

격자기반 암호



— 목차

- [1] 격자란 무엇인가?
- [2] 격자 기반 문제
- [3] 격자 기반 공개키 암호
- [4] 대수적 격자소개
- [5] 대수적 격자 기반 공개키 암호
- [6] 격자 기반 디지털 사인

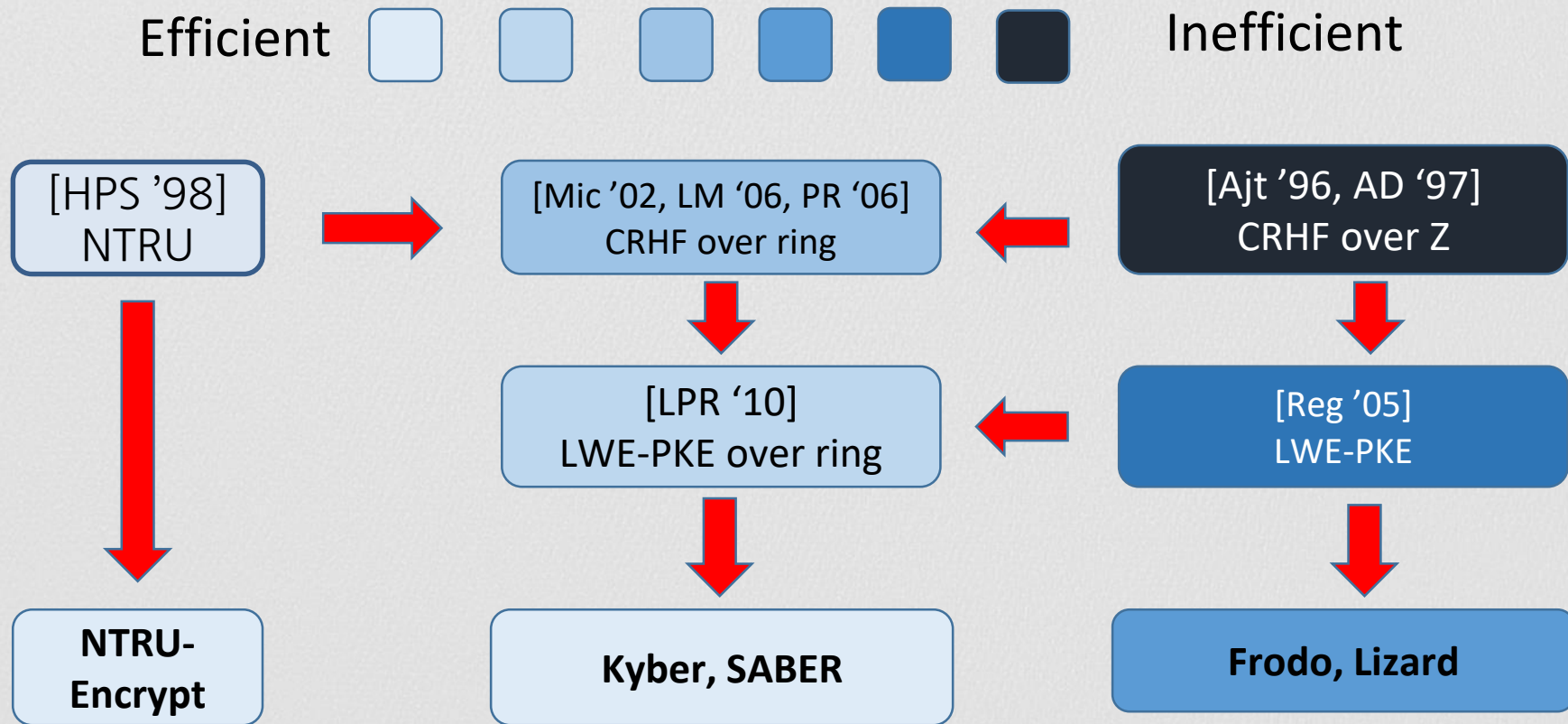


A top-down view of a light gray desk. In the top left, a portion of a silver laptop is visible, showing the keyboard and trackpad. To its right is a small, light blue USB drive. In the bottom right, there is a yellow notepad with spiral binding, a yellow pencil, and a dark gray pen.

