How Not to Instantiate the (Module)-Quadratic Form Equivalence Problem

CHARM Workshop

Henry Bambury [1,2], Phong Nguyen [1]

[1]DIENS, Inria Team CASCADE [2]DGA

Tuesday, June 17th, 2025

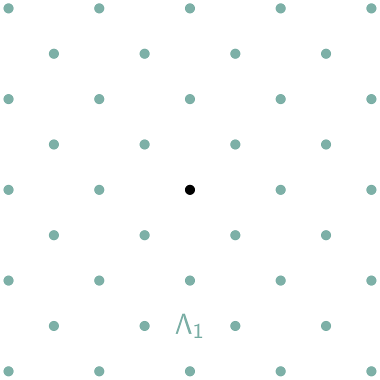
Outline

I. Intro: (Module)-Quadratic Form Equivalence?

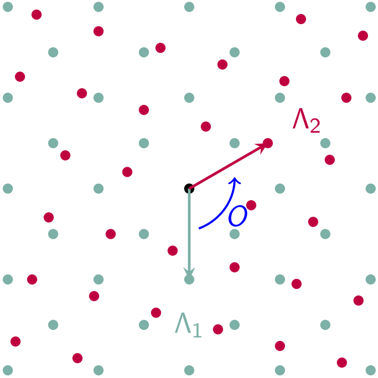
II. The DEFI signature scheme by Feussner and Semaev

III. A key-recovery attack on DEFI

A recent problem in lattice crypto [DvW22,BGPS23]

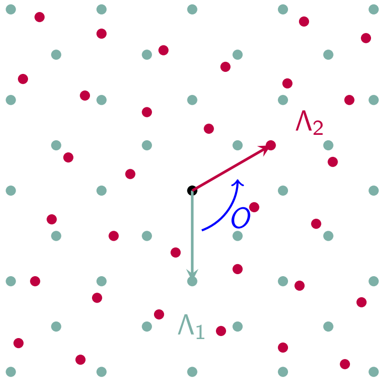


A recent problem in lattice crypto [DvW22,BGPS23]



$$\Lambda_2 = O \cdot \Lambda_1$$

A recent problem in lattice crypto [DvW22,BGPS23]



$\Lambda_2 = O \cdot \Lambda_1$

(search)-Lattice Isomorphism Problem: LIP

Given two lattices $\Lambda_1, \Lambda_2 \subset \mathbb{R}^n$ such that there exists $O \in \mathcal{O}_n(\mathbb{R})$ for which $\Lambda_1 = O \cdot \Lambda_2$, recover a O (up to automorphism).

Λ is *integral* if $\langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z}$ for all $\mathbf{x}, \mathbf{y} \in \Lambda$.
In particular if $\mathbf{B}$ is a basis of Λ, $\mathbf{B}^T\mathbf{B} \in S_n(\mathbb{Z})$.

Lattice Isomorphism Problem

Λ is *integral* if $\langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z}$ for all $\mathbf{x}, \mathbf{y} \in \Lambda$.
In particular if $\mathbf{B}$ is a basis of Λ, $\mathbf{B}^T\mathbf{B} \in S_n(\mathbb{Z})$.

LIP: Gram Matrix version

Let $\mathbf{Q} \in S_n(\mathbb{Z})$ be a positive definite quadratic form. Given $\mathbf{Q}' \in S_n(\mathbb{Z})$ another positive definite quadratic form, find $\mathbf{U} \in \mathrm{GL}_n(\mathbb{Z})$ such that

$$\mathbf{Q}' = \mathbf{U}^T\mathbf{Q}\mathbf{U},$$

assuming such a $\mathbf{U}$ exists.

Quadratic Forms: Terminology

- Over $\mathbb{R}$:
$$\mathbf{x} \mapsto \mathbf{x}^T \mathbf{Q} \mathbf{x},$$
where $\mathbf{x} \in \mathbb{R}^n$ and $\mathbf{Q}$ is **symmetric**.

Quadratic Forms: Terminology

- Over $\mathbb{R}$:
$$\mathbf{x} \mapsto \mathbf{x}^T \mathbf{Q} \mathbf{x},$$
where $\mathbf{x} \in \mathbb{R}^n$ and $\mathbf{Q}$ is **symmetric**.

- Over $\mathbb{C}$:
$$\mathbf{z} \mapsto \overline{\mathbf{z}^T} \mathbf{H} \mathbf{z},$$
where $\mathbf{z} \in \mathbb{C}^n$ and $\mathbf{H}$ is **Hermitian**.

Quadratic Forms: Terminology

- Over $\mathbb{R}$:
$$\mathbf{x} \mapsto \mathbf{x}^T \mathbf{Q} \mathbf{x},$$
where $\mathbf{x} \in \mathbb{R}^n$ and $\mathbf{Q}$ is **symmetric**.

- Over $\mathbb{C}$:
$$\mathbf{z} \mapsto \overline{\mathbf{z}^T} \mathbf{H} \mathbf{z},$$
where $\mathbf{z} \in \mathbb{C}^n$ and $\mathbf{H}$ is **Hermitian**.

- $\mathbf{Q}$ can be **positive definite** if $\mathbf{x}^T \mathbf{Q} \mathbf{x} > 0$ for $\mathbf{x} \neq \mathbf{0}$.
- If the sign of $\mathbf{x}^T \mathbf{Q} \mathbf{x}$ changes, we say $\mathbf{Q}$ is **indefinite**.
- A vector $\mathbf{x} \neq \mathbf{0}$ such that $\mathbf{x}^T \mathbf{Q} \mathbf{x} = 0$ is called **isotropic**.

