KpqC 공모전 격자기반 알고리즘 증명 가능한 안전성 분석 기술 연구

2023.11.13.

Sangmyung University. Dept. of Computer Science

Jong Hwan Park

KpqC 공모전

❖ 국내 양자내성암호 국가공모전(KpqC)

◆ 1차 라운드 암호화 기법 7개, 서명 기법 9개 제출 (22.10)

기법	기반문제	알고리즘
KEM	Lattice	NTRU+
	Lattice	SMAUG
	Lattice	TiGER
	Code	REDOG
	Code	PALOMA
	Code	Layered ROLLO-I
	Graph PDF	IPCC
Signature	Lattice	GCKSign
	Lattice	HAETAE
	Lattice	NCC_Sign
	Lattice	Peregrine
	Lattice	SOLMAE
	Code	Enhanced pqsigRM
	Isogeny	FIBS
	Hash	AIMER
	Multivariate	MQ-Sign

[KpqC 공모전 주요 일정(안)]

시기	내용	비고
'22. 2. 18.	'개발 계획서' 접수 마감	
'22. 3. 18.	'개발 계획서' 평가 완료	결과는 개별 통보 예정
'22. 7.	2022 KpqC 1차 워크숍	알고리즘 설계 현황 발표
'22. 10.	'1라운드 제안서' 접수 마감	
- KpqC 공모전 1라운드 -		
'22. 11.	2022 KpqC 2차 워크숍	1라운드 제안 알고리즘 발표
'23. 7./11.	2023 KpqC 1/2차 워크숍	알고리즘 분석/개선 결과 공유
'23. 12.	공모전 1라운드 결과 발표	2라운드 후보 목록 공개
'24. 2.	'2라운드 제안서' 접수 마감	
- KpqC 공모전 2라운드 -		
'24. 3.	2024 KpqC 1차 워크숍	2라운드 제안 알고리즘 발표
'24. 9.	2024 KpqC 2차 워크숍	알고리즘 분석/개선 결과 공유
	KpqC 공모전 최종 결과 발표	알고리즘 ○종 선정 예정

KpqC 공모전 알고리즘 안전성 분석 연구

❖ 격자 기반 알고리즘의 설계 원리 및 안전성 증명 논리 분석 연구

◆ 1차 라운드 제출 격자 기반 알고리즘

- KEM 기법 : SMAUG, TiGER, NTRU+
- 서명 기법 : GCKSign, HAETAE, NCC-Sign, Peregrine, SOLMAE

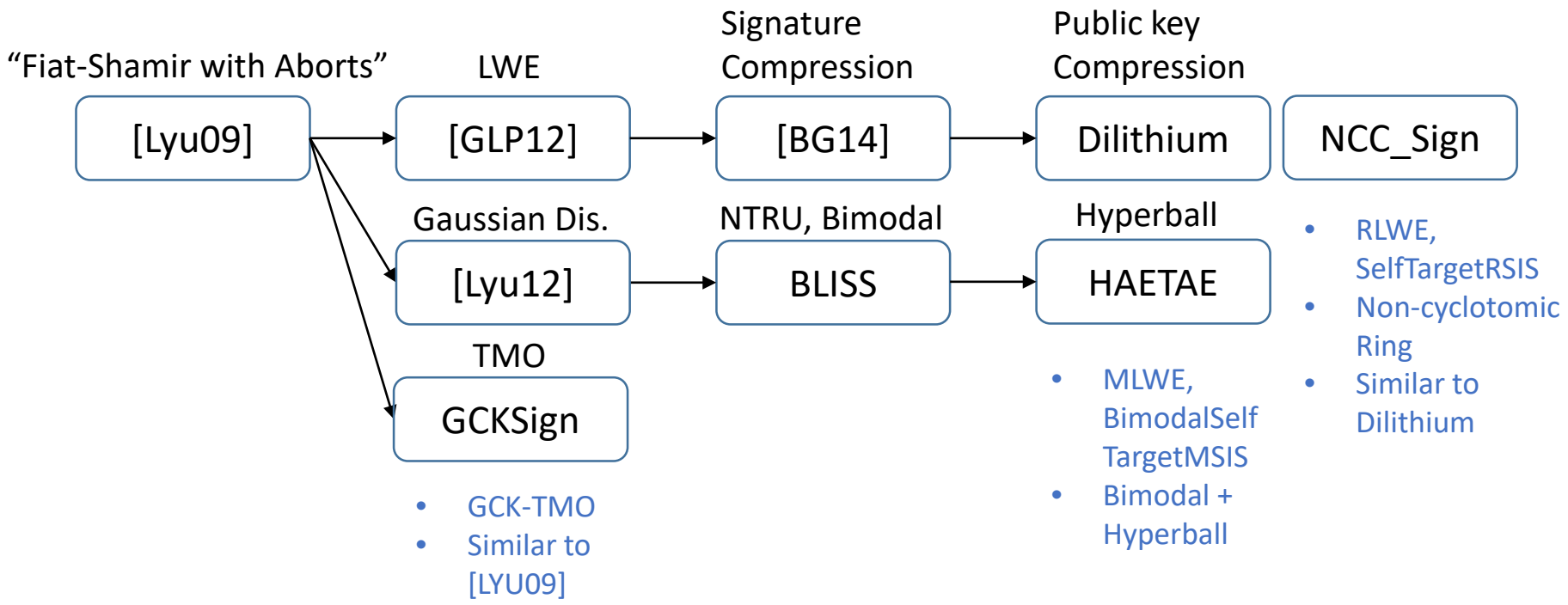
◆ 격자 기반 알고리즘의 증명 가능한 안전성 분석 기술 연구

- ElGamal 기반 KEM (SMAUG, TiGER) 및 NTRU 기반 KEM의 설계 원리 및 안전성 증명 논리 분석
  - 기반 난제, 안전성 증명 논리, 복호화 실패 확률 검증
- Fiat-Shamir 기반 서명 (GCKSign, HAETAE, NCC-Sign)의 설계 원리 및 안전성 증명 논리 분석
  - 기반 난제, 안전성 증명 논리 (영지식성), Rejection sampling 검증

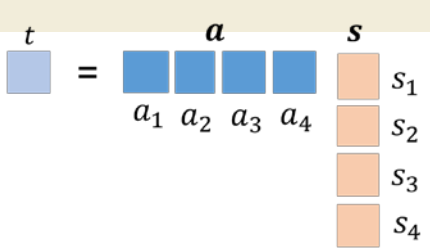
기법	알고리즘	기반 구조
KEM	NTRU+	NTRU
	SMAUG	MLWE
	TiGER	RLWE
Signature	GCKSign	Fiat-Shamir
	HAETAE	Fiat-Shamir
	NCC_Sign	Fiat-Shamir

Lattice-based Signatures

❖ Overview (w/ Fiat-Shamir Transform)



