

Hardness of Hinted ISIS from Space-Time Hardness of Lattice Problems

Martin R. Albrecht^{1,2} **Russell W. F. Lai³** Eamonn W. Postlethwaite¹

¹King's College London

²SandboxAQ

³Aalto University

Joint Estonian-Latvian Theory Days, 26.04.2026

Karlsruhe Institute of Technology, 14.04.2026

Helsinki CS Theory Seminar, 04.03.2026

<https://ia.cr/2026/187>

Why H-ISIS?

H-ISIS = Hinted Inhomogeneous Short Integer Solution

- † Direct application: EUF-CMA security of GPV signatures in ROM without derandomisation nor salting.
- † Broader context: Understand hinted lattice assumptions used for constructing exotic primitives.

This work

Typical crypto theorems

\nexists PPT algorithm for task A (e.g. solving discrete logarithm, finding short vectors in lattices)
 $\implies \nexists$ PPT algorithm for task B (e.g. breaking security of a scheme).

This work in a nutshell

\nexists $2^{O(n)}$ -time $\text{poly}(n)$ -space probabilistic algorithm for finding short vectors in lattices
 $\implies \nexists$ PPT algorithm for H-ISIS.

This work

Typical crypto theorems

\nexists PPT algorithm for task A (e.g. solving discrete logarithm, finding short vectors in lattices)
 $\implies \nexists$ PPT algorithm for task B (e.g. breaking security of a scheme).

This work in a nutshell

$\nexists 2^{O(n)}$ -time $\text{poly}(n)$ -space probabilistic algorithm for finding short vectors in lattices
 $\implies \nexists$ PPT algorithm for H-ISIS.

This work

Typical crypto theorems

\nexists PPT algorithm for task A (e.g. solving discrete logarithm, finding short vectors in lattices)
 $\implies \nexists$ PPT algorithm for task B (e.g. breaking security of a scheme).

This work in a nutshell

\nexists $2^{O(n)}$ -time $\text{poly}(n)$ -space probabilistic algorithm for finding short vectors in lattices
 $\implies \nexists$ PPT algorithm for H-ISIS.

This work

Typical crypto theorems

\nexists PPT algorithm for task A (e.g. solving discrete logarithm, finding short vectors in lattices)
 $\implies \nexists$ PPT algorithm for task B (e.g. breaking security of a scheme).

This work in a nutshell

\nexists $2^{O(n)}$ -time $\text{poly}(n)$ -space probabilistic algorithm for finding short vectors in lattices
 $\implies \nexists$ PPT algorithm for H-ISIS.

This work

Typical crypto theorems

\nexists PPT algorithm for task A (e.g. solving discrete logarithm, finding short vectors in lattices)
 $\implies \nexists$ PPT algorithm for task B (e.g. breaking security of a scheme).

This work in a nutshell

\nexists $2^{O(n)}$ -time $\text{poly}(n)$ -space probabilistic algorithm for finding short vectors in lattices
 $\implies \nexists$ PPT algorithm for H-ISIS.

This work

Typical crypto theorems

\nexists PPT algorithm for task A (e.g. solving discrete logarithm, finding short vectors in lattices)
 $\implies \nexists$ PPT algorithm for task B (e.g. breaking security of a scheme).

This work in a nutshell

\nexists $2^{O(n)}$ -time $\text{poly}(n)$ -space probabilistic algorithm for finding short vectors in lattices
 $\implies \nexists$ PPT algorithm for H-ISIS.

This work

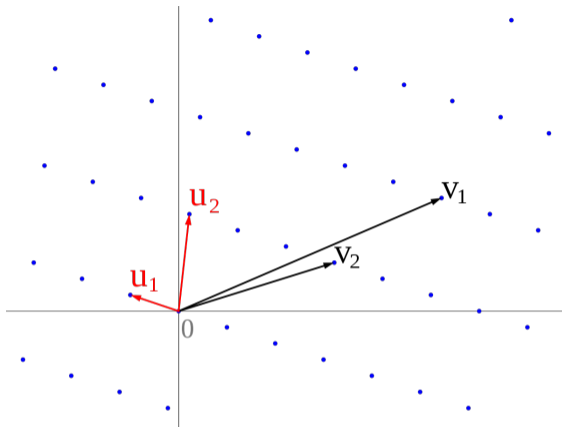
Typical crypto theorems

\nexists PPT algorithm for task A (e.g. solving discrete logarithm, finding short vectors in lattices)
 $\implies \nexists$ PPT algorithm for task B (e.g. breaking security of a scheme).

This work in a nutshell

\nexists $2^{O(n)}$ -time $\text{poly}(n)$ -space probabilistic algorithm for finding short vectors in lattices
 $\implies \nexists$ PPT algorithm for H-ISIS.

Lattices



$\mathbf{B} \in \mathbb{R}^{n \times k}$ basis, $k \leq n$

$$\mathcal{L}(\mathbf{B}) = \mathbf{B} \cdot \mathbb{Z}^k$$

“Full-rank” $\iff k = n$

q -ary lattices

† $\mathbb{Z}_q := \mathbb{Z}/q\mathbb{Z}$

† $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ wide matrix, typically $2n \leq m \leq 2n \log q$

† $\Lambda_q^\perp(\mathbf{A}) = \{\mathbf{x} \in \mathbb{Z}^m : \mathbf{A}\mathbf{x} = \mathbf{0} \pmod{q}\}$ “kernel lattice of \mathbf{A} ”

† Note $q \cdot \mathbb{Z}^m \subseteq \Lambda_q^\perp(\mathbf{A}) \subseteq \mathbb{Z}^m$ are full-rank m -dimensional lattices.

