Adventures in SIS with Hints

Embracing the brave new world where we make it up as we go

Martin R. Albrecht

10 June 2024

Programme

- The SIS with Hints Zoo is an attempt to keep track of all those new SIS-like assumptions that hand out additional hints.
- I will discuss several of these assumptions here, with a focus on computational hardness rather than design.

  Designers Please consider whether you can re-use one of those many newfangled assumptions before introducing yet another one.

  Cryptanalysts Analyse them!
- I will also dive a bit deeper into some recent adventures in SIS with hints.

Teaser

WHAT IF I TOLD YOU
THAT ISIS IS HARD EVEN GIVEN A TRAPDOOR

Notation I

Definition (M-(I)SIS)

- An instance of M-SIS is given by $\mathbf{A} \leftarrow\!\!\$\; \mathcal{R}_q^{n\times m}$ and has solutions $\mathbf{u}^\star \in \mathcal{R}^m$ such that $\|\mathbf{u}^\star\| \leq \beta^\star$ and $\mathbf{A}\cdot\mathbf{u}^\star \equiv \mathbf{0} \bmod q$.
- An instance of M-ISIS is given by $(\mathbf{A},\mathbf{t}) \leftarrow\!\!\$\; \mathcal{R}_q^{n\times m} \times \mathcal{R}_q^{n}$ and has solutions $\mathbf{u}^\star$ such that $\|\mathbf{u}^\star\| \leq \beta$ and $\mathbf{A}\cdot\mathbf{u}^\star \equiv \mathbf{t} \bmod q$.

- Throughout, feel free to set $\mathcal{R} := \mathbb{Z}$.
- I am not going to discuss issues arising over cyclotomic rings in any detail.

Notation II

- The kernel lattice $\Lambda_q^\perp(\mathbf{A})$ of $\mathbf{A}$ consists of all integral vectors $\mathcal{R}_q$-orthogonal to rows of $\mathbf{A}$:

$$\Lambda_q^\perp(\mathbf{A}) \coloneqq \{\mathbf{x} \in \mathcal{R}^m : \mathbf{A} \cdot \mathbf{x} \equiv \mathbf{0} \bmod q\}.$$

- $\Lambda_q^\perp(\mathbf{A})$ has rank m because $q\mathcal{R}^m \subseteq \Lambda_q^\perp(\mathbf{A}) \subseteq \mathcal{R}^m$.
- I write $\mathbf{G}$ for ”the Gadget matrix”

$$\mathbf{G} \coloneqq \begin{pmatrix} 1 & 2 & 4 & \dots & \lfloor q/2 \rfloor & \dots & 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 0 & \dots & 1 & 2 & 4 & \dots & \lfloor q/2 \rfloor \end{pmatrix}$$

K-SIS

The Original: K-SIS

Definition

For any integer $k \geq 0$, an instance of the k-M-SIS problem[1] is a matrix $\mathbf{A} \in \mathcal{R}_q^{n \times m}$ and a set of k vectors $\mathbf{u}_1, \dots \mathbf{u}_k$ s.t. $\mathbf{A} \cdot \mathbf{u}_i \equiv \mathbf{0} \bmod q$ with $\|\mathbf{u}_i\| \leq \beta$. A solution to the problem is a nonzero vector $\mathbf{u}^\star \in \mathcal{R}^m$ such that

$$\|\mathbf{u}^\star\| \leq \beta^*, \quad \mathbf{A} \cdot \mathbf{u}^\star \equiv \mathbf{0} \bmod q, \quad \text{and} \quad \mathbf{u}^\star \notin \mathcal{K}\text{-}\mathsf{span}(\{\mathbf{u}_i\}_{1 \leq i \leq k}).$$

Dan Boneh and David Mandell Freeman. Linearly Homomorphic Signatures over Binary Fields and New Tools for Lattice-Based Signatures. In: *PKC 2011*. Ed. by Dario Catalano, Nelly Fazio, Rosario Gennaro and Antonio Nicolosi. Vol. 6571. LNCS. Springer, Heidelberg, Mar. 2011, pp. 1–16. DOI: 10.1007/978-3-642-19379-8_1

[1] This is the module variant defined in [ACLMT22].

K-SIS Hardness

- [BF11] showed that k-SIS (over $\mathbb{Z}$) is hard if SIS is hard for uniform $\mathbf{A}$, for discrete Gaussian $\mathbf{u}_i$ and for $k = O(1)$.
- This reduction was improved in [LPSS14] to cover $k = \mathcal{O}(m)$.
- No proof was provided for the module variant in [ACLMT22] but Sasha Laphia later proved it (unpublished).

