Vanishing Short Integer Solution (vSIS)

Russell W. F. Lai

Aalto University

Novel Lattice Assumptions workshop, ICMS, 2026

Goal of this talk

† Vanishing SIS is (arguably) the simplest structured lattice assumption beyond ring/module SIS

† Breaking vSIS is a natural strategy towards breaking other novel lattice assumptions.

† $\Longrightarrow$ Natural first target for reductions and attacks.

† Goal: Establish common notation and language so we can work together

Short Integer Solution (SIS)

$\underline{\mathrm{SIS}_{\mathbb{Z},n,m,q,\beta}}$

- Given: $\mathbf{A} \leftarrow\!\!\$\ \mathbb{Z}_q^{n\times m}$
- Find: $\mathbf{x} \in \mathbb{Z}^m$ such that
  - $\mathbf{A}\mathbf{x} = \mathbf{0} \bmod q$ and
  - $0 < \|\mathbf{x}\| \leq \beta$

- n: Number of rows / module rank / number of points (explained later)
- m: Witness dimension
- q: Modulus
- β: Norm bound
- $\mathcal{R}$: Some ring, typically cyclotomic, with some embedding $\psi : \mathcal{R}^m \to \mathbb{R}^{\varphi m}$
- $\|\cdot\|$: Some norm defined via the embedding ψ, i.e. $\|\mathbf{x}\| := \|\psi(\mathbf{x})\|$

Short Integer Solution (SIS)

$\underline{\mathrm{SIS}_{\mathcal{R},n,m,q,\beta}}$

- Given: $\mathbf{A} \leftarrow\!\!\$\ \mathcal{R}_q^{n \times m}$
- Find: $\mathbf{x} \in \mathcal{R}^m$ such that
  - $\mathbf{A}\mathbf{x} = \mathbf{0} \bmod q$ and
  - $0 < \|\mathbf{x}\| \leq \beta$

- n: Number of rows / module rank / number of points (explained later)
- m: Witness dimension
- q: Modulus
- β: Norm bound
- $\mathcal{R}$: Some ring, typically cyclotomic, with some embedding $\psi : \mathcal{R}^m \to \mathbb{R}^{\varphi m}$
- $\|\cdot\|$: Some norm defined via the embedding ψ, i.e. $\|\mathbf{x}\| := \|\psi(\mathbf{x})\|$

Functional point of view

Traditional point of view

$\mathrm{SIS}_{\mathcal{R},n,m,q,\beta}$

- Given: $\mathbf{A} \hookleftarrow \$ \; \mathcal{R}_q^{n \times m}$
- Find: $\mathbf{x} \in \mathcal{R}^m$ such that
  - $\mathbf{A}\mathbf{x} = \mathbf{0} \bmod q$ and
  - $0 < \|\mathbf{x}\| \leq \beta$

Functional point of view

$\mathrm{SIS}_{\mathcal{R},n,m,q,\beta}$

- Given: $\mathbf{a}_1, \ldots, \mathbf{a}_n \hookleftarrow \$ \; \mathcal{R}_q^m$ (rows of $\mathbf{A}$)
- Find: linear $f : \mathcal{R}^m \to \mathcal{R}$ such that
  - $f(\mathbf{a}_i) = 0 \bmod q$ for all $i \in [n]$ and
  - $0 < \|f\| \leq \beta$

SIS asks to find a linear function with short coefficients which vanishes at the n given random points.

Why should the class of functions be linear?

Functional point of view

Traditional point of view

$\mathrm{SIS}_{\mathcal{R},n,m,q,\beta}$

- Given: $\mathbf{A} \hookleftarrow \$ \; \mathcal{R}_q^{n \times m}$
- Find: $\mathbf{x} \in \mathcal{R}^m$ such that
  - $\mathbf{A}\mathbf{x} = \mathbf{0} \bmod q$ and
  - $0 < \|\mathbf{x}\| \leq \beta$

Functional point of view

$\mathrm{SIS}_{\mathcal{R},n,m,q,\beta}$

- Given: $\mathbf{a}_1, \ldots, \mathbf{a}_n \hookleftarrow \$ \; \mathcal{R}_q^m$ (rows of $\mathbf{A}$)
- Find: linear $f : \mathcal{R}^m \to \mathcal{R}$ such that
  - $f(\mathbf{a}_i) = 0 \bmod q$ for all $i \in [n]$ and
  - $0 < \|f\| \leq \beta$

SIS asks to find a linear function with short coefficients which vanishes at the n given random points.

Why should the class of functions be linear?

Functional point of view

Traditional point of view

$\mathrm{SIS}_{\mathcal{R},n,m,q,\beta}$

- Given: $\mathbf{A} \hookleftarrow \$ \; \mathcal{R}_q^{n \times m}$
- Find: $\mathbf{x} \in \mathcal{R}^m$ such that
  - $\mathbf{A}\mathbf{x} = \mathbf{0} \bmod q$ and
  - $0 < \|\mathbf{x}\| \leq \beta$

Functional point of view

$\mathrm{SIS}_{\mathcal{R},n,m,q,\beta}$

- Given: $\mathbf{a}_1, \ldots, \mathbf{a}_n \hookleftarrow \$ \; \mathcal{R}_q^m$ (rows of $\mathbf{A}$)
- Find: linear $f : \mathcal{R}^m \to \mathcal{R}$ such that
  - $f(\mathbf{a}_i) = 0 \bmod q$ for all $i \in [n]$ and
  - $0 < \|f\| \leq \beta$

SIS asks to find a linear function with short coefficients which vanishes at the n given random points.