5

대수적 격자 기반 암호

Encryption scheme overview



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

$$f(x) = \begin{matrix} \text{red box with } x \\ \text{blue box with } A \end{matrix} \bmod q$$

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

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

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 h and $h = \frac{g}{f} \bmod q$

$$\text{Enc}(m) = 2hr + m \bmod q = c$$

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

$$\text{Dec}(c) = \frac{cf \bmod q}{f} \bmod 2$$

NTRU 기반 PKE

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

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

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

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

NTRU 기반 PKE

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

$$\text{Dec}(c) = \frac{c \cdot f \bmod q}{f} \bmod 2 = \left(c \cdot f \bmod q \right) / f \bmod 2$$

$$= \left(2 \cdot g \cdot r + m \cdot f \right) / f \bmod 2$$

$$= m \cdot f / f \bmod 2 = m$$

RLWE 기반 PKE

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

$$\text{Sk} \quad \boxed{s} \quad \text{Enc}(m) = \boxed{r} \boxed{A} \boxed{t}$$

+

$$\boxed{e'}$$

+

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

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

$$\boxed{0} \boxed{m^*}$$

=

$$\boxed{u} \boxed{v}$$

RLWE 기반 PKE

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

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

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

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

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

Algebraic LWE 기반 PKE

Pk

$$\begin{bmatrix} \square & \square & \square \\ \square & A & \square \\ \square & \square & \square \end{bmatrix} \begin{bmatrix} \square \\ t \\ \square \end{bmatrix} = \begin{bmatrix} \square & \square & \square \\ \square & A & \square \\ \square & \square & \square \end{bmatrix} \begin{bmatrix} \square \\ s \\ \square \end{bmatrix} + \begin{bmatrix} \square \\ e \\ \square \end{bmatrix} \pmod{q}$$

Sk

$$\begin{bmatrix} \square \\ s \\ \square \end{bmatrix}$$

Algebraic LWE 기반 PKE

$$\begin{aligned}
 \text{Enc}(m) = & \text{r} \begin{bmatrix} & & & \\ & A & & t \\ & & & \end{bmatrix} \\
 & + \\
 & \text{e}' \\
 & + \\
 & \begin{bmatrix} 0 & m^* \end{bmatrix} \\
 = & \\
 & \begin{bmatrix} u & v \end{bmatrix}
 \end{aligned}$$

$m \in \{0, 1\}^n$
 $m^* = \frac{q-1}{2} \cdot m$

$$\begin{aligned}
 \text{Dec}(c) = & \begin{bmatrix} v \end{bmatrix} - \begin{bmatrix} u \end{bmatrix} \begin{bmatrix} s \end{bmatrix} \\
 = & (m_1, \dots, m_n)
 \end{aligned}$$

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

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

$$\begin{bmatrix} & & \\ & A & \\ & & \end{bmatrix} \begin{bmatrix} \\ t \\ \end{bmatrix} = \begin{bmatrix} & & \\ & A & \\ & & \end{bmatrix} \begin{bmatrix} \\ s \\ \end{bmatrix} + \begin{bmatrix} \\ e \\ \end{bmatrix} \pmod{q}$$

Sk

$$\begin{bmatrix} \\ s \\ \end{bmatrix}$$

고속화 설계 - (1)

$$\left(\begin{array}{|c|c|c|} \hline \square & \square & \square \\ \hline \square & A & \square \\ \hline \square & \square & \square \\ \hline \end{array} \right) \times \frac{p}{q} .\text{rounding}()$$
$$\begin{array}{|c|} \hline \square \\ \hline t \\ \hline \square \\ \hline \end{array} = \left(\begin{array}{|c|c|c|} \hline \square & \square & \square \\ \hline \square & A & \square \\ \hline \square & \square & \square \\ \hline \end{array} \begin{array}{|c|} \hline \square \\ \hline s \\ \hline \square \\ \hline \end{array} \times \frac{p}{q} .\text{rounding}()$$

