One-more (I)SIS

Elena Kirshanova

at workshop Novel Lattice Assumptions

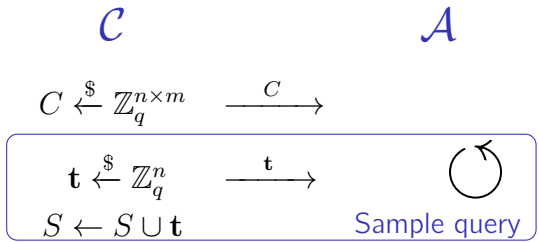
International Centre for Mathematical Sciences
Edinburgh

One-more ISIS$_\beta$: Definition

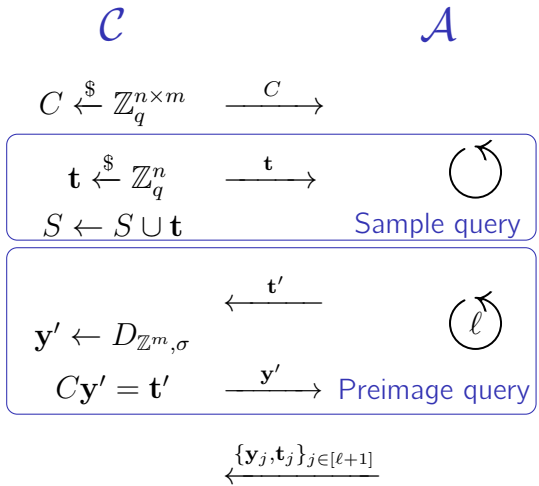
$\mathcal{C}$ $\qquad\qquad$ $\mathcal{A}$

$C \xleftarrow{\$} \mathbb{Z}_q^{n\times m} \qquad \xrightarrow{\qquad C \qquad}$

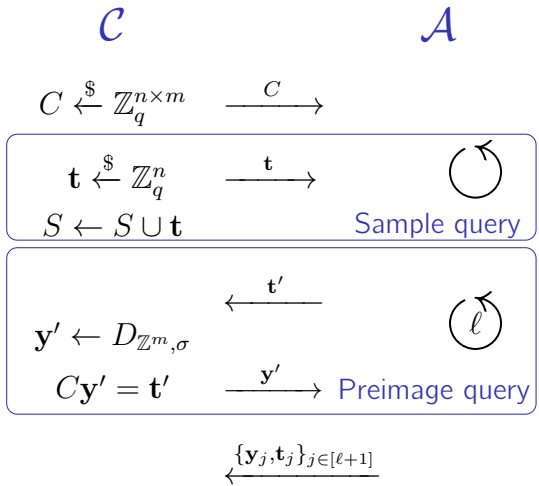
One-more ISIS$_\beta$: Definition



One-more ISIS$_\beta$: Definition



One-more ISIS$_\beta$: Definition



$\mathcal{A}$ wins, if

- $C\mathbf{y}_i = \mathbf{t}_i, \mathbf{t}_i \in S\ \forall i$,
- $\|\mathbf{y}_i\| \leq \beta$.

Why useful?

- Security foundation in a blind signature construction from [AKSY22]. Solving one-more ISIS $\implies$ signature forgery
- randomized OM-ISIS (rOM-ISIS) gives a non-interactive blind signature [BSGY24]
- However, we do have a construction of blind signature on standard lattice assumptions [BLNS23]

One-more ISIS hardness

- If you can solve Standard SIS, you can solve OM-SIS
- Not comparable with k-SIS:[1] one-more SIS does not have restriction on subspace, but more strict on the norm of the solution
- If $\sigma = \mathcal{O}(1) \implies$ One-more ISIS is easy: after $\Theta(m)$ preimage queries, the adversary already has a very good basis of $\Lambda^{\perp}(C)$. Known efficient algorithms produce $\sigma = \widetilde{\Theta}(\sqrt{m})$

[1] In k-SIS, given A and Gaussian $\mathbf{y}_i$ s.t. $A\mathbf{y}_i = 0 \bmod q$, find a short $\mathbf{y}$ s.t. $A\mathbf{y} = 0$ and $\mathbf{y} \notin \mathrm{Span}_{\mathbb{Q}}\{\mathbf{y}_i\}_i$

Attacks: Lattice reduction

1. From C or from $\mathrm{poly}(m)$ Preimage queries, build a basis B for
$$L^{\perp}(C) = \{\mathbf{y} \in \mathbb{Z}^m \ : \ C\mathbf{y} = 0 \bmod q\}$$
2. Run BKZ reduction on B with block-size b, obtain $B^{\mathtt{red}}$
3. For a challenge $\mathbf{t}$, run Babai Nearest Plane using $B^{\mathtt{red}}$

$$\text{Time} = 2^{\mathcal{O}(b)} \qquad \text{Quality} = \Theta\left(b^{\mathcal{O}(m/b)}\sqrt{mn\log q}\right)$$

By Quality I mean the Euclidean norm of the returned preimage.