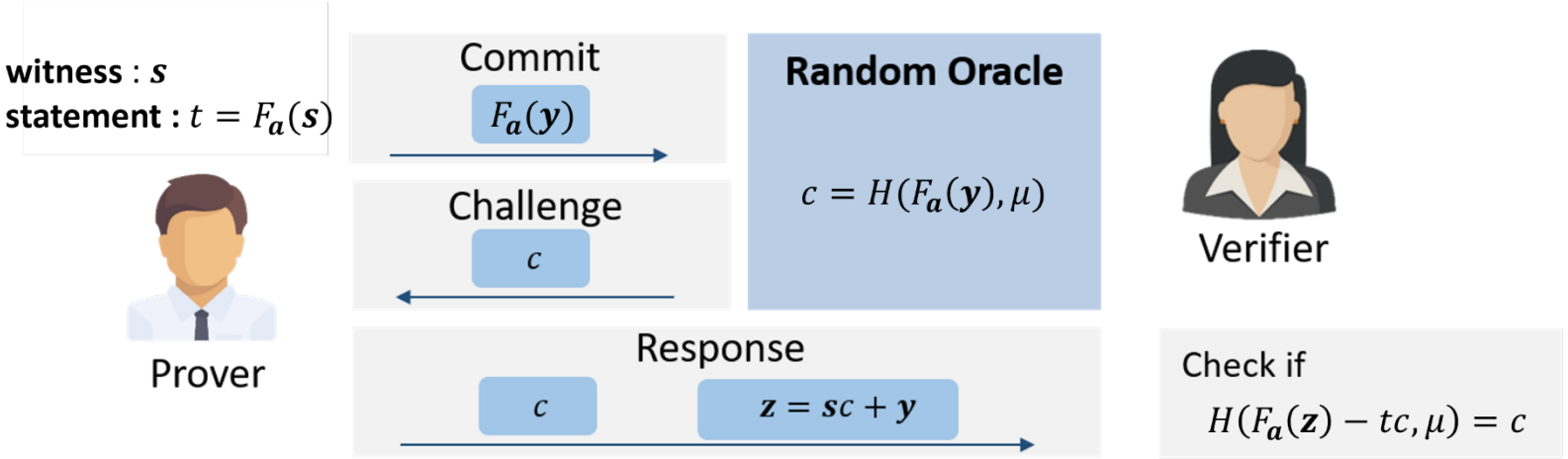
Lattice-based Signatures



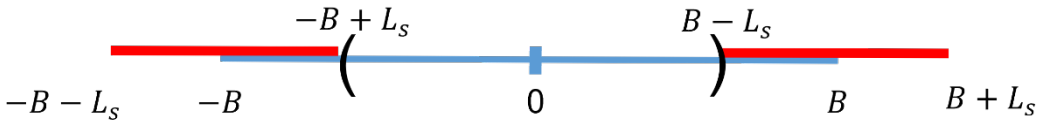
❖ Lattice-based Signature

◆ 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*

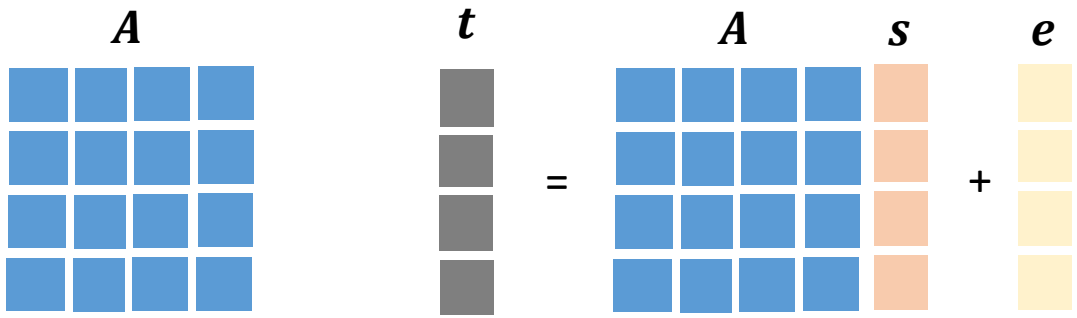
Lattice-based Signatures

❖ LWE-based Signature Scheme*

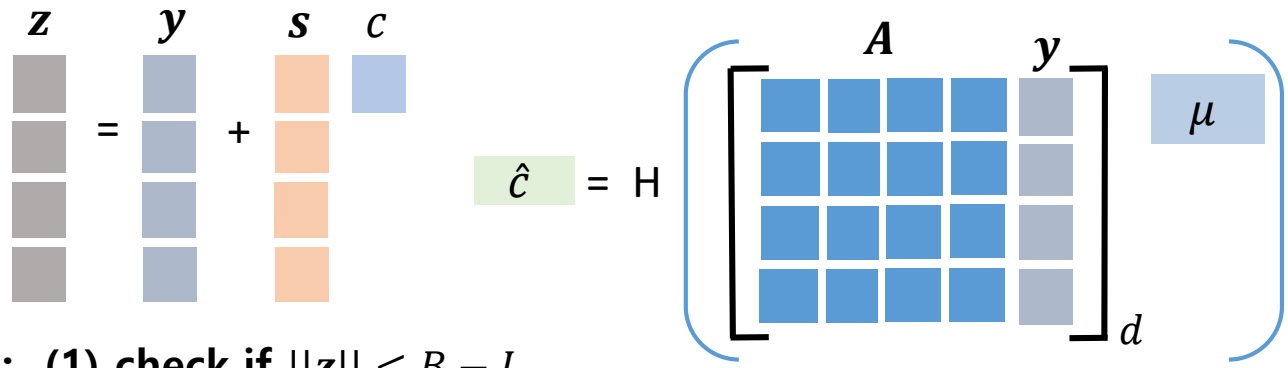
- **Public key :** $\left(A \in R_q^{k \times \ell}, t = As + e\right)$ **Secret key :** (s, e)
- **Sign :** $(z, \hat{c}) = (y + c \cdot s,\ \hat{c} = H([Ay]_d,\ \mu)) \in R^m_{[-B+L_s, B-L_s]} \times \{0,1\}^t$

  Check if $||y + c \cdot s|| < B - L_s$ and $[A \cdot y - c \cdot e]_d = [A \cdot y]_d$

PK :



Sig :



- **Verification:** **(1) check if** $||z|| < B - L_s$

  (2) check if $\hat{c} = H([Az - ct]_d, \mu)$

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

Lattice-based Signatures

❖ Security Proof (Sketch)

◆ UF-CMA Security Proof

- G_0 : The original UF-CMA game
- G_1 : Changing the signing oracle with sk
- G_2 : Changing the signing oracle without sk
- G_3 : Public key → random

Min-entropy (commitment)

Zero-knowledge

Decisional LWE

$$|Adv_0 - Adv_1| < Q_s \cdot 2^{-\alpha+1}$$

$$|Adv_1 - Adv_2| < Q_s \cdot \epsilon_{zk}$$

$$|Adv_2 - Adv_3| < Adv^{LWE}_{m,n,q,\chi}$$

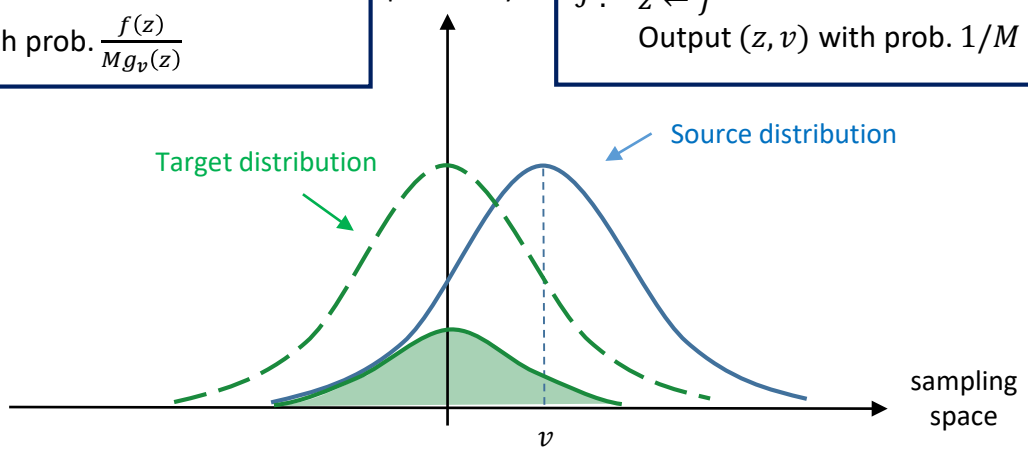
$$Adv_3 < Adv^{\{SelftargetMSIS\}}$$

◆ Zero-knowledge $(\boldsymbol{z = y + c \cdot s})$

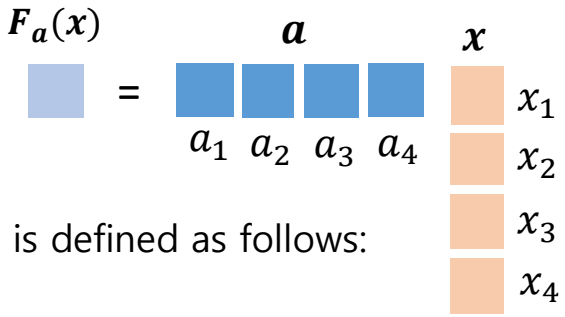
- Rejection Sampling
  - Source distribution = g & Target distribution = f
  - If $\exists M$ such that $\Pr[Mg(z) \geq f(z); z \leftarrow f] \geq 1 - \epsilon$, $\mathrm{dis}(\mathcal{A}, \mathcal{F}) = \epsilon / M$ (where dis = statistical distance)

$\mathcal{A}$: $z \leftarrow g_v$
Output (z, v) with prob. $\frac{f(z)}{Mg_v(z)}$

$\mathcal{F}$: $z \leftarrow f$
Output (z, v) with prob. $1/M$



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



❖ 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 $F_{\boldsymbol{a}}(\boldsymbol{x}) = F_{\boldsymbol{a}}(\boldsymbol{y})$

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

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

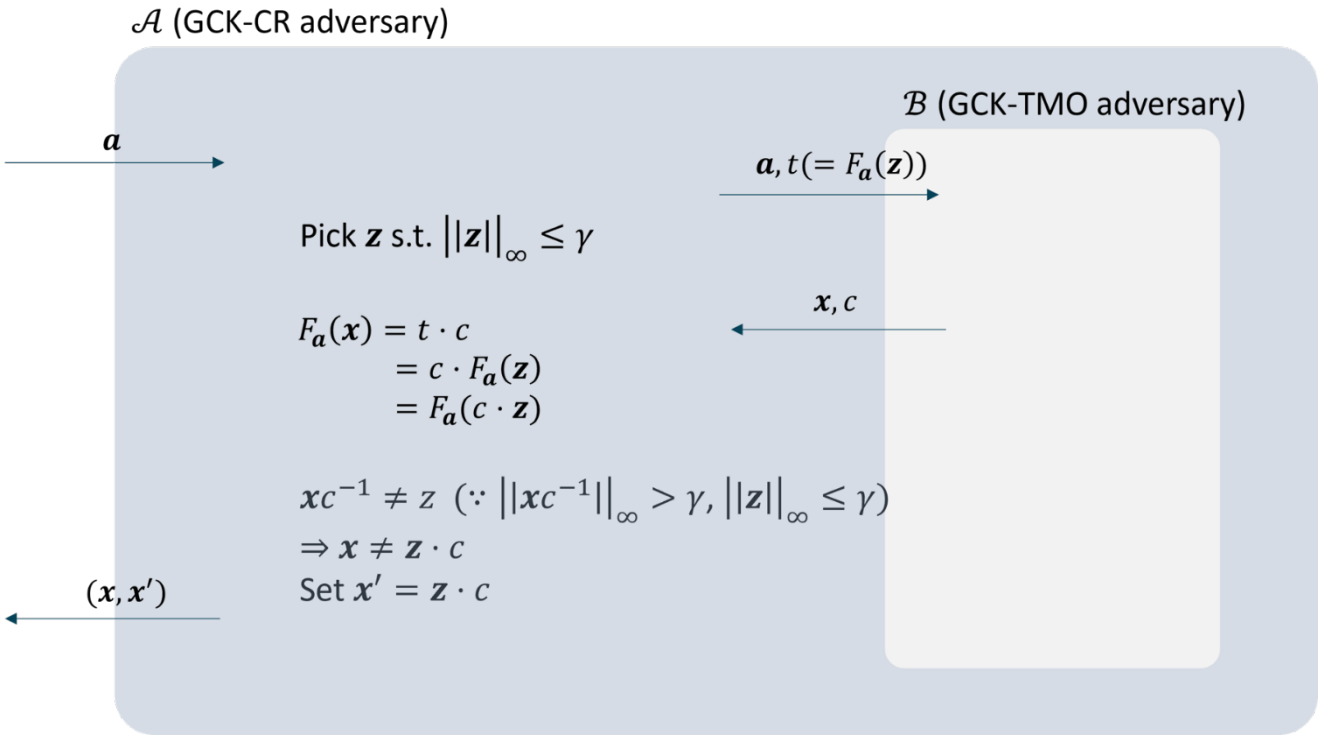
[LM06] V. Lyubashevsky et al., "*Generalized Compact Knapsacks Are Collision Resistant*", *ICALP 2006*

