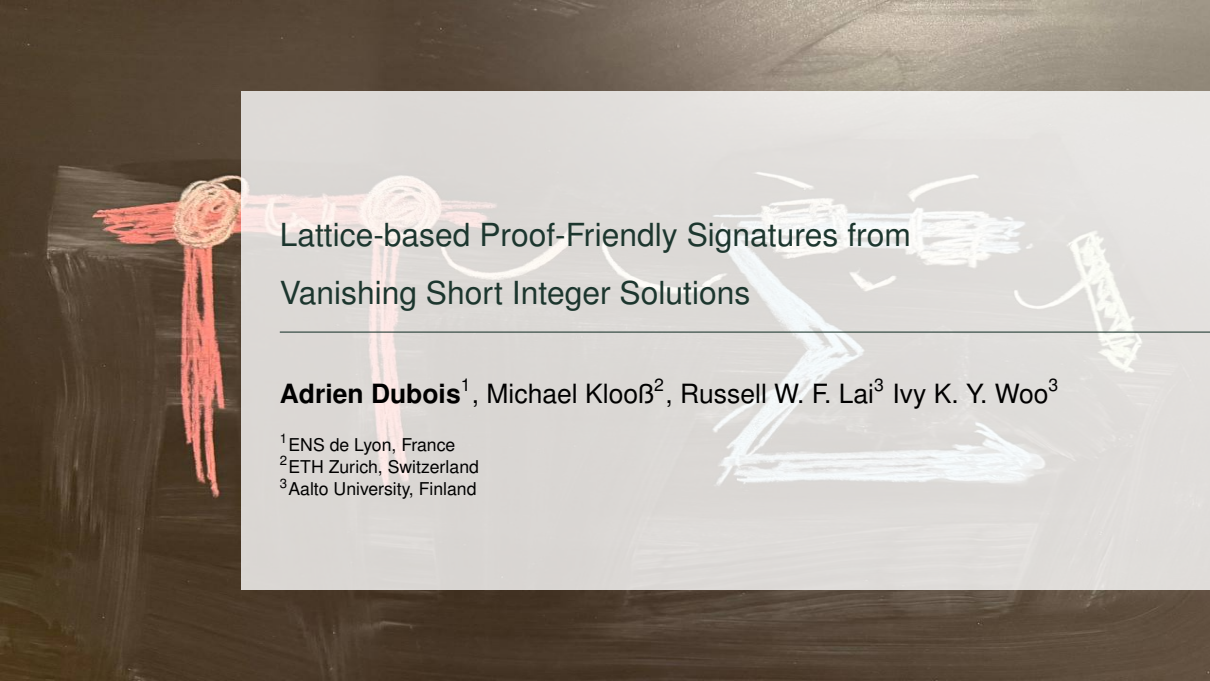
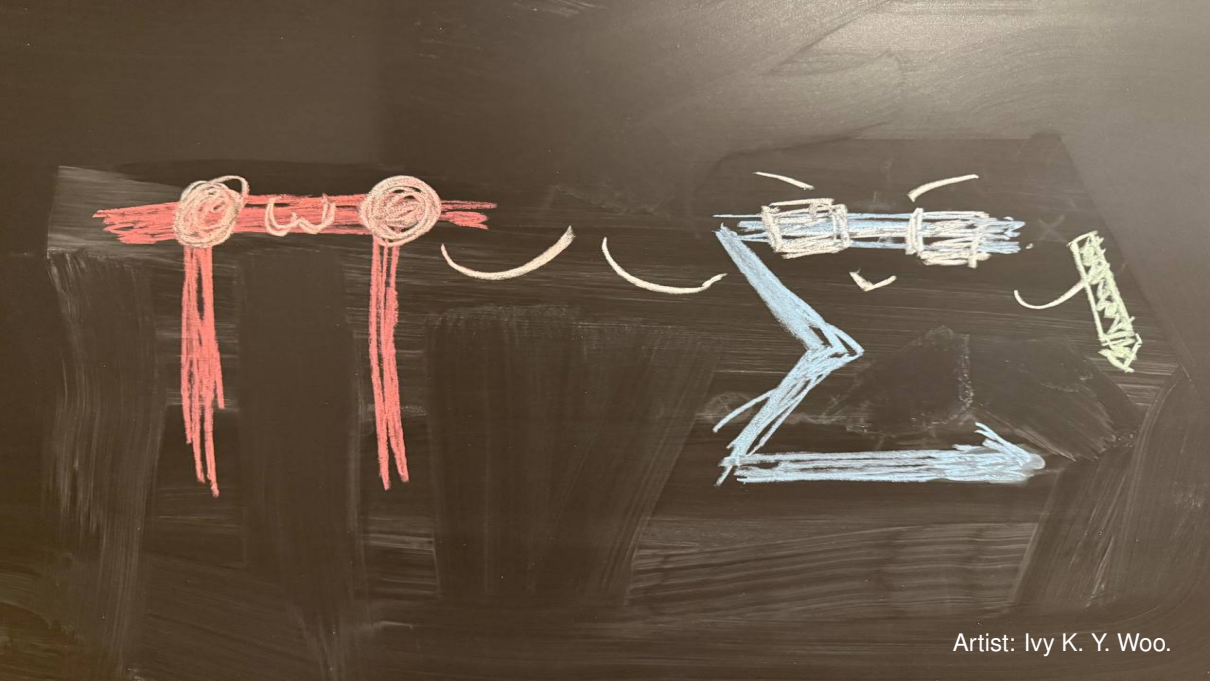


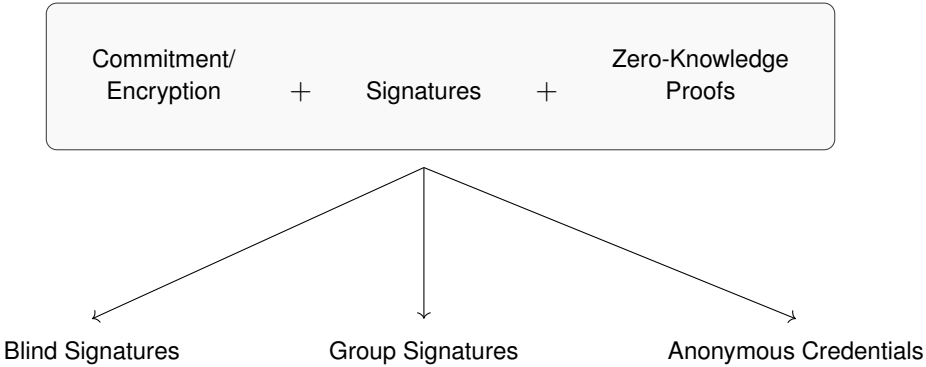
Lattice-based Proof-Friendly Signatures from Vanishing Short Integer Solutions

Adrien Dubois[1], Michael Klooß[2], Russell W. F. Lai[3] Ivy K. Y. Woo[3]

[1]ENS de Lyon, France
[2]ETH Zurich, Switzerland
[3]Aalto University, Finland


Artist: Ivy K. Y. Woo.