Quadratic Forms: Equivalence

Equivalence of forms - unstructured

Quadratic forms $\mathbf{Q}, \mathbf{Q}' \in S_n(\mathbb{Z})$ are $\mathbb{Z}$-equivalent if there exists $\mathbf{U} \in \mathrm{GL}_n(\mathbb{Z})$ such that

$$\mathbf{Q}' = \mathbf{U}^T \mathbf{Q} \mathbf{U}.$$

Quadratic Forms: Equivalence

Equivalence of forms - unstructured

Quadratic forms $\mathbf{Q}, \mathbf{Q}' \in S_n(\mathbb{Z})$ are $\mathbb{Z}$-equivalent if there exists $\mathbf{U} \in \mathrm{GL}_n(\mathbb{Z})$ such that

$$\mathbf{Q}' = \mathbf{U}^T \mathbf{Q} \mathbf{U}.$$

More generally, let $\mathbb{Z} \subseteq R \subset \mathbb{C}$ be a ring.

Equivalence of forms - structured

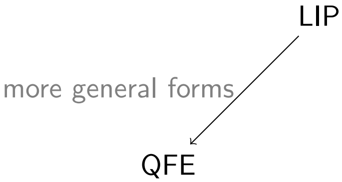
Hermitian forms $\mathbf{H}, \mathbf{H}' \in H_r(R)$ are R-equivalent if there exists $\mathbf{U} \in \mathrm{GL}_r(R)$ such that

$$\mathbf{H}' = \overline{\mathbf{U}}^T \mathbf{H} \mathbf{U}.$$

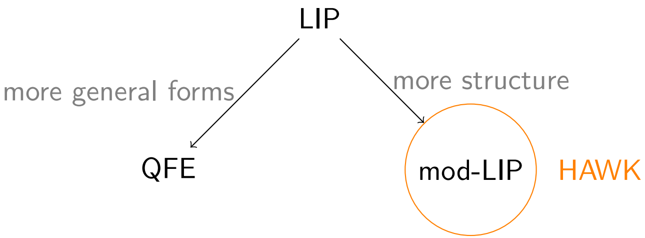
Where do we go from now?

LIP

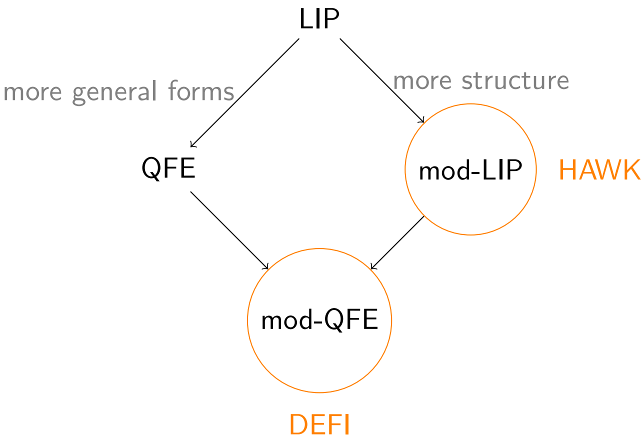
Where do we go from now?



Where do we go from now?



Where do we go from now?



Examples

- HAWK uses $\mathbf{H} = \mathrm{Diag}(1,1) \in R^{2\times 2}$:
  Given $\mathbf{H}' \in R^{2\times 2}$ R-equivalent to $\mathbf{H}$, find $\mathbf{B} \in \mathrm{GL}_2(R)$ such that $\mathbf{H}' = \overline{\mathbf{B}}^T \mathbf{B}$.

Examples

- HAWK uses $\mathbf{H} = \mathrm{Diag}(1,1) \in R^{2\times 2}$:
  Given $\mathbf{H}' \in R^{2\times 2}$ R-equivalent to $\mathbf{H}$, find $\mathbf{B} \in \mathrm{GL}_2(R)$ such that $\mathbf{H}' = \overline{\mathbf{B}}^T\mathbf{B}$.

- DEFI uses $\mathbf{J} = \mathrm{Diag}(1,1,-1,-1) \in R^{4\times 4}$.
  Given $\mathbf{C} \in R^{4\times 4}$ R-equivalent to $\mathbf{J}$, find $\mathbf{B} \in \mathrm{GL}_4(R)$ such that $\mathbf{C} = \mathbf{B}^T\mathbf{J}\mathbf{B}$.

Examples

- HAWK uses $\mathbf{H} = \mathrm{Diag}(1, 1) \in R^{2\times 2}$:
  Given $\mathbf{H}' \in R^{2\times 2}$ R-equivalent to $\mathbf{H}$, find $\mathbf{B} \in \mathrm{GL}_2(R)$ such that $\mathbf{H}' = \overline{\mathbf{B}}^T \mathbf{B}$.

- DEFI uses $\mathbf{J} = \mathrm{Diag}(1, 1, -1, -1) \in R^{4\times 4}$.
  Given $\mathbf{C} \in R^{4\times 4}$ R-equivalent to $\mathbf{J}$, find $\mathbf{B} \in \mathrm{GL}_4(R)$ such that $\mathbf{C} = \mathbf{B}^T \mathbf{J} \mathbf{B}$.

In both cases, $R = \mathbb{Z}[X]/(X^{2^k} + 1)$ is used in practice.

