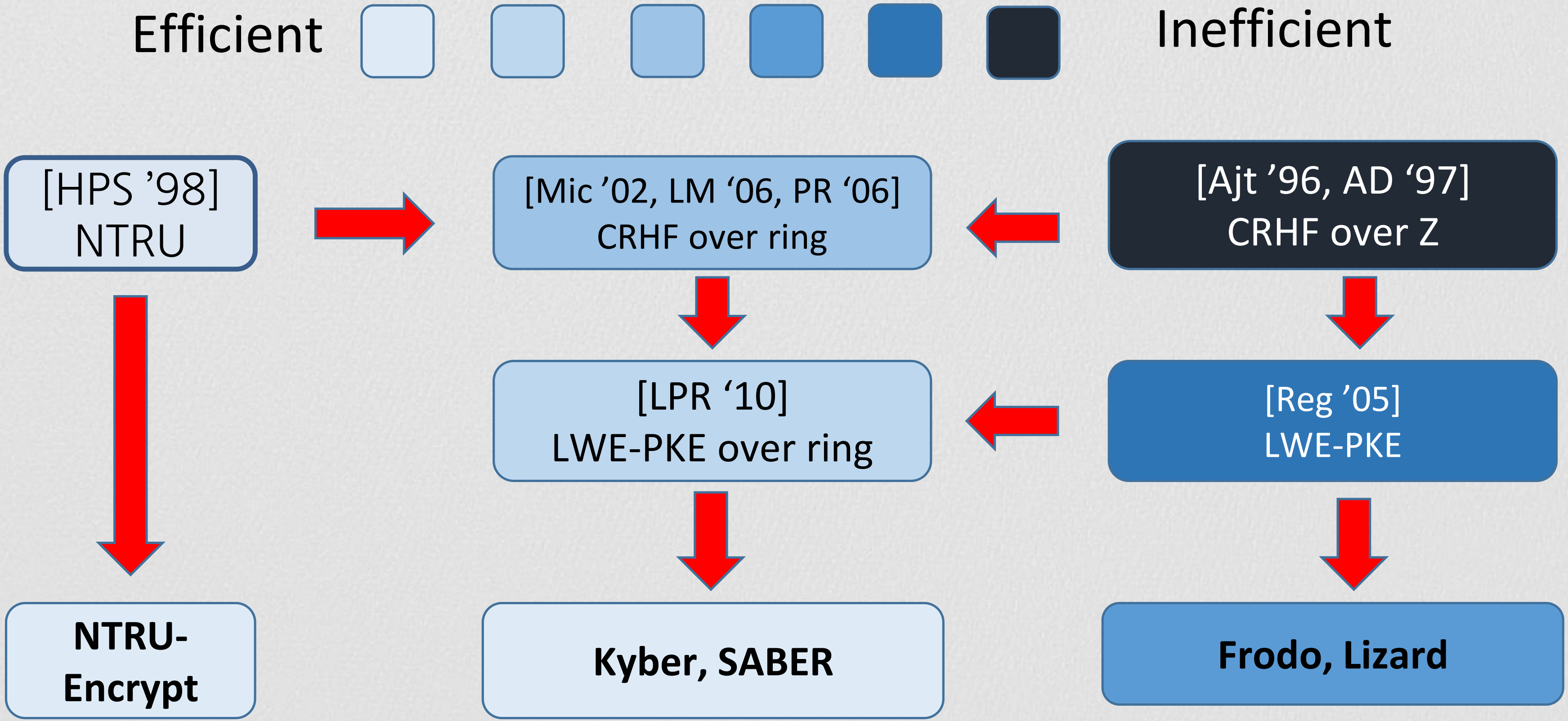
격자기반 암호

목차

5

대수적 격자 기반 암호

Encryption scheme overview



Cited from 'Lattice Cryptography in the NIST Standardization Process', Vadim Lyubashevsky

격자기반 암호 CRHF

- Collision - Resistant Hash Functions (CRHF)

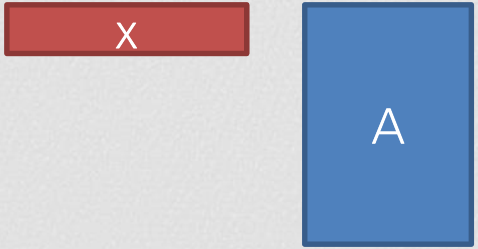
  Input: $\{0,1\}^m$

  Output: $\mathbb{Z}_q^n$

  Hard to find collisions; $x \neq y,\ f(x) = f(y)$

- 격자 기반 CRHF

$f(x) =$



$\bmod q$

대수적 격자기반 암호 CRHF

- Collision - Resistant Hash Functions (CRHF)