Why proof-friendly signatures?



Why proof-friendly signatures?

Commitment/
Encryption $+$  $+$ Zero-Knowledge
Proofs

Efficient
Blind Signatures

Efficient
Group Signatures

Efficient
Anonymous Credentials

Starting point for proof-friendly signatures

Pairing-based Cryptography

Boneh-Boyen (BB) Signatures

Boneh-Boyen-Shacham (BBS) Signatures

Starting point for proof-friendly signatures

Pairing-based Cryptography

Boneh-Boyen (BB) Signatures

Boneh-Boyen-Shacham (BBS) Signatures

Boneh Boyen (BB) signatures (lite version) [BB04]

The simplest pairing-based (proof-friendly) signature scheme.

Setting:

- † Cyclic groups $\mathbb{G}$ and $\mathbb{G}_T$ of prime order q
- † Implicit notation for group elements: $[a] = a \cdot [1]$, $[a]_T = a \cdot [1]_T$, $[a] + [b] = [a + b]$
- † Pairing $\cdot : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$, $[a] \cdot [b] = [ab]_T$

Construction:

$$\text{public key} : [x] \in \mathbb{G}$$
$$\text{secret key} : x \in \mathbb{Z}_q$$
$$\text{signature of } m \in \mathbb{Z}_q : [u] = \left[\frac{1}{x - m}\right] \in \mathbb{G}$$

Verification:

$$([x] - [1] \cdot m) \cdot [u] \stackrel{?}{=} [1]_T$$

Boneh Boyen (BB) signatures (lite version) [BB04]

The simplest pairing-based (proof-friendly) signature scheme.

Setting:

- † Cyclic groups $\mathbb{G}$ and $\mathbb{G}_T$ of prime order q
- † Implicit notation for group elements: $[a] = a \cdot [1]$, $[a]_T = a \cdot [1]_T$, $[a] + [b] = [a + b]$
- † Pairing $\cdot : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$, $[a] \cdot [b] = [ab]_T$

Construction:

$$\text{public key} : [x] \in \mathbb{G}$$

$$\text{secret key} : x \in \mathbb{Z}_q$$

$$\text{signature of } m \in \mathbb{Z}_q : [u] = \left[\frac{1}{x - m}\right] \in \mathbb{G}$$

Verification:

$$([x] - [1] \cdot m) \cdot [u] \stackrel{?}{=} [1]_T$$

Boneh Boyen (BB) signatures (lite version) [BB04]

The simplest pairing-based (proof-friendly) signature scheme.

Setting:

- Cyclic groups $\mathbb{G}$ and $\mathbb{G}_T$ of prime order q
- Implicit notation for group elements: $[a] = a \cdot [1]$, $[a]_T = a \cdot [1]_T$, $[a] + [b] = [a + b]$
- Pairing $\cdot : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$, $[a] \cdot [b] = [ab]_T$

Construction:

$$\text{public key} : [x] \in \mathbb{G}$$
$$\text{secret key} : x \in \mathbb{Z}_q$$
$$\text{signature of } m \in \mathbb{Z}_q : [u] = \left[\frac{1}{x - m}\right] \in \mathbb{G}$$

Verification:

$$([x] - [1] \cdot m) \cdot [u] \stackrel{?}{=} [1]_T$$

Boneh Boyen Shacham (BBS) signatures [BBS04]

A popular pairing-based proof-friendly signature scheme.
Extension of BB signatures which allows to **sign committed messages**.

Construction:

$$\text{public key} : [\mathbf{c}] \in \mathbb{G}^{\ell}, [d] \in \mathbb{G}, [x] \in \mathbb{G}$$
$$\text{secret key} : x \in \mathbb{Z}_q$$
$$\text{signature of } \mathbf{m} \in \mathbb{Z}_q^{\ell} : [u] \in \mathbb{G}, t \in \mathbb{Z}_q \text{ where } [u] = \frac{\langle [\mathbf{c}], \mathbf{m} \rangle + [d]}{x - t}$$

Verification:

$$([x] - [1] \cdot t) \cdot [u] \stackrel{?}{=} \langle [\mathbf{c}], \mathbf{m} \rangle + [d]$$

Verification is a single pairing equation, i.e. quadratic in $(\mathbf{m}, [u], t)$
– very friendly to the Groth-Sahai proof system.

Boneh Boyen Shacham (BBS) signatures [BBS04]

A popular pairing-based proof-friendly signature scheme.
Extension of BB signatures which allows to **sign committed messages**.

Construction:

$$\text{public key} : [\mathbf{c}] \in \mathbb{G}^{\ell}, [d] \in \mathbb{G}, [x] \in \mathbb{G}$$
$$\text{secret key} : x \in \mathbb{Z}_q$$
$$\text{signature of } \mathbf{m} \in \mathbb{Z}_q^{\ell} : [u] \in \mathbb{G}, t \in \mathbb{Z}_q \text{ where } [u] = \frac{\langle [\mathbf{c}], \mathbf{m} \rangle + [d]}{x - t}$$

Verification:

$$([x] - [1] \cdot t) \cdot [u] \stackrel{?}{=} \langle [\mathbf{c}], \mathbf{m} \rangle + [d]$$

Verification is a single pairing equation, i.e. quadratic in $(\mathbf{m}, [u], t)$
– very friendly to the Groth-Sahai proof system.

Boneh Boyen Shacham (BBS) signatures [BBS04]

A popular pairing-based proof-friendly signature scheme.
Extension of BB signatures which allows to **sign committed messages**.

Construction:

$$\text{public key} : [\mathbf{c}] \in \mathbb{G}^{\ell}, [d] \in \mathbb{G}, [x] \in \mathbb{G}$$
$$\text{secret key} : x \in \mathbb{Z}_q$$
$$\text{signature of } \mathbf{m} \in \mathbb{Z}_q^{\ell} : [u] \in \mathbb{G}, t \in \mathbb{Z}_q \text{ where } [u] = \frac{\langle [\mathbf{c}], \mathbf{m} \rangle + [d]}{x - t}$$

Verification:

$$([x] - [1] \cdot t) \cdot [u] \stackrel{?}{=} \langle [\mathbf{c}], \mathbf{m} \rangle + [d]$$

Verification is a single pairing equation, i.e. quadratic in $(\mathbf{m}, [u], t)$
– very friendly to the Groth-Sahai proof system.