LIP with Gram Matrices

$\mathbf{Q}$ = positive definite quadratic form $\in R^{r\times r}$. Given $\mathbf{Q}'$ equivalent to $\mathbf{Q}$, find $\mathbf{U} \in \mathrm{GL}_r(R)$ such that

$$\mathbf{Q}' = \overline{\mathbf{U}}^T \mathbf{Q} \mathbf{U}.$$

↓

New! Quadratic Form Equivalence

$\mathbf{J}$ = ~~positive definite~~ indefinite quadratic form $\in R^{r\times r}$. Given $\mathbf{C}$ equivalent to $\mathbf{J}$, find $\mathbf{B} \in \mathrm{GL}_r(R)$ such that

$$\mathbf{C} = \mathbf{B}^T \mathbf{J} \mathbf{B}.$$

(Polynomial Ring) MQ[1] Problem

Given (c_{ij}), solve

$$\begin{cases} c_{11} &= b_{11}^2 + b_{12}^2 - b_{13}^2 - b_{14}^2 \\ c_{22} &= b_{21}^2 + b_{22}^2 - b_{23}^2 - b_{24}^2 \\ c_{33} &= b_{31}^2 + b_{32}^2 - b_{33}^2 - b_{34}^2 \\ c_{44} &= b_{41}^2 + b_{42}^2 - b_{43}^2 - b_{44}^2 \\ & \vdots \end{cases},$$

where

$$b_{ij}, c_{ij} \in R = \mathbb{Z}[X]/(X^{2^k} + 1).$$

[1] MQ = Multivariate Quadratic.

...is this lattice or multivariate crypto?

LIP with Gram Matrices

$\mathbf{Q}$ = positive definite quadratic form $\in R^{r\times r}$. Given $\mathbf{Q}'$ equivalent to $\mathbf{Q}$, find $\mathbf{U} \in$ ...

$\mathbf{Q}'$ ...

MQ is hard so QFE should also be?

New! Quadratic Form Equivalence

$\mathbf{J}$ = ~~positive definite~~ indefinite quadratic form $\in R^{r\times r}$. Given $\mathbf{C}$ equivalent to $\mathbf{J}$, find $\mathbf{B} \in \mathrm{GL}_r(R)$ such that

$$\mathbf{C} = \mathbf{B}^T\mathbf{J}\mathbf{B}.$$

(Polynomial Ring) MQ[1] Problem

$$\begin{cases} c_{11} &= b_{11}^2 + b_{12}^2 - b_{13}^2 - b_{14}^2 \\ c_{22} &= b_{21}^2 + b_{22}^2 - b_{23}^2 - b_{24}^2 \\ c_{33} &= b_{31}^2 + b_{32}^2 - b_{33}^2 - b_{34}^2 \\ c_{44} &= b_{41}^2 + b_{42}^2 - b_{43}^2 - b_{44}^2 \\ & \vdots \end{cases},$$

where

$$b_{ij}, c_{ij} \in R = \mathbb{Z}[X]/(X^{2^k}+1).$$

[1] MQ = Multivariate Quadratic.

LIP with Gram Matrices

$\mathbf{Q}$ = positive definite quadratic form $\in R^{r\times r}$. Given $\mathbf{Q}'$ equivalent to $\mathbf{Q}$, find $\mathbf{U} \in$ ...

$\mathbf{Q}'$ ...

MQ is hard so QFE should also be?

(Polynomial Ring) MQ[1] Problem

$$\begin{cases} c_{11} &= b_{11}^2 + b_{12}^2 - b_{13}^2 - b_{14}^2 \\ & \quad + b_{22}^2 - b_{23}^2 - b_{24}^2 \\ & \quad + b_{32}^2 - b_{33}^2 - b_{34}^2, \\ c_{44} &= b_{41}^2 + b_{42}^2 - b_{43}^2 - b_{44}^2 \\ & \vdots \end{cases}$$

where

$$b_{ij}, c_{ij} \in R = \mathbb{Z}[X]/(X^{2^k}+1).$$

Is QFE as hard as LIP??

New! Quadratic Form ...

$\mathbf{J}$ = ~~positive definite~~ indefinite quadratic form $\in R^{r\times r}$. Given $\mathbf{C}$ equivalent to $\mathbf{J}$, find $\mathbf{B} \in \mathrm{GL}_r(R)$ such that

$$\mathbf{C} = \mathbf{B}^T\mathbf{J}\mathbf{B}.$$

[1] MQ = Multivariate Quadratic.

LIP with Gram Matrices

$\mathbf{Q}$ = positive definite quadratic form $\in R^{r\times r}$. Given $\mathbf{Q}'$ equivalent to $\mathbf{Q}$, find $\mathbf{U} \in$ ...

$\mathbf{Q}'$ ...

MQ is hard so QFE should also be?

New! Quadratic For...

$\mathbf{J}$ = ~~positive definite~~ indefinite quadratic form ... equivalent to $\mathbf{J}$, ... such that

$$\mathbf{C} = \mathbf{B}^T \mathbf{J} \mathbf{B}.$$

Is QFE as hard as LIP??

(Polynomial Ring) MQ[1] Problem

$$\begin{cases} c_{11} = b_{11}^2 + b_{12}^2 - b_{13}^2 - b_{14}^2 \\ \quad \dots + b_{22}^2 - b_{23}^2 - b_{24}^2 \\ \quad \dots + b_{32}^2 - b_{33}^2 - b_{34}^2, \\ c_{44} = \dots + b_{42}^2 - b_{43}^2 - b_{44}^2 \\ \quad \vdots \end{cases}$$

Can it be used to make nice schemes?

where

$$b_{ij}, c_{ij} \in R = \mathbb{Z}[X]/(X^{2^k} + 1).$$

[1] MQ = Multivariate Quadratic.

