中国科学院大学
University of Chinese Academy of Sciences

Cryptanalysis of Rank-2 Module-LIP with Symplectic Automorphisms

Hengyi Luo **Kaijie Jiang** **Yanbin Pan** **Anyu Wang**

Academy of Mathematics and Systems Science, Chinese Academy of Sciences

数系天地 勤笃求真

AsiaCrypt2024
December 13, 2024

Contents

HAWK

Lattice-based Signatures

Algorithm	Algorithm Information	Submitters	Comments
HAWK	Specification Zip file Website	Joppe W. Bos Olivier Bronchain Léo Ducas Serge Fehr Yu-Hsuan Huang Thomas Pornin Eamonn W. Postlethwaite Thomas Prest Ludo N. Pulles Wessel van Woerden	Submit Comment View Comments

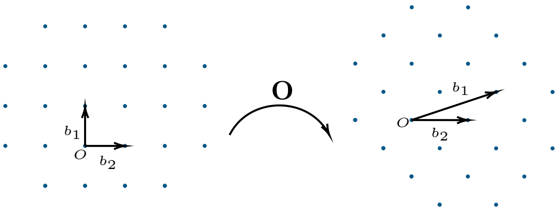
Figure: HAWK

- NIST submission additional call for signatures Round 2
- efficient / compact
- based on Lattice Isomorphism Problem

Lattices Isomorphism Problem

LIP(geometric version)

Given lattices bases $\mathbf{B}_1, \mathbf{B}_2 \in \mathrm{GL}_n(\mathbb{R})$ of isomorphic lattices, find $\mathbf{O} \in \mathcal{O}_n(\mathbb{R})$ and $\mathbf{U} \in \mathrm{GL}_n(\mathbb{Z})$ s.t. $\mathbf{B}_1 = \mathbf{O}\mathbf{B}_2\mathbf{U}$.



Lattices Isomorphism Problem: Another Definition

- For two positive definite matrices (quadratic forms) $\mathbf{G}_1, \mathbf{G}_2 \in \mathbb{Z}^{n\times n}$, we say $\mathbf{G}_1 \cong \mathbf{G}_2$ if there exists a unimodular matrix $\mathbf{U}$ such that $\mathbf{U}^\top \mathbf{G}_1 \mathbf{U} = \mathbf{G}_2$.
- Denote $\mathbf{G}_1 = \mathbf{B}_1^\top \mathbf{B}_1$, $\mathbf{G}_2 = \mathbf{B}_2^\top \mathbf{B}_2$, if $\mathbf{B}_1 = \mathbf{O}\mathbf{B}_2\mathbf{U}$, then

$$\mathbf{G}_1 \cong \mathbf{G}_2.$$

LIP: (quadratic form version)

Given two matrices $\mathbf{G}_1 \cong \mathbf{G}_2$, find a unimodular matrix $\mathbf{U}$ such that $\mathbf{U}^\top \mathbf{G}_2 \mathbf{U} = \mathbf{G}_1$. In particular, If $\mathbf{G}_1 = \mathbf{I}_n$, we call this problem $\mathbb{Z}$LIP.

Related cryptographic works

Algorithms

- In [HR14], Haviv and Regev propose an $n^{O(n)}$-time algorithm for the general LIP, which remains the fastest known algorithm for solving LIP.
- In [BGPSD23], Bennett et al. give a $2^{n/2}$-time algorithm for $\mathbb{Z}$LIP through reducing $\mathbb{Z}$LIP to $O(1)-$ uSVP.
- In [Duc23], Ducas gives a $2^{n/2}$-time algorithm for $\mathbb{Z}$LIP through reducing $\mathbb{Z}$LIP to $n/2$ dimension SVP.

Cryptographic constructions

- LIP with unstructured lattices [DvW22, BGPSD23], e.g. $\mathcal{L} = \mathbb{Z}^n$.

