GCKSign

Simple and Efficient Signature Schemes from Generalized Compact Knapsacks

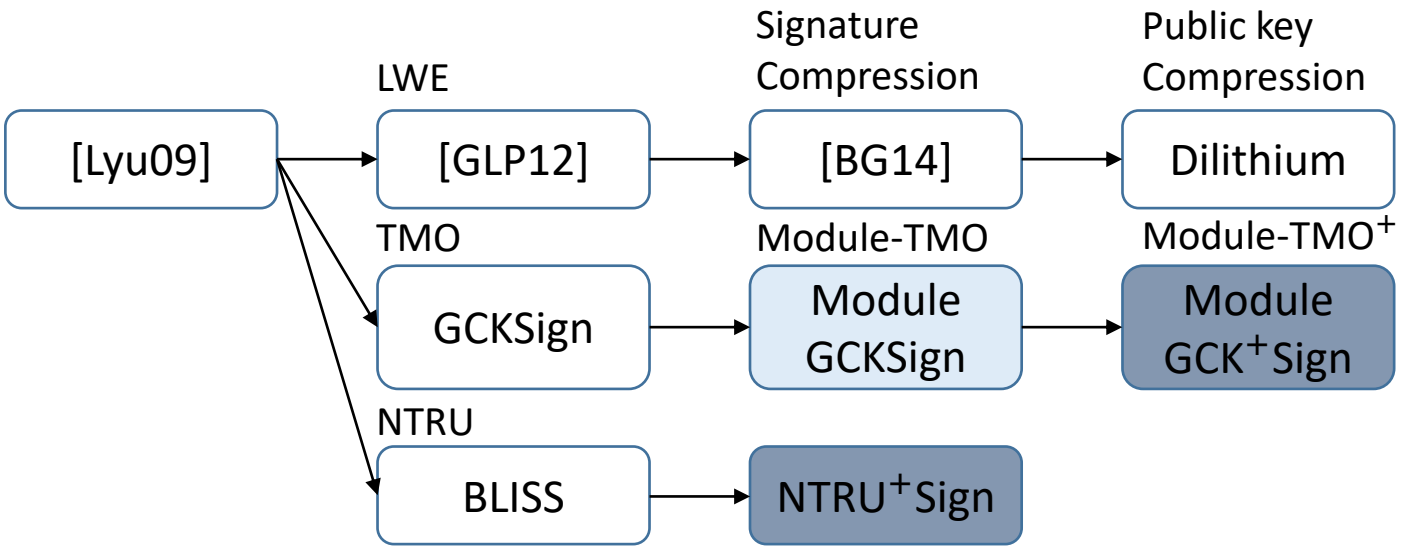
2023.05.17.

고려대학교

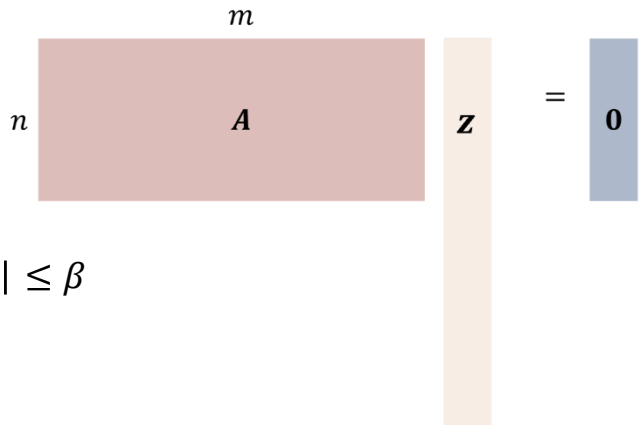
우 주

Lattice-based Signatures

❖ Overview (w/ Fiat-Shamir Transform)



Lattice Problems



❖ Short Integer Solutions(SIS) Problem

◆ Definition

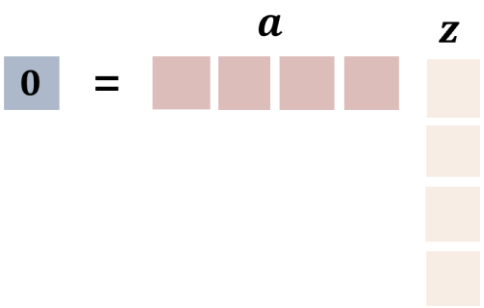
- Given a matrix $\boldsymbol{A} \in \mathbb{Z}_q^{n \times m}$ and a real β,
  find a vector $\boldsymbol{z} \in \mathbb{Z}^m$ such that $\boldsymbol{Az} = \mathbf{0}$ mod q and $0 < \|\boldsymbol{z}\| \leq \beta$

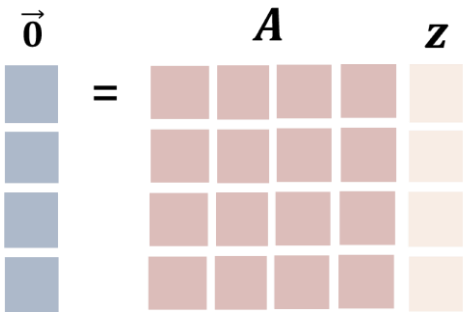
◆ Ring-SIS Problem

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

◆ 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 $\boldsymbol{A} \cdot \boldsymbol{z} = \mathbf{0}$ mod q and $0 < \|\boldsymbol{z}\| \leq \beta$





Lattice Problems

❖ Learning with Errors(LWE) Problem

◆ Definition

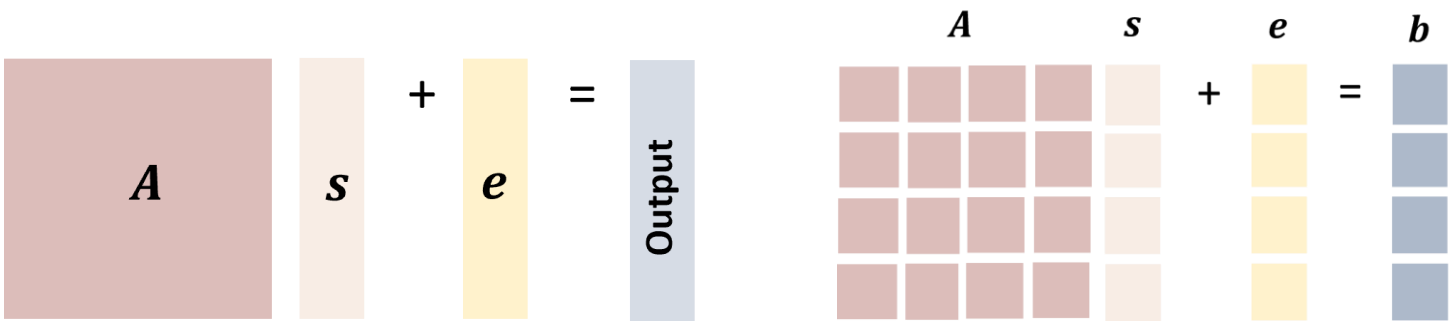
- **Search** : Given $\boldsymbol{A} \in \mathbb{Z}_q^{m \times n}$ and $\boldsymbol{b} = \boldsymbol{As} + \boldsymbol{e}$ where $\boldsymbol{e} \leftarrow \chi$, find a vector $s \in \mathbb{Z}_q^n$
- **Decision** : Distinguish $(\boldsymbol{A}, \boldsymbol{As} + \boldsymbol{e})$ from uniform $(\boldsymbol{A},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

◆ Ring-LWE Problem

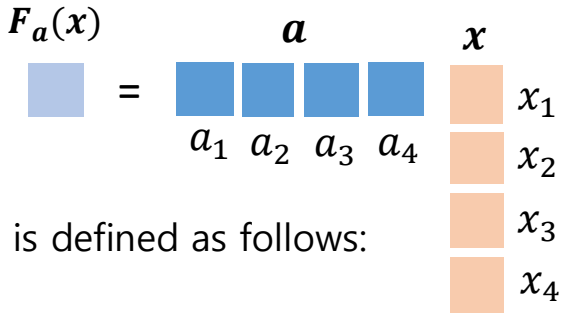
- Given $\boldsymbol{a} \in R_q^k$ and $\boldsymbol{b} = \boldsymbol{a} \cdot s + \boldsymbol{e}$ where $\boldsymbol{e} \leftarrow \chi$, find $s \in R_q$

◆ 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 $F_{\boldsymbol{a}}: R^m \rightarrow R$ is defined as follows:

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

◆ Onewayness of GCK problem

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

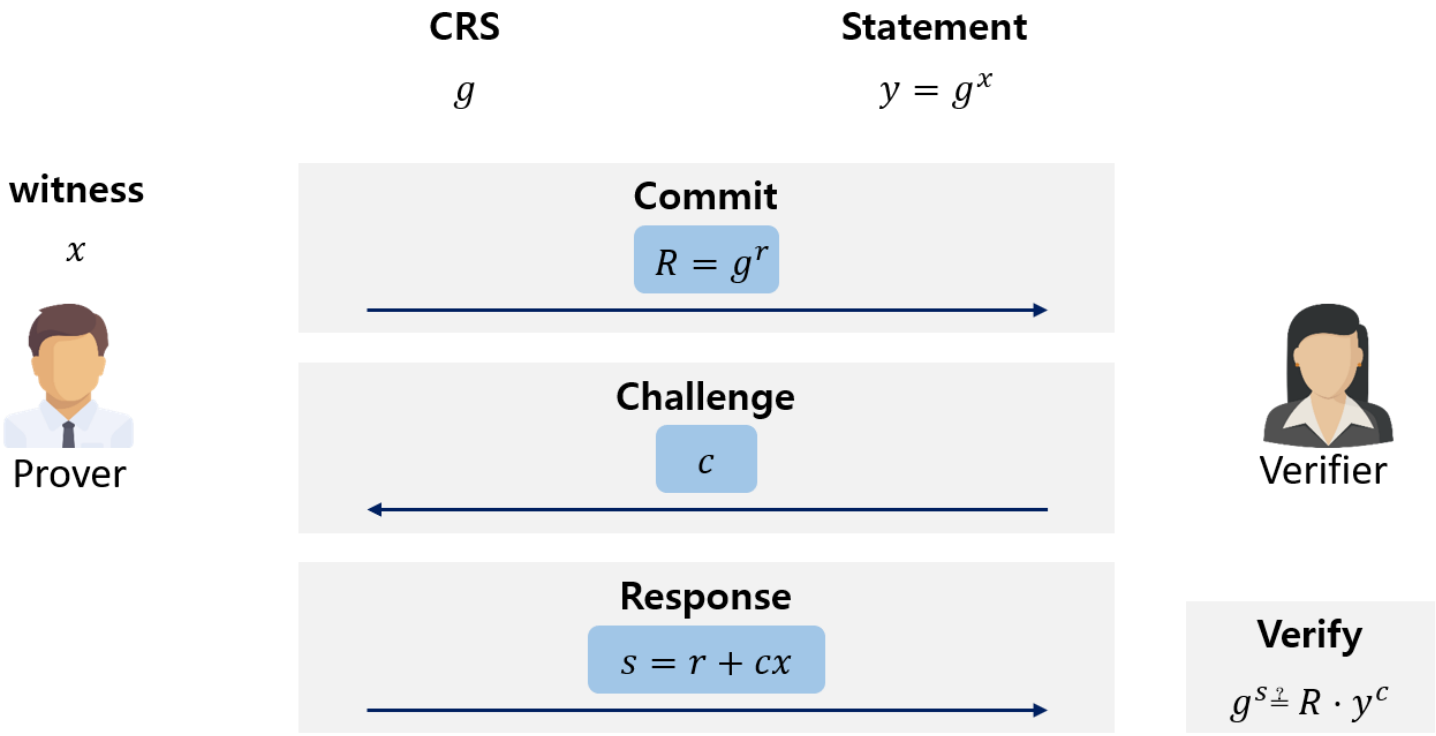
[LM06] V. Lyubashevsky et al., "*Generalized Compact Knapsacks Are Collision Resistant*", *ICALP 2006*