Proof Idea

Let $\mathcal{R}_q := \mathbb{Z}_q$ be a field. Given the challenge $\mathbf{B} \in \mathcal{R}_q^{n \times (m-k)}$

1. Sample a small Gaussian full rank matrix $\mathbf{E} \in \mathbb{Z}^{m \times k}$ and write

$$\mathbf{E} = \begin{pmatrix} \mathbf{F} \\ \mathbf{H} \end{pmatrix} \text{ with } \mathbf{H} \in \mathcal{R}^{k \times k} \text{ and invertible over } \mathcal{K}.$$

2. Set $\mathbf{U} := -\mathbf{B} \cdot \mathbf{F} \cdot \mathbf{H}^{-1}$ and $\mathbf{A} := [\mathbf{B}|\mathbf{U}]$.
   - We have $\mathbf{A} \cdot \mathbf{E} = \mathbf{0}$ since $\mathbf{B} \cdot \mathbf{F} - \mathbf{B} \cdot \mathbf{F} \cdot \mathbf{H}^{-1} \cdot \mathbf{H} \equiv \mathbf{0}$.
   - We also have that $\mathbf{A}$ is close to uniform since $\mathbf{B} \cdot \mathbf{F}$ is close to uniform and $\mathbf{H}$ is invertible.
3. When the adversary outputs $\mathbf{u}^{\star} = (\mathbf{f}, \mathbf{g})$, we have
   - $\mathbf{0} \equiv \mathbf{B} \cdot \mathbf{f} - \mathbf{B} \cdot \mathbf{F} \cdot \mathbf{H}^{-1} \cdot \mathbf{g}$
   - $\mathbf{0} = \det(\mathbf{H}) \cdot \mathbf{B} \cdot \mathbf{f} - \det(\mathbf{H}) \cdot \mathbf{B} \cdot \mathbf{F} \cdot \mathbf{H}^{-1} \cdot \mathbf{g}$ over $\mathbb{Z}$.
   - $\mathbf{0} = \mathbf{B} \cdot \left(\det(\mathbf{H}) \cdot \mathbf{f} - \det(\mathbf{H}) \cdot \mathbf{F} \cdot \mathbf{H}^{-1} \cdot \mathbf{g}\right)$

From $O(1)$ to $O(m)$

- $\det(\mathbf{H})$ grows quickly with k
- [LPSS14] essentially samples small $\mathbf{H}$ with small inverse, but non-trivial to make the result look Gaussian.

What can it do?

- linearly homomorphic signatures
- removing the random oracle from GPV signatures at the price of restricting to k signatures
- traitor-tracing (by extension to k-LWE[2])
- ...

[2] It is exactly what you think it is

Perspective

Leakage Resilience

Alice has $\mathbf{A}, \mathbf{T}$ s.t. $\mathbf{T} \in \mathcal{R}^{m \times m}$ is short and $\mathbf{A} \cdot \mathbf{T} \equiv \mathbf{0} \bmod q$, i.e. $\mathbf{T}$ is trapdoor. Even given, say, $1/2$ of $\mathbf{T}$ it is hard to recover a full trapdoor.

The Crisis of Knowledge Assumptions

K-R-ISIS

Definition (K-M-ISIS Admissible)

Let $g(\mathbf{X}) = \mathbf{X}^{\mathbf{e}} := \prod_{i \in \mathbb{Z}_w} X_i^{e_i}$ for some exponent vector $\mathbf{e} \in \mathbb{Z}^w$. Let $\mathcal{G} \subset \mathcal{R}(\mathbf{X})$ be a set of such monomials with $k := |\mathcal{G}|$. We call a family $\mathcal{G}$ **k-M-ISIS-admissible** if (1) all $g \in \mathcal{G}$ have constant degree, (2) all $g \in \mathcal{G}$ are distinct and $0 \notin \mathcal{G}$.

Definition (K-M-ISIS Assumption)

Let $\mathbf{t} = (1, 0, \ldots, 0)$. Let $\mathcal{G}$ be k-M-ISIS-admissible. Let $\mathbf{A} \leftarrow_\$ \mathcal{R}_q^{n \times m}$, $\mathbf{v} \leftarrow_\$ (\mathcal{R}_q^\star)^w$. Given $(\mathbf{A}, \mathbf{v}, \mathbf{t}, \{\mathbf{u}_g\})$ with $\mathbf{u}_g$ short and $g(\mathbf{v}) \cdot \mathbf{t} \equiv \mathbf{A} \cdot \mathbf{u}_g \bmod q$ it is hard to find a short $\mathbf{u}^\star$ and small $s^\star$ s.t. $s^\star \cdot \mathbf{t} \equiv \mathbf{A} \cdot \mathbf{u}^\star \bmod q$.

When $n = 1$, we call the problem **K-R-ISIS**.

Martin R. Albrecht, Valerio Cini, Russell W. F. Lai, Giulio Malavolta and Sri Aravinda Krishnan Thyagarajan. Lattice-Based SNARKs: Publicly Verifiable, Preprocessing, and Recursively Composable - (Extended Abstract). In: *CRYPTO 2022, Part II*. ed. by Yevgeniy Dodis and Thomas Shrimpton. Vol. 13508. LNCS. Springer, Heidelberg, Aug. 2022, pp. 102–132. DOI: `10.1007/978-3-031-15979-4_4`

K-R-ISIS Hardness

Some reductions (none cover the interesting cases):

- K-R-ISIS is as hard as R-SIS when $m > k$ or when the system generated by $\mathcal{G}$ is efficiently invertible.
- k-M-ISIS is at least as hard as K-R-ISIS and that K-M-ISIS is a true generalisation of K-R-SIS.
- Scaling $(\mathcal{G}, g^*)$ multiplicatively by any non-zero g does not change the hardness, e.g. we may choose to normalise instances to $g^* \equiv 1$.
- $(\mathcal{G}, 1)$ is as hard as $(\mathcal{G}, 0)$ for any $\mathcal{G}$: non-homogeneous variant is no easier than the homogeneous variant.

