GCKSign

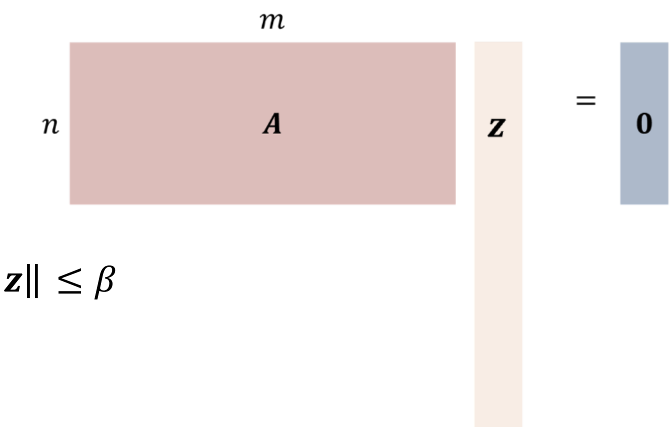
Simple and Efficient Signature Schemes from Generalized Compact Knapsacks

2023.02.22.

고려대학교

우 주

Lattice Problems



❖ Short Integer Solutions(SIS) Problem

◆ Definition

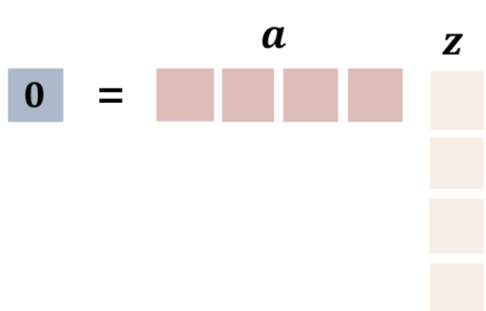
- Given a matrix $\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}$ and a real β,
  find a vector $\boldsymbol{z} \in \mathbb{Z}^m$ such that $\boldsymbol{Az} = \boldsymbol{0}$ mod q and $0 < \|\boldsymbol{z}\| \le \beta$

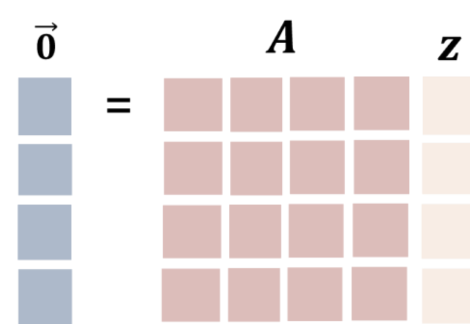
◆ Ring-SIS Problem

- Given a matrix $a_1, \dots, a_\ell \in R_q$ and a real β,
  find a vector $\boldsymbol{z} \in R^\ell$ s.t. $\sum_{i=1}^{\ell} a_i \cdot z_i = \boldsymbol{0}$ mod q and $0 < \|\boldsymbol{z}\| \le \beta$

◆ Module-SIS Problem

- Given a matrix $\boldsymbol{A} \in R_q^{k\times \ell}$ and a real β,
  find a vector $\boldsymbol{z} \in R^\ell$ such that $\boldsymbol{A} \cdot \boldsymbol{z} = \boldsymbol{0}$ mod q and $0 < \|\boldsymbol{z}\| \le \beta$





Learning with Errors(LWE) Problem

Definition

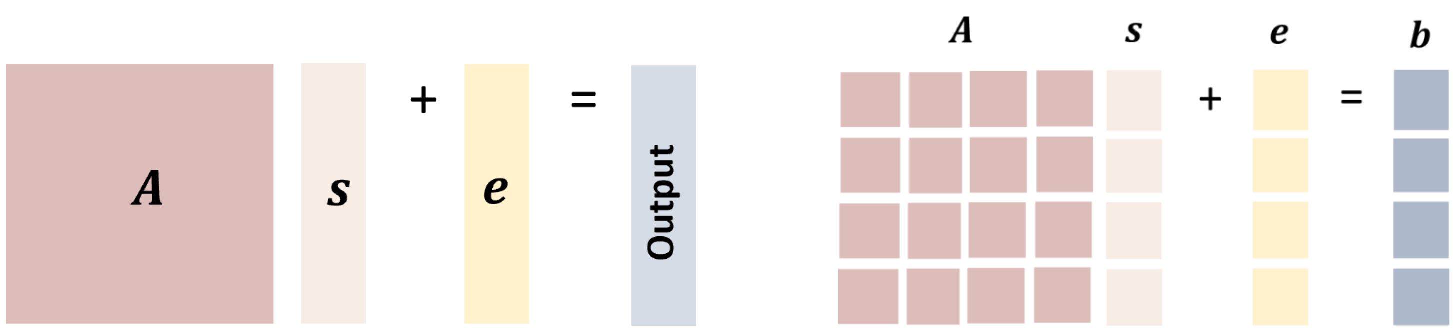
- **Search** : Given $\boldsymbol{A} \in \mathbb{Z}_q^{m\times n}$ and $\boldsymbol{b} = \boldsymbol{A}\boldsymbol{s} + \boldsymbol{e}$ where $\boldsymbol{e} \leftarrow \chi$, find a vector $s \in \mathbb{Z}_q^n$
- **Decision** : Distinguish $(\boldsymbol{A}, \boldsymbol{A}\boldsymbol{s} + \boldsymbol{e})$ from uniform $(\boldsymbol{A}, \boldsymbol{u})$ pairs

Ring-LWE Problem

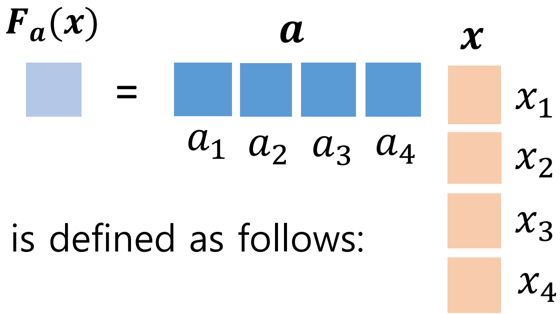
- Given $\boldsymbol{a} \in R_q^k$ and $\boldsymbol{b} = \boldsymbol{a} \cdot s + \boldsymbol{e}$ where $\boldsymbol{e} \leftarrow \chi$, find $s \in R_q$

Module-LWE Problem

- Given a matrix $\boldsymbol{A} \in R_q^{k\times\ell}$ and $\boldsymbol{b} = \boldsymbol{A} \cdot \boldsymbol{s} + \boldsymbol{e}$ where $\boldsymbol{e} \leftarrow \chi$, find a vector $\boldsymbol{s} \in R_q^{\ell}$



GCK Function



❖ Generalized Compact Knapsack(GCK)

◆ Definition

- For a ring R, small integer $m > 1$, GCK function $F_{\boldsymbol{a}}: R^m \to R$ is defined as follows:

$$F_{\boldsymbol{a}}(\boldsymbol{x}) = \sum_{i=1}^{m} x_i \cdot a_i \text{ where } \boldsymbol{x} = (x_1, \dots, x_m) \in R_q^m \text{ and } \|\boldsymbol{x}\|_\infty \le \beta$$

◆ Onewayness of GCK problem

- Given $\boldsymbol{a} = (a_1, \dots, a_m) \in R^m$ and $t \in R$, **find $\boldsymbol{x}$** s.t. $\|\boldsymbol{x}\|_\infty \le \beta$ and $F_{\boldsymbol{a}}(\boldsymbol{x}) = t$

◆ Collision-Resistance of GCK problem

- Given $\boldsymbol{a} = (a_1, \dots, a_m) \in R^m$, **find $\boldsymbol{x}, \boldsymbol{y} \in R_q^m$** s.t. $\boldsymbol{x} \ne \boldsymbol{y}$, $\|\boldsymbol{x}\|_\infty \le \beta$, $\|\boldsymbol{y}\|_\infty \le \beta$ and $F_{\boldsymbol{a}}(\boldsymbol{x}) = F_{\boldsymbol{a}}(\boldsymbol{y})$