Attacks: Combinatorics

Consider a set

$$A = \{\mathbf{e}_i a,\ i \in [n],\ a \in \mathbb{Z}_q\} \quad \mathbf{e}_i = (0, \ldots, 1, \ldots, 0) \qquad |A| = (q-1) \cdot n$$

Any vector $\mathbf{t} \in \mathbb{Z}_q^n$ is a sum of n vectors from A.

1. Run preimage query for all elements from A, obtain $\mathbf{y}$ s.t. $\|\mathbf{y}\| \leq \Theta(\sqrt{m}\sigma)$ w.h.p.
2. Express the received challenge $\mathbf{t}$ as a sum of n vectors from A
3. The sum of the corresponding $\mathbf{y}$'s is a pre-image for $\mathbf{t}$ of expected norm $\|\mathbf{y}\| \leq \Theta(\sqrt{nm}\sigma)$

$$\text{Time} = (q-1) \cdot n \qquad \text{Quality} = \Theta(\sqrt{nm}\sigma)$$

Attacks: Combinatorics

In general, when Q-many queries are allowed, A consists of partial sums of $\mathbf{e}_i a$. This leads to

$$\text{Time} = Q \qquad \text{Quality} = \Theta\left(\sqrt{1 + \frac{n \log q}{\log(Q/n^2)}}\sqrt{m}\sigma\right)$$

Attacks: Combinatorics

In general, when Q-many queries are allowed, A consists of partial sums of $\mathbf{e}_i a$. This leads to

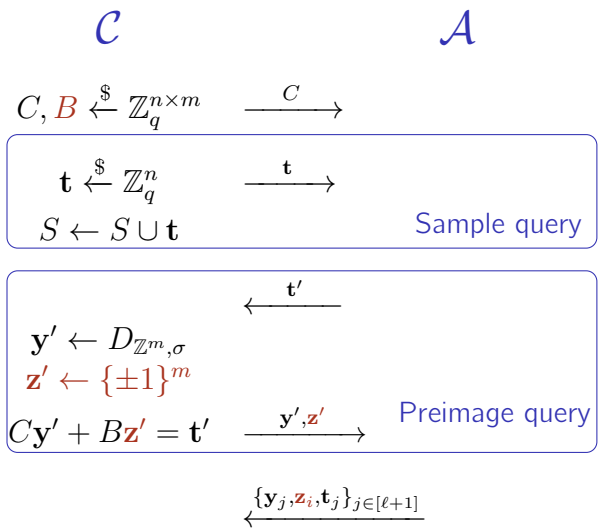
$$\text{Time} = Q \qquad \text{Quality} = \Theta\left(\sqrt{1 + \frac{n \log q}{\log(Q/n^2)}}\sqrt{m}\sigma\right)$$

cf. for lattices reduction:

$$\text{Time} = 2^{\mathcal{O}(b)} \qquad \text{Quality} = \Theta\left(b^{\mathcal{O}(m/b)}\sqrt{mn \log q}\right)$$

Randomised OM-ISIS$_\beta$, [BCGY24]

:



$\mathcal{A}$ wins, if

- $C\mathbf{y}_i + B\mathbf{z}_i = \mathbf{t}_i, \mathbf{t}_i \in S$
- $\|\mathbf{y}_i\| \leq \beta$.
- $\mathbf{z}_i \in \{\pm 1\}^m$.

Complexity statements about rOM-SIS$_\beta$

- Randomised OM-ISIS$_\beta$ is at least as hard as OM-ISIS$_{\beta+m^{3/2}}$, [NS26]
- The combinatorial attack on OM-ISIS does not transfer to Randomised OM-ISIS due to $\mathbf{z}' \in \{\pm 1\}^m$
- Lattice attack:
  1. From C, construct a basis B of $\Lambda^\perp(C)$
  2. BKZ-reduce B
  3. For a given target $\mathbf{t}$, sample $\mathbf{z} \leftarrow \{\pm 1\}^m$
  4. Run Babai Nearest Plane using BKZ-reduced B on target $\mathbf{t} - B\mathbf{z}$

Open questions

1. Better lattice reduction for one-more-SIS (we already have a pretty good basis)
2. Better Babai's Nearest Plane exploiting the knowledge of a short generating set (but not a shortest)
3. Reverse reduction: from Randomized OM-SIS$_\beta$ to OM-SIS$_{\beta'}$

References

[AKSY22] Shweta Agrawal, Elena Kirshanova, Damien Stehlé, and Anshu Yadav. Practical, Round-Optimal Lattice-Based Blind Signatures.

[BCGY24] Foteini Baldimtsi, Jiaqi Cheng, Rishab Goyal, and Aayush Yadav. Non-Interactive Blind Signatures: Post-Quantum and Stronger Security.

[BLNS23] Lattice-Based Blind Signatures: Short, Efficient, and Round-Optimal

[NS26] Ngoc Khanh Nguyen and Jan Niklas Siemer. Tight Reductions for SIS-with-Hints Assumptions with Applications to Anonymous Credentials.