Lattice-based proof-friendly signatures

Q: What is “proof-friendly” for lattice-based signatures?

A: Verification is checking bounded-norm satisfiability of system of linear and low-degree polynomials
$\rightsquigarrow$ very friendly to e.g. the [LNP22] proof system.

Jeudy, Roux-Langlois and Sanders [JRS23]:

$$(\mathbf{A} \mid \mathbf{B} + t \cdot \mathbf{G}) \cdot \mathbf{u} \stackrel{?}{=} \mathbf{C} \cdot \mathbf{m} + \mathbf{d} \bmod q$$
$$\wedge \quad \|\mathbf{m}\|, \|\mathbf{u}\| \stackrel{?}{\leq} \beta \quad \wedge \quad t \stackrel{?}{\in} \mathcal{T}$$

$\rightarrow$ Require gadget trapdoor
$\Longrightarrow$ Large (e.g. $>$ 100 kB) signature size

Bootle, Lyubashevsky, Nguyen and Sorniotti [BLNS23]:

$$\mathbf{A} \cdot \mathbf{u} \stackrel{?}{=} \mathbf{C} \cdot \mathbf{m} + f(t) \bmod q$$
$$\wedge \quad \|\mathbf{m}\|, \|\mathbf{u}\| \stackrel{?}{\leq} \beta \quad \wedge \quad t \stackrel{?}{\in} \mathcal{T}$$

$\rightarrow$ Security critically depends on choice of f
$\rightarrow$ [BLNS23] focuses on $f =$ binary decomposition

Lattice-based proof-friendly signatures

Q: What is "proof-friendly" for lattice-based signatures?

A: Verification is checking bounded-norm satisfiability of system of linear and low-degree polynomials
$\rightsquigarrow$ very friendly to e.g. the [LNP22] proof system.

Jeudy, Roux-Langlois and Sanders [JRS23]:

$$(\mathbf{A} \mid \mathbf{B} + t \cdot \mathbf{G}) \cdot \mathbf{u} \stackrel{?}{=} \mathbf{C} \cdot \mathbf{m} + \mathbf{d} \bmod q$$
$$\wedge \quad \|\mathbf{m}\|, \|\mathbf{u}\| \stackrel{?}{\leq} \beta \quad \wedge \quad t \stackrel{?}{\in} \mathcal{T}$$

$\rightarrow$ Require gadget trapdoor
$\Longrightarrow$ Large (e.g. $>$ 100 kB) signature size

Bootle, Lyubashevsky, Nguyen and Sorniotti [BLNS23]:

$$\mathbf{A} \cdot \mathbf{u} \stackrel{?}{=} \mathbf{C} \cdot \mathbf{m} + f(t) \bmod q$$
$$\wedge \quad \|\mathbf{m}\|, \|\mathbf{u}\| \stackrel{?}{\leq} \beta \quad \wedge \quad t \stackrel{?}{\in} \mathcal{T}$$

$\rightarrow$ Security critically depends on choice of f
$\rightarrow$ [BLNS23] focuses on f = binary decomposition

Lattice-based proof-friendly signatures

Q: What is “proof-friendly” for lattice-based signatures?

A: Verification is checking bounded-norm satisfiability of system of linear and low-degree polynomials
$\rightsquigarrow$ very friendly to e.g. the [LNP22] proof system.

Jeudy, Roux-Langlois and Sanders [JRS23]:

$$(\mathbf{A} \mid \mathbf{B} + t \cdot \mathbf{G}) \cdot \mathbf{u} \stackrel{?}{=} \mathbf{C} \cdot \mathbf{m} + \mathbf{d} \bmod q$$
$$\wedge \quad \|\mathbf{m}\|, \|\mathbf{u}\| \stackrel{?}{\leq} \beta \quad \wedge \quad t \stackrel{?}{\in} \mathcal{T}$$

$\rightarrow$ Require gadget trapdoor
$\Longrightarrow$ Large (e.g. $>$ 100 kB) signature size

Bootle, Lyubashevsky, Nguyen and Sorniotti [BLNS23]:

$$\mathbf{A} \cdot \mathbf{u} \stackrel{?}{=} \mathbf{C} \cdot \mathbf{m} + f(t) \bmod q$$
$$\wedge \quad \|\mathbf{m}\|, \|\mathbf{u}\| \stackrel{?}{\leq} \beta \quad \wedge \quad t \stackrel{?}{\in} \mathcal{T}$$

$\rightarrow$ Security critically depends on choice of f
$\rightarrow$ [BLNS23] focuses on $f =$ binary decomposition

Lattice-based proof-friendly signatures

Q: What is "proof-friendly" for lattice-based signatures?

A: Verification is checking bounded-norm satisfiability of system of linear and low-degree polynomials
$\rightsquigarrow$ very friendly to e.g. the [LNP22] proof system.

Jeudy, Roux-Langlois and Sanders [JRS23]:

$$(\mathbf{A} \mid \mathbf{B} + t \cdot \mathbf{G}) \cdot \mathbf{u} \stackrel{?}{=} \mathbf{C} \cdot \mathbf{m} + \mathbf{d} \bmod q$$
$$\wedge \quad \|\mathbf{m}\|, \|\mathbf{u}\| \stackrel{?}{\leq} \beta \quad \wedge \quad t \stackrel{?}{\in} \mathcal{T}$$

$\rightarrow$ Require gadget trapdoor
$\Longrightarrow$ Large (e.g. $>$ 100 kB) signature size

Bootle, Lyubashevsky, Nguyen and Sorniotti [BLNS23]:

$$\mathbf{A} \cdot \mathbf{u} \stackrel{?}{=} \mathbf{C} \cdot \mathbf{m} + f(t) \bmod q$$
$$\wedge \quad \|\mathbf{m}\|, \|\mathbf{u}\| \stackrel{?}{\leq} \beta \quad \wedge \quad t \stackrel{?}{\in} \mathcal{T}$$

$\rightarrow$ Security critically depends on choice of f
$\rightarrow$ [BLNS23] focuses on $f =$ binary decomposition

Lattice-based proof-friendly signatures

Q: What is "proof-friendly" for lattice-based signatures?

A: Verification is checking bounded-norm satisfiability of system of linear and low-degree polynomials
$\rightsquigarrow$ very friendly to e.g. the [LNP22] proof system.