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

New GCK Problem

❖ Reduction between GCK problems

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



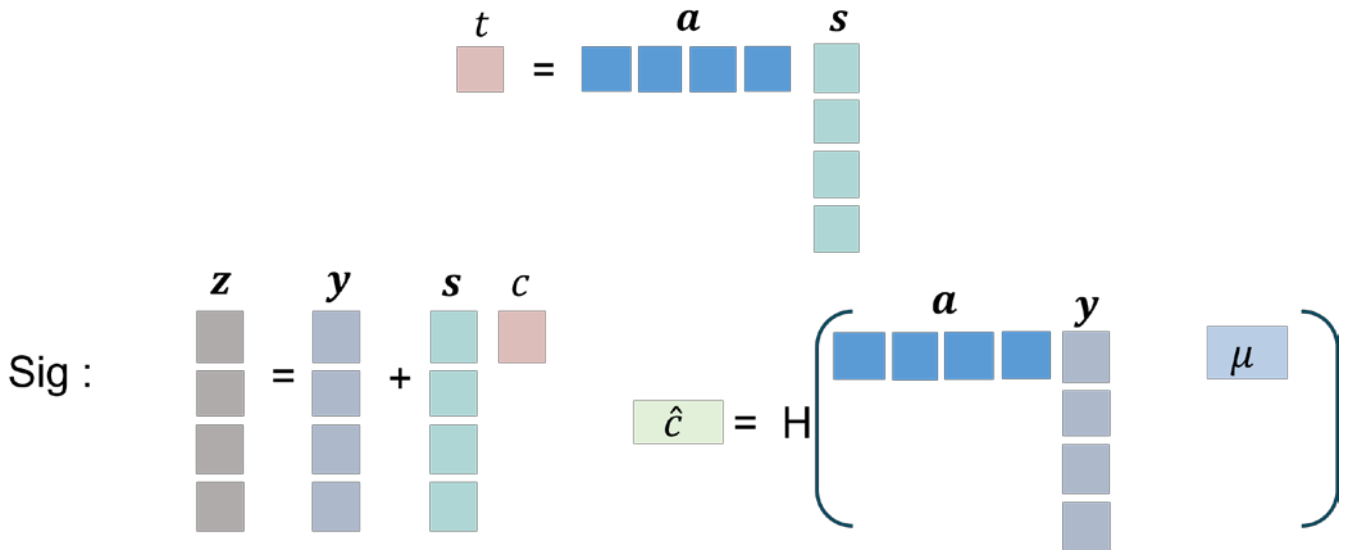
Case 1) $\|\boldsymbol{x}c^{-1}\|_\infty > \gamma$ ⇒ Solving GCK−CR$_{n,m,\beta}$ **(WRONG** part!!)

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

where $n \cdot \alpha \cdot \gamma \leq \beta$ (⇒ Solving GCK−CR$_{n,m,\beta}$)

❖ Signature Scheme

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

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

GCKSign

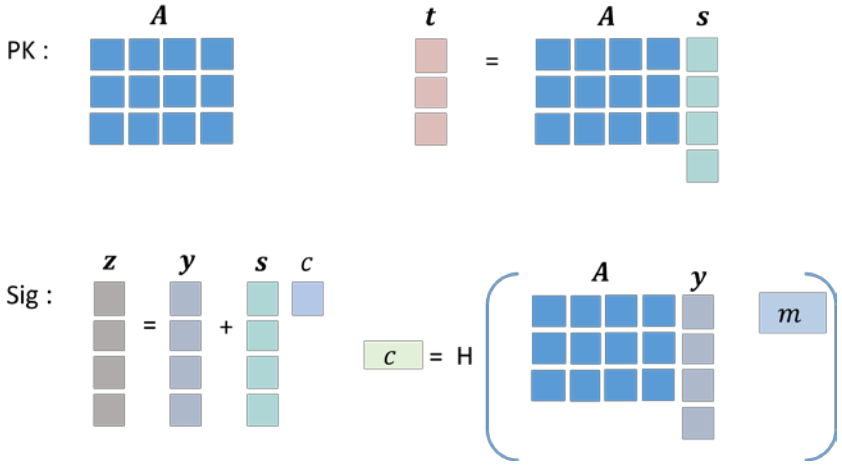
Key Recovery Attack*
"Low-density SIS problem"

❖ Signature Scheme

- **Public key :** $(a,\ t = F_a(s)) \in R_q^m \times R_q$ **Secret key :** $s \in R_{[-\eta,\eta]}^m$
- **Sign :** $(z, \hat{c}) = (y + c \cdot s,\ \hat{c} = H(F_a(y),\ \mu)) \in R_{[-B+L_s,B-L_s]}^m \times \{0,1\}^{\ell_1}$
- **Verification:** (1) compute $a \cdot z - c \cdot t = a \cdot y$
  (2) check if $\hat{c} = H(a \cdot y,\ \mu)$

❖ Revised Signature Scheme (modulization)

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



*Minkyu Kim et al., "Analysis of GCKSign", KpqC Forum, 2023.

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

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

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

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

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

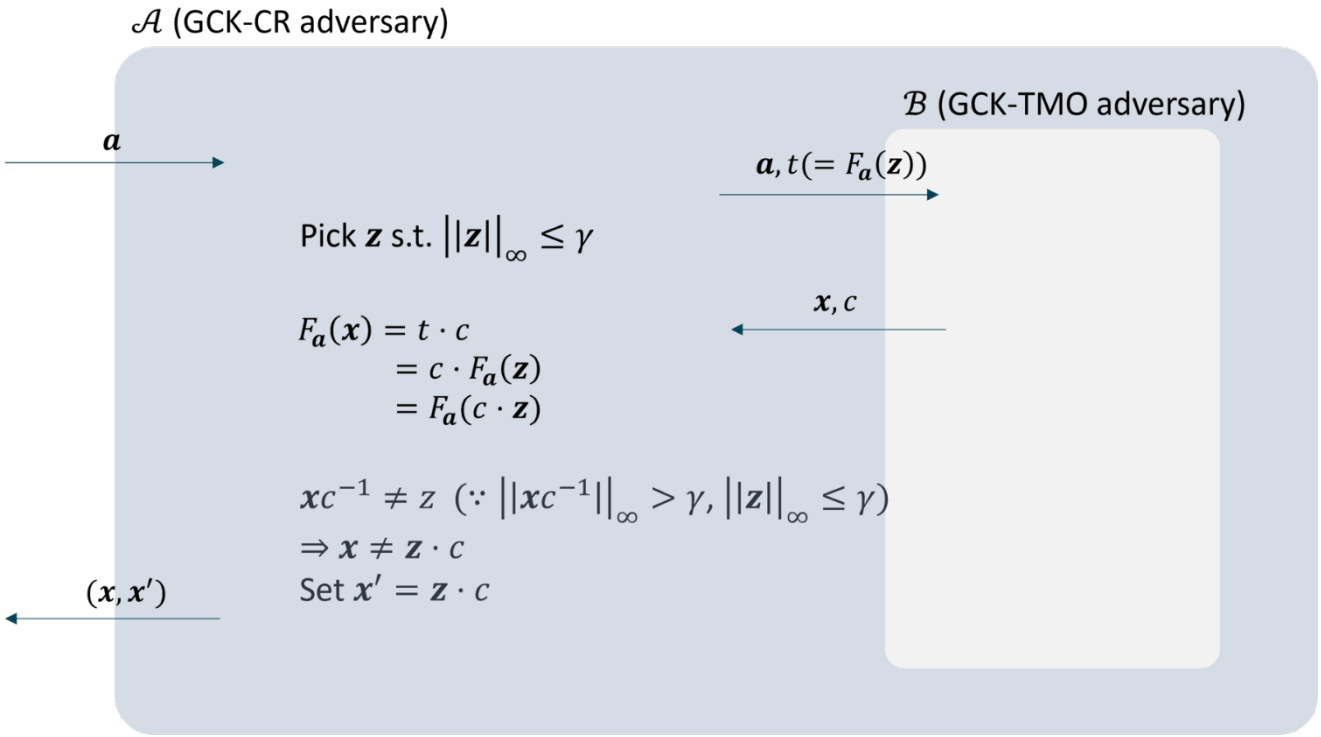
- $\pi_{d-b+1}(\boldsymbol{v})$: projection of $\boldsymbol{v}$ onto the vector space spanned by the last b Gram-Schmidt vectors
- $\delta = \left(((\pi b)^{1/b} b)/2\pi e\right)^{1/(2(b-1))}$, $||\pi_{d-b+1}(\boldsymbol{v})|| \approx \frac{\sqrt{b}}{\sqrt{d}}||\boldsymbol{v}||$, $||b^*_{d-b+1}|| = \delta^{2b-d}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

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

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$_{n,m,\beta}$)

