Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.29, NO.3, Jun. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.3.503

우수한 공간 효율성을 제공하는 순서노출암호 기법*

김 기 성†‡
대구가톨릭대학교

A More Storage-Efficient Order-Revealing Encryption Scheme*

Kee Sung Kim†‡
DAEGU CATHOLIC UNIVERSITY

요 약

순서노출암호(order-revealing encryption)는 암호화된 데이터에서 효율적인 범위 검색(range query)을 가능하게 하는 암호 기술로 IoT(internet of things), 스마트 제조(smart manufacturing), 클라우드 컴퓨팅(cloud computing) 등 수집 데이터가 경쟁력으로 직결되는 산업분야에서 중요한 보안 기술 중 하나로 주목받고 있다. 2015년 평문의 순서 정보 이외의 어떠한 추가 정보도 노출하지 않는 "이상적인 안전성(ideal-security)"을 만족하는 순서노출암호가 발표되었다. 하지만 구현 가능한 효율성을 제공하지 못하며, 기반을 두고 있는 multilinear maps의 안전성을 의심할만한 다양한 연구결과들이 발표되었다. 최근에는 이상적인 안전성을 우선으로 만족하기 보다는 실제 사용가능한 수준의 효율성 달성에 초점을 맞춘 보다 현실적인 기법들이 제안되고 있는 추세이다. 이에 본 논문에서는 현재 가장 우수하다고 평가 받는 Lewi 등이 제안한 순서노출암호의 효율성을 분석하고, 동일한 안전성 대비 보다 짧은 암호문을 생성할 수 있는 설계 논리를 제시하여, 공간 복잡도 측면에서 보다 우수한 새로운 순서노출암호를 제안하고자 한다.

ABSTRACT

Order-revealing encryption which enables a range query over encrypted data is attracting attention as one of the important security technologies in industry such as IoT, smart manufacturing, and cloud computing. In 2015, an ideally-secure order-revealing encryption whose ciphertexts reveal no additional information beyond the order of the underlying plaintexts has been proposed. However, their construction is too inefficient for practical use and some security analysis of multilinear maps, which their construction relies on, have been proposed. Recently, more practical schemes have been proposed, focusing on achieving practically usable efficiency rather than the ideal security. In this paper, we propose a more storage-efficient order-revealing encryption scheme than the Lewi et al.'s scheme most recently published by presenting an idea that can generate shorter ciphertexts without any security loss.

Keywords: Order-Revealing Encryption, Database Encryption, Samrt Manufacturing Security, Cloud Security

I. 서 론

최근 다양한 산업 분야에서 생산성 향상을 위해 정보통신기술(ICT)을 융합하는 것은 일반적인 전략이 되었다. 특히, 자동차, 의료, 공장 등을 중심으로 제어 시스템 및 설비 등에 ICT 기술을 접목하는 스마트 제조가 급속도로 진행되고 있다. 상대적으로 폐쇄적이던 제조 환경이 ICT 기술과 융합되면서 자연

Received(04. 12. 2019), Modified(05. 22. 2019), Accepted(05. 23. 2019)
* 이 결과물은 2019년도 대구가톨릭대학교 학술연구비 지원에 의한 것임
† 주저자, kee21@cu.ac.kr
‡ 교신저자, kee21@cu.ac.kr(Corresponding author)

스럽게 각종 해킹 위협 및 공격에 노출되는 부작용이 발생하고 있다. 이로 인해, 융합보안 연구에 대한 필요성이 날로 증가하고 있으며, 특히 스마트 제조 보안 분야가 화두로 떠오르고 있다.

제조 환경이 외부와 네트워크로 연결되고, 개방되는 환경에서 보안을 위해서는 신호, 제어, 센서 등 스마트 제조 환경에서 발생하는 데이터에 대한 암호화 및 인증이 필수적으로 요구된다. 특히, 현장에서 수집 및 가공되어 저장되는 각종 데이터는 제조 효율성 향상, 품질 유지, 노하우 활용, 마켓팅 등에 매우 중요한 기업 자산으로 활용될 수 있기 때문에 암호화 조치가 반드시 수반되어야 한다.

암호화는 데이터에 대한 강력한 보안을 가능하게 하지만, 검색을 포함한 다양한 연산을 수행할 수 없게 하는 부작용을 발생시킨다. 일반적인 블록암호를 활용해 데이터를 암호화 하는 경우, 단순 범위연산을 지원하기 위해 전체 데이터를 복호화 해야 하는 비효율성을 초래한다.