Discrete Gaussians

$$\mathcal{D}_{\Lambda_q^\perp(\mathbf{A}),s,\mathbf{c}}(\mathbf{x}) \propto \exp\left(-\pi \cdot \frac{\|\mathbf{x} - \mathbf{c}\|^2}{s^2}\right)$$

- † Support restricted to $\Lambda_q^\perp(\mathbf{A})$
- † Gaussian parameter s / standard deviation $\approx s/\sqrt{2\pi}$
- † Centre \mathbf{c} , omitted if $\mathbf{c} = \mathbf{0}$.

Short Integer Solution (SIS)

Short Integer Solution ($\text{SIS}_{n,m,q,\beta}$)

Given $\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$, find $\mathbf{v} \in \mathbb{Z}^m$ such that

$$\mathbf{A} \cdot \mathbf{v} \equiv \mathbf{0} \pmod{q} \quad \text{and} \quad 0 < \|\mathbf{v}\| \leq \beta.$$

In lattice terms

Given $\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$, find $\mathbf{v} \in \mathbb{Z}^m$ such that

$$\mathbf{v} \in \Lambda_q^\perp(\mathbf{A}) \quad \text{and} \quad 0 < \|\mathbf{v}\| \leq \beta.$$

Short Integer Solution (SIS)

Short Integer Solution ($\text{SIS}_{n,m,q,\beta}$)

Given $\mathbf{A} \leftarrow_{\$} \mathbb{Z}_q^{n \times m}$, find $\mathbf{v} \in \mathbb{Z}^m$ such that

$$\mathbf{A} \cdot \mathbf{v} \equiv \mathbf{0} \pmod{q} \quad \text{and} \quad 0 < \|\mathbf{v}\| \leq \beta.$$

In lattice terms

Given $\mathbf{A} \leftarrow_{\$} \mathbb{Z}_q^{n \times m}$, find $\mathbf{v} \in \mathbb{Z}^m$ such that

$$\mathbf{v} \in \Lambda_q^\perp(\mathbf{A}) \quad \text{and} \quad 0 < \|\mathbf{v}\| \leq \beta.$$

Inhomogeneous Short Integer Solution (ISIS)

Inhomogeneous Short Integer Solution (ISIS _{n,m,q,β})

Given $\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$ and $\mathbf{t} \leftarrow \mathbb{Z}_q^n$, find $\mathbf{v} \in \mathbb{Z}^m$ such that

$$\mathbf{A} \cdot \mathbf{v} \equiv \mathbf{t} \pmod{q} \quad \text{and} \quad \|\mathbf{v}\| \leq \beta.$$

In lattice terms

Given $\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$ and $\mathbf{t} \leftarrow \mathbb{Z}_q^n$, find $\mathbf{v} \in \mathbb{Z}^m$ such that

$$\mathbf{v} \in \Lambda_q^\perp(\mathbf{A}) + \mathbf{c} \quad \text{and} \quad \|\mathbf{v}\| \leq \beta$$

where \mathbf{c} is any fixed vector satisfying $\mathbf{A} \cdot \mathbf{c} = \mathbf{t} \pmod{q}$.

Algorithms for finding short vectors / solving (I)SIS

Let $\Lambda \subset \mathbb{R}^n$ lattice. How to find a short vector in (cosets of) Λ (in worst-/average-case)?

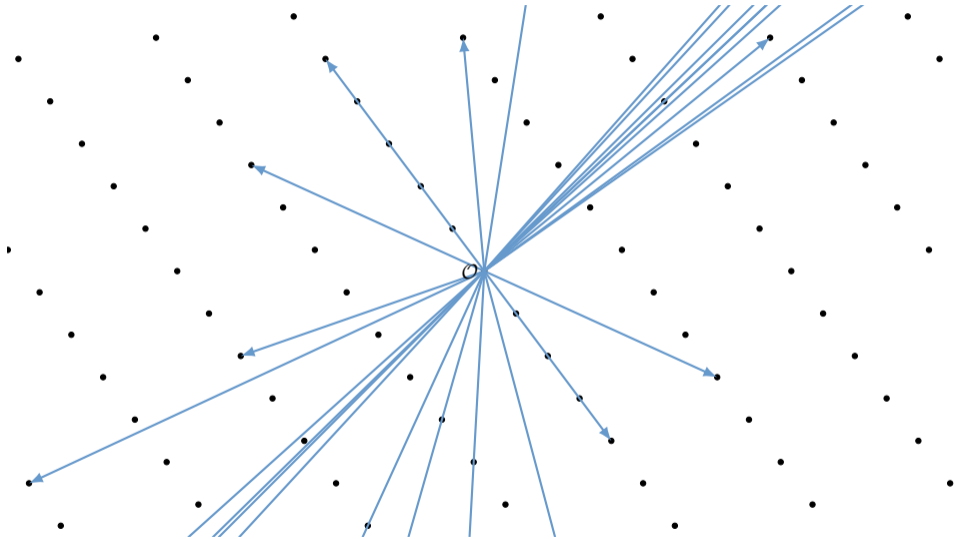
Enumeration

- † Search through vectors smaller than a given bound: project down to 1-dim problem, lift to 2-dim problem ...
- † **Time:** $n^{\Theta(n)}$
- † **Memory:** $\text{poly}(n)$