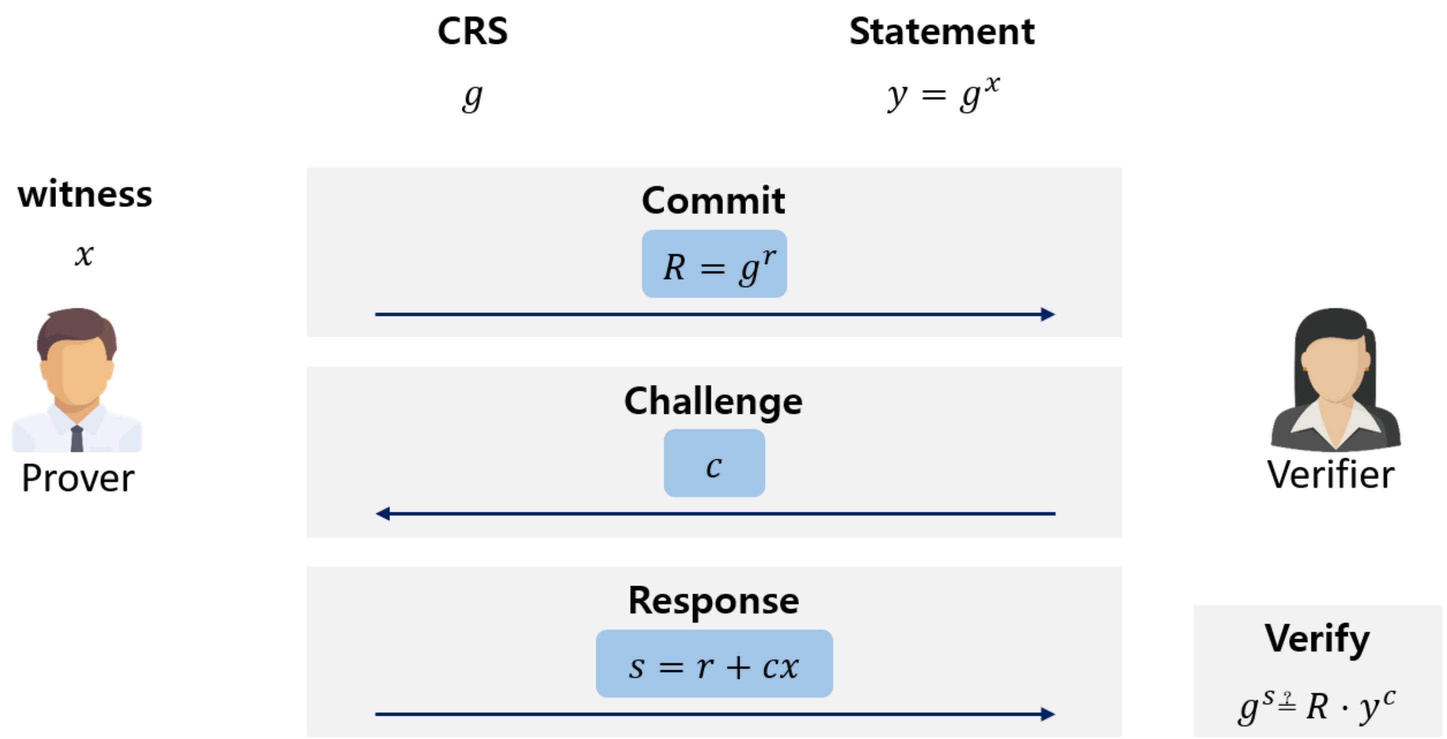
[Mic02] D. Micciancio., “*Generalized compact knapsacks, cyclic lattices, and efficient one-way functions*”, *FOCS 2002*

[LM06] V. Lyubashevsky et al., “*Generalized Compact Knapsacks Are Collision Resistant*”, *ICALP 2006*

[PR06] C. Peikert et al., “*Efficient Collision-Resistant Hashing from Worst-Case Assumption on cyclic Lattices*”, *TCC 2006*

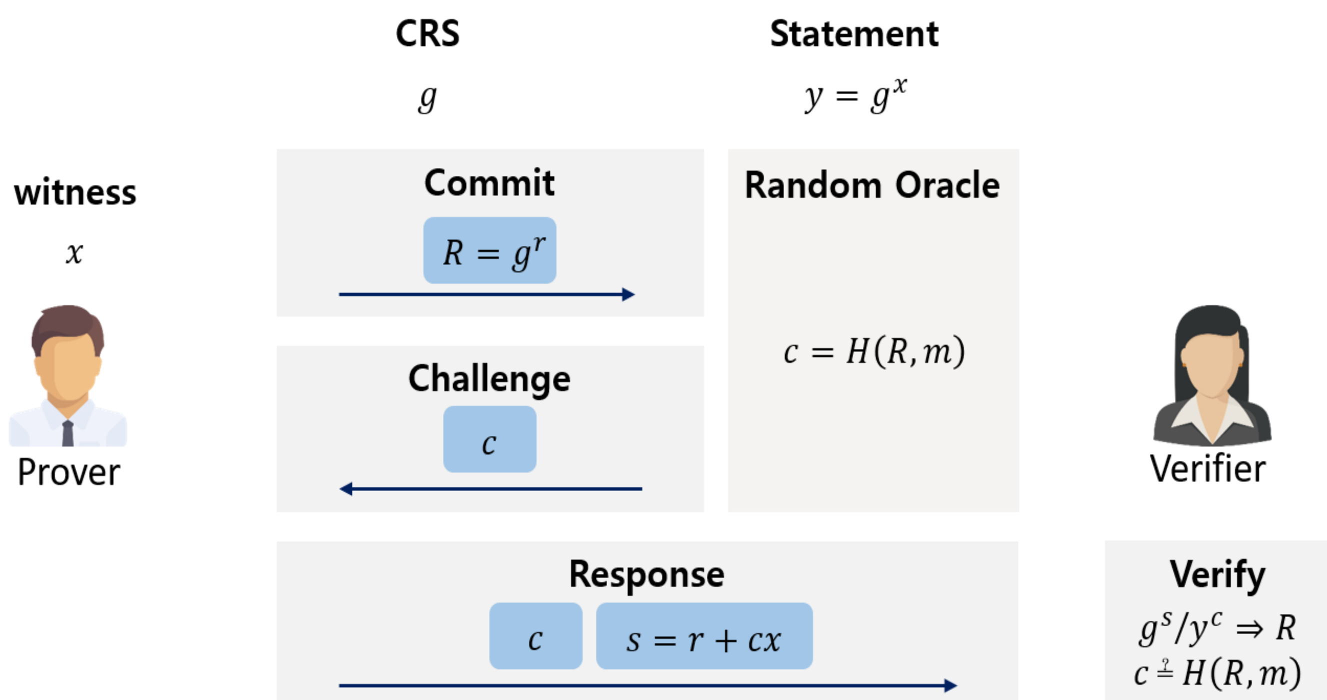
❖ Lattice-based Signature

- **Schnorr Identification**

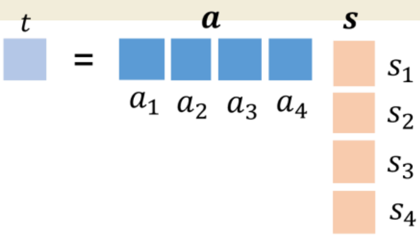


Lattice-based Signature

- **Schnorr Signature (w/ Fiat-Shamir Transform)**



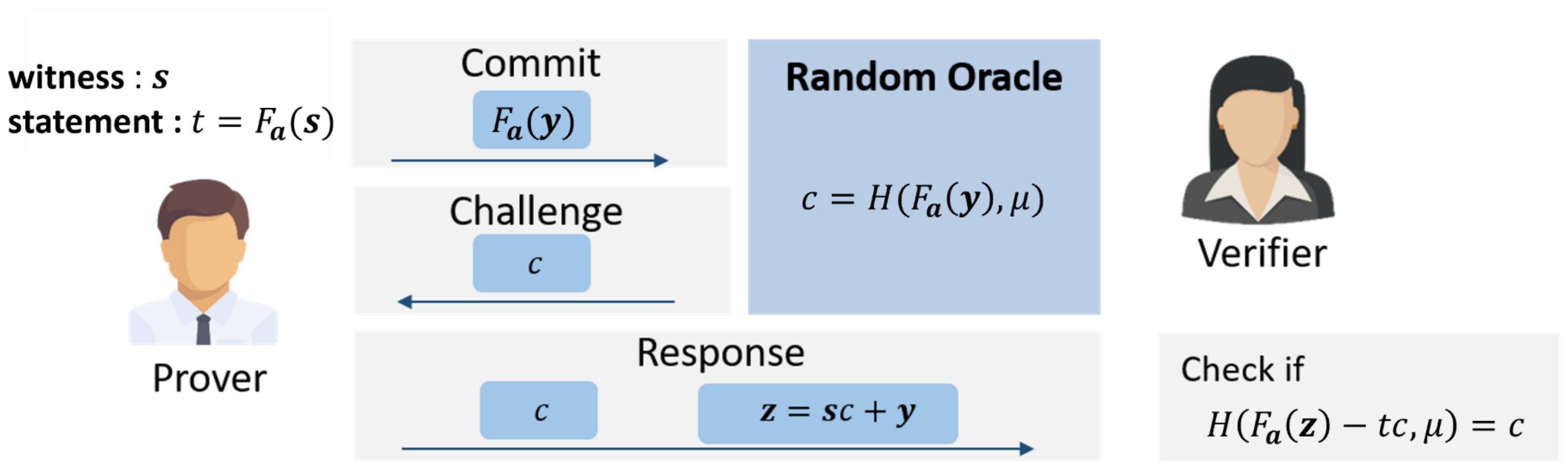
Lattice-based Signatures



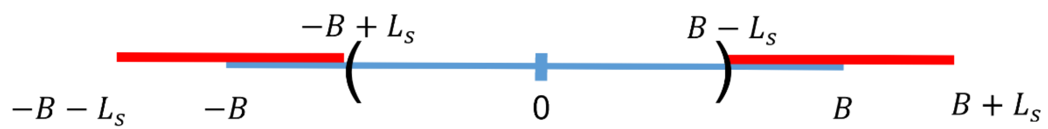
❖ Lattice-based Signature

◆ Lyubashevsky's Identification Scheme

- Principle : Proof Knowledge of the input $\boldsymbol{s} \in R^m$ such that $F_{\boldsymbol{a}}(\boldsymbol{s}) = \sum_{i=1}^{m} a_i \cdot s_i$ and $\|\boldsymbol{s}\|_\infty \le \beta$

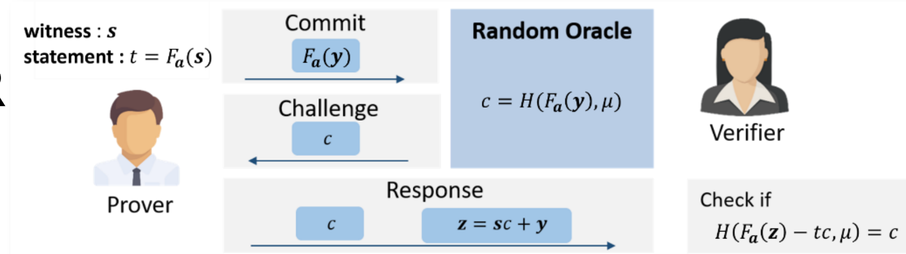


- Rejection Sampling ($\boldsymbol{z}$)



