

Simple and More Efficient PRFs with Tight Security from LWE and Matrix-DDH

Coding & Communication Research Lab.



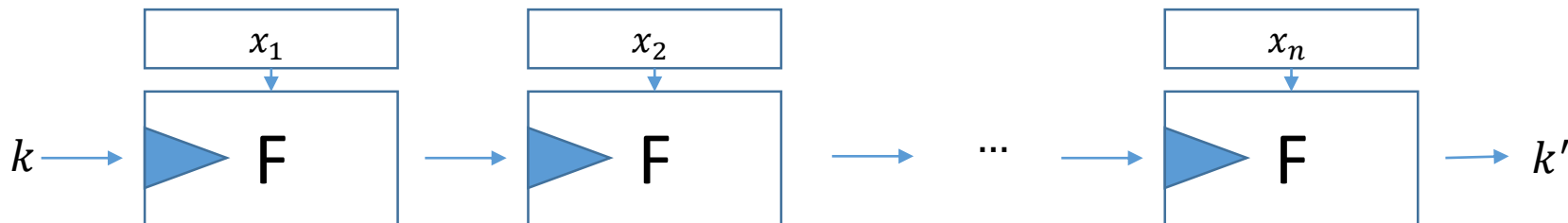
HANYANG UNIVERSITY

한양대학교 Coding & Communication Research Lab.
발표자: 이승환

- Abstract
 - PPT 전반에 대한 내용 설명
- 1. All prefix - Almost Universal Hash functionPseudorandom Functions
- 2. Perfectly One-time secure
- 3. Efficient Construction Technique
- 4. Matrix-DDH based Pseudorandom Function (Skip)
- 5. Decisional-LWE based Pseudorandom Function
- 6. Applying to Lattice based PRF

- [BMR10] augmented cascade PRF에 대하여 Q-parallel security 개념을 도입하여 효율을 향상시켰다.

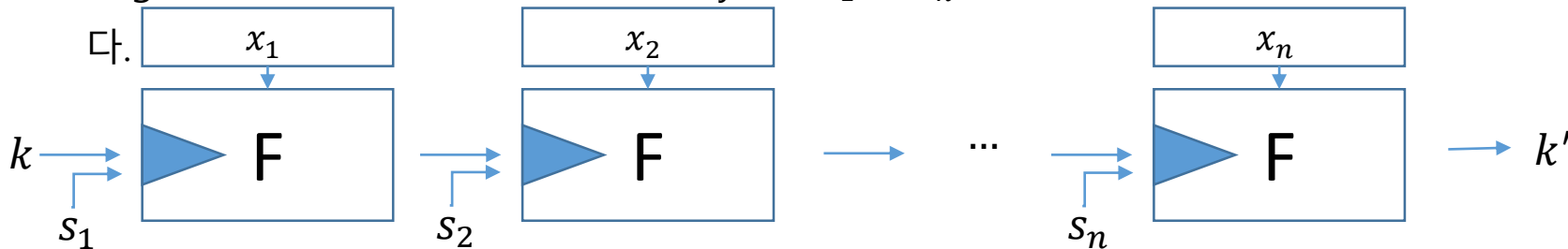
- Cascade construction, key = (k) . PRF F 에 대해 F^{*n} 은 다음과 같다



- q 개의 query로 F^{*n} 을 깨는 \mathcal{A} 와 F 을 깨는 \mathcal{B} 와의 관계는 다음과 같다 [BCK96b]

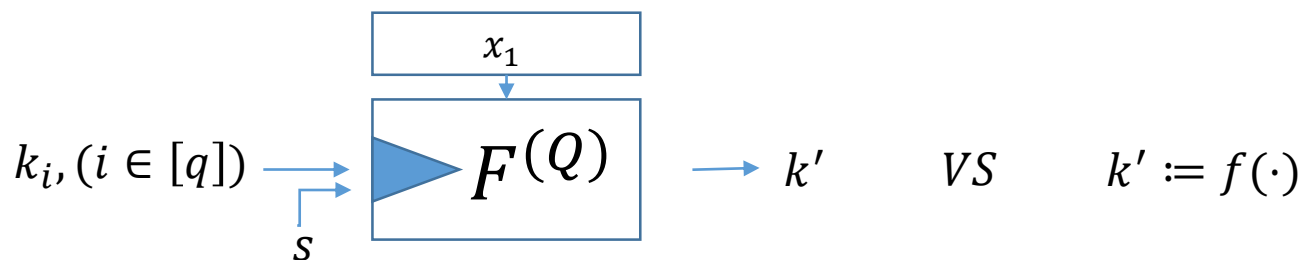
$$\square PRF_{adv}[\mathcal{A}, F^{*n}] \leq nq \cdot PRF_{adv}[\mathcal{B}, F]$$

- Augmented Cascade construction, key = (k, s_1, \dots, s_n) , PRF F 에 대해 F^{*n} 은 다음과 같다.



- [BMR10] augmented cascade PRF에 대하여 Q -parallel security 개념을 도입하여 효율을 향상시켰다.

- PRF를 쓰더라도 모든 augmented cascade construction이 secure 하진 않다.
- Q - parallel security를 만족시키는 PRF F 만을 사용한다면 secure 하다. (sufficient)
 - $(s, k_1, x), (s, k_2, x), \dots, (s, k_q, x)$ 쿼리에 대해 PRF F 가 Random function $f(\cdot)$ 와 indistinguishable 하다면, Q - parallel security 라고 하고 이러한 함수를 $F^{(Q)}(\cdot)$ 로 쓰자.



- Q 개의 query로 F^{*n} 을 깨는 \mathcal{A} 와 $F^{(q)}$ 을 깨는 \mathcal{B} 와의 관계는 다음과 같다.
- $$PRF_{adv}[\mathcal{A}, F^{*n}] \leq n \cdot PRF_{adv}[\mathcal{B}, F^{(Q)}]$$

▪ [JKP19] 본 논문에서는

- 1. Q – parallel security 대신 **One Time Security PRF**에 대해 정의하고,
- 2. **All prefix almost universal** hash 함수 $\mathcal{H}_{n,m}$ 을 정의하고 사용한다면, 더 Tight security를 만들 수 있음을 증명했다.

$$\square [\text{BMR10}] \text{PRF}_{adv}[\mathcal{A}, F^{*n}] \leq \mathbf{n} \cdot \text{PRF}_{adv}[\mathcal{B}, F^{(Q)}]$$

$$\square [\text{JKP19}] \text{PRF}_{adv}[\mathcal{A}, \hat{F}^{\mathcal{H}_{n,m}}] \leq \mathbf{2} \cdot \text{PRF}_{adv}[\mathcal{B}, \hat{F}^j], \quad j = O(\log \lambda), \quad m = w(\log \lambda)$$

- 본 논문은 다음과 같은 의의를 갖는다.
 - Key로 사용되는 s_1, \dots, s_n 이 **n의 super logarithm** 개수로 바뀌었다.
 - Security loss는 input n과 관계없이 **Constant**에 가깝도록 효율을 증대 시켰다.