Direct cryptanalysis:

- a direct SIS attack on $\mathbf{A}$.
- finding short $\mathbb{Z}$-linear combinations of $\mathbf{u}_i$
- finding $\mathbb{Q}$-linear combinations of $\mathbf{u}_i$ that produce short images.

… all seem hard.

Knowledge K-R-ISIS

The assumption states that for any element $c \cdot \mathbf{t}$ that the adversary can produce together with a short preimage, it produced that as some small linear combination of the preimages $\{\mathbf{u}_g\}$ we have given it. Thus, roughly:

Definition (Knowledge K-R-ISIS)

If an adversary outputs any $c, \mathbf{u}_c$ s.t.

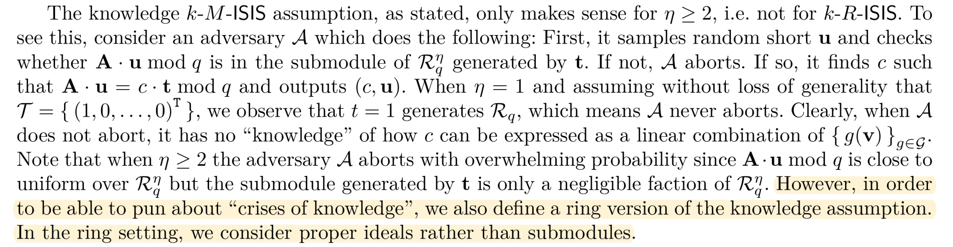
$$c \cdot \mathbf{t} \equiv \mathbf{A} \cdot \mathbf{u}_c \bmod q$$

There is an extractor that – given the adversary's randomness – outputs short $\{c_g\}$ s.t.

$$c \equiv \sum_{g \in \mathcal{G}} c_g \cdot g(\mathbf{v}) \bmod q.$$

Think $\mathbf{t} = (1, 0)$ and the second component serves as a ”check equation”: The assumption only makes sense for $n > 1$.

Knowledge K-R-ISIS: The Audacity



The knowledge k-M-ISIS assumption, as stated, only makes sense for $\eta \geq 2$, i.e. not for k-R-ISIS. To see this, consider an adversary $\mathcal{A}$ which does the following: First, it samples random short $\mathbf{u}$ and checks whether $\mathbf{A} \cdot \mathbf{u} \bmod q$ is in the submodule of $\mathcal{R}_q^\eta$ generated by $\mathbf{t}$. If not, $\mathcal{A}$ aborts. If so, it finds c such that $\mathbf{A} \cdot \mathbf{u} = c \cdot \mathbf{t} \bmod q$ and outputs $(c, \mathbf{u})$. When $\eta = 1$ and assuming without loss of generality that $\mathcal{T} = \{\, (1, 0, \ldots, 0)^\mathtt{T} \,\}$, we observe that $t = 1$ generates $\mathcal{R}_q$, which means $\mathcal{A}$ never aborts. Clearly, when $\mathcal{A}$ does not abort, it has no "knowledge" of how c can be expressed as a linear combination of $\{\, g(\mathbf{v}) \,\}_{g \in \mathcal{G}}$. Note that when $\eta \geq 2$ the adversary $\mathcal{A}$ aborts with overwhelming probability since $\mathbf{A} \cdot \mathbf{u} \bmod q$ is close to uniform over $\mathcal{R}_q^\eta$ but the submodule generated by $\mathbf{t}$ is only a negligible faction of $\mathcal{R}_q^\eta$. However, in order to be able to pun about "crises of knowledge", we also define a ring version of the knowledge assumption. In the ring setting, we consider proper ideals rather than submodules.

Knowledge K-R-ISIS: Almost Instant Karma

The Knowledge K-M-ISIS assumptions is ”morally”[3] false.

$$\begin{pmatrix}\mathbf{C}\\ \mathbf{0}\end{pmatrix} \equiv \begin{pmatrix}\mathbf{A}_0\\ \mathbf{A}_1\end{pmatrix} \cdot \mathbf{U} \bmod q.$$

- $\mathbf{U}$ is a trapdoor for $\mathbf{A}_1$
- Use it to find a short preimage of some $(\mathbf{c}^\star, \mathbf{0})$ using, say, Babai rounding.
- It will change $\mathbf{c}^\star$ but we’re allowed to output anything in the first component.

Hoeteck Wee and David J. Wu. Lattice-Based Functional Commitments: Fast Verification and Cryptanalysis. In: *ASIACRYPT 2023, Part V*. ed. by Jian Guo and Ron Steinfeld. Vol. 14442. LNCS. Springer, Heidelberg, Dec. 2023, pp. 201–235. DOI: `10.1007/978-981-99-8733-7_7`

[3] The assumption is technically unfalsifiable but for all intents and purposes it is wrong by inspection of the attack.