  Input: $\{0,1\}^m$

  Output: R_q

  Hard to find collisions; $x \neq y,\ f(x) = f(y)$

- 격자 기반 CRHF

$$f(x) = \begin{bmatrix} x & y & z & w \end{bmatrix} \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} \bmod q$$

대수적 격자/ 격자기반 CRHF 비교

	격자	아이디얼 격자
Storage	$\tilde{O}(n^2)$	$\tilde{O}(n)$
Computing Time	$\tilde{O}(n^2)$	$\tilde{O}(n)$
Hardness Assumption	SIVP	SVP
Break Known attack time	$2^{\Omega(n)}$	$2^{\Omega(n)}$

NTRU 기반 PKE

Given $\boxed{h}$ and $\boxed{h} = \dfrac{\boxed{g}}{\boxed{f}} \bmod q$

$$\mathrm{Enc}(m) = 2\,\boxed{h}\,\boxed{r} + \boxed{m} \bmod q = \boxed{c}$$

$$m \in \{0,1\}^n$$

$$\mathrm{Dec(c)} = \frac{\boxed{c}\,\boxed{f} \bmod q}{\boxed{f}} \bmod 2$$

NTRU 기반 PKE

Given $\boxed{h}$ and $\boxed{h} = \dfrac{\boxed{g}}{\boxed{f}} \bmod q$

$$\mathrm{Enc}(m) = 2\,\boxed{h}\,\boxed{r} + \boxed{m} \bmod q = \boxed{c}$$

$$= 2\,\frac{\boxed{g}}{\boxed{f}}\,\boxed{r} + \boxed{m} \bmod q$$

$$= \frac{2\,\boxed{g}\,\boxed{r} + \boxed{m}\,\boxed{f}}{\boxed{f}} \bmod q$$

NTRU 기반 PKE

Given $\boxed{h}$ and $\boxed{h} = \dfrac{\boxed{g}}{\boxed{f}} \mod q$

$$\mathrm{Dec(c)} = \frac{\boxed{c}\,\boxed{f} \mod q}{\boxed{f}} \mod 2 = \left(\boxed{c}\,\boxed{f} \mod q\right) \Big/ \boxed{f} \mod 2$$

$$= \left(2\,\boxed{g}\,\boxed{r} + \boxed{m}\,\boxed{f}\right) \Big/ \boxed{f} \mod 2$$

$$= \boxed{m}\,\boxed{f} \Big/ \boxed{f} \mod 2 = \boxed{m}$$

RLWE 기반 PKE

Pk $\boxed{A}\ \boxed{t} = \boxed{A}\,\boxed{s} + \boxed{e} \bmod q$

Sk $\boxed{s}$

$$\mathrm{Enc}(m) = \boxed{r}\,\boxed{A \mid t} + \boxed{e'} + \boxed{0 \mid m^*} = \boxed{u \mid v}$$

$$m \in \{0,1\}^n$$

$$m^* = \tfrac{q-1}{2} \cdot m$$

RLWE 기반 PKE

$\mathrm{Dec}(c) = \boxed{v} - \boxed{u}\,\boxed{s}$

$$= (m_1, \ldots, m_n) \quad m_i = \begin{cases} 0 & \text{if } m_i^* \approx 0 \\ 1 & \text{if } m_i^* \approx \frac{q-1}{2} \end{cases}$$

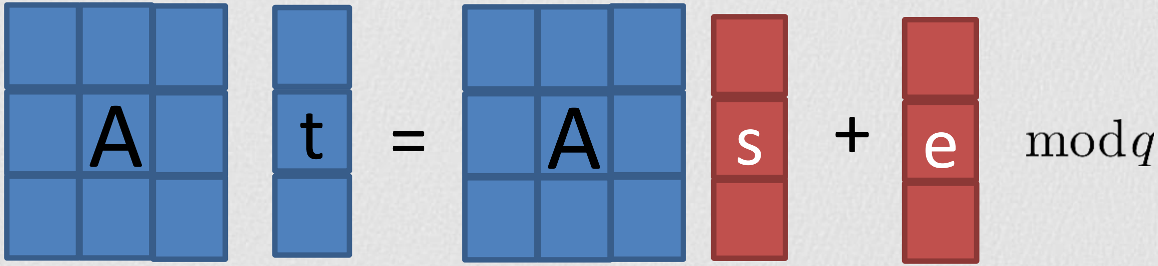
$\boxed{v} = \boxed{r}\,\boxed{t} + \boxed{e'} + \boxed{m^*}$