2004년에 처음 등장한 순서보존암호[1-4]는 평문 데이터의 크기 순서를 암호문에 그대로 반영하여 암호화를 진행하는 기술로, 복호화 과정 없이 암호문에서 직접 범위검색을 지원하는 암호 기술이다. 이러한 특징으로 인해 IoT, 스마트 제조, 클라우드 환경과 맞물려 최근 가장 주목받는 암호 기술 중 하나이다. 하지만, 순서보존암호의 경우 암호문 자체에 평문의 크기를 그대로 노출하기 때문에 설계 시 제약조건이 심하여, 기존 블록암호 대비 안전성 확보에 어려움이 크다. 또한, 평문의 크기 정보이외의 어떠한 정보도 노출하지 않는다는 "이상적인 안전성(ideal security)"을 만족하는 순서보존암호는 일반적인 방법으로는 설계할 수 없음이 증명됨[2]에 따라 연구에 어려움을 겪게 된다.

2015년 암호문 자체에 크기 정보를 반영하는 기존 순서보존암호 설계 방식에서 탈피해, 임의의 두 암호문을 입력으로 하고, 두 암호문에 대응하는 평문의 크기 관계를 출력으로 하는 공개 함수를 설계하여 추가하는 순서노출암호[5-7] 개념이 처음으로 등장하게 된다. 또한, 이상적인 안전성을 만족하는 설계 기법이 등장함에 따라 최근 가장 주목받고 있는 암호 연구 분야 중 하나이다.

II. 관련 연구

2004년[1] 암호화된 데이터에서 효율적인 범위검색을 지원하기 위해 평문 크기 순서를 암호문에 그대로 보존하는 순서보존암호의 개념이 처음으로 제안되었다. 이후, 순서보존암호의 안전성 개념에 대한 다양한 연구 결과가 발표되었고, 2009년 Boldyreva 등[2]에 의해 처음으로 안전성 개념이 정립되었다. [2]에서는 순서보존암호의 이상적인 안전성을 제시하였고, 동시에 일반적인 설계 방식으로는 해당 안전성을 만족할 수 없음을 보인다. 또한, 자체적으로 임의의 순서보존함수와 구별이 불가능한 순서보존암호를 제시하지만, 후속 연구에 의해 암호문에서 평문의 상위 절반 비트가 노출됨이 증명된다.

[3-4]에서는 암호문이 계속해서 변경될 수 있고(mutable encryption), 현재까지 암호화 된 모든 평문과 암호문 정보를 유지해야 한다(stateful encryption)는 강력한 조건을 추가하여 이상적인 안전성을 제공할 수 있는 순서보존암호를 제시한다. 하지만, 현재까지 제안된 모든 이상적 안전성 제공 순서보존암호는 통신 복잡도 및 공간 복잡도 측면에서 비효율적이다. 또한, 주기적으로 암호문에 대한 전체적인 업데이트가 발생하여 가용성에 문제를 발생시킨다.

2015년 처음으로 이상적인 안전성을 갖는 순서노출암호를 제시한다[7]. Multilinear maps 기반으로 다중입력함수암호(multi-input functional encryption)를 설계하고, 이에 대한 하나의 응용으로 이상적인 안전성을 갖는 순서노출암호의 설계가 가능함을 보인 연구결과이다. 하지만, 현재까지 개발된 multilinear maps의 연산 복잡도는 구현 불가능한 수준이며, 안전성 분석 결과 [8-9]들이 발표되면서 안전성에 의문이 제기되는 상황이다.

Chenette 등[5]은 [7]에서 문제가 되던 효율성 문제를 개선하기 위해 안전성을 낮추고 사용가능한 수준의 효율성을 제공하는 순서노출암호를 설계한다. 하지만 두 암호문을 비교하여 해당 평문의 크기 순서를 판단할 때, 처음으로 달라지는 비트 위치가 노출되는 단점이 있다.

Lewi 등[6]은 [5]에서 문제가 되던 처음으로 달라지는 비트 위치 정보 노출을 블록 위치 정보로 낮출 수 있는 보다 안전한 순서노출암호 설계논리를 제시한다.