Abstract

- All prefix almost universal hash function $\mathcal{H}_{n,m}$ 를 실제로 적용했을 때,
- 두개의 Augment Cascaded PRF에 대한 Security효율을 향상시켰다.

Assumption	Paper	Pseudorandom Function	Time Analysis / Advantage Analysis	Improvement
Matrix Diffie Hellman	[EHK+17]	$\left[\left(\prod_{i:x_i=1}^m \mathbf{T}_i \right) \cdot \mathbf{h} \right]$	$t_{\mathfrak{B}} = \Theta(t_{\mathcal{A}}), \epsilon_{\mathfrak{B}} \geq \frac{\epsilon_{\mathcal{A}}}{dm}$	$t_{\mathfrak{B}'} = \Theta(t_{\mathcal{A}}), \epsilon_{\mathfrak{B}'} \geq \frac{\epsilon_{\mathcal{A}}}{2dj},$ $j = O(\log \lambda)$
Learning With Error	[BPR12]	$\left[\left(\prod_{i:x_i=1}^m \mathbf{s}_i \right) \cdot \mathbf{h} \right]_q$	$t_{\mathfrak{B}} = \Theta(t_{\mathcal{A}}), \epsilon_{\mathfrak{B}} \geq \frac{\epsilon_{\mathcal{A}}}{m \cdot N}$	$t_{\mathfrak{B}'} = \Theta(t_{\mathcal{A}}), \epsilon_{\mathfrak{B}'} \geq \frac{\epsilon_{\mathcal{A}}}{2j \cdot N} - 2^{\Omega(N)}$ $, j = O(\log \lambda)$

1. All prefix - Almost Universal Hash function

▪ Universal hash function의 정의 [CW79]

- 모든 페어 (x, x') 에 대해 collision이 일어날 확률은 2^{-m} 보다 작다.

Definition 2 ([CW79]). A family \mathcal{H} of hash functions mapping finite set $\{0, 1\}^n$ to finite set $\{0, 1\}^m$ is universal, if for all $x, x' \in \{0, 1\}^n$ with $x \neq x'$ holds that

$$\Pr_{h \xleftarrow{\$} \mathcal{H}} [h(x) = h(x')] \leq 2^{-m}.$$

▪ Almost Universal hash function의 정의

- 모든 페어 (x, x') 에 대해 collision이 일어날 확률은 2^{-m+1} 보다 작다.

Definition 3. A family \mathcal{H} of hash functions mapping finite set $\{0, 1\}^n$ to finite set $\{0, 1\}^m$ is almost-universal, if for all $x, x' \in \{0, 1\}^n$ with $x \neq x'$ holds that

$$\Pr_{h \xleftarrow{\$} \mathcal{H}} [h(x) = h(x')] \leq 2^{-m+1}.$$

1. All prefix - Almost Universal Hash function

■ Almost Universal hash function First Construction [DHKP97]

- $m, n \in \mathbb{N}, m \leq n$
- $\mathcal{H}_{n,m} := \{h_a : a \in \llbracket 2^n - 1 \rrbracket, a \text{ is odd}\}$ be the family of hash functions, $|\mathcal{H}_{n,m}| = 2^{n-1}$
- For $x \in \mathbb{Z}_{2^n}$, $h_a(x) := (ax \bmod 2^n) \operatorname{div} 2^{n-m}$

□ (참조) div 연산은 $(ax \bmod 2^n)$ 이후의 결과에 대해 m 개의 MSB만을 취한다.

(m bit)

(n-m bit)



1. All prefix - Almost Universal Hash function

▪ $h_a(x) := (ax \bmod 2^n) \div 2^{n-m}$ 는 $\Pr_{h \leftarrow \mathcal{H}} [h(x) = h(x')] \leq 2^{m-1}$ 증명

- 증명 방식: 어떠한 pair (x, x') 를 주더라도 $h(x) = h(x')$ 을 만족하는 a 의 개수가 2^{n-m} 보다 작음을 보이자.
- Proof : 주어진 pair (x, x') 대해 $h(x) = h(x')$ 를 만족한다면, m 개의 MSB가 같다. 즉
- $|(ax \bmod 2^n) - (ax' \bmod 2^n)| < 2^{n-m} \quad \dots (1)$
- 이때 $x > x'$ 로 순서를 잡고, $z = x - x'$ 로 놓는다면, (1)을 만족하는 z 는 다음을 만족한다.
 - $az \bmod 2^n \in \{1, 2, \dots, 2^{n-m} - 1\} \cup \{2^n - 2^{n-m} + 1, \dots, 2^n\} \dots (2)$ (최악의 경우 $2 * 2^{n-m}$ 개)
 - $z = z'2^s$ 을 만족하는 홀수 z' 과 $0 \leq s < n$ 인 s 를 생각하자.
 - 홀수 $a < 2^n$ 과 2^n 은 Relative Prime이므로 a 는 Multiplicative Group을 형성한다.
 - (2)를 만족하는 $az'2^s \bmod 2^n$ a 의 객수를 찾는 문제와 $a' = az'$ 에 대해 (2)를 만족하는 $a'2^s \bmod 2^n$ 의 a' 의 객수를 찾는 것과 같다.
- $a'2^s \bmod 2^n \in \{1, 2, \dots, 2^{n-m} - 1\} \cup \{2^n - 2^{n-m} + 1, \dots, 2^n\}$ 에 대해서
 $s = 0$ 이면 2^{n-m} 개, $s \neq 0$ 이면 $2^{n-m} - 1$ 개가 된다.

1. All prefix - Almost Universal Hash function

- All prefix Universal Hash function

Definition 4. Let \mathcal{H} be a family of hash functions mapping $\{0, 1\}^n$ to $\{0, 1\}^m$. We say that \mathcal{H} is a family of all-prefix universal hash functions, if for all $x, x' \in \{0, 1\}^n$ with $x \neq x'$ and all $w \in \llbracket m \rrbracket$ holds that

$$\Pr_{h \xleftarrow{\$} \mathcal{H}} [h(x)_{1:w} = h(x')_{1:w}] \leq 2^{-w}.$$

- All-prefix almost-universal hash functions (APUHF)

Definition 5. Let \mathcal{H} be a family of hash functions mapping $\{0, 1\}^n$ to $\{0, 1\}^m$. We say that \mathcal{H} is a family of all-prefix almost-universal hash functions (APUHF), if for all $x, x' \in \{0, 1\}^n$ with $x \neq x'$ and all

$$\Pr_{h \xleftarrow{\$} \mathcal{H}} [h(x)_{1:w} = h(x')_{1:w}] \leq 2^{-w+1}.$$

- 앞선 Construction은 All-prefix 성질도 만족한다.[JKP19]

1. All prefix - Almost Universal Hash function

▪ All-prefix Universal Hash function은 가능한가?

- 가능하다[JKP19]! 다음과 같은 추가적인 **pairwise independent** Definition을 보자.