$= \boxed{r}\left(\boxed{A}\,\boxed{s} + \boxed{e}\right) + \boxed{e'} + \boxed{m^*}$

$= \boxed{u}\,\boxed{s} + \boxed{} + \boxed{m^*}$

Algebraic LWE 기반 PKE

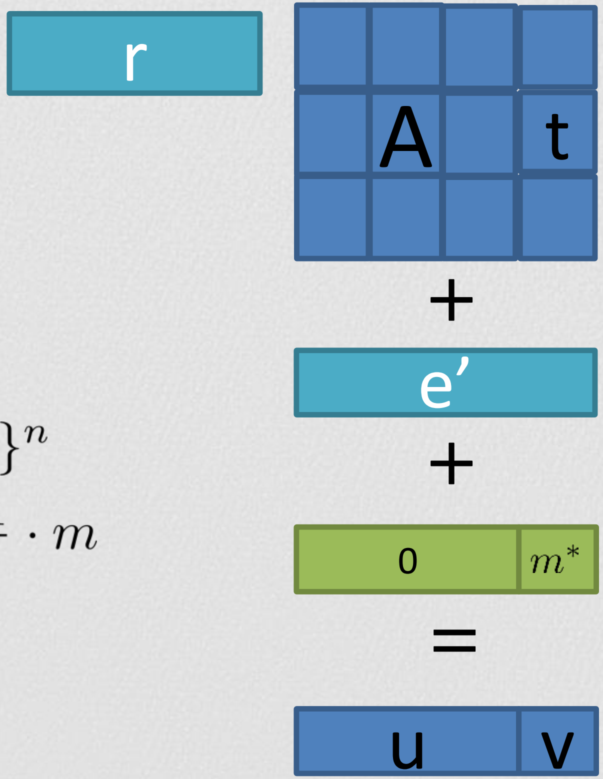
Pk



Sk

Algebraic LWE 기반 PKE

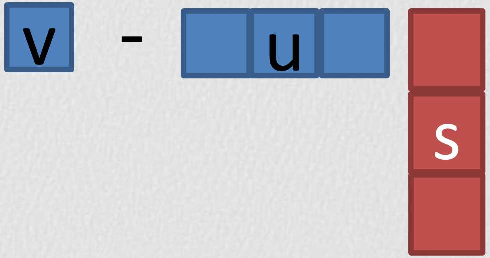
$\mathrm{Enc}(m) =$



$m \in \{0,1\}^n$

$m^* = \frac{q-1}{2} \cdot m$

$\mathrm{Dec}(c) =$



$= (m_1, \ldots, m_n)$

$$m_i = \begin{cases} 0 & \text{if } m_i^* \approx 0 \\ 1 & \text{if } m_i^* \approx \frac{q-1}{2} \end{cases}$$