Why should the class of functions be linear?

Vanishing SIS

$\mathsf{vSIS}_{\mathcal{R},n,k,q,\beta,\mathcal{F}}$ [CLM23]

Let $\mathcal{F} = \{f_1, \ldots, f_m\}$ be a set of k-variate functions from $\mathcal{D}_{\mathcal{F}} \subseteq \mathcal{R}_q^k$ to $\mathcal{R}_q$.

† Given: $\mathbf{a}_1, \ldots, \mathbf{a}_n \leftarrow\!\!\$\ \mathcal{D}_{\mathcal{F}} \subseteq \mathcal{R}_q^k$

† Find: $\mathbf{u}^* = (u_1^*, \ldots, u_m^*) \in \mathcal{R}^m$ such that $f(\cdot) = \sum_{i=1}^m u_i^* \cdot f_i(\cdot)$ satisfies

‡ $f(\mathbf{a}_i) = 0 \bmod q$ for all $i \in [n]$ and

‡ $0 < \|\mathbf{u}^*\| \leq \beta$

---

† [CLM23] Valerio Cini, Russell W. F. Lai, and Giulio Malavolta.
"Lattice-Based Succinct Arguments from Vanishing Polynomials - (Extended Abstract)".
In: *CRYPTO 2023*. 2023

Vanishing SIS as Structured SIS

Equivalent, we can represent vSIS as a *structured SIS* problem.

$\mathrm{vSIS}_{\mathcal{R},n,k,q,\beta,\mathcal{F}}$

Let $\mathcal{F} = \{f_1, \ldots, f_m\}$ be a set of k-variate functions from $\mathcal{D}_{\mathcal{F}} \subseteq \mathcal{R}_q^k$ to $\mathcal{R}_q$.

- Given: $\mathbf{A} \leftarrow\!\$\ \mathcal{D}_{\mathcal{F}}^n \subseteq \mathcal{R}_q^{n \times k}$
- Find: $\mathbf{u}^* \in \mathcal{R}^m$
  - $\mathcal{F}(\mathbf{A}) \cdot \mathbf{u}^* = \mathbf{0} \bmod q$ and
  - $0 < \|\mathbf{u}^*\| \leq \beta$

  where

$$\mathcal{F}(\mathbf{A}) := \begin{bmatrix} f_1(\mathbf{a}_1) & \cdots & f_m(\mathbf{a}_1) \\ \vdots & \ddots & \vdots \\ f_1(\mathbf{a}_n) & \cdots & f_m(\mathbf{a}_n) \end{bmatrix} \in \mathcal{R}_q^{n \times m}.$$

A motivating example

Take $\mathcal{F} = \{1, X, \ldots, X^d\}$, the univariate polynomials of degree at most d.

The vSIS commitment [SLNS24]

Commit to a short degree-d polynomial f by evaluating it at the public random points:

$$\mathrm{Com}(f) := (f(a_1), \ldots, f(a_n)) \bmod q.$$

† **Binding $\iff$ vSIS.** If $f \neq g$ are short degree-d polynomials with $\mathrm{Com}(f) = \mathrm{Com}(g)$, then $f - g$ is a non-zero short degree-d polynomial with

$$(f - g)(a_i) = 0 \bmod q \quad \text{for all } i \in [n].$$

† **Multiplicative structure.** Component-wise product $\mathrm{Com}(f) \odot \mathrm{Com}(g)$ is a commitment to $f \cdot g$, since

$$(f \cdot g)(a_i) = f(a_i) \cdot g(a_i) \bmod q,$$

binding under univariate vSIS with degree $2d$ and norm bound $\approx d \cdot \beta^2$.

A motivating example

Take $\mathcal{F} = \{1, X, \ldots, X^d\}$, the univariate polynomials of degree at most d.

The vSIS commitment [CLM23]

Commit to a short degree-d polynomial f by evaluating it at the public random points:

$$\mathrm{Com}(f) := (f(a_1), \ldots, f(a_n)) \bmod q.$$

† **Binding $\iff$ vSIS.** If $f \neq g$ are short degree-d polynomials with $\mathrm{Com}(f) = \mathrm{Com}(g)$, then $f - g$ is a non-zero short degree-d polynomial with

$$(f - g)(a_i) = 0 \bmod q \quad \text{for all } i \in [n].$$

† **Multiplicative structure.** Component-wise product $\mathrm{Com}(f) \odot \mathrm{Com}(g)$ is a commitment to $f \cdot g$, since

$$(f \cdot g)(a_i) = f(a_i) \cdot g(a_i) \bmod q,$$

binding under univariate vSIS with degree $2d$ and norm bound $\approx d \cdot \beta^2$.

A motivating example

Take $\mathcal{F} = \{1, X, \ldots, X^d\}$, the univariate polynomials of degree at most d.

The vSIS commitment [CLM23]

Commit to a short degree-d polynomial f by evaluating it at the public random points:

$$\mathrm{Com}(f) := (f(a_1), \ldots, f(a_n)) \bmod q.$$

† **Binding $\iff$ vSIS.** If $f \neq g$ are short degree-d polynomials with $\mathrm{Com}(f) = \mathrm{Com}(g)$, then $f - g$ is a non-zero short degree-d polynomial with

$$(f - g)(a_i) = 0 \bmod q \quad \text{for all } i \in [n].$$

† **Multiplicative structure.** Component-wise product $\mathrm{Com}(f) \odot \mathrm{Com}(g)$ is a commitment to $f \cdot g$, since

$$(f \cdot g)(a_i) = f(a_i) \cdot g(a_i) \bmod q,$$

binding under univariate vSIS with degree $2d$ and norm bound $\approx d \cdot \beta^2$.