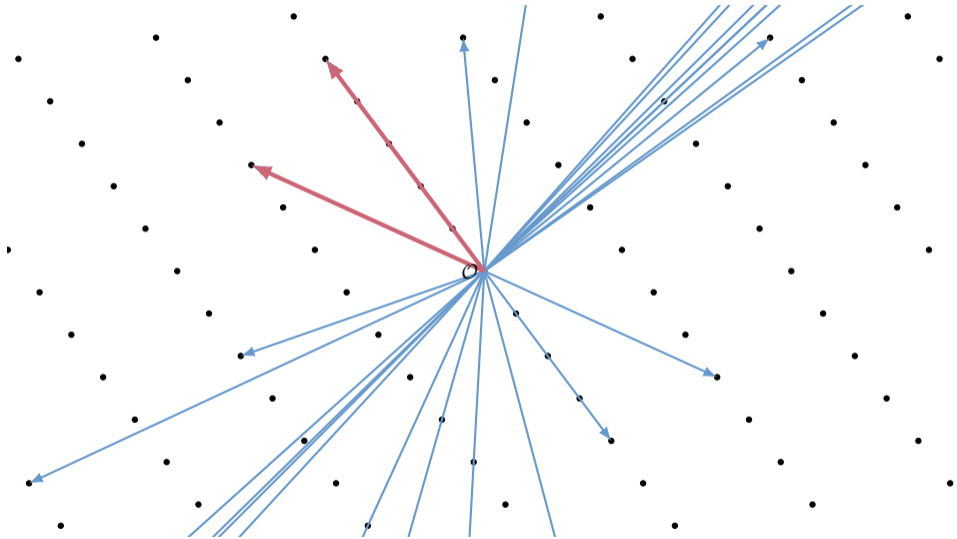
Sieving

- † Produce new, shorter vectors by considering sums and differences of existing vectors
- † **Time:** $2^{\Theta(n)}$
- † **Memory:** $2^{\Theta(n)}$

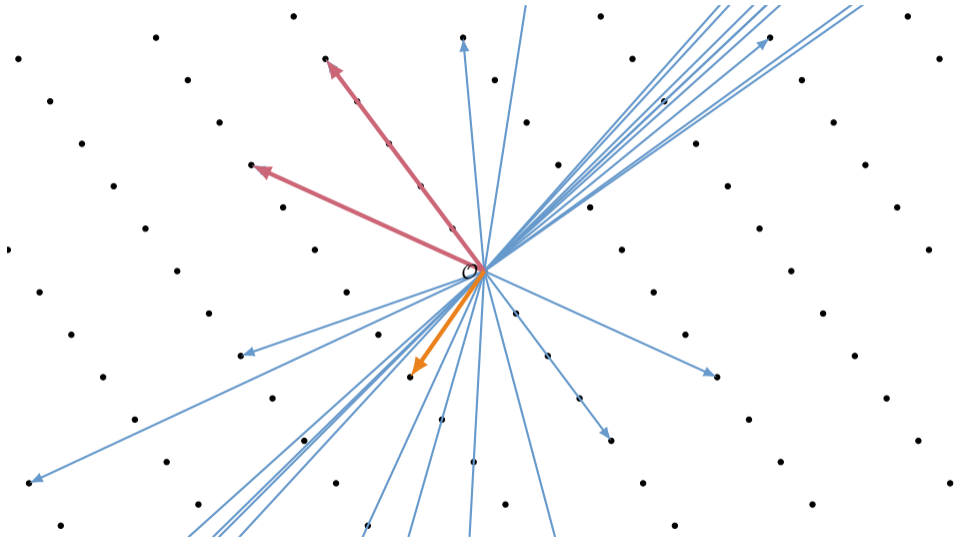
Sieving



Sieving



Sieving



Space-time hardness: cryptanalysis

- † “It is still unclear if we can get a $2^{O(n)}$ algorithm that uses only polynomial space” [MV10]
- † “is it possible to achieve exponential time complexity with a polynomially bounded space requirement?” [HPS11]
- † “A more general open problem is whether SVP can be solved in singly exponential time but only polynomial space.” [ADRS15]