$$= \begin{array}{|c|c|c|} \hline \square & \square & \square \\ \hline \square & A & \square \\ \hline \square & \square & \square \\ \hline \end{array} \times \frac{p}{q} + \begin{array}{|c|c|c|} \hline \square & \square & \square \\ \hline \square & \square & \square \\ \hline \square & \square & \square \\ \hline \end{array}$$
$$= \begin{array}{|c|c|c|} \hline \square & \square & \square \\ \hline \square & A & \square \\ \hline \square & \square & \square \\ \hline \end{array} \begin{array}{|c|} \hline \square \\ \hline s \\ \hline \square \\ \hline \end{array} \times \frac{p}{q} + \begin{array}{|c|} \hline \square \\ \hline \square \\ \hline \square \\ \hline \end{array} \bmod p$$

고속화 설계 - (1)

$$\begin{array}{|c|} \hline \text{t} \\ \hline \end{array} - \left(\begin{array}{|c|c|c|} \hline & & \\ \hline & A & \\ \hline & & \\ \hline \end{array} \times \frac{p}{q} \right) \text{.rounding}() \begin{array}{|c|} \hline \text{s} \\ \hline \end{array}$$

$$= \begin{array}{|c|c|} \hline & \\ \hline A & \text{s} \\ \hline & \\ \hline \end{array} \times \frac{p}{q} + \begin{array}{|c|} \hline \\ \hline \\ \hline \end{array} - \left(\begin{array}{|c|c|c|} \hline & & \\ \hline & A & \\ \hline & & \\ \hline \end{array} \times \frac{p}{q} + \begin{array}{|c|c|c|} \hline & & \\ \hline & & \\ \hline & & \\ \hline \end{array} \right) \begin{array}{|c|} \hline \text{s} \\ \hline \end{array}$$

$$= \begin{array}{|c|} \hline \\ \hline \end{array}$$

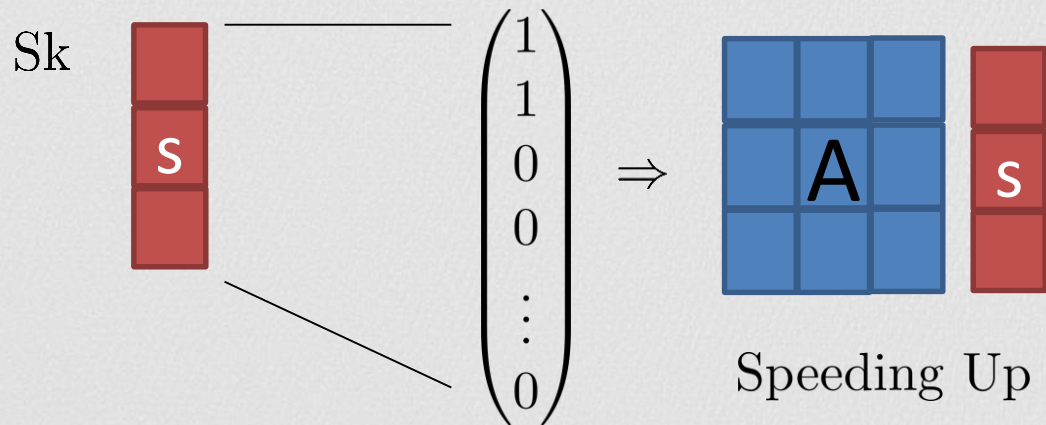
고속화 설계 - (1)

$$\left(\begin{array}{c|c} \begin{array}{|c|c|c|} \hline & & \\ \hline A & & \\ \hline & & \\ \hline \end{array} & \begin{array}{|c|} \hline \\ \hline s \\ \hline \\ \hline \end{array} \end{array} \right) \times \frac{p}{q} .\text{rounding}()$$

$$= \left(\begin{array}{c|c} \begin{array}{|c|c|c|} \hline & & \\ \hline A & & \\ \hline & & \\ \hline \end{array} & \begin{array}{|c|} \hline \\ \hline s \\ \hline \\ \hline \end{array} + \begin{array}{|c|} \hline \\ \hline e \\ \hline \\ \hline \end{array} \end{array} \right) \times \frac{p}{q} .\text{rounding}() = \left(\begin{array}{|c|} \hline \\ \hline u \\ \hline \\ \hline \end{array} \right) \times \frac{p}{q} .\text{rounding}()$$