A motivating example

Take $\mathcal{F} = \{1, X, \ldots, X^d\}$, the univariate polynomials of degree at most d.

The vSIS commitment [CLM23]

Commit to a short degree-d polynomial f by evaluating it at the public random points:

$$\mathrm{Com}(f) := (f(a_1), \ldots, f(a_n)) \bmod q.$$

† **Binding $\iff$ vSIS.** If $f \neq g$ are short degree-d polynomials with $\mathrm{Com}(f) = \mathrm{Com}(g)$, then $f - g$ is a non-zero short degree-d polynomial with

$$(f - g)(a_i) = 0 \bmod q \quad \text{for all } i \in [n].$$

† **Multiplicative structure.** Component-wise product $\mathrm{Com}(f) \odot \mathrm{Com}(g)$ is a commitment to $f \cdot g$, since

$$(f \cdot g)(a_i) = f(a_i) \cdot g(a_i) \bmod q,$$

binding under univariate vSIS with degree $2d$ and norm bound $\approx d \cdot \beta^2$.

Example instantiations of $\mathcal{F}$

$\mathcal{F}$	Description
$\{X_1, \ldots, X_m\}$	Linear monomials, i.e. the SIS case
$\{1, X, \ldots, X^d\}$	Univariate monomials
$\{1, X^{\pm 1}, \ldots, X^{\pm d}\}$	Laurent monomials
$\{\prod_{i=1}^{\mu} X_i^{b_i} : (b_1, \ldots, b_\mu) \in \{0,1\}^\mu\}$	Multilinear monomials
$\{\prod_{i=1}^{\mu} X_{i,j_i} : (j_1, \ldots, j_\mu) \in \{0,1\}^\mu\}$	Set-multilinear monomials
$\{1/(X - e_i) : i \in [m]\}$	Elementary fractions

The SIS case

$$\mathcal{F} = \{X_1, \ldots, X_m\}.$$
$$\mathcal{F}(\mathbf{A}) = \mathbf{A}.$$

$\mathcal{F}(\mathbf{A})$: Univariate monomials $\Rightarrow$ Vandermonde

$$\mathcal{F} = \{1, X, \ldots, X^7\}.$$

$$\mathcal{F}(\mathbf{A}) = \begin{bmatrix} 1 & a & a^2 & a^3 & a^4 & a^5 & a^6 & a^7 \\ 1 & b & b^2 & b^3 & b^4 & b^5 & b^6 & b^7 \\ 1 & c & c^2 & c^3 & c^4 & c^5 & c^6 & c^7 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & a^4 \\ 1 & b^4 \\ 1 & c^4 \end{bmatrix} \bullet \begin{bmatrix} 1 & a^2 \\ 1 & b^2 \\ 1 & c^2 \end{bmatrix} \bullet \begin{bmatrix} 1 & a \\ 1 & b \\ 1 & c \end{bmatrix}$$

where $\bullet$ denotes the row-wise tensor product.

The row-tensor structure is useful for succinct arguments [CLM23; KLNO24; KLNO25; OKCLM25; KLOT25; KLNOT26].

$\mathcal{F}(\mathbf{A})$: Set-multilinear monomials

$$\mathcal{F} = \left\{ \begin{array}{llll} X_{1,0}X_{2,0}X_{3,0}, & X_{1,0}X_{2,0}X_{3,1}, & X_{1,0}X_{2,1}X_{3,0}, & X_{1,0}X_{2,1}X_{3,1}, \\ X_{1,1}X_{2,0}X_{3,0}, & X_{1,1}X_{2,0}X_{3,1}, & X_{1,1}X_{2,1}X_{3,0}, & X_{1,1}X_{2,1}X_{3,1} \end{array} \right\}.$$

$$\mathcal{F}(\mathbf{A}) = \begin{bmatrix} a_{1,0}b_{1,0}c_{1,0} & a_{1,0}b_{1,0}c_{1,1} & a_{1,0}b_{1,1}c_{1,0} & a_{1,0}b_{1,1}c_{1,1} & a_{1,1}b_{1,0}c_{1,0} & a_{1,1}b_{1,0}c_{1,1} & a_{1,1}b_{1,1}c_{1,0} & a_{1,1}b_{1,1}c_{1,1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{n,0}b_{n,0}c_{n,0} & a_{n,0}b_{n,0}c_{n,1} & a_{n,0}b_{n,1}c_{n,0} & a_{n,0}b_{n,1}c_{n,1} & a_{n,1}b_{n,0}c_{n,0} & a_{n,1}b_{n,0}c_{n,1} & a_{n,1}b_{n,1}c_{n,0} & a_{n,1}b_{n,1}c_{n,1} \end{bmatrix}$$

$$= \begin{bmatrix} a_{1,0} & a_{1,1} \\ \vdots & \vdots \\ a_{n,0} & a_{n,1} \end{bmatrix} \bullet \begin{bmatrix} b_{1,0} & b_{1,1} \\ \vdots & \vdots \\ b_{n,0} & b_{n,1} \end{bmatrix} \bullet \begin{bmatrix} c_{1,0} & c_{1,1} \\ \vdots & \vdots \\ c_{n,0} & c_{n,1} \end{bmatrix}$$

In general $\mathcal{F}(\mathbf{A}) = \mathbf{A}_1 \bullet \cdots \bullet \mathbf{A}_\mu$ for independently random $\mathbf{A}_1, \ldots, \mathbf{A}_\mu$.