-
- † [MV10]: Daniele Micciancio and Panagiotis Voulgaris. “Faster Exponential Time Algorithms for the Shortest Vector Problem”. In: *21st SODA*. ed. by Moses Charika. ACM-SIAM, Jan. 2010, pp. 1468–1480. DOI: [10.1137/1.9781611973075.119](https://doi.org/10.1137/1.9781611973075.119)
 - † [HPS11]: Guillaume Hanrot, Xavier Pujol, and Damien Stehlé. “Algorithms for the Shortest and Closest Lattice Vector Problems”. In: *Coding and Cryptology - Third International Workshop, IWCC 2011*. Ed. by Yeow Meng Chee, Zhenbo Guo, San Ling, Fengjing Shao, Yuansheng Tang, Huaxiong Wang, and Chaoping Xing. Vol. 6639. Lecture Notes in Computer Science. Springer, 2011, pp. 159–190. DOI: [10.1007/978-3-642-20901-7_10](https://doi.org/10.1007/978-3-642-20901-7_10)
 - † [ADRS15]: Divesh Aggarwal, Daniel Dadush, Oded Regev, and Noah Stephens-Davidowitz. “Solving the Shortest Vector Problem in 2^n Time Using Discrete Gaussian Sampling: Extended Abstract”. In: *47th ACM STOC*. ed. by Rocco A. Servedio and Ronitt Rubinfeld. ACM Press, June 2015, pp. 733–742. DOI: [10.1145/2746539.2746606](https://doi.org/10.1145/2746539.2746606)

Space-time hardness: conjecture

Corollary 2.2. *The conclusion of Theorem 2.2 follows from the assumption that worst-case $\gamma(n)$ -GapSVP (for a fixed $\gamma(n) = \text{poly}(n)$) cannot be solved in time $n^{o(n)}$ with $\text{poly}(n)$ space and $\text{poly}(n)$ bits of nonuniform advice (independent of the lattice).*

Polynomial-space algorithms for GapSVP have themselves been an object of study for over 25 years [Kan83, KF16, BLS16, ABF+20], but the current best (poly-space) algorithms for this problem run in time $n^{\Omega(\epsilon n)}$ for approximation factor $n^{1/\epsilon}$. Therefore, under a sufficiently strong (and plausible) worst-case assumption about GapSVP, we have a polynomial-time Fiat-Shamir compiler without complexity leveraging.

† [LV20]: Alex Lombardi and Vinod Vaikuntanathan. “Fiat-Shamir for Repeated Squaring with Applications to PPAD-Hardness and VDFs”. In: *CRYPTO 2020, Part III*. ed. by Daniele Micciancio and Thomas Ristenpart. Vol. 12172. LNCS. Springer, Cham, Aug. 2020, pp. 632–651. DOI: [10.1007/978-3-030-56877-1_22](https://doi.org/10.1007/978-3-030-56877-1_22)

A corollary

From $\text{GapSVP} \leq \text{SIS}$ we get:

Assumption: Space-time hard SIS

For sensible $m, q, \beta \in \text{poly}(n)$, we have $(2^{O(n)}, \text{poly}(n))\text{-SIS}_{n,m,q,\beta} = \emptyset$.

A corollary (a specialisation)

Viewing $\text{SIS}_{n,m,q,\beta}$ as a lattice problem over $\Lambda_q^\perp(\mathbf{A})$, an m -dimensional lattice:

Assumption: Space-time hard ISIS

For sensible $q, \beta \in \text{poly}(n)$, $m \in O(n)$ we have $(2^{O(m)}, \text{poly}(m))\text{-SIS}_{n,m,q,\beta} = \emptyset$.

- † When $m \leq O(n)$ then $2^{O(n)} = 2^{O(m)}$; we consider only this case in this talk.
- † In the paper we also consider $m \leq o(n \log n)$, which is covered by the conjecture.
- † When $m \geq \Omega(n \log n)$, there are algorithms in $(2^{O(m)}, \text{poly}(m))\text{-SIS}_{n,m,q,\beta}$.

Hinted ISIS (H-ISIS)

$\text{Exp-H-ISIS}_{(k,n,m,q,\beta,s),\mathcal{A}}(1^n)$

$(\mathbf{A}, \mathbf{t}) \leftarrow_{\$} \mathbb{Z}_q^{n \times m} \times \mathbb{Z}_q^n$

$\mathbf{u}_1, \dots, \mathbf{u}_k \leftarrow_{\$} \mathcal{D}_{\Lambda_q^\perp(\mathbf{A}),s} \quad / \quad \|\mathbf{u}_i\| \approx \sqrt{m} \cdot s$

$\mathbf{v} \leftarrow \mathcal{A}(\mathbf{A}, \mathbf{t}, \mathbf{u}_1, \dots, \mathbf{u}_k)$

return $[\mathbf{A} \cdot \mathbf{v} \equiv \mathbf{t} \pmod{q} \wedge \|\mathbf{v}\| \leq \beta]$

By default, we consider $m \ll k \in \text{poly}(n)$, i.e. many hints.

Parameter regimes

† $\beta \geq \Omega(m \cdot s)$: Trivially easy – run Babai's Nearest Plane algorithm

† $\beta \leq O(\sqrt{m} \cdot s)$: Plausibly hard

† $\beta = \sqrt{m} \cdot s$: Assumed for simplicity in this talk

Hinted ISIS (H-ISIS)

$\text{Exp-H-ISIS}_{(k,n,m,q,\beta,s),\mathcal{A}}(1^n)$

$(\mathbf{A}, \mathbf{t}) \leftarrow_{\$} \mathbb{Z}_q^{n \times m} \times \mathbb{Z}_q^n$

$\mathbf{u}_1, \dots, \mathbf{u}_k \leftarrow_{\$} \mathcal{D}_{\Lambda_q^\perp(\mathbf{A}),s} \quad / \quad \|\mathbf{u}_i\| \approx \sqrt{m} \cdot s$

$\mathbf{v} \leftarrow \mathcal{A}(\mathbf{A}, \mathbf{t}, \mathbf{u}_1, \dots, \mathbf{u}_k)$

return $[\mathbf{A} \cdot \mathbf{v} \equiv \mathbf{t} \pmod{q} \wedge \|\mathbf{v}\| \leq \beta]$

By default, we consider $m \ll k \in \text{poly}(n)$, i.e. many hints.