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

Lattice-based Signatures

❖ Lattice-based Signature

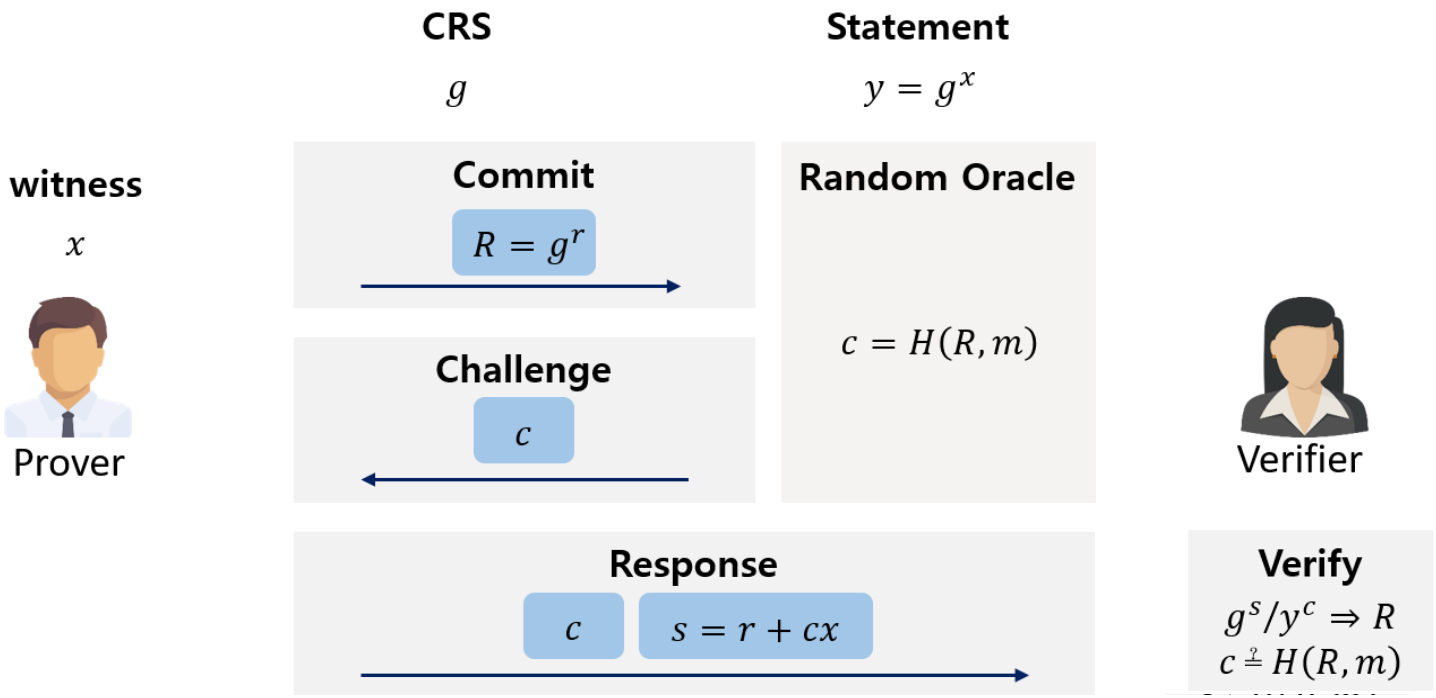
◆ Schnorr Identification



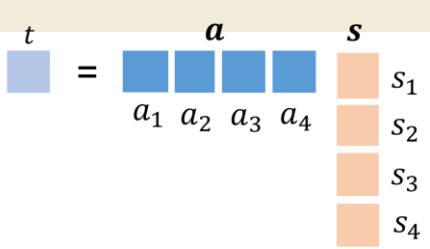
Lattice-based Signatures

❖ Lattice-based Signature

◆ Schnorr Signature (w/ Fiat-Shamir Transform)



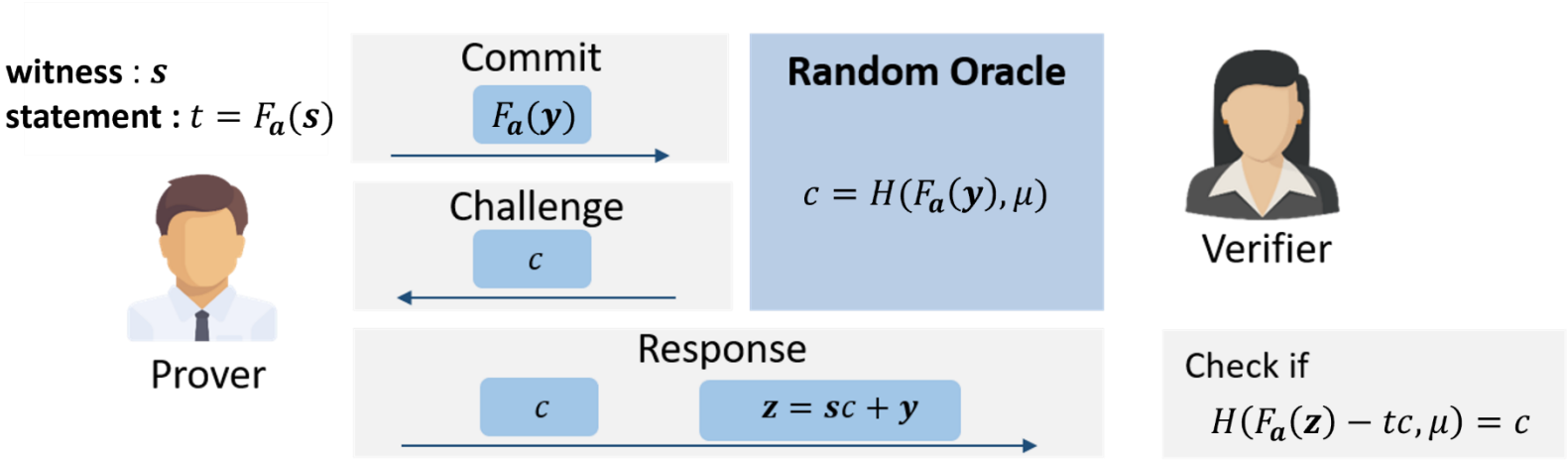
Lattice-based Signatures



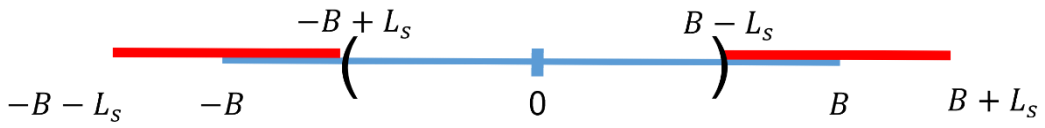
❖ Lattice-based Signature

◆ 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 $\|\boldsymbol{s}\|_\infty \leq \beta$



- 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)

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

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

$\boldsymbol{a}$

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

$\boldsymbol{a}, t$

$Y = F_a(\boldsymbol{y})$

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

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

By rewinding technique

Set $\boldsymbol{x} = \boldsymbol{z} - \boldsymbol{sc}$, $\boldsymbol{x}' = \boldsymbol{z}' - \boldsymbol{sc}'$ $\left(\begin{matrix} \neq \boldsymbol{y} + \boldsymbol{sc} - \boldsymbol{sc} \\ \neq \boldsymbol{y} + \boldsymbol{sc}' - \boldsymbol{sc}' \end{matrix}\right)$

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

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

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

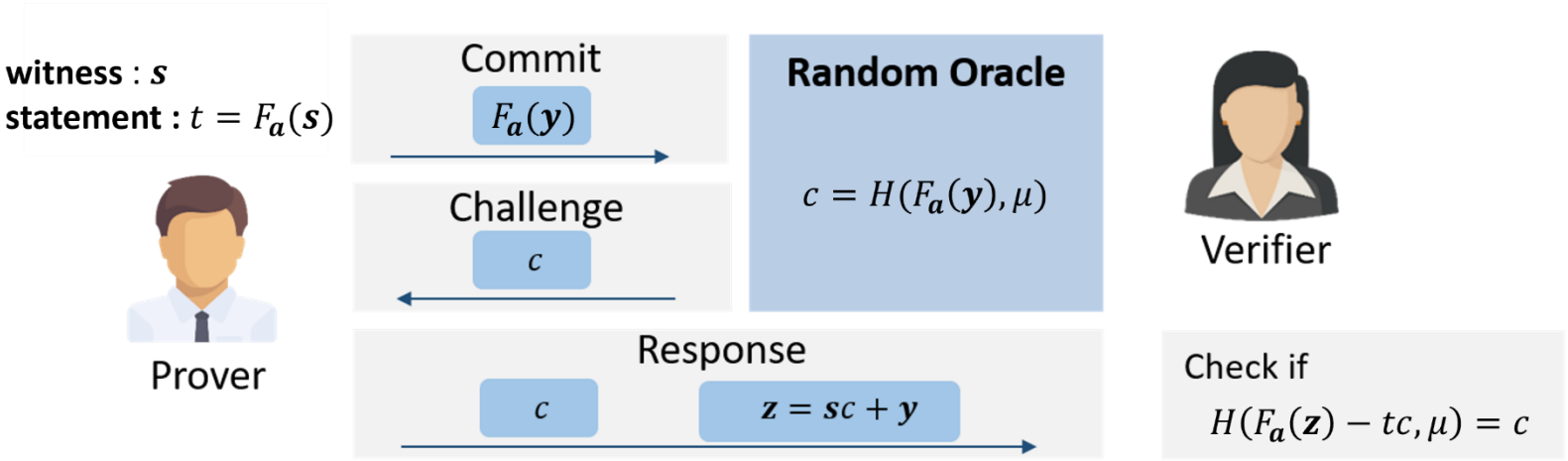
[Lyu09] V. Lyubashevsky., "*Fiat-Shamir with Aborts: Applications to Lattice and Factoring-based Signatures*", *ASIACRYPT 2009*

Lattice-based Signatures

❖ Lyubashevsky's Identification Scheme

◆ Principle

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



◆ Limitation

- Security proof based on GCK collision-resistance problem + additional security requirement