$\mathcal{F}(\mathbf{A})$: Elementary fractions $\Rightarrow$ Cauchy

Fix distinct public poles $e_1, \ldots, e_m \in \mathcal{R}_q$, and

$$\mathcal{F} = \left\{ \frac{1}{X - e_1}, \ \ldots, \ \frac{1}{X - e_m} \right\}, \qquad \mathcal{D}_{\mathcal{F}} = \{ a \in \mathcal{R}_q : a - e_j \in \mathcal{R}_q^{\times} \text{ for all } j \}.$$

$$\mathcal{F}(\mathbf{A}) = \begin{bmatrix} \frac{1}{a_1 - e_1} & \frac{1}{a_1 - e_2} & \cdots & \frac{1}{a_1 - e_m} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{a_n - e_1} & \frac{1}{a_n - e_2} & \cdots & \frac{1}{a_n - e_m} \end{bmatrix}$$

Cauchy matrix with nodes $a_1, \ldots, a_n$ and poles $e_1, \ldots, e_m$.

Applications

Vanishing SIS (for polynomials) has been used to build

- † Practical lattice-based SNARKs [KLNO24; KLNO25; KLOT25; KLNOT26]
- † Lattice-based verifiable delay functions [OKCLM25] (+ sequentiality assumption)
- † Fully algebraic homomorphic signatures for low-degree polynomials [JL25] (+ vSIS trapdoor)

- † [KLNO24] Michael Klooß, Russell W. F. Lai, Ngoc Khanh Nguyen, and Michal Osadnik.
  "RoK, Paper, SISsors Toolkit for Lattice-Based Succinct Arguments - (Extended Abstract)".
  In: *ASIACRYPT 2024*. 2024
- † [KLNO25] Michael Klooß, Russell W. F. Lai, Ngoc Khanh Nguyen, and Michal Osadnik.
  "RoK and Roll - Verifier-Efficient Random Projection for $\tilde{O}(\lambda)$-Size Lattice Arguments - (Extended Abstract)".
  In: *ASIACRYPT 2025*. 2025
- † [KLOT25] Shuto Kuriyama, Russell W. F. Lai, Michał Osadnik, and Lorenzo Tucci.
  SALSAA – Sumcheck-Aided Lattice-based Succinct Arguments and Applications.
  Cryptology ePrint Archive, Report 2025/2124. 2025
- † [KLNOT26] Michael Klooss, Russell W. F. Lai, Ngoc Khanh Nguyen, Michał Osadnik, and Lorenzo Tucci.
  RoKoko: Lattice-based Succinct Arguments, a Committed Refinement.
  Cryptology ePrint Archive, Paper 2026/575. 2026
- † [OKCLM25] Michal Osadnik, Darya Kaviani, Valerio Cini, Russell W. F. Lai, and Giulio Malavolta.
  "Papercraft: Lattice-Based Verifiable Delay Function Implemented".
  In: *2025 IEEE Symposium on Security and Privacy*. 2025
- † [JL25] Kalle Jyrkinen and Russell W. F. Lai.
  "Vanishing Short Integer Solution, Revisited - Reductions, Trapdoors, Homomorphic Signatures for Low-Degree Polynomials".
  In: *PKC 2025*. 2025

Hinted vSIS

Assuming Evasive SIS, vSIS $\implies$ Hint-vSIS.

Hint-vSIS$_{\mathcal{R},n,k,q,\beta,s,\mathcal{F},\mathcal{G},\mathcal{H}}$ [DKLW25]

Target and hint functions $\mathcal{G}$ and $\mathcal{H}$ from $\mathcal{R}_q^k$ to $\mathcal{R}_q$, Gaussian width s.

- † $\mathcal{A}$ first picks $\mathcal{Q} \subseteq \mathcal{H}$ and a target $g^* \in \mathcal{G} \setminus \mathcal{Q}$.
- † Given: $\mathbf{A} \leftarrow\!\$\ \mathcal{D}^n_{\mathcal{F}\cup\mathcal{G}\cup\mathcal{H}}$ and hints $\mathbf{U} \in \mathcal{R}^{m\times|\mathcal{Q}|}$ of Gaussian width s s.t. $\mathcal{F}(\mathbf{A}) \cdot \mathbf{U} = \mathcal{Q}(\mathbf{A}) \bmod q$
- † Find: $\mathbf{u}^* \in \mathcal{R}^m$ such that $\mathcal{F}(\mathbf{A}) \cdot \mathbf{u}^* = g^*(\mathbf{A}) \bmod q$ and $0 < \|\mathbf{u}^*\| \leq \beta$

Variants:

- † Strong (s-Hint-vSIS): $\mathcal{A}$ picks $g^* \in \mathcal{G} \setminus \mathcal{Q}$ *after* seeing $\mathbf{A}$ and the hints.
- † Strong random-hinted (s-$Hint-vSIS): as strong, but $\mathcal{Q}$ is a uniformly random Q-subset of $\mathcal{H}$, not chosen by $\mathcal{A}$.
- † kRISIS / kMISIS [ACLMT22]: essentially a special case with $\mathcal{F} = \mathcal{F}_{\mathsf{SIS}}$, $\mathcal{Q} = \mathcal{H}$, and $\mathcal{G} = \{g^*\}$ disjoint from $\mathcal{H}$.

