

# ● 논문 의미

automorphism 으로 plain text 도 생성,  
canonical & Norm 생김, see A.9 appendix

=> AES 를 동형암호화 하였고 그 과정 사용된 테크닉들 소개

↳ 이는 BGV 성능을 대폭 향상

Automorphism, 갈루아군

↳ 자기자신으로 가는 사상 (행동, 공약) 들의 집합

ex)  $f(x) = (x^2 - 2)(x^2 - 3)$   $\begin{pmatrix} \sqrt{2} & \times & = & \times & = \\ -\sqrt{2} & \times & = & = & \end{pmatrix}$  => 4개다.

↳ 6개의 automorphism 으로 평문 아크공을 성질 가지게 된다

$x_1$   $\begin{bmatrix} m_1 & m_2 & m_3 & m_4 \end{bmatrix}$

↓

$x_2$   $\begin{bmatrix} m_2 & m_3 & m_4 & m_1 \end{bmatrix}$

) =>

여러번의 암호

AES Shift 연산 바를

"  
 $x_3$   $\begin{bmatrix} m_1 & m_2 & . & . \\ m_2 & m_3 & . & . \end{bmatrix}$

\* 가결은 Cypher text 에 관심있을지라도 그런 바 도 신경쓰지

마리 좋은 성질 만들어 준다 (very cool technique)

$$\Phi(x) = \prod_{i \in (\mathbb{Z}/m\mathbb{Z})^*} (x - z^i)$$

$F_z = F_1 \times F_2 \times F_3 \times F_4$  인데  $\Rightarrow$  공간을 나누서 번갈아가며 효율적으로 쓸수있다.

$$\Phi_m = F \text{ 라고 하면 } \subseteq F_1 = (x - z^1) \quad F_2 = (x - z^2) \dots$$

성질을 만족하면 좋은데 이는 특정한 값들이 있는것이다

$$(m = 0, 0 = \bigcirc) = m = 0 \text{ 인 경우 전체 계수 10이고 } + 0 \text{ 이다.}$$

Curriculum embedded Norm은

식에  $(z^1, z^2, z^3, z^4, \dots)$  를 대입해서

이들 벡터들 가장 큰 값을 의미하고 이는 noise 특성하는데  
비슷하다,

$$\prod_{i=1}^2 \mathbb{Z}[x] / f_i \cong \mathbb{Z}[x] / \Phi_m(x) \rightarrow \mathbb{Z}[x] / \Phi_n(x) = A_d$$

(각본 것들 decomposition 한다) next space cirt space

Contribution (Plane 공간도 polynomial (Lattice) 을 위한 norm 설정)

poly 는  $E(a(x) + b(x))$ ,  $E(a(x) \times b(x))$  해석이 가능  
우리가 정말 원하는 것은 아니다.

$$\text{2244-1} \quad \mathbb{Z}_m(x) = \prod_{i=1}^l f_i(\text{mod } p) \text{ 을 공간으로 } \mathbb{Z} / \mathbb{Z}_m(x)$$

2244-1 Vector를 생각.

$$\therefore A = (a_1(x), a_2(x), \dots, a_n(x))$$

↖ slot      ↗ slot      ↘ slot

$$B = (b_1(x), b_2(x), \dots, b_n(x))$$

$$\text{2244-2} \quad A+B \rightarrow a(x) + b(x) \rightarrow c_1(x) + c_2(x)$$

$$A \otimes B \rightarrow a(x) \times b(x) \rightarrow \text{mul}(c_1(x) \times c_2(x))$$

(불가능했던 plane에서 연산이 유효해졌고, 1차원 공간 잘 사용)

$$G_{x^t} \in A_q \quad (\mathbb{Z}_q[x] / \Phi_n(x))$$

$$\mathbb{Z}_q[x] / \Phi_n(x) \simeq \prod_{i \in \mathbb{Z}_m^*} \mathbb{Z}_q[x] / (x - z^i) = \mathbb{Z}_q[x] / (x - z) \times \mathbb{Z}_q[x] / (x - z^2) \dots$$

$$f \longmapsto (f \bmod (x - z^1), f \bmod (x - z^2), \dots)$$

$$\downarrow \qquad \qquad \downarrow$$

$$f(z^1), \qquad f(z^2),$$

polynomial 을 그래프로 보는데 아티라 특별한 점들에서  
evaluation 하는데 ( $q \equiv 1 \pmod{m}$  되면  $z \in \mathbb{Z}_q$  에 들어감 )  
↳ 특별한 성질

저런 성질 쓰면  $z \in \mathbb{Z}_q$  라서 예쁘게 됨,

degree 낮음  
(CRT, FFT)

$$(q = \prod_{i=1}^t p_i)$$

$$\mathbb{Z}_q \simeq \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \dots \times \mathbb{Z}_{p_t} \quad (\mathbb{Z}_q \text{ 을 작게 함})$$

$$a \longmapsto (a)_{p_1}, (a)_{p_2}, \dots$$

⇒ 2개 방법 (FFT, CRT) ⇒ Double CRT가 됨.