...is this lattice or multivariate crypto?

LIP with Gram Matrices

Q = positive definite quadratic form $\in R^{r\times r}$. Given **Q**′ equivalent to **Q**, find **U** ∈ [illegible]

Q′ [illegible]

MQ is hard so QFE should also be?

New! Quadratic For[illegible]

J = ~~positive definite~~ indefinite quadratic form [illegible] equivalent to **J**, [illegible] such that

$$\mathbf{C} = \mathbf{B}^T \mathbf{J} \mathbf{B}.$$

Is QFE as hard as LIP??

(Polynomial Ring) MQ[1] Problem

$$\begin{cases} c_{11} = b_{11}^2 + b_{12}^2 - b_{13}^2 - b_{14}^2 \\ \ldots + b_{22}^2 - b_{23}^2 - b_{24}^2 \\ \ldots + b_{32}^2 - b_{33}^2 - b_{34}^2 , \\ c_{44} = b_{41}^2 + b_{42}^2 - b_{43}^2 - b_{44}^2 \\ \vdots \end{cases}$$

Can it be used to make nice schemes?

where

$$b_{ij}, c_{ij} \in R = \mathbb{Z}[X]/(X^{2^k} + 1).$$

Let's see...

[1] MQ = Multivariate Quadratic.

Outline

I. Intro: (Module)-Quadratic Form Equivalence?

II. The DEFI signature scheme by Feussner and Semaev

III. A key-recovery attack on DEFI

DEFI: A Hash-and-Sign Signature Scheme [FS24a]

- $R = \mathbb{Z}[X]/(X^{64}+1)$
- $\mathbf{J} = \mathrm{Diag}(1,1,-1,-1) \in R^{4\times 4}$

KeyGen

- The Private key is a **small** $\mathbf{B} = \begin{pmatrix} 1 & \mathbf{0}_{1\times 3} \\ \mathbf{B}_{21} & \mathbf{B}_{22} \end{pmatrix} \in \mathrm{SL}_4(R)$.
- The Public key is $\mathbf{C} := \mathbf{B}^T\mathbf{J}\mathbf{B}$.

Sign(μ, B)

- Complete $H(\mu)$ into an **isotropic** $\mathbf{z}$ (i.e. $\mathbf{z}^T\mathbf{J}\mathbf{z} = 0$).
- Return $\mathbf{y} := \mathbf{B}^{-1}\mathbf{z}$.

Verif(y, μ, C)

- Accept iff $H(\mu) = \mathbf{e}_1^T\mathbf{y}$ and $\mathbf{y}^T\mathbf{C}\mathbf{y} = 0$.

DEFI: A Hash-and-Sign Signature Scheme [FS24a]

- $R = \mathbb{Z}[X]/(X^{64}+1)$
- $\mathbf{J} = \mathrm{Diag}(1,1,-1,-1) \in R^{4\times 4}$

KeyGen

- The Private key is a **small** $\mathbf{B} = \begin{pmatrix} 1 & \mathbf{0}_{1\times 3} \\ \mathbf{B}_{21} & \mathbf{B}_{22} \end{pmatrix} \in \mathrm{SL}_4(R)$.
- The Public key is $\mathbf{C} := \mathbf{B}^T\mathbf{J}\mathbf{B}$.

Sign(μ, B)

- Complete $H(\mu)$ into an **isotropic** $\mathbf{z}$ (i.e. $\mathbf{z}^T\mathbf{J}\mathbf{z} = 0$). $\leftarrow$ **Trapdoor operation**
- Return $\mathbf{y} := \mathbf{B}^{-1}\mathbf{z}$.

Verif(y, μ, C)

- Accept iff $H(\mu) = \mathbf{e}_1^T\mathbf{y}$ and $\mathbf{y}^T\mathbf{C}\mathbf{y} = 0$.

DEFI: A Hash-and-Sign Signature Scheme [FS24a]

- $R = \mathbb{Z}[X]/(X^{64}+1)$
- $\mathbf{J} = \mathrm{Diag}(1, 1, -1, -1) \in R^{4\times 4}$

KeyGen

- The Private key is a small $\mathbf{B} = \begin{pmatrix} 1 & \mathbf{0}_{1\times 3} \\ \mathbf{B}_{21} & \mathbf{B}_{22} \end{pmatrix} \in \mathrm{SL}_4(R)$.
- The Public key is $\mathbf{C} := \mathbf{B}^T \mathbf{J} \mathbf{B}$.

Sign(μ, B)

- Complete $H(\mu)$ into an isotropic $\mathbf{z}$ (i.e. $\mathbf{z}^T \mathbf{J} \mathbf{z} = 0$). ← **Trapdoor operation**
- Return $\mathbf{y} := \mathbf{B}^{-1}\mathbf{z}$. ← **Obfuscation step**

Verif(y, μ, C)

- Accept iff $H(\mu) = \mathbf{e}_1^T \mathbf{y}$ and $\mathbf{y}^T \mathbf{C} \mathbf{y} = 0$.