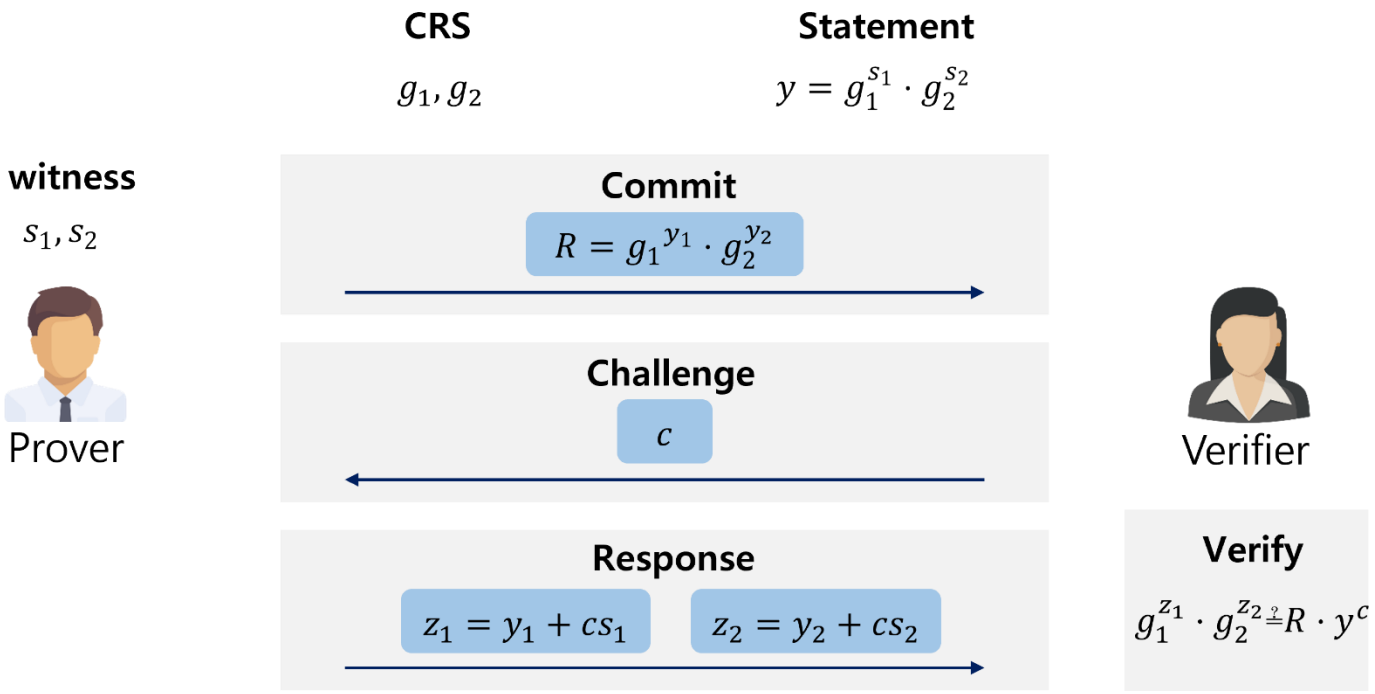
	n	s	L_s	q	m	B	Pk (Bytes)	Sig (Bytes)	Sk (Bytes)	Bandwidth (Pk + Sig)	SIS Hardness
Lyu09	512	2,047	$\approx 2^{15}$	$\approx 2^{95.8}$	5	$\approx 2^{28.6}$	6,125	14,875	6,125	21,000	127
Dilithium	256	2	78	$\approx 2^{23}$	(4,4)	2^{17}	1,312	2,420	2,544	3,732	123

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

Lattice-based Signatures

❖ Lattice-based Signature

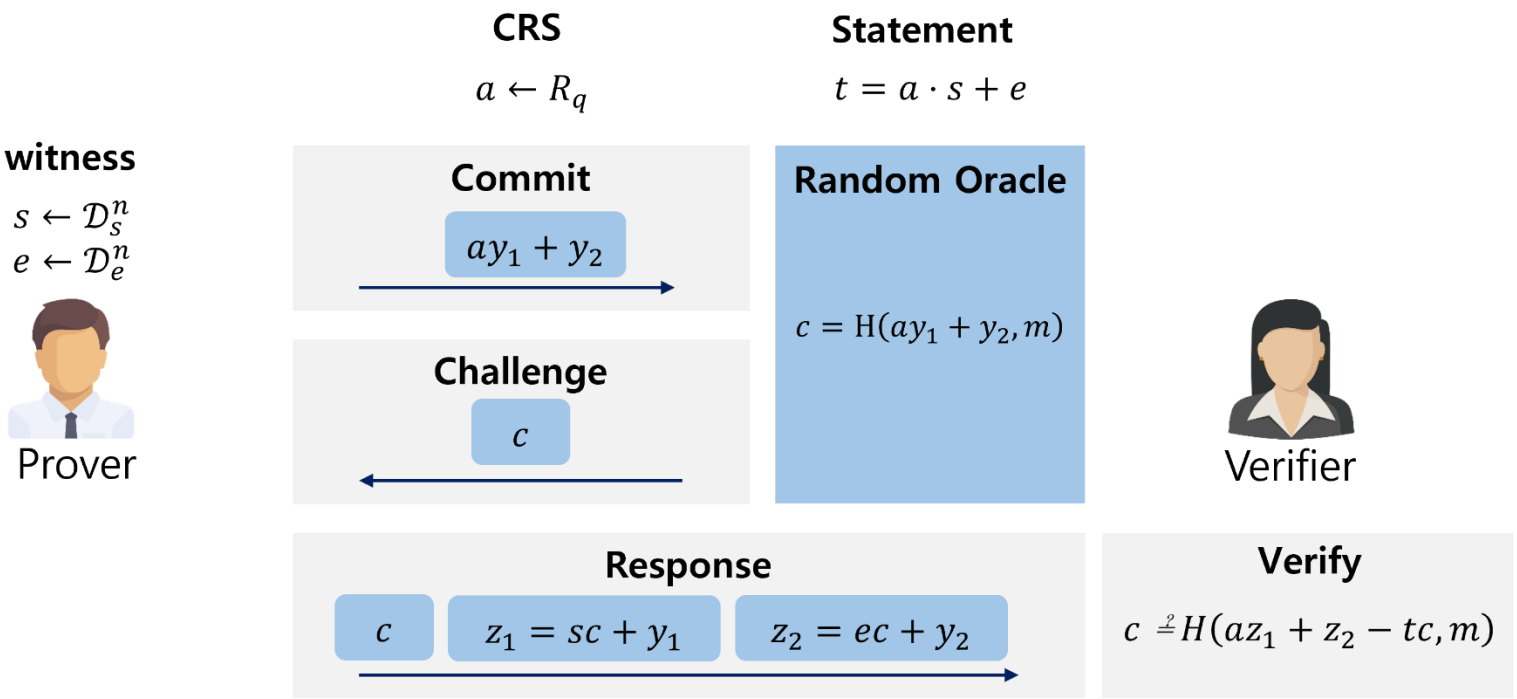
◆ A Variant of Schnorr Identification



Lattice-based Signatures

❖ Lattice-based Signature

◆ Identification Protocol [GLP12]



[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 $\boldsymbol{x_1, x_2}$
such that $\boldsymbol{ax_1 + x_2 = 0}$

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

$\boldsymbol{a}$

Decisional – LWE problem

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

$\boldsymbol{a}, t$

$Y = ay_1 + y_2$

get two forgery $(c, \boldsymbol{z}), (c', \boldsymbol{z'})$
Such that
$\boldsymbol{az_1 + z_2 - tc = Y},$
$\boldsymbol{az_1' + z_2' - tc' = Y}$

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

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

$\boldsymbol{x_1, x_2}$

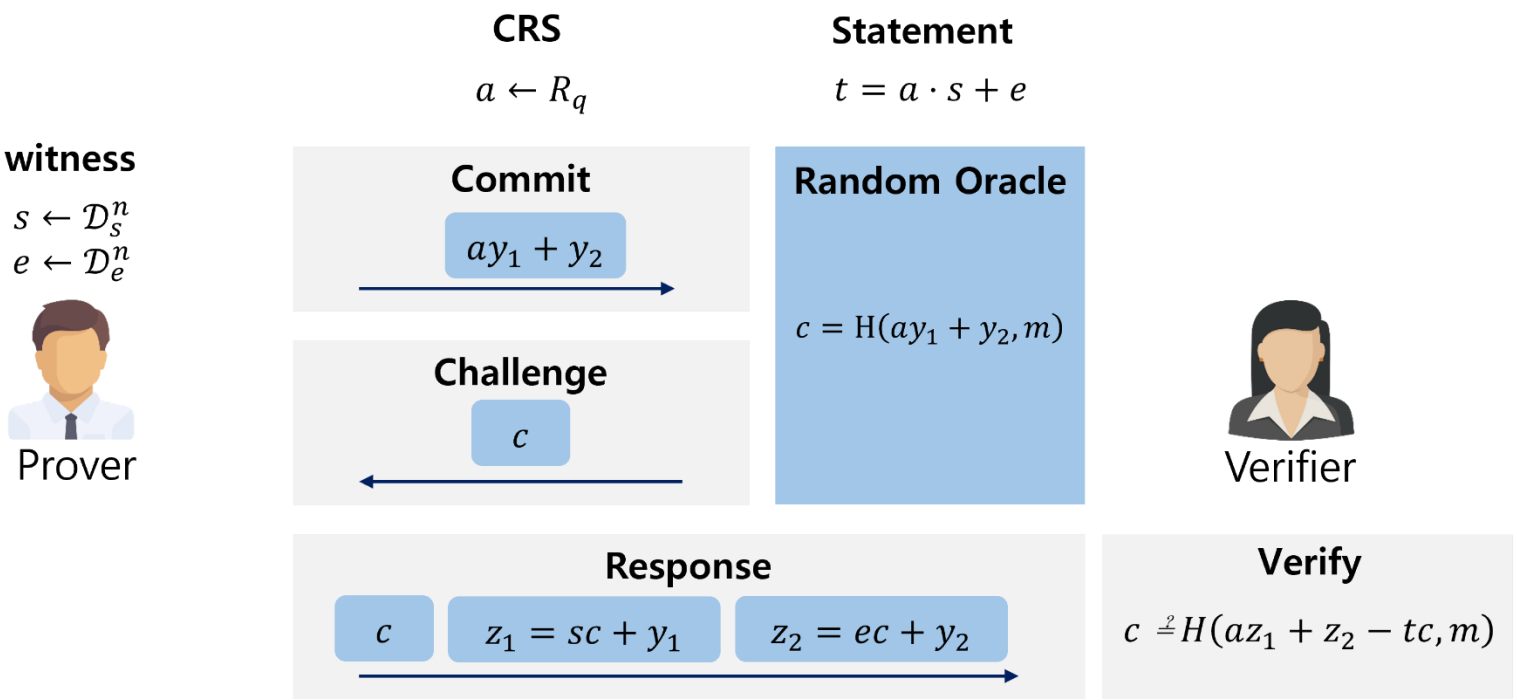
$\boldsymbol{x_1 \neq 0}$ & $\boldsymbol{x' \neq 0}$ ***by*** *witness indsistinguishability* ⇒ ~~Security Requirement : $q^n \ll (2\beta + 1)^{mn}$~~

[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 [GLP12]



