Paillier의 확률 공개키 암호 방식의 효율적인 개선

정회원 최 덕 환*, 준회원 조 석 향**, 정회원 최 승 복***, 종신회원 원 동 호****

Improvement of Paillier Probabilistic Public Key Cryptosystem for Efficiency

Dug-Hwan Choi* *Regular Member*, Seok-Hyang Cho** *Associate Member*,
Seung-Bok Choi*** *Regular Member*, Dong-Ho Won**** *Life Member*

요 약

본 논문에서는 Paillier가 제안한 확률 공개키 암호 방식을 개선하였다. Paillier의 확률 공개키 암호 방식은 이산 대수 함수를 기반으로 하고 있으며 메시지는 두 개의 이산 대수 함수의 모듈라 곱으로 계산되고, 이 중 하나는 주어진 공개키에 따른 고정된 값을 갖는다. 공개키를 적절히 선택함으로써 Paillier가 제안한 암호 방식을 개선하여 일방향성과 어의적 안전성을 유지하면서 효율적인 방식을 얻을 수 있다. 또한 이러한 공개키를 쉽게 구할 수 있는 방법도 제시하였다..

Key Words : probabilistic public key cryptosystem; discrete logarithm; composite residuosity class; semantic security; one-way function.

ABSTRACT

We investigate a probabilistic public key cryptosystem proposed by Paillier. It is based on the discrete logarithmic function and the messages are calculated from the modular product of two those functions, one of which has a fixed value depending on a given public key. The improvement is achieved by a good choice for the public key so that it is possible to get efficient schemes without losing the onewayness and semantic security. Also we suggest the method to get the public key for our schemes.

I. 서 론

Diffie와 Hellman에 의해 공개키 암호 방식[1]이 제안된 이후로 많은 연구가 이루어졌지만 확실하게 안전한 비대칭 암호 방식들은 그 수가 대단히 적다. 제안된 공개키 암호 방식 중에서, 단지 RSA-Rabin과 Diffie-Hellman의 제안만이 실제적으로 사용되어 왔다.

지금까지 Rabin 방식[2]과 그 변형만이 소인수분해 문제와 동치임이 증명되었지만 Rabin 방식과 그 변형이 암호문으로부터 평문에 대한 어떠한 부분 정보도 유출될 수 없음을 보장하는 것은 아니다. 이러한 보안 수준을 위해 Goldwasser와 Micali에 의해 어의적 안전성(semantic security)이라는 개념이 도입되었다. 따라서, 하나의 평문이 암호화 시에 선택한 임의의 수에 따라 서로 상이한 많은 암호문을 갖게 되는 확률 공개키 암호 방식(probabilistic public key cryptosystem)[3]이 제안되었다.

새로운 덫문(trapdoor) 방식으로 이산 대수에 의한 덫문(trapdoor in the discrete logarithm) 방식이 제시되고 있는데 고차 잉여류를 대수적 기반으로

* 성균관대학교 수학과(ameschoi@skku.edu), ** 성균관대학교 정보통신공학부(shcho@dosan.skku.ac.kr),
*** (주)퓨쳐시스템 암호체계센터(shchoi@future.co.kr), **** 성균관대학교 컴퓨터공학과(dhwon@simsan.skku.ac.kr)
논문번호 : 020377-0830, 접수일자 : 2002년 9월 3일

이용하는 것이다. Okamoto-Uchiyama[4]는 소수 p에 대해 $Z^*_{p^2}$의 Sylow p-부분군에서 정의된 이산 대수를 이용한 확률 공개키 암호 방식을 제안하였다. Paillier[5]도 이러한 이산 대수를 이용한 새로운 확률 암호 방식을 제안하였다. 소수에 대한 잉여류를 다루는 것과는 대조적으로, 두 개의 소수의 곱으로 이루어진 합성수에 대한 합성 잉여류(composite residuosity class)에 기반을 두었다. 이 방식은 또한 적절한 가정 아래 일방향 함수가 되고, 선택 평문 공격(chosen plaintext attack)에 대해 어의적으로 안전함이 증명되었다. 이것은 조작불가능성(non-malleability)[6]을 만족시키지는 않지만 [7]에 의해 조작 불가능하게 변환하는 것이 가능하다. Naccache-Stern[8]도 같은 합성 잉여류에 기반을 둔 이산 대수를 이용한 공개키 암호 방식을 제안하였다.

