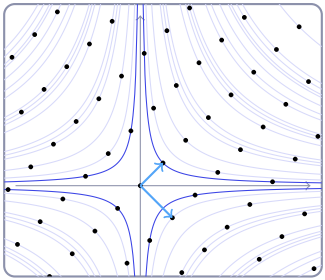
- key exchange [DW22,BGPS23]
- public key encryption [ARW24]

[DW22] Ducas and van Woerden. On the lattice isomorphism problem, quadratic forms, remarkable lattices and cryptography. Eurocrypt

[BGPS23] Bennett, Ganju, Peetathawatchai, Stephens-Davidowitz. Just how hard are rotations of $\mathbb{Z}^n$? [...] Eurocrypt

[ARW24] Ackermann, Roux-Langlois, Wallet. Public-key encryption from the lattice isomorphism problem. WCC presentation.

The Module Lattice Isomorphism Problem



I lied a bit

Hawk relies on

the module lattice isomorphism problem (module-LIP)

I lied a bit

Hawk relies on

the module lattice isomorphism problem (module-LIP)

- structured variant of LIP

  module-LIP = LIP restricted to module lattices + module-compatible transformations

I lied a bit

Hawk relies on

the module lattice isomorphism problem (module-LIP)

- structured variant of LIP

  module-LIP = LIP restricted to module lattices + module-compatible transformations

- allows faster operations

Number fields

Number field: $K = \mathbb{Q}[X]/P(X)$ (P irreducible, $\deg(P) = d$)

- $K = \mathbb{Q}$
- $K = \mathbb{Q}[X]/(X^d + 1)$ with $d = 2^\ell$ $\rightsquigarrow$ power-of-two cyclotomic field
- $K = \mathbb{Q}[X]/(X^d - X - 1)$ with d prime $\rightsquigarrow$ NTRUPrime field

Number fields

Number field: $K = \mathbb{Q}[X]/P(X)$ (P irreducible, $\deg(P) = d$)

- $K = \mathbb{Q}$
- $K = \mathbb{Q}[X]/(X^d + 1)$ with $d = 2^\ell \rightsquigarrow$ power-of-two cyclotomic field
- $K = \mathbb{Q}[X]/(X^d - X - 1)$ with d prime $\rightsquigarrow$ NTRUPrime field

Ring of integers: $\mathcal{O}_K \subset K$, for this talk $\mathcal{O}_K = \mathbb{Z}[X]/P(X)$

(more generally $\mathbb{Z}[X]/P(X) \subseteq \mathcal{O}_K$ but $\mathcal{O}_K$ can be larger)

Number fields

Number field: $K = \mathbb{Q}[X]/P(X)$ (P irreducible, $\deg(P) = d$)

- $K = \mathbb{Q}$
- $K = \mathbb{Q}[X]/(X^d + 1)$ with $d = 2^\ell \rightsquigarrow$ power-of-two cyclotomic field
- $K = \mathbb{Q}[X]/(X^d - X - 1)$ with d prime $\rightsquigarrow$ NTRUPrime field

Ring of integers: $\mathcal{O}_K \subset K$, for this talk $\mathcal{O}_K = \mathbb{Z}[X]/P(X)$

(more generally $\mathbb{Z}[X]/P(X) \subseteq \mathcal{O}_K$ but $\mathcal{O}_K$ can be larger)

- $\mathcal{O}_K = \mathbb{Z}$
- $\mathcal{O}_K = \mathbb{Z}[X]/(X^d + 1)$ with $d = 2^\ell \rightsquigarrow$ power-of-two cyclotomic ring
- $\mathcal{O}_K = \mathbb{Z}[X]/(X^d - X - 1)$ with d prime $\rightsquigarrow$ NTRUPrime ring of integers

The canonical embedding

$(K = \mathbb{Q}[X]/P(X), \quad \alpha_1, \cdots, \alpha_d$ complex roots of $P(X))$

Canonical embedding: $\sigma : \begin{array}{ccc} K & \to & \mathbb{C}^d \\ a(X) & \mapsto & (a(\alpha_1), \cdots, a(\alpha_d)) \end{array}$

The canonical embedding

$(K = \mathbb{Q}[X]/P(X), \quad \alpha_1, \cdots, \alpha_d$ complex roots of $P(X))$

Canonical embedding: $\sigma : \begin{array}{rcl} K & \to & \mathbb{C}^d \\ a(X) & \mapsto & (a(\alpha_1), \cdots, a(\alpha_d)) \end{array}$