Hinted vSIS

Assuming Evasive SIS, vSIS $\implies$ Hint-vSIS.

Hint-vSIS$_{\mathcal{R},n,k,q,\beta,s,\mathcal{F},\mathcal{G},\mathcal{H}}$ [DKLW25]

Target and hint functions $\mathcal{G}$ and $\mathcal{H}$ from $\mathcal{R}_q^k$ to $\mathcal{R}_q$, Gaussian width s.

- $\mathcal{A}$ first picks $\mathcal{Q} \subseteq \mathcal{H}$ and a target $g^* \in \mathcal{G} \setminus \mathcal{Q}$.
- Given: $\mathbf{A} \leftarrow\$ \mathcal{D}^n_{\mathcal{F}\cup\mathcal{G}\cup\mathcal{H}}$ and hints $\mathbf{U} \in \mathcal{R}^{m\times|\mathcal{Q}|}$ of Gaussian width s s.t. $\mathcal{F}(\mathbf{A}) \cdot \mathbf{U} = \mathcal{Q}(\mathbf{A}) \bmod q$
- Find: $\mathbf{u}^* \in \mathcal{R}^m$ such that $\mathcal{F}(\mathbf{A}) \cdot \mathbf{u}^* = g^*(\mathbf{A}) \bmod q$ and $0 < \|\mathbf{u}^*\| \leq \beta$

Variants:

- Strong (s-Hint-vSIS): $\mathcal{A}$ picks $g^* \in \mathcal{G} \setminus \mathcal{Q}$ *after* seeing $\mathbf{A}$ and the hints.
- Strong random-hinted (s-$Hint-vSIS): as strong, but $\mathcal{Q}$ is a uniformly random Q-subset of $\mathcal{H}$, not chosen by $\mathcal{A}$.
- kRISIS / kMISIS [ACLMT22]: essentially a special case with $\mathcal{F} = \mathcal{F}_{\mathsf{SIS}}$, $\mathcal{Q} = \mathcal{H}$, and $\mathcal{G} = \{g^*\}$ disjoint from $\mathcal{H}$.

Applications: the hinted variant

The *hinted* variant is used to build

- † Proof-friendly signatures (e.g. for practical anonymous credentials) [DKLW25]
- † Functional commitments for polynomials [ACLMT22; CLM23; FLV23] and circuits [BCFL23] (via kRISIS/kMISIS)

- † [DKLW25] Adrien Dubois, Michael Klooß, Russell W. F. Lai, and Ivy K. Y. Woo.
"Lattice-Based Proof-Friendly Signatures from Vanishing Short Integer Solutions".
In: *PKC 2025*. 2025
- † [ACLMT22] 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*. 2022
- † [CLM23] Valerio Cini, Russell W. F. Lai, and Giulio Malavolta.
"Lattice-Based Succinct Arguments from Vanishing Polynomials - (Extended Abstract)".
In: *CRYPTO 2023*. 2023
- † [FLV23] Ben Fisch, Zeyu Liu, and Psi Vesely.
"Orbweaver: Succinct Linear Functional Commitments from Lattices".
In: *CRYPTO 2023*. 2023
- † [BCFL23] David Balbás, Dario Catalano, Dario Fiore, and Russell W. F. Lai.
"Chainable Functional Commitments for Unbounded-Depth Circuits".
In: *TCC 2023*. 2023

LWE analogues: $\mathcal{F}(\mathbf{A})$ or $\mathcal{F}(\mathbf{S})$ (or both)

These assumptions are not in the literature. I am introducing them now.

Public span: Span-LWE$_{\mathcal{R},n,k,q,\chi_s,\chi_e,\mathcal{F}}$

† Given: $\mathbf{A} \hookleftarrow \$ \; \mathcal{D}_{\mathcal{F}}^{n} \subseteq \mathcal{R}_q^{n \times k}$

† Distinguish: $\mathbf{s}^{\mathsf{T}} \cdot \mathcal{F}(\mathbf{A}) + \mathbf{e}^{\mathsf{T}} \bmod q \quad$ from $\quad \mathbf{b}^{\mathsf{T}}$

where $\mathbf{s} \hookleftarrow \$ \; \chi_s^n$, $\mathbf{e} \hookleftarrow \$ \; \chi_e^m$, $\mathbf{b} \hookleftarrow \$ \; \mathcal{R}_q^m$.

Hidden span: Hidden-Span-LWE$_{\mathcal{R},n,k,\ell,q,\chi_s,\chi_e,\mathcal{F}}$

† Given: $\mathbf{A} \hookleftarrow \$ \; \mathcal{R}_q^{n \times \ell}$

† Distinguish: $\mathcal{F}(\mathbf{S})^{\mathsf{T}} \cdot \mathbf{A} + \mathbf{E} \bmod q \quad$ from $\quad \mathbf{B}$

where $\mathbf{S} \hookleftarrow \$ \; \chi_s^{n \times k} \subseteq \mathcal{D}_{\mathcal{F}}^{n}$, $\mathbf{E} \hookleftarrow \$ \; \chi_e^{m \times \ell}$, $\mathbf{B} \hookleftarrow \$ \; \mathcal{R}_q^{m \times \ell}$.