Jeudy, Roux-Langlois and Sanders [JRS23]:

$$(\mathbf{A} \mid \mathbf{B} + t \cdot \mathbf{G}) \cdot \mathbf{u} \stackrel{?}{=} \mathbf{C} \cdot \mathbf{m} + \mathbf{d} \bmod q$$
$$\wedge \quad \|\mathbf{m}\|, \|\mathbf{u}\| \stackrel{?}{\leq} \beta \quad \wedge \quad t \stackrel{?}{\in} \mathcal{T}$$

$\rightarrow$ Require gadget trapdoor
$\Longrightarrow$ Large (e.g. $>$ 100 kB) signature size

Bootle, Lyubashevsky, Nguyen and Sorniotti [BLNS23]:

$$\mathbf{A} \cdot \mathbf{u} \stackrel{?}{=} \mathbf{C} \cdot \mathbf{m} + f(t) \bmod q$$
$$\wedge \quad \|\mathbf{m}\|, \|\mathbf{u}\| \stackrel{?}{\leq} \beta \quad \wedge \quad t \stackrel{?}{\in} \mathcal{T}$$

$\rightarrow$ Security critically depends on choice of f
$\rightarrow$ [BLNS23] focuses on $f =$ binary decomposition

More proof-friendly signatures?

Gist:

- Lattice-based proof-friendly signatures are scarce
- Idea: Following [ACLMT22], translate BB/BBS to lattice setting!
- Goal: Efficient designs and need from new plausible assumptions

Roadmap:

- Vanishing short integer solution (vSIS) [CLM23]
- Strong hinted vSIS (s-Hint-vSIS)
- (Selectively secure) signatures from s-Hint-vSIS
- Connection with ISIS_f [BLNS23] and upgrade to adaptive security

More proof-friendly signatures?

Gist:

- Lattice-based proof-friendly signatures are scarce
- Idea: Following [ACLMT22], translate BB/BBS to lattice setting!
- Goal: Efficient designs and need from new plausible assumptions

Roadmap:

- Vanishing short integer solution (vSIS) [CLM23]
- Strong hinted vSIS (s-Hint-vSIS)
- (Selectively secure) signatures from s-Hint-vSIS
- Connection with ISIS_f [BLNS23] and upgrade to adaptive security

SIS

† **Input:** matrix $\mathbf{A} \leftarrow\!\!\$\ \mathbb{Z}_q^{n \times m}$

† **Output:** vector $\mathbf{u}^* \in \mathbb{Z}^m$

† **Winning condition:**

$$\begin{pmatrix} \\ \mathbf{A} \\ \\ \end{pmatrix} \begin{pmatrix} \\ \mathbf{u}^* \\ \\ \end{pmatrix} = \begin{pmatrix} \\ \mathbf{0} \\ \\ \end{pmatrix} \bmod q \quad \text{such that} \quad 0 < \|\mathbf{u}^*\| \leq \beta$$

SIS to vSIS

$$\begin{pmatrix} & \mathbf{A} & \end{pmatrix} \begin{pmatrix} u_1^* \\ u_2^* \\ \vdots \\ u_m^* \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \bmod q$$

SIS to vSIS

$$\begin{pmatrix} a_{1,1} & \cdots & a_{1,m} \\ a_{2,1} & \cdots & a_{2,m} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,m} \end{pmatrix} \begin{pmatrix} u_1^* \\ u_2^* \\ \vdots \\ u_m^* \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \bmod q$$

SIS to vSIS

$$\begin{pmatrix} a_{1,1}^2 & \cdots & a_{1,m}^2 \\ a_{2,1}^2 & \cdots & a_{2,m}^2 \\ \vdots & \ddots & \vdots \\ a_{n,1}^2 & \cdots & a_{n,m}^2 \end{pmatrix} \begin{pmatrix} u_1^* \\ u_2^* \\ \vdots \\ u_m^* \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \bmod q$$

SIS to vSIS

Uniformly sampled $\mathbf{A} = \begin{pmatrix} \mathbf{a}_1^T \\ \vdots \\ \mathbf{a}_n^T \end{pmatrix} \in \mathbb{Z}_q^{n \times m}$

Set of m-variate rational functions $\mathcal{F} = \{f_1, \cdots, f_k\}$.

$$\begin{pmatrix} f_1(\mathbf{a}_1) & \cdots & f_k(\mathbf{a}_1) \\ f_1(\mathbf{a}_2) & \cdots & f_k(\mathbf{a}_2) \\ \vdots & \ddots & \vdots \\ f_1(\mathbf{a}_n) & \cdots & f_k(\mathbf{a}_n) \end{pmatrix} \begin{pmatrix} u_1^* \\ u_2^* \\ \vdots \\ u_m^* \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \bmod q$$

Vanishing short integer solution (vSIS)

Proposed by Cini, Lai and Malavolta [CLM23]

- **Parameters:** $\mathcal{R}$, n, m, q, β,
  family $\mathcal{F}$ of m-variate rational functions over $\mathcal{R}$
- **Input:** matrix $\mathbf{A} \leftarrow\!\!\$\ \mathcal{R}_q^{n \times m}$
- **Output:** vector $\mathbf{u}^* \in \mathcal{R}^{\mathcal{F}}$
- **Winning conditions:**
  - For each row $\mathbf{a}_i$ of $\mathbf{A}$,
    it holds that $\sum_{f \in \mathcal{F}} f(\mathbf{a}_i) \cdot u_f^* = \mathcal{F}(\mathbf{a}_i) \cdot \mathbf{u}^* = 0 \bmod q$
  - $0 < \|\mathbf{u}^*\| \leq \beta$

For trivial $\mathcal{F}$ where $\mathcal{F}(\mathbf{A}) = \mathbf{A}$, we recover the standard SIS problem (with parameters $\mathcal{R}, n, m, q$).

Vanishing short integer solution (vSIS)

Proposed by Cini, Lai and Malavolta [CLM23]

- **Parameters:** $\mathcal{R}$, n, m, q, β,
  family $\mathcal{F}$ of m-variate rational functions over $\mathcal{R}$
- **Input:** matrix $\mathbf{A} \leftarrow\!\!\$\ \mathcal{R}_q^{n \times m}$
- **Output:** vector $\mathbf{u}^* \in \mathcal{R}^{\mathcal{F}}$
- **Winning conditions:**
  - For each row $\mathbf{a}_i$ of $\mathbf{A}$,
    it holds that $\sum_{f \in \mathcal{F}} f(\mathbf{a}_i) \cdot u_f^* = \mathcal{F}(\mathbf{a}_i) \cdot \mathbf{u}^* = 0 \bmod q$
  - $0 < \|\mathbf{u}^*\| \leq \beta$

For trivial $\mathcal{F}$ where $\mathcal{F}(\mathbf{A}) = \mathbf{A}$, we recover the standard SIS problem (with parameters $\mathcal{R}$, n, m, q).