Definition 6. Let \mathcal{H} be a family of hash functions with domain $\{0, 1\}^n$ and range $\{0, 1\}^m$. We say that \mathcal{H} is pairwise independent, if for all $x, x' \in \{0, 1\}^n$ with $x \neq x'$ and all $y, z \in \{0, 1\}^m$ holds that

$$\Pr_{h \xleftarrow{\$} \mathcal{H}} [h(x) = y \wedge h(x') = z] = 2^{-2m}.$$

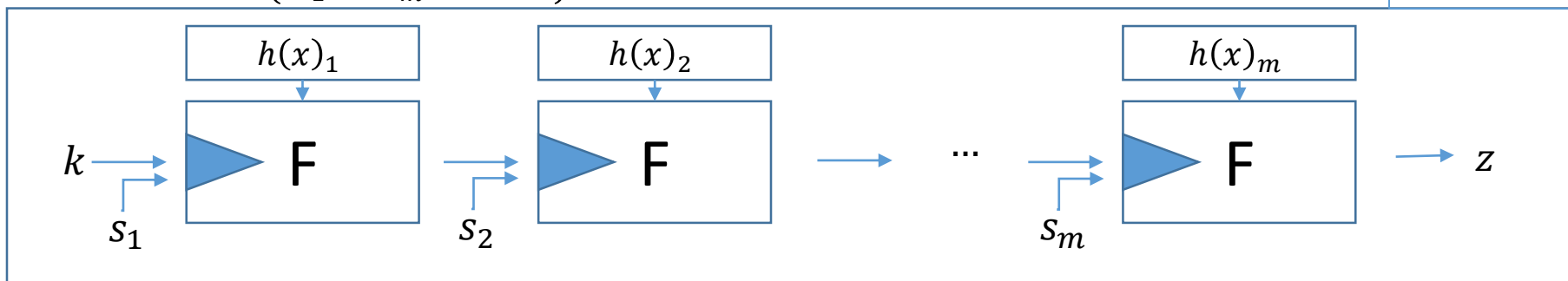
- pairwise independent 하면 All-prefix Universal Hash function이다 [JKP19]
 - $\mathcal{H}_n := \{h_{a,b} : a, b \in \{0, 1\}^n\}$, $h_{a,b} : GF(2^n) \rightarrow GF(2^n); x \mapsto ax + b$
 - 이때 arithmetic operation은 $GF(2^n)$ 에서 정의됨
 - 실제로 이 논문에서는 크게 중요하지 않는다. (APUHFs 만으로 충분하다.)

2. Perfectly One-time secure

▪ Augmented Cascade 구조에 대한 고찰

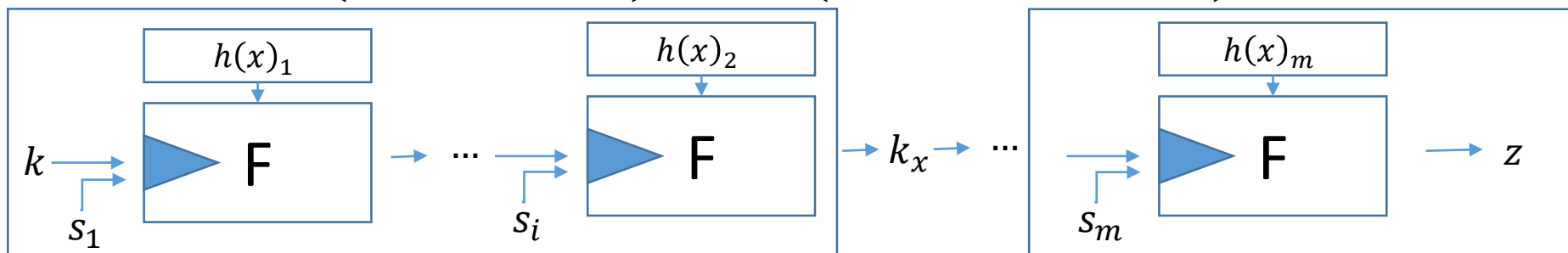
$$\bullet z = \hat{F}^m((s_1, \dots, s_m), k, h(x))$$

$$\hat{F}^m(\cdot)$$



▪ 다음과 같이 나누어 생각할 수 있다.

$$\bullet k_x := \hat{F}^i((s_1, \dots, s_i), k, h(x)_{1:i}), \quad z = \hat{F}^{m-i}((s_{i+1}, \dots, s_m), k_x, h(x)_{i+1:m})$$



2. Perfectly One-time secure

- [Definition 9, JKP19] $F: S \times K \times \{0,1\}^m \rightarrow K$ 에 대해 다음을 만족하면 Perfectly One-time secure 라고 하자.

$$\Pr_{\substack{\$ \\ k \leftarrow K}} [F(s, k, x) = k'] = \frac{1}{|K|} \text{ for all } (s, x, k') \in S \times \{0,1\}^m \times K$$

- [Lemma 5, JKP19] F 가 perfectly One-time secure 하면 \hat{F}^m 역시 다음을 만족한다. (One-time secure 하다)

$$\Pr_{\substack{\$ \\ k \leftarrow K}} [\hat{F}^m(s_1, \dots, s_m, k, x) = k'] = \frac{1}{|K|} \text{ for all } (s_1, \dots, s_m, x, k') \in S^m \times \{0,1\}^m \times K$$

- 증명 sketch: 이전 슬라이드 처럼 \hat{F}^m 을 m 개의 F 로 나누면, F 의 output은 Uniform이기 때문에 \hat{F}^m 역시 Output은 Uniform 하게 나온다.

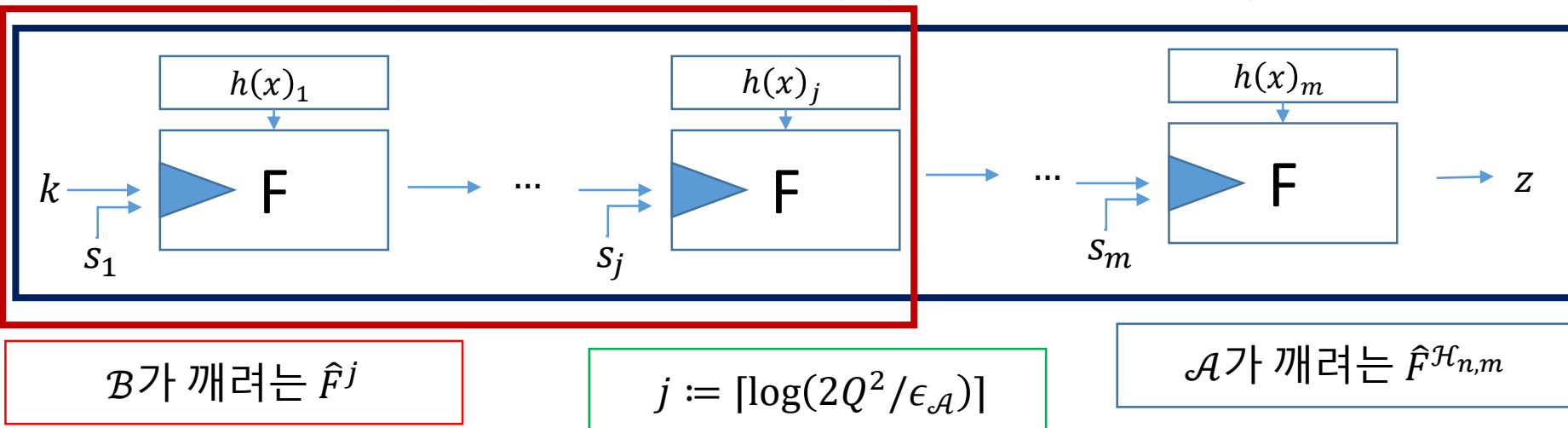
3. Efficient Construction Technique

▪ [Theorem 4, JKP19, 메인 결과]

Theorem 4. Let $m = \omega(\log \lambda)$ be (slightly) super-logarithmic, $\mathcal{H}_{n,m}$ be a family of all-prefix almost universal hash functions and F be perfectly one-time secure.