[Lyu09] V. Lyubashevsky., *"Fiat-Shamir with Aborts: Applications to Lattice and Factoring-based Signatures"*, *ASIACRYPT 2009*

Lattice-based Signatures



❖ Security Proof based on GCK-CR

- **[Lyu09]**

$\mathcal{A}$ (GCK-CR adversary)

$Goal:\ find\ \boldsymbol{x}, \boldsymbol{x}'$
$such\ that\ F_{\boldsymbol{a}}(\boldsymbol{x}) = F_{\boldsymbol{a}}(\boldsymbol{x}')$

$\mathcal{B}$ (EUF-CMA Forger)

$\boldsymbol{a}$

$public\ key:\ t = F_{\boldsymbol{a}}(\boldsymbol{s})$

$\boldsymbol{a}, t$

$Y = F_{\boldsymbol{a}}(\boldsymbol{y})$

$get\ two\ forgery\ (c, \boldsymbol{z}), (c', \boldsymbol{z}')$
$Such\ that$
$F_{\boldsymbol{a}}(\boldsymbol{z}) - tc = Y,$
$F_{\boldsymbol{a}}(\boldsymbol{z}') - tc' = Y$

$(c, \boldsymbol{z}), (c', \boldsymbol{z}')$

By rewinding technique

$$\textbf{Set } \boldsymbol{x} = \boldsymbol{z} - \boldsymbol{s}c, \quad \boldsymbol{x}' = \boldsymbol{z}' - \boldsymbol{s}c' \quad \begin{pmatrix} \neq \boldsymbol{y} + \boldsymbol{s}c - \boldsymbol{s}c \\ \neq \boldsymbol{y} + \boldsymbol{s}c' - \boldsymbol{s}c' \end{pmatrix}$$

$\boldsymbol{x}, \boldsymbol{x}'$

$$\text{※} F_{\boldsymbol{a}}(\boldsymbol{x}) = F_{\boldsymbol{a}}(\boldsymbol{z} - \boldsymbol{s}c) = F_{\boldsymbol{a}}(\boldsymbol{z}) - tc$$
$$= Y = F_{\boldsymbol{a}}(\boldsymbol{z}') - tc'$$
$$= F_{\boldsymbol{a}}(\boldsymbol{z}' - \boldsymbol{s}c') = F_{\boldsymbol{a}}(\boldsymbol{x}')$$

$\boldsymbol{x} \neq \boldsymbol{x}'$ **by** $witness\ indsistinguishability$ $\Rightarrow$ **Security Requirement :** $q^n \ll (2\beta + 1)^{mn}$

[Lyu09] V. Lyubashevsky., *"Fiat-Shamir with Aborts: Applications to Lattice and Factoring-based Signatures"*, *ASIACRYPT 2009*

Lattice-based Signatures

❖ Lattice-based Signature

◆ A Variant of Schnorr Identification

CRS

g_1, g_2

Statement

$y = g_1^{s_1} \cdot g_2^{s_2}$

witness

s_1, s_2

Prover

Commit

$R = g_1^{y_1} \cdot g_2^{y_2}$

Challenge

c

Response

$z_1 = y_1 + cs_1$ $z_2 = y_2 + cs_2$

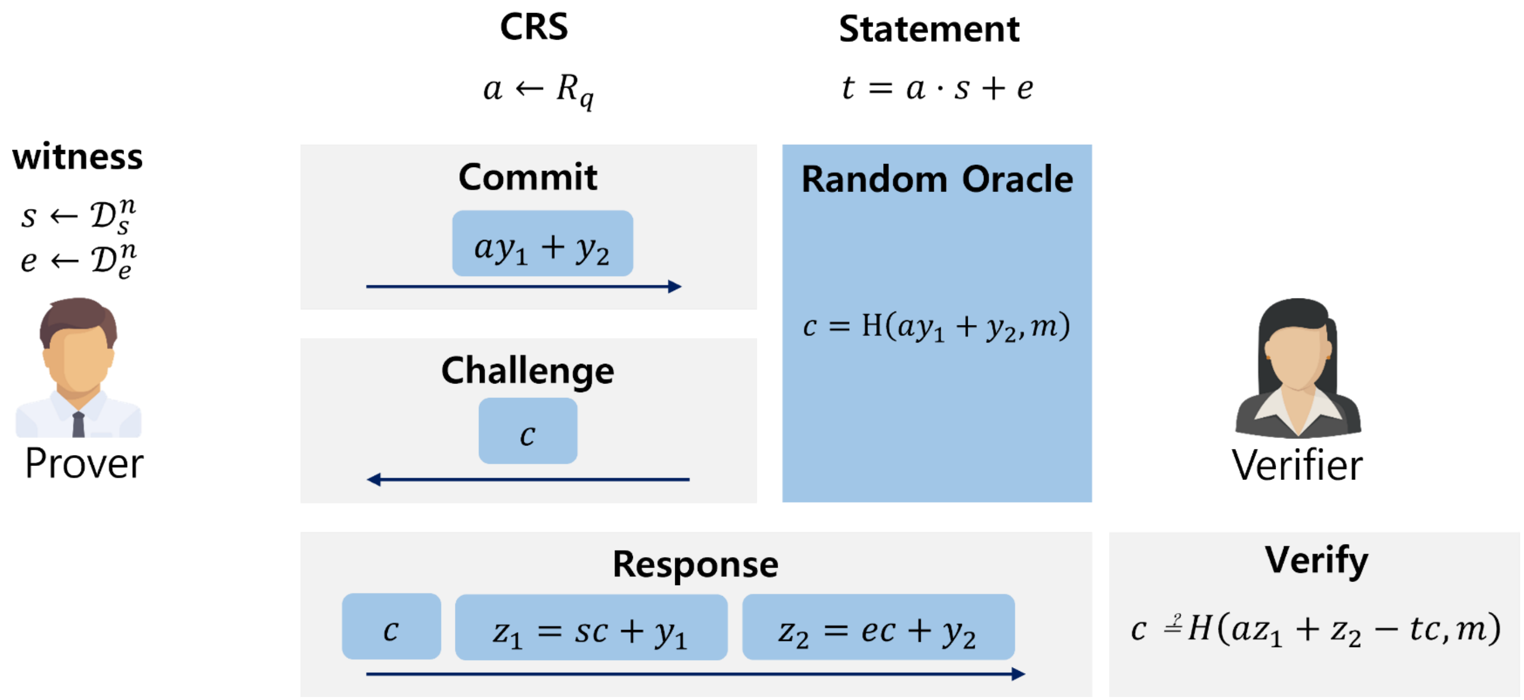
Verifier

Verify

$g_1^{z_1} \cdot g_2^{z_2} \stackrel{?}{=} R \cdot y^c$

❖ Lattice-based Signature

- **Identification Protocol (LWE + SIS)**



[GLP12] T. Güneysu et al., "*Practical Lattice-based Cryptography: A Signature Scheme for Embedded Systems*", *CHES 2012*

Lattice-based Signatures

$c = \mathrm{H}(ay_1 + y_2, m)$

Verify

$c \stackrel{?}{=} H(az_1 + z_2 - tc, m)$

❖ Security Proof based on Ring-SIS

- **[GLP12]**

$\mathcal{A}$ (Ring-SIS adversary)

$Goal:\ find\ \boldsymbol{x_1}, \boldsymbol{x_2}$
$such\ that\ \boldsymbol{a}\boldsymbol{x}_1 + \boldsymbol{x}_2 = \boldsymbol{0}$

$\boldsymbol{a}$

$public\ key:\ t = \boldsymbol{as} + \boldsymbol{e}$
$= \boldsymbol{as}' + \boldsymbol{e}'$

$\boldsymbol{a}, t$

$\mathcal{B}$ (EUF-CMA Forger)

$Y = ay_1 + y_2$

$get\ two\ forgery\ (c, \boldsymbol{z}), (c', \boldsymbol{z}')$
$Such\ that$
$\boldsymbol{a}\boldsymbol{z}_1 + \boldsymbol{z}_2 - tc = \boldsymbol{Y},$
$\boldsymbol{a}\boldsymbol{z}_1' + \boldsymbol{z}_2' - tc' = \boldsymbol{Y}$

$(c, \boldsymbol{z}), (c', \boldsymbol{z}')$

$$\boldsymbol{Set\ x_1 = z_1 - sc - z_1' + sc',}$$
$$\boldsymbol{x_2 = z_2' - ec - z_2' + ec'}$$