Parameter regimes

- † $\beta \geq \Omega(m \cdot s)$: Trivially easy – run Babai's Nearest Plane algorithm
- † $\beta \leq O(\sqrt{m} \cdot s)$: Plausibly hard
- † $\beta = \sqrt{m} \cdot s$: Assumed for simplicity in this talk

Main result

Theorem

$(2^{O(m)}, \text{poly}(m))$ -SIS $_{n,m,q,\beta^*} = \emptyset$, where $\beta^* \geq \tilde{\Omega}(m)$ · (smallest possible)
 \implies There exists k, β, s such that $(\text{poly}(n), \text{poly}(n))$ -H-ISIS $_{k,n,m,q,\beta,s} = \emptyset$.

H-ISIS solver \implies Malicious-centre Gaussian sampler

† Suppose $\mathcal{A}(\mathbf{A}, \mathbf{t}, \mathbf{u}_1, \dots, \mathbf{u}_k)$ is an $\text{H-ISIS}_{k,n,m,q,\beta,s}$ solver (with probability 1 for simplicity).

† Recall $\mathbf{u}_1, \dots, \mathbf{u}_k \leftarrow_{\$} \mathcal{D}_{\Lambda_q^\perp(\mathbf{A}),s}$.

† Let $1 < \gamma \in O(1)$ “shrink factor” and $s' = s/\sqrt{2}\gamma$.

$\mathcal{B}(\mathbf{A}, \mathbf{u}_1, \dots, \mathbf{u}_k)$ / Essentially the standard SIS to ISIS reduction.

$\mathbf{x} \leftarrow_{\$} \mathcal{D}_{\mathbb{Z}^m, s'}$ / $\|\mathbf{x}\| \approx \sqrt{m} \cdot s'$

$\mathbf{t} := \mathbf{A} \cdot \mathbf{x} \bmod q$ / $(\mathbf{A}, \mathbf{t}) \approx (\mathbf{A}, \$)$

$\mathbf{c} \leftarrow \mathcal{A}(\mathbf{A}, \mathbf{t}, \mathbf{u}_1, \dots, \mathbf{u}_k)$ / $\mathbf{A} \cdot \mathbf{c} = \mathbf{t} \bmod q$

$\mathbf{v} := \mathbf{c} - \mathbf{x}$

return (\mathbf{c}, \mathbf{v})

Interpretation: $\mathcal{B}(\mathbf{A}, \mathbf{u}_1, \dots, \mathbf{u}_k)$ is a statistically good sampler for the following distribution:

† First pick centre \mathbf{c} from some (adversarial) distribution satisfying $\|\mathbf{c}\| \leq \sqrt{m} \cdot s$.

† Draw Gaussian sample $\mathbf{v} \leftarrow_{\$} \mathcal{D}_{\Lambda_q^\perp(\mathbf{A}),s',\mathbf{c}}$.

(This sample is quite long, $\|\mathbf{v}\| \approx \sqrt{m} \cdot s$, because \mathbf{c} is quite long.)

Sieving the centres

$\mathcal{C}(\mathbf{A}, \mathbf{u}_1, \dots, \mathbf{u}_k)$

- 1 : **for** $i = 1, \dots, 2^{O(m)}$
- 2 : $(\mathbf{c}'_i, \mathbf{v}'_i) \leftarrow \mathcal{B}(\mathbf{A}, \mathbf{u}_1, \dots, \mathbf{u}_k) \quad / \quad \mathbf{v}'_i \leftarrow \mathcal{D}_{\Lambda_q^\perp(\mathbf{A}), s', \mathbf{c}'_i}$
- 3 : $(\mathbf{c}''_i, \mathbf{v}''_i) \leftarrow \mathcal{B}(\mathbf{A}, \mathbf{u}_1, \dots, \mathbf{u}_k) \quad / \quad \mathbf{v}''_i \leftarrow \mathcal{D}_{\Lambda_q^\perp(\mathbf{A}), s', \mathbf{c}''_i}$
- 4 : **if** $\|\mathbf{c}'_i - \mathbf{c}''_i\| \leq \beta/(2\gamma)$
- 5 : $\mathbf{v}_i := \mathbf{v}'_i - \mathbf{v}''_i \quad / \quad \mathbf{v}_i \sim \mathcal{D}_{\Lambda_q^\perp(\mathbf{A}), \sqrt{2}s', \mathbf{c}'_i - \mathbf{c}''_i} = \mathcal{D}_{\Lambda_q^\perp(\mathbf{A}), s/\gamma, \mathbf{c}'_i - \mathbf{c}''_i}$
- 6 : $\mathbf{u}' \leftarrow \text{RejectionSampling}(\mathbf{v}_i, \mathcal{D}_{\Lambda_q^\perp(\mathbf{A}), s/\gamma}) \quad / \quad \text{A } 1/2^{O(m)} \text{ fraction will be accepted.}$
- 7 : **if** $\mathbf{u}' \neq \perp$
- 8 : **return** \mathbf{u}'

† If for some run Steps 4 and 7 both accept, \mathcal{C} outputs a sample $\mathbf{u}' \leftarrow \mathcal{D}_{\Lambda_q^\perp(\mathbf{A}), s/\gamma}$ – a factor γ improvement.