Paillier가 제안하는 공개키 암호 방식에서 암호문을 평문으로 복호화 할 때 적절한 공개키의 선택으로 원래의 방식에서 주어진 보안 수준을 저하시키지 않고 모듈러 곱을 배제할 수 있음을 알았다. 우리가 제안한 방식은 메시지가 긴 경우에 원래의 방식보다 빠르게 복호화 할 수 있다. Paillier가 제안한 공개키 집합에서 일부분만을 선택하더라도 제안된 방식은 어의적 안전성과 일방향성을 만족한다. Paillier가 공개키의 타당성을 검사하기 위해 제안한 식을 사용하지 않고, 개선된 방식의 공개키를 얻기 위한 구체적인 방법을 제시했다.

<Notations>

p와 q가 큰 소수일 때, $n=pq$, $\phi(n)=(p-1)(q-1)$, $\lambda(n)=\mathrm{lcm}(p-1, q-1)$이고 여기서 $\phi(n)$과 $\lambda(n)$은 각각 n에 대한 Euler의 함수와 Carmichael의 함수이다. n이 고정된 값을 가질 때 각각의 고정된 함수 값을 ϕ와 λ로 표기하도록 하자.

우리가 필요로 하는 두 가지 사실은 $|Z^*_{n^2}|=n\phi$ 라는 사실과

$$\forall \omega \in Z^*_{n^2},\ \begin{cases} \omega^{\lambda}\equiv 1 \mod n \\ \omega^{n\lambda}\equiv 1 \mod n^2 \end{cases}$$

을 의미하는 Carmichael의 정리이다.

Ⅱ. Paillier의 확률 공개키 암호 방식

2.1 Paillier 방식의 검토

$n=pq$의 소인수분해가 알려지지 않은 상태에서 *RSA[n, e]*는 법 n 상의 e차 근을 구하는 문제를 의미한다고 하자.

$z \in Z_{n^2}$ 이 주어지고 다음의 식

$$z = y^n \mod n^2$$

을 만족하는 $y \in Z^*_{n^2}$이 존재한다면 z는 n^2을 법으로 하는 n차 잉여라고 한다. n차 잉여를 n차 비잉여와 구분하는 것을 *CR[n]*으로 표기하도록 하자.

$g \in Z^*_{n^2}$일 때 함수 Ξ_g는 다음과 같이 정의한다.

$$Z_n \times Z^*_n \to Z^*_{n^2};\ (x, y) \mapsto g^x y^n \mod n^2$$

[5]의 도움정리 3에 의해, $Z^*_{n^2}$에 속하는 g의 위수가 $n\mu$ ($\mu=1, 2, \cdots, \lambda$)일 때, 함수 Ξ_g는 일대일대응 함수이다. 위의 조건을 만족하는 $g \in Z^*_{n^2}$이 주어질 때, $\omega \in Z^*_{n^2}$은 ω의 n차 잉여류 (n-th residuosity class of ω) $\ll\omega\gg_g$와 $y \in Z^*_n$에 대응되는데 이들은

$$\Xi_g(\ll\omega\gg_g, y) = \omega$$

를 만족한다. 합성 잉여류 문제(composite residuosity class problem) *Class[n]*은 $Z^*_{n^2}$에 속하는 ω와 g가 주어지고 g의 위수는 0이 아닌 n의 배수일 때, $Z^*_{n^2}$에 속하는 $\ll\omega\gg_g$를 계산함을 의미한다. *Class[n]*은 계산하기 어렵다고 여겨진다. *D-Class[n]*은 *Class[n]*과 관계된 결정적 문제이다. 즉, $n \mid |g|\neq 0$을 만족하는 $\omega, g \in Z^*_{n^2}$과 $x \in Z_n$이 주어질 때, $x=\ll\omega\gg_g$ 여부를 결정.