$\boldsymbol{x}_1, \boldsymbol{x}_2$

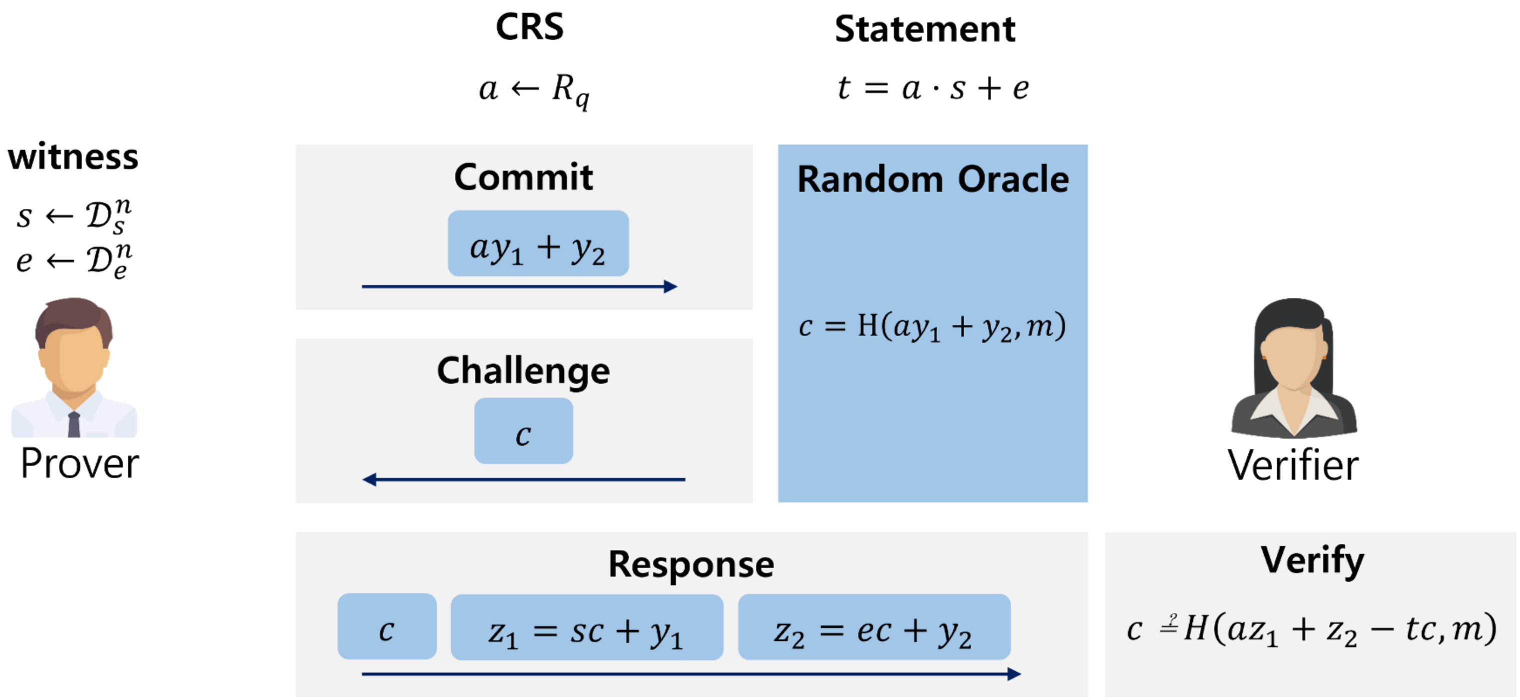
$\boldsymbol{x_1} \neq \boldsymbol{0}\ \&\ \boldsymbol{x}' \neq \boldsymbol{0}\ \ \boldsymbol{by}\ witness\ indsistinguishability \ \Rightarrow$ ~~Security Requirement : $q^n \ll (2\beta+1)^{mn}$~~

[GLP12] T. Güneysu et al., "*Practical Lattice-based Cryptography: A Signature Scheme for Embedded Systems*", *CHES 2012*

Lattice-based Signatures

❖ Lattice-based Signature

- **Identification Protocol (LWE + SIS)**

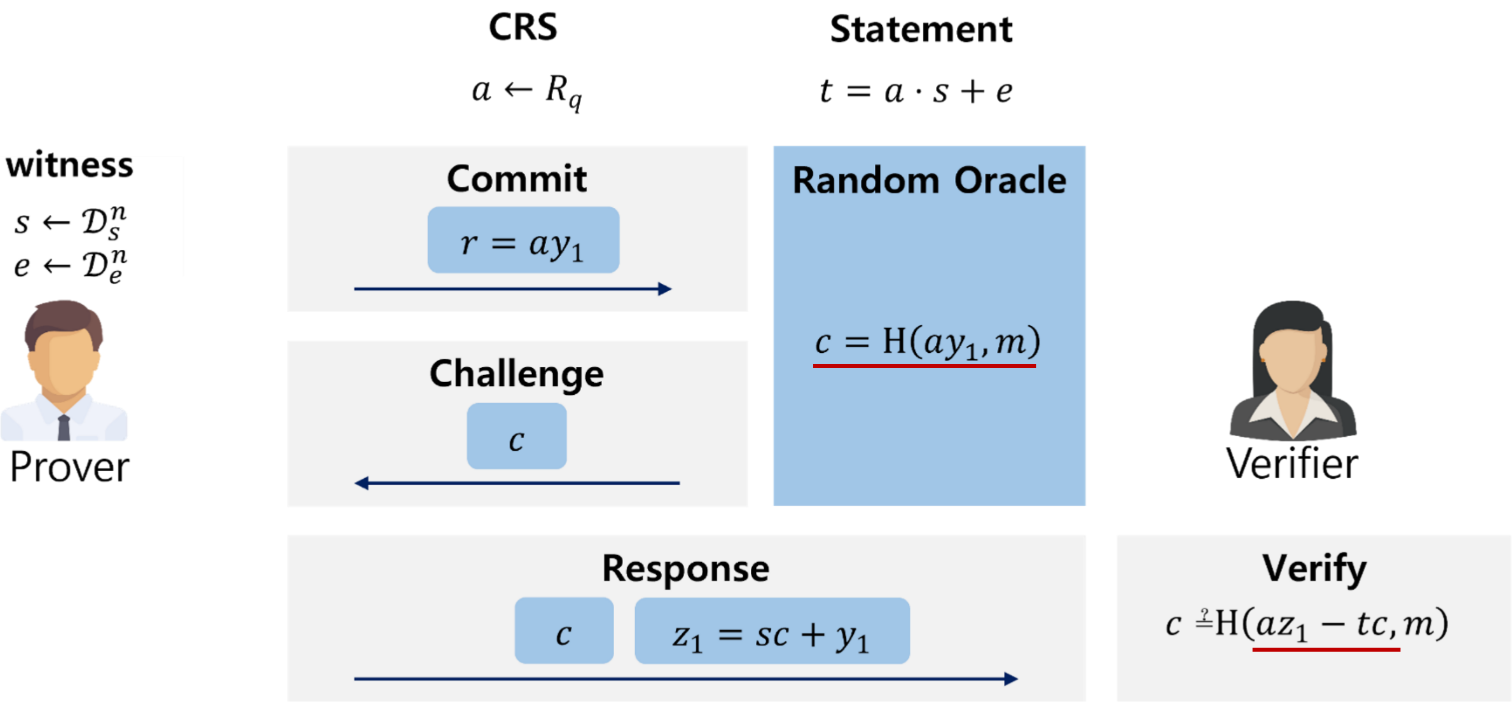


[GLP12] T. Güneysu et al., "*Practical Lattice-based Cryptography: A Signature Scheme for Embedded Systems*", *CHES 2012*

❖ Lattice-based Signature

- **Improved Identification Protocol (LWE + SIS)**

Signature Size Reduction



1	0	1	1	1	0	1	1	0	1	1	$\neq$	1	0	1	1	1	0	1	0	1	1	1

1	0	1	1	$=$	1	0	1	1

$$
\begin{aligned}
& az_1 - tc \\
&= a(sc + y_1) - (as + e)c \\
&= ay_1 - ec \\
&\approx ay_1
\end{aligned}
$$

[BG14] S. Bai et al., "*An Improved Compression Technique for Signatures based on Learning with Errors*", *CT-RSA 2014*

❖ Lattice-based Signature

- **Dilithium (MLWE + MSIS)**

PK compression

α-bit

$\boldsymbol{t} = \quad t_1 \quad t_0$

$t_1 = [\boldsymbol{t}]_\alpha = high(t) \qquad t_0 = low(t)$

CRS

$\boldsymbol{A} \leftarrow R_q^{k\times\ell}$

Statement

$\boldsymbol{t} \equiv \boldsymbol{As} + \boldsymbol{e} = \boldsymbol{t}_1 \cdot 2^\alpha + \boldsymbol{t}_0$

witness

$\boldsymbol{s} \leftarrow \mathcal{D}_s^\ell$

$\boldsymbol{e} \leftarrow \mathcal{D}_e^k$

Prover

Commit

$\boldsymbol{r} \equiv \boldsymbol{Ay}$

Challenge

c

Random Oracle

$c = \mathrm{H}(\lceil \boldsymbol{Ay} \rfloor_d, \mu)$

Verifier

Response

$c \quad \boldsymbol{z} = \boldsymbol{s}c + \boldsymbol{y}$

Verify

$\boldsymbol{c} \stackrel{?}{=} \mathrm{H}(\lceil \boldsymbol{Az} - 2^\alpha \boldsymbol{t}_1 c \rfloor_d, m)$

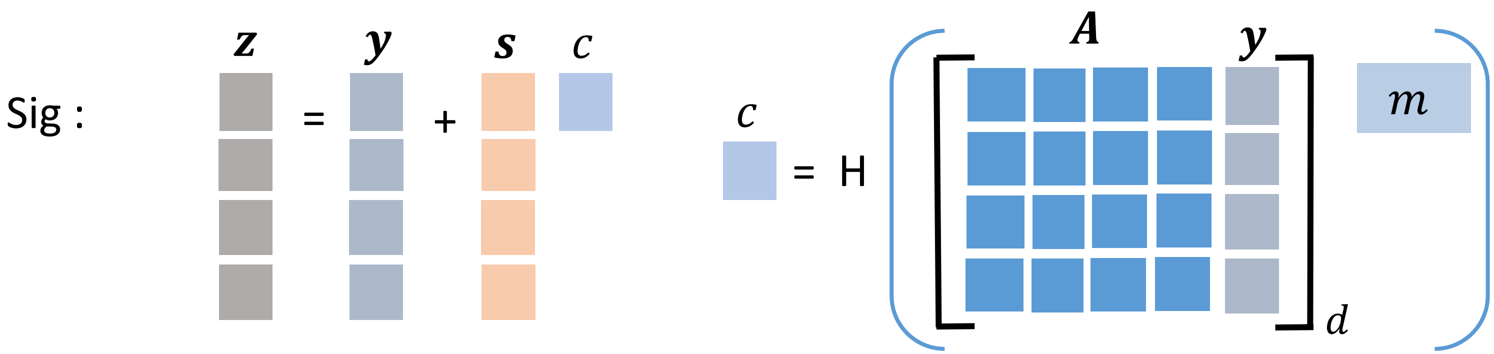
$$\boldsymbol{Az} - c\boldsymbol{t}_1 \cdot 2^\alpha = \boldsymbol{Az} - c(\boldsymbol{t} - \boldsymbol{t}_0)$$
$$= \boldsymbol{Az} - \boldsymbol{t}c - c\boldsymbol{t}_0$$
$$= \boldsymbol{Ay} - \boldsymbol{e}c - c\boldsymbol{t}_0$$