† Repeat to get a new set of hints $\{\mathbf{u}'_i\}_{1 \leq i \leq k}$ and feed back to \mathcal{C} .

† Remains to show that $\|\mathbf{c}'_i - \mathbf{c}''_i\| \leq \beta/(2\gamma)$ happens with probability at least $\frac{1}{2^{O(m)}}$.

Sieving the centres

$\mathcal{C}(\mathbf{A}, \mathbf{u}_1, \dots, \mathbf{u}_k)$

- 1 : **for** $i = 1, \dots, 2^{O(m)}$
- 2 : $(\mathbf{c}'_i, \mathbf{v}'_i) \leftarrow \mathcal{B}(\mathbf{A}, \mathbf{u}_1, \dots, \mathbf{u}_k) \quad / \quad \mathbf{v}'_i \leftarrow_{\$} \mathcal{D}_{\Lambda_q^\perp(\mathbf{A}), s', \mathbf{c}'_i}$
- 3 : $(\mathbf{c}''_i, \mathbf{v}''_i) \leftarrow \mathcal{B}(\mathbf{A}, \mathbf{u}_1, \dots, \mathbf{u}_k) \quad / \quad \mathbf{v}''_i \leftarrow_{\$} \mathcal{D}_{\Lambda_q^\perp(\mathbf{A}), s', \mathbf{c}''_i}$
- 4 : **if** $\|\mathbf{c}'_i - \mathbf{c}''_i\| \leq \beta/(2\gamma)$
- 5 : $\mathbf{v}_i := \mathbf{v}'_i - \mathbf{v}''_i \quad / \quad \mathbf{v}_i \sim \mathcal{D}_{\Lambda_q^\perp(\mathbf{A}), \sqrt{2}s', \mathbf{c}'_i - \mathbf{c}''_i} = \mathcal{D}_{\Lambda_q^\perp(\mathbf{A}), s/\gamma, \mathbf{c}'_i - \mathbf{c}''_i}$
- 6 : $\mathbf{u}' \leftarrow \text{RejectionSampling}(\mathbf{v}_i, \mathcal{D}_{\Lambda_q^\perp(\mathbf{A}), s/\gamma}) \quad / \quad \text{A } 1/2^{O(m)} \text{ fraction will be accepted.}$
- 7 : **if** $\mathbf{u}' \neq \perp$
- 8 : **return** \mathbf{u}'

† If for some run Steps 4 and 7 both accept, \mathcal{C} outputs a sample $\mathbf{u}' \leftarrow_{\$} \mathcal{D}_{\Lambda_q^\perp(\mathbf{A}), s/\gamma}$ – a factor γ improvement.

† Repeat to get a new set of hints $\{\mathbf{u}'_i\}_{1 \leq i \leq k}$ and feed back to \mathcal{C} .

† Remains to show that $\|\mathbf{c}'_i - \mathbf{c}''_i\| \leq \beta/(2\gamma)$ happens with probability at least $\frac{1}{2^{O(m)}}$.

Sieving the centres

$\mathcal{C}(\mathbf{A}, \mathbf{u}_1, \dots, \mathbf{u}_k)$

- 1 : **for** $i = 1, \dots, 2^{O(m)}$
- 2 : $(\mathbf{c}'_i, \mathbf{v}'_i) \leftarrow \mathcal{B}(\mathbf{A}, \mathbf{u}_1, \dots, \mathbf{u}_k) \quad / \quad \mathbf{v}'_i \leftarrow \mathcal{D}_{\Lambda_q^\perp(\mathbf{A}), s', \mathbf{c}'_i}$
- 3 : $(\mathbf{c}''_i, \mathbf{v}''_i) \leftarrow \mathcal{B}(\mathbf{A}, \mathbf{u}_1, \dots, \mathbf{u}_k) \quad / \quad \mathbf{v}''_i \leftarrow \mathcal{D}_{\Lambda_q^\perp(\mathbf{A}), s', \mathbf{c}''_i}$
- 4 : **if** $\|\mathbf{c}'_i - \mathbf{c}''_i\| \leq \beta/(2\gamma)$
- 5 : $\mathbf{v}_i := \mathbf{v}'_i - \mathbf{v}''_i \quad / \quad \mathbf{v}_i \sim \mathcal{D}_{\Lambda_q^\perp(\mathbf{A}), \sqrt{2}s', \mathbf{c}'_i - \mathbf{c}''_i} = \mathcal{D}_{\Lambda_q^\perp(\mathbf{A}), s/\gamma, \mathbf{c}'_i - \mathbf{c}''_i}$
- 6 : $\mathbf{u}' \leftarrow \text{RejectionSampling}(\mathbf{v}_i, \mathcal{D}_{\Lambda_q^\perp(\mathbf{A}), s/\gamma}) \quad / \quad \text{A } 1/2^{O(m)} \text{ fraction will be accepted.}$
- 7 : **if** $\mathbf{u}' \neq \perp$
- 8 : **return** \mathbf{u}'

† If for some run Steps 4 and 7 both accept, \mathcal{C} outputs a sample $\mathbf{u}' \leftarrow \mathcal{D}_{\Lambda_q^\perp(\mathbf{A}), s/\gamma}$ – a factor γ improvement.