대수적 격자/ 격자기반 PKE 비교

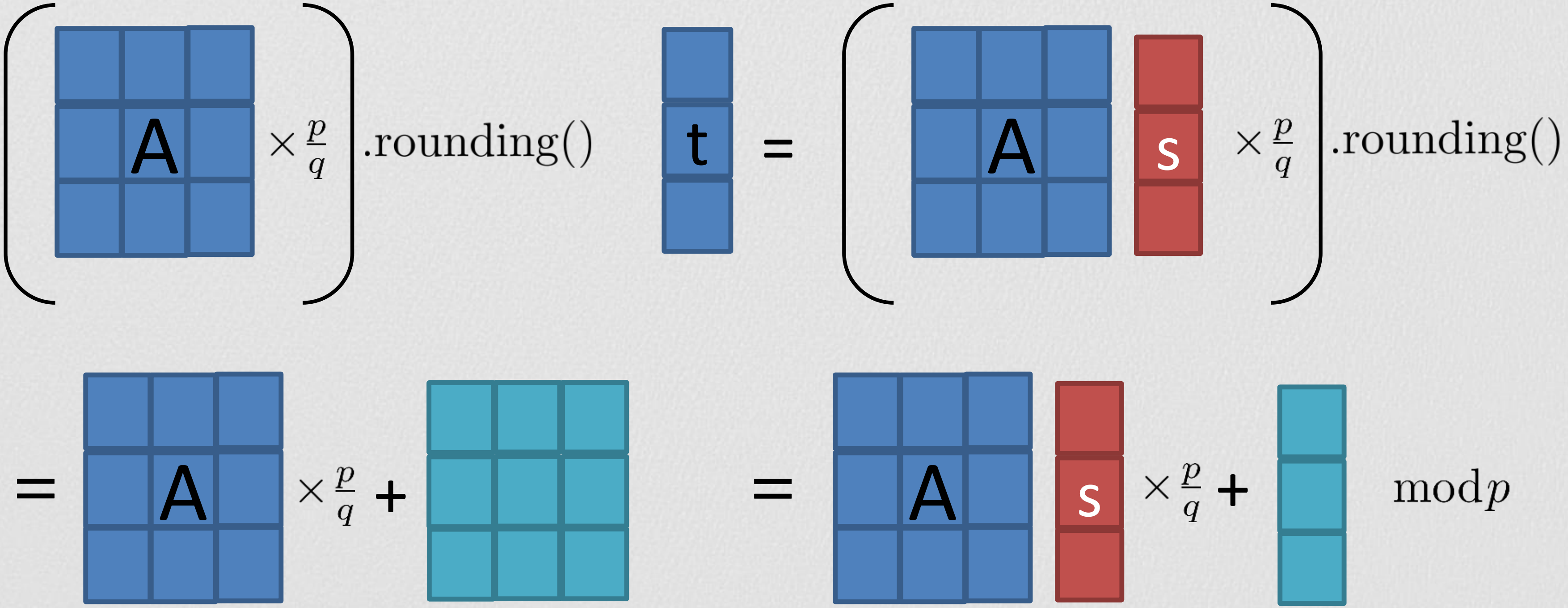
	격자	아이디얼 격자
Storage	$\tilde{O}(n^2)$	$\tilde{O}(n)$
Computing Time	$\tilde{O}(n^2)$	$\tilde{O}(n)$
Hardness Assumption	LWE	RLWE/ NTRU
Break Known attack time	$2^{\Omega(n)}$	$2^{\Omega(n)}$