*Class[n]*은 n을 소인수분해하는 문제로 귀착된

다. 곱셈에 대한 부분군

$$S_n = \{u \in Z_{n^2} \mid u = 1 + an,\ a \in Z_n\}$$

으로부터 다음과 같이 잘 정의된(well-defined) 함수

$$L : S_n \to Z_n ;\ u \mapsto \frac{u-1}{n}$$

을 얻는다. n을 소인수분해할 수 있다면 λ를 얻는다. 따라서, 임의의 $\omega \in Z_{n^2}^*$는 정리 9([5])에 의해

$$\frac{L(\omega^\lambda \bmod n^2)}{L(g^\lambda \bmod n^2)} = \ll \omega \gg_g \qquad (1)$$

을 만족한다.

임의로 선택된 $g \in Z_{n^2}^*$의 위수가 0이 아닌 n의 배수인지 결정하기 위해서

$$\gcd\ (L(g^\lambda \bmod n^2), n) = 1 \qquad (2)$$

을 만족하는지 검사하는 효율적인 방법이 있다.

[5]에서 각각의 정리 14와 정리 15에 의해, 만약 *Class[n]*과 *D-Class[n]*이 계산하기 어렵다면, 다음에 제시된 Paillier의 기본 방식은 일방향성과 어의적 안전성을 만족한다.

< Paillier의 기본 방식 >

$g \in Z_{n^2}^*$ 은 $n = pq$ 인 0이 아닌 n의 배수인 위수를 갖는다고 하자.

[공개키] $(n,\ g)$.

[비밀키] λ.

[암호화] $m \in Z_n$은 평문이라 하고, $r \in Z_n^*$ 을 임의로 선택한다.

$$C = g^m r^n \bmod n^2.$$

[복호화] $C_\lambda = C^\lambda \bmod n^2$이고

$g_\lambda = g^\lambda \bmod n^2$일 때,

$$m = \frac{L(C_\lambda)}{L(g_\lambda)} \bmod n.$$

이 기본 방식은 전체 암호문이 $Z_{n^2}^*$의 부분군 $\langle g \rangle$로 제한되고 이것의 위수가 $n\alpha$이며 α의 범위는 $1 \le \alpha \le \lambda$ 일 때 아래의 식 (3)에 의해 변형된 방법을 가질 수 있다. 위와 같이 동일한 조건 하에서, 다음과 같이 식 (1)을 확장할 수 있다.

$\forall \omega \in \langle g \rangle$,

$$\ll \omega \gg_g = \frac{L(\omega^\alpha \bmod n^2)}{L(g^\alpha \bmod n^2)} \bmod n. \qquad (3)$$

$h \in Z_{n^2}^*$ 의 위수가 $n\lambda$이고 λ는 α로 나누어질 때, $g = h^{\lambda/\alpha} \bmod n^2$이라고 하자.

< Paillier의 부분군 변형 >

$g \in Z_{n^2}^*$는 $n = pq$ 일 때 0이 아닌 n의 배수인 위수를 갖는다고 하자.

[공개키] $(n,\ g)$.

[비밀키] α.

[암호화] $m \in Z_n$은 평문이라 하고, $r \in Z_n^*$ 을 임의로 선택한다.

$$C = g^{m + rn} \bmod n^2.$$

[복호화] $C_\alpha = C^\alpha \bmod n^2$이고

$g_\alpha = g^\alpha \bmod n^2$ 일 때,

$$m = \frac{L(C_\alpha)}{L(g_\alpha)} \bmod n.$$

부분 이산 대수 문제 *PDL[n, g]*는 다음과 같이 정의된다 :

$\omega \in \langle g \rangle$ 가 주어지면, $\ll \omega \gg_g$ 를 계산한다.

결정적 부분 이산 대수 문제 *D-PDL[n, g]*는 다음과 같이 정의된다 :

$\omega \in \langle g \rangle$와 $x \in Z_n$ 가 주어지면, $\ll \omega \gg_g = x$ 여부를 결정한다.

[5]에서 각각의 정리 19 와 정리 20 에 의해, 만약 *PDL[n, g]*와 *D-PDL[n, g]*가 어렵다면 이 변형된 방식은 일방향성과 어의적 안전성을 만족한다.