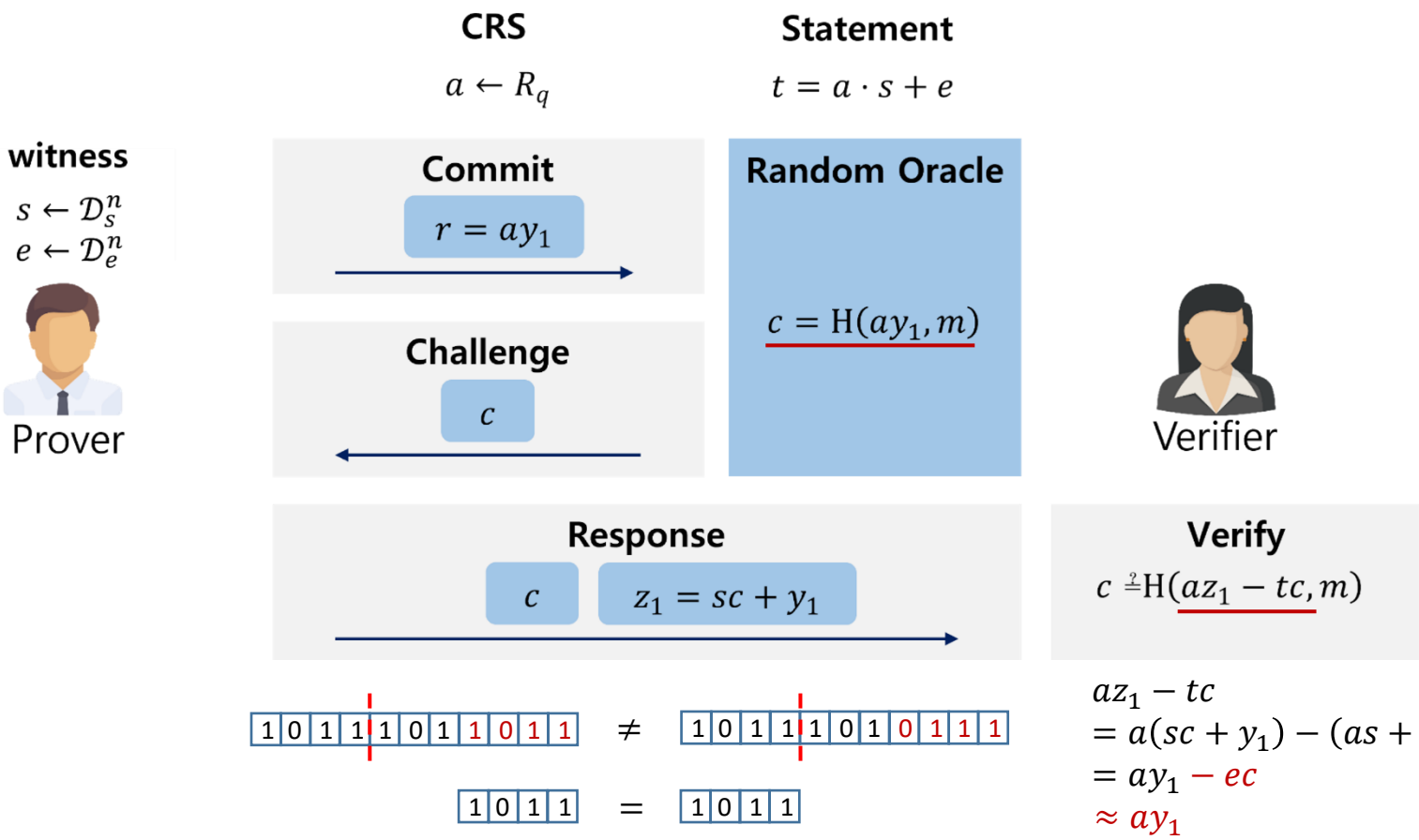
[GLP12] T. Güneysu et al., "*Practical Lattice-based Cryptography: A Signature Scheme for Embedded Systems*", *CHES 2012*

Lattice-based Signatures

❖ Lattice-based Signature

◆ Improved Identification Protocol [BG14]

Signature Size Reduction



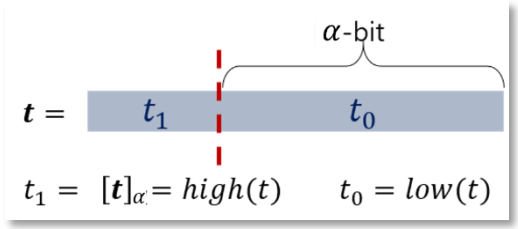
[BG14] S. Bai et al., "*An Improved Compression Technique for Signatures based on Learning with Errors*", *CT-RSA 2014*

Lattice-based Signatures

❖ Lattice-based Signature

◆ Dilithium (MLWE + MSIS)

PK compression



CRS

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

Statement

$t \equiv As + e = t_1 \cdot 2^{\alpha} + t_0$

witness

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

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

Prover

Commit

$r \equiv Ay$

Challenge

c

Random Oracle

$c = \mathrm{H}([Ay]_d, \mu)$

Verifier

Response

c $\quad z = sc + y$

Verify

$c \stackrel{?}{=} \mathrm{H}([Az - 2^{\alpha} t_1 c]_d, m)$

$$Az - ct_1 \cdot 2^{\alpha} = Az - c(t - t_0)$$
$$= Az - tc - ct_0$$
$$= Ay - ec - ct_0$$

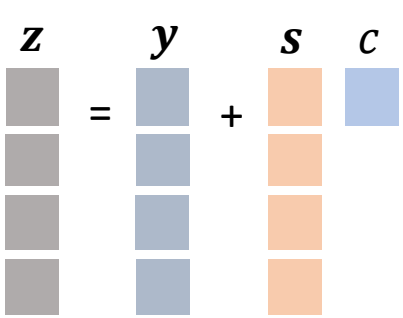
[DKL+18] L. Ducas et al., "*CRYSTALS-Dilithium: A Lattice-based Digital Signature Scheme*", *TCHES 2018*

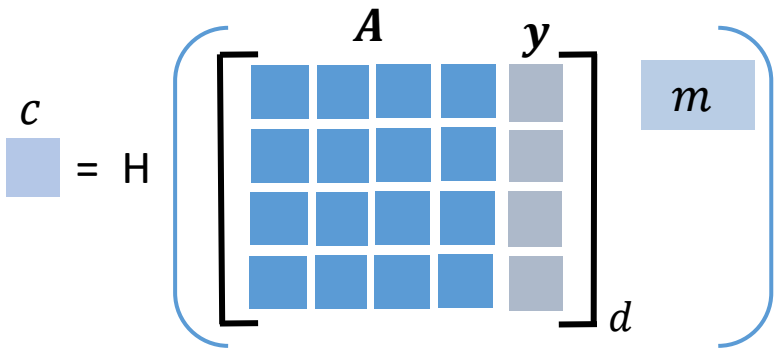
Lattice-based Signatures

❖ 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 :** $(\boldsymbol{z}, c, h) = (\boldsymbol{y}+c\boldsymbol{s},\ \ c = H([\boldsymbol{Ay}]_{\boldsymbol{d}},\ m), h = Hint(-c\boldsymbol{t}_0,\ \boldsymbol{Ay}-\ c\boldsymbol{e}\ + c\boldsymbol{t}_0,\ d))$

Sig :





- **Check if** $||\boldsymbol{y}+c\boldsymbol{s}||_\infty < B - L_s$

  $||low(\boldsymbol{Ay}-\ c\boldsymbol{e})||_\infty < 2^d - L_e$

  $||low(c\boldsymbol{t}_0)||_\infty < 2^d$

Security check on s [Lyu09]

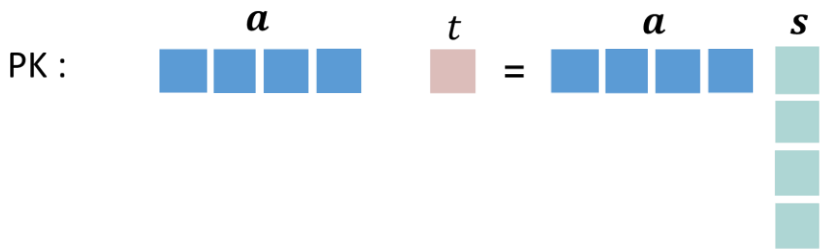
Security check on e [GLP12], [BG14]

Correctness check for hint [Dilithium]

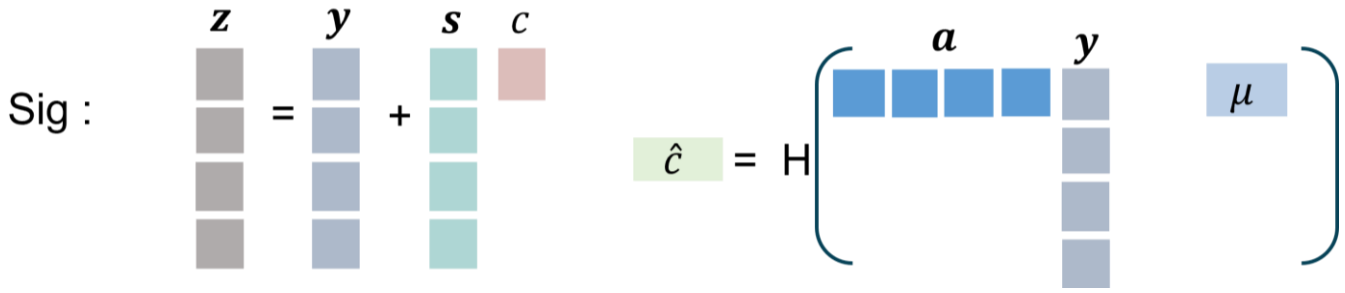
GCK-Based Signatures (1)

❖ **GCK function F_a and $R_q = Z_q[x]/< x^n + 1 >$, $q = prime$** for NTT

- **Public key :** $(a,\ t = F_a(s)) \in R_q^m \times R_q$ **Secret key :** $s \in R_{[-\eta,\eta]}^m$



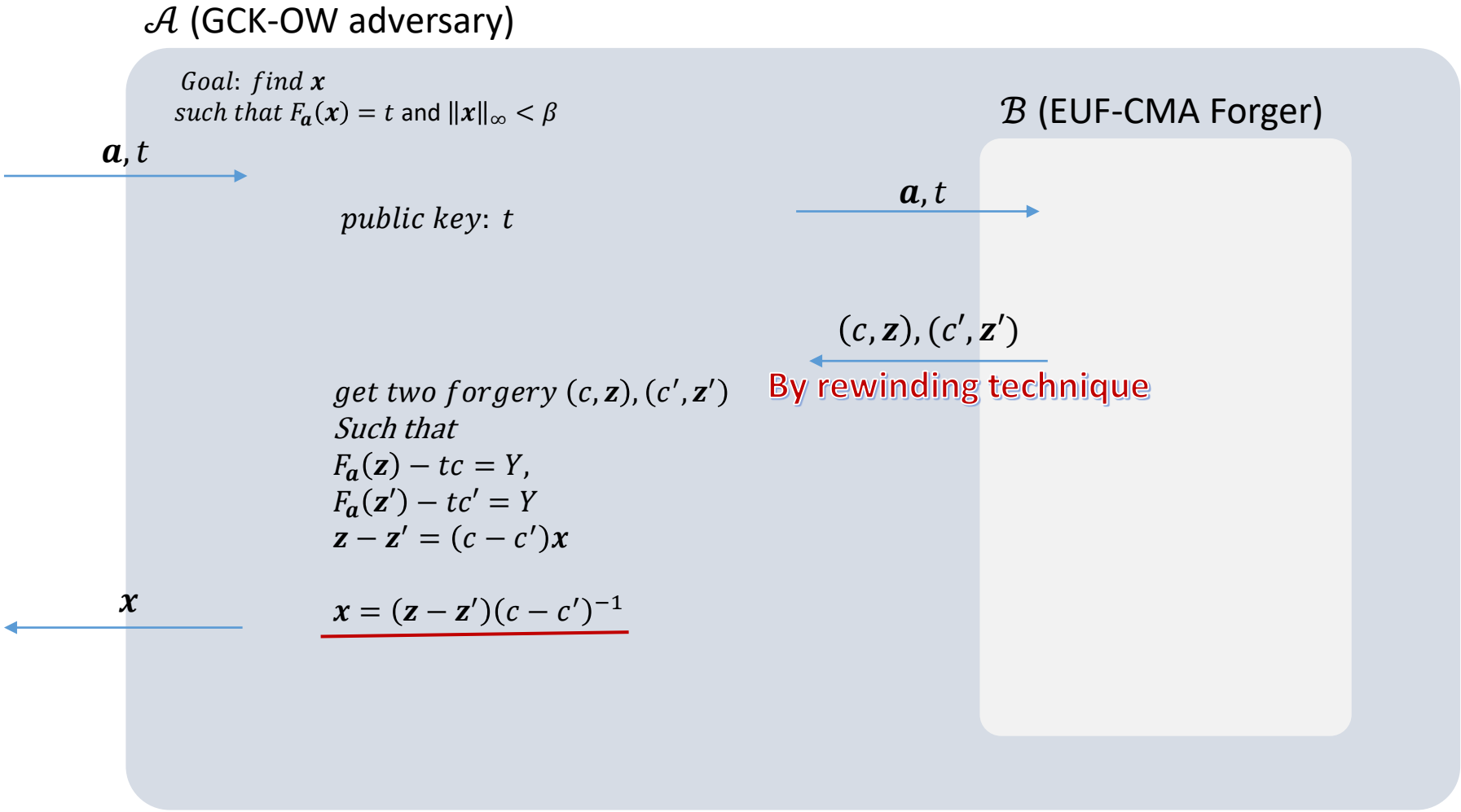
- **Sign :** $(z, \hat{c}) = (y + c \cdot s,\ \hat{c} = H(F_a(y),\ \mu)) \in R_{[-B+L_s,B-L_s]}^m \times \{0,1\}^{\ell_1}$