Structurally: module-LIP

- A number field $\mathbb{K}$ is a finite extension of the rational numbers $\mathbb{Q}$. Let $\mathcal{O}_{\mathbb{K}}$ be the ring of integers of certain number field $\mathbb{K}$.
  Examples: $K = \mathbb{Q}[X]/(X^{2^k}+1)$ and $\mathcal{O}_K = \mathbb{Z}[X]/(X^{2^k}+1)$ (or $K = \mathbb{Q}$ and $\mathcal{O}_K = \mathbb{Z}$).
- For any extension $\mathbb{K}$ of degree d, there are exactly d embeddings $\sigma_1, ..., \sigma_d$ from $\mathbb{K}$ into the complex numbers $\mathbb{C}$.
- We call this map $\sigma : x \in \mathbb{K} \mapsto (\sigma_1(x), \ldots, \sigma_d(x))^T \in \mathbb{C}^d$ canonical embedding of number field $\mathbb{K}$.
- We will often identify $\mathbb{K}$ with the image underlying its canonical embedding, then $\mathcal{O}_{\mathbb{K}}$ is a lattice.

Structurally: module-LIP

- An $\mathcal{O}_{\mathbb{K}}$-module lattice is a finitely generated module in $\mathbb{K}^\ell$ over $\mathcal{O}_{\mathbb{K}}$. It has the form $b_1\mathcal{I}_1 + \cdots + b_r\mathcal{I}_r$ where $b_i \in \mathbb{K}^\ell$, $\mathcal{I}_i \subseteq \mathbb{K}$ is an $\mathcal{O}_{\mathbb{K}}$-ideal.
- We call r the rank of this module lattice and usually consider the case when $r = \ell$.

Structurally: module-LIP

- Notation:$X^* := \overline{X}^T$, for any $X \in M_2(\mathbb{K})$.

quadratic form version(free module case)[DPPvW22]

Given $B, G \in \mathsf{GL}_2(\mathbb{K})$, find $U \in \mathsf{GL}_2(\mathcal{O}_\mathbb{K})$ such that $(BU)^*(BU) = G$.

- In [MPMPW24], Mureau et al. give the definition of module-LIP for general module lattices through pseudo-basis.

Related cryptographic works

Algorithms

- There are a series of work about solve LIP with certain symmetry [GS02, JS14, JS17, LJS19], e.g. ideal lattices in $\mathbb{Z}[x]/(x^n+1)$.
- In [MPMPW24], Mureau et al. propose a **heuristic probability** algorithm to solve rank 2 module-LIP in totally real number fields which runs in polynomial time for a large class of the inputs.

Construction

Signature scheme Hawk [DPPvW22]. Instantiated on the module $\mathcal{O}_{\mathbb{K}}^2$ where $\mathbb{K}=\mathbb{Q}(\zeta_{2^d})$.

中国科学院大学
University of Chinese Academy of Sciences

Our Works

- We propose a **provable deterministic** polynomial-time algorithm that solves module-LIP for the rank-2 module $M \subset \mathbb{K}^2$ where $\mathbb{K}$ is a totally real number field.
- We **invalidates the omSVP assumption** introduced by HAWK to prove its forgery security. We stress that our results **haven't yielded any actual attack** against HAWK.

Key tool

New lattice automorphism for rank 2 module lattice.

Lattice Automorphism

Lattice automorphism

Lattice automorphism

Given a lattice base $\mathbf{B} \in \mathsf{GL}_n(\mathbb{R})$, find $\mathbf{O} \in \mathcal{O}_n(\mathbb{R})$ and $\mathbf{U} \in \mathsf{GL}_n(\mathbb{Z})$ s.t. $\mathbf{B} = \mathbf{OBU}$. We denote all such O by $\mathcal{O}(\mathcal{L}(\mathbf{B}))$ and all such U by $\mathsf{Aut}(\mathbf{B}^T\mathbf{B})$. We refer to all of them as lattice automorphisms.

Notice that:

$$U \in \mathsf{Aut}(\mathbf{B}^T\mathbf{B})$$

$$\updownarrow$$

$$\forall v, w \in \mathbb{Z}^n, \langle v, w \rangle_{\mathbf{B}^T\mathbf{B}} = v^T B^T B w = v^T U^T B^T B U w = \langle Uv, Uw \rangle_{\mathbf{B}^T\mathbf{B}}.$$

Motivation: why we focus on lattice automorphism

- In [GS02], Gentry and Szydlo provide a polynomial-time algorithm for the ideal Lattice Isomorphism Problem (ideal-LIP).
  - Specifically, for an element f in the ring $R = \mathbb{Z}[x]/(x^n + 1)$, given (f) and $f^* \cdot f$, it is possible to efficiently recover f (up to multiplication by x^i).
- In [JS17], Lenstra and Silverberge point out that essence of successful is: let $G = \{x^i | i \in [2n]\}$, then $G \subseteq \mathcal{O}(R)$ and satisfies certain properties.
- In [JWL$^+$23], Jiang et al. show that if we are able to find non-trivial lattice automorphisms of the input to $\mathbb{Z}$LIP, then we can solve $\mathbb{Z}$LIP.