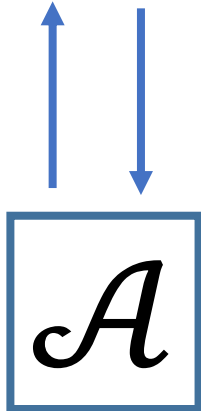
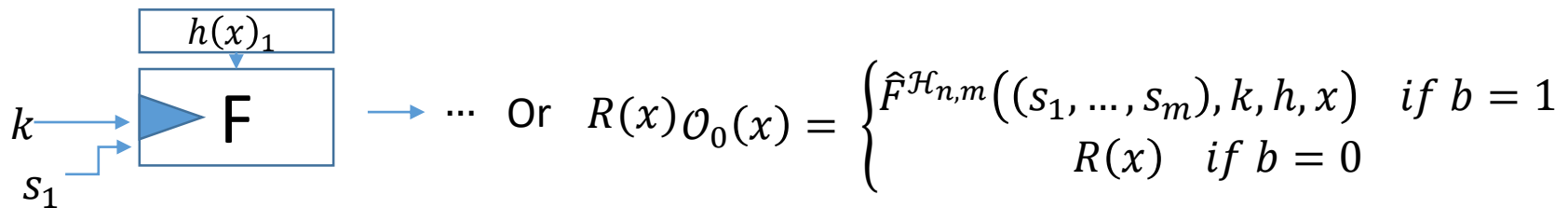
From each adversary \mathcal{A} that $(t_{\mathcal{A}}, \epsilon_{\mathcal{A}}, Q)$ -breaks the pseudorandomness of $\hat{F}^{\mathcal{H}_{n,m}}$ with $Q/\epsilon_{\mathcal{A}} = \text{poly}(\lambda)$ for some polynomial poly , we can construct an adversary \mathcal{B} that $(t_{\mathcal{B}}, \epsilon_{\mathcal{B}}, Q)$ -breaks the pseudorandomness of \hat{F}^j , where

$$j = O(\log \lambda) \quad \text{and} \quad t_{\mathcal{B}} = \Theta(t_{\mathcal{A}}) \quad \text{and} \quad \epsilon_{\mathcal{B}} \geq \epsilon_{\mathcal{A}}/2$$



3. Efficient Construction Technique

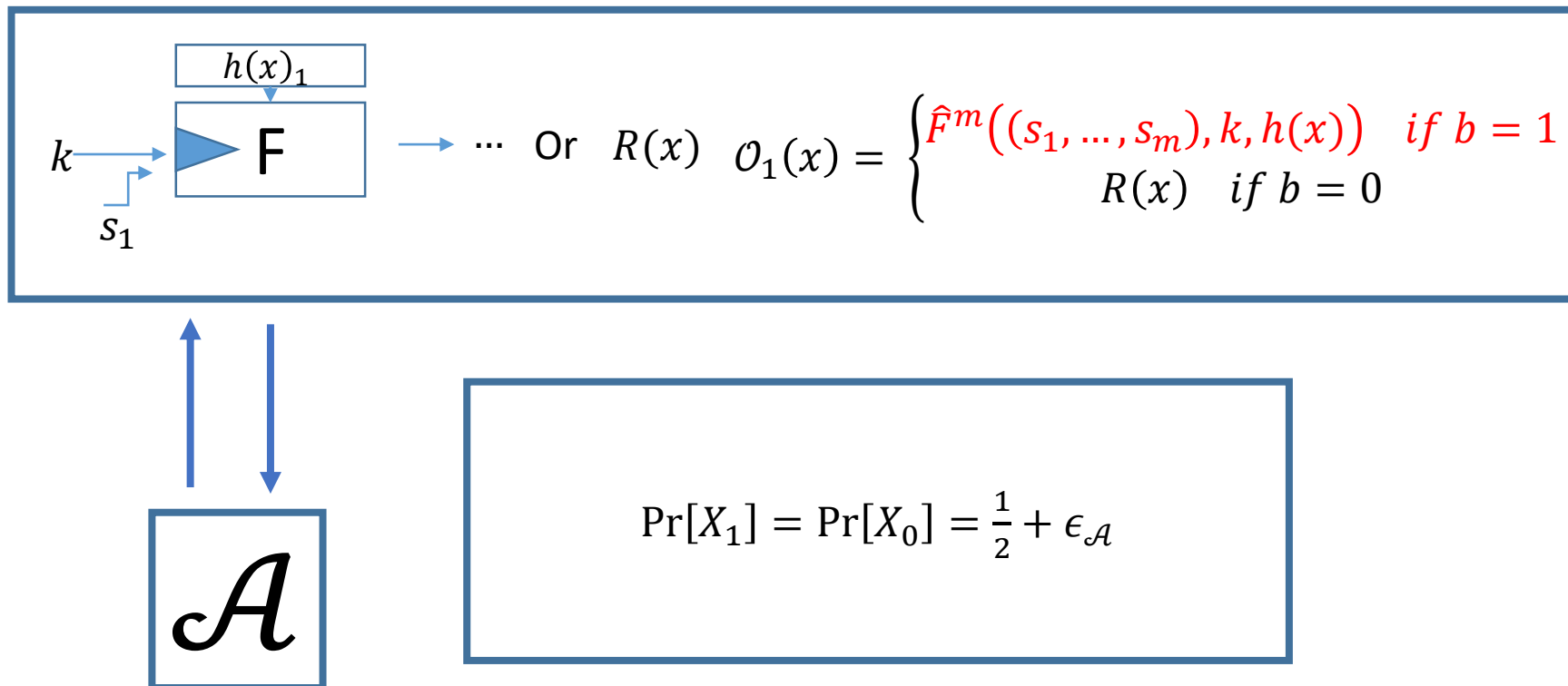
- Proof. 다음과 같은 Game 들로 증명하자.
- (Game0) Random function과 $\hat{F}^{\mathcal{H}_{n,m}}$ 를 구분하는 게임



$$\Pr[X_0] = \Pr[Exp_{\mathcal{A},F}^{PRF}(\lambda) = 1] = \Pr[Exp_{\mathcal{A}}^{PRF}(\lambda) = 1 | b = 1] \geq \frac{1}{2} + \epsilon_{\mathcal{A}}$$