본 논문에서는 [6]에서 제시한 순서노출암호의 효율성을 분석하고, 동일한 안전성 대비 보다 짧은 암호문을 생성할 수 있는 설계 논리를 개발하여, 공간 복잡도 측면에서 보다 우수한 새로운 기법을 제안하

고자 한다.

III. 기호 및 정의

임의의 양의 정수 n에 대해 [n]은 {1,2,...,n}을 의미하며, 임의의 분포 D에 대해 x ← D은 분포 D에 따라 x를 임의로 하나 선택함을 의미한다. x||y는 비트열 x와 y를 연접하는 것을 의미하며, 유한집합 S에 대해 $x \leftarrow_R S$은 S의 원소를 균등분포에서 하나 임의로 선택하는 것을 의미한다. 논문 전체에서 λ은 안전성 파라미터를 의미한다. 함수 f(λ)가 모든 자연수 c에 대해 $f = o(1/\lambda^c)$인 경우 λ에서 무시할 만큼 작다(negligible)라고 말하고, 간략히 negl(λ)로 표현한다. 이와는 별개로 poly(λ)는 다항식(polynomial) 함수를 의미한다.

정의 1. 의사난수함수 (pseudo-random function) F : K × X → Y가 안전하다는 것은 $F(k, \cdot)$ ($k \leftarrow_R K$)와 정의역 X와 치역 Y에 대해 정의한 임의의 함수 f(·)에 대해 공격자가 원하는 입력에 대한 함수 값을 얻을 수 있는 상황에서도 의미있는 확률로 두 함수를 구별할 수 있는 공격자가 존재하지 않는다는 것을 의미한다.

정의 2. 의사난수치환 (pseudo-random permutation) π : K × X → X가 안전하다는 것은 $\pi(k, \cdot)$ ($k \leftarrow_R K$)와 정의역 및 치역 X에 대해 정의한 임의의 치환 π(·)에 대해 공격자가 원하는 입력에 대한 함수 값을 얻을 수 있는 상황에서도 의미있는 확률로 두 치환을 구별할 수 있는 공격자가 존재하지 않는다는 것을 의미한다.

정의 3. 순서노출암호 (order-revealing encryption)는 정의역 D에서 다음 3개의 알고리즘으로 구성된다.

- $\text{Setup}(1^\lambda) \rightarrow sk$: 안전성 파라미터 λ를 입력받아 비밀키 sk를 생성한다.
- $\text{Encrypt}(sk,m) \rightarrow ct$: 비밀키 sk와 메시지 m을 입력받아 암호문 ct를 생성한다.
- $\text{Compare}(ct_1,ct_2) \rightarrow b$: 두 개의 암호문 ct_1와 ct_2을 입력받아 비트 b를 출력한다.

정의역 D에서 정의된 순서노출암호가 $sk \leftarrow \text{Setup}(1^\lambda)$와 모든 메시지 $m_1, m_2 \in D$ ($m_1 < m_2$)에 대해 아래의 수식을 만족하면 정합성을 갖는다고 말한다.

$$\Pr[\text{Compare}(ct_1,ct_2) = 1] = 1 - \text{negl}(1^\lambda)$$

본 논문에서는 [5]에서 제시한 시뮬레이션 기반의 순서노출암호 안전성 모델을 사용하고자 한다. 지면 활용을 위해 해당 안전성 모델을 아래의 정의 4에서 개념 위주로 간략히 인용했으며, 보다 상세한 모델은 [5]에서 확인할 수 있다.

정의 4. 주어진 순서노출암호에 대해 임의의 다항식 시간 선택평문공격자(polynomially-bounded chosen plaintext attacker)에 대해 오직 평문 사이의 순서 정보만으로 실제와 구별 불가능한 암호문을 시뮬레이션 할 수 있을 때, 이상적인 안전성(ideal security)을 제공한다고 말한다.