[DKL+18] L. Ducas et al., "*CRYSTALS-Dilithium: A Lattice-based Digital Signature Scheme*", *TCHES 2018*

Lattice-based Signatures

❖ Dilithium

- **Public key :** $(A,\ \boldsymbol{t_1} = [\boldsymbol{A}\cdot\boldsymbol{s}+\boldsymbol{e}]_\alpha) \in R_q^{k\times\ell}\times R_q^k$ **Secret key :** $\boldsymbol{s},\boldsymbol{e},\boldsymbol{t_0}$
- **Sign :** $(\boldsymbol{z},c,h) = (\boldsymbol{y}+c\cdot\boldsymbol{s},\ \ c = H([\boldsymbol{A}\cdot\boldsymbol{y}]_{\boldsymbol{d}},\ m)) \in R^k_{[-B,B]}\times\{0,1\}^t\times\{0,1\}^{256k}$



- **Check if** $||\boldsymbol{y}+c\cdot\boldsymbol{s}|| < B - L_s$ — Security check on s

  $||low(\boldsymbol{A}\cdot\boldsymbol{y} - c\cdot\boldsymbol{e})|| < 2^d - L_e$ — Security check on e

  $[\boldsymbol{A}\cdot\boldsymbol{y} - c\cdot\boldsymbol{e}]_d = [\boldsymbol{A}\cdot\boldsymbol{y}]_d$ — Correctness check

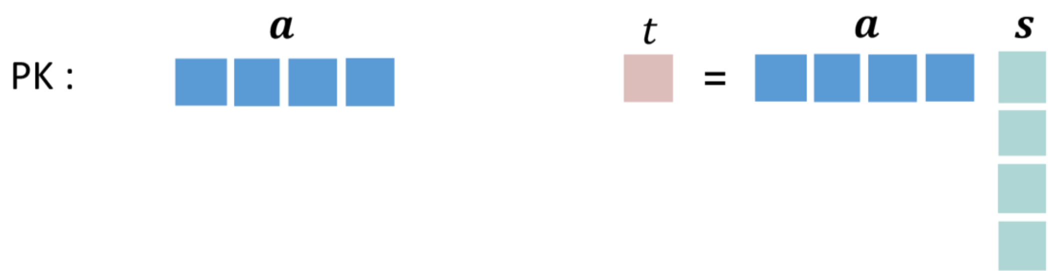
- **Create** $h = Hint(-c\cdot\boldsymbol{t}_0,\ \boldsymbol{A}\cdot\boldsymbol{y} - c\cdot\boldsymbol{e} + c\cdot\boldsymbol{t}_0,\ d)$ — Create a carry bit hint vector h caused by ignoring $c\cdot\boldsymbol{t}_0$

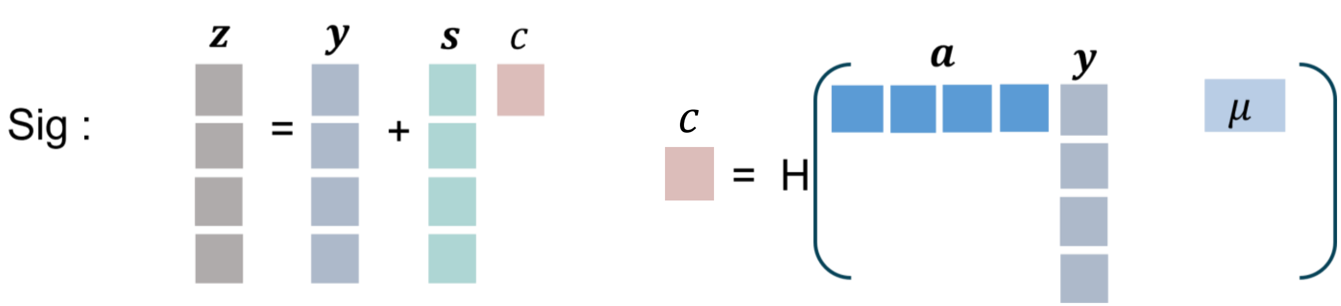
GCK-Based Signatures (1)

- GCK function F_a and $R_q = Z_q[x]/< x^n + 1 >$, $q = prime$
  - Public key :$(a,\ t = F_a(s)) \in R_q^m \times R_q$ Secret key : s
  - Sign : $(z, c) = (y + c \cdot s,\ c = H(F_a(y),\ \mu)) \in R^m_{[-B+L_s, B-L_s]} \times \{0,1\}^\ell$

$\boxed{s \leftarrow R^m_{[-\eta,\eta]}}$

$\boxed{y \leftarrow R^m_{[-B,B]}}$





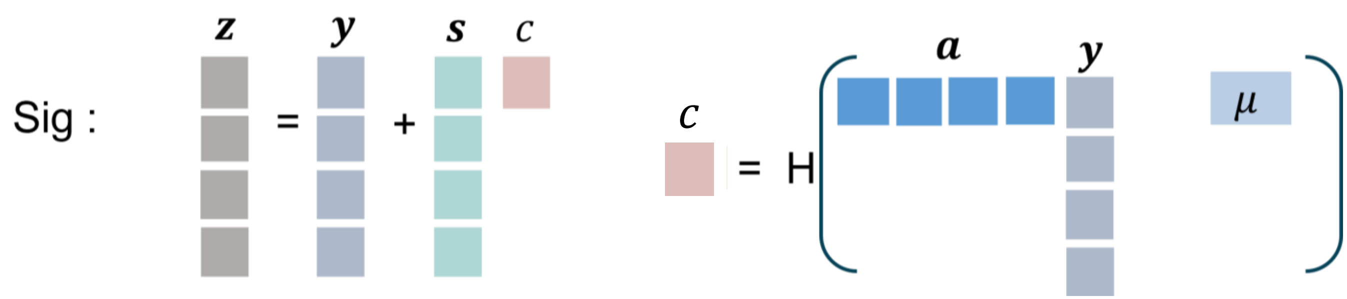
- Verification: (1) compute $F_a(z) - c \cdot t = F_a(y)$
  (2) check if $c = H(F_a(y),\ \mu)$

GCK-Based Signatures (2)

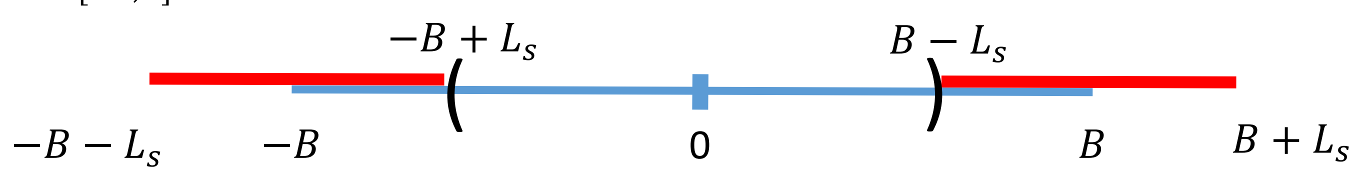
- **GCK function** $F_{\boldsymbol{a}}$ **and** $\boldsymbol{R_q = Z_q[x]/< x^n + 1 >}$, $q = prime$
  - **Public key :** $(a,\ t = F_{\boldsymbol{a}}(\boldsymbol{s})) \in R_q^m \times R_q$ **Secret key :** $\boldsymbol{s}$
  - **Sign :** $(z, c) = (\boldsymbol{y} + c \cdot \boldsymbol{s},\ c = H(F_{\boldsymbol{a}}(\boldsymbol{y}),\ \mu)) \in R^m_{[-B+L_s, B-L_s]} \times \{0,1\}^{\ell}$

$\boldsymbol{s} \leftarrow R^m_{[-\eta,\eta]}$

$\boldsymbol{y} \leftarrow R^m_{[-B,B]}$



- $||c \cdot \boldsymbol{s}|| < L_s$ $\leftarrow$ c : sparse ternary distribution and $\boldsymbol{s} \leftarrow R^m_{[-\eta,\eta]}$
- $\boldsymbol{y} \leftarrow R^m_{[-B,B]}$



- Check if $||\boldsymbol{z}|| = \boxed{||\boldsymbol{y} + c \cdot \boldsymbol{s}|| < B - L_s}$ to prevent leakage of $\boldsymbol{s}$ from $\boldsymbol{z}$

❖ Security Proof based on GCK-OW

$\mathcal{A}$ (GCK-OW adversary)

$Goal\text{: } find\ \boldsymbol{x}$
$such\ that\ F_{\boldsymbol{a}}(\boldsymbol{x}) = t$ and $\|\boldsymbol{x}\|_\infty < \beta$

