Vanishing Short Integer Solution, Revisited

Reductions, Trapdoors, Homomorphic Signatures for Low-Degree Polynomials

Kalle Jyrkinen[1] and **Russell W. F. Lai**[1]

[1] Aalto University

PKC 2025. ePrint: ia.cr/2025/360.

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
  - $\|\mathbf{x}\| \leq \beta$

- (Worst-case to average-case) reduction from SIVP [Ajt96]
  $\implies$ Conjectured post-quantum security
- Trapdoors [GPV08; MP12]
- Many applications, in particular homomorphic signatures [GVW15]
- Generalisation to rings and modules [LPR10; LS15] $\implies$ Concrete efficiency
- More or less the same story for learning with errors (LWE) [Reg05]

Hinted and Structured Lattice Assumptions

- Beyond ring/module structures?
  - Hinted and structured lattice assumptions $\Longrightarrow$
    - Practical advanced primitives
    - New functionalities
  - Hardness poorly understood. More research needed!
- A hinted/structured SIS family:
  - BASIS (basis-augmented SIS) [WW23]
    $\leq$ kRISIS (k-ring inhomogeneous SIS) [ACLMT22]
    $\leq$ vSIS (vanishing SIS) [CLM23]
  - (Strong-)hinted-vSIS [DKLW25] $\leq$ vSIS
- Applications:
  - Proof-friendly signatures (e.g. for practical anonymous credentials) [DKLW25]
  - Functional commitments for polynomials [ACLMT22] and circuits [WW23; BCFL23]
  - Practical lattice-based SNARKs [KLNO24; OKCLM25]
- This work: vSIS Revisited

Hinted and Structured Lattice Assumptions

- Beyond ring/module structures?
  - Hinted and structured lattice assumptions $\Longrightarrow$
    - Practical advanced primitives
    - New functionalities
  - Hardness poorly understood. More research needed!
- A hinted/structured SIS family:
  - BASIS (basis-augmented SIS) [WW23]
    $\leq$ kRISIS (k-ring inhomogeneous SIS) [ACLMT22]
    $\leq$ vSIS (vanishing SIS) [CLM23]
  - (Strong-)hinted-vSIS [DKLW25] $\leq$ vSIS
- Applications:
  - Proof-friendly signatures (e.g. for practical anonymous credentials) [DKLW25]
  - Functional commitments for polynomials [ACLMT22] and circuits [WW23; BCFL23]
  - Practical lattice-based SNARKs [KLNO24; OKCLM25]
- This work: vSIS Revisited

Hinted and Structured Lattice Assumptions

- Beyond ring/module structures?
  - Hinted and structured lattice assumptions $\Longrightarrow$
    - Practical advanced primitives
    - New functionalities
  - Hardness poorly understood. More research needed!
- A hinted/structured SIS family:
  - BASIS (basis-augmented SIS) [WW23]
    $\leq$ kRISIS (k-ring inhomogeneous SIS) [ACLMT22]
    $\leq$ vSIS (vanishing SIS) [CLM23]
  - (Strong-)hinted-vSIS [DKLW25] $\leq$ vSIS
- Applications:
  - Proof-friendly signatures (e.g. for practical anonymous credentials) [DKLW25]
  - Functional commitments for polynomials [ACLMT22] and circuits [WW23; BCFL23]
  - Practical lattice-based SNARKs [KLNO24; OKCLM25]
- This work: vSIS Revisited

Hinted and Structured Lattice Assumptions

- Beyond ring/module structures?
  - Hinted and structured lattice assumptions $\Longrightarrow$
    - Practical advanced primitives
    - New functionalities
  - Hardness poorly understood. More research needed!
- A hinted/structured SIS family:
  - BASIS (basis-augmented SIS) [WW23]
    $\leq$ kRISIS (k-ring inhomogeneous SIS) [ACLMT22]
    $\leq$ vSIS (vanishing SIS) [CLM23]
  - (Strong-)hinted-vSIS [DKLW25] $\leq$ vSIS
- Applications:
  - Proof-friendly signatures (e.g. for practical anonymous credentials) [DKLW25]
  - Functional commitments for polynomials [ACLMT22] and circuits [WW23; BCFL23]
  - Practical lattice-based SNARKs [KLNO24; OKCLM25]
- This work: vSIS Revisited

What is Vanishing SIS? A simple variant

"Simple vSIS"

- Parameter: Degree $d = O(1)$
- Given: Random point $v \bmod q$
- Find: Degree-d polynomial p with short coefficients such that $p(v) = 0 \bmod q$

Overview of Results

1. Reduction

(Worst-case) simple vSIS is as hard as IdSVP (over some class of ideals, with a lot of caveats).