Algebraic LWE 기반 PKE

Pk $\quad A \quad t = A \quad s + e \mod q$

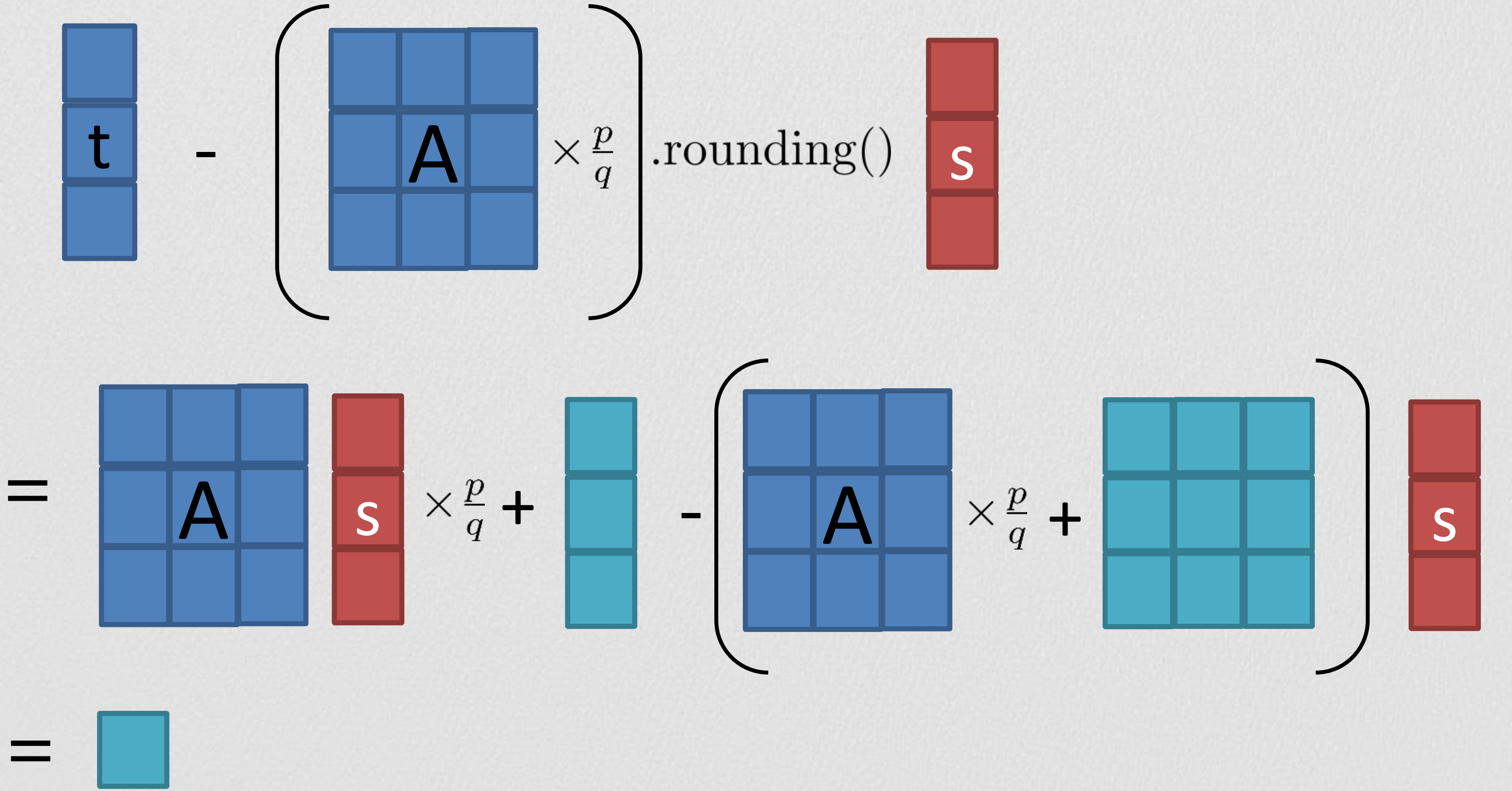
Sk $\quad s$

고속화 설계 – (1)



A
$\times \frac{p}{q}$
.rounding()
t
=
A
s
$\times \frac{p}{q}$
.rounding()
=
A
$\times \frac{p}{q}$ +
=
A
s
$\times \frac{p}{q}$ +
mod p

고속화 설계 – (1)



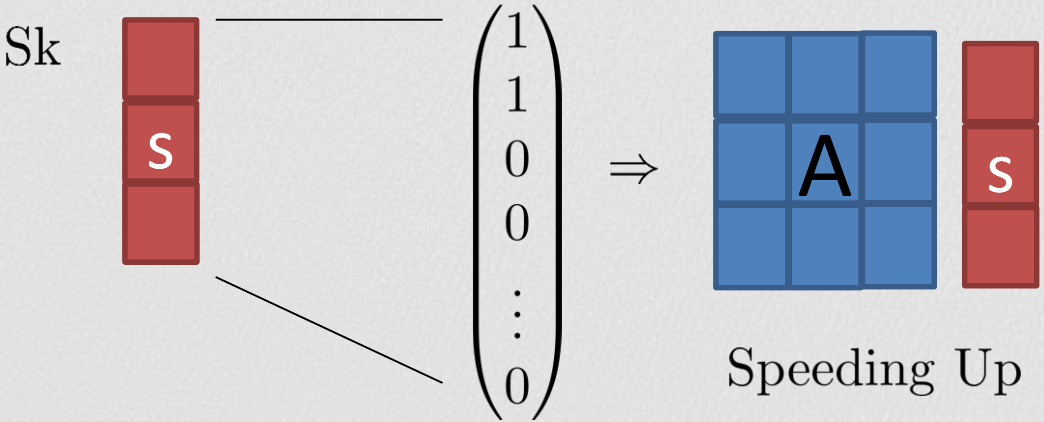
고속화 설계 – (1)

$$\left(A s \times \frac{p}{q}\right).\mathrm{rounding}()$$

$$= \left((A s + e) \times \frac{p}{q} \right).\mathrm{rounding}() = \left(u \times \frac{p}{q} \right).\mathrm{rounding}()$$

e.x $\lfloor 8 \times \frac{2}{3} \rceil = \lfloor 7 \times \frac{2}{3} \rceil = 5$

고속화 설계 – (2)



Question: Security?