- $||c \cdot s|| < L_s$ ← c : sparse ternary distribution and $s \leftarrow R_{[-\eta,\eta]}^m$
- Check if $||z|| = ||y + c \cdot s|| < B - L_s$ to prevent leakage of s from z

- **Verification: (1) compute** $a \cdot z - c \cdot t = a \cdot y$
  (2) check if $\hat{c} = H(a \cdot y,\ \mu)$

❖ Security Proof based on GCK-OW (trial)



New GCK Problem

❖ Generalized Compact Knapsack(GCK)

◆ One-wayness of GCK problem

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

◆ Collision-Resistance of GCK problem

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

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

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

New GCK Problem

❖ Security Proof

◆ Security based on GCK-TMO Problem

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

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

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

$\boldsymbol{a}, t$

public key: t

$\boldsymbol{a}, t$

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

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

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

By rewinding technique

◆ **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. $\|c\|_\infty \leq \alpha$, $\|x_i\|_\infty \leq \beta$, and $F_{\boldsymbol{a}}(\boldsymbol{x}) = c \cdot t$

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

$||\boldsymbol{x}||_\infty \leq 2(B - L_s)$
$||\tilde{c}||_\infty \leq 2$

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

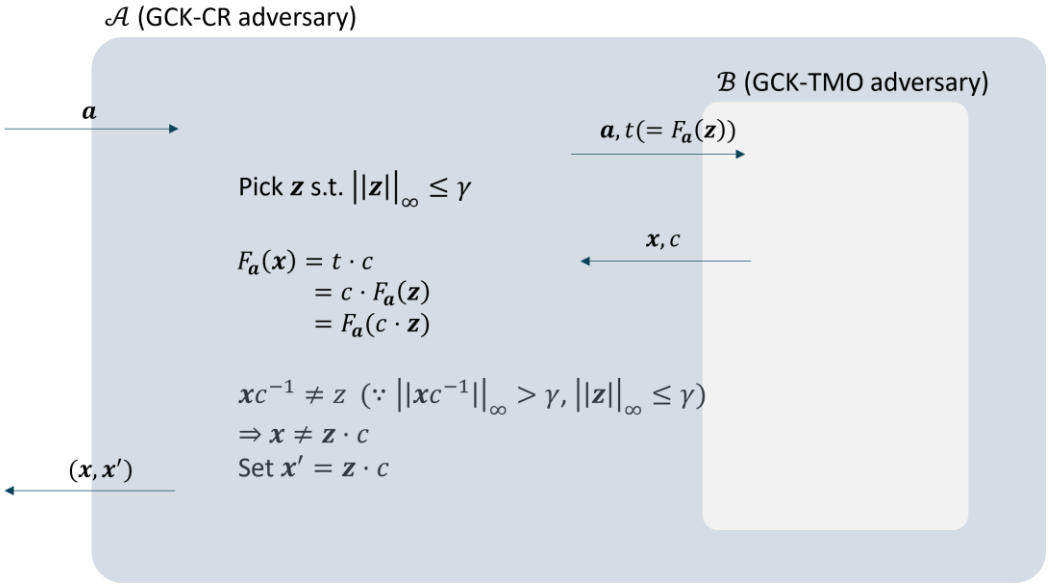
$\Rightarrow$ Set $\boldsymbol{z} = \boldsymbol{x} \cdot c^{-1}$

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

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

Case 2) $\left|\left|\boldsymbol{x}c^{-1}\right|\right|_\infty > \gamma$

$\Rightarrow$ Solving GCK−CR$_{n,m,\beta}$



Comparison

❖ Parameter selection & Performance Analysis (v0.1)

◆ Security parameters are determined by SIS hardness estimator

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

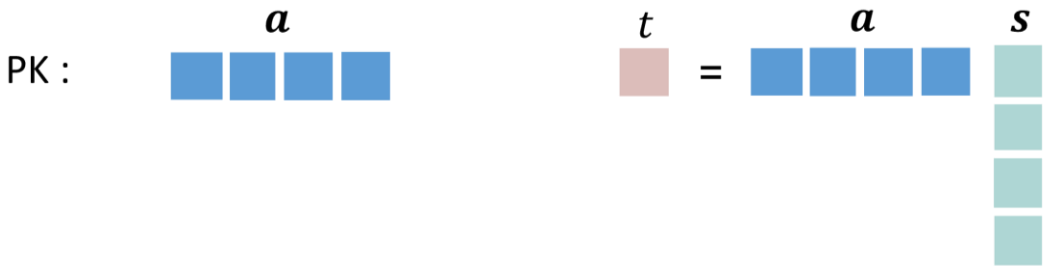
NIST-III	n	s	q	m	B	Pk (Bytes)	Sig (Bytes)	Sk (Bytes)	Bandwidth (Pk + Sig)	KeyGen (K cycle)	Sign (K cycle)	Verify (K cycle)	SIS Hardness
Dilithium	256	4	$\approx 2^{23}$	(6,5)	2^{19}	1,952	3,293	4,016	5,245	495	2,155	520	182
Ours	256	1	$\approx 2^{60}$	4	$2^{14}+2^{9}$	1,952	2,080	288	4,032	202	1,240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

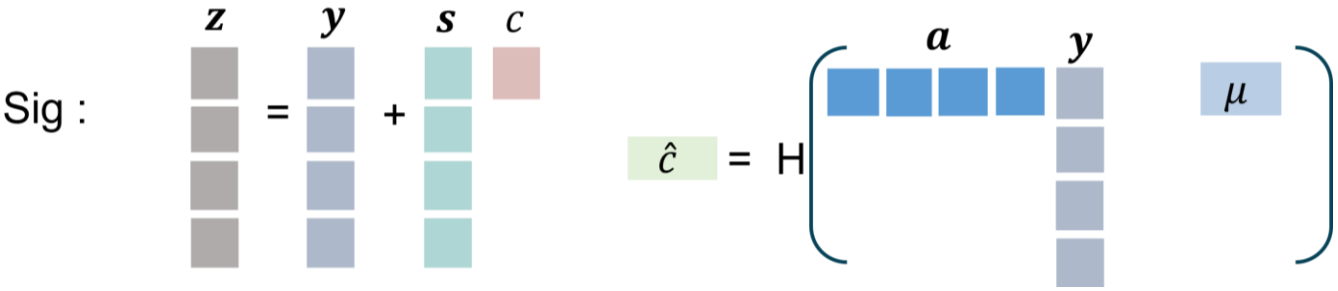
❖ **GCK function F_a and $R_q = Z_q[x]/< x^n + 1 >$, $q = prime$** for NTT

- **Public key :** $(a,\ t = F_a(s)) \in R_q^m \times R_q$ **Secret key :** $s \in R_{[-\eta,\eta]}^m$



← Key Recovery Attack
(KpqC Forum, Minkyu Kim)

- **Sign :** $(z, \hat{c}) = (y + c \cdot s,\ \hat{c} = H(F_a(y),\ \mu)) \in R_{[-B+L_s,B-L_s]}^m \times \{0,1\}^{\ell_1}$



- **Verification:** **(1) compute** $a \cdot z - c \cdot t = a \cdot y$
  (2) check if $\hat{c} = H(a \cdot y,\ \mu)$

LWE Attack

❖ Primal Attack (uSVP) – (Low-density SIS Problem)

$$a_1 s_1 + \cdots + a_m s_m \equiv t \bmod q$$

$$\Lambda = \{\boldsymbol{x} \in R^{m+1} : a_1 x_1 + \cdots + a_m x_m - t x_{m+1} \equiv 0 \bmod q\}$$

◆ Attack (Success Condition)

- BKZ with the Geometric Series Assumption (GSA) : $||\boldsymbol{b}_i^*|| = \delta^{d-2i-1} \cdot \mathrm{Vol}(\Lambda)^{1/d}$
- uSVP solution $\boldsymbol{v}$ will be detected if

$$||\pi_{d-b+1}(\boldsymbol{v})|| \leq ||b_{d-b+1}^*||$$

$$\Rightarrow \frac{\eta\sqrt{nmb}}{\sqrt{(m+1)n}} \leq \delta^{2b-d} q^{1/(m+1)}$$