Per the rules of the workshop, I will kill ≥ 2 assumptions which are special cases of the above.

Instantiating $\mathcal{F}$: the assumptions in the literature

Power RLWE [ARS24]: public span, $n = k = 1$

$$\mathcal{F} = \{1, X, \ldots, X^{m-1}\} \qquad \Longrightarrow \qquad \left(a,\ \{a^i \cdot s + e_i\}_{i\in[0,m-1]}\right) \approx_c \left(a,\ \{b_i\}_{i\in[0,m-1]}\right)$$

Applications: Succinct HSS [ARS24]; public-key PCF for OT [ABCR26] (with secret-power).

---

† [ARS24] Damiano Abram, Lawrence Roy, and Peter Scholl.
"Succinct Homomorphic Secret Sharing".
In: *EUROCRYPT 2024*. 2024

† [ABCR26] Shweta Agrawal, Kaartik Bhushan, Geoffroy Couteau, and Mahshid Riahinia.
"Post-Quantum Public-Key Pseudorandom Correlation Functions for OT".
In: *CRYPTO 2026*. 2026

Instantiating $\mathcal{F}$: the assumptions in the literature

Secret-power RLWE [ABCR26]: hidden span, short secret, $n = k = \ell = 1$

$$\mathcal{F} = \{X, X^{-1}, \ldots, X^{-(m-1)}\}$$
$$\implies \left(a,\ a \cdot s + e_0,\ \{a \cdot s^{-i} + e_i\}_{i \in [m-1]}\right) \approx_c \left(a,\ b_0,\ \{b_i\}_{i \in [m-1]}\right)$$

Applications: Constrained PRF for low-degree polynomials [ABCR26]; public-key PCF for OT (with public-power).

Secret-power RLWE [ILL25]: hidden span, short secret, $n = k = 1$, ℓ free

$$\mathcal{F} = \{X, X^2\} \qquad \implies \qquad \left(\mathbf{a},\ s \cdot \mathbf{a} + \mathbf{e}_1,\ s^2 \cdot \mathbf{a} + \mathbf{e}_2\right) \approx_c \left(\mathbf{a},\ \mathbf{b}_1,\ \mathbf{b}_2\right)$$

Applications: Succinct garbling [ILL25].

† [ILL25] Yuval Ishai, Hanjun Li, and Huijia Lin.
"A Unified Framework for Succinct Garbling from Homomorphic Secret Sharing".
In: *CRYPTO 2025*. 2025

Trivially False Instances of $\mathrm{vSIS}_{\mathcal{F}}$

1. $\mathcal{F}$ is $\mathcal{R}$-linearly dependent. A short non-zero $\mathbf{u}^*$ with $\sum_i u_i^* \cdot f_i = 0$ *as a function*. Examples:
   - ‡ $0 \in \mathcal{F}$
   - ‡ $\{1, X, 1 + X\} \subseteq \mathcal{F}$
2. $\mathcal{R}$-linear combination of $\mathcal{F}$ vanishes at random point with non-negligible probability. Examples:
   - ‡ Fully splitting prime q and $\{1, X^{q-1}\} \subseteq \mathcal{F}$.
     Reason: $\mathcal{R}_q \cong \mathbb{F}_q^{\varphi}$, so $a^{q-1} = 1 \bmod q$ for every $a \in \mathcal{R}_q^{\times}$.
   - ‡ Power-2 cyclotomic $\mathcal{R}$, $q = 2^{\ell}$, $X^{\ell\varphi} \in \mathcal{F}$.
     Reason: $q\mathcal{R} = \mathcal{I}^{\ell\varphi}$ with $\mathcal{N}(\mathcal{I}) = 2$, so $a \leftarrow\!\$\, \mathcal{R}_q$ satisfies $a^{\ell\varphi} = 0 \bmod q$ with probability $1/2$.

Strong Linear Independence criterion

Strong Linear Independence (relaxed and simplified from [DKLW25, Def. 6])

For $\epsilon > 0$, $\mathcal{F}$ is ϵ-*strongly linearly independent* if

- † $\mathcal{F}$ is linearly independent and
- † every non-constant $h \in \mathcal{R}_q\text{-span}(\mathcal{F})$ has min-entropy $\geq \log(1/\epsilon)$ at a random point.

---

† [DKLW25] Adrien Dubois, Michael Klooß, Russell W. F. Lai, and Ivy K. Y. Woo. "Lattice-Based Proof-Friendly Signatures from Vanishing Short Integer Solutions". In: *PKC 2025*. 2025

Let's try to analyse the simplest setting

We focus on:

- Univariate degree-d polynomials: $\mathcal{F} = \{1, X, \ldots, X^d\}$
- Single point: $n = 1$

vSIS$_{\mathcal{R},n,k,q,\beta,\mathcal{F}}$

- Given: $a \leftarrow\!\$\ \mathcal{R}_q$
- Find: $\mathbf{u}^* \in \mathcal{R}^m$ such that

$$\begin{bmatrix} 1 & a & \ldots & a^d \end{bmatrix} \cdot \mathbf{u}^* = 0 \bmod q \qquad \text{and} \qquad 0 < \|\mathbf{u}^*\| \leq \beta.$$

If $d = 1$, we essentially recover (search-)NTRU, except that NTRU restricts a to be of the form

$$a = f/g \bmod q$$

where $f, g \leftarrow\!\$\ \mathcal{R}_q^\times$ are low-norm.