$\boldsymbol{a}, t$

$public\ key\text{: } t$

$\mathcal{B}$ (EUF-CMA Forger)

$\boldsymbol{a}, t$

$(c, \boldsymbol{z}), (c', \boldsymbol{z}')$

By rewinding technique

$get\ two\ forgery\ (c, \boldsymbol{z}), (c', \boldsymbol{z}')$
$Such\ that$
$F_{\boldsymbol{a}}(\boldsymbol{z}) - tc = Y,$
$F_{\boldsymbol{a}}(\boldsymbol{z}') - tc' = Y$
$\boldsymbol{z} - \boldsymbol{z}' = (c - c')\boldsymbol{x}$

$\boldsymbol{x}$

$\boldsymbol{x} = (\boldsymbol{z} - \boldsymbol{z}')(c - c')^{-1}$

New GCK Problem

❖ Generalized Compact Knapsack(GCK)

◆ One-wayness of GCK problem

- Given $\boldsymbol{a} = (a_1, \dots, a_m) \in R^m$ and $t \in R$
  find $\boldsymbol{x}$ s.t. $\|\boldsymbol{x}\|_\infty \le \beta$ and $F_{\boldsymbol{a}}(\boldsymbol{x}) = t$

◆ Collision-Resistance of GCK problem

- Given $\boldsymbol{a} = (a_1, \dots, a_m) \in R^m$, **find** $\boldsymbol{x}, \boldsymbol{y} \in \boldsymbol{R}_q^m$
  s.t. $\boldsymbol{x} \ne \boldsymbol{y}$, $\|\boldsymbol{x}\|_\infty \le \beta$, $\|\boldsymbol{y}\|_\infty \le \beta$ and $F_{\boldsymbol{a}}(\boldsymbol{x}) = F_{\boldsymbol{a}}(\boldsymbol{y})$

◆ Target-modified One-wayness of GCK problem (TMO)

- Given $\boldsymbol{a} = (a_1, \dots, a_m) \in R^m$ and $t \in R$,
  find $\boldsymbol{x}, c$ s.t. $\|c\|_\infty \le \alpha$, $\|\boldsymbol{x}\|_\infty \le \beta$, and $F_{\boldsymbol{a}}(\boldsymbol{x}) = c \cdot t$

Approximate version of OW problem (multiplicative)

Definition 3.1 (Approximate ISIS). *For any $n, m, q \in \mathbb{N}$ and $\alpha, \beta \in \mathbb{R}$, define the approximate inhomogeneous short integer solution problem* Approx.ISIS$_{n,m,q,\alpha,\beta}$ *as follows: Given $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, $\mathbf{y} \in \mathbb{Z}_q^n$, find a vector $\mathbf{x} \in \mathbb{Z}^m$ such that $\|\mathbf{x}\| \le \beta$, and there is a vector $\mathbf{z} \in \mathbb{Z}^n$ satisfying*

$$\|\mathbf{z}\| \le \alpha \quad \text{and} \quad \mathbf{A}\mathbf{x} = \mathbf{y} + \mathbf{z} \pmod q.$$

Let us remark that the approximate ISIS is only non-trivial when the bounds α, β are relatively small compared to the modulus q. Also, our definition chooses to allow the zero vector to be a valid

[CGM19] Y. Chen et al., "*Approximate Trapdoors for Lattices and Smaller Hash-and-Sign Signatures*", *ASIACRYPT 2019*

New GCK Problem

❖ Security Proof

◆ Security based on Target-Modified One-wayness of GCK

$\mathcal{A}$ (GCK-TMO adversary)

Goal: *find* $\boldsymbol{x}, c$
such that $F_{\boldsymbol{a}}(\boldsymbol{x}) = c \cdot t$

$\boldsymbol{a}, t$

public key: t

$\mathcal{B}$ (EUF-CMA Forger)

$\boldsymbol{a}, t$

$Y = F_{\boldsymbol{a}}(\boldsymbol{y})$

$(c, \boldsymbol{z}), (c', \boldsymbol{z}')$

By rewinding technique

Get two forgery $(\boldsymbol{z}, c), (\boldsymbol{z}', c')$
Such that
$F_{\boldsymbol{a}}(\boldsymbol{z}) - tc = Y$
$F_{\boldsymbol{a}}(\boldsymbol{z}') - tc' = Y$
$F_{\boldsymbol{a}}(\boldsymbol{z} - \boldsymbol{z}') = (c - c')t$

Set $\boldsymbol{x} = \boldsymbol{z} - \boldsymbol{z}', \ \tilde{c} = (c - c')$

$\boldsymbol{x}, \tilde{c}$

- **Target-modified Onewayness of GCK problem (TMO)**
  - Given $\boldsymbol{a} = (a_1, \ldots, a_m) \in R^m$ and $t \in R$,
    find $\boldsymbol{x}, c$ s.t. $\|c\|_\infty \le \alpha$, $\|x_i\|_\infty \le \beta$, and $F_{\boldsymbol{a}}(\boldsymbol{x}) = c \cdot t$

New GCK Problem

❖ Reduction between GCK problems

$\mathcal{B}$ (GCK-TMO adversary) $\rightarrow (\boldsymbol{x}, c)$ s.t. $\|c\|_\infty \leq \alpha$, $\|\boldsymbol{x}\|_\infty \leq \beta$, and $F_{\boldsymbol{a}}(\boldsymbol{x}) = \mathrm{c} \cdot t$

Case 1) $\left\|\boldsymbol{x}c^{-1}\right\|_\infty \leq \gamma$ satisfying $n \cdot \alpha \cdot \gamma \leq \beta$

$\Rightarrow$ Set $\boldsymbol{z} = \boldsymbol{x} \cdot c^{-1}$

$\Rightarrow$ Then it is satisfied that $F_{\boldsymbol{a}}(\boldsymbol{z}) = F_{\boldsymbol{a}}(\boldsymbol{x} \cdot c^{-1}) = t$

$\Rightarrow$ Solving GCK−OW$_{n,m,\gamma}$

New GCK Problem

❖ Reduction between GCK problems

$\mathcal{B}$ (GCK-TMO adversary) $\rightarrow$ $(\boldsymbol{x}, c)$ s.t. $\|c\|_\infty \leq \alpha$, $\|\boldsymbol{x}\|_\infty \leq \beta$, and $F_{\boldsymbol{a}}(\boldsymbol{x}) = c \cdot t$

Case 2) $\left\|\boldsymbol{x}c^{-1}\right\|_\infty > \gamma$ $\Rightarrow$ Solving GCK−CR$_{n,m,\beta}$

$\mathcal{A}$ (GCK-CR adversary)

$\mathcal{B}$ (GCK-TMO adversary)

$\boldsymbol{a}$ →

$\boldsymbol{a}, t(= F_{\boldsymbol{a}}(\boldsymbol{z}))$ →

Pick $\boldsymbol{z}$ s.t. $\left||\boldsymbol{z}|\right|_\infty \leq \gamma$

← $\boldsymbol{x}, c$

$$
\begin{aligned}
F_{\boldsymbol{a}}(\boldsymbol{x}) &= t \cdot c \\
&= c \cdot F_{\boldsymbol{a}}(\boldsymbol{z}) \\
&= F_{\boldsymbol{a}}(c \cdot \boldsymbol{z})
\end{aligned}
$$

$\boldsymbol{x}c^{-1} \neq z$ $\left(\because \left||\boldsymbol{x}c^{-1}|\right|_\infty > \gamma, \left||\boldsymbol{z}|\right|_\infty \leq \gamma\right)$

$\Rightarrow \boldsymbol{x} \neq \boldsymbol{z} \cdot c$

Set $\boldsymbol{x}' = \boldsymbol{z} \cdot c$

← $(\boldsymbol{x}, \boldsymbol{x}')$

New GCK Problem

❖ Reduction between GCK problems

$\mathcal{B}$ (GCK-TMO adversary) $\rightarrow (\boldsymbol{x}, c)$ s.t. $\|c\|_\infty \leq \alpha$, $\|\boldsymbol{x}\|_\infty \leq \beta$, and $F_{\boldsymbol{a}}(\boldsymbol{x}) = c \cdot t$

$\mathcal{A}$ (GCK-CR adversary)

$\mathcal{B}$ (GCK-TMO adversary)

$\boldsymbol{a}$ →

$\boldsymbol{a}, t(= F_{\boldsymbol{a}}(\boldsymbol{z}))$ →

Pick $\boldsymbol{z}$ s.t. $\|\boldsymbol{z}\|_\infty \leq \gamma$

← $\boldsymbol{x}, c$

$$\begin{aligned} F_{\boldsymbol{a}}(\boldsymbol{x}) &= t \cdot c \\ &= c \cdot F_{\boldsymbol{a}}(\boldsymbol{z}) \\ &= F_{\boldsymbol{a}}(c \cdot \boldsymbol{z}) \end{aligned}$$

$\boldsymbol{x}c^{-1} \neq z$ $(\because \|\boldsymbol{x}c^{-1}\|_\infty > \gamma, \|\boldsymbol{z}\|_\infty \leq \gamma)$

$\Rightarrow \boldsymbol{x} \neq \boldsymbol{z} \cdot c$

Set $\boldsymbol{x}' = \boldsymbol{z} \cdot c$

← $(\boldsymbol{x}, \boldsymbol{x}')$

Case 1) $\|\boldsymbol{x}c^{-1}\|_\infty > \gamma$ $\Rightarrow$ Solving $\text{GCK-CR}_{n,m,\beta}$

Case 2) $\|\boldsymbol{x}c^{-1}\|_\infty \leq \gamma$ $\Rightarrow$ Solving $\text{GCK-OW}_{n,m,\gamma}$

New GCK Problem

❖ Reduction between GCK problems

$$Adv_{n,m,\alpha,\beta}^{GCK-TMO} \leq Adv_{n,m,\beta}^{GCK-CR} + Adv_{n,m,\beta/n\alpha}^{GCK-OW}$$

Corollary 1.2. *Let $n \geq k > 1$ be powers of 2 and $p = 2k+1 \pmod{4k}$ be a prime. Then the polynomial $X^n + 1$ factors as*

$$X^n + 1 \equiv \prod_{j=1}^{k} (X^{n/k} - r_j) \pmod{p}$$

for distinct $r_j \in \mathbb{Z}_p^*$ where $X^{n/k} - r_j$ are irreducible in the ring $\mathbb{Z}_p[X]$. Furthermore, any $\mathbf{y}$ in $\mathbb{Z}_p[X]/(X^n+1)$ that satisfies either

$$0 < \|\mathbf{y}\|_\infty < \frac{1}{\sqrt{k}} \cdot p^{1/k}$$

or

$$0 < \|\mathbf{y}\| < p^{1/k}$$

has an inverse in $\mathbb{Z}_p[X]/(X^n+1)$.