- we can see K as a subset of $\mathbb{C}^d$

The canonical embedding

($K = \mathbb{Q}[X]/P(X)$, $\alpha_1, \cdots, \alpha_d$ complex roots of $P(X)$)

Canonical embedding: $\sigma : \begin{array}{ccc} K & \to & \mathbb{C}^d \\ a(X) & \mapsto & (a(\alpha_1), \cdots, a(\alpha_d)) \end{array}$

- we can see K as a subset of $\mathbb{C}^d$
- this induces a geometry on K (using the hermitian norm in $\mathbb{C}^d$): for $a \in K$

$$\|a\| := \|\sigma(a)\|_2 = \sqrt{\overline{\sigma(a)}^T \sigma(a)}.$$

(Free) module:

$$M = \{B \cdot x \mid x \in {\mathcal{O}_K}^k\} \text{ for some matrix } B \in {\mathcal{O}_K}^{k \times k} \text{ with } \det_K(B) \neq 0$$

- k is the module rank
- B is a module basis of M

Example: $M = {\mathcal{O}_K}^2$ is a module of rank 2, with basis $B = I_2$

(Free) module:

$$M = \{B \cdot x \,|\, x \in {\mathcal{O}_K}^k\} \text{ for some matrix } B \in {\mathcal{O}_K}^{k \times k} \text{ with } \det_K(B) \neq 0$$

- k is the module rank
- B is a module basis of M

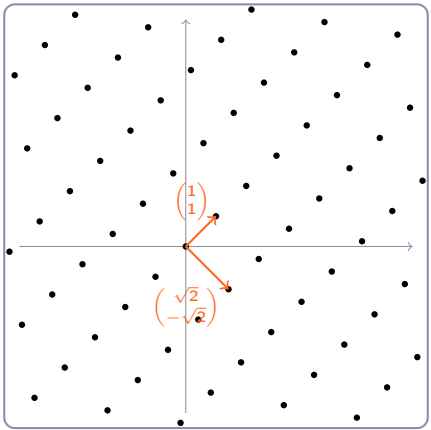
Example: $M = {\mathcal{O}_K}^2$ is a module of rank 2, with basis $B = I_2$

$\sigma(M)$ is a lattice: of $\mathbb{Z}$-rank $n := d \cdot k$, included in $\mathbb{C}^n$

$\Rightarrow \sigma(M)$ is called a module lattice

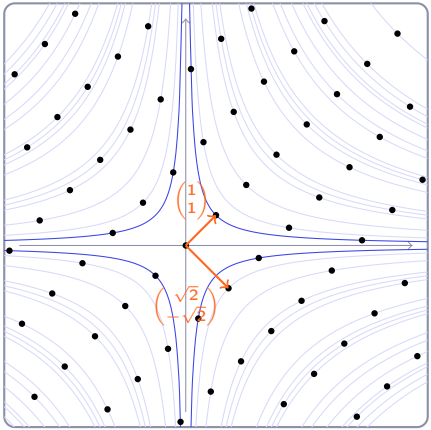
An example

$K = \mathbb{Q}[X]/(X^2+2)$, $\mathcal{O}_K = \mathbb{Z}[X]/(X^2+2)$, $\sigma : a + bX \mapsto \begin{pmatrix} a+b\sqrt{2} \\ a-b\sqrt{2} \end{pmatrix}$, $\mathcal{L} = \sigma(\mathcal{O}_K)$



An example

$K = \mathbb{Q}[X]/(X^2+2)$, $\mathcal{O}_K = \mathbb{Z}[X]/(X^2+2)$, $\sigma : a + bX \mapsto \begin{pmatrix} a+b\sqrt{2} \\ a-b\sqrt{2} \end{pmatrix}$, $\mathcal{L} = \sigma(\mathcal{O}_K)$



The module lattice isomorphism problem

Lattice isomorphism problem:
Given $G = C^T C$ with C a basis of $\mathbb{Z}^n$, find C

The module lattice isomorphism problem

Lattice isomorphism problem:
Given $G = C^T C$ with C a basis of $\mathbb{Z}^n$, find C

Module lattice isomorphism problem:
Given $G = \overline{\sigma(C)}^T \sigma(C)$ with C a basis of ${\mathcal{O}_K}^2$, find C

The module lattice isomorphism problem

Lattice isomorphism problem:
Given $G = C^T C$ with C a basis of $\mathbb{Z}^n$, find C

Module lattice isomorphism problem:
Given $G = \overline{\sigma(C)^T}\sigma(C)$ with C a basis of ${\mathcal{O}_K}^2$, find C

Remarks.