Strong hinted vSIS (s-Hint-vSIS)

† **Parameters:** $\mathcal{R}$, n, m, q, β, s, Q,
families $\mathcal{F}, \mathcal{G}, \mathcal{H}$ of m-variate rational functions over $\mathcal{R}$

† **Input:** matrix $\mathbf{A} \leftarrow\!\$\ \mathcal{R}_q^{n \times m}$

† **Hints:** On selectively choosen queries subset $\{h_1, .., h_Q\} \subseteq_Q \mathcal{H}$, the hints are $\mathbf{u}_1, .., \mathbf{u}_Q$ such that

‡ For each $j \in [m]$, $\mathcal{F}(\mathbf{a}_j) \cdot \mathbf{u}_i = h_i(\mathbf{a}_j) \bmod q$ (or more compactly $\mathcal{F}(\mathbf{A}) \cdot \mathbf{u}_i = h_i(\mathbf{A})$)

‡ $0 < \|\mathbf{u}_i\| \leq \beta$

† **Output:** vector $\mathbf{u}^* \in \mathcal{R}^{\mathcal{F}}$ and $g^* \in \mathcal{G} \setminus \mathcal{Q}$

† **Winning conditions:**

‡ $\mathcal{F}(\mathbf{A}) \cdot \mathbf{u}^* = g^*(\mathbf{A}) \bmod q$

‡ $0 < \|\mathbf{u}^*\| \leq \beta$

"Strong" in the sense of e.g. Q-strong Diffie Hellman (Q-SDH), i.e. $\mathcal{A}$ can choose g^* adaptively.

Strong hinted vSIS (s-Hint-vSIS)

† **Parameters:** $\mathcal{R}$, n, m, q, β, s, Q,
families $\mathcal{F}, \mathcal{G}, \mathcal{H}$ of m-variate rational functions over $\mathcal{R}$

† **Input:** matrix $\mathbf{A} \leftarrow\!\!\$\ \mathcal{R}_q^{n \times m}$

† **Hints:** On selectively choosen queries subset $\{h_1, .., h_Q\} \subseteq_Q \mathcal{H}$, the hints are $\mathbf{u}_1, .., \mathbf{u}_Q$ such that

‡ For each $j \in [m]$, $\mathcal{F}(\mathbf{a}_j) \cdot \mathbf{u}_i = h_i(\mathbf{a}_j) \bmod q$ $\big($ or more compactly $\mathcal{F}(\mathbf{A}) \cdot \mathbf{u}_i = h_i(\mathbf{A})\big)$

‡ $0 < \|\mathbf{u}_i\| \leq \beta$

† **Output:** vector $\mathbf{u}^* \in \mathcal{R}^{\mathcal{F}}$ and $g^* \in \mathcal{G} \setminus \mathcal{Q}$

† **Winning conditions:**

‡ $\mathcal{F}(\mathbf{A}) \cdot \mathbf{u}^* = g^*(\mathbf{A}) \bmod q$

‡ $0 < \|\mathbf{u}^*\| \leq \beta$

"Strong" in the sense of e.g. Q-strong Diffie Hellman (Q-SDH), i.e. $\mathcal{A}$ can choose g^* adaptively.

Strong hinted vSIS (s-Hint-vSIS)

† **Parameters:** $\mathcal{R}$, n, m, q, β, s, Q,
families $\mathcal{F}, \mathcal{G}, \mathcal{H}$ of m-variate rational functions over $\mathcal{R}$

† **Input:** matrix $\mathbf{A} \leftarrow\!\!\$\ \mathcal{R}_q^{n \times m}$

† **Hints:** On selectively choosen queries subset $\{h_1, .., h_Q\} \subseteq_Q \mathcal{H}$, the hints are $\mathbf{u}_1, .., \mathbf{u}_Q$ such that

‡ For each $j \in [m]$, $\mathcal{F}(\mathbf{a}_j) \cdot \mathbf{u}_i = h_i(\mathbf{a}_j) \bmod q$ $\big($ or more compactly $\mathcal{F}(\mathbf{A}) \cdot \mathbf{u}_i = h_i(\mathbf{A})\big)$

‡ $0 < \|\mathbf{u}_i\| \leq \beta$

† **Output:** vector $\mathbf{u}^* \in \mathcal{R}^{\mathcal{F}}$ and $g^* \in \mathcal{G} \setminus \mathcal{Q}$

† **Winning conditions:**

‡ $\mathcal{F}(\mathbf{A}) \cdot \mathbf{u}^* = g^*(\mathbf{A}) \bmod q$

‡ $0 < \|\mathbf{u}^*\| \leq \beta$

"Strong" in the sense of e.g. Q-strong Diffie Hellman (Q-SDH), i.e. $\mathcal{A}$ can choose g^* adaptively.

Strong hinted vSIS (s-Hint-vSIS)

† **Parameters:** $\mathcal{R}$, n, m, q, β, s, Q,
families $\mathcal{F}, \mathcal{G}, \mathcal{H}$ of m-variate rational functions over $\mathcal{R}$

† **Input:** matrix $\mathbf{A} \leftarrow\!\!\$\ \mathcal{R}_q^{n \times m}$

† **Hints:** On selectively choosen queries subset $\{h_1, .., h_Q\} \subseteq_Q \mathcal{H}$, the hints are $\mathbf{u}_1, .., \mathbf{u}_Q$ such that

‡ For each $j \in [m]$, $\mathcal{F}(\mathbf{a}_j) \cdot \mathbf{u}_i = h_i(\mathbf{a}_j) \bmod q$ $\big($ or more compactly $\mathcal{F}(\mathbf{A}) \cdot \mathbf{u}_i = h_i(\mathbf{A})\big)$

‡ $0 < \|\mathbf{u}_i\| \leq \beta$

† **Output:** vector $\mathbf{u}^* \in \mathcal{R}^{\mathcal{F}}$ and $g^* \in \mathcal{G} \setminus \mathcal{Q}$

† **Winning conditions:**

‡ $\mathcal{F}(\mathbf{A}) \cdot \mathbf{u}^* = g^*(\mathbf{A}) \bmod q$

‡ $0 < \|\mathbf{u}^*\| \leq \beta$

"Strong" in the sense of e.g. Q-strong Diffie Hellman (Q-SDH), i.e. $\mathcal{A}$ can choose g^* adaptively.