Prime $q > 2^{20}$: $k = 8, q \equiv 17 \pmod{32}$, $||c||_\infty \leq 2$

Prime $q > 2^{48}$: $k = 16, q \equiv 33 \pmod{64}$, $||c||_\infty \leq 2$

[LS18] V. Lyubashevsky et al., "*Short, Invertible Elements in Partially Splitting Cyclotomic Rings and Applications to Lattice-based Zero-Knowledge Proofs*", *EUROCRYPT 2018*

Comparison

❖ Parameter selection & Performance Analysis (~~version 1~~)

- Security parameters are determined by SIS hardness estimator – **Public key attack!**

NIST-II	n	s	q	m	B	Pk (Bytes)	Sig (Bytes)	Sk (Bytes)	Bandwidth (Pk + Sig)	KeyGen (K cycle)	Sign (K cycle)	Verify (K cycle)	SIS Hardness
Dilithium	256	2	$\approx 2^{23}$	(4,4)	2^{17}	1,312	2,420	2,544	3,732	272	1,323	298	123
Ours	256	1	$\approx 2^{54}$	4	$2^{14}-1$	1,760	1,952	288	3,712	184	1,062	237	125

NIST-III	n	s	q	m	B	Pk (Bytes)	Sig (Bytes)	Sk (Bytes)	Bandwidth (Pk + Sig)	KeyGen (K cycle)	Sign (K cycle)	Verify (K cycle)	SIS Hardness
Dilithium	256	4	$\approx 2^{23}$	(6,5)	2^{19}	1,952	3,293	4,016	5,245	495	2,155	520	182
Ours	256	1	$\approx 2^{60}$	4	$2^{14}+2^{9}$	1,952	2,080	288	4,032	202	1,240	253	183

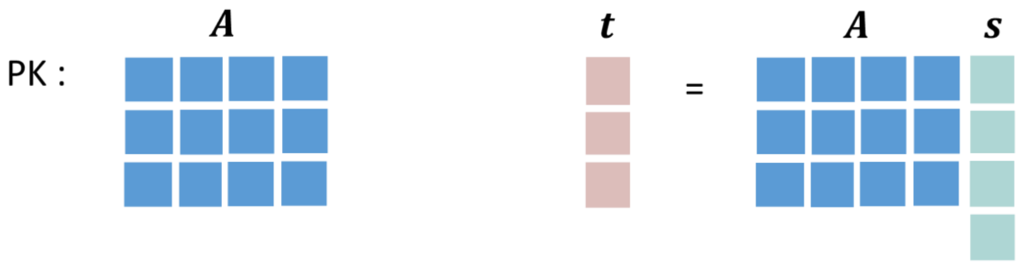
NIST-V	n	s	q	m	B	Pk (Bytes)	Sig (Bytes)	Sk (Bytes)	Bandwidth (Pk + Sig)	KeyGen (K cycle)	Sign (K cycle)	Verify (K cycle)	SIS Hardness
Dilithium	256	2	$\approx 2^{23}$	(8,7)	2^{19}	2,592	4,595	4,880	7,187	728	2,592	779	265
Ours	512	1	$\approx 2^{47}$	3	$2^{15}-1$	3,040	3,104	588	6,144	265	1,421	373	268

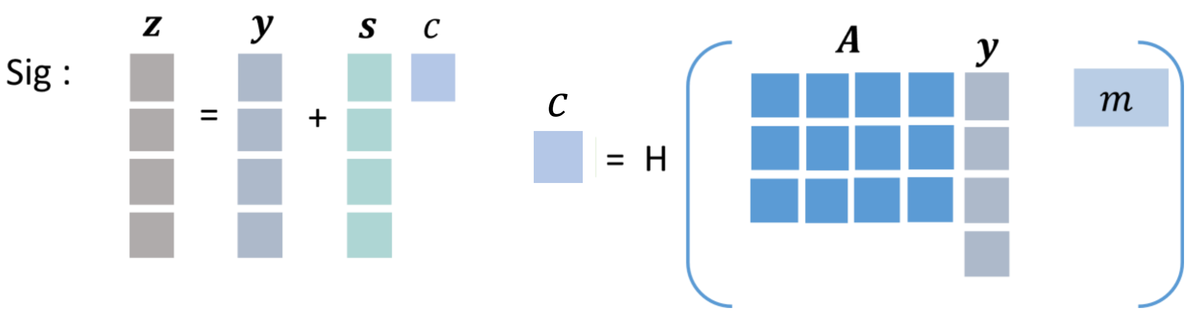
GCK-Based Signatures (3)

- **GCK function** F_a **and** $\boldsymbol{R_q = Z_q[x]/< x^n + 1 >}$, $q = prime$
  - **Public key :**$(A,\ \boldsymbol{t} = F_A(\boldsymbol{s}))\ \in R_q^{k\times\ell} \times R_q^k$ **Secret key :** $\boldsymbol{s}$
  - **Sign :** $(\boldsymbol{z}, c) = (\boldsymbol{y} + c \cdot \boldsymbol{s},\ c = H(F_A(\boldsymbol{y}),\ m)) \in R^{\ell}_{[-B+L_s, B-L_s]} \times \{0,1\}^w$

$\boldsymbol{s} \leftarrow R^{\ell}_{[-\eta,\eta]}$

$\boldsymbol{y} \leftarrow R^{\ell}_{[-B,B]}$





- **Verification: (1) compute** $\mathrm{F}_A(\mathbf{z}) - c \cdot \boldsymbol{t} = \mathrm{F}_A(\mathbf{y})$

  (2) check if $c = H(F_A(\boldsymbol{y}), m)$

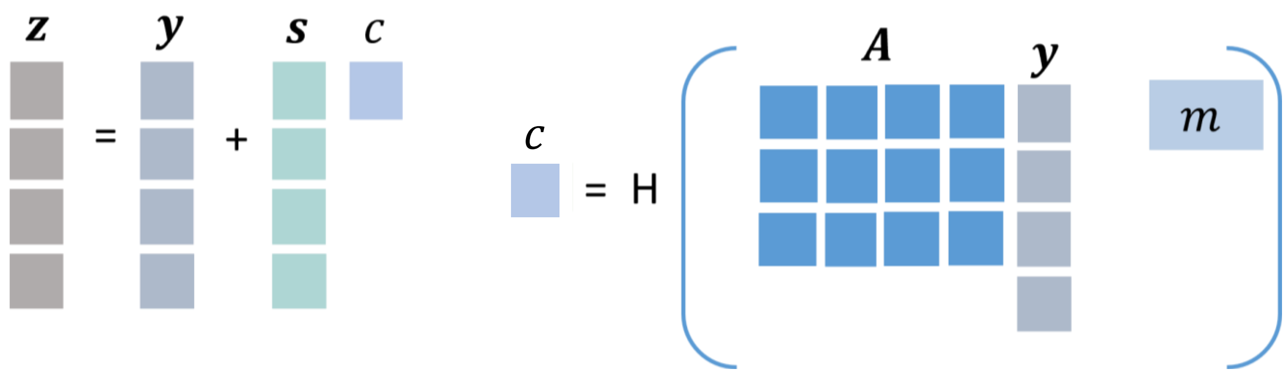
GCK-Based Signatures (4)

- **GCK function** F_a **and** $\boldsymbol{R_q} = \boldsymbol{Z_q}[\boldsymbol{x}]/< \boldsymbol{x^n} + \mathbf{1} >$, $q = prime$
  - **Public key :** $(A,\ \boldsymbol{t} = F_{\boldsymbol{A}}(\boldsymbol{s})) \in R_q^{k\times\ell} \times R_q^k$ **Secret key :** $\boldsymbol{s}$
  - **Sign :** $(\boldsymbol{z}, c) = (\boldsymbol{y} + c \cdot \boldsymbol{s},\ c = H(F_{\boldsymbol{A}}(\boldsymbol{y}),\ m)) \in R^{\ell}_{[-B+L_S, B-L_S]} \times \{0,1\}^w$

$\boldsymbol{s} \leftarrow R^{\ell}_{[-\eta,\eta]}$

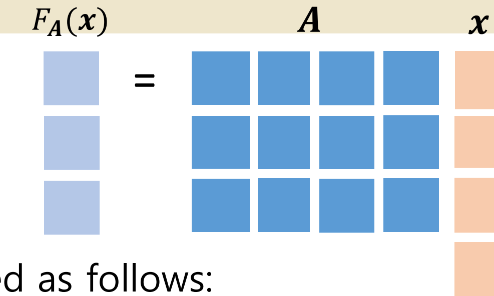
$\boldsymbol{y} \leftarrow R^{\ell}_{[-B,B]}$