Motivation: why we focus on lattice automorphism

- For the instance used in HAWK, $\mathcal{O}_{\mathbb{K}}^2$ also has some known lattice automorphisms: $\{\zeta_{2^d}^i\}$.
- Its forgery security is based on the hardness of the one more SVP, which implied the difficulty of computing other lattice automorphisms.

So there is a natural question:

Does the algebraic structure of $\mathcal{O}_{\mathbb{K}}^2$ give us more lattice automorphisms?

Answer: Yes.

New lattice automorphism induced by symplectic matrix

- Let $J_2 := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.
- Let $\mathbb{L}$ be a CM number field (e.g. cyclotomic field), $B \in \mathsf{GL}_2(\mathbb{L})$, $U \in \mathsf{GL}_2(\mathcal{O}_{\mathbb{L}})$, $G' = (BU)^*(BU)$.
- Define $t_* : \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{L}^2 \mapsto \begin{pmatrix} x^* \\ y^* \end{pmatrix} \in \mathbb{L}^2$ as a $\mathbb{Q}$ linear map.

New lattice automorphism induced by symplectic matrix

New lattice automorphism

$(BU)^{-1}J_2t_*(BU)$ is a lattice automorphism for quadratic $G'=(BU)^*BU$.

$\forall v_i=(BU)^{-1}(x_i,y_i)^T\in\mathbb{L}^2$, i = 1,2,
then $(BU)^{-1}J_2t_*(BU)v_i=(BU)^{-1}(y_i^*,-x_i^*)^T$, i=1,2.

$$
\begin{aligned}
&\langle v_1,v_2\rangle_{G'}\\
=&\mathrm{tr}_{L/\mathbb{Q}}(v_1^*G'v_2)=\mathrm{tr}_{L/\mathbb{Q}}((x_1^*,y_1^*)(x_2,y_2)^T)\\
=&\mathrm{tr}_{L/\mathbb{Q}}(x_1^*x_2+y_1^*y_2)=\mathrm{tr}_{L/\mathbb{Q}}(x_1x_2^*+y_1y_2^*)\\
=&\mathrm{tr}_{L/\mathbb{Q}}((y_1,-x_1)(y_2^*,-x_2^*)^T)\\
=&\mathrm{tr}_{L/\mathbb{Q}}((((BU)^{-1}J_2t_*(BU)v_1)^*G'((BU)^{-1}J_2t_*(BU)v_2))\\
=&\left\langle (BU)^{-1}J_2t_*(BU)v_1,(BU)^{-1}J_2t_*(BU)v_2\right\rangle_{G'}.
\end{aligned}
$$

How to compute $(BU)^{-1}J_2t_*(BU)$

Proposition 1

$\forall S \in GL_2(\mathbb{L}), S^{-1}J_2t_*S = (\det(S)^*I_2) \cdot (S^*S)^{-1} \cdot J_2t_*.$

Given $(BU)^*(BU)$, B, from the above proposition, we only need to compute $\det(BU)$.

- $\det(U) \cdot \det(U)^* \longleftarrow \det((BU)^*(BU))/(\det(B) \cdot \det(B)^*))$
- $(\det(U)) \longleftarrow \mathcal{O}_{\mathbb{K}}$, if $U \in GL_2(\mathcal{O}_{\mathbb{L}})$ (hold on the free module-LIP case)
- $\det(U)$ (up to multiplication by ζ^i) $\longleftarrow$ solver for ideal-LIP.

For general module-LIP case, we need a more detailed argument to obtain $(\det(U))$.

Application

- Above lattice automorphism invalidates the omSVP assumption used in HAWK's forgery security analysis, although it **does not** yield any actual attacks against HAWK itself.
- But it may help the side channel attacks. For example, in [GR24], it is necessary to guess the preimage of two vectors, while using the lattice automorphism only requires guessing the preimage of one vector.
- For **totally real number fields** case, we can use it to solve the rank 2 module-LIP.