IV. Lewi 등의 기법

2016년[6] Lewi 등은 [5]에서 발생하는 "비트위치 노출로 인한 두 평문사이의 비교적 정확한 거리 유추" 문제를 해결하기 위해 비트위치가 아닌 블록위치로 정보 덩어리를 확장하는 방식을 새롭게 제안한다. 이로부터 공격자는 비트 위치가 노출되는 경우에 비해 상대적으로 두 평문 사이의 거리를 유추하기가 어렵게 된다. 이를 위해, 우선 다항식 크기의 평문 공간에서 이상적인 안전성을 갖는 순서노출암호를 다음과 같이 정의한다. H, F, π는 각각 해시함수, 의사난수함수, 의사난수치환을 의미하고, 암호문 ct는 다음 두 개의 암호문 ct_L와 ct_R로 구성된다. N(=poly(n))은 전체 평문 공간 크기를 의미하고, F는 λ비트 출력값을 가지며, H의 출력 공간은 {0,1,2}로 정의된다.

$$ct_L = (F(k,\pi(m)),\pi(m))$$
$$ct_R = (r,v_1,v_2,\ldots,v_N),\ r \leftarrow_R \{0,1\}^\lambda$$

위의 각 v_i는 $\text{CMP}(\pi^{-1}(i),m) + H(F(k,i),r) \bmod 3$로 계산되며, $\text{CMP}(m_1,m_2)$의 결과값은 각각 -1 ($m_1 > m_2$), 0 ($m_1 = m_2$), 1 ($m_1 < m_2$)을 의미한다. 해당 기법의 핵심 아이디어는 평문 공간이 충분히 작기 때문에 각 암호문에 전체 평문과의 크기 순서를 암호화하여 삽입하는 것이다. 평문 정보를 숨기기 위해 π을 활용했으며, 각 메시지에 대응하는 비

밀값을 생성하기 위해 F를 사용하였다. 안전성 파리미터 λ에 대해 해당 기법의 암호문 크기는 2λ + ⌈log N⌉ + ⌈Nlog 3⌉으로 계산된다.

[6]에서는 이와 같이 작은 평문 공간에서 정의된 순서노출암호를 다음과 같은 방법으로 임의의 평문 공간에서 사용가능하게 하였다. 평문 x가 d진수 $x = x_1||x_2||...||x_n$으로 표현될 때, 각각의 x_i를 위의 이상적 안전성을 제공하는 순서노출암호를 사용해 암호화하여 연접하는 방식이다. ct_R에서 사용된 난수 r은 각 블록에서 공유할 수 있기 때문에 전체 암호문 크기는 $(n+1)\lambda+n(\lceil \log d \rceil + \lceil d\log 3 \rceil)$이 된다. 하지만 단순히 이와 같이 암호문을 생성하는 경우 임의의 두 평문에 대해 서로 다른 모든 블록 위치를 노출하게 된다. 이러한 문제를 해결하기 위해 [5]에서 제시한 각 암호문 블록에 대한 의사난수함수를 활용한 운영모드 아이디어를 동일하게 적용하여, 처음으로 달라지는 블록 위치만 노출하도록 설계하였다.

[6]에서 제시한 순서노출암호는 현재 사용 가능한 효율성을 보장하는 기법 중에서 가장 높은 안전성을 제공하고 있다. 하지만 위에서 분석한 대로 매번 난수를 암호문에 삽입해야하고, CMP 출력값을 1비트로 표현할 수 없는 등의 이유로 암호문 크기 측면에서 개선할 부분이 있다. 본 논문에서는 동일한 안전성을 유지하면서 암호문 크기를 최소화할 수 있는 새로운 설계논리를 제시하여, 공간 복잡도 측면에서 보다 우수한 새로운 순서노출암호를 제안하고자 한다.

V. 제안하는 기법

본 논문에서는 다항식 크기의 평문 공간 [N]에 대해 이상적인 안전성을 갖는 순서노출암호를 다음과 같이 제안한다. H: $\{0,1\}^* \rightarrow \{0,1\}$는 1비트 출력을 갖는 해시함수이며, 안전성 증명과정에서 랜덤오라클로 활용된다. F와 π는 각각 안전한 의사난수함수와 의사난수치환을 의미한다. 제안하는 기법에서 사용하는 $CMP(m_1,m_2)$는 $m_1 \leqq m_2$인 경우 1을 아닌 경우 0을 출력하는 것으로 정의한다. 이와 같이 1비트로 설정하는 경우에도 $CMP(m_2,m_1)$을 함께 연산하여 확인하는 것으로 두 평문 사이의 순서 관계를 명확히 파악할 수 있다.