Solution space

- Solutions live in the ideal of $\mathcal{R}[X]$ consisting of all polynomials vanishing at a modulo q.
- The solution space is a lattice with highly structured (bad) bases:

$$\begin{bmatrix} q & -a & & & \\ & 1 & -a & & \\ & & 1 & \ddots & \\ & & & \ddots & -a \\ & & & & 1 \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} q & -a & -a^2 & \dots & -a^d \\ & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{bmatrix}$$

Casting vSIS as IdSVP in extension fields

- Let $\mathcal{R} = \mathcal{O}_{\mathcal{K}}$ for some number field $\mathcal{K}$.
- Let $F(X) \in \mathcal{R}[X]$ be monic of degree $d+1$ with $F(a) = 0 \bmod q$ and irreducible over $\mathcal{K}$.
- Finding such F is efficient: Most F satisfying $F(a) = 0 \bmod q$ should be irreducible over $\mathcal{K}$.
- Let $\mathcal{L} := \mathcal{K}[X]/(F)$, a number field of degree $(d+1)\varphi$, and $\hat{\mathcal{R}} := \mathcal{R}[X]/(F) \subseteq \mathcal{O}_{\mathcal{L}}$.
- Then $\mathfrak{q} := \langle q, X - a \rangle \subseteq \hat{\mathcal{R}}$ satisfies $\hat{\mathcal{R}}/\mathfrak{q} \cong \mathcal{R}_q$ via $\alpha \mapsto \alpha(a) \bmod q$, so

$$\mathfrak{q} = \{\alpha : \alpha(a) = 0 \bmod q\}, \qquad \mathcal{N}(\mathfrak{q}) = q^{\varphi},$$

  and the degree-$\leq d$ representatives of $\mathfrak{q}$ are exactly the vSIS coefficient lattice.
- $\implies$ Single-point vSIS *is* IdSVP for $\mathfrak{q}$ in $\hat{\mathcal{R}}$ measured in a "weird" norm – a hybrid between the coefficient norm in the basis $1, X, \ldots, X^d$ and the vSIS norm defined over $\mathcal{K}$.

IdHSVP $\leq$ vSIS

Ideal Hermite Shortest Vector Problem γ-IdHSVP$_{\mathcal{R}}$

Given an ideal $\mathcal{I} \subseteq \mathcal{R}$, find an element $x \in \mathcal{I}$ with norm satisfying $0 < \|x\| \leq \gamma \cdot \varphi \cdot \mathcal{N}(\mathcal{I})^{1/\varphi}$.

Theorem: IdHSVP $\leq$ vSIS [JL25, Updated]

Let $\theta \leq \varphi$ and N be parameters. Let modulus $q = t^d + s$ with $|s| \leq (2\varphi/\theta)^d$, and

$$\beta = 2\,\varphi^{d+1} \cdot N, \qquad t > 16\,\varphi^{2d+2} \cdot N^2, \qquad \gamma \geq 2\,\varphi^d \cdot N.$$

Worst-case vSIS$_{\mathcal{R},d,q,\beta}$ is as hard as γ-IdHSVP$_{\mathcal{R}}$ for ideals $\mathcal{I} \subseteq \mathcal{R}$ satisfying the following:

† $\mathcal{N}(\mathcal{I}) \leq N^{\varphi}$,

† $\mathcal{I} = \langle z^d \rangle \cap \mathcal{R}$ is represented by some $z \in \mathcal{K}$ with $\|z^{-1}\|_{\infty} \leq \theta/2$.

Updates: joint work with Kalle Jyrkinen and Shuto Kuriyama. The PKC 2025 version [JL25] is more restrictive.

† [JL25] Kalle Jyrkinen and Russell W. F. Lai.
"Vanishing Short Integer Solution, Revisited - Reductions, Trapdoors, Homomorphic Signatures for Low-Degree Polynomials".
In: *PKC 2025*. 2025

Proof Idea

Generalisation of [PS21], who considered $d = 1$ (i.e. search NTRU).

$\mathsf{ldHSVP\text{-}to\text{-}vSIS}^{\mathcal{A}}(\mathcal{I})$

$v := \left\lfloor \frac{t}{z} \right\rceil \bmod q$

$p \leftarrow \mathcal{A}(v)$

$/\!/\ p(v) = 0 \bmod q$

$/\!/\ \|p\| \leq \beta$

return lead. coef. p_d

† $q = t^d + s$

† Small rounding error $\varepsilon := \frac{t}{z} - v$

† $\alpha \in \mathcal{I} \setminus \{0\}$ shortest $\mathcal{I}$ element

† $r := \alpha / z^d \in \mathcal{R}$

Existence: v is a valid instance – it admits a solution

$$p^*(X) := \alpha \cdot (X + \varepsilon)^d + s \cdot r \in \mathcal{R}[X],$$

$$p^*(v) = \alpha \cdot \left(\tfrac{t}{z}\right)^d + sr = r \cdot (t^d + s) = r \cdot q = 0 \bmod q,$$

and $\|p^*\| \approx \varphi^d \cdot \|\alpha\| \leq \beta$.

Recovery: For every short solution $p(X) = p_d \cdot X^d + \ldots$ with $p(v) = q \cdot u$,

$$\alpha \cdot \frac{p_d}{z^d} = \alpha \cdot u \in \mathcal{R}$$

as all remaining terms are too small to be non-zero.

$\implies p_d = z^d \cdot u \in \mathcal{I} \setminus \{0\}$.