† Repeat to get a new set of hints $\{\mathbf{u}'_i\}_{1 \leq i \leq k}$ and feed back to \mathcal{C} .

† Remains to show that $\|\mathbf{c}'_i - \mathbf{c}''_i\| \leq \beta/(2\gamma)$ happens with probability at least $\frac{1}{2^{O(m)}}$.

Geometry of sieves

Lemma: "There cannot be too many points in a ball that are far apart."

Let $S \subset \mathcal{B}^m(\beta)$.

If $|S| > 2^{m \log(1+4\gamma)}$, there exist distinct $\mathbf{c}', \mathbf{c}'' \in S$ with $\|\mathbf{c}' - \mathbf{c}''\| \leq \beta/2\gamma$.

Proof.

- † Place balls of radii $r = \beta/4\gamma$ at points that are distance $\beta/2\gamma$ apart.
- † Compare total volume of these balls with the volume of the ball with radius $\beta + r$.

Geometry of sieves

Lemma: "There cannot be too many points in a ball that are far apart."

Let $S \subset \mathcal{B}^m(\beta)$.

If $|S| > 2^{m \log(1+4\gamma)}$, there exist distinct $\mathbf{c}', \mathbf{c}'' \in S$ with $\|\mathbf{c}' - \mathbf{c}''\| \leq \beta/2\gamma$.

Proof.

- † Place balls of radii $r = \beta/4\gamma$ at points that are distance $\beta/2\gamma$ apart.
- † Compare total volume of these balls with the volume of the ball with radius $\beta + r$.

Probabilistic upgrade

Lemma: “No distribution over a ball can avoid close pairs.”

For **any (malicious) distribution** D over $\mathcal{B}^m(\beta)$ with finite support:

$$\Pr_{\mathbf{c}', \mathbf{c}'' \leftarrow D} [\|\mathbf{c}' - \mathbf{c}''\| > \beta/2\gamma] \leq 1 - 2^{-m \log(1+4\gamma)}. \quad / \text{Note: } \mathbf{c}' = \mathbf{c}'' \text{ falls into the event.}$$

Motzkin–Straus Theorem [MS65]

Let G undirected simple graph, clique number $\omega(G)$, and adjacency matrix \mathbf{M} .

$$\max_{\mathbf{d} \in [0,1]^n: \|\mathbf{d}\|_1=1} \mathbf{d}^T \cdot \mathbf{M} \cdot \mathbf{d} = 1 - \frac{1}{\omega(G)}.$$

Proof of Lemma. Define G so that \mathbf{x} and \mathbf{y} are connected iff $\|\mathbf{x} - \mathbf{y}\| > \beta/2\gamma$. Clique = “(anti-)cluster” of far-apart points. Apply Motzkin–Straus on G . By geometry of sieves, $\omega(G) \leq 2^{m \log(1+4\gamma)}$.

† [MS65]: T. S. Motzkin and E. G. Straus. “Maxima for Graphs and a New Proof of a Theorem of Turán”. In: *Canadian Journal of Mathematics* 17 (1965), pp. 533–540. DOI: 10.4153/CJM-1965-053-6

Probabilistic upgrade

Lemma: “No distribution over a ball can avoid close pairs.”

For **any (malicious) distribution** D over $\mathcal{B}^m(\beta)$ with finite support:

$$\Pr_{\mathbf{c}', \mathbf{c}'' \leftarrow D} [\|\mathbf{c}' - \mathbf{c}''\| > \beta/2\gamma] \leq 1 - 2^{-m \log(1+4\gamma)}. \quad / \text{Note: } \mathbf{c}' = \mathbf{c}'' \text{ falls into the event.}$$

Motzkin–Straus Theorem [MS65]

Let G undirected simple graph, clique number $\omega(G)$, and adjacency matrix \mathbf{M} .

$$\max_{\mathbf{d} \in [0,1]^n: \|\mathbf{d}\|_1=1} \mathbf{d}^T \cdot \mathbf{M} \cdot \mathbf{d} = 1 - \frac{1}{\omega(G)}.$$

Proof of Lemma. Define G so that \mathbf{x} and \mathbf{y} are connected iff $\|\mathbf{x} - \mathbf{y}\| > \beta/2\gamma$. Clique = “(anti-)cluster” of far-apart points. Apply Motzkin–Straus on G . By geometry of sieves, $\omega(G) \leq 2^{m \log(1+4\gamma)}$.

† [MS65]: T. S. Motzkin and E. G. Straus. “Maxima for Graphs and a New Proof of a Theorem of Turán”. In: *Canadian Journal of Mathematics* 17 (1965), pp. 533–540. DOI: [10.4153/CJM-1965-053-6](https://doi.org/10.4153/CJM-1965-053-6)

Probabilistic upgrade

Lemma: “No distribution over a ball can avoid close pairs.”