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

고속화 설계 - (2)



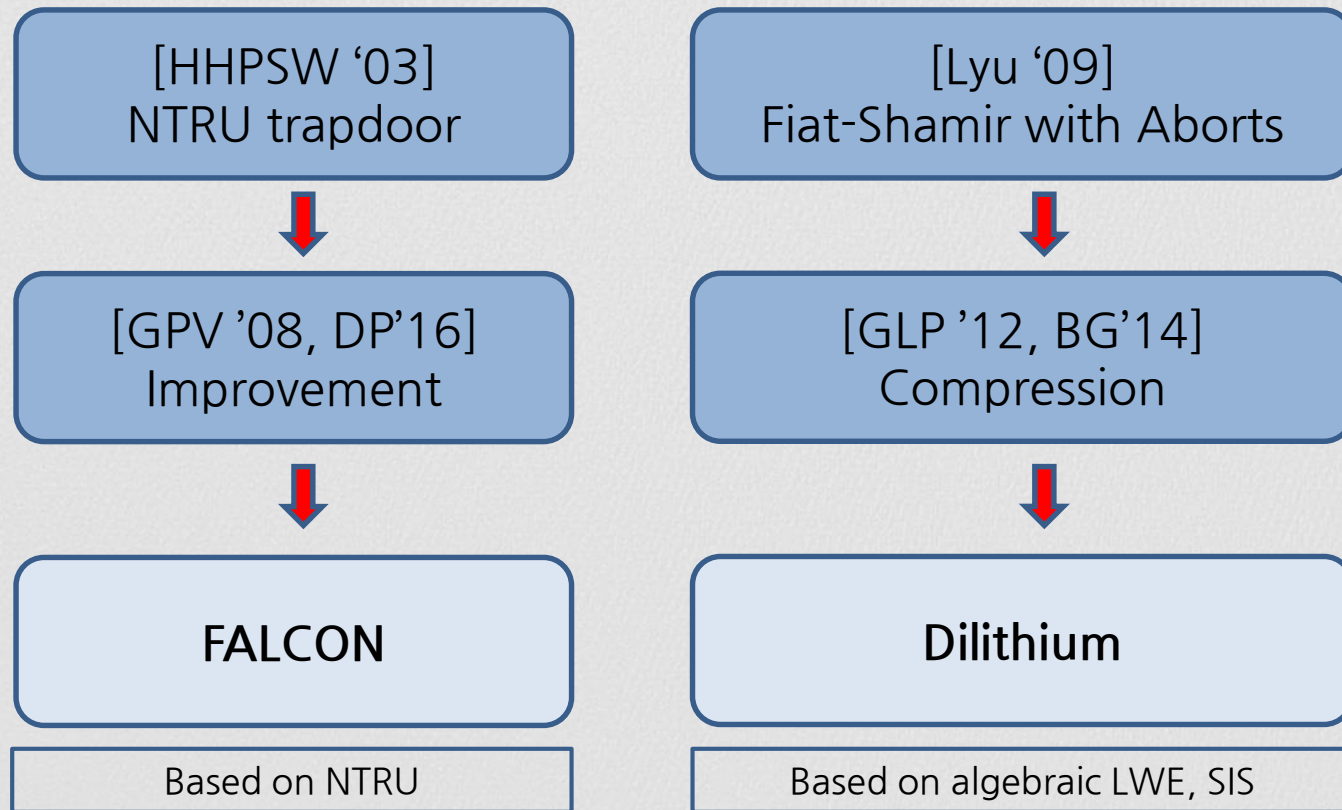
Question: Security?