- we consider $\overline{\sigma(C)}$ because we use hermitian norm in $\mathbb{C}^{2d}$
- only rank 2 modules in this talk (and even only ${\mathcal{O}_K}^2$)

The module lattice isomorphism problem

Lattice isomorphism problem:
Given $G = C^T C$ with C a basis of $\mathbb{Z}^n$, find C

Module lattice isomorphism problem:
Given $G = \overline{\sigma(C)^T}\sigma(C)$ with C a basis of ${\mathcal{O}_K}^2$, find C

Remarks.

- we consider $\overline{\sigma(C)}$ because we use hermitian norm in $\mathbb{C}^{2d}$
- only rank 2 modules in this talk (and even only ${\mathcal{O}_K}^2$)

Hawk relies on
module-LIP for the module ${\mathcal{O}_K}^2$, in a power-of-two cyclotomic field
($K = \mathbb{Q}[X]/(X^d + 1)$ with $d = 512$ or $d = 1024$)

Section's conclusion

Module lattices: module (algebraic object) + lattice (geometric object)

Section's conclusion

Module lattices: module (algebraic object) + lattice (geometric object)

Module-LIP: LIP restricted to module lattices (+ module-compatible transformations)

Section's conclusion

Module lattices: module (algebraic object) + lattice (geometric object)

Module-LIP: LIP restricted to module lattices (+ module-compatible transformations)

Advantages:

- smaller storage size required, faster operations
  - more efficient cryptographic protocols
  - used in all standardized lattice-based schemes (Kyber, Dilithium, Falcon)

Section's conclusion

Module lattices: module (algebraic object) + lattice (geometric object)

Module-LIP: LIP restricted to module lattices (+ module-compatible transformations)

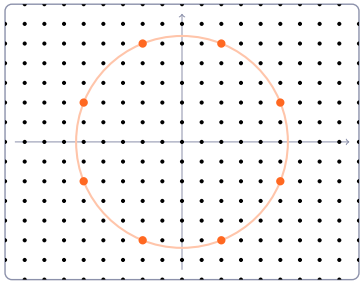
Advantages:

- smaller storage size required, faster operations
  - more efficient cryptographic protocols
  - used in all standardized lattice-based schemes (Kyber, Dilithium, Falcon)

Drawbacks:

- maybe more efficient attacks using algebraic structure? (see next section)

Cryptanalysis of module-LIP



Cryptanalysis status

Lattice isomorphism problem (unstructured lattices)

- studied by mathematicians for ≥ 25 years (before crypto) [PS97]
- all known algorithms require computation of short vectors (expensive)

[PS97] Plesken, Souvignier. Computing isometries of lattices. Journal of Symbolic Computation.

Cryptanalysis status

Lattice isomorphism problem (unstructured lattices)

- studied by mathematicians for ≥ 25 years (before crypto) [PS97]
- all known algorithms require computation of short vectors (expensive)

Module lattice isomorphism problem

- very recent [DPPW23]

[DPPW23] Ducas, Postlethwaite, Pulles, van Woerden. Hawk: Module LIP makes lattice signatures Fast, Compact and Simple. Asiacrypt

Cryptanalysis status

Lattice isomorphism problem (unstructured lattices)

- studied by mathematicians for ≥ 25 years (before crypto) [PS97]
- all known algorithms require computation of short vectors (expensive)

Module lattice isomorphism problem

- very recent [DPPW23]
- for $k \geq 2$, best algorithm was thought to be the same as in the unstructured case (k = module rank)

[DPPW23] Ducas, Postlethwaite, Pulles, van Woerden. Hawk: Module LIP makes lattice signatures Fast, Compact and Simple. Asiacrypt

Cryptanalysis status

Lattice isomorphism problem (unstructured lattices)

- studied by mathematicians for ≥ 25 years (before crypto) [PS97]
- all known algorithms require computation of short vectors (expensive)

Module lattice isomorphism problem

- very recent [DPPW23]
- for $k \geq 2$, best algorithm was thought to be the same as in the unstructured case (k = module rank)
- recent works show that for $k = 2$ and certain number fields, the module structure can be exploited! (this does not break Hawk so far) [MPPW24,LJPW24,CFMPW24,EP24]

[MPPW24] Mureau, Pellet-Mary, Pliatsok, Wallet. Cryptanalysis of rank-2 module-LIP in Totally Real Number Fields. Eurocrypt.