덧셈, 곱셈 가능

$$\therefore \mathbb{Z}_q[x] / \Phi_n(x) \simeq \prod_{i \in \mathbb{Z}_m^*} \prod_{j=1}^L \mathbb{Z}_{p_i}^{(j)} / (x - z^i)$$

(왜 3?)  
⇒ 조각고 / 작도 ↓  
(왜  $p_i = 1009$ ,  $3 \in \mathbb{Z}_{p_i}$ )

$$[f(z^1)]_{p_1} \quad [f(z^1)]_{p_2} \quad [f(z^1)]_{p_3} \quad \dots$$

$$[f(z^2)]_{p_1}$$

$$[f(z^3)]_{p_1}$$

⋮

⇒ 이렇게 저장

문제를  $(p_1, p_2, \dots, p_k)$  를 mod 해야 했는데!

$p_1, p_2, p_3, \dots$  각각 곱셈으로 해서 계산 빨라진다.

$$O(n^2) \rightarrow O(n)$$



→



⇒

대부분 빨라짐.

# Modulus Switching

$$q_L = \prod_{i=0}^j p_i, \quad q_{L-1} = \prod_{i=0}^{j-1} p_i \Rightarrow \frac{q_{L-1}}{q_L} = p_L$$

$$c_0 + c_1 \cdot s = m + \underbrace{2e}_{\rightarrow \text{크기만 증가}} \pmod{q_L}$$

$\rightarrow$  계수도 줄어든다.

$$\frac{1}{p_L} (c_0 + c_1 s) = m + \frac{2e}{p_L} \pmod{q_{L-1}}$$

$\rightarrow$  scale 이라는 상수로 m은 건드리 않는다  $\Rightarrow + B_{\text{scale}}$   
보정값이 붙음

## Key Switching

$$c_0 + c_1 s = m + 2e [q]$$

$$c_0' + c_1' s = m' + 2e' [q]$$

다항식

$\uparrow$

$$c_0 c_0' + s(c_1 c_1' + c_1 c_0') + s^2(c_1 c_1') = m m' + 2\tilde{e} [q]$$

$\rightarrow$  해가 생겨서 문제

$$Des = x(1-s) \text{ 한다.}$$

$$d_0 + d_1 s + d_2 s^2 = m m' + 2\tilde{e} \approx \underbrace{\tilde{c}_0}_{\downarrow d_0 + D} + \underbrace{\tilde{c}_1 s}_{\downarrow d_1 + D} \pmod{q}$$

$\rightarrow$  해를 구하고 싶다

\* 2차항(2차)에 한  $d_2 s^2 \approx D + Ds$  이나  $D$  값으로  
linearization (key switching)

$$\underline{d_2 s^2} \approx 12 + 12s$$

↳  $mss$ 로 생각해서  $s$ 로 Enc 한다 생각한다.

$$\frac{d_2 s^2 + 2e + as - as}{\downarrow}$$

$$b - as$$

)  $s^2$ 을 공개  $s$ 로 암호화

$$(m + 2e + as, a)$$

↓  $d_2 s^2 \rightarrow$  해시리크 보이기 때문

$$(b + 2e + as, a)$$

↓

$$b - as \quad (b, a \in \text{evaluation key, relinearization key})$$

$$d_2 \frac{(s^2 + 2e + as - as)}{b} \quad a \leftarrow A_4$$

$b$

$$\therefore d_2 b - d_2 as$$

$$\rightarrow d_0 + d_1 s + d_2 s^2 = C_0 1 + C_1 s \pmod{q}$$

Var 1

$$\downarrow$$

$$d_0 + d_2 b$$

$$\downarrow$$

$$d_1 - d_2 a$$

( 공개준다 ) ( binary로 )

Var 2

$$d_3 s^2 = \sum_{i=0}^n d_i 2^i s^2 \approx \sum_{i=0}^n d_i \frac{(2^i s^2 + 2e_i + a_i s - a_i s)}{(b, a_i)}$$

Var 3 (이번 논문)

$$d_2 s^2 \approx 12 + 12.5 \pmod{q}$$

→ 쿼리

$$P d_2 s^2 = d_2 (P_2 s^2) = \pmod{Pq}$$

$$\approx d_2 \cdot \frac{(P_2 s^2 + as + 2e - as)}{(b, a)} \pmod{Pq}$$

$$\text{Mod Switch} \left[ \begin{array}{l} (d_2 b, b_2 a) \pmod{Pq} \\ \rightarrow (\text{Scale}) \pmod{q} \end{array} \right.$$

⇓

그냥 자체를 P로 분리고

error 살펴보고

다시 P로 내림