A top-down view of a minimalist desk setup. In the top left, a portion of a silver laptop is visible, showing the keyboard and trackpad. To its right is a small, light blue USB drive. In the bottom right corner, there is a yellow spiral-bound notepad, a yellow pencil with a pink eraser, and a grey ballpoint pen. The entire scene is set against a light grey, textured background.

6

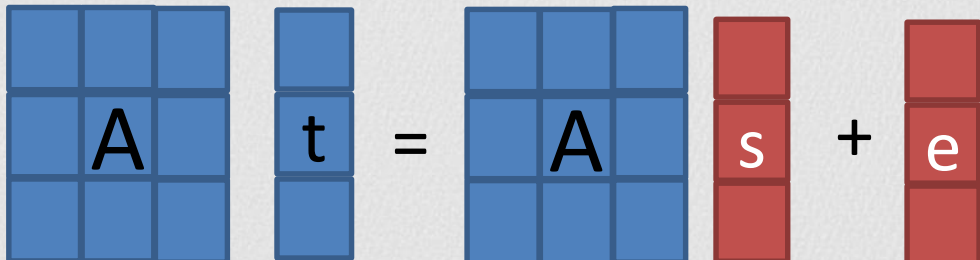
격자 기반 디지털 사인

Digital Signature Overview




Algebraic LWE 기반 Signature

P_k


$$\begin{bmatrix} & & \\ & A & \\ & & \end{bmatrix} \begin{bmatrix} \\ t \\ \end{bmatrix} = \begin{bmatrix} & & \\ & A & \\ & & \end{bmatrix} \begin{bmatrix} \\ s \\ \end{bmatrix} + \begin{bmatrix} \\ e \\ \end{bmatrix} \pmod{q}$$

S_k


$$\begin{bmatrix} \\ s \\ \end{bmatrix} \quad \begin{bmatrix} \\ e \\ \end{bmatrix}$$

Algebraic LWE 기반 Signature

$$\text{Sign}(m) = \begin{bmatrix} c \\ z \end{bmatrix}$$

$$\begin{bmatrix} c \end{bmatrix} = \text{Hash} \left(\text{MSB} \left(\begin{bmatrix} \begin{bmatrix} \square & \square & \square \\ \square & A & \square \\ \square & \square & \square \end{bmatrix} & \begin{bmatrix} \square \\ y \\ \square \end{bmatrix} \right) \parallel m \right)$$

$$\begin{bmatrix} \square \\ z \\ \square \end{bmatrix} = \begin{bmatrix} \square \\ y \\ \square \end{bmatrix} + \begin{bmatrix} \square \\ c \\ \square \end{bmatrix} \begin{bmatrix} \square \\ s \\ \square \end{bmatrix}$$

Algebraic LWE 기반 Signature

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

$$\mathbf{c} = \text{Hash} \left(\text{MSB} \left(\begin{bmatrix} \square & \square & \square \\ \square & \mathbf{A} & \square \\ \square & \square & \square \end{bmatrix} \begin{bmatrix} \square \\ \mathbf{z} \\ \square \end{bmatrix} - \begin{bmatrix} \square \\ \mathbf{c} \\ \square \end{bmatrix} \begin{bmatrix} \square \\ \mathbf{t} \\ \square \end{bmatrix} \right) \begin{bmatrix} \square \\ m \\ \square \end{bmatrix} \right)$$

Algebraic LWE 기반 Signature

$$\text{MSB} \left(\begin{bmatrix} \square & \square & \square \\ \square & A & \square \\ \square & \square & \square \end{bmatrix} \begin{bmatrix} \square \\ z \\ \square \end{bmatrix} - \begin{bmatrix} \square \\ c \end{bmatrix} \begin{bmatrix} \square \\ t \\ \square \end{bmatrix} \right)$$

$$= \text{MSB} \left(\begin{bmatrix} \square & \square & \square \\ \square & A & \square \\ \square & \square & \square \end{bmatrix} \left(\begin{bmatrix} \square \\ y \\ \square \end{bmatrix} + \begin{bmatrix} \square \\ c \end{bmatrix} \begin{bmatrix} \square \\ s \\ \square \end{bmatrix} \right) - \begin{bmatrix} \square \\ c \end{bmatrix} \left(\begin{bmatrix} \square & \square & \square \\ \square & A & \square \\ \square & \square & \square \end{bmatrix} \begin{bmatrix} \square \\ s \\ \square \end{bmatrix} + \begin{bmatrix} \square \\ e \\ \square \end{bmatrix} \right) \right)$$