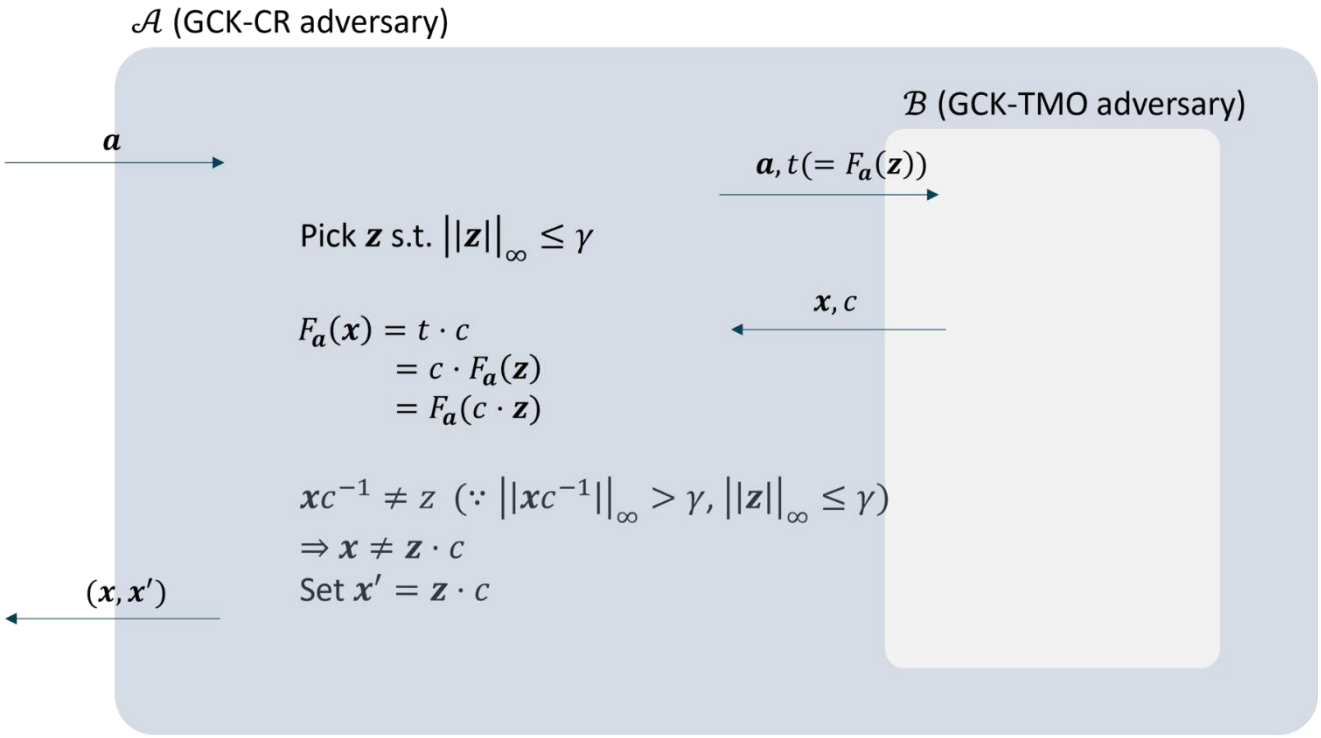
NIST-II	n	s	q	m	B	Pk (Bytes)	Sig (Bytes)	Pk+Sig (Bytes)	SIS Hardness	LWE Hardness
Dilithium	256	2	$\approx 2^{23}$	(4,4)	2^{17}	1,312	2,420	3,732	123	123
Ours	256	1	$\approx 2^{54}$	4	$2^{14} - 1$	1,760	1,952	288	125	< 64

[ADPS15] E. Alkim et al., "*Post-quantum Key Exchange – A New Hope*", USENIX 2016

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

Case 2) $\|\boldsymbol{x}c^{-1}\|_\infty \leq \gamma$ $\Rightarrow$ Solving GCK−OW$_{n,m,\gamma}$ ($\not\Rightarrow$ Solving GCK−OW$_{n,m,\beta}$)
where $n \cdot \alpha \cdot \gamma \leq \beta$

GCK-Based Signatures (2)

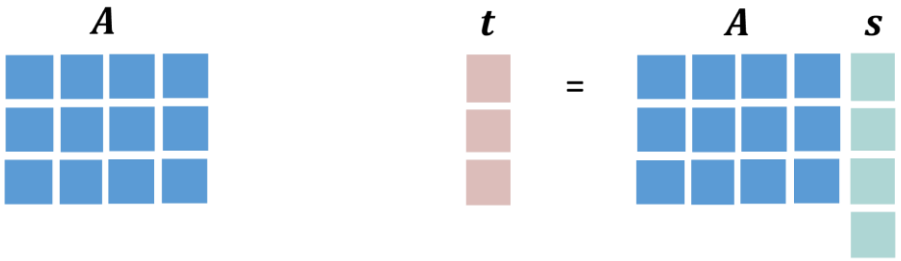
❖ GCK function F_a and $R_q = Z_q[x]/< x^n + 1 >$, $q = prime$

- **Public key :** $(A,\ t = F_A(s)) \in R_q^{k\times\ell} \times R_q^k$ **Secret key :** s
- **Sign :** $(z, c) = (y + c \cdot s,\ c = H(F_A(y),\ m)) \in R^{\ell}_{[-B+L_S, B-L_S]} \times \{0,1\}^w$

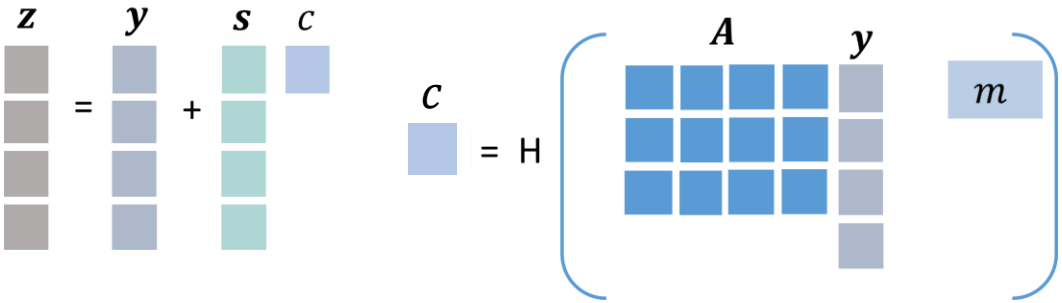
$s \leftarrow R^{\ell}_{[-\eta,\eta]}$

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

PK :

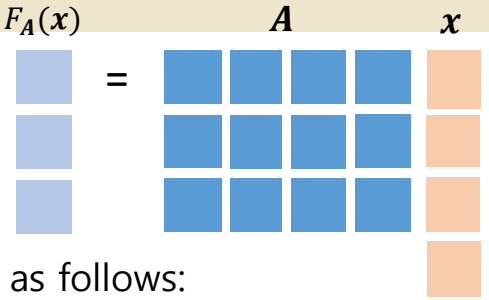


Sig :



- **Verification:** (1) compute $\mathrm{F}_A(\mathbf{z}) - c \cdot t = \mathrm{F}_A(\mathbf{y})$
  (2) check if $c = H(F_A(y),\ m)$

Module-GCK Function



❖ Module-GCK

◆ Definition

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

$$F_A(\boldsymbol{x}) = \boldsymbol{t} \text{ where } \boldsymbol{t} = \boldsymbol{A} \cdot \boldsymbol{x} \text{ and } \|\boldsymbol{x}\|_\infty \leq \beta$$

◆ 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. $\|\boldsymbol{x}\|_\infty \leq \beta$ and $F_A(\boldsymbol{x}) = \boldsymbol{t}$

◆ CR of Module-GCK problem

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

◆ 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. $\|c\|_\infty \leq \alpha$, $\|\boldsymbol{x}\|_\infty \leq \beta$, and $F_A(\boldsymbol{x}) = c \cdot \boldsymbol{t}$

LWE Attack

❖ Low-density (I)SIS Problem to LWE Problem

$$A_1 : \boxed{\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}} \begin{pmatrix} a_5 \\ a_6 \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ s_3 \end{pmatrix} \equiv \begin{pmatrix} t_1 \\ t_2 \end{pmatrix} \bmod q$$

$\mathrm{Adv}^{\mathrm{OW}}_{n,k\times\ell,q,\beta}$

If $\exists (A_1)^{-1}$ where $A_1 := \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}$

$$(A_1)^{-1} \cdot \begin{pmatrix} a_1 & a_2 & a_5 \\ a_3 & a_4 & a_6 \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ s_3 \end{pmatrix} \equiv (A_1)^{-1} \cdot \begin{pmatrix} t_1 \\ t_2 \end{pmatrix} \bmod q$$

$$\begin{pmatrix} 1 & 0 & a'_5 \\ 0 & 1 & a'_6 \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ s_3 \end{pmatrix} \equiv \begin{pmatrix} t'_1 \\ t'_2 \end{pmatrix} \bmod q$$

$$\begin{pmatrix} a'_5 \\ a'_6 \end{pmatrix} \cdot s_3 + \begin{pmatrix} s_1 \\ s_2 \end{pmatrix} \equiv \begin{pmatrix} t'_1 \\ t'_2 \end{pmatrix} \bmod q$$

$\mathrm{Adv}^{\mathrm{LWE}}_{n,k\times(\ell-k),q,\beta}$

◆ **Attack (Success Condition)**

- BKZ with the Geometric Series Assumption (GSA) : $||\boldsymbol{b}_i^*|| = \delta^{d-2i-1} \cdot \mathrm{Vol}(\Lambda)^{1/d}$
- uSVP solution $\boldsymbol{v}$ will be detected if

$$||\pi_{d-b+1}(\boldsymbol{v})|| \leq ||b^*_{d-b+1}||$$

- $\pi_{d-b+1}(\boldsymbol{v})$: projection of $\boldsymbol{v}$ onto the vector space spanned by the last b Gram-Schmidt vectors
- $\delta = \left((\pi b)^{1/b} b\right)/2\pi e\Big)^{1/(2(b-1))}$, $||\pi_{d-b+1}(\boldsymbol{v})|| \approx \frac{\sqrt{b}}{\sqrt{d}}||\boldsymbol{v}||$, $||b^*_{d-b+1}|| = \delta^{2b-d} q^{1/(m+1)}$

Minkyu Kim et al., “Analysis of GCKSign”, KpqC Forum, 2023.

Comparison

❖ Parameter selection (v0.2)

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

NIST-II	n	s	q	m	B	Pk (Bytes)	Sig (Bytes)	Pk+Sig (Bytes)	LWE Hardness	SIS Hardness
Dilithium	256	2	$\approx 2^{23}$	$(4,4)$	2^{17}	1,312	2,420	3,732	123	123
Ours	256	1	$\approx 2^{20}$	$(3,4)$	$2^{15}-1$	1,952	2,080	4,032	$136 \rightarrow 14$	142

NIST-III	n	s	q	m	B	Pk (Bytes)	Sig (Bytes)	Pk+Sig (Bytes)	LWE Hardness	SIS Hardness
Dilithium	256	4	$\approx 2^{23}$	$(6,5)$	2^{19}	1,952	3,293	5,245	182	186
Ours	256	1	$\approx 2^{19}$	$(4,5)$	$2^{15}+2^{12}$	2,464	2,752	5,216	$191 \rightarrow 14$	194

NIST-V	n	s	q	m	B	Pk (Bytes)	Sig (Bytes)	Pk+Sig (Bytes)	LWE Hardness	SIS Hardness
Dilithium	256	2	$\approx 2^{23}$	$(8,7)$	2^{19}	2,592	4,595	7,187	252	265
Ours	256	1	$\approx 2^{21}$	$(5,7)$	$2^{15}+2^{13}$	3,392	3,840	7,232	$262 \rightarrow 48$	272

Comparison

❖ Parameter selection (v0.3)

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

Dilithium	n	s	q	m	B	Pk (Bytes)	Sig (Bytes)	Pk+Sig (Bytes)	LWE Hardness	SIS Hardness
NIST-II	256	2	$\approx 2^{23}$	(4,4)	2^{17}	1,312	2,420	3,732	123	123
NIST-III	256	4	$\approx 2^{23}$	(6,5)	2^{19}	1,952	3,293	5,245	182	186
NIST-V	256	2	$\approx 2^{23}$	(8,7)	2^{19}	2,592	4,595	7,187	252	265

	n	(k, ℓ)	q	η	sig (bytes)	pk (bytes)	sk (bytes)	$pk + sig$ (bytes)	Classical security	Hardness problem
[Lyu09]	512	$(1, 5)$	$\approx 2^{60}$	2047	9,000	3,875	3,875	12,875	71	GCK-CR
	512	$(1, 8)$	$\approx 2^{96}$	2047	14,875	6,125	6,125	21,000	132	
	1,024	$(1, 8)$	$\approx 2^{96}$	2047	30,750	12,250	12,250	43,000	283	
Ours	256	$(2, 5)$	$\approx 2^{25}$	1	2,592	1,632	352	4,224	71	GCK-TMO
	256	$(3, 8)$	$\approx 2^{26}$	1	4,384	2,528	544	6,912	134	
	256	$(7, 17)$	$\approx 2^{27}$	1	10,368	6,080	1,120	16,448	291	

$$\mathrm{Adv}^{\mathrm{M-TMO}}_{n,k\times\ell,q,\alpha,\beta} \leq \mathrm{Adv}^{\mathrm{M-CR}}_{n,k\times\ell,q,\beta} + \mathrm{Adv}^{\mathrm{M-OW}}_{n,k\times\ell,q,\gamma(\leq\beta/n\alpha)} \text{ where } \alpha = 2,\ \ \beta = 2(B - L_s)$$