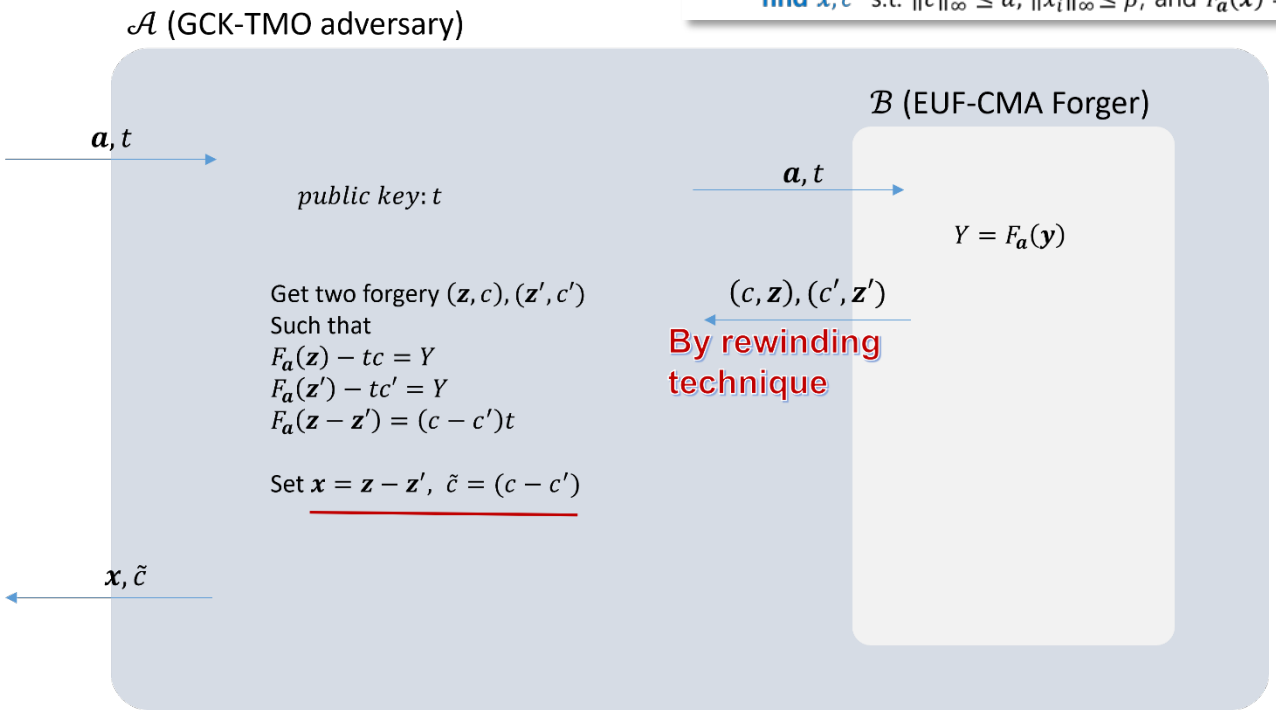
($\because$Low-density SIS $\not\leq$ High-density SIS)

❖ Security Proof

◆ Security based on GCK-TMO Problem

◆ **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 $F_{\boldsymbol{a}}(\boldsymbol{x}) = c \cdot t$



$$\mathrm{Adv}^{\mathrm{UF-CMA}}_{GCKSign} \leq \mathrm{Adv}^{\mathrm{TMO}}_{n,m,q,\alpha,\beta} \text{ where } \alpha = 2, \quad \beta = 2(B - L_s)$$

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

GCKSign

❖ Revised Signature Scheme (modulization)

- **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 :** $(\boldsymbol{z}, c) = (\boldsymbol{y} + c \cdot \boldsymbol{s},\ c = H(F_{\boldsymbol{A}}(\boldsymbol{y}),\ m)) \in R^{\ell}_{[-B+L_s, B-L_s]} \times \{0,1\}^w$
- **Verification:** **(1) compute** $\mathrm{F}_{\boldsymbol{A}}(\mathbf{z}) - c \cdot \boldsymbol{t} = \mathrm{F}_{\mathbf{A}}(\mathbf{y})$
  (2) check if $c = H(F_{\boldsymbol{A}}(\boldsymbol{y}),\ m)$

❖ Parameter selection

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

	n	(k, ℓ)	q	η	sig (bytes)	pk (bytes)	sk (bytes)	$pk + sig$ (bytes)	Classical security	Hardness problem
GCKSign	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	

❖ Hardness problems

◆ Decision-MLWE

- Given $\boldsymbol{A} \leftarrow R_q^{k \times l}$ and $\boldsymbol{b} \in R_q^k$
  $\boldsymbol{b}$ is **indistinguishable** from $\boldsymbol{As_1 + s_2}$

◆ Search-MSIS

- Given $\boldsymbol{A} \leftarrow R_q^{k \times l}$ **find** $\boldsymbol{x}$ s.t $0 < \|\boldsymbol{x}\|_2 \leq 2\beta$ and $(\boldsymbol{A}|\boldsymbol{ID_k}) \cdot \boldsymbol{x} = 0 \; mod \; q$

◆ BimodalSelfTargetMSIS

- Given $(\boldsymbol{A_0}, \boldsymbol{b}) \leftarrow R_q^{k \times (l-1)} \times R_q^k$ where $\boldsymbol{A} = (-2\boldsymbol{b} + q\boldsymbol{j} | 2\boldsymbol{A_0} | 2\boldsymbol{ID_k}) \; mod 2q$
  find $\boldsymbol{x}, c, M$ s.t $0 < \|\boldsymbol{x}\|_2 \leq \beta$ and $H(\boldsymbol{Ax} - qc\boldsymbol{j} \; mod 2q, M) = c$

◆ SelfTargetRSIS

- Given $(\boldsymbol{a_1}, \boldsymbol{a_2}) \leftarrow R_q \times R_q$
  find $\vec{x} \coloneqq \begin{bmatrix} \boldsymbol{r_1} \\ \boldsymbol{r_2} \\ \boldsymbol{c} \end{bmatrix}, M$ s.t $0 < \|\vec{\boldsymbol{x}}\|_\infty \leq \gamma$ and $H(M || [1 \quad a_1 \quad a_2] \cdot \vec{x}) = c$

NCC-Sign

Non-cyclotomic Ring

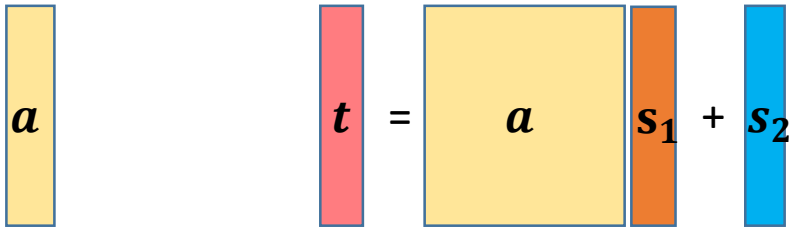
❖ **RLWE and** $R_q := \mathbb{Z}_q[X]/(X^p - X - 1)$

- **Public key :** $(a,\ t = a \cdot s_1 + s_2) \in R_q^2$ **Secret key :** (s_1, s_2)
- **Sign :** $(\hat{c}, z) = (H([ay]_d \bmod q, \mu),\ y + c \cdot s_1) \in \{0,1\}^t \times R_{[-B+L_s, B-L_s]}$

$s_1, s_2 \leftarrow U_{[-\eta,\eta]}$

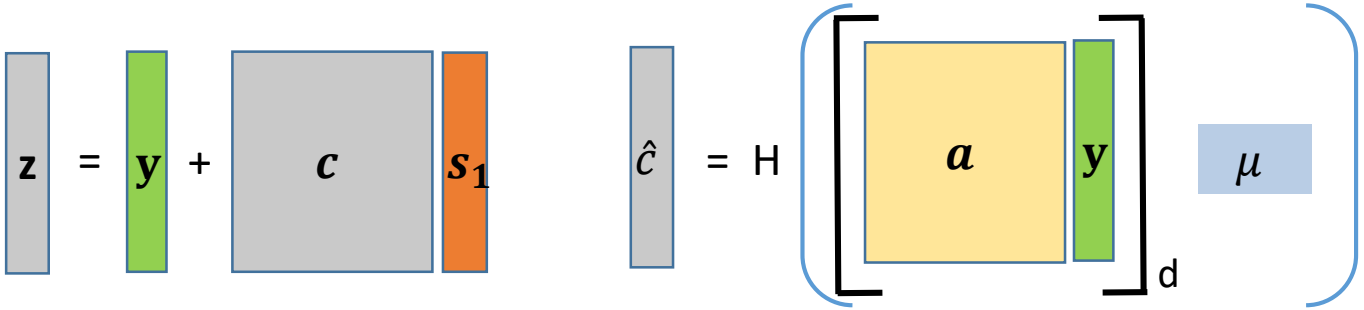
$y \leftarrow U_{[-B,B]}$

PK :



$c \in R_q \leftarrow \hat{c} \in \{0,1\}^t$

Sig :



- **Verification:** **(1) check if** $\|z\|_\infty < B - L_{s_1}$

  (2) compute $a \cdot z - c \cdot t = a \cdot y - c \cdot s_2$ → $[a \cdot y - c \cdot s_2]_d = [a \cdot y]_d$

  check if $\hat{c} = H(a \cdot z - c \cdot t \bmod q,\ \mu)$

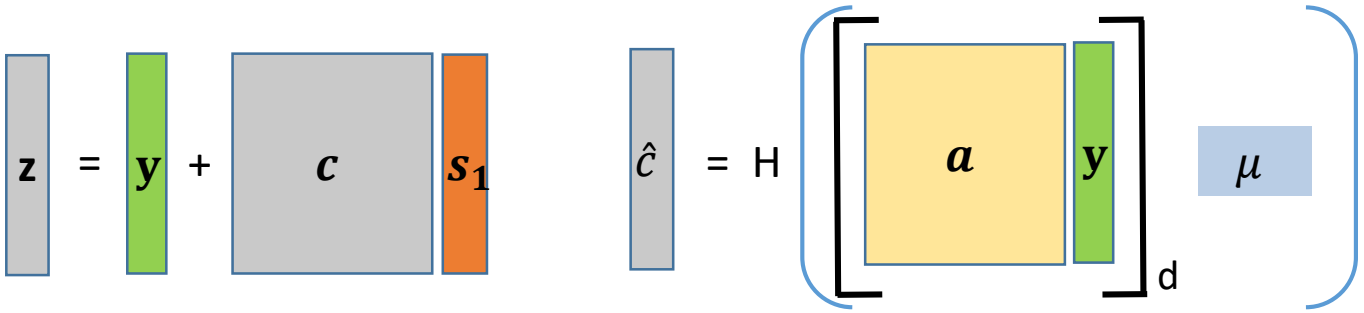
NCC-Sign

❖ **RLWE and** $R_q := \mathbb{Z}_q[X]/(X^p - X - 1)$

- **Public key :** $(a,\ t = a \cdot s_1 + s_2) \in R_q^2$ **Secret key :** (s_1, s_2)
- **Sign :** $(\hat{c}, z) = (H([ay]_d \bmod q, \mu),\ \ y + c \cdot s_1) \in \{0,1\}^t \times R_{[-B+L_s, B-L_s]}$