Algebraic LWE 기반 Signature

$$\text{MSB} \left[\begin{array}{c} \begin{array}{|c|c|c|} \hline \square & \square & \square \\ \hline \square & A & \square \\ \hline \square & \square & \square \\ \hline \end{array} \left(\begin{array}{|c|} \hline y \\ \hline \end{array} + \begin{array}{|c|} \hline c \\ \hline \end{array} \begin{array}{|c|} \hline s \\ \hline \end{array} \right) - \begin{array}{|c|} \hline c \\ \hline \end{array} \left(\begin{array}{|c|c|c|} \hline \square & \square & \square \\ \hline \square & A & \square \\ \hline \square & \square & \square \\ \hline \end{array} \begin{array}{|c|} \hline s \\ \hline \end{array} + \begin{array}{|c|} \hline e \\ \hline \end{array} \right) \end{array} \right]$$

$$= \text{MSB} \left[\begin{array}{c} \begin{array}{|c|c|c|} \hline \square & \square & \square \\ \hline \square & A & \square \\ \hline \square & \square & \square \\ \hline \end{array} \begin{array}{|c|} \hline y \\ \hline \end{array} - \begin{array}{|c|} \hline c \\ \hline \end{array} \begin{array}{|c|} \hline e \\ \hline \end{array} \end{array} \right] = \text{MSB} \left[\begin{array}{c} \begin{array}{|c|c|c|} \hline \square & \square & \square \\ \hline \square & A & \square \\ \hline \square & \square & \square \\ \hline \end{array} \begin{array}{|c|} \hline y \\ \hline \end{array} \end{array} \right]$$

Algebraic LWE 기반 Signature

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

$$\mathbf{c} = \text{Hash} \left(\text{MSB} \left(\begin{bmatrix} \text{3x3 grid} \\ \text{A} \end{bmatrix} \mathbf{z} - \mathbf{c} \mathbf{t} \right) m \right)$$

$$= \text{Hash} \left(\text{MSB} \left(\begin{bmatrix} \text{3x3 grid} \\ \text{A} \end{bmatrix} \mathbf{y} \right) m \right)$$

NTRU 기반 Signature

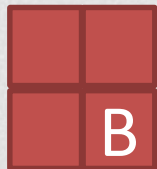
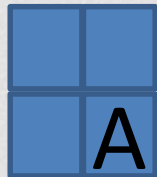
P_k



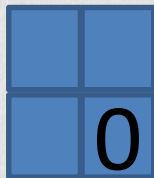
S_k



s.t



=



NTRU 기반 Signature

$Sign(m)$

$$\begin{bmatrix} \text{ } \\ c \end{bmatrix} = \begin{bmatrix} \text{ } & A^{-1} \\ A & \text{ } \end{bmatrix} \times \text{Hash} \left(\begin{bmatrix} m \end{bmatrix} \right)$$

$$\begin{bmatrix} \text{ } \\ v \end{bmatrix} = \text{CVP} \left(\begin{bmatrix} \text{ } \\ c \end{bmatrix}, \begin{bmatrix} \text{ } & \text{ } \\ \text{ } & B \end{bmatrix} \right)$$

$$Sign(m) = \begin{bmatrix} \text{ } \\ c \end{bmatrix} - \begin{bmatrix} \text{ } \\ v \end{bmatrix}$$