The polynomial time algorithm for rank 2 module-LIP in totally real number fields

Module-LIP

- A number field $\mathbb{K}$ is called totally real if for each embedding of $\mathbb{K}$ into the complex numbers the image lies inside the real numbers.
  e.g., $\mathbb{K} = \mathbb{Q}(\zeta) \cap \mathbb{R} = \mathbb{Q}(\zeta + \zeta^{-1})$
- In this case, t_* is commutative with BU, so what we actually obtain is $J_{BU} := (BU)^{-1} J_2 (BU)$.

Recall:

module-LIP(free module version)

Assume $\mathbb{K}$ is a totally real number fields and $\mathbb{L} = \mathbb{K}(\imath)$. Given $B, G' \in \mathsf{GL}_2(\mathbb{K})$, assume $(BU)^*(BU) = G'$. We want to find such a $U \in \mathsf{GL}_2(\mathcal{O}_\mathbb{K})$.

Naive attempt

Combining J_{BU} with $\{\mathrm{diag}(a,a)\}$, use the previous algorithm [LJS19].

$\mathcal{O}_{\mathbb{K}}^2$ case:✓ general case:✗

Reason: Previous algorithms needs strong symmetry of the lattice.

Another attempt: sub module lattice under isomorphism

- BU transform $\mathcal{O}_{\mathbb{L}}^2$ to $B\mathcal{O}_{\mathbb{L}}^2$.
- Can we find a sub (module) lattice $M \subseteq \mathcal{O}_{\mathbb{L}}^2$, $M' \subseteq B\mathcal{O}_{\mathbb{L}}^2$ with lower rank using J_{BU} s.t. BU transform M to M'?
- Let E_λ be the eigenspace of eigenvalue λ. $J_2 \in M_2(\mathbb{L})$ has eigenvalue $\pm\imath$.
- For $B \in \mathsf{GL}_2(\mathbb{L})$, $U \in \mathsf{GL}_2(\mathcal{O}_{\mathbb{L}})$, we have

$$E_\imath(J_{BU}) \cap \mathcal{O}_{\mathbb{L}}^2 = U^{-1}(E_\imath(J_B) \cap \mathcal{O}_{\mathbb{L}}^2) = (BU)^{-1}(E_\imath(J_2) \cap B\mathcal{O}_{\mathbb{L}}^2),$$

  which is a rank 1 module lattice (not full rank).

Deal with rank 1 module-LIP

For a given rank 1 module M, we can write it as $\mathcal{I} \cdot v$

Rank 1 module-LIP

Given $S^{-1}\mathcal{I}v$, $\mathcal{I}, v$, and S^*S for some vector $v \in \mathbb{L}^d$, $\mathcal{O}_{\mathbb{L}}$-ideal $\mathcal{I} \subseteq \mathbb{L}$, matrix $S \in \mathsf{GL}_n(\mathbb{L})$, ask finding $S^{-1}v$.

- $d = 1$: it's just ideal-LIP. In this time $S, v \in \mathbb{L}$, multiplying the inverse of $\mathcal{I}v$ to $S^{-1}\mathcal{I}v$, the problem translates into the classical case:
  finding S, given $\mathcal{O}_{\mathbb{L}}S^{-1}$ and S^*S.
  This has been solved in previous works.
- $d \geq 1$: we do similar treatment: multiplying the inverse of $\mathcal{I}$ to $S^{-1}\mathcal{I}v$.
  The problem translates into:
  finding $S^{-1}v$, given v, $\mathcal{O}_{\mathbb{L}}S^{-1}v$ and S^*S.
  This can be solved using the algorithm in [LJS19].

Summary

Main steps(free module case)

- Compute J_{BU}.
- Compute $\mathcal{L}_{BU} = \ker(J_{BU} - m_\imath) \cap \mathcal{O}_{\mathbb{L}}^2$ and vector $v_B \in \mathbb{L}^2$, ideal $\mathcal{I}_B \subseteq \mathbb{L}$ s.t. $\ker(J_2 - m_\imath) \cap B\mathcal{O}_{\mathbb{L}}^2 = \mathcal{I}_B \cdot v_B$.
- Find $(BU)^{-1}v_B$ from $\mathcal{L}_{BU}, \mathcal{I}_B, v_B$ and then recover BU.

In general case, we need use the properties of the pseudo-basis for more refined handling.