2.2 Paillier 방식의 성질

1) *CR[n]*과 *Class[n]*은 *PDL[n, g]* 그리고 *D-PDL[n, g]*와 더불어 각각이 대단히 어려운 문제이다.

2) 두 개의 암호화 함수

$m \mapsto g^m r^n \bmod n^2$과

$m \mapsto g^{m+nr} \bmod n^2$은 Z_n 상에서 덧셈에 대하여 준동형 사상을 만족한다. 특히 이들은 다음과 같은 등식을 유도한다 :

$\forall\, m_1, m_2 \in Z_n \;\&\; k \in N$

$$D(E(m_1)E(m_2) \bmod n^2) = m_1 + m_2 \bmod n$$
$$D((E(m))^k \bmod n^2) = km \bmod n$$

$$D(E(m_1) g^{m_2} \bmod n^2) = m_1 + m_2 \bmod n$$

$$D((E(m_1))^{m_2} \bmod n^2) = m_1 m_2 \bmod n$$

$$D((E(m_2))^{m_1} \bmod n^2) = m_1 m_2 \bmod n.$$

3) 동일한 평문에 대해 여러 가지 암호문을 가질 수 있다 :

$\forall\, m \in Z_n \;\&\; r \in N$

$$D(E(m) r^n \bmod n^2) = m \bmod n \bigvee D(E(m) g^{nr} \bmod n^2) = m \bmod n.$$

Ⅲ. 제안하는 암호 방식

Paillier 방식을 개선하고자 한다.

3.1 공개키

$\Gamma = \{\gamma \in Z_{n^2}^* \mid \gamma \equiv 1 \bmod n\}$은 $Z_{n^2}^*$의 곱셈에 대한 순환 부분군 $\langle 1+n \rangle$이다. 함수 $L : (\Gamma, \cdot) \to (Z_n, +)\ ;\ \gamma \mapsto \frac{\gamma-1}{n}$은 [4]로부터 Γ 상에서 잘 정의된 함수임을 알았다.

도움 정리 1.

함수 $L : (\Gamma, \cdot) \to (Z_n, +)$는 동형사상이다.

증명 우선 $L(\gamma\delta) = L(\gamma) + L(\delta)$임을 보이려 한다.

$$\begin{aligned} L(\gamma\delta) &\equiv \frac{\gamma\delta-1}{n} \bmod n \\ &\equiv \frac{(\gamma-1)(\delta-1)+(\gamma-1)+(\delta-1)}{n} \bmod n \\ &\equiv \frac{\gamma-1}{n}(\delta-1) + \frac{\gamma-1}{n} + \frac{\delta-1}{n} \bmod n \\ &\equiv \frac{\gamma-1}{n} + \frac{\delta-1}{n} \bmod n \\ &\equiv L(\gamma) + L(\delta) \bmod n. \end{aligned}$$

또한 $\ker L = 1$임은 명백하다. 그러므로 L은 동형사상이다. □

$\mu, \nu \in Z_n$ 일 때, $z \in Z_{n^2}$가 $\mu n + \nu$로 나타낼 수 있음은 명백하다. $Z_{n^2}^*$은 Z_{n^2}의 부분집합이므로 동일한 표현이 가능하다.

$\Phi : Z_n \times Z_n^* \to Z_{n^2}^*$는 $\Phi((\mu, \nu)) = \mu n + \nu$를 만족하는 사상이 된다고 하자.

도움 정리 2.

$z \in Z_{n^2}^*$을 만족하는 필요충분조건은 $(z \bmod n) \in Z_n^*$이다.

증명 ($\to$) 임의의 $z \in Z_{n^2}^*$에 대해 $z = \mu n + \nu$를 만족하는 $\mu \in Z_n$과 $\nu \in Z_n$이 존재함은 자명하다. 우리는 $\nu \in Z_n^*$임을 보여야 한다.