2. Trapdoor

Decision NTRU $\implies$ Trapdoors for simple vSIS.
(Allows sampling of short polynomials evaluating to given values at given points.)

3. Homomorphic Signatures

vSIS trapdoors $\implies$ Fully algebraic homomorphic signatures.
(Not practical (yet?), mostly for demonstrative purposes.)

Setting

Notation	Description	Example 1	Example 2
$\mathfrak{f}$	conductor / cyclotomic index	1	2^{k+1}
$\zeta = \zeta_{\mathfrak{f}}$	a primitive $\mathfrak{f}$-th root of unity	1	$e^{2\pi i/\mathfrak{f}}$
$\mathcal{K} = \mathbb{Q}(\zeta)$	$\mathfrak{f}$-th cyclotomic field	$\mathcal{K} = \mathbb{Q}$	$\mathcal{K} \cong \mathbb{Q}[X]/\langle X^{2^k}+1\rangle$
$\mathcal{R} = \mathbb{Z}[\zeta]$	ring of integers of $\mathcal{K}$	$\mathcal{R} = \mathbb{Z}$	$\mathcal{R} \cong \mathbb{Z}[X]/\langle X^{2^k}+1\rangle$
$\varphi = \varphi(\mathfrak{f})$	degree of $\mathcal{K}$	1	2^k

SIS - Two Points of View

Traditional point of view

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

- 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
  - $\|\mathbf{x}\| \leq \beta$

Function point of view

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

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

SIS - Two Points of View

Traditional point of view

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

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

Function point of view

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

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

Vanishing Short Integer Solution (vSIS)

- Many ways to define, many parameters.
- Here we focus on one of the simplest cases – univariate polynomial vanishing at a single point:

$\underline{\mathsf{vSIS}_{\mathcal{R},d,q,\beta}}$

- Given: $v \xleftarrow{\$} \mathcal{R}_q$
- Find: degree-d polynomial $p \in \mathcal{R}[X]$ such that
  - $p(v) = 0 \bmod q$ and
  - norm of coefficients $\|p\| \leq \beta$

- Think of ring degree $\varphi = \Theta(\lambda)$, polynomial degree $d = O(1)$, $q = \mathrm{poly}(\lambda)$, $\beta = \mathrm{poly}(\lambda)$.
- If $d = 1$, we essentially recover (search-)NTRU, except that NTRU restricts v to be of the form

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

where $f, g \xleftarrow{\$} \mathcal{R}$ are low-norm.

Vanishing Short Integer Solution (vSIS)

- Many ways to define, many parameters.
- Here we focus on one of the simplest cases – univariate polynomial vanishing at a single point:

$\underline{\mathsf{vSIS}_{\mathcal{R},d,q,\beta}}$

- Given: $v \xleftarrow{\$} \mathcal{R}_q$
- Find: degree-d polynomial $p \in \mathcal{R}[X]$ such that
  - $p(v) = 0 \bmod q$ and
  - norm of coefficients $\|p\| \leq \beta$

- Think of ring degree $\varphi = \Theta(\lambda)$, polynomial degree $d = O(1)$, $q = \mathrm{poly}(\lambda)$, $\beta = \mathrm{poly}(\lambda)$.
- If $d = 1$, we essentially recover (search-)NTRU, except that NTRU restricts v to be of the form

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

where $f, g \xleftarrow{\$} \mathcal{R}$ are low-norm.

Vanishing Short Integer Solution (vSIS)

† Many ways to define, many parameters.