Known knowledge assumptions are easy quantumly

> *Our main result is a quantum polynomial-time algorithm that samples well-distributed LWE instances while provably not knowing the solution, under the assumption that LWE is hard. Moreover, the approach works for a vast range of LWE parametrizations, including those used in the above-mentioned SNARKs.*

Thomas Debris-Alazard, Pouria Fallahpour and Damien Stehlé. Quantum Oblivious LWE Sampling and Insecurity of Standard Model Lattice-Based SNARKs. Cryptology ePrint Archive, Paper 2024/030. 2024. URL: `https://eprint.iacr.org/2024/030`

BASIS

BASIS (Random)

We consider $k = 2$, for simplicity.

Definition ($\mathsf{BASIS}_{\text{rand}}$)

Let $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$. We're given

$$\mathbf{B} := \begin{pmatrix} \mathbf{A}_0 & \mathbf{0} & -\mathbf{G} \\ \mathbf{0} & \mathbf{A}_1 & -\mathbf{G} \end{pmatrix}$$

and a short $\mathbf{T}$ s.t. $\mathbf{G} \equiv \mathbf{B} \cdot \mathbf{T} \bmod q$ where $\mathbf{A}_i$ are uniformly random for $i > 0$ and $\mathbf{A}_0 := [\mathbf{a} | \mathbf{A}^T]^T$ for uniformly random $\mathbf{A}$ and $\mathbf{a}$.

Given $(\mathbf{B}, \mathbf{T})$ it is hard to find a short $\mathbf{u}^\star$ s.t. $\mathbf{A} \cdot \mathbf{u}^\star \equiv \mathbf{0} \bmod q$.

Hoeteck Wee and David J. Wu. Succinct Vector, Polynomial, and Functional Commitments from Lattices. In: *EUROCRYPT 2023, Part III*. ed. by Carmit Hazay and Martijn Stam. Vol. 14006. LNCS. Springer, Heidelberg, Apr. 2023, pp. 385–416. DOI: 10.1007/978-3-031-30620-4_13

Hardness

$\mathrm{BASIS}_{\mathrm{rand}}$ is as hard as SIS.

- We can construct $\mathbf{B}$ given $\mathbf{A}$ since we can trapdoor all $\mathbf{A}_i$ for $i > 0$.
- For each column $\mathbf{t} = (\mathbf{t}^{(0)}, \mathbf{t}^{(1)}, \mathbf{t}^{(G)})$ of $\mathbf{T}$ we have $\mathbf{A}_i \cdot \mathbf{t}^{(i)} \equiv \mathbf{G} \cdot \mathbf{t}^{(G)}$ where $\mathbf{G} \cdot \mathbf{t}^{(G)}$ is close to uniform.
- We can sample $\mathbf{t}^{(0)}$, compute $\mathbf{y} := \mathbf{A}_0 \cdot \mathbf{t}^{(0)}$ and then use the gadget structure of $\mathbf{G}$ to find a short $\mathbf{t}^{(G)}$ s.t. $\mathbf{A}_i \cdot \mathbf{t}^{(i)} \equiv \mathbf{G} \cdot \mathbf{t}^{(G)}$.
- Using the trapdoors for $\mathbf{A}_i$ with $i > 0$ we can find $\mathbf{t}^{(i)}$ s.t. $\mathbf{A}_i \cdot \mathbf{t}^{(i)} \equiv \mathbf{G} \cdot \mathbf{t}^{(G)}$.

BASIS (STRUCTURED)

We consider $k = 2$, for simplicity.

Definition (BASIS$_{\text{struct}}$)

Let $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$. We're given

$$\mathbf{B} := \begin{pmatrix} \mathbf{A}_0 & \mathbf{0} & -\mathbf{G} \\ \mathbf{0} & \mathbf{A}_1 & -\mathbf{G} \end{pmatrix}$$

and a short $\mathbf{T}$ s.t. $\mathbf{G}_{\eta'} \equiv \mathbf{B} \cdot \mathbf{T} \bmod q$ where $\mathbf{A}_i := \mathbf{W}_i \cdot \mathbf{A}$ for known $\mathbf{W}_i \in \mathbb{Z}_q^{n \times n}$.

Given $(\mathbf{B}, \mathbf{T})$ it is hard to find a short $\mathbf{u}^\star$ s.t. $\mathbf{A} \cdot \mathbf{u}^\star \equiv \mathbf{0} \bmod q$.

Hoeteck Wee and David J. Wu. Succinct Vector, Polynomial, and Functional Commitments from Lattices. In: *EUROCRYPT 2023, Part III*. ed. by Carmit Hazay and Martijn Stam. Vol. 14006. LNCS. Springer, Heidelberg, Apr. 2023, pp. 385–416. DOI: `10.1007/978-3-031-30620-4_13`

Hardness

Given an algorithm for solving $\mathsf{BASIS}_{\mathsf{struct}}$ there is an algorithm for solving k-M-ISIS.