DEFI: A Hash-and-Sign Signature Scheme [FS24a]

- $R = \mathbb{Z}[X]/(X^{64}+1)$
- $\mathbf{J} = \mathrm{Diag}(1, 1, -1, -1) \in R^{4\times 4}$

KeyGen

- The Private key is a **small** $\mathbf{B} = \begin{pmatrix} 1 & \mathbf{0}_{1\times 3} \\ \mathbf{B}_{21} & \mathbf{B}_{22} \end{pmatrix} \in \mathrm{SL}_4(R)$.
- The Public key is $\mathbf{C} := \mathbf{B}^T \mathbf{J} \mathbf{B}$.

Sign(μ, B)

- Complete $H(\mu)$ into an **isotropic** $\mathbf{z}$ (i.e. $\mathbf{z}^T \mathbf{J} \mathbf{z} = 0$).
- Return $\mathbf{y} := \mathbf{B}^{-1}\mathbf{z}$.

Verif(y, μ, C)

- Accept iff $H(\mu) = \mathbf{e}_1^T \mathbf{y}$ and $\mathbf{y}^T \mathbf{C} \mathbf{y} = 0$.

Correctness:

$$\begin{aligned} \mathbf{y}^T\mathbf{C}\mathbf{y} &= \mathbf{y}^T(\mathbf{B}^T\mathbf{J}\mathbf{B})\mathbf{y} \\ &= (\mathbf{B}\mathbf{y})^T\mathbf{J}(\mathbf{B}\mathbf{y}) \\ &= \mathbf{z}^T\mathbf{J}\mathbf{z} = 0. \end{aligned}$$

The DEFI Trapdoor operation

Sign(μ, B)

- Complete $H(\mu)$ into an **isotropic** $\mathbf{z}$ (i.e. $\mathbf{z}^T \mathbf{J} \mathbf{z} = 0$). $\leftarrow$ **Trapdoor operation**
- Return $\mathbf{y} := \mathbf{B}^{-1}\mathbf{z}$. $\leftarrow$ **Obfuscation step**

Trapdoor($h := H(\mu)$)

- Generate **small** polynomials $u, v \leftarrow R$. $\leftarrow$ **Nonces**
- Return

$$\mathbf{z} := \begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \end{pmatrix} = \begin{pmatrix} h \\ v + u^2 v - hv \\ v - u^2 v + hv \\ 2uv - h \end{pmatrix}.$$

The DEFI Trapdoor operation

Sign(μ, B)

- Complete $H(\mu)$ into an **isotropic** $\mathbf{z}$ (i.e. $\mathbf{z}^T\mathbf{J}\mathbf{z} = 0$). $\leftarrow$ **Trapdoor operation**
- Return $\mathbf{y} := \mathbf{B}^{-1}\mathbf{z}$. $\leftarrow$ **Obfuscation step**

Trapdoor($h := H(\mu)$)

- Generate **small** polynomials $u, v \leftarrow R$.
- Return

$$\mathbf{z} := \begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \end{pmatrix} = \begin{pmatrix} h \\ v + u^2 v - hv \\ v - u^2 v + hv \\ 2uv - h \end{pmatrix}.$$

Trapdoor correctness:

$$\mathbf{z}^T\mathbf{J}\mathbf{z} = z_1^2 + z_2^2 - z_3^2 - z_4^2$$
$$= \cdots = 0.$$

The DEFI Trapdoor operation

Sign(μ, B)

- Complete $H(\mu)$ into an **isotropic** $\mathbf{z}$ (i.e. $\mathbf{z}^T\mathbf{J}\mathbf{z} = 0$). $\leftarrow$ **Trapdoor operation**
- Return $\mathbf{y} := \mathbf{B}^{-1}\mathbf{z}$. $\leftarrow$ **Obfuscation step**

Trapdoor($h := H(\mu)$)

- Generate **small** polynomials $u, v \leftarrow R$.
- Return

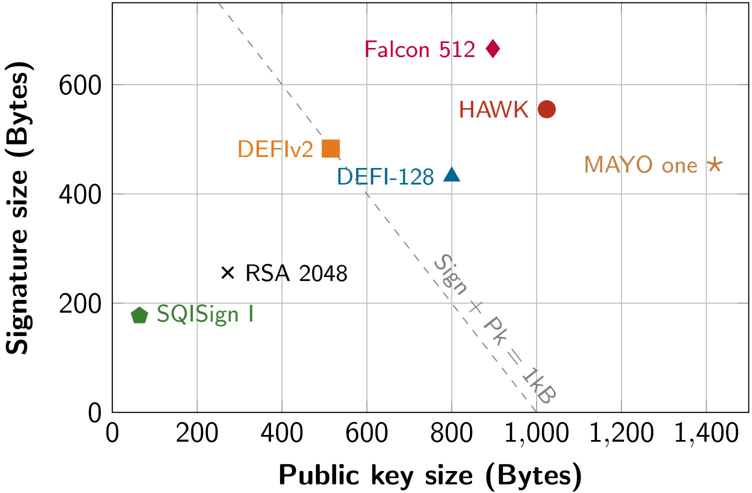
$$\mathbf{z} := \begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \end{pmatrix} = \begin{pmatrix} h \\ v + u^2v - hv \\ v - u^2v + hv \\ 2uv - h \end{pmatrix}.$$

Trapdoor correctness:

$$\mathbf{z}^T\mathbf{J}\mathbf{z} = z_1^2 + z_2^2 - z_3^2 - z_4^2$$
$$= \cdots = 0.$$

For future reference: notice that $z_2 + z_3 = 2v$ and $z_1 + z_4 = 2\mathbf{uv}$.