† Here we focus on one of the simplest cases – univariate polynomial vanishing at a single point:

$\underline{\mathsf{vSIS}_{\mathcal{R},d,q,\beta}}$

‡ Given: $v \xleftarrow{\$} \mathcal{R}_q$

‡ Find: degree-d polynomial $p \in \mathcal{R}[X]$ such that

‡‡ $p(v) = 0 \bmod q$ and
‡‡ norm of coefficients $\|p\| \leq \beta$

† Think of ring degree $\varphi = \Theta(\lambda)$, polynomial degree $d = O(1)$, $q = \mathrm{poly}(\lambda)$, $\beta = \mathrm{poly}(\lambda)$.

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

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

where $f, g \xleftarrow{\$} \mathcal{R}$ are low-norm.

IdHSVP $\leq$ vSIS

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

Given an ideal $\mathcal{I} \subseteq \mathcal{R}$, find an element $x \in \mathcal{I}$ at most γ times longer than the shortest*, i.e.

$$\|x\| \leq \gamma \cdot \varphi \cdot \mathcal{N}(\mathcal{I})^{1/\varphi}.$$

Theorem: IdHSVP $\leq$ vSIS

Let $d \in \mathbb{N}$ be constant, $\varphi, \theta, n = \text{poly}(\lambda)$,

$$\beta = \varphi^{d+1} \cdot n, \qquad q > \varphi^{d+2} \cdot n^2 \cdot \max\left\{4\theta^{d-1}, 2\varphi^d\right\}, \qquad \gamma \geq \varphi^d \cdot n.$$

Worst-case vSIS$_{\mathcal{R},d,q^d,\beta}$ 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 $\|z^{-1}\|_{\infty} \leq \theta/2$.

IdHSVP $\leq$ vSIS

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

Given an ideal $\mathcal{I} \subseteq \mathcal{R}$, find an element $x \in \mathcal{I}$ at most γ times longer than the shortest*, i.e.

$$\|x\| \leq \gamma \cdot \varphi \cdot \mathcal{N}(\mathcal{I})^{1/\varphi}.$$

Theorem: IdHSVP $\leq$ vSIS

Let $d \in \mathbb{N}$ be constant, $\varphi, \theta, n = \text{poly}(\lambda)$,

$$\beta = \varphi^{d+1} \cdot n, \qquad q > \varphi^{d+2} \cdot n^2 \cdot \max\left\{4\theta^{d-1}, 2\varphi^d\right\}, \qquad \gamma \geq \varphi^d \cdot n.$$

Worst-case vSIS$_{\mathcal{R},d,q^d,\beta}$ 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 $\|z^{-1}\|_{\infty} \leq \theta/2$.

Proof Idea

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

$\mathsf{IdHSVP\text{-}to\text{-}vSIS}^{\mathcal{A}}_{\mathcal{R},d,q^d,\beta}(\mathcal{I})$

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

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

$/\!/\ p(v) = 0 \bmod q^d,\ \|p\| \leq \beta$

return leading coefficient of p

† Let $\alpha \in \mathcal{I} \setminus \{0\}$ be the shortest element. (No need to find explicitly.)

† Examine α / z^d times the leading coefficient p_d of p and show that

$$\alpha \cdot \frac{p_d}{z^d} = \alpha \cdot r$$

for some $r \in \mathcal{R}$.

Proof Idea

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

$\mathsf{IdHSVP\text{-}to\text{-}vSIS}^{\mathcal{A}}_{\mathcal{R},d,q^d,\beta}(\mathcal{I})$

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

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

$/\!/\ p(v) = 0 \bmod q^d,\ \|p\| \leq \beta$

return leading coefficient of p

† Let $\alpha \in \mathcal{I} \setminus \{0\}$ be the shortest element. (No need to find explicitly.)

† Examine α / z^d times the leading coefficient p_d of p and show that

$$\alpha \cdot \frac{p_d}{z^d} = \alpha \cdot r$$

for some $r \in \mathcal{R}$.

Proof Idea

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

$\mathsf{IdHSVP\text{-}to\text{-}vSIS}^{\mathcal{A}}_{\mathcal{R},d,q^d,\beta}(\mathcal{I})$

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

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

$/\!/\ p(v) = 0 \bmod q^d,\ \|p\| \leq \beta$

return leading coefficient of p

† Let $\alpha \in \mathcal{I} \setminus \{0\}$ be the shortest element. (No need to find explicitly.)