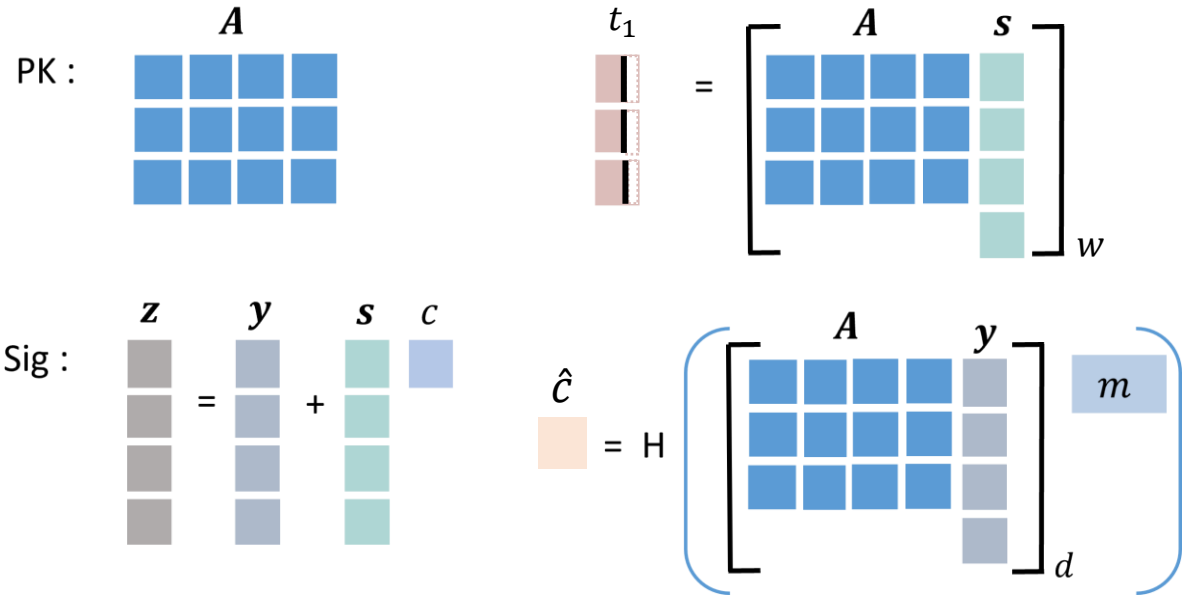
GCK-Based Signatures (3)

❖ GCK function F_a and $R_q = Z_q[x]/< x^n + 1 >$, $q = prime$

- **Public key :** $(A,\ t_1 = [As]_w) \in R_q^{k\times\ell} \times R_q^k$ **Secret key :** (s, t_0)
- **Sign :** $(z, \hat{c}, h) = (y + c \cdot s,\ \hat{c} = H([Ay]_d, \mu), h)$

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

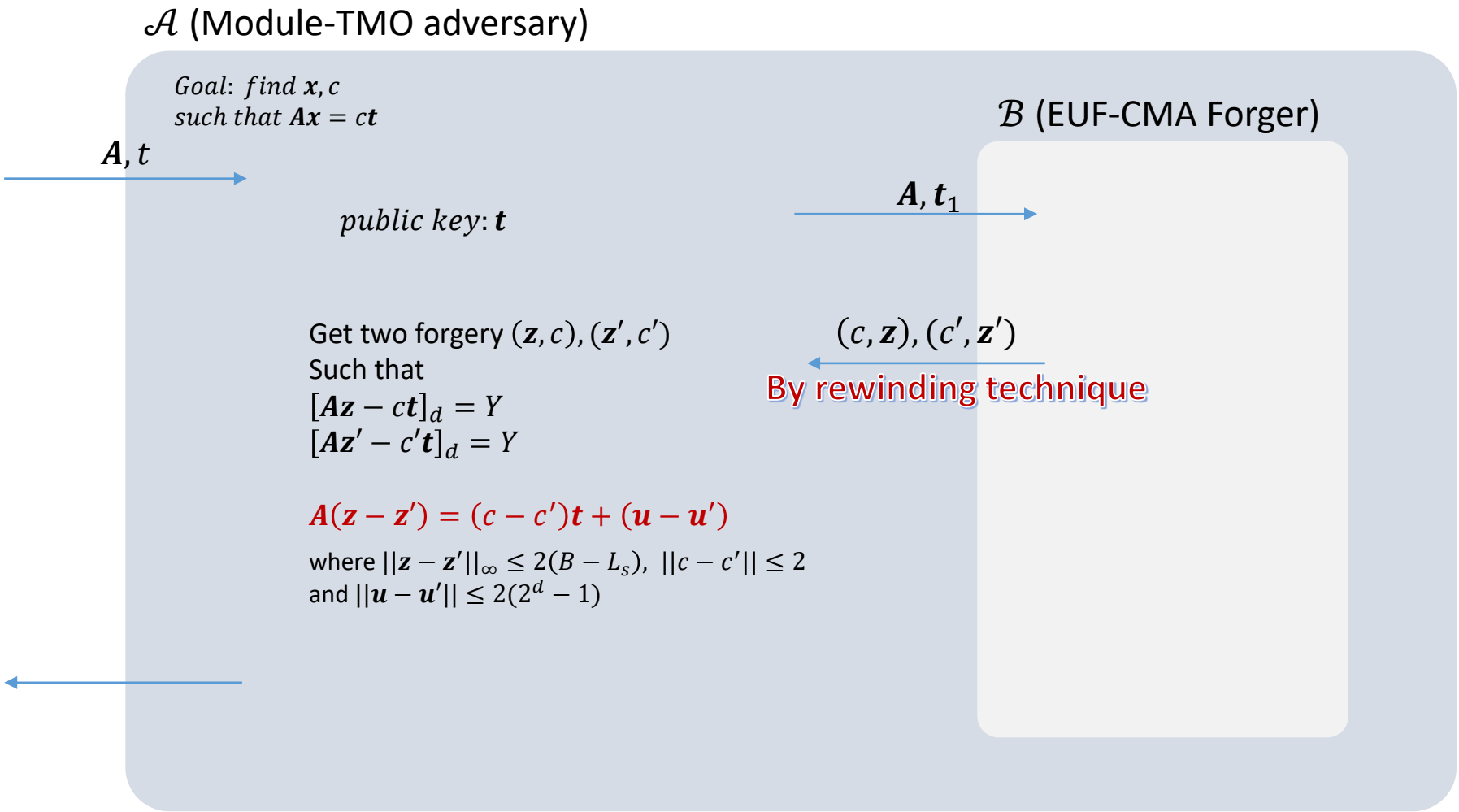
$y \leftarrow R^{\ell}_{[-B,B]}$



- **Verification:** check if $c = H([Az - ct_1]_d + h, \mu)$

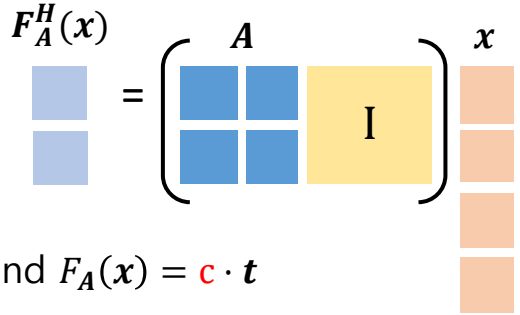
GCK-Based Signatures (3)

❖ Security Proof based on GCK-TMO



GCK-Based Signatures (3)

❖ Module-GCK



◆ 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. $\|c\|_\infty \leq \alpha$, $\|\boldsymbol{x}\|_\infty \leq \beta$, and $F_{\boldsymbol{A}}(\boldsymbol{x}) = \mathrm{c} \cdot \boldsymbol{t}$

◆ HNF.TMO of Module-GCK problem (Hermite normal form)

- Given $\boldsymbol{A} \in R^{k \times (\ell - k)}$ and $\boldsymbol{t} = F_{\boldsymbol{A}}^H(\boldsymbol{z}) \in R^k$,
  find $\boldsymbol{x}, c$ s.t. $\|c\|_\infty \leq \alpha$, $\|\boldsymbol{x}\|_\infty \leq \beta$, and $[\boldsymbol{A} || \boldsymbol{I}_k] \cdot [\boldsymbol{x}_1 || \boldsymbol{x}_2]^T = \mathrm{c} \cdot \boldsymbol{t}$

◆ TMO+ of Module-GCK problem

- Given $\boldsymbol{A} \in R^{k \times \ell}$ and $\boldsymbol{t} \in R^k$, **find $\boldsymbol{x}, c, \boldsymbol{u}$** s.t. $\|c\|_\infty \leq \alpha$, $\|\boldsymbol{x}\|_\infty \leq \beta$, $\|\boldsymbol{u}\|_\infty \leq \omega$ and $\boldsymbol{A}\boldsymbol{x} = c \cdot \boldsymbol{t} + \boldsymbol{u}$

◆ HNF.TMO+ of Module-GCK problem

- Given $\boldsymbol{A} \in R^{k \times (\ell - k)}$ and $\boldsymbol{t} = F_{\boldsymbol{A}}^H(\boldsymbol{z}) \in R^k$,
  find $\boldsymbol{x}, c, \boldsymbol{u}$ s.t. $\|c\|_\infty \leq \alpha$, $\|\boldsymbol{x}\|_\infty \leq \beta$, $\|\boldsymbol{u}\|_\infty \leq \omega$ and $[\boldsymbol{A} || \boldsymbol{I}_k] \cdot [\boldsymbol{x}_1 || \boldsymbol{x}_2]^T = \mathrm{c} \cdot \boldsymbol{t} + \boldsymbol{u}$

GCK-Based Signatures (3)