[LJPW24] Luo, Jiang, Pan, Wang. Cryptanalysis of Rank-2 Module-LIP with Symplectic Automorphisms. Asiacrypt.

[CFMPW24] Chevignard, Fouque, Mureau, Pellet-Mary, Wallet. A reduction from Hawk to the principal ideal problem in a quaternion algebra. Eprint.

[EP24] Espitau, Pliatsok. On hermitian decomposition lattices and the module-LIP problem in rank 2. Eprint.

Cryptanalysis of LIP

Objective: Given $\mathcal{L}$ and $\mathcal{L}' = O \cdot \mathcal{L}$ (O orthogonal), recover O

Cryptanalysis of LIP

Objective: Given $\mathcal{L}$ and $\mathcal{L}' = O \cdot \mathcal{L}$ (O orthogonal), recover O

Main strategy: [PS97, HR14, SHVW20]

1. Compute all short vectors of $\mathcal{L}$ and $\mathcal{L}'$

[PS97] Plesken, Souvignier. Computing isometries of lattices. Journal of Symbolic Computation.

[HR14] Haviv, Regev. On the lattice isomorphism problem. SODA.

[SHVW20] Sikirić, Haensch, Voight, van Woerden. A canonical form for positive definite matrices. Open book series.

Cryptanalysis of LIP

Objective: Given $\mathcal{L}$ and $\mathcal{L}' = O \cdot \mathcal{L}$ (O orthogonal), recover O

Main strategy: [PS97, HR14, SHVW20]

1. Compute all short vectors of $\mathcal{L}$ and $\mathcal{L}'$
2. Try to match the short vectors in a consistent way (that respects inner products)

[PS97] Plesken, Souvignier. Computing isometries of lattices. Journal of Symbolic Computation.

[HR14] Haviv, Regev. On the lattice isomorphism problem. SODA.

[SHVW20] Sikirić, Haensch, Voight, van Woerden. A canonical form for positive definite matrices. Open book series.

Cryptanalysis of LIP

Objective: Given $\mathcal{L}$ and $\mathcal{L}' = O \cdot \mathcal{L}$ (O orthogonal), recover O

Main strategy: [PS97, HR14, SHVW20]

1. Compute all short vectors of $\mathcal{L}$ and $\mathcal{L}'$
2. Try to match the short vectors in a consistent way (that respects inner products)

Cost:

- at least as high as computing shortest vectors in $\mathcal{L}$ and $\mathcal{L}'$
- in very special worst cases, the matching part 2. may dominate
  (the number of shortest vectors may be huge)

[PS97] Plesken, Souvignier. Computing isometries of lattices. Journal of Symbolic Computation.

[HR14] Haviv, Regev. On the lattice isomorphism problem. SODA.

[SHVW20] Sikirić, Haensch, Voight, van Woerden. A canonical form for positive definite matrices. Open book series.

Cryptanalysis of module-LIP: when P has a real root

Notations: $K = \mathbb{Q}[X]/P(X)$, $\mathcal{O}_K = \mathbb{Z}[X]/P(X)$

Objective: Given $G := \overline{C}^T C$, recover C (where $C = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in {\mathcal{O}_K}^{2\times 2}$)

Cryptanalysis of module-LIP: when P has a real root

Notations: $K = \mathbb{Q}[X]/P(X)$, $\mathcal{O}_K = \mathbb{Z}[X]/P(X)$

Objective: Given $G := \overline{C}^T C$, recover C (where $C = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in {\mathcal{O}_K}^{2\times 2}$)

Key point: if P has at least 1 real root, then from G we can recover

$$C^T C = \begin{pmatrix} a^2 + b^2 & ac + bd \\ ac + bd & c^2 + d^2 \end{pmatrix}$$

Cryptanalysis of module-LIP: when P has a real root

Notations: $K = \mathbb{Q}[X]/P(X)$, $\mathcal{O}_K = \mathbb{Z}[X]/P(X)$

Objective: Given $G := \overline{C}^T C$, recover C (where $C = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in {\mathcal{O}_K}^{2\times 2}$)