- $Setup(1^\lambda) \rightarrow sk$: $sk \leftarrow_R \{0,1\}^\lambda$
- $Encrypt(sk,m) \rightarrow ct$: 각 $i \in [N]$에 대해, 비트 v_i를 ($\pi^{-1}(i) \neq m$인 경우) $CMP(\pi^{-1}(i),m) \oplus H(F(sk,m),F(sk,\pi^{-1}(i)))$로 계산하거나, ($\pi^{-1}(i) = m$인 경우) null로 계산한다. $(F(sk,m), v_1, v_2,..., v_N)$을 m에 대한 암호문으로 출력한다. 단, 암호문 비트열 $(v_1, v_2,..., v_N)$에서 v_k = null의 정보를 표현하기 위해서는 $(v_1, v_2,..., v_{k-1})$와 $(v_{k+1}, v_2,..., v_N)$로 분할하는 방법 등을 적용할 수 있다.
- $Compare(ct_1,ct_2) \rightarrow b$: 먼저, $ct_1 = (a, v_1, v_2,..., v_N)$에서 v_x = null을 만족하는 x 값을 찾는다. $ct_2 = (b, v'_1, v'_2,..., v'_N)$로부터 $v'_x \oplus H(b,a)$을 계산하여, $CMP(m_1,m_2)$의 결과값을 확인한다. 동일한 방법으로 $Compare(ct_2,ct_1)$에 대한 연산을 추가적으로 수행하여 m_2과 m_1의 크기 순서를 명확히 확인한다.

정리 1. 제안하는 순서노출암호 정합성을 제공한다.

증명. m_1, m_2 ($m_1 < m_2$)에 대해 $Compare(ct_1,ct_2) = 1$이 아니라고 가정하자. m_1에 대한 암호문 $ct_1 = (a, v_1, v_2,..., v_N)$에서 v_x = null이라고 할 때, m_2에 대한 암호문 $ct_2 = (b, v'_1, v'_2,..., v'_N)$에서 v'_x는 Encrypt 알고리즘에 의해 $CMP(m_1,m_2) \oplus H(F(sk,m_2),F(sk,m_1))$으로 계산된다. 따라서, Compare 알고리즘에서는 $v'_x \oplus H(F(sk,m_2),F(sk,m_1))$을 연산하고, 결과값으로 $CMP(m_1,m_2)$을 출력한다. CMP 정의에 의해 $m_1 < m_2$인 경우 $CMP(m_1,m_2) = 1$이기 때문에 $Compare(ct_1,ct_2) = 1$이 아니라는 것은 모순이다. □

VI. 안전성 및 효율성 분석

(효율성 분석) 5장에서 제안한 순서노출암호의 암호문은 의사난수함수 F의 출력 값과 N개의 암호화된 순서 정보 비트로 구성된다. 따라서 총 길이는 λ + N이 된다. [6]에서와 동일한 방법으로 해당 알고리즘을 일반적인 크기의 평문공간으로 확장할 수 있다. 즉, 임의의 평문 $x = x_1||x_2||...||x_n$ (d 진수)에 대해 각 평문 블록 x_i를 제안하는 순서노출암호를 활용하여 암호화 하는 것이다. 따라서 n개의 암호문이 생성되기 때문에 최종 암호문의 길이는 n(λ + N)이다. [6]과 동일한 안전성을 제공하기 위해서는 해당 논문에서와 같이 [5]에서 제시한 블록 단위 암호문에 대한 운영모드를 적용해야 한다. [6]

Table 1. Storage Comparison (block size = ciphertext size for plaintext $[N]$, total ct size= ciphertext size for d-ary plaintext $x = x_1x_2...x_n$.

	block size	total ct size
[6]	$2\lambda + \lceil \log N \rceil + \lceil N\log 3 \rceil$	$(n+1)\lambda + n(\lceil \log d \rceil + \lceil d\log 3 \rceil)$
Ours	$\lambda + N$	$n(\lambda + d)$

에서 제시한 기법에 비해 한 개의 평문 블록당 약 $\lambda + \lceil \log N \rceil$ 이상의 공간 효율성을 개선할 수 있으며, 전체 암호문 크기에 대해서는 약 $n\lceil \log d \rceil + \lambda$ 이상의 공간 효율성 향상을 기대할 수 있다.

본 단락에서는 5장에서 제안한 순서노출암호에 대한 안전성을 분석하고자 한다.

(안전성 분석) 정리 2. 5장에서 제안하는 순서노출암호는 랜덤오라클 모델에서 이상적인 안전성을 제공한다.