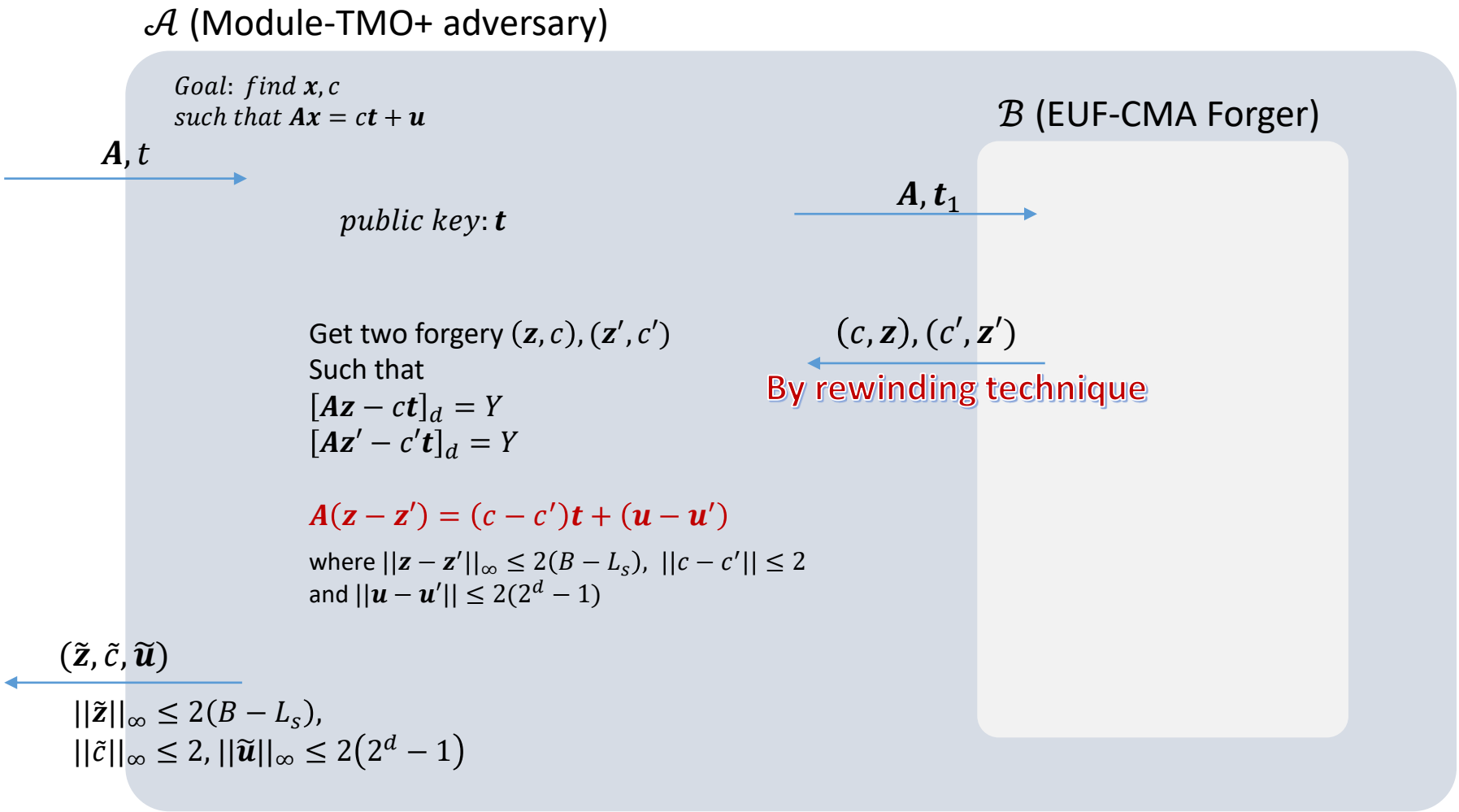
❖ Module-GCK

- $\mathbf{TMO}_{n,k\times\ell,q,\alpha,\beta} = \mathbf{HNF.TMO}_{n,k\times\ell,q,\alpha,\beta}$
  - Proof) $([\boldsymbol{A}_1||\boldsymbol{A}_2)\cdot\boldsymbol{z} = c\boldsymbol{t} \Leftrightarrow (\boldsymbol{I}||(\boldsymbol{A}_1)^{-1}\boldsymbol{A}_2)\cdot\boldsymbol{z} = c\boldsymbol{t}'$ where $\boldsymbol{t}' = (\boldsymbol{A}_1)^{-1}\boldsymbol{t}$
- $\mathbf{HNF.TMO+}_{n,k\times\ell,q,\alpha,\beta,\omega} \leq \mathbf{HNF.TMO}_{n,k\times\ell,q,\alpha,\beta+\omega}$
  - Proof) $(\boldsymbol{I}||\boldsymbol{A})\cdot(\boldsymbol{z}_1||\boldsymbol{z}_2)^T = c\boldsymbol{t}+\boldsymbol{u} \Longrightarrow (\boldsymbol{I}||\boldsymbol{A})\cdot(\boldsymbol{z}_1-\boldsymbol{u}||\boldsymbol{z}_2)^T = c\boldsymbol{t}$
- $\mathbf{TMO+}_{n,k\times\ell,q,\alpha,\beta,\omega} \leq \mathbf{HNF.TMO+}_{n,k\times(\ell+k),q,\alpha,\beta,\omega}$
  - Proof) $\boldsymbol{A}\cdot\boldsymbol{z} = c\boldsymbol{t}+\boldsymbol{u} \Longrightarrow (\boldsymbol{I}||\boldsymbol{A})\cdot(\boldsymbol{0}||\boldsymbol{z})^T = c\boldsymbol{t}+\boldsymbol{u}$
- $\mathbf{TMO+}_{n,k\times\ell,q,\alpha,\beta,\omega} \leq \mathbf{TMO}_{n,k\times(\ell+k),q,\alpha,\beta+\omega}$
- $\mathbf{TMO}_{n,k\times\ell,q,\alpha,\beta} \leq \mathbf{M\text{-}CR}_{n,k\times\ell,q,\beta} + \mathbf{M\text{-}OW}_{n,k\times\ell),q,\leq\beta/n\alpha}$

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

GCK-Based Signatures (3)

❖ Security Proof based on Module-TMO+



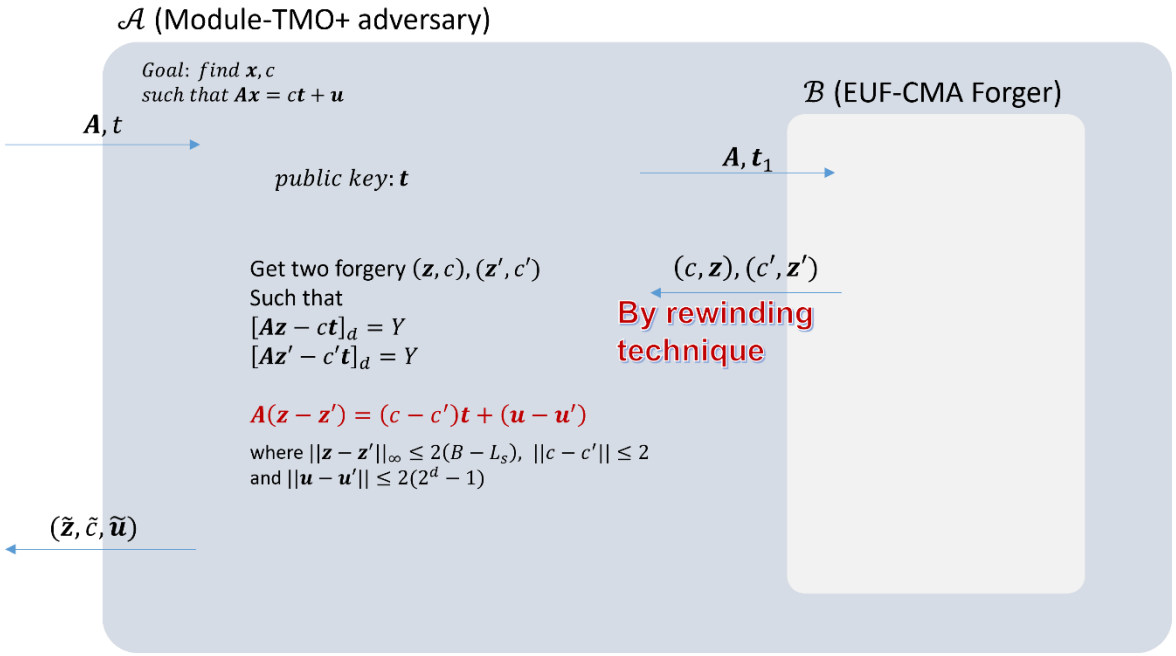
GCK-Based Signatures (3)

❖ Module-GCK

PK $= (\boldsymbol{A},\ \boldsymbol{t}_1 = [\boldsymbol{As}]_{\boldsymbol{w}} = (\boldsymbol{As} + \boldsymbol{e})/2^w)$
where $||\boldsymbol{s}||_\infty \le \eta, ||\boldsymbol{e}||_\infty \le 2^w - 1$

◆ TMO+ of Module-GCK problem

- Given $\boldsymbol{A} \in R^{k\times\ell}$ and $\boldsymbol{t} \in R^k$, **find $\boldsymbol{x}, c, \boldsymbol{u}$** s.t. $\|c\|_\infty \le \alpha$, $\|\boldsymbol{x}\|_\infty \le \beta$, $\|\boldsymbol{u}\|_\infty \le \omega$ and $\boldsymbol{Ax} = c\boldsymbol{t} + \boldsymbol{u}$



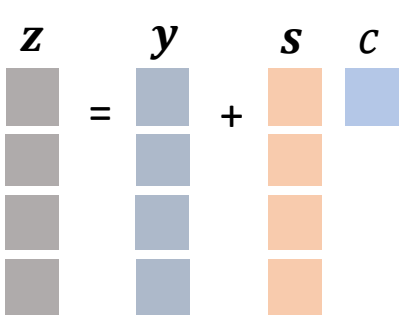
- $\text{TMO+}_{n,k\times\ell,q,\alpha,\beta,\omega} \le \text{TMO}_{n,k\times(\ell+k),q,\alpha,\beta+\omega}$ $\left(\alpha = 2, \beta = 2(B - L_s), \omega = 2\left(2^d - 1\right)\right)$
- $\text{TMO}_{n,k\times(\ell+k),q,\alpha,\beta+\omega} \le \text{M–OW}_{n,k\times(\ell+k),q,\alpha,\gamma} + \text{M–CR}_{n,k\times(\ell+k),q,\alpha,\beta+\omega}$
  $\le \text{M–LWE}_{n,k\times\ell,q,\alpha,\gamma} + \text{M–SIS}_{n,k\times(\ell+k),q,\alpha,2(\beta+\omega)}$

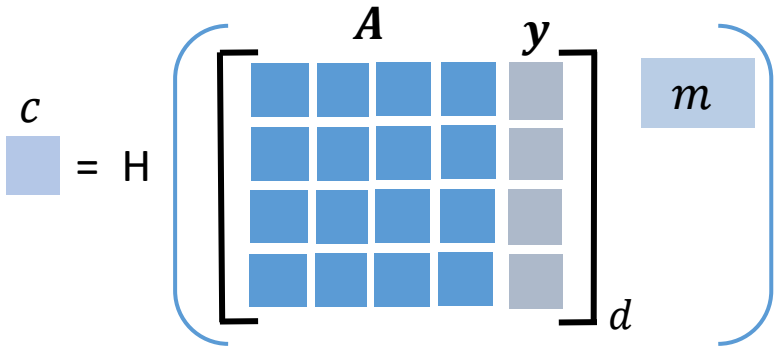
GCK-Based Signatures (3)

❖ 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 :** $(\boldsymbol{z}, c, h) = (\boldsymbol{y}+c\boldsymbol{s},\ \ c = H([\boldsymbol{Ay}]_{\boldsymbol{d}},\ m), h = Hint(-c\boldsymbol{t}_0,\ \boldsymbol{Ay} - \ c\boldsymbol{e}\ + c\boldsymbol{t}_0,\ d))$

Sig :





- **Check if** $||\boldsymbol{y}+c\boldsymbol{s}||_\infty < B - L_s$

  $||low(\boldsymbol{Ay} - \ c\boldsymbol{e})||_\infty < 2^d - L_e$

  $||low(c\boldsymbol{t}_0)||_\infty < 2^d$

Security check on s [Lyu09]

Security check on e [GLP12], [BG14]

Correctness check for hint [Dilithium]

Thank You

Q&A