PRISIS

Definition (PRISIS)

Let $\mathbf{A} \in \mathcal{R}_q^{n \times m}$. We're given

$$\mathbf{B} := \begin{pmatrix} \mathbf{A} & \mathbf{0} & \cdots & -\mathbf{G} \\ \mathbf{0} & w \cdot \mathbf{A} & \cdots & -\mathbf{G} \\ \mathbf{0} & \mathbf{0} & \ddots & -\mathbf{G} \\ \mathbf{0} & \cdots & w^{k-1} \cdot \mathbf{A} & -\mathbf{G} \end{pmatrix}$$

and a short $\mathbf{T}$ s.t. $\mathbf{G} \equiv \mathbf{B} \cdot \mathbf{T} \bmod q$.

Given $(\mathbf{A}, \mathbf{B}, w, \mathbf{T})$ it is hard to find a short $\mathbf{u}^\star$ s.t. $\mathbf{A} \cdot \mathbf{u}^\star \equiv \mathbf{0}$.

Giacomo Fenzi, Hossein Moghaddas and Ngoc Khanh Nguyen. Lattice-Based Polynomial Commitments: Towards Asymptotic and Concrete Efficiency. Cryptology ePrint Archive, Paper 2023/846. `https://eprint.iacr.org/2023/846`. 2023. URL: `https://eprint.iacr.org/2023/846`

Hardness

PRISIS's additional structure allows to prove a broader regime of parameters as hard as M-SIS

If $k = 2$ then PRISIS is no easier than M-SIS

$$\mathbf{B} := \begin{pmatrix} \mathbf{A} & \mathbf{0} & \cdots & -\mathbf{G} \\ \mathbf{0} & w \cdot \mathbf{A} & \cdots & -\mathbf{G} \end{pmatrix}$$

The Trick

- Plant an NTRU instance in w, and use its trapdoor to construct the global trapdoor $\mathbf{T}$
- Can pick parameters for NTRU that are statistically secure

h-PRISIS

h-PRISIS [AFLN23] is a multi-instance version of PRISIS.

Definition (h-PRISIS)

Let $\mathbf{A}_i \in \mathcal{R}_q^{n\times m}$ for $i \in \{0, , h-1\}$. We're given

$$\mathbf{B}_i := \begin{pmatrix} \mathbf{A}_i & \mathbf{0} & \cdots & -\mathbf{G} \\ \mathbf{0} & w_i \cdot \mathbf{A}_i & \cdots & -\mathbf{G} \\ \mathbf{0} & \mathbf{0} & \ddots & -\mathbf{G} \\ \mathbf{0} & \cdots & w_i^{\ell-1} \cdot \mathbf{A}_i & -\mathbf{G} \end{pmatrix}$$

and a short $\mathbf{T}_i$ s.t. $\mathbf{G} \equiv \mathbf{B}_i \cdot \mathbf{T}_i \bmod q$.

Given $(\{\mathbf{A}_i\}, \{\mathbf{B}_i\}, \{w_i\}, \{\mathbf{T}\}_i)$ it is hard to find a short $\mathbf{u}_i^\star$ s.t. $\sum \mathbf{A}_i \cdot \mathbf{u}_i^\star \equiv \mathbf{0} \bmod q$.

Hardness

h-PRISIS is no easier than PRISIS [AFLN23]. In particular, if $\ell = 2$ then h-PRISIS is no easier than M-SIS [AFLN23].

The Trick

- Let $\mathbf{U}, \mathbf{V}$ be short and satisfy $\mathbf{U} \cdot \mathbf{V} \equiv \mathbf{I}$.
- We can re-randomise $\mathbf{A}_0$ to $\mathbf{A}_i$ as $\mathbf{A}_i := \mathbf{A}_0 \cdot \mathbf{U}$ and $\mathbf{T}$ as $\mathbf{T}_i := \mathbf{V} \cdot \mathbf{T}$
- We have $\mathbf{A}_i \cdot \mathbf{T}_i \equiv \mathbf{A}_0 \cdot \mathbf{U} \cdot \mathbf{V} \cdot \mathbf{T} \equiv \mathbf{A} \cdot \mathbf{T}$.
- $\mathbf{U} := \begin{pmatrix} \mathbf{I} & \mathbf{R}_1 \\ 0 & \mathbf{I} \end{pmatrix} \cdot \begin{pmatrix} \mathbf{I} & 0 \\ \mathbf{R}_2 & \mathbf{I} \end{pmatrix}$ and $\mathbf{V} := \begin{pmatrix} \mathbf{I} & 0 \\ -\mathbf{R}_2 & \mathbf{I} \end{pmatrix} \cdot \begin{pmatrix} \mathbf{I} & -\mathbf{R}_1 \\ 0 & \mathbf{I} \end{pmatrix}$ where $\mathbf{R}_i$ are small.

What can it do?

Polynomial commitment schemes, see Khanh’s talk.

One-more-ISIS

One-more-ISIS

Definition (One-more-ISIS)

Let $\mathbf{A} \leftarrow\$ \mathbb{Z}_q^{n\times m}$.

Syndrome queries: can request a random challenge vector $\mathbf{t} \leftarrow\$ \mathbb{Z}_q^n$ which is added to some set $\mathcal{S}$.