† Examine α/z^d times the leading coefficient p_d of p and show that

$$\alpha \cdot \frac{p_d}{z^d} = \alpha \cdot r$$

for some $r \in \mathcal{R}$.

Limitations

- † Multi-point?
- † Multivariate?
- † Beyond constant degree?
- † Remove restrictions on ideal $\mathcal{I}$?
- † Modulus q instead of q^d?
- † Worst-case to average-case?

Limitations

- † Multi-point?
- † Multivariate?
- † Beyond constant degree?
- † Remove restrictions on ideal $\mathcal{I}$?
- † Modulus q instead of q^d?
- † Worst-case to average-case?

Limitations

- † Multi-point?
- † Multivariate?
- † Beyond constant degree?
- † Remove restrictions on ideal $\mathcal{I}$?
- † Modulus q instead of q^d?
- † Worst-case to average-case?

Trapdoors for vSIS

† Recall: Trapdoor for SIS instance $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ allows to sample short vector $\mathbf{x} \in \mathbb{Z}^m$ satisfying

$$\mathbf{A}\mathbf{x} = \mathbf{y} \bmod q$$

for any given $\mathbf{y} \in \mathbb{Z}_q^n$.

† vSIS Trapdoor for a point $v \in \mathcal{R}_q$: Allows to sample short degree-d polynomial $p \in \mathcal{R}[X]$ such that

$$p(v) = r \bmod q$$

for any given $r \in \mathcal{R}_q$.

Result: vSIS Trapdoors

There exists a generalisation of the heuristic PPT NTRU trapdoor algorithm (i.e. $d = 1$) which samples degree-d vSIS trapdoors of near optimal (Gram-Schmidt) norm

$$\|\tilde{\mathbf{T}}\| \approx \beta_d := \sqrt{\varphi} \cdot q^{1/(d+1)}.$$

Trapdoors for vSIS

† Recall: Trapdoor for SIS instance $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ allows to sample short vector $\mathbf{x} \in \mathbb{Z}^m$ satisfying

$$\mathbf{A}\mathbf{x} = \mathbf{y} \bmod q$$

for any given $\mathbf{y} \in \mathbb{Z}_q^n$.

† vSIS Trapdoor for a point $v \in \mathcal{R}_q$: Allows to sample short degree-d polynomial $p \in \mathcal{R}[X]$ such that

$$p(v) = r \bmod q$$

for any given $r \in \mathcal{R}_q$.

Result: vSIS Trapdoors

There exists a generalisation of the heuristic PPT NTRU trapdoor algorithm (i.e. $d = 1$) which samples degree-d vSIS trapdoors of near optimal (Gram-Schmidt) norm

$$\|\tilde{\mathbf{T}}\| \approx \beta_d := \sqrt{\varphi} \cdot q^{1/(d+1)}.$$

Trapdoors for vSIS

† Recall: Trapdoor for SIS instance $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ allows to sample short vector $\mathbf{x} \in \mathbb{Z}^m$ satisfying

$$\mathbf{A}\mathbf{x} = \mathbf{y} \bmod q$$

for any given $\mathbf{y} \in \mathbb{Z}_q^n$.

† vSIS Trapdoor for a point $v \in \mathcal{R}_q$: Allows to sample short degree-d polynomial $p \in \mathcal{R}[X]$ such that

$$p(v) = r \bmod q$$

for any given $r \in \mathcal{R}_q$.

Result: vSIS Trapdoors

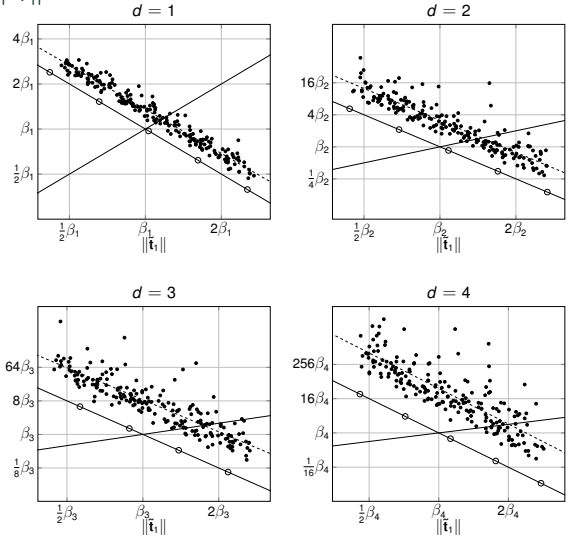
There exists a generalisation of the heuristic PPT NTRU trapdoor algorithm (i.e. $d = 1$) which samples degree-d vSIS trapdoors of near optimal (Gram-Schmidt) norm