Suspiciously good performances



Reported speed:

- **KeyGen** < 1 ms
- **Sign** ≈ 0.1 ms
- **Verif** < 0.1 ms

Security

Isotropic Vector Problem (IVP)

Given $\mathbf{C} \in R^{4\times 4}$ R-equivalent to $\mathrm{Diag}(1,1,-1,1)$, find $\mathbf{y} \in R^4$ such that

$$\mathbf{y}^T\mathbf{C}\mathbf{y} = 0.$$

Reduces to

(Module) Quad. Form Equivalence (QFE)

$\mathbf{J} = \mathrm{Diag}(1,1,-1,1)$.
Given $\mathbf{C} \in R^{4\times 4}$ R-equivalent to $\mathbf{J}$, find $\mathbf{B} \in \mathrm{GL}_4(R)$ such that

$$\mathbf{C} = \mathbf{B}^T\mathbf{J}\mathbf{B}.$$

Security

Dream World:

- *forgery* breaks **IVP**
- *key-recovery* breaks **QFE**

Typical in Multivariate Crypto

Reality:

- No formal security proof
- Signatures leak information

Isotropic Vector Problem (**IVP**)

Given $\mathbf{C} \in R^{4\times 4}$ R-equivalent to $\mathrm{Diag}(1,1,-1,1)$, find $\mathbf{y} \in R^4$ such that

$$\mathbf{y}^T\mathbf{C}\mathbf{y} = 0.$$

Reduces to

(Module) Quad. Form Equivalence (**QFE**)

$\mathbf{J} = \mathrm{Diag}(1,1,-1,1)$.
Given $\mathbf{C} \in R^{4\times 4}$ R-equivalent to $\mathbf{J}$, find $\mathbf{B} \in \mathrm{GL}_4(R)$ such that

$$\mathbf{C} = \mathbf{B}^T\mathbf{J}\mathbf{B}.$$

Security

Dream World:

- *forgery* breaks **IVP**
- *key-recovery* breaks **QFE**

Typical in Multivariate Crypto

Reality:

- No formal security proof
- Signatures leak information

Can we exploit the leakage?

Isotropic Vector Problem (IVP)

Given $\mathbf{C} \in R^{4\times4}$ R-equivalent to $\mathrm{Diag}(1,1,-1,1)$, find $\mathbf{y} \in R^4$ such that

$$\mathbf{y}^T\mathbf{C}\mathbf{y} = 0.$$

Reduces to

(Module) Quad. Form Equivalence (QFE)

$\mathbf{J} = \mathrm{Diag}(1,1,-1,1)$.
Given $\mathbf{C} \in R^{4\times4}$ R-equivalent to $\mathbf{J}$, find $\mathbf{B} \in \mathrm{GL}_4(R)$ such that

$$\mathbf{C} = \mathbf{B}^T\mathbf{J}\mathbf{B}.$$

Outline

I. Intro: (Module)-Quadratic Form Equivalence?

II. The DEFI signature scheme by Feussner and Semaev

III. A key-recovery attack on DEFI

Attack Strategy: STEP I

Assuming access to multiple signatures $(\mathbf{y}^{(i)})_{i\in[k]}$.

The vulnerability lies in the trapdoor construction.

- The b_{ij} are small.
- The nonces $u^{(i)}, v^{(i)}$ are small.

STEP I:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ b_{21} & b_{22} & b_{23} & b_{24} \\ b_{31} & b_{32} & b_{33} & b_{34} \\ b_{41} & b_{42} & b_{43} & b_{44} \end{pmatrix}$$

Essential Equation I:

$$\begin{aligned} \begin{pmatrix} 0 & 1 & 1 & 0 \end{pmatrix} \cdot \mathbf{B}\mathbf{y}^{(i)} &= z_2^{(i)} + z_3^{(i)} \\ &= 2v^{(i)} \end{aligned}$$

STEP I: A friendly lattice

From Equation to Lattice

Define

$$L_1 := \left\{ \mathbf{x}^T \begin{pmatrix} | & | & | & | & | & & | \\ \mathbf{e}_1 & \mathbf{e}_2 & \mathbf{e}_3 & \mathbf{e}_4 & \mathbf{y}^{(1)} & \cdots & \mathbf{y}^{(k)} \\ | & | & | & | & | & & | \end{pmatrix} : \mathbf{x} \in R^4 \right\}.$$

Then from $\mathbf{x}_1 = \begin{pmatrix} 0 & 1 & 1 & 0 \end{pmatrix} \cdot \mathbf{B}$ we get $\mathbf{s}_1 = (\mathbf{x}_1 \| 2v^{(1)}, \ldots, 2v^{(k)}) \in L_1$.

Reducing L_1

- $\mathbf{s}_1$ is a **short vector** of L_1.
- As k increases, $\mathrm{rk}(L_1) = 4\dim(R)$ stays constant, but $\|\mathbf{s}_1\| \ll \mathrm{GH}(L_1)$.
- For k large enough, LLL recovers some rotation $X^r \cdot \mathbf{s}_1$.