Preimage queries: can submit **any** vector $\mathbf{t}' \in \mathbb{Z}_q^n$ will get a short vector $\mathbf{u}' \leftarrow\$ D_{\mathbb{Z}^m,\sigma}$ such that $\mathbf{A}\cdot\mathbf{u}' \equiv \mathbf{t}' \bmod q$. Denote k for the number of preimage queries.

The adversary is asked to output $k+1$ pairs $\{(\mathbf{u}_i^\star, \mathbf{t}_i)\}_{1\leq i\leq k+1}$ satisfying:

$$\mathbf{A}\cdot\mathbf{u}_i^\star \equiv \mathbf{t}_i \bmod q, \|\mathbf{u}_i^\star\| \leq \beta^\star \text{ and } \mathbf{t}_i \in \mathcal{S}.$$

Shweta Agrawal, Elena Kirshanova, Damien Stehlé and Anshu Yadav. Practical, Round-Optimal Lattice-Based Blind Signatures. In: *ACM CCS 2022*. Ed. by Heng Yin, Angelos Stavrou, Cas Cremers and Elaine Shi. ACM Press, Nov. 2022, pp. 39–53. DOI: `10.1145/3548606.3560650`

Hardness

The hardness of the problem is analysed using direct cryptanalysis in the original paper. The authors give a combinatorial attack and a lattice attack.

The Trick

The key ingredient is that β^* is only marginally bigger than $\sqrt{m} \cdot \sigma$.

Hardness: Lattice Attack

- The adversary requests $\geq \ell$ preimages of zero and uses that to produce a short basis T for the kernel of A, i.e.

$$\mathsf{A} \cdot \mathsf{T} \equiv \mathbf{0} \bmod q.$$

- This constitutes a trapdoor for A and thus permits to return short preimages for any target.
- However, this trapdoor is of degraded quality relative to the trapdoor used by the challenger.

Challenge

The key computational challenge then is to fix-up or improve this degraded trapdoor in order to be able to sample sufficiently short vectors.

What can it do?

Blind signatures.[4]

[4] But see Ward Beullens, Vadim Lyubashevsky, Ngoc Khanh Nguyen and Gregor Seiler. Lattice-Based Blind Signatures: Short, Efficient, and Round-Optimal. Cryptology ePrint Archive, Report 2023/077. https://eprint.iacr.org/2023/077. 2023.

Hinted Lattice Problems as Hard as Finding Short Vectors in PSPACE ∩ E

Hinted Lattice Problems as Hard as Finding Short Vectors in PSPACE $\cap$ E

joint work with Russell W. F. Lai[5] and Eamonn W. Postlethwaite

[5] some slides nicked from Russell.

GPV

Public Key Matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$.

Secret Key Short basis of $\Lambda_q^{\perp}(\mathbf{A})$ of norm α.

Signature of μ Short vector $\mathbf{u}$ satisfying

$$\mathbf{A} \cdot \mathbf{u} \equiv \mathrm{H}(\mu) \bmod q \quad \text{and} \quad \|\mathbf{u}\| \leq \beta$$

where $\mathrm{H} : \{0,1\}^{\star} \rightarrow \mathbb{Z}_q^n$ is hash function modelled as random oracle,
$\beta \approx \sqrt{m} \cdot \alpha$.

Security Proof ≈ argument against signing the same μ twice:

- Signing same μ twice $\implies$

$$\mathbf{A} \cdot \mathbf{u}_0 \equiv \mathbf{A} \cdot \mathbf{u}_1 = \mathrm{H}(\mu) \bmod q,$$
$$\mathbf{A} \cdot (\mathbf{u}_0 - \mathbf{u}_1) = \mathbf{0} \bmod q,$$

  i.e. giving away short vector $\mathbf{x}_0 - \mathbf{x}_1 \in \Lambda_q^{\perp}(\mathbf{A})$.
- Do this for many $\mu \implies$ adversary gets short(-ish) basis of $\Lambda_q^{\perp}(\mathbf{A})$ of norm $\approx \sqrt{m} \cdot \alpha$.

Does this (really) help adversary forge signatures?

One-more-ISIS assumption suggest ”no”!

The k-hint Inhomogeneous Short Integer Solution Problem:

Definition (k-H-ISIS)

Let k, n, m, q, β, HintGen, where

$$\forall\, \mathbf{A} \in \mathbb{Z}_q^{n\times m},\ \mathsf{HintGen}(\mathbf{A}) \subseteq_k \Lambda_q^{\perp}(\mathbf{A}) \quad \text{and} \quad \beta \leq r \cdot \|\mathsf{HintGen}(\mathbf{A})\|$$

for some ratio $r \leq \mathrm{polylog}(m)$. (We mostly care about $r \leq O(1)$ or at least $r \leq O(\log m)$.)