Sig :



- Check if $||\boldsymbol{y} + c \cdot \boldsymbol{s}|| < B - L_s$ Security check on s
  $\cancel{||low(\boldsymbol{A} \cdot \boldsymbol{y} - c \cdot \boldsymbol{e})|| < 2^d - L_e}$ Correctness check
  $\cancel{[\boldsymbol{A} \cdot \boldsymbol{y} - c \cdot \boldsymbol{e}]_d = [\boldsymbol{A} \cdot \boldsymbol{y}]_d}$

GCK Function



❖ Module-GCK

◆ Definition

- For a ring R, integer k, ℓ, GCK function $F_{\boldsymbol{A}}: R^{k\times\ell} \to R^k$ is defined as follows:

$$F_{\boldsymbol{A}}(\boldsymbol{x}) = (t_1, \dots, t_k) \text{ where } t_i = \sum_{j=1}^{\ell} x_j \cdot a_{ij} \text{ and } \|\boldsymbol{x}\|_\infty \le \beta$$

◆ OW of Module-GCK problem

- Given $\boldsymbol{A} \in R^{k\times\ell}$ and $\boldsymbol{t} \in R^k$, **find $\boldsymbol{x} \in \boldsymbol{R}^{\ell}$** s.t. $\|\boldsymbol{x}\|_\infty \le \beta$ and $F_{\boldsymbol{A}}(\boldsymbol{x}) = \boldsymbol{t}$

◆ CR of Module-GCK problem

- Given $\boldsymbol{A} \in R^{k\times\ell}$, **find $\boldsymbol{x}, \boldsymbol{y} \in \boldsymbol{R}^{\ell}$** s.t. $\boldsymbol{x} \ne \boldsymbol{y}$, $\|\boldsymbol{x}\|_\infty \le \beta$, $\|\boldsymbol{y}\|_\infty \le \beta$ and $F_{\boldsymbol{A}}(\boldsymbol{x}) = F_{\boldsymbol{A}}(\boldsymbol{y})$

◆ TMO of Module-GCK problem

- Given $\boldsymbol{A} \in R^{k\times\ell}$ and $\boldsymbol{t} \in R^k$, **find $\boldsymbol{x}, c$** s.t. $\|c\|_\infty \le \alpha$, $\|\boldsymbol{x}\|_\infty \le \beta$, and $F_{\boldsymbol{A}}(\boldsymbol{x}) = c \cdot \boldsymbol{t}$

Comparison

❖ Parameter selection & Performance Analysis (revised)

- **Security parameters are determined by LWE & SIS hardness estimator**

NIST-II	n	s	q	(k,ℓ)	B	Pk (Bytes)	Sig (Bytes)	Pk+Sig (Bytes)	Sk (Bytes)	LWE Hardness	SIS Hardness
Dilithium	256	2	$\approx 2^{23}$	(4,4)	2^{17}	1,312	2,420	3,732	2,544	123	123
Ours	256	1	$\approx 2^{20}$	(3,4)	$2^{15}-1$	1,952	2,080	4,032	288	136	142

NIST-III	n	s	q	(k,ℓ)	B	Pk (Bytes)	Sig (Bytes)	Pk+Sig (Bytes)	Sk (Bytes)	LWE Hardness	SIS Hardness
Dilithium	256	4	$\approx 2^{23}$	(6,5)	2^{19}	1,952	3,293	5,245	4,016	182	186
Ours	256	1	$\approx 2^{19}$	(4,5)	$2^{15}+2^{12}$	2,464	2,752	5,216	352	191	194

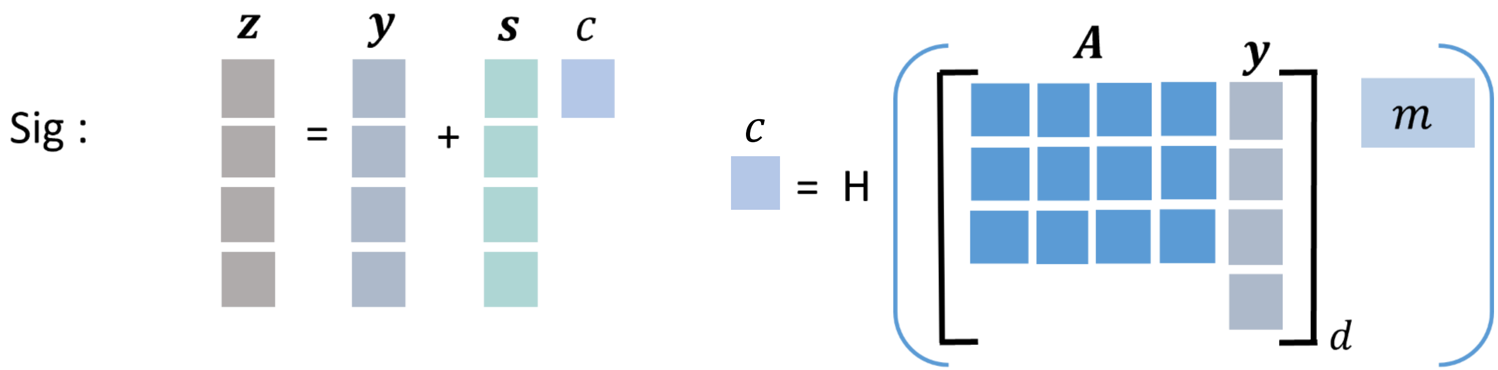
NIST-V	n	s	q	(k,ℓ)	B	Pk (Bytes)	Sig (Bytes)	Pk+Sig (Bytes)	Sk (Bytes)	LWE Hardness	SIS Hardness
Dilithium	256	2	$\approx 2^{23}$	(8,7)	2^{19}	2,592	4,595	7,187	4,880	252	265
Ours	256	1	$\approx 2^{21}$	(5,7)	$2^{15}+2^{13}$	3,392	3,840	7,232	480	262	272

GCK-Based Signatures (ongoing)

- **GCK function** F_a **and** $\boldsymbol{R_q} = \boldsymbol{Z_q}[\boldsymbol{x}]/<\boldsymbol{x^n}+\boldsymbol{1}>$, $q = prime$
  - **Public key :** $(A,\ \boldsymbol{t}_1 = [F_{\boldsymbol{A}}(\boldsymbol{s})]_\alpha) \in R_q^{k\times\ell} \times R_q^k$ **Secret key :** $\boldsymbol{s}, \boldsymbol{t}_0$
  - **Sign :** $(\boldsymbol{z}, c) = (\boldsymbol{y} + c\cdot\boldsymbol{s},\ c = H([F_{\boldsymbol{A}}(\boldsymbol{y})]_d,\ m))$

$\boxed{\boldsymbol{s} \leftarrow R^{\ell}_{[-\eta,\eta]}}$

$\boxed{\boldsymbol{y} \leftarrow R^{\ell}_{[-B,B]}}$



- Check if $||\boldsymbol{y} + c\cdot\boldsymbol{s}|| < B - L_s$ — Security check on s
  $\cancel{||low(\boldsymbol{A}\cdot\boldsymbol{y} - c\cdot\boldsymbol{e})|| < 2^d - L_e}$ — ~~Correctness check~~
  $\cancel{[\boldsymbol{A}\cdot\boldsymbol{y} - c\cdot\boldsymbol{e}]_d = [\boldsymbol{A}\cdot\boldsymbol{y}]_d}$

- Create $h = Hint(-c\cdot\boldsymbol{t}_0,\ \boldsymbol{A}\cdot\boldsymbol{y} + c\cdot\boldsymbol{t}_0,\ d)$

Create a carry bit hint vector h caused by ignoring $c\cdot\boldsymbol{t}_0$

Comparison(expected)

❖ Parameter selection & Performance Analysis (ongoing)

- **Security parameters are determined by LWE & SIS hardness estimator**

NIST-II	n	s	q	(k,ℓ)	B	Pk (Bytes)	Sig (Bytes)	Pk+Sig (Bytes)	Sk (Bytes)	LWE Hardness	SIS Hardness
Dilithium	256	2	$\approx 2^{23}$	(4,4)	2^{17}	1,312	2,420	3,732	2,544	123	123
Ours	256	1	$\approx 2^{20}$	(3,4)	$2^{15}-1$	1,952	2,080	4,032	288	136	142
w/ hint	-	-	-	-	-	992	2,080	3,072	1,248	136	142

NIST-III	n	s	q	(k,ℓ)	B	Pk (Bytes)	Sig (Bytes)	Pk+Sig (Bytes)	Sk (Bytes)	LWE Hardness	SIS Hardness
Dilithium	256	4	$\approx 2^{23}$	(6,5)	2^{19}	1,952	3,293	5,245	4,016	182	186
Ours	256	1	$\approx 2^{19}$	(4,5)	$2^{15}+2^{12}$	2,464	2,752	5,216	352	191	194
w/ hint	-	-	-	-	-	1,248	2,752	4,000	1,568	191	194

NIST-V	n	s	q	(k,ℓ)	B	Pk (Bytes)	Sig (Bytes)	Pk+Sig (Bytes)	Sk (Bytes)	LWE Hardness	SIS Hardness
Dilithium	256	2	$\approx 2^{23}$	(8,7)	2^{19}	2,592	4,595	7,187	4,880	252	265
Ours	256	1	$\approx 2^{21}$	(5,7)	$2^{15}+2^{13}$	3,392	3,840	7,232	480	262	272
w/ hint	-	-	-	-	-	1,712	3,840	5,552	2,160	262	272

Thank You

Q&A