$s_1, s_2 \leftarrow U_{[-\eta,\eta]}$

Sig :



- Rejection sampling
- Check if $||y + c \cdot s_1|| < B - L_{s_1}$ Security check on s_1

  $||low(a \cdot y - c \cdot s_2)|| < 2^d - L_{s_2}$ Security check on s_2

  $[a \cdot y - c \cdot s_2]_d = [a \cdot y]_d$ Correctness check

- **Verification: (1) check if** $\|z\|_\infty < B - L_{s_1}$

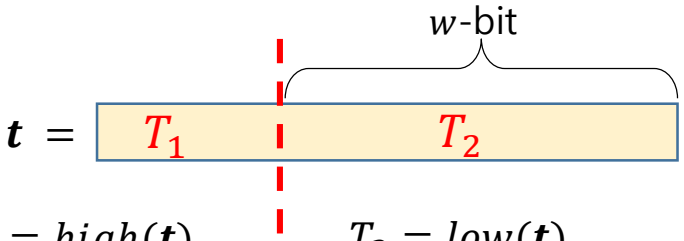
  (2) check if $\hat{c} = H(a \cdot z - c \cdot t \bmod q,\ \mu)$

❖ RLWE and $R_q := \mathbb{Z}_q[X]/(X^p - X - 1)$

- **Public key :** $(a,\ t = a \cdot s_1 + s_2) \in R_q^2$ **Secret key :** (s_1, s_2)

$s_1, s_2 \leftarrow U_{[-\eta,\eta]}$

$$t = a \cdot s_1 + s_2 = T_1 \cdot 2^w + T_2$$

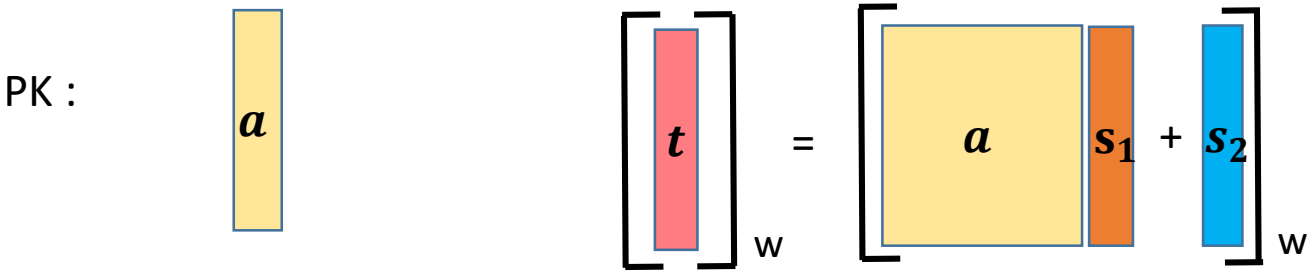


$T_1 = [t]_w = high(t)$ $T_2 = low(t)$

PK compression

- **In NCC-Sign,** $q \approx 23$ bits and $w = 12$

PK :



NCC-Sign

❖ **RLWE and** $R_q := \mathbb{Z}_q[X]/(X^p - X - 1)$

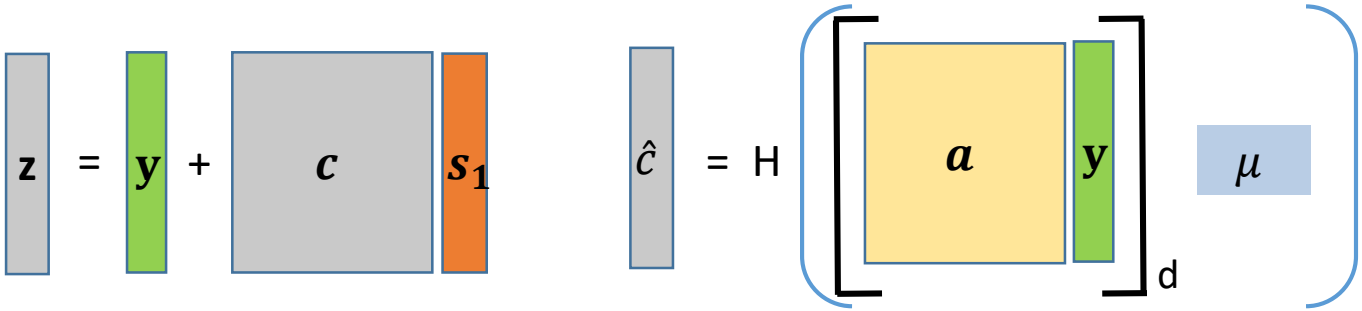
◆ **Public key :** $(a,\ t = a \cdot s_1 + s_2) \in R_q^2$ **Secret key :** (s_1, s_2)

◆ **Sign :** $(\hat{c}, z) = (H([ay]_d \bmod q, \mu),\ \ y + c \cdot s_1) \in \{0,1\}^t \times R_{[-B+L_s, B-L_s]}$

$s_1, s_2 \leftarrow U_{[-\eta,\eta]}$

$y \leftarrow U_{[-B,B]}$

Sig :



- Rejection sampling
- Check if $||y + c \cdot s_1|| < B - L_{s_1}$ Security check on s_1

  $||low(a \cdot y - c \cdot s_2)|| < 2^d - L_{s_2}$ Security check on s_2

  $[a \cdot y - c \cdot s_2]_d = [a \cdot y]_d$ Correctness check

- Create $h = Hint(-c \cdot T_2,\ a \cdot y - c \cdot s_2 + c \cdot T_2,\ d)$ Create a carry bit hint vector h caused by ignoring $c \cdot T_2$

NCC-Sign

❖ **RLWE and** $R_q := \mathbb{Z}_q[X]/(X^p - X - 1)$

$s_1, s_2 \leftarrow U_{[-\eta,\eta]}$

$y \leftarrow U_{[-B,B]}$

- **Public key :** $(a,\ t = a \cdot s_1 + s_2) \in R_q^2$ **Secret key :** (s_1, s_2)
- **Sign :** $(\hat{c}, z) = (H([ay]_d \bmod q, \mu),\ \ y + c \cdot s_1) \in \{0,1\}^t \times R_{[-B+L_s, B-L_s]}$
  - Rejection sampling
  - Check if $||y + c \cdot s_1|| < B - L_{s_1}$ Security check on s_1

    $||low(a \cdot y - c \cdot s_2)|| < 2^d - L_{s_2}$ Security check on s_2

    $[a \cdot y - c \cdot s_2]_d = [a \cdot y]_d$ Correctness check
  - Create $h = Hint(-c \cdot T_2,\ a \cdot y - c \cdot s_2 + c \cdot T_2,\ d)$ Create a carry bit hint vector h caused by ignoring $c \cdot T_2$

- **Verification: (1) compute** $a \cdot z - c \cdot T_1 \cdot 2^w = a \cdot y - c \cdot s_2 + c \cdot T_2$

  (2) Using hint h, **compute** $[a \cdot z - c \cdot T_1 \cdot 2^w]_d = [a \cdot y]_d$

  (3) check if $\hat{c} = H([a \cdot y]_d,\ m)$ & $\|z\|_\infty < B - L_{s_1}$

❖ Compare to Dilithium

◆ Non-cyclotomic Ring

- Ring: $\boldsymbol{R_q} \coloneqq \mathbb{Z}_q[X]/(X^p - X - 1)$
- NTT ⟶ Toom-cook & Karatsuba polynomial multiplication
- Similar modulus q for same Exp.Reps as Dilithium
- Inert modulus q for $\mathbb{Z}_q[X]/(X^p - X - 1)$: field

  $\Leftrightarrow X^p - X - 1$: irr in $\mathbb{Z}[x]$, $\mathbb{Z}_q[x]$

◆ New SampleInBall algorithm

- Sampling challenge $c \in \{-1,0,1\}^p$ as choosing $c_1, c_2 \ s.t \ c = c_2 + c_1 \cdot X^{p_2}$
- $\|cs\|_\infty < \beta \ \rightarrow \ \|c_2 s\|_\infty < \beta_1 \ \wedge \ \|(c_1 \cdot X^{p_2})s\|_\infty < \beta_2$

  $\Longrightarrow$ Exp.Reps ↓

- **SelfTargetRSIS**
  - Given $(a_1, a_2) \leftarrow R_q \times R_q$

    find $\vec{x} := \begin{bmatrix} r_1 \\ r_2 \\ c \end{bmatrix}, M$ s.t $0 < \|\vec{x}\|_\infty \leq \gamma$ and $H(M \| [1 \quad a_1 \quad a_2] \cdot \vec{x}) = c$

❖ Security Proof

◆ Reduction from RSIS to SelfTargetRSIS

$\mathcal{A}$ (RSIS adversary)

$\mathcal{B}$ (SelfTargetRSIS adversary)

(a_1, a_2)

(a_1, a_2)

$A = (1 | a_1 | a_2)$

$get \ ([r_1, r_2, c], M), ([r_1', r_2', c'], M')$
$s.t \ A[r_1, r_2, c] = A[r_1', r_2', c'] \ mod q$

$\Rightarrow [r_1 - r_1', r_2 - r_2', c - c'] \neq 0 \ (\because c \neq c')$

$([r_1, r_2, c], M), ([r_1', r_2', c'], M')$

By rewinding technique

$[r_1 - r_1', r_2 - r_2', c - c']$

❖ Security Proof

◆ Reduction from UF-NMA to UF-CMA

- **[KLS18]**

1. deterministic
2. Zero-knowledgeness

→ **UF-NMA reduces to UF-CMA**

◆ **UF-CMA Security Proof**

- G_0 : The original UF-CMA game
- G_1 : Changing the signing oracle with sk
- G_2 : Changing the signing oracle without sk
- G_3 : Public key → random