$$\|\tilde{\mathbf{T}}\| \approx \beta_d := \sqrt{\varphi} \cdot q^{1/(d+1)}.$$

Empirical values of $\|\tilde{\mathbf{t}}_{d+1}\|$ against $\|\tilde{\mathbf{t}}_1\|$

Parameters:

- $f = 128$
- $q = 1000193 = 2^8 \cdot 3907 + 1$
- $\beta_d = \sqrt{\varphi} \cdot q^{1/(d+1)} \leq \|\tilde{\mathbf{T}}\|$
- Optimal: $\|\tilde{\mathbf{t}}_{d+1}\| \approx \|\tilde{\mathbf{t}}_1\| \approx \beta_d$



Limitations

- Multi-point?
- Multivariate?
- Beyond constant degree?

Homomorphic Signatures from vSIS Trapdoors

To demonstrate the homomorphic properties of vSIS trapdoors, we showcase a homomorphic signatures.

Construction idea:

- $\mathsf{pp} = (r_1, \ldots, r_N) \leftarrow\!\!\$\ \mathcal{R}_q^N$
- $(\mathsf{pk}, \mathsf{sk}) = (v, \mathsf{td}) \leftarrow \mathsf{vSISTrapGen}(\mathcal{R}, d)$
- Signature of $x_i \in \mathcal{R}$: short degree-d polynomial f_i such that

$$f_i(0) = x_i \bmod q \qquad \text{and} \qquad f_i(v_i) = r_i \bmod q$$

- Homomorphic evaluation of polynomial low-norm $g(X_1, \ldots, X_N)$: Return polynomial

$$h = g(f_1, \ldots, f_N)$$

- Verify signature h for (g, y) with $y = g(x_1, \ldots, x_N)$:

$$h(0) = y \bmod q \qquad \text{and} \qquad h(v) = g(r_1, \ldots, r_N) \bmod q$$

Homomorphic Signatures from vSIS Trapdoors

To demonstrate the homomorphic properties of vSIS trapdoors, we showcase a homomorphic signatures.

Construction idea:

- $\mathsf{pp} = (r_1, \ldots, r_N) \leftarrow\!\!\$\ \mathcal{R}_q^N$
- $(\mathsf{pk}, \mathsf{sk}) = (v, \mathsf{td}) \leftarrow \mathsf{vSISTrapGen}(\mathcal{R}, d)$
- Signature of $x_i \in \mathcal{R}$: short degree-d polynomial f_i such that

$$f_i(0) = x_i \bmod q \qquad \text{and} \qquad f_i(v_i) = r_i \bmod q$$

- Homomorphic evaluation of polynomial low-norm $g(X_1, \ldots, X_N)$: Return polynomial

$$h = g(f_1, \ldots, f_N)$$

- Verify signature h for (g, y) with $y = g(x_1, \ldots, x_N)$:

$$h(0) = y \bmod q \qquad \text{and} \qquad h(v) = g(r_1, \ldots, r_N) \bmod q$$

Homomorphic Signatures from vSIS Trapdoors

To demonstrate the homomorphic properties of vSIS trapdoors, we showcase a homomorphic signatures.