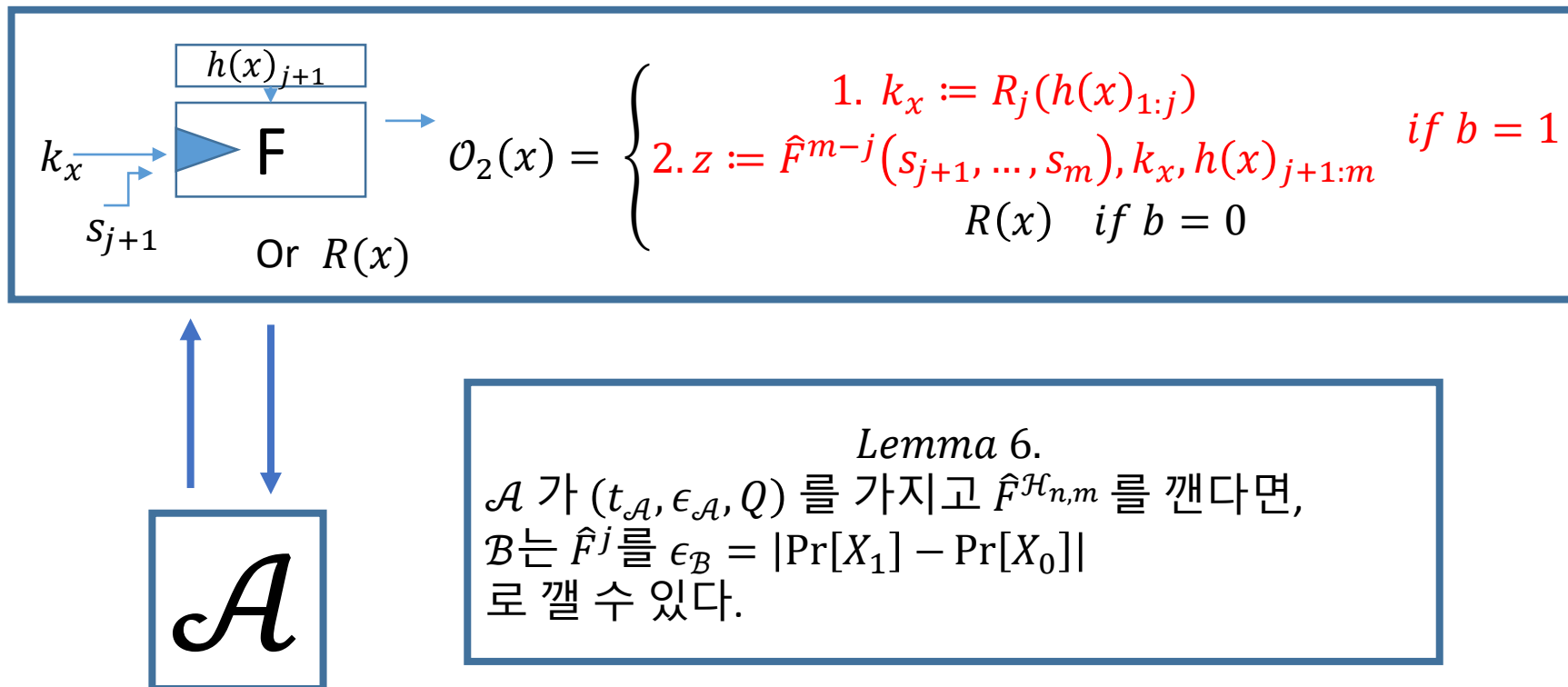
3. Efficient Construction Technique

- (Game1) Game0와 같지만, $\hat{F}^{\mathcal{H}_{n,m}}$ 를 APUFs로 encoding 된 \hat{F}^m 을 구분하는 게임



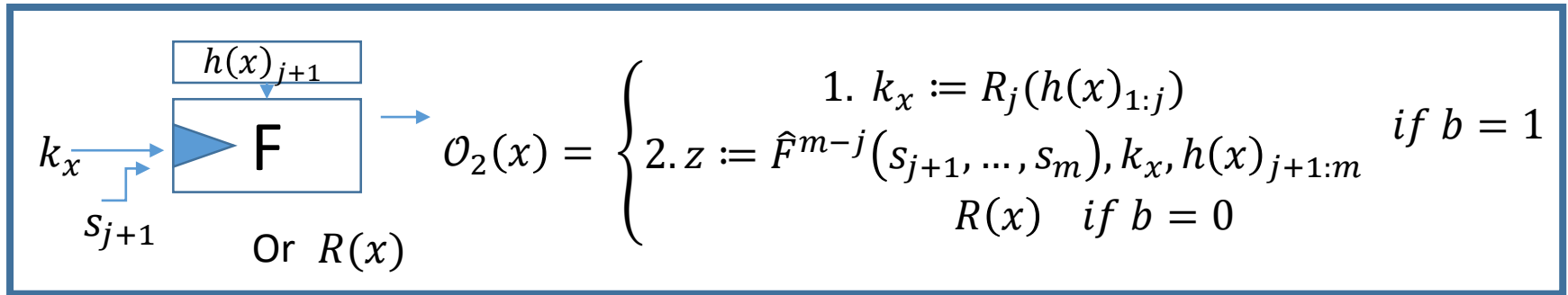
3. Efficient Construction Technique

- (Game2) Game1과 같지만, $j \leq m$ 번째까지는 Random function으로 바꾼다.



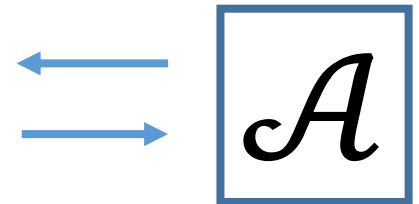
3. Efficient Construction Technique

▪ Lemma.6 Proof



$$\mathcal{B} \leftarrow \begin{cases} 1. k_x \leftarrow O_2(x) \\ 2. z := \hat{F}^{m-j}(s_{j+1}, \dots, s_m), k_x, h(x)_{j+1:m} \end{cases} \text{ if } b' = 1$$

$$R(x) \text{ if } b' = 0$$



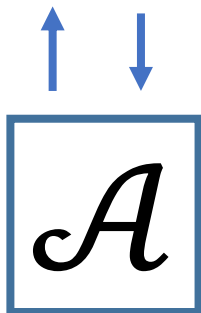
O_2 의 $b = 1$ 이면 \mathcal{A} 는 $\mathcal{B}=O_1$ 처럼 보이고 $b = 0$ 이면 \mathcal{A} 는 $\mathcal{B}=O_2$ 처럼 보인다.

3. Efficient Construction Technique

- (Game 3) Game 2와 같지만, b 값이 무엇이든지, 주어진 x 에 대해 지금까지 query x' 들과 전부 비교해서 $h(x)_{1:j} = h(x')_{1:j}$ 이면 **coll**을 내고 Abort 한다.