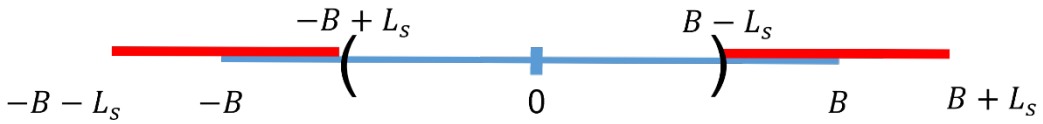
Min-entropy (commitment)

Zero-knowledge

Decisional LWE

Condition 1. deterministic

Condition 2. Zero-knowledgeness

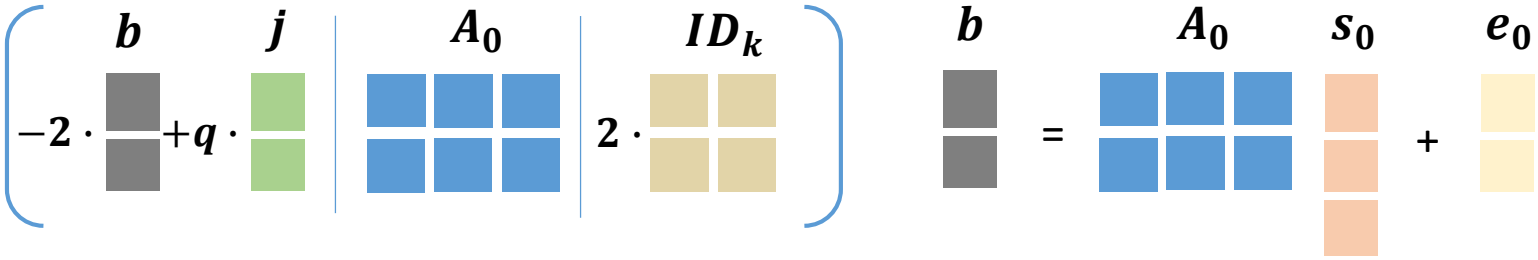


[KLS18] E. Kiltz. et al., *"A concrete treatment of fiat-shamir sigantures in the quantum random-oracle model"*, EUROCRYPT 2018

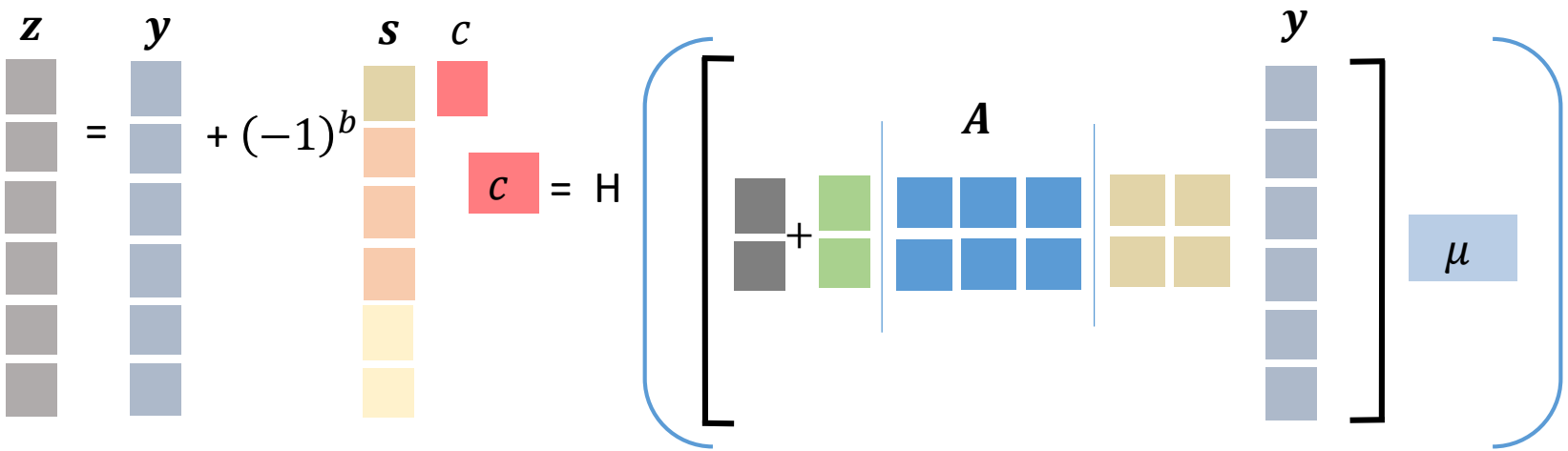
❖ Signature Scheme based on Bimodal Hyperball distribution

- **Public key :** $(\boldsymbol{A}, \boldsymbol{b}) = ((-2\boldsymbol{b} + q\boldsymbol{j} | 2\boldsymbol{A_0} | 2\boldsymbol{ID_k}) \bmod 2q,\ \boldsymbol{b} = \boldsymbol{A_0} \cdot \boldsymbol{s_0} + \boldsymbol{e_0})$
- **Secret key :** $(\boldsymbol{S}) = (1, \boldsymbol{s_0}, \boldsymbol{e_0})$
- **Sign :** $(\mathrm{c}, \boldsymbol{z}) = (H(\boldsymbol{Ay} \bmod 2q, \mu),\ \boldsymbol{y} + (-1)^b c \cdot \boldsymbol{S})$

PK :



Sig :



❖ Signature Scheme based on Bimodal Hyperball distribution

◆ Key Generation(1^λ)

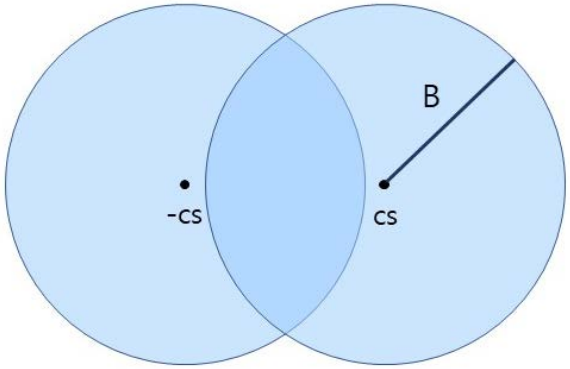
1. $\boldsymbol{A_0} \leftarrow R_q^{k\times(l-1)}$, $(\boldsymbol{s_0}, \boldsymbol{e_0}) \leftarrow S_\eta^{l-1} \times S_\eta^k$
2. $\boldsymbol{b} = \boldsymbol{A_0} \cdot \boldsymbol{s_0} + \boldsymbol{e_0} \in R_q^k$
3. $\boldsymbol{A} = (-2\boldsymbol{b} + q\boldsymbol{j} | 2\boldsymbol{A_0} | 2\boldsymbol{ID_k}) \, mod 2q$
4. $\boldsymbol{S} = (1, \boldsymbol{s_0}, \boldsymbol{e_0})$
5. if $f(\boldsymbol{S}) > n\beta^2/\tau^2$, then restart
6. **return** $sk = \boldsymbol{S}, pk = (\boldsymbol{A_0}, \boldsymbol{b})$

◆ Sign(sk,M)

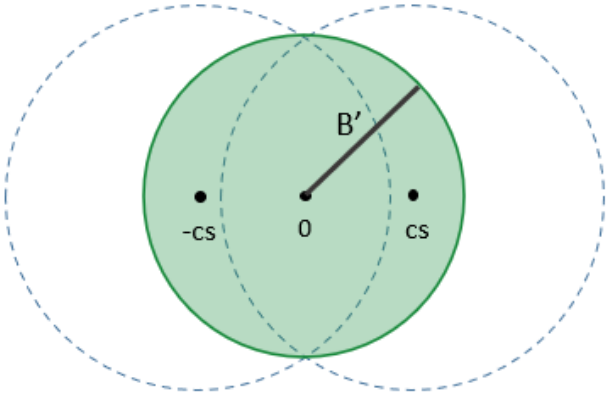
1. $\boldsymbol{y} \leftarrow U\big(HB(B)\big)$
2. $c = H(\boldsymbol{A}\boldsymbol{y}, M) \in R_2$
3. $\boldsymbol{z} = \boldsymbol{y} + (-1)^b c \cdot \boldsymbol{S}$ for $b \leftarrow U(\{0,1\})$
4. **return** $\sigma = (c, \boldsymbol{z})$ with prob. $p(\boldsymbol{z})$

◆ Verify(pk,M,σ)

1. $\boldsymbol{w} = \boldsymbol{A}\boldsymbol{z} - qc\boldsymbol{j}$
2. **return** $\big(c = H(w, M)\big) \wedge \ (\|\boldsymbol{z}\|_2 < B'')$



Source distribution



Target distribution

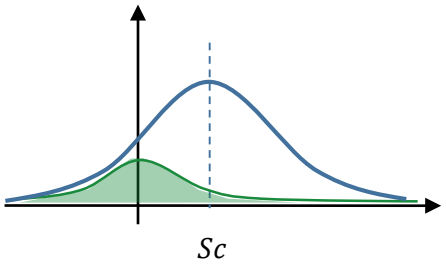
❖ Bimodal Hyperball distribution

◆ Bimodal distribution [DDLL13]

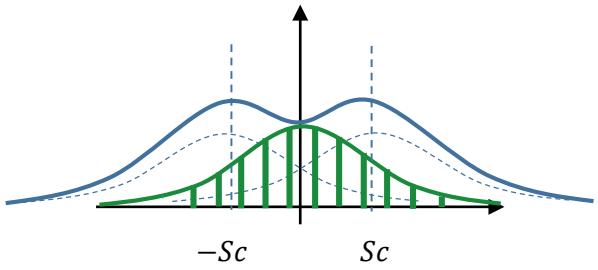
Algorithm 1: Signature Algorithm

Input: Message μ, public key $\mathbf{A} \in \mathbb{Z}_{2q}^{n \times m}$, secret key $\mathbf{S} \in \mathbb{Z}_{2q}^{m \times n}$, stand. dev. $\sigma \in \mathbb{R}$
Output: A signature $(\mathbf{z}, \mathbf{c})$ of the message μ
1: $\mathbf{y} \leftarrow D_\sigma^m$
2: $\mathbf{c} \leftarrow H(\mathbf{Ay} \bmod 2q, \mu)$
3: Choose a random bit $b \in \{0, 1\}$
4: $\mathbf{z} \leftarrow \mathbf{y} + (-1)^b\mathbf{Sc}$
5: **Output**$(\mathbf{z}, \mathbf{c})$ with probability $1 \Big/ \left(M \exp\left(-\frac{\|\mathbf{Sc}\|^2}{2\sigma^2}\right) \cosh\left(\frac{\langle \mathbf{z}, \mathbf{Sc} \rangle}{\sigma^2}\right)\right)$ otherwise **restart**