NTRU 기반 Signature

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

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

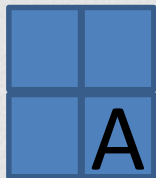
2) $\begin{bmatrix} \square & \square \\ \square & A \end{bmatrix} \times \begin{bmatrix} \square \\ s \end{bmatrix} = \text{Hash}\left(\begin{bmatrix} m \end{bmatrix}\right)$

NTRU 기반 Signature

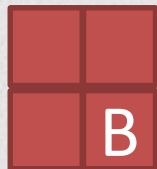
$$\begin{aligned} & \begin{bmatrix} & \\ & \\ & \\ A & \end{bmatrix} \times \left(\begin{bmatrix} \\ c \\ \end{bmatrix} - \begin{bmatrix} \\ v \\ \end{bmatrix} \right) \\ &= \text{Hash} \left(\begin{bmatrix} m \\ \end{bmatrix} \right) - \begin{bmatrix} & \\ & \\ & \\ A & \end{bmatrix} \times \begin{bmatrix} \\ v \\ \end{bmatrix} \\ &= \text{Hash} \left(\begin{bmatrix} m \\ \end{bmatrix} \right) \begin{bmatrix} \\ v \\ \end{bmatrix} = \text{CVP} \left(\begin{bmatrix} \\ c \\ \end{bmatrix}, \begin{bmatrix} & \\ & \\ & \\ B & \end{bmatrix} \right) \end{aligned}$$

NTRU 기반 Signature

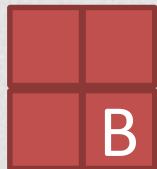
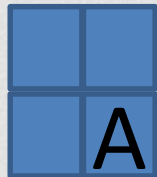
P_k



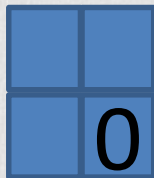
S_k



s.t



=



NTRU 문제

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

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

Recover g and f

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

NTRU 기반 Signature

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

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

$$\begin{bmatrix} F & g \end{bmatrix} + \begin{bmatrix} G & f \end{bmatrix} = q \Leftarrow \text{Ring } \div$$

$$\Leftrightarrow \begin{bmatrix} F \end{bmatrix} \frac{\begin{bmatrix} g \end{bmatrix}}{\begin{bmatrix} f \end{bmatrix}} + \begin{bmatrix} G \end{bmatrix} \frac{\begin{bmatrix} f \end{bmatrix}}{\begin{bmatrix} f \end{bmatrix}} = \begin{bmatrix} 0 \end{bmatrix} \pmod{q}$$

NTRU 기반 Signature

$$\begin{bmatrix} F \end{bmatrix} \frac{\begin{bmatrix} g \end{bmatrix}}{\begin{bmatrix} f \end{bmatrix}} + \begin{bmatrix} G \end{bmatrix} \frac{\begin{bmatrix} f \end{bmatrix}}{\begin{bmatrix} f \end{bmatrix}} = \begin{bmatrix} 0 \end{bmatrix} \pmod{q}$$

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

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

NTRU 기반 Signature

$$\text{CVP} \left(\begin{array}{|c|} \hline \text{blue box} \\ \hline \text{c} \\ \hline \end{array} \quad \begin{array}{|c|c|} \hline \text{red box} & \text{red box} \\ \hline \text{red box} & \text{B} \\ \hline \end{array} \right) =$$

$$\begin{array}{|c|} \hline \text{blue box} \\ \hline \text{c} \\ \hline \end{array} = \begin{array}{|c|c|} \hline \text{red box} & \text{red box} \\ \hline \text{red box} & \text{B} \\ \hline \end{array} \begin{array}{|c|} \hline \text{green box} \\ \hline \text{t} \\ \hline \end{array}$$

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

$$\begin{array}{|c|} \hline \text{blue box} \\ \hline \text{c} \\ \hline \end{array} - \begin{array}{|c|c|} \hline \text{red box} & \text{red box} \\ \hline \text{red box} & \text{B} \\ \hline \end{array} \begin{array}{|c|} \hline \text{green box} \\ \hline \text{t}^* \\ \hline \end{array}$$

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