Strong hinted vSIS (s-Hint-vSIS)

† **Parameters:** $\mathcal{R}$, n, m, q, β, s, Q,
families $\mathcal{F}, \mathcal{G}, \mathcal{H}$ of m-variate rational functions over $\mathcal{R}$

† **Input:** matrix $\mathbf{A} \leftarrow\!\!\$\ \mathcal{R}_q^{n \times m}$

† **Hints:** On selectively choosen queries subset $\{h_1, .., h_Q\} \subseteq_Q \mathcal{H}$, the hints are $\mathbf{u}_1, .., \mathbf{u}_Q$ such that

‡ For each $j \in [m]$, $\mathcal{F}(\mathbf{a}_j) \cdot \mathbf{u}_i = h_i(\mathbf{a}_j) \bmod q$ $\big($ or more compactly $\mathcal{F}(\mathbf{A}) \cdot \mathbf{u}_i = h_i(\mathbf{A})\big)$

‡ $0 < \|\mathbf{u}_i\| \leq \beta$

† **Output:** vector $\mathbf{u}^* \in \mathcal{R}^{\mathcal{F}}$ and $g^* \in \mathcal{G} \setminus \mathcal{Q}$

† **Winning conditions:**

‡ $\mathcal{F}(\mathbf{A}) \cdot \mathbf{u}^* = g^*(\mathbf{A}) \bmod q$

‡ $0 < \|\mathbf{u}^*\| \leq \beta$

"Strong" in the sense of e.g. Q-strong Diffie Hellman (Q-SDH), i.e. $\mathcal{A}$ can choose g^* adaptively.

How plausible is s-Hint-vSIS**?**

Heuristic: Strong Linear Independance

If $\mathcal{F}$ is "strongly linearly independent", i.e. (roughly) for any non-zero $\mathbf{u} \in \mathcal{R}^{\mathcal{F}}$

$$\Pr\left[\mathcal{F}(\mathbf{A}) \cdot \mathbf{u} = \mathbf{0} \bmod q \;\middle|\; \mathbf{A} \xleftarrow{\$} \mathcal{R}_q^{n \times m}\right] \leq \mathsf{negl}(\lambda),$$

then the vSIS assumption for $\mathcal{F}$ holds.

Signatures from strong hinted vSIS

- For each message μ and randomness τ, define rational function $h_{\mu,\tau}$.
  Example: $h_{\mu,\tau}(\mathbf{B}) = \frac{1}{\tau-\mu}$
- $\mathcal{F}(\mathbf{A}) = \mathbf{A}$, $\mathcal{H} = \{h_{\mu,\tau}\}_{\mu,\tau}$, $\mathcal{G} = \mathcal{H} \cup \{0\}$.
- **Construction:**
  - Public key: $\mathsf{pk} = \mathbf{A} \in \mathcal{R}_q^{n\times m}, \mathbf{B} \in \mathcal{R}_q^{n\times \ell}$
  - Secret key: $\mathsf{sk} =$ trapdoor of $\mathbf{A}$
  - Signature of μ: randomness $\tau \leftarrow\!\$\ \mathcal{T}$ and vector $\mathbf{u} \in \mathcal{R}^m$ where

$$\mathbf{A}\cdot\mathbf{u} = h_{\mu,\tau}(\mathbf{B}) \bmod q \ \ \wedge \ \ \|\mathbf{u}\| \le \beta.$$

Theorem

Under the s-Hint-vSIS assumption for $(\mathcal{F},\mathcal{G},\mathcal{H})$ the signature scheme is strongly existentially unforgeable under selective message attack (sEUF-SMA).

Signatures from strong hinted vSIS

† For each message μ and randomness τ, define rational function $h_{\mu,\tau}$.
Example: $h_{\mu,\tau}(\mathbf{B}) = \frac{1}{\tau-\mu}$

† $\mathcal{F}(\mathbf{A}) = \mathbf{A}$, $\mathcal{H} = \{h_{\mu,\tau}\}_{\mu,\tau}$, $\mathcal{G} = \mathcal{H} \cup \{0\}$.

† **Construction:**

‡ Public key: $\mathsf{pk} = \mathbf{A} \in \mathcal{R}_q^{n\times m}$, $\mathbf{B} \in \mathcal{R}_q^{n\times \ell}$

‡ Secret key: sk = trapdoor of $\mathbf{A}$

‡ Signature of μ: randomness $\tau \leftarrow\!\$\ \mathcal{T}$ and vector $\mathbf{u} \in \mathcal{R}^m$ where

$$\mathbf{A}\cdot\mathbf{u} = h_{\mu,\tau}(\mathbf{B}) \bmod q \ \wedge\ \|\mathbf{u}\| \le \beta.$$

Theorem

Under the s-Hint-vSIS assumption for $(\mathcal{F},\mathcal{G},\mathcal{H})$ the signature scheme is strongly existentially unforgeable under selective message attack (sEUF-SMA).

Signatures from strong hinted vSIS

† For each message μ and randomness τ, define rational function $h_{\mu,\tau}$.
Example: $h_{\mu,\tau}(\mathbf{B}) = \frac{1}{\tau-\mu}$

† $\mathcal{F}(\mathbf{A}) = \mathbf{A}$, $\mathcal{H} = \{h_{\mu,\tau}\}_{\mu,\tau}$, $\mathcal{G} = \mathcal{H} \cup \{0\}$.

† **Construction:**

‡ Public key: $\mathsf{pk} = \mathbf{A} \in \mathcal{R}_q^{n\times m}$, $\mathbf{B} \in \mathcal{R}_q^{n\times \ell}$

‡ Secret key: sk = trapdoor of $\mathbf{A}$

‡ Signature of μ: randomness $\tau \leftarrow\!\$\ \mathcal{T}$ and vector $\mathbf{u} \in \mathcal{R}^m$ where

$$\mathbf{A} \cdot \mathbf{u} = h_{\mu,\tau}(\mathbf{B}) \bmod q \ \ \wedge \ \ \|\mathbf{u}\| \leq \beta.$$

Theorem

Under the s-Hint-vSIS assumption for $(\mathcal{F}, \mathcal{G}, \mathcal{H})$ the signature scheme is strongly existentially unforgeable under selective message attack (sEUF-SMA).