Given $(\mathbf{A}, \mathbf{y}, \mathbf{U})$ where

$$\mathbf{A} \leftarrow\!\!\$\ \mathbb{Z}_q^{n\times m}, \quad \mathbf{y} \leftarrow\!\!\$\ \mathbb{Z}_q^{n}, \quad \mathbf{U} \leftarrow \mathsf{HintGen}(\mathbf{A}).$$

find $\mathbf{u}^\star \in \mathbb{Z}^m$ such that

$$\mathbf{A} \cdot \mathbf{u}^\star \equiv \mathbf{y} \bmod q \quad \text{and} \quad \|\mathbf{u}^\star\| \leq \beta.$$

The k-hint (Homogeneous) Short Integer Solution (k-H-SIS) problem: Same thing but $\mathbf{y} = \mathbf{0}$.

Successive Minima and SIVP

- Successive minima $\lambda_i(\Lambda) =$ radius of smallest ball containing i linearly independent lattice vectors.
- SIVP$_\gamma$: Given lattice $\Lambda \subseteq \mathbb{R}^m$, find m linearly independent lattice vectors of norm at most $\gamma \cdot \lambda_m(\Lambda)$.
- We will discuss asymptotic complexities in terms of m.

Enumeration and Sieving

Two types of lattice algorithms for $\gamma \leq \mathrm{poly}(m)$:

Enumeration-type

- Enumerate over all non-zero vectors in Λ of norm at most β.
- Output the shortest vector.

Sieving-type

- Start with a long list of vectors in Λ.
- Search for an integer combination of vectors in the list which gives a shorter vector.
- Add resulting vector to the list.
- Repeat.

Landscape

Space-time complexity of SIVP_γ over $\Lambda_q^\perp(\mathbf{A})$:

Algorithms	Time	Memory	Assumptions
Enumeration	$m^{\Omega(m)}$	$\mathrm{poly}(m)$	-
Sieving	$2^{\Omega(m)}$	$2^{\Omega(m)}$	-
Sieving (this work)	$2^{\Omega(m)}$	$\mathrm{poly}(m)$	1) sub. exp. OWF and 2) k-H-SIS is easy

Our Interpretation

Hinted lattice problems seem hard.

Step 1: Entropic Reduction from k-H-SIS to k-H-ISIS

We show that the classic SIS to ISIS reduction gives the following:

k-H-SIS → k-H-ISIS

Let $\mathcal{A}$ be PPT adversary against k-H-ISIS, then there exists a PPT adversary $\mathcal{B}$ against k-H-SIS. The output of $\mathcal{B}$ follows a Gaussian distribution (with some centre) with high min-entropy.

$\mathcal{B}$'s outputs are drawn from the following distribution:

- Choose a centre $\mathbf{c}$ from some distribution (somehow chosen by $\mathcal{A}$).
- Output a sample from $\mathcal{D}_{\Lambda_q^\perp(\mathsf{A}),s,\mathbf{c}}$, where the Gaussian parameter s satisfies

$$s \geq \sqrt{m} \cdot \lambda_m(\Lambda_q^\perp(\mathsf{A})) \geq \eta_\epsilon(\Lambda_q^\perp(\mathsf{A}))$$

  with high probability.

Step 2: Gaussian Vectors Generate the Lattice

We prove the following lattice generation theorem:

Gaussian vectors generate the lattice

Let $\Lambda \subseteq \mathbb{R}^m$ be any lattice and suppose $s \geq \sqrt{m} \cdot \lambda_m(\Lambda)$.
Let $\mathbf{x}_i \leftarrow\$ \mathcal{D}_{\Lambda,s,\mathbf{c}_i}$ for $i = 1, 2, \ldots, t$ with arbitrary and potentially distinct centres $\mathbf{c}_i$.
There exists $t^* = O(m \cdot \log(s\sqrt{m}))$ s.t. if $t \geq t^*$, then $\{\mathbf{x}_i\}_{i \in \{1 \ldots t\}}$ generates Λ with probability at least $1 - 2^{-\Omega(m)}$.

This was known only for $\mathbf{c}_i := \mathbf{0}, \forall\, i$.[6]

[6] Ishay Haviv and Oded Regev. On the Lattice Isomorphism Problem. In: *25th SODA*. ed. by Chandra Chekuri. ACM-SIAM, Jan. 2014, pp. 391–404. DOI: 10.1137/1.9781611973402.29.

Step 3: Improved Analysis of Sieves

We prove the following sieving theorem:

Number of points in a ball

Let $S = \{\mathbf{x}_1, \ldots, \mathbf{x}_t\} \subseteq \mathbb{R}^m$ be any set of t distinct vectors of norm $\|\mathbf{x}_i\| \leq \beta$.
Let $1 < r = o(\log m)$ be some improvement ratio.
There exists $t^* \leq 2^{O(m \log r)}$ s.t., if $t \geq t^*$, then there exist i, j s.t. $0 < \left\|\mathbf{x}_i - \mathbf{x}_j\right\| \leq \beta / r$.

Previous sieve analyses were

- heuristic (assuming vectors are uniformly distributed on the surface of a sphere) and
- only for $r = O(1)$.

Step 4: Finding One Mildly Short Vector

Suppose there exists a PPT entropic k-H-SIS solver $\mathcal{B}$ with ratio $r > 1$.

We construct a $(2^{O(m)}, \mathrm{poly}(m))$ time/memory k-H-SIS solver $\mathcal{B}'$ with constant ratio $r' < 1$.