$\nu \notin Z_n^*$이라고 가정하자. 만일 ν가 0이라면 $\gcd(z, n^2) = n$이므로 $z \notin Z_{n^2}^*$이다. 따라서 $\nu \neq 0 \bmod n$이어야 한다. $\nu \notin Z_n^*$이고 $\nu \neq 0 \bmod n$이라면 p 혹은 q가 ν를 나누므

로 $\gcd(z, n^2)$은 p 혹은 q를 갖는다. 왜냐하면 $z=\mu n+\nu=\mu pq+\nu$이기 때문이다. 그러므로 $z \notin Z_{n^2}^*$이다.

($\Leftarrow$) 임의의 $z=\mu n+\nu \in Z_{n^2}$이 $(z \bmod n)=\nu \in Z_n^*$을 만족한다고 하자. $z=\mu n+\nu=\mu pq+\nu$이므로 $\gcd(z, n^2)=1$이다. 왜냐하면 n^2의 인수는 p 혹은 q만을 갖고 $\gcd(z, p)=1=\gcd(z, q)$이기 때문이다. □

도움 정리 3.

Φ는 일대일 대응이다.

증명 $Z_n \times Z_n^*$와 $Z_{n^2}^*$은 다같이 위수가 $n\phi$인 집합이므로, Φ가 일대일 함수임을 증명할 필요가 있다. Φ가 일대일 함수임을 보이는 것은 자명하다. □

λ는 Z_n^*의 원소이므로, $\lambda\lambda^{-1}=1$을 만족하는 $\lambda^{-1} \in Z_n^*$이 존재한다. 또한 각각의 $\nu \in Z_n^* \subset Z_{n^2}^*$에 대하여, $\nu_\lambda=\nu^\lambda \bmod n^2$은 Γ의 원소이므로 $L(\nu_\lambda)$는 Z_n의 원소이다. 이 때 $\mu \in Z_n$을 다음과 같이 정의한다.

$$\mu = \lambda^{-1}\nu - \lambda^{-1}\nu\, L(\nu_\lambda) \mod n \qquad (4)$$

정리 1.

합동식 (4)를 만족하는 $\mu \in Z_n$과 $\nu \in Z_{n^2}^*$에 대하여 $g=\mu n+\nu$라 하자. $g^\lambda \bmod n^2$은 Γ의 생성원이다. 즉, $g^\lambda \equiv 1+n \mod n^2$.

증명 $(Z_{n^2}, +, \cdot)$이 환일 때 μ와 ν의 조건 때문에, g는 $Z_{n^2}^* \subset Z_{n^2}$의 원소이다.

$(Z_{n^2}, +, \cdot)$은 가환환이므로 이항정리(binomial theorem)에 의하여 다음과 같은 성질이 만족함을 보일 수 있다.

$$\begin{aligned} g^\lambda &\equiv (\mu n+\nu)^\lambda \mod n^2 \\ &\equiv \nu^\lambda + \lambda\mu\nu^{\lambda-1} n \mod n^2 \\ &\equiv 1 + L(\nu_\lambda)n + (\nu^\lambda - \nu^\lambda L(\nu_\lambda) \bmod n)n \mod n^2 \\ &\equiv 1+n \mod n^2. \end{aligned}$$

마지막 과정은 Carmichael의 정리에 의해 성립한다. □

정리 1에 의해, $L(g_\lambda)=L(g^\lambda \bmod n^2)=1$. 그러므로 $m<n$이고 $r<n$에 대하여

$$\begin{aligned} m &= L(1+mn \bmod n^2) \bmod n \\ &= L((g^m r^n)^\lambda \bmod n^2) \bmod n \end{aligned}$$

이 성립한다.

<개선된 기본 방식>

다음 관계식을 만족하는 $\mu \in Z_n$과 $\nu \in Z_n^*$에 대하여 $g=\mu n+\nu \in Z_{n^2}^*$라 하자.

$$\mu = \lambda^{-1}\nu - \lambda^{-1}\nu\, L(\nu_\lambda) \mod n$$

[공개키] (n, g).

[비밀키] λ.