Construction idea:

- $\mathsf{pp} = (r_1, \ldots, r_N) \leftarrow\!\!\$\ \mathcal{R}_q^N$
- $(\mathsf{pk}, \mathsf{sk}) = (v, \mathsf{td}) \leftarrow \mathsf{vSISTrapGen}(\mathcal{R}, d)$
- Signature of $x_i \in \mathcal{R}$: short degree-d polynomial f_i such that

$$f_i(0) = x_i \bmod q \qquad \text{and} \qquad f_i(v_i) = r_i \bmod q$$

- Homomorphic evaluation of polynomial low-norm $g(X_1, \ldots, X_N)$: Return polynomial

$$h = g(f_1, \ldots, f_N)$$

- Verify signature h for (g, y) with $y = g(x_1, \ldots, x_N)$:

$$h(0) = y \bmod q \qquad \text{and} \qquad h(v) = g(r_1, \ldots, r_N) \bmod q$$

Homomorphic Signatures from vSIS Trapdoors

To demonstrate the homomorphic properties of vSIS trapdoors, we showcase a homomorphic signatures.

Construction idea:

- $\mathsf{pp} = (r_1, \ldots, r_N) \leftarrow\!\!\$\ \mathcal{R}_q^N$
- $(\mathsf{pk}, \mathsf{sk}) = (v, \mathsf{td}) \leftarrow \mathsf{vSISTrapGen}(\mathcal{R}, d)$
- Signature of $x_i \in \mathcal{R}$: short degree-d polynomial f_i such that

$$f_i(0) = x_i \bmod q \qquad \text{and} \qquad f_i(v_i) = r_i \bmod q$$

- Homomorphic evaluation of polynomial low-norm $g(X_1, \ldots, X_N)$: Return polynomial

$$h = g(f_1, \ldots, f_N)$$

- Verify signature h for (g, y) with $y = g(x_1, \ldots, x_N)$:

$$h(0) = y \bmod q \qquad \text{and} \qquad h(v) = g(r_1, \ldots, r_N) \bmod q$$

Homomorphic Signatures from vSIS Trapdoors

To demonstrate the homomorphic properties of vSIS trapdoors, we showcase a homomorphic signatures.

Construction idea:

- $\mathsf{pp} = (r_1, \ldots, r_N) \leftarrow\!\!\$\ \mathcal{R}_q^N$
- $(\mathsf{pk}, \mathsf{sk}) = (v, \mathsf{td}) \leftarrow \mathsf{vSISTrapGen}(\mathcal{R}, d)$
- Signature of $x_i \in \mathcal{R}$: short degree-d polynomial f_i such that

$$f_i(0) = x_i \bmod q \qquad \text{and} \qquad f_i(v_i) = r_i \bmod q$$

- Homomorphic evaluation of polynomial low-norm $g(X_1, \ldots, X_N)$: Return polynomial

$$h = g(f_1, \ldots, f_N)$$

- Verify signature h for (g, y) with $y = g(x_1, \ldots, x_N)$:

$$h(0) = y \bmod q \qquad \text{and} \qquad h(v) = g(r_1, \ldots, r_N) \bmod q$$

Homomorphic Signatures from vSIS Trapdoors

To demonstrate the homomorphic properties of vSIS trapdoors, we showcase a homomorphic signatures.

Construction idea:

† $\mathsf{pp} = (r_1, \ldots, r_N) \leftarrow\!\!\$\ \mathcal{R}_q^N$

† $(\mathsf{pk}, \mathsf{sk}) = (v, \mathsf{td}) \leftarrow \mathsf{vSISTrapGen}(\mathcal{R}, d)$

† Signature of $x_i \in \mathcal{R}$: short degree-d polynomial f_i such that

$$f_i(0) = x_i \bmod q \qquad \text{and} \qquad f_i(v_i) = r_i \bmod q$$

† Homomorphic evaluation of polynomial low-norm $g(X_1, \ldots, X_N)$: Return polynomial

$$h = g(f_1, \ldots, f_N)$$

† Verify signature h for (g, y) with $y = g(x_1, \ldots, x_N)$:

$$h(0) = y \bmod q \qquad \text{and} \qquad h(v) = g(r_1, \ldots, r_N) \bmod q$$

Homomorphic Signatures from vSIS Trapdoors

Theorem: Homomorphic Signatures from vSIS Trapdoors

Assume decision-NTRU and vSIS with appropriate parameters. There exists a homomorphic signature scheme for low-norm constant-degree multivariate polynomials.