$z = y + Sc$



$z = y + (-1)^b Sc$



- Exp.Reps ↓
- signature size ↓

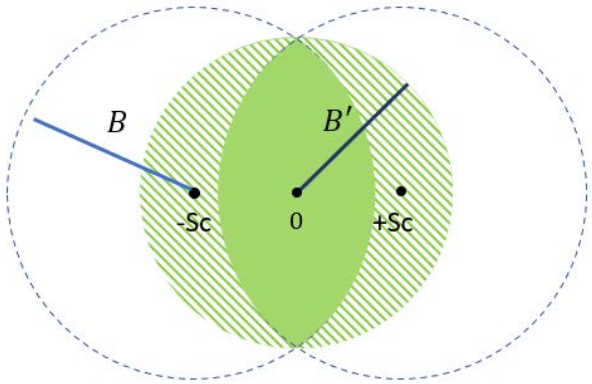
[DDLL13] L. Ducas. et al., *"Lattice signatures and bimodal Gaussians"*, CRYPTO 2013

❖ Bimodal Hyperball Uniform distribution

◆ rejection sampling condition

▪ Uniform Hyperball distribution

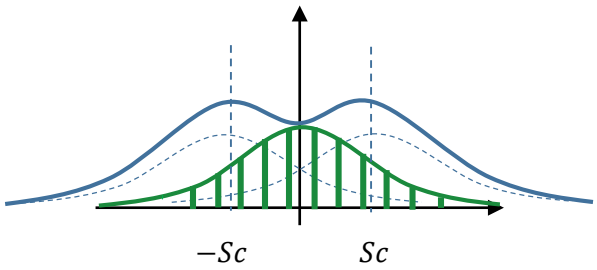
$$\frac{f(z)}{Mg(z)} = \begin{cases} 0 & \text{if } \|z\| \geq B' \\ 1/2 & \text{else if } \|z - Sc\| < B \wedge \|z + Sc\| < B \\ 1 & otherwise \end{cases}$$



- Simple rejection condition
- Optimal rejection rate [DFPS22]

▪ Gaussian distribution [LYU12,DDLL13]

$$\frac{f(z)}{Mg(z)} = 1/\left(M\, exp\left(-\frac{\|Sc\|^2}{2\sigma^2}\right) cosh\left(\frac{<z,Sc>}{\sigma^2}\right)\right)$$



- Complicate rejection rate
- Risk of side-channel attacks [EFGT17]

[LYU12] V. Lyubashevsky, *"Lattice Signatures without Trapdoors"*, Eurocrypt 2012
[DDLL13] L. Ducas. et al., *"Lattice signatures and bimodal Gaussians"*, CRYPTO 2013
[EFGT17] T. Espitau. et al., *"Side-channel attacks on BLISS lattice-based signatures"*, CCS 2017
[DFPS22] J. Devevey. et al., *"On Rejection Sampling in Lyubashevsky's Signature Scheme"*, ASIACRYPT 2022

- **BimodalSelfTargetMSIS**
  - Given $(\boldsymbol{A_0}, \boldsymbol{b}) \leftarrow R_q^{k\times(l-1)} \times R_q^k$ where $\boldsymbol{A} = (-2\boldsymbol{b} + q\boldsymbol{j} | 2\boldsymbol{A_0} | 2\boldsymbol{ID_k}) \; mod 2q$
    find $\boldsymbol{x}, c, M$ s.t $0 < \|\boldsymbol{x}\|_2 \leq \beta$ and $H(\boldsymbol{Ax} - qc\boldsymbol{j} \; mod 2q, M) = c$

❖ Security Proof

◆ Reduction from MSIS to BimodalSelfTargetMSIS

$\mathcal{A}$ (MSIS adversary)

$\mathcal{B}$ (BimodalSelfTargetMSIS adversary)

$\boldsymbol{A}$

$\boldsymbol{A} = (\boldsymbol{b} | \boldsymbol{A_0})$

$\boldsymbol{A}$

$\boldsymbol{A}' = (-2\boldsymbol{b} + q\boldsymbol{j} | 2\boldsymbol{A_0} | 2\boldsymbol{I}_k) \; mod 2q$

$\boldsymbol{w} = \boldsymbol{A}'\boldsymbol{y}$

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

By rewinding technique

$get \;\; (\boldsymbol{z}, c, M), (\boldsymbol{z}', c', M')$
$s.t \; \boldsymbol{A}'\boldsymbol{z} - qc\boldsymbol{j} = \boldsymbol{w} \; mod 2q,$
$\boldsymbol{A}'\boldsymbol{z}' - qc'\boldsymbol{j} = \boldsymbol{w} \; mod 2q$
$\Leftrightarrow \boldsymbol{A}'(\boldsymbol{z} - \boldsymbol{z}') = q(c - c')\boldsymbol{j} \; mod 2q$

$\Longrightarrow c - c' \neq 0 \; mod 2 \; (\because c \in \{0,1\}^n, c \neq c')$
$\Longrightarrow \boldsymbol{z} - \boldsymbol{z}' \neq 0 \; mod 2q$
$\Longrightarrow \boldsymbol{A}'(\boldsymbol{z} - \boldsymbol{z}') \equiv (-2\boldsymbol{b} | 2\boldsymbol{A_0} | 2\boldsymbol{I_k})(\boldsymbol{z} - \boldsymbol{z}')$
$\equiv 0 \; mod q$
$\& \; 0 < \|\boldsymbol{z} - \boldsymbol{z}'\|_2 < 2\beta$

$\boldsymbol{z} - \boldsymbol{z}'$

❖ Security Proof

◆ Reduction from UF-NMA to UF-CMA

- **[DFPS23] Theorem 4**

1. high min-entropy of commitment
2. ID protocol Σ = HVZK

→ **UF-NMA reduces to UF-CMA**

◆ UF-CMA Security Proof

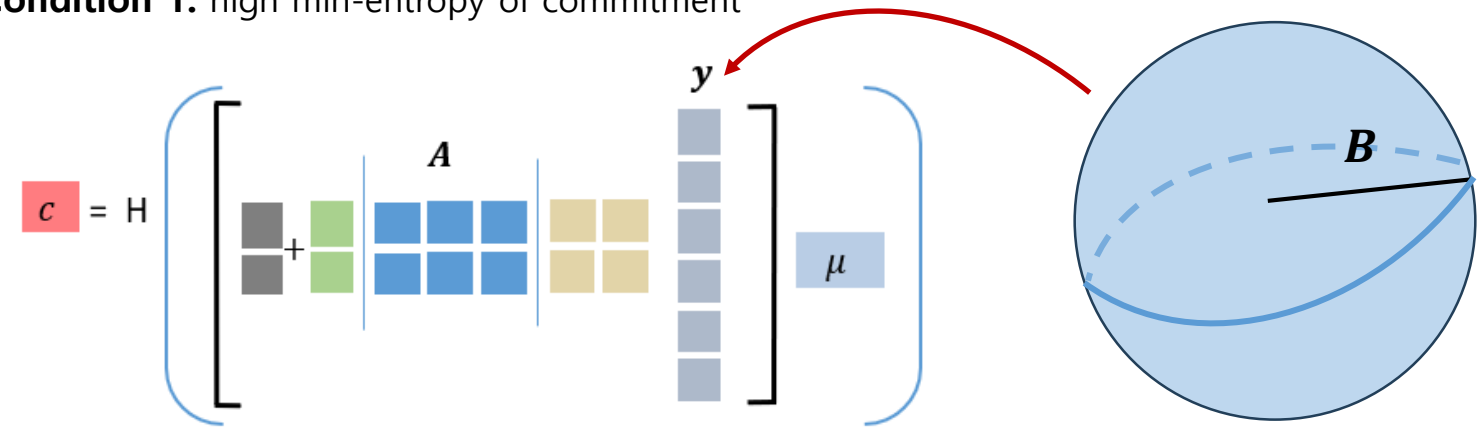
- G_0 : The original UF-CMA game
- G_1 : Changing the signing oracle with sk
- G_2 : Changing the signing oracle without sk
- G_3 : Public key → random

Min-entropy (commitment)

Zero-knowledge

Decisional LWE

Condition 1. high min-entropy of commitment



Condition 2. ID protocol Σ = HVZK

[DFPS23] J. Devevey. et al., *"A detailed analysis of Fiat-Shamir with aborts"*, CRYPTO 2023

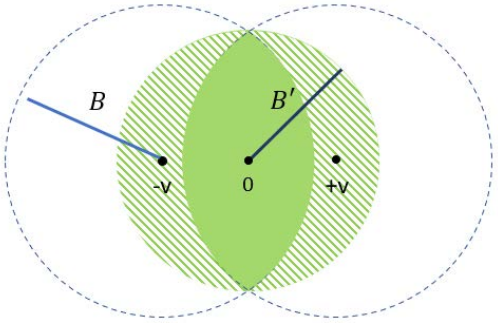
❖ Bimodal Hyperball Rejection Sampling

◆ Lemma 1 [Discrete Bimodal Hyperball Rejection sampling]

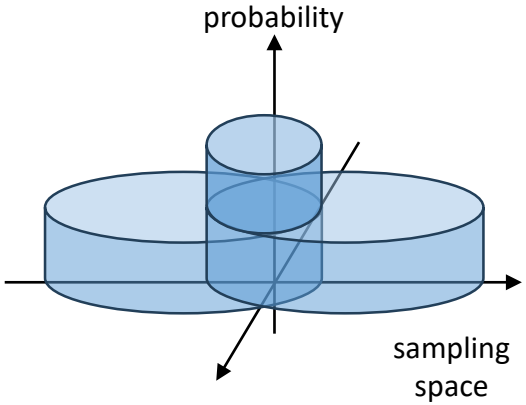
n: degree of R, $c > 1, B', t, m > 0, B \geq \sqrt{(B')^2 + t^2}$