Basic Idea

Run entropic kHSIS solver $\mathcal{B}$ many times to get $2^{\Omega(m)}$ vectors, then apply sieving theorem.

Step 4: Finding One Mildly Short Vector (More Details)

1. Success probability amplification: Repeat $\mathcal{B}$ to make success probability overwhelming.
2. Randomised memory-inefficient sieve:
    - Fill random tape of (amplified) $\mathcal{B}$ with $t \geq 2^{\Omega(m)}$ independent randomness $\chi_1, \ldots, \chi_t$.
    - For each $i, j \in [t]$:
        - Compute $\mathbf{x}_i \leftarrow \mathcal{B}(\mathbf{A}, \mathbf{U}; \chi_i)$.
        - Compute $\mathbf{x}_j \leftarrow \mathcal{B}(\mathbf{A}, \mathbf{U}; \chi_j)$.
        - Output $\mathbf{x}_i - \mathbf{x}_j$ if $0 < \left\|\mathbf{x}_i - \mathbf{x}_j\right\| \leq \|\mathbf{U}\| / r'$.
        - Entropic-ness of $\mathcal{B}$ + sieving theorem $\implies$ Successful output with overwhelming probability.
3. Derandomisation: derandomise the double-loop with sub-exp. secure PRF.

Step 5: Finding Lots of Mildly Short Vectors

Suppose further that the entropic kHSIS solver $\mathcal{B}$ has Gaussian outputs.

We construct a $(2^{O(m)}, \mathrm{poly}(m))$ sieving routine $\mathcal{C}$:

Input $(\mathbf{A}, \mathbf{U})$ where $\mathbf{U}$ generates $\Lambda_q^\perp(\mathbf{A})$.

Output $\mathbf{U}' \subset \Lambda_q^\perp(\mathbf{A})$ generating $\Lambda_q^\perp(\mathbf{A})$ with $\|\mathbf{U}'\| \leq \|\mathbf{U}\| / r'$.

Basic Idea

Run $\mathcal{B}'$ many times to get $\Omega(m \cdot \log(s\sqrt{m}))$ vectors, then apply lattice generation theorem.

Step 6: Iterated Sieving

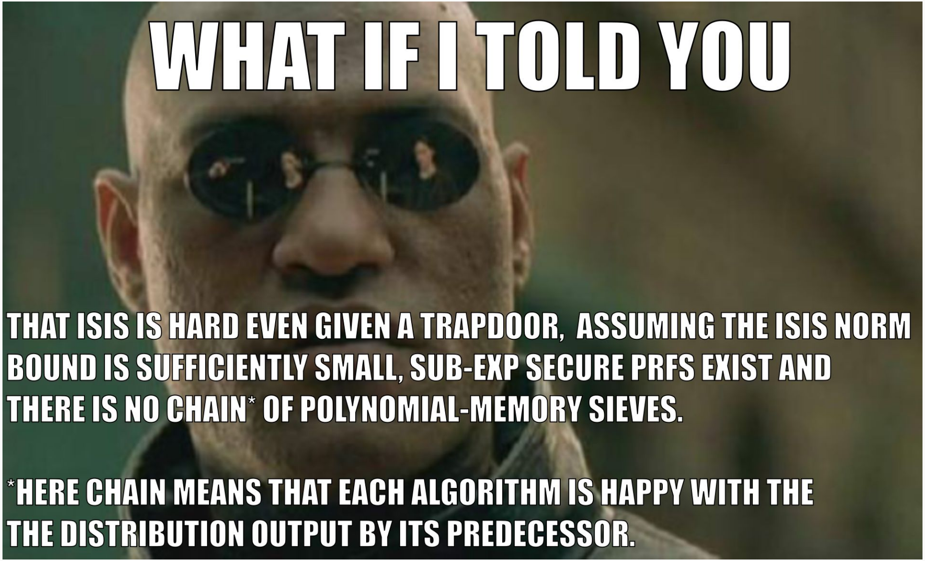
Assume the existence of a chain of entropic k-H-SIS solvers $\mathcal{B}_1, \mathcal{B}_2, \dots$ with Gaussian outputs with arbitrary (small) centres, accepting Gaussian inputs with arbitrary (small) centres.

We construct a $(2^{O(m)}, \mathrm{poly}(m))$-memory algorithm which solves SIVP_γ for $\Lambda_q^\perp(\mathsf{A})$ with $\gamma \geq m$.

Basic Idea

Feed output of sieving subroutine to itself until improvement stops.

I lied!



WHAT IF I TOLD YOU

THAT ISIS IS HARD EVEN GIVEN A TRAPDOOR, ASSUMING THE ISIS NORM BOUND IS SUFFICIENTLY SMALL, SUB-EXP SECURE PRFS EXIST AND THERE IS NO CHAIN* OF POLYNOMIAL-MEMORY SIEVES.

*HERE CHAIN MEANS THAT EACH ALGORITHM IS HAPPY WITH THE THE DISTRIBUTION OUTPUT BY ITS PREDECESSOR.

Fin

Designers Please consider whether you can re-use one of those many newfangled assumptions before introducing yet another one.

Cryptanalysts Analyse them!