Example instantiations

Instantiations obtained by translating Boneh Boyen (BB) and Boneh Boyen Shacham (BBS):

	Message μ	Randomness τ	Function $h_{\mu,\tau}$
BB-lite	m	-	$\frac{1}{b-m}$
BB-full	$\mathbf{m}$	-	$\frac{1}{\mathbf{c}^\top\mathbf{m}+d}$
BBS	$\mathbf{m}$	t	$\frac{\mathbf{c}^\top\mathbf{m}+d}{b-t}$
BB-tran	$\mathbf{m}$	t	$\mathbf{c}^\top\mathbf{m} + \frac{1}{b-t}$

Example instantiations

Instantiations obtained by translating Boneh Boyen (BB) and Boneh Boyen Shacham (BBS):

	Message μ	Randomness τ	Function $h_{\mu,\tau}$
BB-lite	m	-	$\frac{1}{b-m}$
BB-full	$\mathbf{m}$	-	$\frac{1}{\mathbf{c}^\top\mathbf{m}+d}$
BBS	$\mathbf{m}$	t	$\frac{\mathbf{c}^\top\mathbf{m}+d}{b-t}$
BB-tran	$\mathbf{m}$	t	$\mathbf{c}^\top\mathbf{m} + \frac{1}{b-t}$

Assumption: ISIS$_f$

Proposed by Bootle, Lyubashevsky, Nguyen and Sorniotti [BLNS23]

- **Parameters:** $\mathcal{R}$, n, m, q, s, β, a function $f : \mathcal{T} \to \mathcal{R}_q^n$
- **Input:** $\mathbf{A} \leftarrow\!\!\$\ \mathcal{R}_q^{n \times m}$
- **Hints:** queries oracle which samples $(\mathbf{u}_i, t_i)$ where $\mathbf{u}_i$ Gaussian with parameter s and $t_i \leftarrow\!\!\$\ \mathcal{T}$ subject to

$$\mathbf{A} \cdot \mathbf{u}_i = f(t_i) \bmod q$$

- **Output:** $(\mathbf{u}^*, t^*)$
- **Winning conditions:**
  - $\mathbf{A} \cdot \mathbf{u}^* = f(t^*) \bmod q$
  - $0 < \|\mathbf{u}^*\| \leq \beta$
  - $(\mathbf{u}^*, t^*) \notin \{(\mathbf{u}_i, t_i)\}_i$

Theorem [BLNS23]

ISIS$_f$ $\implies$ interactive version of ISIS$_f$ $\implies$ (s)EUF-CMA-secure signatures.

Assumption: ISIS$_f$

Proposed by Bootle, Lyubashevsky, Nguyen and Sorniotti [BLNS23]

† **Parameters:** $\mathcal{R}$, n, m, q, s, β, a function $f : \mathcal{T} \to \mathcal{R}_q^n$

† **Input:** $\mathbf{A} \leftarrow\!\!\$\ \mathcal{R}_q^{n \times m}$

† **Hints:** queries oracle which samples $(\mathbf{u}_i, t_i)$ where $\mathbf{u}_i$ Gaussian with parameter s and $t_i \leftarrow\!\!\$\ \mathcal{T}$ subject to

$$\mathbf{A} \cdot \mathbf{u}_i = f(t_i) \bmod q$$

† **Output:** $(\mathbf{u}^*, t^*)$

† **Winning conditions:**

‡ $\mathbf{A} \cdot \mathbf{u}^* = f(t^*) \bmod q$

‡ $0 < \|\mathbf{u}^*\| \leq \beta$

‡ $(\mathbf{u}^*, t^*) \notin \{(\mathbf{u}_i, t_i)\}_i$

Theorem [BLNS23]

ISIS$_f$ $\implies$ interactive version of ISIS$_f$ $\implies$ (s)EUF-CMA-secure signatures.

Assumption: ISIS$_f$

Proposed by Bootle, Lyubashevsky, Nguyen and Sorniotti [BLNS23]

- **Parameters:** $\mathcal{R}$, n, m, q, s, β, a function $f : \mathcal{T} \to \mathcal{R}_q^n$
- **Input:** $\mathbf{A} \leftarrow\!\!\$\ \mathcal{R}_q^{n \times m}$
- **Hints:** queries oracle which samples $(\mathbf{u}_i, t_i)$ where $\mathbf{u}_i$ Gaussian with parameter s and $t_i \leftarrow\!\!\$\ \mathcal{T}$ subject to
$$\mathbf{A} \cdot \mathbf{u}_i = f(t_i) \bmod q$$
- **Output:** $(\mathbf{u}^*, t^*)$
- **Winning conditions:**
  - $\mathbf{A} \cdot \mathbf{u}^* = f(t^*) \bmod q$
  - $0 < \|\mathbf{u}^*\| \leq \beta$
  - $(\mathbf{u}^*, t^*) \notin \{(\mathbf{u}_i, t_i)\}_i$

Theorem [BLNS23]

ISIS$_f$ $\implies$ interactive version of ISIS$_f$ $\implies$ (s)EUF-CMA-secure signatures.

Assumption: GenISIS$_f$

A minor generalisation where f is keyed/replaced by a family.

- **Parameters:** $\mathcal{R}$, n, m, q, s, β, a function $f : \mathcal{K} \times \mathcal{T} \to \mathcal{R}_q^n$
- **Input:** $\mathbf{A} \leftarrow\!\$\ \mathcal{R}_q^{n \times m}$ and key $k \leftarrow\!\$\ \mathcal{K}$
- **Hints:** queries oracle which samples $(\mathbf{u}_i, t_i)$ where $\mathbf{u}_i$ Gaussian with parameter s and $t_i \leftarrow\!\$\ \mathcal{T}$ subject to

$$\mathbf{A} \cdot \mathbf{u}_i = f(k, t_i) \bmod q$$

- **Output:** $(\mathbf{u}^*, t^*)$
- **Winning conditions:**
  - $\mathbf{A} \cdot \mathbf{u}^* = f(t^*) \bmod q$
  - $0 < \|\mathbf{u}^*\| \leq \beta$
  - $(\mathbf{u}^*, t^*) \notin \{(\mathbf{u}_i, t_i)\}_i$

s-Hint-vSIS $\implies$ sEUF-SMA of Σ $\implies$ sEUF-RMA of $\Sigma \equiv$ GenISIS$_f$ for $f(\mathbf{B}, (\mu, \tau)) = h_{\mu,\tau}(\mathbf{B})$

Assumption: GenISIS$_f$

A minor generalisation where f is keyed/replaced by a family.

- † **Parameters:** $\mathcal{R}$, n, m, q, s, β, a function $f : \mathcal{K} \times \mathcal{T} \to \mathcal{R}_q^n$
- † **Input:** $\mathbf{A} \leftarrow\!\!\$\ \mathcal{R}_q^{n \times m}$ and key $k \leftarrow\!\!\$\ \mathcal{K}$
- † **Hints:** queries oracle which samples $(\mathbf{u}_i, t_i)$ where $\mathbf{u}_i$ Gaussian with parameter s and $t_i \leftarrow\!\!\$\ \mathcal{T}$ subject to

$$\mathbf{A} \cdot \mathbf{u}_i = f(k, t_i) \bmod q$$

- † **Output:** $(\mathbf{u}^*, t^*)$
- † **Winning conditions:**
  - ‡ $\mathbf{A} \cdot \mathbf{u}^* = f(t^*) \bmod q$
  - ‡ $0 < \|\mathbf{u}^*\| \leq \beta$
  - ‡ $(\mathbf{u}^*, t^*) \notin \{(\mathbf{u}_i, t_i)\}_i$

s-Hint-vSIS $\implies$ sEUF-SMA of Σ $\implies$ sEUF-RMA of $\Sigma \equiv$ GenISIS$_f$ for $f(\mathbf{B}, (\mu, \tau)) = h_{\mu,\tau}(\mathbf{B})$

Assumption: GenISIS$_f$

A minor generalisation where f is keyed/replaced by a family.