6

격자 기반 디지털 사인

Digital Signature Overview

[HHPSW ‘03]
NTRU trapdoor

[GPV ’08, DP’16]
Improvement

FALCON

Based on NTRU

[Lyu ‘09]
Fiat-Shamir with Aborts

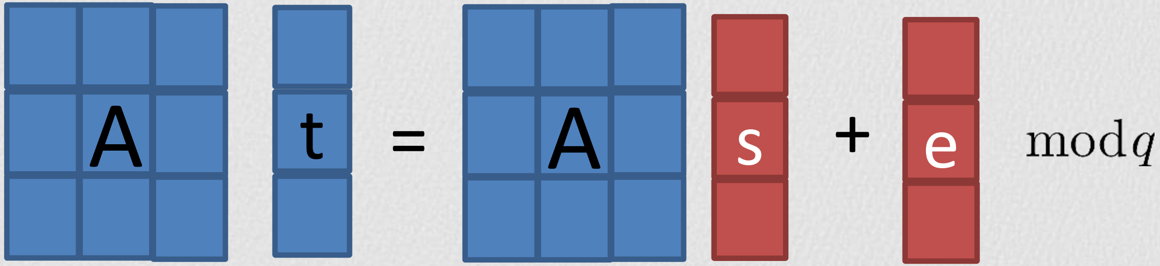
[GLP ’12, BG’14]
Compression

Dilithium

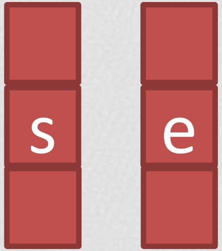
Based on algebraic LWE, SIS

Algebraic LWE 기반 Signature

Pk



Sk



Algebraic LWE 기반 Signature

$$Sign(m) = \boxed{c}\ \boxed{z}$$

$$\boxed{c} = \mathrm{Hash}\left(\mathrm{MSB}\left(\mathbf{A}\,\mathbf{y}\right) m\right)$$

$$\mathbf{z} = \mathbf{y} + c\,\mathbf{s}$$

Algebraic LWE 기반 Signature

$$verify(\boxed{c}, \boxed{z}, m)$$

$$\boxed{c} = \mathrm{Hash}\left(\mathrm{MSB}\left(\boxed{A}\,\boxed{z} - \boxed{c}\,\boxed{t}\right)\;\boxed{m}\right)$$

Algebraic LWE 기반 Signature

$$\mathrm{MSB}\left(A z - c t \right)$$

$$= \mathrm{MSB}\left(A \left(y + c s \right) - c \left(A s + e \right) \right)$$