Define $M = 2(B/B')^{mn}$ and $N \geq \frac{1}{c^{1/(mn)}-1}\frac{\sqrt{mn}}{2}\left(\frac{c^{1/(mn)}}{B'} + \frac{1}{B}\right)$

Let $v \in R^m \cap HB_{(1/N)R,m}(t)$ and $p: \mathbb{R}^m \to \{0, 1/2, 1\}$ be defined as follows



$$p(z) = \begin{cases} 0 & \text{if } \|z\| \geq B' \\ 1/2 & \text{else if } \|z - v\| < B \wedge \|z + v\| < B \\ 1 & otherwise \end{cases}$$



Then $\exists M' < cM$ $s.t$ $output\ distribution\ of\ \mathcal{A}(v), \mathcal{B}, \mathcal{A}(0)$ $are\ identical$

$\mathcal{A}(v)$:
1. $\boldsymbol{y} \leftarrow U(HB_{(1/N)R,m}(B))$
2. $b \leftarrow U(\{0,1\})$
3. $\boldsymbol{z} \leftarrow \boldsymbol{y} + (-1)^b \boldsymbol{v}$
4. return $\boldsymbol{z}$ with $p(\boldsymbol{z})$
5. else return $\perp$

$\mathcal{B}$:
1. $\boldsymbol{z} \leftarrow U(HB_{(1/N)R,m}(B'))$
2. return $\boldsymbol{z}$ with $1/M'$
3. else return $\perp$

$\mathcal{A}(0)$:
1. $\boldsymbol{y} \leftarrow U(HB_{(1/N)R,m}(B))$
2. $\boldsymbol{z} \leftarrow \boldsymbol{y}$
3. return $\boldsymbol{z}$ with $p(\boldsymbol{z})$
4. else return $\perp$

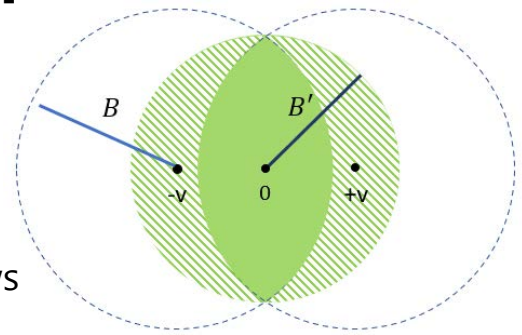
❖ Bimodal Hyperball Rejection Sampling

◆ Lemma 1 [Discrete Bimodal Hyperball Rejection sampling]

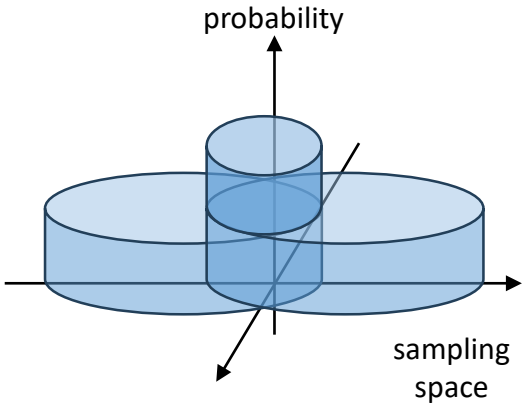
n: degree of R, $c > 1, B', t, m > 0, B \geq \sqrt{(B')^2 + t^2}$

Define $M = 2(B/B')^{mn}$ and $N \geq \frac{1}{c^{1/(mn)}-1}\frac{\sqrt{mn}}{2}\left(\frac{c^{1/(mn)}}{B'} + \frac{1}{B}\right)$

Let $v \in R^m \cap HB_{(1/N)R,m}(t)$ and $p: \mathbb{R}^m \to \{0, 1/2, 1\}$ be defined as follows



$$p(z) = \begin{cases} 0 & \text{if } \|z\| \geq B' \\ 1/2 & \text{else if } \|z - v\| < B \wedge \|z + v\| < B \\ 1 & otherwise \end{cases}$$



Then $\exists M' < cM$ $s.t$ $output\ distribution\ of\ \mathcal{A}(v), \mathcal{B}, \mathcal{A}(0)$ $are\ identical$

$\mathcal{A}(v)$:
1. $\boldsymbol{y} \leftarrow U(HB_{(1/N)R,m}(B))$
2. $b \leftarrow U(\{0,1\})$
3. $\boldsymbol{z} \leftarrow \boldsymbol{y} + (-1)^b \boldsymbol{v}$
4. return $\boldsymbol{z}$ with $p(\boldsymbol{z})$
5. else return $\perp$

No guarantees for polynomial time simulator

$\mathcal{A}(0)$:
1. $\boldsymbol{y} \leftarrow U(HB_{(1/N)R,m}(B))$
2. $\boldsymbol{z} \leftarrow \boldsymbol{y}$
3. return $\boldsymbol{z}$ with $p(\boldsymbol{z})$
4. else return $\perp$

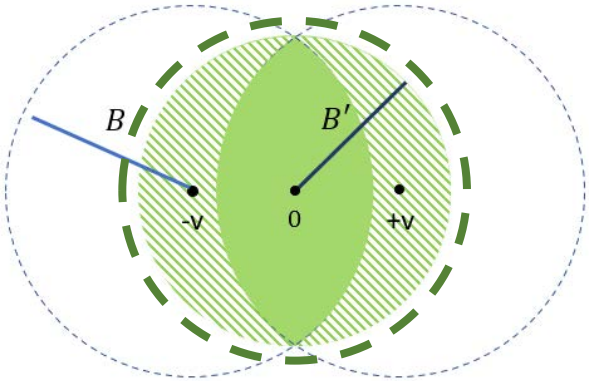
❖ Bimodal Hyperball Rejection Sampling

◆ Lemma 1 [Discretized Bimodal Hyperball Rejection sampling]

$B \geq \sqrt{(B')^2+t^2}$, $M = 2(B/B')^{mn}$ and $v \in R^m \cap HB_{(1/N)R,m}(t)$

Let $p: \mathbb{R}^m \to \{0, 1/2, 1\}$ be defined as follows

$$p(z) = \begin{cases} 0 & \text{if } \|z\| \geq B' \\ 1/2 & \text{else if } \|z-v\| < B \wedge \|z+v\| < B \\ 1 & otherwise \end{cases}$$



Then $\exists M' < cM \; s.t$ *output distribution of* $\mathcal{A}(v), \mathcal{A}(0)$ *are identical*

$\mathcal{A}(v)$:

1. $\boldsymbol{y} \leftarrow U(HB_{(1/N)R,m}(B))$
2. $b \leftarrow U(\{0,1\})$
3. $\boldsymbol{z} \leftarrow \boldsymbol{y} + (-1)^b \boldsymbol{v}$
4. return $\boldsymbol{z}$ with $p(\boldsymbol{z})$
5. else return $\perp$

$\mathcal{A}(0)$:

1. $\boldsymbol{y} \leftarrow U(HB_{(1/N)\mathcal{R},m}(B))$
2. $\boldsymbol{z} \leftarrow \boldsymbol{y}$
3. return $\boldsymbol{z}$ with $p(\boldsymbol{z})$
4. else return $\perp$

Recommend!
Or prove M' can be calculated in polynomial time

비교

Security Level	λ	Parameter Sets	n	(k,l)	q	pk (Bytes)	sig (Bytes)	sk (Bytes)	pk+sig (Bytes)	M
Ⅰ -	71	GCK - Ⅰ	256	(2,5)	$\approx 2^{25}$	1,632	2,592	352	4,224	2.55
Ⅱ	133.9	NCC - Ⅰ	1021	-	8339581	1,564	2,458	2,266	4,022	6.6
	119	HAETAE-120	256	(2,4)	64513	**992**	**1,463**	1,376	**2,455**	6.0
	123	Dilithium - Ⅱ	256	(4,4)	8380417	1,312	2,420	-	3,732	4.25
	134	GCK - Ⅱ	256	(3,8)	$\approx 2^{26}$	2,528	4,384	544	6,912	3.38
Ⅲ	198.1	NCC - Ⅲ	1429	-	8376649	1,997	3,605	3,312	5,602	5.7
	180	HAETAE-180	256	(3,6)	64513	**1,472**	**2,337**	2,080	**3,809**	5.0
	182	Dilithium - Ⅲ	256	(6,5)	8380417	1,952	3,293	-	5,245	5.1
Ⅴ	259.8	NCC - Ⅴ	1913	-	8343469	2,663	5,055	4,402	7,718	5.5
	256	HAETAE-260	256	(4,7)	64513	**2,080**	**2,908**	2,720	**4,988**	6.0
	252	Dilithium - Ⅴ	256	(8,7)	8380417	2,592	4,595	-	7,187	3.85
	291	GCK - Ⅴ	256	(7,17)	$\approx 2^{27}$	6,080	10,368	1,120	16,448	3.41

분석 결과 요약

❖ GCKSign

- **GCK TMO** 기반 안전성 증명
- **신규 난제 GCK TMO**를 정의하여 [LYU09]의 안전성 증명에서 요구되는 추가적인 조건을 제거
- **키 복구 공격**에 안전하게 수정하여 **공개키 및 서명 크기가 증가**함

❖ HAETAE

- **Module LWE** 및 **BimodalSelfTargetMSIS** 기반 안전성 증명
- **Bimodal Hyperball distribution**을 사용하여 서명의 크기를 줄임
- **Rejection sampling**에서 **효율적인 simulator**에 대한 추가적인 증명이 필요함

❖ NCC-Sign

- **Ring LWE** 및 **SelfTargetRSIS** 기반 안전성 증명
- **non-cyclotomic ring**을 사용하여 부채널 공격의 위험성을 줄임
- 기법의 신규성이 떨어짐

Thank You

Q&A