STEP I: A friendly lattice

From Equation to Lattice

Define

$$L_1 := \left\{ \mathbf{x}^T \begin{pmatrix} | & | & | & | & | & & | \\ \mathbf{e}_1 & \mathbf{e}_2 & \mathbf{e}_3 & \mathbf{e}_4 & \mathbf{y}^{(1)} & \cdots & \mathbf{y}^{(k)} \\ | & | & | & | & | & & | \end{pmatrix} : \mathbf{x} \in R^4 \right\}.$$

Then from $\mathbf{x}_1 = \begin{pmatrix} 0 & 1 & 1 & 0 \end{pmatrix} \cdot \mathbf{B}$ we get $\mathbf{s}_1 = (\mathbf{x}_1 \| 2v^{(1)}, \ldots, 2v^{(k)}) \in L_1$.

Reducing L_1

Analysis is heuristic

- $\mathbf{s}_1$ is a **short vector** of L_1.
- As k increases, $\mathrm{rk}(L_1) = 4\dim(R)$ stays constant, but $\|\mathbf{s}_1\| \ll \mathrm{GH}(L_1)$.
- For k large enough, LLL recovers some rotation $X^r \cdot \mathbf{s}_1$.

STEP I: Partial Analysis

Lemma

If $\mathbf{A}$ and $\mathbf{B}$ are non-negative Hermitian matrices in $M_n(\mathbb{C})$,

$$\det(\mathbf{A}+\mathbf{B})^{1/n} \geq \det(\mathbf{A})^{1/n} + \det(\mathbf{B})^{1/n}.$$

We use this lemma to lower bound the covolume of L_1. If $m := \dim(R)$ and $4|k$, we model L_1 as

$$\left(\mathbf{I}_{4m} \quad || \quad \mathbf{A}_1 \quad || \quad \ldots \quad || \quad \mathbf{A}_{k/4}\right),$$

where all $\mathbf{A}_i$ are square, independently sampled from the same distribution.

$$\mathrm{vol}(L_1)^{\frac{2}{4m}} = \det\left(\mathbf{I}_{4m} + \mathbf{A}_1\mathbf{A}_1^T + \ldots + \mathbf{A}_{k/4}\mathbf{A}_{k/4}^T\right)^{\frac{1}{4m}} \geq 1 + \sum_{i=1}^{k/4} \det\left(\mathbf{A}_i\mathbf{A}_i^T\right)^{\frac{1}{4m}}.$$

$\|\mathbf{s}_1\|$ is easy to estimate.

STEP I: Wrapping up

After step I

If LLL succeeds we know rotations of:

- $b_{2j} + b_{3j}$.
- All the nonces $v^{(i)}$.

- We considered a few extra improvements.
- We do not care that we only get a rotation.

Attack Strategy: STEP II

Assuming access to multiple signatures $(\mathbf{y}^{(i)})_{i \in [k]}$.

The vulnerability lies in the trapdoor construction.

- The b_{ij} are small.
- The nonces $u^{(i)}, v^{(i)}$ are small.

STEP II:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ b_{21} & b_{22} & b_{23} & b_{24} \\ b_{31} & b_{32} & b_{33} & b_{34} \\ \boxed{b_{41}} & \boxed{b_{42}} & \boxed{b_{43}} & \boxed{b_{44}} \end{pmatrix}$$

Essential Equation II:

$$\begin{aligned} \begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix} \cdot \mathbf{B}\mathbf{y}^{(i)} &= z_1^{(i)} + z_4^{(i)} \\ &= 2u^{(i)}v^{(i)} \end{aligned}$$

STEP II: We need a better lattice!

$2u^{(i)}v^{(i)}$ is too big for the same lattice to work. But we know (a rotation of) $v^{(i)}$.

The trick

- Define $R_q := R/qR$, where q is a large prime number.
- The polynomials $2v^{(i)}$ are now invertible in R_q.

Lattice 2.0

$$L_2 := \left\{ \mathbf{x}^T \begin{pmatrix} | & | & | & | & | & & | \\ \mathbf{e}_1 & \mathbf{e}_2 & \mathbf{e}_3 & \mathbf{e}_4 & (2v^{(1)})^{-1}\mathbf{y}^{(1)} & \cdots & (2v^{(k)})^{-1}\mathbf{y}^{(k)} \\ | & | & | & | & | & & | \end{pmatrix} : \mathbf{x} \in R_q^4 \right\}.$$

From $\mathbf{x}_2 = \begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix} \cdot \mathbf{B}$ we get $\mathbf{s}_2 = (\mathbf{x}_2 || u^{(1)}, \ldots, u^{(k)}) \in L_2$.

STEP II: The annoying lattice

Attempting to reduce L_2

- $\mathbf{s}_2$ is a **short vector** of L_2. But not the shortest!
- $\mathbf{s}_2' = (\mathbf{x}_1 || 1, 1, \ldots, 1) \in L_2$.
- L_2 is q-ary, therefore $\mathrm{rk}(L_2) = (k+4)\dim(R)$. This is a problem!

STEP II: The annoying lattice

Attempting to reduce L_2

- $\mathbf{s}_2$ is a **short vector** of L_2. But not the shortest!
- $\mathbf{s}_2' = (\mathbf{x}_1 || 1, 1, \ldots, 1) \in L_2$.
- L_2 is q-ary, therefore $\mathrm{rk}(L_2) = (k+4)\dim(R)$. This is a problem!

We know **a lot** of suspiciously short vectors:

$$L_2' := \langle \mathbf{s}_2, \mathbf{s}_2' \rangle_R \subset L_2.$$

STEP II: The annoying lattice

Attempting to reduce L_2

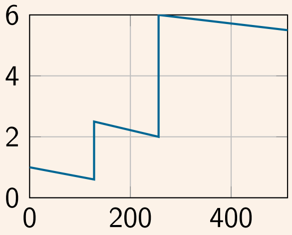
- $\mathbf{s}_2$ is a **short vector** of L_2.
- L_2 is q-ary, therefore $\mathrm{rk}(L_2) = (k+4)\dim(R)$. This is a problem!