Algebraic LWE 기반 Signature

$$\mathrm{MSB}\left(A\left(y + c\,s \right) - c\left(A s + e \right) \right)$$

$$= \mathrm{MSB}\left(A y - c\,e \right) = \mathrm{MSB}\left(A y \right)$$

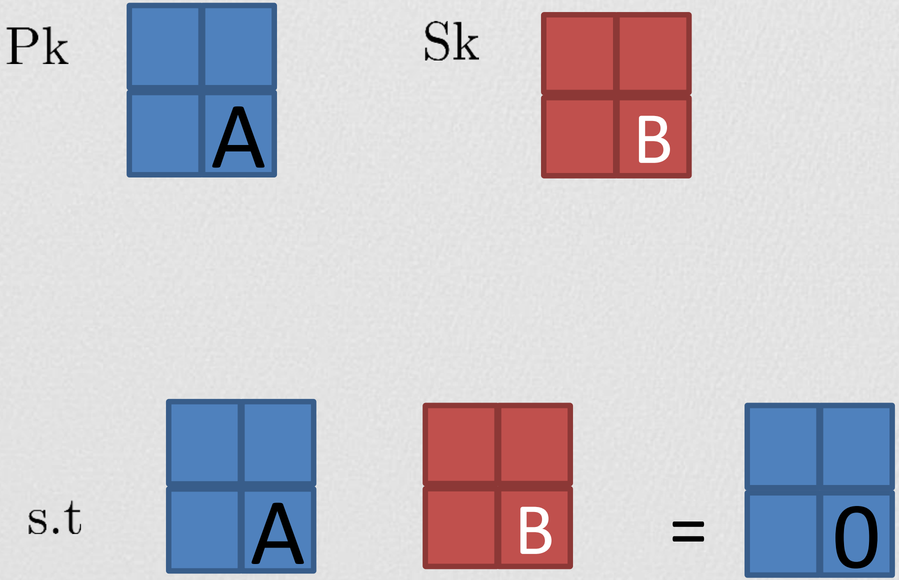
Algebraic LWE 기반 Signature

$$verify(\boxed{c}, \boxed{z}, m)$$

$$\boxed{c} = \mathrm{Hash}\left(\mathrm{MSB}\left(A z - c\, t\right) m\right)$$

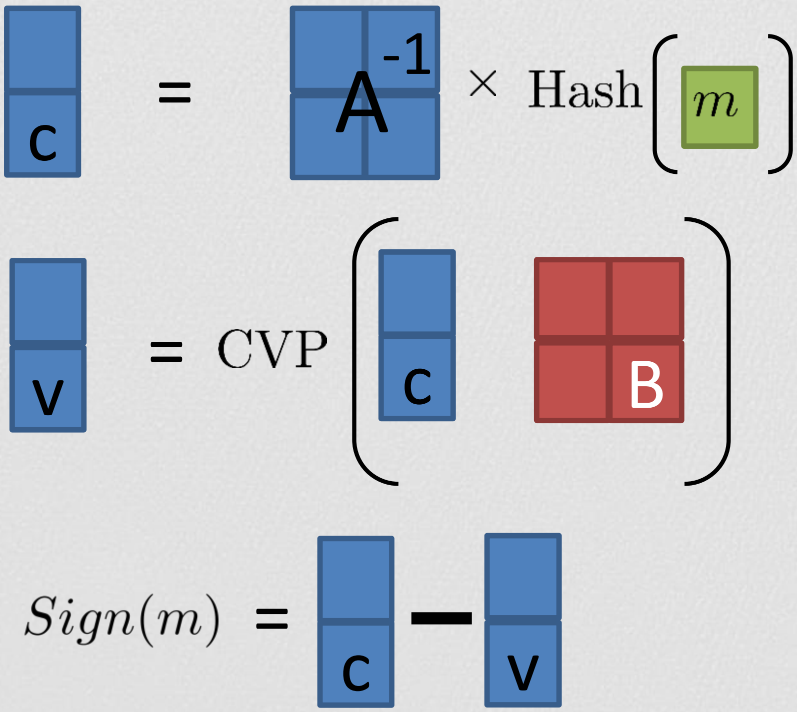
$$= \mathrm{Hash}\left(\mathrm{MSB}\left(A y\right) m\right)$$