For **any (malicious) distribution** D over $\mathcal{B}^m(\beta)$ with finite support:

$$\Pr_{\mathbf{c}', \mathbf{c}'' \leftarrow D} [\|\mathbf{c}' - \mathbf{c}''\| > \beta/2\gamma] \leq 1 - 2^{-m \log(1+4\gamma)}. \quad / \text{Note: } \mathbf{c}' = \mathbf{c}'' \text{ falls into the event.}$$

Motzkin–Straus Theorem [MS65]

Let G undirected simple graph, clique number $\omega(G)$, and adjacency matrix \mathbf{M} .

$$\max_{\mathbf{d} \in [0,1]^n: \|\mathbf{d}\|_1=1} \mathbf{d}^T \cdot \mathbf{M} \cdot \mathbf{d} = 1 - \frac{1}{\omega(G)}.$$

Proof of Lemma. Define G so that \mathbf{x} and \mathbf{y} are connected iff $\|\mathbf{x} - \mathbf{y}\| > \beta/2\gamma$. Clique = “(anti-)cluster” of far-apart points. Apply Motzkin–Straus on G . By geometry of sieves, $\omega(G) \leq 2^{m \log(1+4\gamma)}$.

† [MS65]: T. S. Motzkin and E. G. Straus. “Maxima for Graphs and a New Proof of a Theorem of Turán”. In: *Canadian Journal of Mathematics* 17 (1965), pp. 533–540. DOI: [10.4153/CJM-1965-053-6](https://doi.org/10.4153/CJM-1965-053-6)

Starting and stopping conditions

$\mathcal{C}(\mathbf{A}, \mathbf{u}_1, \dots, \mathbf{u}_k)$

```
1: for  $i = 1, \dots, 2^{O(m)}$ 
2:    $(\mathbf{c}'_i, \mathbf{v}'_i) \leftarrow \mathcal{B}(\mathbf{A}, \mathbf{u}_1, \dots, \mathbf{u}_k)$ 
3:    $(\mathbf{c}''_i, \mathbf{v}''_i) \leftarrow \mathcal{B}(\mathbf{A}, \mathbf{u}_1, \dots, \mathbf{u}_k)$ 
4:   if  $\|\mathbf{c}'_i - \mathbf{c}''_i\| \leq \beta/(2\gamma)$ 
5:      $\mathbf{v}_i := \mathbf{v}'_i - \mathbf{v}''_i$ 
6:      $\mathbf{u}' \leftarrow \text{RejSamp}(\mathbf{v}_i, \mathcal{D}_{\Lambda_q^\perp(\mathbf{A}), s/\gamma})$ 
7:     if  $\mathbf{u}' \neq \perp$ 
8:       return  $\mathbf{u}'$ 
```

Starting condition

We kickstart \mathcal{C} with trivial hints, $\|\mathbf{u}_i\| \approx \sqrt{m} \cdot q$.

Stopping conditions

Norm bound $\beta \geq \tilde{\Omega}(m) \cdot \lambda_1(\Lambda_q^\perp(\mathbf{A}))$ violated.
(Simulation of ISIS challenge fails.)

Starting and stopping conditions

$\mathcal{C}(\mathbf{A}, \mathbf{u}_1, \dots, \mathbf{u}_k)$

```
1: for  $i = 1, \dots, 2^{O(m)}$ 
2:    $(\mathbf{c}'_i, \mathbf{v}'_i) \leftarrow \mathcal{B}(\mathbf{A}, \mathbf{u}_1, \dots, \mathbf{u}_k)$ 
3:    $(\mathbf{c}''_i, \mathbf{v}''_i) \leftarrow \mathcal{B}(\mathbf{A}, \mathbf{u}_1, \dots, \mathbf{u}_k)$ 
4:   if  $\|\mathbf{c}'_i - \mathbf{c}''_i\| \leq \beta/(2\gamma)$ 
5:      $\mathbf{v}_i := \mathbf{v}'_i - \mathbf{v}''_i$ 
6:      $\mathbf{u}' \leftarrow \text{RejSamp}(\mathbf{v}_i, \mathcal{D}_{\Lambda_q^\perp(\mathbf{A}), s/\gamma})$ 
7:     if  $\mathbf{u}' \neq \perp$ 
8:       return  $\mathbf{u}'$ 
```

Starting condition

We kickstart \mathcal{C} with trivial hints, $\|\mathbf{u}_i\| \approx \sqrt{m} \cdot q$.

Stopping conditions

Norm bound $\beta \geq \tilde{\Omega}(m) \cdot \lambda_1(\Lambda_q^\perp(\mathbf{A}))$ violated.
(Simulation of ISIS challenge fails.)

Caveats

† We need to assume existence of a chain of adversaries for different parameters.

† The whole chain of adversaries need to be happy with the same **A**.

⇒ (Conditionally) rule out H-ISIS adversaries for **some** parameters but we don't know which.

Take away

Theorem

$(2^{O(m)}, \text{poly}(m))$ -SIS $_{n,m,q,\beta^*} = \emptyset$
 \implies There exists k, β, s such that $(\text{poly}(n), \text{poly}(n))$ -H-ISIS $_{k,n,m,q,\beta,s} = \emptyset$.

Directions

1. What else can we build from H-ISIS?
2. Reduce space-time hardness of lattice problems to other hinted lattice problems?
In particular, Hinted **Decision** Learning with Errors?

† <https://ia.cr/2026/187>

Kiitos!