If coll, 0 혹은 1을 random으로 출력 아니면,

$$O_3(x) = \begin{cases} 1. k_x := R_j(h(x)_{1:j}) \\ 2. z := \hat{F}^{m-j}(s_{j+1}, \dots, s_m), k_x, h(x)_{j+1:m} \\ R(x) \end{cases} \quad \begin{matrix} \text{if } b = 1 \\ \text{if } b = 0 \end{matrix}$$



Coll이 발생하기 전까지는 X_2 는 X_3 과 identical 하다.
 $\rightarrow |\Pr[X_2] - \Pr[X_3]| \leq |\Pr[X_2 \cap \text{coll}] - \Pr[X_3 \cap \text{coll}]|$
 $\leq \Pr[\text{coll}]$

3. Efficient Construction Technique

- Lemma 7. F 가 perfectly one-time secure 하다면, $\Pr[\text{coll}^c] \leq \frac{\epsilon_{\mathcal{A}}}{2}$ 이고

$\Pr[X_3|\text{coll}] = \frac{1}{2}$ 이다. (여기서 j 의 조건이 나온다)

- Proof . \mathcal{A} 가 만든 x_1, \dots, x_Q 의 query 가 있고 $j := \lceil \log(2Q^2/\epsilon_{\mathcal{A}}) \rceil$ 라 하자.

$$\bullet \Pr[\text{coll}] \leq \Pr\left[\bigcup_{i=2}^Q X_i \text{ makes Coll}\right] \leq \sum_{i=2}^Q \Pr\left[\bigcup_{k=1}^{i-1} (X_k, X_i) \text{ are Coll}\right] \leq \sum_{i=2}^Q \sum_{k=1}^{i-1} \frac{1}{2^{j-1}} =$$

$$\sum_{i=2}^Q \frac{i-1}{2^{j-1}} \leq \frac{Q^2}{2^j} \leq \frac{Q^2 \epsilon_{\mathcal{A}}}{2Q^2} = \frac{\epsilon_{\mathcal{A}}}{2}$$

- $\Pr[X_3|\text{coll}^c] = \frac{1}{2}$ 임을 확인해보자. Collision이 없다면, $R_j(h(x)_{1:j})$ 는 uniform random 값을 전달하고, Perfect One Time secure \hat{F}^{m-j} 는 \mathcal{A} 에게 아무런 정보도 전달하지 않는다.

3. Efficient Construction Technique

▪ 결과 종합.

$$\Pr[X_3] = \Pr[X_3|coll] \Pr[coll] + \Pr[X_3|coll^c](1 - \Pr[coll])$$

$$= \frac{1}{2} \Pr[coll] + \frac{1}{2} (1 - \Pr[coll]) = \frac{1}{2}$$

$$\therefore \Pr[X_0] = \frac{1}{2} + \epsilon_{\mathcal{A}} = \Pr[X_1] \leq \Pr[X_2] + \epsilon_{\mathcal{B}} \leq \Pr[X_3] + \Pr[coll] + \epsilon_{\mathcal{B}}$$

$$\leq \frac{1}{2} + \frac{\epsilon_{\mathcal{A}}}{2} + \epsilon_{\mathcal{B}}$$

따라서 $\frac{\epsilon_{\mathcal{A}}}{2} \leq \epsilon_{\mathcal{B}}$

3. Efficient Construction Technique

■ 결과에 관한 고찰

- 본 결과의 의의는 Universal hash 함수가 충돌이 나지 않을 만큼 j 를 키우고 싶을 뿐 더러 Security 측면에서의 tight reduction을 위해 충분히 작기를 원했다.
 - 그런 측면에서 j 를 Q 와 $\epsilon_{\mathcal{A}}$ 로 정의한 것은 매우 성공적인 결과이다.
- 또한 단순히 Universal Hash Function으로 단순히 collision probability를 bound 할 수 있지만, $m = w(\log \lambda)$ 즉, super-logarithm의 Tightness를 가진다, 이는 logarithm의 tightness를 가지는 APUHFs가 매우 효과적임을 의미한다.

Application: Latticed based PRF

4. Matrix-DDH based Pseudorandom Function (Skip)

▪ [EHK 17] Notation:

- $[a] \in \mathbb{G}$. $[a]$ 로부터 a 를 계산하기 어렵다 (DL in \mathbb{G})
- $[b]_{T_k} \in \mathbb{G}_{T_k}$. $[b]_{T_k}$ 로부터 $b \in \mathbb{Z}_q$ 를 계산하기 어렵다. (DL in \mathbb{G}_{T_k})
- 혹은 $[b] \in \mathbb{G}$ 를 계산하기 어렵다. (Pairing inversion problem)

▪ Diffie-Hellman (DDH) Assumption

- $(\mathcal{G}, [x], [y], [xy])$ 와 $(\mathcal{G}, [x], [y], [z])$ 를 구분하기 어렵다.

▪ $\mathcal{D}_{l,k}$ -Matrix Diffie-Hellman ($\mathcal{D}_{l,k}$ -MDDH) Assumption

- $\mathcal{D}_{l,k}$ distribution 에서 생성된 matrix $A \in \mathbb{Z}_q^{l \times k}$ 와 $r \xleftarrow{\$} \mathbb{Z}_q^k$, $u \xleftarrow{\$} \mathbb{G}^l$ 에 대해
- $([A \| A \cdot r], [A \| u]) \in \mathbb{G}^{l \times (k+1)}$ 을 구분하기 어렵다.

4. Matrix-DDH based Pseudorandom Function (Skip)

$$\mathcal{C}_2 : \mathbf{A} = \begin{pmatrix} a_1 & 0 \\ 1 & a_2 \\ 0 & 1 \end{pmatrix} \quad \mathcal{SC}_2 : \mathbf{A} = \begin{pmatrix} a & 0 \\ 1 & a \\ 0 & 1 \end{pmatrix} \quad \mathcal{L}_2 : \mathbf{A} = \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \\ 1 & 1 \end{pmatrix} \quad \mathcal{IL}_2 : \mathbf{A} = \begin{pmatrix} a & 0 \\ 0 & a+1 \\ 1 & 1 \end{pmatrix},$$

Example 2 (k -Linear Assumption/ k -Lin). We define the distribution \mathcal{L}_k as follows