Key point: if P has at least 1 real root, then from G we can recover

$$C^T C = \begin{pmatrix} a^2 + b^2 & ac + bd \\ ac + bd & c^2 + d^2 \end{pmatrix}$$

New objective: given α $(= a^2 + b^2)$, find all solutions $(x, y) \in {\mathcal{O}_K}^2$ of the equation

$$x^2 + y^2 = \alpha$$

Solving sum of two square equations

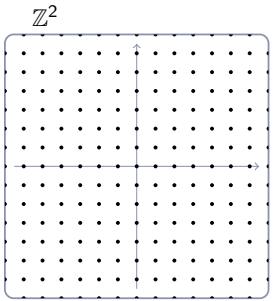
For simplicity, take $\mathcal{O}_K = \mathbb{Z}$ (similar strategy for general $\mathcal{O}_K$)

Objective: for $\alpha \in \mathbb{Z}$, find all $(x, y) \in \mathbb{Z}^2$ s.t. $x^2 + y^2 = \alpha$

Solving sum of two square equations

For simplicity, take $\mathcal{O}_K = \mathbb{Z}$ (similar strategy for general $\mathcal{O}_K$)

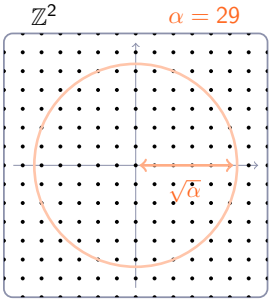
Objective: for $\alpha \in \mathbb{Z}$, find all $(x, y) \in \mathbb{Z}^2$ s.t. $x^2 + y^2 = \alpha$



Solving sum of two square equations

For simplicity, take $\mathcal{O}_K = \mathbb{Z}$ (similar strategy for general $\mathcal{O}_K$)

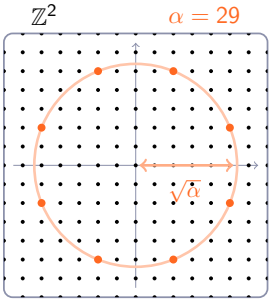
Objective: for $\alpha \in \mathbb{Z}$, find all $(x, y) \in \mathbb{Z}^2$ s.t. $x^2 + y^2 = \alpha$



Solving sum of two square equations

For simplicity, take $\mathcal{O}_K = \mathbb{Z}$ (similar strategy for general $\mathcal{O}_K$)

Objective: for $\alpha \in \mathbb{Z}$, find all $(x, y) \in \mathbb{Z}^2$ s.t. $x^2 + y^2 = \alpha$



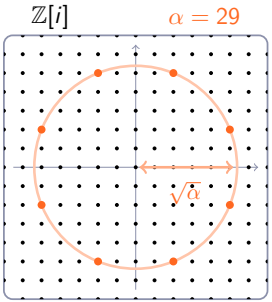
Solving sum of two square equations

For simplicity, take $\mathcal{O}_K = \mathbb{Z}$ (similar strategy for general $\mathcal{O}_K$)

Objective: for $\alpha \in \mathbb{Z}$, find all $(x, y) \in \mathbb{Z}^2$ s.t. $x^2 + y^2 = \alpha$

Reformulate:

- take $\mathbb{Z}[i] \subseteq \mathbb{C}$
- for $z = x + iy \in \mathbb{Z}[i]$, $\bar{z}z = x^2 + y^2$
- solve $\bar{z}z = \alpha$, for $z \in \mathbb{Z}[i]$



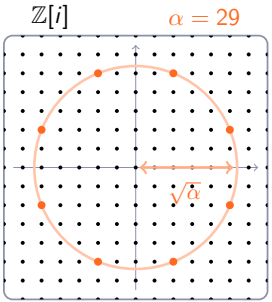
Solving sum of two square equations

For simplicity, take $\mathcal{O}_K = \mathbb{Z}$ (similar strategy for general $\mathcal{O}_K$)

Objective: for $\alpha \in \mathbb{Z}$, find all $(x, y) \in \mathbb{Z}^2$ s.t. $x^2 + y^2 = \alpha$

Reformulate:

- take $\mathbb{Z}[i] \subseteq \mathbb{C}$
- for $z = x + iy \in \mathbb{Z}[i]$, $\bar{z}z = x^2 + y^2$
- solve $\bar{z}z = \alpha$, for $z \in \mathbb{Z}[i]$