- **Parameters:** $\mathcal{R}$, n, m, q, s, β,
  a function $f : \mathcal{K} \times \mathcal{T} \to \mathcal{R}_q^n$
- **Input:** $\mathbf{A} \leftarrow\!\!\$\ \mathcal{R}_q^{n \times m}$ and key $k \leftarrow\!\!\$\ \mathcal{K}$
- **Hints:** queries oracle which samples $(\mathbf{u}_i, t_i)$ where $\mathbf{u}_i$ Gaussian with parameter s and $t_i \leftarrow\!\!\$\ \mathcal{T}$ subject to

$$\mathbf{A} \cdot \mathbf{u}_i = f(k, t_i) \bmod q$$

- **Output:** $(\mathbf{u}^*, t^*)$
- **Winning conditions:**
  - $\mathbf{A} \cdot \mathbf{u}^* = f(t^*) \bmod q$
  - $0 < \|\mathbf{u}^*\| \leq \beta$
  - $(\mathbf{u}^*, t^*) \notin \{(\mathbf{u}_i, t_i)\}_i$

s-Hint-vSIS $\implies$ sEUF-SMA of Σ $\implies$ sEUF-RMA of $\Sigma \equiv$ GenISIS$_f$ for $f(\mathbf{B}, (\mu, \tau)) = h_{\mu,\tau}(\mathbf{B})$

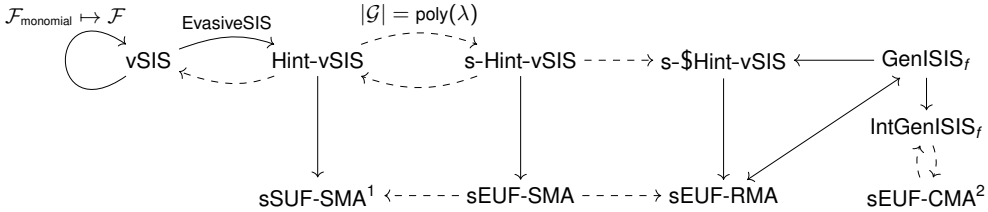
Parameters

Security Level	φ	q	β	s	ℓ_m	ℓ_r	$\lvert\mathsf{pk}\rvert$	$\lvert\mathsf{Sig}\rvert$
193	1024	2^{20}	$2^{18.99}$	2^{13}	1	2	2.5	9.5
150	1024	2^{25}	$2^{23.73}$	2^{16}	128	2	3.1	11.9
399	2048	2^{22}	$2^{20.77}$	2^{14}	1	2	5.5	20.8
312	2048	2^{27}	$2^{25.50}$	2^{17}	128	2	6.8	25.5

Table: Estimated parameters for BB-tran and BBS. Sizes are in KB.

Summary

More lattice assumptions and more proof-friendly signatures!



† SUF/EUF: Strong/Existential Unforgeability

† SMA/RMA/CMA: Selective/Random/Chosen Message Attack

Adrien Dubois

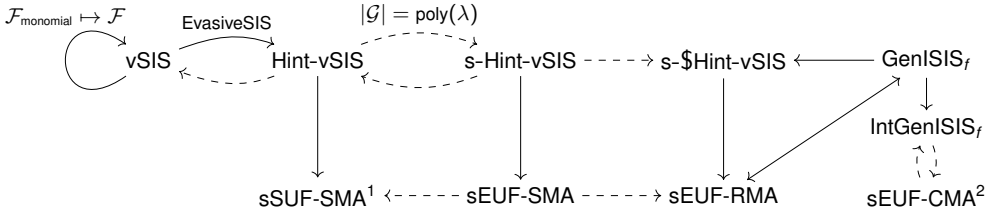
ENS de Lyon, France

adrien.dubois@ens-lyon.fr

ia.cr/2025/356 – **Thank You!**

Summary

More lattice assumptions and more proof-friendly signatures!



† SUF/EUF: Strong/Existential Unforgeability

† SMA/RMA/CMA: Selective/Random/Chosen Message Attack

Adrien Dubois

ENS de Lyon, France

adrien.dubois@ens-lyon.fr

ia.cr/2025/356 – **Thank You!**

[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*. Vol. 13508. 2022, pp. 102–132. DOI: 10.1007/978-3-031-15979-4_4 (pages 18, 19).

[BB04] Dan Boneh and Xavier Boyen. “Short Signatures Without Random Oracles”. In: *EUROCRYPT 2004*. Vol. 3027. 2004, pp. 56–73. DOI: 10.1007/978-3-540-24676-3_4 (pages 7–9).

[BBS04] Dan Boneh, Xavier Boyen, and Hovav Shacham. “Short Group Signatures”. In: *CRYPTO 2004*. Vol. 3152. 2004, pp. 41–55. DOI: 10.1007/978-3-540-28628-8_3 (pages 10–12).

[BLNS23] Jonathan Bootle, Vadim Lyubashevsky, Ngoc Khanh Nguyen, and Alessandro Sorniotti. “A Framework for Practical Anonymous Credentials from Lattices”. In: *CRYPTO 2023, Part II*. Vol. 14082. 2023, pp. 384–417. DOI: 10.1007/978-3-031-38545-2_13 (pages 13–19, 38–40).

[CLM23] Valerio Cini, Russell W. F. Lai, and Giulio Malavolta. “Lattice-Based Succinct Arguments from Vanishing Polynomials - (Extended Abstract)”. In: *CRYPTO 2023, Part II*. Vol. 14082. 2023, pp. 72–105. DOI: 10.1007/978-3-031-38545-2_3 (pages 18, 19, 25, 26).

[JRS23] Corentin Jeudy, Adeline Roux-Langlois, and Olivier Sanders. “Lattice Signature with Efficient Protocols, Application to Anonymous Credentials”. In: *CRYPTO 2023, Part II*. Vol. 14082. 2023, pp. 351–383. DOI: 10.1007/978-3-031-38545-2_12 (pages 13–17).

[LNP22] Vadim Lyubashevsky, Ngoc Khanh Nguyen, and Maxime Plançon. “Lattice-Based Zero-Knowledge Proofs and Applications: Shorter, Simpler, and More General”. In: *CRYPTO 2022, Part II*. Vol. 13508. 2022, pp. 71–101. DOI: 10.1007/978-3-031-15979-4_3 (pages 13–17).