† [PS21] Alice Pellet-Mary and Damien Stehlé. "On the Hardness of the NTRU Problem". In: *ASIACRYPT 2021*. 2021

Limitations

- Multi-point?
- Multivariate?
- Beyond polylog degree?
- Remove restrictions on ideal $\mathcal{I}$?
- Arbitrary (not near d-th power) modulus q?
- Worst-case to average-case?

Open problems

Let $\mathcal{F} : \mathcal{R}_q^k \to \mathcal{R}_q^m$ be strongly linearly independent.

$$\mathsf{vSIS}_{\mathcal{R},n,k,q,\beta,\mathcal{F}} \overset{?}{\approx} \mathsf{SIS}_{\mathcal{R},n,m,q,\beta}$$

$$\mathsf{Span\text{-}LWE}_{\mathcal{R},n,k,q,\chi_s,\chi_e,\mathcal{F}} \overset{?}{\approx} \mathsf{LWE}_{\mathcal{R},n,m,q,\chi_s,\chi_e}$$

$$\mathsf{Hidden\text{-}Span\text{-}LWE}_{\mathcal{R},n,k,\ell,q,\chi_s,\chi_e,\mathcal{F}} \overset{?}{\approx} \left(\mathsf{LWE}_{\mathcal{R},n,\ell,q,\chi_s',\chi_e}\right)^m$$

Russell W. F. Lai

Aalto University, Finland

russell.lai@aalto.fi

russell-lai.hk

research.cs.aalto.fi/crypto

latticeassumptionzoo.org/vsis/

Kiitos!

References I

[ABCR26] Shweta Agrawal, Kaartik Bhushan, Geoffroy Couteau, and Mahshid Riahinia.
"Post-Quantum Public-Key Pseudorandom Correlation Functions for OT".
In: *CRYPTO 2026*. 2026 (pages 24, 25).

[ACLMT22] 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*. 2022 (pages 20–22).

[ARS24] Damiano Abram, Lawrence Roy, and Peter Scholl.
"Succinct Homomorphic Secret Sharing".
In: *EUROCRYPT 2024*. 2024 (page 24).

[BCFL23] David Balbás, Dario Catalano, Dario Fiore, and Russell W. F. Lai.
"Chainable Functional Commitments for Unbounded-Depth Circuits".
In: *TCC 2023*. 2023 (page 22).

References II

[CLM23] Valerio Cini, Russell W. F. Lai, and Giulio Malavolta.
"Lattice-Based Succinct Arguments from Vanishing Polynomials - (Extended Abstract)".
In: *CRYPTO 2023*. 2023 (pages 8, 10–13, 16, 22).

[DKLW25] Adrien Dubois, Michael Klooß, Russell W. F. Lai, and Ivy K. Y. Woo.
"Lattice-Based Proof-Friendly Signatures from Vanishing Short Integer Solutions".
In: *PKC 2025*. 2025 (pages 20–22, 27).

[FLV23] Ben Fisch, Zeyu Liu, and Psi Vesely.
"Orbweaver: Succinct Linear Functional Commitments from Lattices".
In: *CRYPTO 2023*. 2023 (page 22).

[ILL25] Yuval Ishai, Hanjun Li, and Huijia Lin.
"A Unified Framework for Succinct Garbling from Homomorphic Secret Sharing".
In: *CRYPTO 2025*. 2025 (page 25).

[JL25] Kalle Jyrkinen and Russell W. F. Lai.
"Vanishing Short Integer Solution, Revisited - Reductions, Trapdoors, Homomorphic Signatures for Low-Degree Polynomials".
In: *PKC 2025*. 2025 (pages 19, 31).

References III

[KLNO24] Michael Klooß, Russell W. F. Lai, Ngoc Khanh Nguyen, and Michal Osadnik.
"RoK, Paper, SISsors Toolkit for Lattice-Based Succinct Arguments - (Extended Abstract)".
In: *ASIACRYPT 2024*. 2024 (pages 16, 19).

[KLNO25] Michael Klooß, Russell W. F. Lai, Ngoc Khanh Nguyen, and Michal Osadnik.
"RoK and Roll - Verifier-Efficient Random Projection for $\tilde{O}(\lambda)$-Size Lattice Arguments - (Extended Abstract)".
In: *ASIACRYPT 2025*. 2025 (pages 16, 19).

[KLNOT26] Michael Klooss, Russell W. F. Lai, Ngoc Khanh Nguyen, Michał Osadnik, and Lorenzo Tucci.
RoKoko: Lattice-based Succinct Arguments, a Committed Refinement.
Cryptology ePrint Archive, Paper 2026/575. 2026 (pages 16, 19).

[KLOT25] Shuto Kuriyama, Russell W. F. Lai, Michał Osadnik, and Lorenzo Tucci.
SALSAA – Sumcheck-Aided Lattice-based Succinct Arguments and Applications.
Cryptology ePrint Archive, Report 2025/2124. 2025 (pages 16, 19).

References IV

[OKCLM25] Michal Osadnik, Darya Kaviani, Valerio Cini, Russell W. F. Lai, and Giulio Malavolta.
"Papercraft: Lattice-Based Verifiable Delay Function Implemented".
In: *2025 IEEE Symposium on Security and Privacy*. 2025 (pages 16, 19).

[PS21] Alice Pellet-Mary and Damien Stehlé.
"On the Hardness of the NTRU Problem".
In: *ASIACRYPT 2021*. 2021 (page 32).