Conclude: solve $\bar{z}z = \alpha$ using Gentry-Szydlo algorithm [GS02,LS19]

[GS02] Gentry, Szydlo. Cryptanalysis of the revised NTRU signature scheme. Eurocrypt

[LS19] Lenstra, Silverberg. Testing isomorphism of lattices over CM-orders. Journal on Computing

Fields with one real embedding: summary

Notations: $K = \mathbb{Q}[X]/P(X)$, $\mathcal{O}_K = \mathbb{Z}[X]/P(X)$, k module rank

Assumptions:

- P has (at least) one real root
- $k = 2$

Heuristic quantum poly time algorithm for module-LIP [MPPW24,APW25]

[MPPW24] Mureau, Pellet-Mary, Pliatsok, Wallet. Cryptanalysis of rank-2 module-LIP in Totally Real Number Fields. Eurocrypt.

[APW25] Allombert, Pellet-Mary, van Woerden. Cryptanalysis of rank-2 module-LIP: a single real embedding is all it takes. ePrint (soon)

Fields with one real embedding: summary

Notations: $K = \mathbb{Q}[X]/P(X)$, $\mathcal{O}_K = \mathbb{Z}[X]/P(X)$, k module rank

Assumptions:

- P has (at least) one real root
- $k = 2$

Heuristic quantum poly time algorithm for module-LIP [MPPW24,APW25]

- with more restrictions on $P \Rightarrow$ classical heuristic poly time algorithm

[MPPW24] Mureau, Pellet-Mary, Pliatsok, Wallet. Cryptanalysis of rank-2 module-LIP in Totally Real Number Fields. Eurocrypt.

[APW25] Allombert, Pellet-Mary, van Woerden. Cryptanalysis of rank-2 module-LIP: a single real embedding is all it takes. ePrint (soon)

Fields with one real embedding: summary

Notations: $K = \mathbb{Q}[X]/P(X)$, $\mathcal{O}_K = \mathbb{Z}[X]/P(X)$, k module rank

Assumptions:

- P has (at least) one real root
- $k = 2$

Heuristic quantum poly time algorithm for module-LIP [MPPW24,APW25]

- with more restrictions on $P \Rightarrow$ classical heuristic poly time algorithm
- does not cover cyclotomic fields

[MPPW24] Mureau, Pellet-Mary, Pliatsok, Wallet. Cryptanalysis of rank-2 module-LIP in Totally Real Number Fields. Eurocrypt.

[APW25] Allombert, Pellet-Mary, van Woerden. Cryptanalysis of rank-2 module-LIP: a single real embedding is all it takes. ePrint (soon)

Fields with one real embedding: summary

Notations: $K = \mathbb{Q}[X]/P(X)$, $\mathcal{O}_K = \mathbb{Z}[X]/P(X)$, k module rank

Assumptions:

- P has (at least) one real root
- $k = 2$

Heuristic quantum poly time algorithm for module-LIP [MPPW24,APW25]

- with more restrictions on $P \Rightarrow$ classical heuristic poly time algorithm
- does not cover cyclotomic fields
- do cover NTRUPrime fields ($P = X^p - X - 1$)

[MPPW24] Mureau, Pellet-Mary, Pliatsok, Wallet. Cryptanalysis of rank-2 module-LIP in Totally Real Number Fields. Eurocrypt.

[APW25] Allombert, Pellet-Mary, van Woerden. Cryptanalysis of rank-2 module-LIP: a single real embedding is all it takes. ePrint (soon)

Cryptanalysis of module-LIP: cyclotomic fields

Take $K = \mathbb{Q}[i]$ (for simplicity)

Module-LIP: $C = \begin{pmatrix} a_1 + ia_2 & c_1 + ic_2 \\ b_1 + ib_2 & d_1 + id_2 \end{pmatrix}$ secret, $G = \overline{C}^T C$ public, recover C from G

Cryptanalysis of module-LIP: cyclotomic fields

Take $K = \mathbb{Q}[i]$ (for simplicity)

Module-LIP: $C = \begin{pmatrix} a_1 + ia_2 & c_1 + ic_2 \\ b_1 + ib_2 & d_1 + id_2 \end{pmatrix}$ secret, $G = \overline{C}^T C$ public, recover C from G

$$G = \begin{pmatrix} a_1^2 + a_2^2 + b_1^2 + b_2^2 & * \\ * & c_1^2 + c_2^2 + c_3^2 + c_4^2 \end{pmatrix}$$