NTRU 기반 Signature



NTRU 기반 Signature

$Sign(m)$



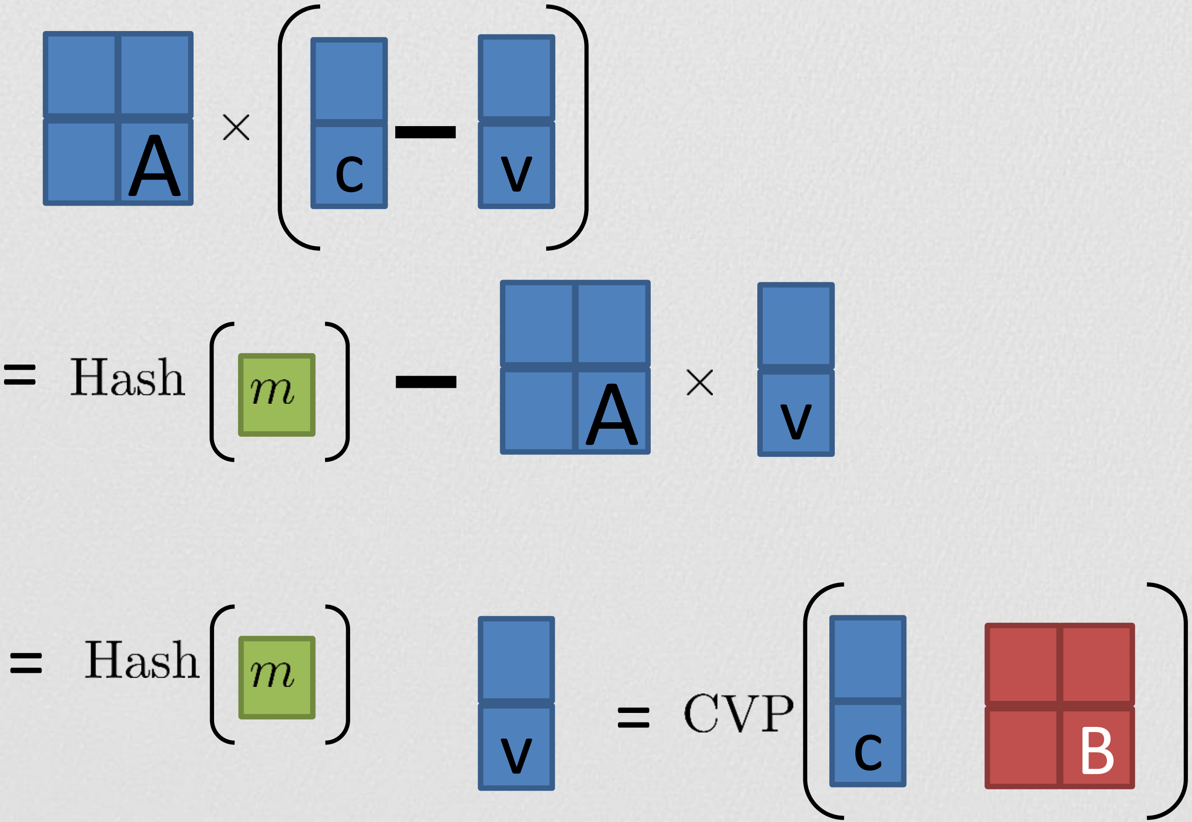
NTRU 기반 Signature

$$verify\left(\begin{bmatrix} \\ s \end{bmatrix}, m\right)$$

1) $\begin{bmatrix} \\ s \end{bmatrix}$ small

2) $\begin{bmatrix} & \\ & A \end{bmatrix} \times \begin{bmatrix} \\ s \end{bmatrix} = \mathrm{Hash}\left(\boxed{m}\right)$

NTRU 기반 Signature



NTRU 기반 Signature

$$\mathrm{Pk} \quad \begin{bmatrix} & \\ & A \end{bmatrix} \qquad \mathrm{Sk} \quad \begin{bmatrix} & \\ & B \end{bmatrix}$$

$$\mathrm{s.t} \quad \begin{bmatrix} & \\ & A \end{bmatrix} \begin{bmatrix} & \\ & B \end{bmatrix} = \begin{bmatrix} & \\ & 0 \end{bmatrix}$$

NTRU 문제

$q \in \mathbb{Z},\ R_q := R/qR = \mathbb{Z}_q[X]/\langle X^n + 1 \rangle$

Given $\boxed{h}$ and $\boxed{h} = \dfrac{\boxed{g}}{\boxed{f}} \bmod q$

Recover g and f

$\boxed{g}\ \boxed{f} \leftarrow \{-1, 0, 1\}^n$

NTRU 기반 Signature

$$h = \frac{g}{f} \qquad 1 = \frac{f}{f}$$

$$\begin{bmatrix} 1 & h \end{bmatrix} \times \begin{bmatrix} g \\ -f \end{bmatrix} = 0 \mod q$$

$$F\,g + G\,f = q \Leftarrow \mathrm{Ring} \div$$

$$\Leftrightarrow F\,\frac{g}{f} + G\,\frac{f}{f} = 0 \mod q$$

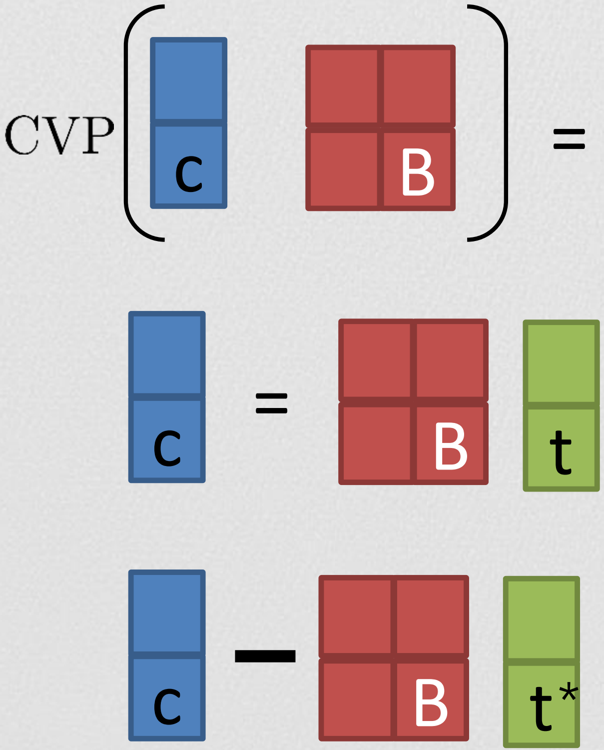
NTRU 기반 Signature

$$F \, \frac{g}{f} + G \, \frac{f}{f} = 0 \mod q$$

$$\Leftrightarrow \begin{bmatrix} 1 & h \end{bmatrix} \times \begin{bmatrix} F \\ G \end{bmatrix} = 0 \mod q$$

$$\begin{bmatrix} 1 & h \\ q & 0 \end{bmatrix} \times \begin{bmatrix} g & F \\ -f & G \end{bmatrix} = 0 \mod q$$

NTRU 기반 Signature



$\mathrm{t} \in \mathbb{Q}^m$

$\mathrm{t}^* \in \mathbb{Z}^m$