증명. 본 논문에서 새롭게 제안한 다항식 크기의 평문 공간에서 정의된 순서노출암호가 이상적인 안전성을 보장함을 보이기 위해서는 정의 4에 의해 선택평문공격자 하여금 오직 평문의 순서정보만을 이용해 실제와 구별 불가능한 암호문을 생성할 수 있음을 보여야 한다. 먼저, 공격자의 총 메시지 질의 횟수 $q(=poly(\lambda))$와 전체 평문 공간 $[N]$에 대해, 2개의 테이블을 아래와 같이 정의한다.

- T_{RO} : 랜덤 오라클의 입력과 출력을 유지하는 테이블로 $(\alpha\in\{0,1\}^{\lambda},\beta\in\{0,1\}^{\lambda},\gamma\in\{0,1\})$ 원소 저장
- T_K : F와 π의 입력과 출력을 유지하는 테이블로 $(a\in[q],b\in\{0,1\}^{\lambda},c\in[N])$ 원소 저장

공격자가 선택한 i번째 평문 $m_i\in[N]$에 대해, 오직 평문의 순서정보만을 이용해 아래와 같은 방법으로 암호문 ct_i를 시뮬레이션 할 수 있다. 만일, m_i가 이전 $t(<i)$번째 평문과 크기가 같다면, 기 생성한 ct_t를 결과로 반환하면 되기 때문에 질의 하는 평문은 서로 다르다고 가정할 수 있다.

- 현재까지 저장된 모든 T_k의 원소의 세 번째 항목 c를 모아놓은 집합을 S라고 할 때, $c \leftarrow_R [N]\backslash S$를 선택한다. 또한, $b \leftarrow_R \{0,1\}^{\lambda}$를 선택하여, (i, b, c)를 T_K에 저장한다. 만일, T_{RO}에 첫 번째 혹은 두 번째 항목이 b인 즉, $(b,\cdot,\cdot) \in T_{RO}$ 또는 $(\cdot,b,\cdot) \in T_{RO}$인 경우, 시뮬레이션을 취소한다.
- N개의 비트 $v_1, v_2,..., v_N$을 랜덤하게 선택하여 m_i에 대한 최종 암호문 ct_i를(b, $v_1, v_2,..., v_N$)으로 설정한다. 마지막으로 v_c = null로 설정한다.

본 시뮬레이션을 완성하기 위해 다음과 같이 랜덤 오라클 H의 연산을 정의한다.

- H: $\{0,1\}^* \rightarrow \{0,1\}$의 입력 (α, β)에 대해 만일 (α, β, γ)가 T_{RO}에 이미 존재한다면, γ을 출력값으로 한다.
- 그렇지 않고 만일, T_K에서 두 번째 항목이 α 또는 β인 원소 2개가 모두 존재한다는 경우 이를 (i, α, ii)와 (j, β, jj)라고 설정하고 다음과 같이 실행한다. 우선, 공격자의 이전 질의 메시지 m_i에 대한 시뮬레이션 된 암호문 ct_i = (b, v_1, $v_2,..., v_N$)에 대해 v_{jj}를 탐색하고, 평문 사이의 노출 정보를 활용해 $CMP(m_j,m_i)$를 계산하여, $CMP(m_j,m_i)\oplus v_{jj}$를 입력 $H(\alpha, \beta)$에 대한 결과로 반환한다. 마지막으로, $(\alpha, \beta, CMP(m_j,m_i)\oplus v_{jj})$을 T_{RO}에 저장한다.
- 만일 위와 같은 경우가 아니라면, $\gamma \leftarrow_R \{0,1\}$을 선택하여, 결과로 반환하고, (α, β, γ)을 T_{RO}에 저장한다.

위와 같은 시뮬레이션이 정상적으로 생성된 암호문과 구별 불가능함을 다음과 같이 보일 수 있다.

게임 0: 제안하는 순서노출암호와 동일한 방법으로 암호문을 생성하여 공격자에게 반환하는 게임

게임 1: 의사난수함수 F와 의사치환함수 π를 랜덤함수 f '와 랜덤치환 π '으로 설정하고, 나머지는 게임 0과 동일하게 구성하는 게임

게임 2: 메시지 m에 대한 암호문 질의를 하지 않은 상태에서 f '(m)값을 랜덤 오라클의 입력으로 질의하는 경우 게임을 취소하며, 나머지는 게임 1과 동