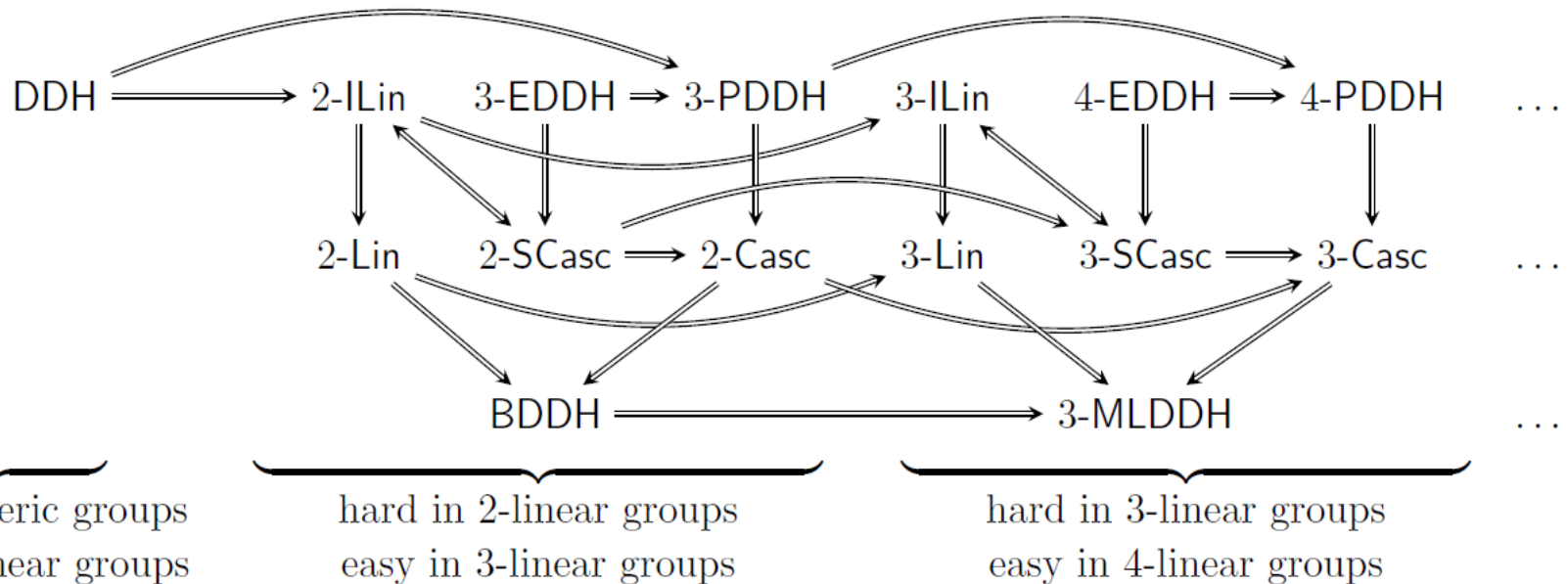
$$\mathbf{A} = \begin{pmatrix} a_1 & 0 & \dots & 0 & 0 \\ 0 & a_2 & \dots & 0 & 0 \\ 0 & 0 & & \ddots & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \dots & 0 & a_k \\ 1 & 1 & \dots & 1 & 1 \end{pmatrix} \in \mathbb{Z}_q^{(k+1) \times k},$$

Example 3 (k -Cascade Assumption/ k -Casc). We define the distribution \mathcal{C}_k as follows

$$\mathbf{A} = \begin{pmatrix} a_1 & 0 & \dots & 0 & 0 \\ 1 & a_2 & \dots & 0 & 0 \\ 0 & 1 & \ddots & & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \dots & 1 & a_k \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix},$$

4. Matrix-DDH based Pseudorandom Function (Skip)

■ Hardness Relationship



5. Decisional-LWE based Pseudorandom Function

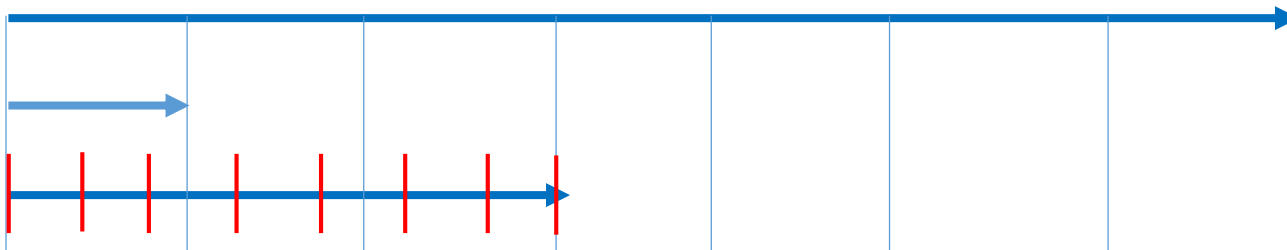
▪ [BPR 12] Preliminary

• Decisional - LWE Assumption

- Security parameter n , modulus $q \geq 2$, distribution χ over \mathbb{Z} , $a \in \mathbb{Z}_q^n$, $s, e \xleftarrow{\$} \chi$ 에 대하여
- LWE distribution $A_{s,\chi}$ over $\mathbb{Z}_q^n \times \mathbb{Z}_q$ 는 $(a, b = \langle a, s \rangle + e \bmod q)$ 로 정의한다.
- Decisional - LWE Assumption은 $A_{s,\chi}$ 와 uniform random을 따르는 $U(\mathbb{Z}_q^n \times \mathbb{Z}_q)$ 을 구별하기 힘든 가정이다.

• Rounding function $[\cdot]_p: \mathbb{Z}_q \rightarrow \mathbb{Z}_p$, where $q \geq p \geq 2$ 는 다음과 같이 정의한다.

$$\square [x]_p = \left\lfloor \left(\frac{p}{q} \right) \cdot (x \bmod q) \right\rfloor \bmod p$$



5. Decisional-LWE based Pseudorandom Function

▪ Game H_0



$$[G(x)]_q = \left[A^T \prod_{i=1}^k S_i^{x_i} \right]_q$$

▪ Game H_1



$$\tilde{G}(x_i) = \tilde{G}(x_{i-1}) \cdot S_i^{x_i} + x_i \cdot E_{x'} \bmod q$$

$$\tilde{G}(x_1, \dots, x_k) = A^T \prod_{i=1}^k S_i^{x_i} + x_1 \prod_{i=2}^k S_i^{x_i} + x_2 \cdot E_{x_1} \prod_{i=2}^k S_i^{x_i} + \dots + x_k E_{x_1, \dots, x_{k-1}} \bmod q$$

$[\tilde{G}(x_1, \dots, x_k)]_q$ 에 접근, BAD Event 가 일어나면 Abort

5. Decisional-LWE based Pseudorandom Function

- Eigen vector 내용

- $G(x) \in \tilde{G}(x) + [-B, B]^{m \times n} \bmod q$

- Bad Event를 정의 $[\tilde{G}(x) + [-B, B]^{m \times n}]_q \neq [\tilde{G}(x)]_q$

- 즉 Bad Event가 일어나지 않으면, $[\tilde{G}(x)]_q = [G(x)]_q$

- 즉 $Adv_{H_0, H_1}(\mathcal{A}) \leq \Pr[Bad \text{ in } H_1] + \text{negl}(n)$ (B bound를 벗어날 확률로 추정됨) 그림
넣기

5. Decisional-LWE based Pseudorandom Function

▪ Game H_2



Choose Uniformly random function U “lazily”
 $[U]_p$ 에 접속, 그러나 Bad event가 일어나면 abort