Regard above algorithm as reduction

Theorem 1

Let $\mathbb{L}$ be a CM number field. Given $B^{-1}J'B$, B^*B and $B\mathcal{O}_{\mathbb{L}}^2$ for any element J' in $\mathcal{U}_2(\mathcal{O}_{\mathbb{L}}) \setminus \mu(\mathbb{L})I_2$, we can find B in polynomial time.

Thanks for your attention!

Huck Bennett, Atul Ganju, Pura Peetathawatchai, and Noah Stephens-Davidowitz.
Just how hard are rotations of zn? algorithms and cryptography with the simplest lattice.
In *Advances in Cryptology – EUROCRYPT 2023: 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23-27, 2023, Proceedings, Part V*, page 252–281, Berlin, Heidelberg, 2023. Springer-Verlag.

Léo Ducas, Eamonn W. Postlethwaite, Ludo N. Pulles, and Wessel P. J. van Woerden.
Hawk: Module LIP makes lattice signatures fast, compact and simple.
In Shweta Agrawal and Dongdai Lin, editors, *Advances in Cryptology - ASIACRYPT 2022 - 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5-9, 2022, Proceedings, Part IV*, volume 13794 of *Lecture Notes in Computer Science*, pages 65–94. Springer, 2022.

Reference

Leo Ducas.
Provable lattice reduction of zn with blocksize n/2.
Designs, Codes and Cryptography, 92:1–8, 11 2023.

Léo Ducas and Wessel P. J. van Woerden.
On the lattice isomorphism problem, quadratic forms, remarkable lattices, and cryptography.
In Orr Dunkelman and Stefan Dziembowski, editors, *Advances in Cryptology - EUROCRYPT 2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30 - June 3, 2022, Proceedings, Part III*, volume 13277 of *Lecture Notes in Computer Science*, pages 643–673. Springer, 2022.

Morgane Guerreau and Mélissa Rossi.
A not so discrete sampler: Power analysis attacks on HAWK signature scheme.
Cryptology ePrint Archive, Paper 2024/1248, 2024.

Craig Gentry and Michael Szydlo.
Cryptanalysis of the revised NTRU signature scheme.
In Lars R. Knudsen, editor, *Advances in Cryptology - EUROCRYPT 2002, International Conference on the Theory and Applications of Cryptographic Techniques, Amsterdam, The Netherlands, April 28 - May 2, 2002, Proceedings*, volume 2332 of *Lecture Notes in Computer Science*, pages 299–320. Springer, 2002.

Ishay Haviv and Oded Regev.
On the lattice isomorphism problem.
In Chandra Chekuri, editor, *Proceedings of the Twenty-Fifth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2014, Portland, Oregon, USA, January 5-7, 2014*, pages 391–404. SIAM, 2014.

Reference

Hendrik W. Lenstra Jr. and Alice Silverberg.
Revisiting the gentry-szydlo algorithm.
In Juan A. Garay and Rosario Gennaro, editors, *Advances in Cryptology - CRYPTO 2014 - 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2014, Proceedings, Part I*, volume 8616 of *Lecture Notes in Computer Science*, pages 280–296. Springer, 2014.

Hendrik W. Lenstra Jr. and Alice Silverberg.
Lattices with symmetry.
J. Cryptol., 30(3):760–804, 2017.

Kaijie Jiang, Anyu Wang, Hengyi Luo, Guoxiao Liu, Yang Yu, and Xiaoyun Wang.
Exploiting the symmetry of zn: Randomization and the automorphism problem.
In *Advances in Cryptology – ASIACRYPT 2023: 29th International Conference on the Theory and Application of Cryptology and Information Security, Guangzhou, China, December 4–8, 2023, Proceedings, Part IV*, page 167–200, Berlin, Heidelberg, 2023. Springer-Verlag.

Reference

Hendrik W Lenstra Jr and Alice Silverberg.
Testing isomorphism of lattices over cm-orders.
SIAM Journal on Computing, 48(4):1300–1334, 2019.

Guilhem Mureau, Alice Pellet-Mary, Georgii Pliatsok, and Alexandre Wallet.
Cryptanalysis of rank-2 module-lip in totally real number fields.
In *Advances in Cryptology – EUROCRYPT 2024: 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zurich, Switzerland, May 26–30, 2024, Proceedings, Part VII*, page 226–255, Berlin, Heidelberg, 2024. Springer-Verlag.