일하게 구성하는 게임

게임 3: 위에서 정의한 시뮬레이션 방법으로 암호문을 생성하여 공격자에게 반환하는 게임

게임 0과 게임 1은 정의 1과 2의 의사난수함수 및 의사치환함수 성질에 의해서 구별 불가능함을 간단히 보일 수 있다. 게임 1과 2번을 구분할 수 있는 경우는 공격자가 총 다항식 횟수만큼 질의하는 동안 우연히 q개의 λ비트 난수 중 한 개를 질의해야 한다. 따라서, 그 확률은 $poly(\lambda)/2^{\lambda}$으로 $negl(\lambda)$이다. 마지막으로, 게임 2번과 3번은 위와 같이 정의한 랜덤 오라클이 정합성을 갖는다는 것을 보임으로써 구별 불가능성을 증명할 수 있다. 만일, m_i과 m_j의 시뮬레이션된 암호문을 각각 $(a, v_1, v_2, \ldots, v_N)$와 $(a', v'_1, v'_2, \ldots, v'_N)$이라고 하고 $\pi(m_j) = k$라고 하자. $H(a, a')$는 $CMP(m_j,m_i)\oplus v_k$으로 모델링되어 있기 때문에 Compare 알고리즘으로 $v_k\oplus CMP(m_j,m_i)\oplus v_k$를 연산하게 되고, 결과적으로 실제 암호문과 동일하게 $CMP(m_j,m_i)$을 얻을 수 있다. □

VII. 결 론

본 논문에서는 2016년 Lewi 등이 제안한 순서노출암호의 효율성을 분석하고, 보다 우수한 공간 효율성을 제공하는 새로운 기법을 제안하였다. 이를 위해, 제한된 평문 공간에서 이상적인 안전성을 제공하면서, 동시에 보다 짧은 암호문을 생성할 수 있는 설계 논리를 제시하였다.

References

[1] R. Agrawal, Rakesh, J. Kiernan, R Srikant, and Y. Xu, "*Order-Preserving Encryption for Numeric Data,*" proceedings of the 2004 ACM SIGMOD international conference on Management of data pp. 563-574, June 2004

[2] A. Boldyreva, N. Chenette, Y. Lee, and A. O'Neill, "*Order-preserving symmetric encryption,*" EUROCRYPT' 09, LNCS 5479, pp. 224 - 241, April 2009

[3] R. Popa, F. Li, and N. Zeldovich, "*An ideal-security protocol for order-preserving encoding,*" S&P'13, pp. 463-477, May 2013

[4] F. Kerschbaum and A. Schroepfer, "*Optimal average-complexity ideal-security order-preserving encryption,*" ACM CCS'14, pp. 275 - 286, Nov. 2014

[5] N. Chenette, K. Lewi, Stephen A. Weis, and D. J. Wu, "*Practical Order-Revealing Encryption with Limited Leakage,*" FSE'16, LNCS 9783, pp. 474-493, Mar. 2016

[6] K. Lewi and D. J. Wu, "*Order-Revealing Encryption: New Constructions, Applications, and Lower Bounds,*" ACM CCS'16, pp. 1167- 1178, Oct. 2016

[7] D. Boneh, K. Lewi, M. Raykova, A. Sahai, M. Zhandry, and J. Zimmerman, "*Semantically Secure Order-Revealing Encryption: Multi-input Functional Encryption Without Obfuscation,*" EUROCRYPT'15, LNCS 9057, pp. 563-594, April 2015

[8] E. Miles, A. Sahai, and M. Zhandry, "*Annihilation Attacks for Multilinear Maps: Cryptanalysis of Indistinguishability Obfuscation over GGH13,*" CRYPTO'16, LNCS 9815, pp. 629-658, Aug. 2016

[9] J. H. Cheon, K. Han, C. Lee, H. Ryu, and D. Stehle, "*Cyptanalysis of the CLT13 MultiLinear Map*", Journal of Cryptology, Vol. 32, Issue 2, pp. 547 - 565, April 2019

〈저자소개〉

김 기 성 (Kee Sung Kim) 정회원
2009년 2월: 서울시립대학교 수학과 졸업
2011년 2월: 고려대학교 정보경영공학전문대학원 석사
2015년 8월: 고려대학교 정보보호대학원 박사
2018년 9월: 국가보안기술연구소 선임연구원
2018년 9월~현재: 대구가톨릭대학교 IT공학부 조교수
〈관심분야〉 암호 알고리즘, DB 암호화, 보안 프로토콜