$\mathbf{L}_2$ has unusual sublattices

- Dense sublattices, e.g.

$$R\mathbf{s}_2 \subset L'_2 \subset L_2.$$

- LLL recovers L'_2 of rank $\mathrm{rk}(L'_2) = 2\dim(R)$.
- Run lattice reduction directly on L'_2.



Profile of LLL-reduced basis of L_2

STEP II: The annoying lattice

Attempting to reduce L_2

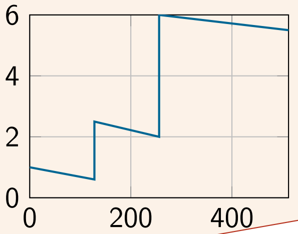
- $\mathbf{s}_2$ is a **short vector** of L_2.
- L_2 is q-ary, therefore $\mathrm{rk}(L_2) = (k+4)\dim(R)$. This is a problem!

$\mathbf{L}_2$ has unusual sublattices

- Dense sublattices, e.g.

$$R\mathbf{s}_2 \subset L_2' \subset L_2.$$

- LLL recovers L_2' of rank $\mathrm{rk}(L_2') = 2\dim(R)$.
- Run lattice reduction directly on L_2'.



Profile of LLL...

Looks like NTRU!

STEP II: Sublattices

LLL inequalities

If $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ is LLL-reduced and $1 \leq k \leq n$, then

$$\det(\mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_k)) \leq 2^{k(n-k)/4} \det(L)^{k/n}.$$

Comparing with the Average Case

For Haar-random real lattices of rank n, the expected number of primitive sublattices L of rank k with $\det(L) \leq H$ is

$$\frac{H^n}{n} \binom{n}{k} \prod_{i=1}^{k} \frac{V(n-i+1)\zeta(i)}{V(i)\zeta(n-i+1)},$$

where $V(i) = \frac{\pi^{i/2}}{\Gamma(1+i/2)}$.

STEP II: Wrapping up

- L_2' is independent of the (artificial) prime q. LLL will recover it for large enough q.
- We separate $R\mathbf{s}_2$ and $R\mathbf{s}_2'$ by reducing a skewed lattice.

STEP II: Wrapping up

- L'_2 is independent of the (artificial) prime q. LLL will recover it for large enough q.
- We separate $R\mathbf{s}_2$ and $R\mathbf{s}'_2$ by reducing a skewed lattice.

After step II

If all succeeds we know rotations of:

- $b_{1j} + b_{4j}$.
- All the nonces $u^{(i)}$.

STEP III: Full key-recovery

Recall

$$\mathbf{C} = \mathbf{B}^T \mathbf{J} \mathbf{B}$$

$c_{ij}, b_{1j}, b_{2j} + b_{3j}, b_{4j}$ are known.

STEP III:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ \boxed{b_{21}} & \boxed{b_{22}} & \boxed{b_{23}} & \boxed{b_{24}} \\ b_{31} & b_{32} & b_{33} & b_{34} \\ b_{41} & b_{42} & b_{43} & b_{44} \end{pmatrix}$$

$$\implies \forall j \in \{1,2,3,4\} \;\; c_{jj}^2 = b_{1j}^2 + b_{2j}^2 - b_{3j}^2 - b_{4j}^2$$

Remember the trick?

If we could invert, we would write

$$b_{2j} - b_{3j} = (b_{2j}^2 - b_{3j}^2)(b_{2j} + b_{3j})^{-1}.$$

- Invert in R_q and then round back to R!
- Detect rotations with parity.

DEFIv2: early thoughts

- Still no convincing security proof.
- Are there reasons why (Module)-QFE might achieve better performances than (Module)-LIP?
- Are there any attacks on (Module)-QFE from decomposition theorems on quadratic forms? What insight does this give on (Module)-LIP?
- Does a variant of our attack still apply?

DEFIv2: changes

- New ring/field! And surprise: it's not cyclotomic

$$K = \mathbb{Q}(X)/(X^{28} + X + 1).$$

- New trapdoor of the form:

$$\mathbf{z} = \begin{pmatrix} V_1 V_4 - V_2 V_3 \\ V_1 V_2 + V_3 V_4 \\ V_1 V_2 - V_3 V_4 \\ V_1 V_4 + V_2 V_3 \end{pmatrix}.$$

Summary and open problems

Conclusions:

- Interesting new assumptions for cryptography: **IVP** and **QFE**.
- A practical lattice attack on DEFI-128: 5min on a laptop with 10 signatures.
- Importance of rigorous security analysis before proposing new schemes.

Open Problems:

- Is a single signature enough to mount the attack?
- What are the exact conditions under which LLL recovers a dense sublattice?
- Can we fix it? New ring and trapdoor in DEFIv2 [FS24b].

Paper: `eprint.iacr.org/2025/133`

References I

Feussner & Semaev.
Isotropic Quadratic Forms, Diophantine Equations and Digital Signatures.
ePrint Archive: https://eprint.iacr.org/archive/2024/679/20240503:175841.

Feussner & Semaev.
Isotropic Quadratic Forms, Diophantine Equations and Digital Signatures, DEFIv2.
ePrint Archive: https://eprint.iacr.org/archive/2024/679/20241105:105112.