Efficiency bottlenecks:

- Dimension growth: $\deg(f_1 \cdot f_2) = \deg(f_1) + \deg(f_2)$
- Norm growth: Homomorphic evaluation of $g \implies$ norm exponential in $\deg(g)$

Homomorphic Signatures from vSIS Trapdoors

Theorem: Homomorphic Signatures from vSIS Trapdoors

Assume decision-NTRU and vSIS with appropriate parameters. There exists a homomorphic signature scheme for low-norm constant-degree multivariate polynomials.

Efficiency bottlenecks:

- Dimension growth: $\deg(f_1 \cdot f_2) = \deg(f_1) + \deg(f_2)$
- Norm growth: Homomorphic evaluation of $g \implies$ norm exponential in $\deg(g)$

Take Away

Summary

- † IdHSVP $\leq$ Worst-case simple vSIS
- † Trapdoor for simple vSIS
- † Homomorphic signatures from vSIS trapdoor

Open Problems

- † Many open problems in all results – reductions, trapdoors, homomorphic signatures
- † Most important: Reduction for beyond constant-degree?
- † Other hinted/structured assumptions?

Russell W. F. Lai
Aalto University, Finland
russell.lai@aalto.fi
russell-lai.hk
research.cs.aalto.fi/crypto
ia.cr/2025/360

Thank You!

Take Away

Summary

- † IdHSVP $\leq$ Worst-case simple vSIS
- † Trapdoor for simple vSIS
- † Homomorphic signatures from vSIS trapdoor

Open Problems

- † Many open problems in all results – reductions, trapdoors, homomorphic signatures
- † Most important: Reduction for beyond constant-degree?
- † Other hinted/structured assumptions?

Russell W. F. Lai
Aalto University, Finland
russell.lai@aalto.fi
russell-lai.hk
research.cs.aalto.fi/crypto
ia.cr/2025/360

Thank You!

References I

[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, Part II*. 2022 (pages 3–6).

[Ajt96] Miklós Ajtai. “Generating Hard Instances of Lattice Problems (Extended Abstract)”. In: *28th ACM STOC*. 1996 (page 2).

[BCFL23] David Balbás, Dario Catalano, Dario Fiore, and Russell W. F. Lai. “Chainable Functional Commitments for Unbounded-Depth Circuits”. In: *TCC 2023, Part III*. 2023 (pages 3–6).

[CLM23] Valerio Cini, Russell W. F. Lai, and Giulio Malavolta. “Lattice-Based Succinct Arguments from Vanishing Polynomials - (Extended Abstract)”. In: *CRYPTO 2023, Part II*. 2023 (pages 3–6).

[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 3–6).

References II

[GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. “Trapdoors for hard lattices and new cryptographic constructions”. In: *40th ACM STOC*. 2008 (page 2).

[GVW15] Sergey Gorbunov, Vinod Vaikuntanathan, and Daniel Wichs. “Leveled Fully Homomorphic Signatures from Standard Lattices”. In: *47th ACM STOC*. 2015 (page 2).

[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, Part V*. 2024 (pages 3–6).

[LPR10] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. “On Ideal Lattices and Learning with Errors over Rings”. In: *EUROCRYPT 2010*. 2010 (page 2).

[LS15] Adeline Langlois and Damien Stehlé. “Worst-case to average-case reductions for module lattices”. In: *DCC* 3 (2015) (page 2).

[MP12] Daniele Micciancio and Chris Peikert. “Trapdoors for Lattices: Simpler, Tighter, Faster, Smaller”. In: *EUROCRYPT 2012*. 2012 (page 2).

References III

[OKCLM25] Michał Osadnik, Darya Kaviani, Valerio Cini, Russell W. F. Lai, and Giulio Malavolta. “Papercraft: Lattice-based Verifiable Delay Function Implemented”. In: S&P 2025. 2025 (pages 3–6).

[PS21] Alice Pellet-Mary and Damien Stehlé. “On the Hardness of the NTRU Problem”. In: *ASIACRYPT 2021, Part I*. 2021 (pages 17–19).

[Reg05] Oded Regev. “On lattices, learning with errors, random linear codes, and cryptography”. In: *37th ACM STOC*. 2005 (page 2).

[WW23] Hoeteck Wee and David J. Wu. “Succinct Vector, Polynomial, and Functional Commitments from Lattices”. In: *EUROCRYPT 2023, Part III*. 2023 (pages 3–6).