▪ Game H_3



Choose Uniformly random function U “lazily”
 $[U]_p$ 에 접속, 그러나 Bad event가 일어나도 계속 수행

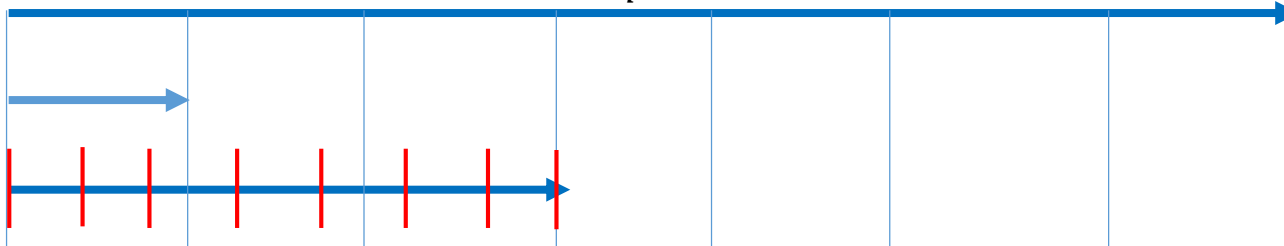
[Theorem5.6 BPR12] LWE Assumption 아래, $\tilde{G}(x)$ 는 U 와 구별 불가능하다.

$$\rightarrow |\Pr[\text{Bad in } H_1] - \Pr[\text{Bad in } H_2]| \leq \text{negl}(n)$$

5. Decisional-LWE based Pseudorandom Function

- H_2 에서 BAD가 일어날 확률

- $\Pr[BAD \text{ in } H_2] \leq (2B + 1) \frac{p}{q} = \text{negl}(n)$



- $\Pr[BAD \text{ in } 1] \leq \text{negl}(n) \rightarrow \text{Adv}_{H_0, H_1}(\mathcal{A}) \leq \text{negl}(n)$

- $\text{Adv}_{H_2, H_3}(\mathcal{A}) \leq \Pr[BAD \text{ in } H_2] = \text{negl}(n)$

5. Decisional-LWE based Pseudorandom Function

- $\chi_\alpha = D_{\mathbb{Z}, \alpha}$ is Discrete Gaussian distribution with parameter $\alpha > 0$, m is message input의 길이. $B := m(C\alpha\sqrt{N})^m$, 적절한 universal Constant C . 적당한 두 개의 moduli p, q 에 대해 $p > q \cdot B \cdot N^{w(1)}$ 로 잡자. 그렇다면 다음 함수는 Pseudorandom Function이다.

- $F_{LWE}^m: \left(\chi_\alpha^{(N \times N)}\right)^m \times \mathbb{Z}_p^N \times \{0,1\}^m \rightarrow \mathbb{Z}_q^N$

- $F_{LWE}^m(S, h, x) := \left[\left(\prod_{i: x_i=1}^m S_i \right) \cdot h \right]_q$, where $S := (S_1, \dots, S_m)$ and $h \stackrel{\$}{\leftarrow} \mathbb{Z}_p^N$

- 만약 $(t_{\mathcal{A}}, \epsilon_{\mathcal{A}}, Q)$ 를 가지고 F_{LWE}^m 을 깨는 알고리즘 \mathcal{A} 가 존재한다면,
 - $t_{\mathcal{B}} = \Theta(t_{\mathcal{A}}), \epsilon_{\mathcal{B}} \geq \frac{\epsilon_{\mathcal{A}}}{m \cdot N}$ 으로 $LWE_{p,N,\alpha}$ 를 깨는 알고리즘 \mathcal{B} 가 존재한다.

6. Applying to Lattice based PRF

■ 제안하는 APUHFs를 사용한 개선된 PRF

- $F_{LWE}^{\mathcal{H}_{n,m}}: (\chi_{\alpha}^{(N \times N)})^m \times \mathbb{Z}_p^N \times \mathcal{H}_{n,m} \times \{0,1\}^m \rightarrow \mathbb{Z}_q^N$
- $F_{LWE}^m(\mathbf{S}, \mathbf{h}, x) := \lfloor (\prod_{i:h(x)_i=1}^m S_i) \cdot h \rfloor_q$

■ Step 1. 기존 F^1 이 perfectly one-time security인지 확인한다.

- [Lemma 9, JKP19] $\Pr_{h \leftarrow \mathbb{Z}_p^N} [F_{LWE}(\mathbf{S}, \mathbf{h}, x) = h'] = \frac{1}{p^N}$
- proof. $x = 0$ 이면 $F_{LWE}(\mathbf{S}, \mathbf{h}, x) = \mathbf{h}$ 이고 uniform random 이다.
- $x = 1$ 이면 $F_{LWE}(\mathbf{S}, \mathbf{h}, x) = \mathbf{S} \cdot \mathbf{h}$ 이고 \mathbf{S} 는 invertible 하므로 역시 uniform random 이다.

6. Applying to Lattice based PRF

▪ Step2. ACUHF를 사용하여 Security를 향상 시킨다.

- [Corollary 1, JKP19]

- $\tilde{F}_{LWE}^j(x) = \left(\prod_{i:x_i=1}^j S_i\right) \cdot h + E(x)$ 가 존재하고 심지어 $1 - 2^{-\Omega(N)}$ 확률로

- $F_{LWE}^m(x) = \left[\left(\prod_{i>j \wedge x_i=1}^m S_i\right) \cdot \tilde{F}_{LWE}^j(x)\right]_q$

6. Applying to Lattice based PRF

- [Theorem 8, JKP19]
- 만약 $(t_{\mathcal{A}}, \epsilon_{\mathcal{A}}, Q)$ 를 가지고 $F_{LWE}^{\mathcal{H}_{n,m}}$ 을 깨는 알고리즘 \mathcal{A} 가 존재한다면,
 - $t'_{\mathcal{B}} = \Theta(t_{\mathcal{A}}), \epsilon'_{\mathcal{B}} \geq \frac{\epsilon_{\mathcal{A}}}{2j \cdot N} - 2^{-\Omega(N)}$ 으로 $LWE_{p,N,\alpha}$ 를 깨는 알고리즘 \mathcal{B} 가 존재한다.
 - Proof 예전 Proof 와 동일한 절차를 가지지만, Game 1에서 $F_{LWE}^m(x)$ 와 $[(\prod_{i>j \wedge x_i=1}^m S_i) \cdot \tilde{F}_{LWE}^j(x)]_q$ 는 statistical distance 가 $2^{-\Omega(N)}$ 만큼 차이가 난다.

Reference

- [JKP19] Simple and More Efficient PRFs with Tight Security from LWE and Matrix-DDH
- [BMR10] Algebraic Pseudorandom Functions with Improved Efficiency from the Augmented Cascade
- [CW79] Larry Carter and Mark N. Wegman. Universal classes of hash functions, 1979
- [DHKP97] A reliable Randomized Algorithm for the Closest-Pair Problem
- [EHK 17] An Algebraic Framework for Diffie –Hellman Assumption
- [BPR12] Pseudorandom Functions and Lattices