Sum of 4 squares equations

Cryptanalysis of module-LIP: cyclotomic fields

Take $K = \mathbb{Q}[i]$ (for simplicity)

Module-LIP: $C = \begin{pmatrix} a_1 + ia_2 & c_1 + ic_2 \\ b_1 + ib_2 & d_1 + id_2 \end{pmatrix}$ secret, $G = \overline{C}^T C$ public, recover C from G

$$G = \begin{pmatrix} a_1^2 + a_2^2 + b_1^2 + b_2^2 & * \\ * & c_1^2 + c_2^2 + c_3^2 + c_4^2 \end{pmatrix}$$

Sum of 4 squares equations

$\Rightarrow$ take $\mathcal{H} = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + ij\mathbb{Q}$ (quaternion algebra, $i^2 = j^2 = -1$, $ij = -ji$)

Cryptanalysis of module-LIP: cyclotomic fields

Take $K = \mathbb{Q}[i]$ (for simplicity)

Module-LIP: $C = \begin{pmatrix} a_1 + ia_2 & c_1 + ic_2 \\ b_1 + ib_2 & d_1 + id_2 \end{pmatrix}$ secret, $G = \overline{C}^T C$ public, recover C from G

$$G = \begin{pmatrix} a_1^2 + a_2^2 + b_1^2 + b_2^2 & * \\ * & c_1^2 + c_2^2 + c_3^2 + c_4^2 \end{pmatrix}$$

Sum of 4 squares equations

$\Rightarrow$ take $\mathcal{H} = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + ij\mathbb{Q}$ (quaternion algebra, $i^2 = j^2 = -1$, $ij = -ji$)

$\Rightarrow$ solve $\bar{z}z = \alpha$ in $\mathcal{H}$

Cyclotomic fields (continued)

Module-LIP $\leq$ solving $z\bar{z} = \alpha$ in $\mathcal{H} = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + ij\mathbb{Q}$

Cyclotomic fields (continued)

Module-LIP $\leq$ solving $z\bar{z} = \alpha$ in $\mathcal{H} = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + ij\mathbb{Q}$

Do we have a Gentry-Szydlo algorithm in $\mathcal{H}$?

- not for the moment (when the degree of P is large)
- cannot conclude the attack in the cyclotomic case

Summing up

Hardness of module-LIP in various fields (modules of rank 2, $K = \mathbb{Q}[X]/P$)

- If P has (at least) one real root: heuristic quantum poly time attack

Summing up

Hardness of module-LIP in various fields (modules of rank 2, $K = \mathbb{Q}[X]/P$)

- If P has (at least) one real root: heuristic quantum poly time attack
- NTRUPrime fields: heuristic classical poly time attack

Summing up

Hardness of module-LIP in various fields (modules of rank 2, $K = \mathbb{Q}[X]/P$)

- If P has (at least) one real root: heuristic quantum poly time attack
- NTRUPrime fields: heuristic classical poly time attack
- Cyclotomic fields: no attack to far...
  ...but a reduction to Gentry-Szydlo in a quaternion algebra

Conclusion

Conclusion

Constructions

- KEM, PKE and signatures from (module-)LIP
- (open) other primitives?
  - possible strategy: rephrase LWE-based constructions in a more geometric way

Conclusion

Constructions

- KEM, PKE and signatures from (module-)LIP
- (open) other primitives?
  - possible strategy: rephrase LWE-based constructions in a more geometric way

Cryptanalysis

- plain LIP (unstructured) seems fine
- module-LIP in $\mathcal{O}_K^2$ $\Rightarrow$ cryptanalysis not yet stabilized
  - hardness seems dependent on the choice of the field
  - luckily, Hawk uses cyclotomic fields $\Rightarrow$ unbroken so far
  - (open) is there really a difference in hardness between fields?

Conclusion

Constructions

- KEM, PKE and signatures from (module-)LIP
- (open) other primitives?
  - possible strategy: rephrase LWE-based constructions in a more geometric way

Cryptanalysis

- plain LIP (unstructured) seems fine
- module-LIP in $\mathcal{O}_K^2$ $\Rightarrow$ cryptanalysis not yet stabilized
  - hardness seems dependent on the choice of the field
  - luckily, Hawk uses cyclotomic fields $\Rightarrow$ unbroken so far
  - (open) is there really a difference in hardness between fields?

Thank you