[암호화] $m \in Z_n$은 평문이라 하고, $r \in Z_n^*$을 임의로 선택한다.

$$C = g^m r^n \mod n^2.$$

[복호화] $C_\lambda = C^\lambda \mod n^2$일 때,

$$m = L(C_\lambda) \mod n.$$

이 개선된 방식은 또한 다른 변형을 가질 수 있다. $h \in Z_{n^2}^*$의 위수가 $n\lambda$이고 λ는 α로 나누어질 때, $g=h^{\lambda/\alpha} \bmod n^2$이라 하자. 다음 식을 보이는 것은 쉽다.

$g^{\alpha} \equiv 1 + n \mod n^2$이고

$$m \equiv L(1+mn \mod n^2) \mod n$$
$$\equiv L((g^{m+rn})^{\alpha} \mod n^2) \mod n.$$

< 개선된 부분군 변형 >

다음 관계식을 만족하는 $\mu \in Z_n$과 $\nu \in Z_n^*$에 대하여 $g = \mu n + \nu \in Z_{n^2}^*$라 하자.

$$\mu = \lambda^{-1}\nu - \lambda^{-1}\nu L(\nu_\lambda) \mod n.$$

$g = h^{\lambda/\alpha} \mod n^2$이라 하자.

[공개키] (n, g).

[비밀키] α.

[암호화] $m \in Z_n$은 평문이라 하고, $r \in Z_n^*$을 임의로 선택한다.

$$C = g^{m+rn} \mod n^2.$$

[복호화] $C_\lambda = C^{\lambda} \mod n^2$ 일 때,

$$m = L(C_\alpha) \mod n.$$

3.2 제안한 방식의 성질

이 논문에서 제안한 개선된 방식은 일방향성과 어의적 안전성을 만족한다.

Paillier는 *Class[n, g]*를 [5]에서 다음과 같이 정의하였다.

"주어진 $\omega \in Z_{n^2}^*$에 대해, $\omega \equiv g^x y^n \mod n^2$을 만족하는 $y \in Z_n^*$가 존재할 $x \in Z_n$를 구하는 문제"

또한 도움정리 7([5])에 의해, Paillier 방식에 대한 공개키들의 집합에 속하는 어떠한 g_1과 g_2에 대해서도 *Class[n, g_1]*과 *Class[n, g_2]*는 동치(equivalent)임을 보였다. 다시 말해서, *Class[n, g]*의 복잡도(complexcity)는 g에 대해 독립이다. 따라서, *Class[n, g]*라는 계산 문제는 순수하게 n에만 의지하는 문제이다. 그러므로, Paillier가 제안한 공개키들의 분산이 우리가 제안하는 공개키들의 분산과 전혀 다르다고 하더라도 *Class[n]*이라는 계산 문제에는 전혀 영향을 미치지 않는다. 왜냐하면 우리가 제안한 공개키들은 Paillier가 제안한 공개키들의 부분집합이기 때문이다. 이 때 Paillier가 제안한 *D-Class[n]*은 *Class[n]*으로 귀착된다는 정리 12([5])도 우리가 제안하는 방식에 적용할 수 있다. 개선된 제안 방식은 Paillier가 제안한 방식보다 더 작은 공개키를 사용함에도 불구하고 일방향성과 어의적 안전성을 유지한다.

정의 1.

*Class[n]*이 intractable하다는 것은 다음을 의미한다.

: 주어진 $g, \omega \in Z_{n^2}^*$에 대하여, $\ll \omega \gg_g$를 계산하는 확률 다항식 시간 알고리즘(probabilistic polynomial time algorithm)이 존재하지 않는다.

정리 2.

개선된 기본 방식이 일방향성을 만족할 필요충분 조건은 *Class[n]*이 intractable 한 것이다.

증명 ($\Rightarrow$) *Class[n]*이 intractable 하지 않다고 가정하자. 즉, 주어진 암호문 $C \in Z_{n^2}$으로부터 $C = g^m r^n \mod n^2$을 만족하는 평문 m을 구하는 확률 다항식 시간 알고리즘이 존재한다. 따라서, 우리가 제안한 방식은 일방향성을 만족하지 않는다.

($\Leftarrow$) 우리가 제안한 방식이 일방향성을 갖지 못한다고 가정하자. 주어진 암호문 $C \in Z_{n^2}$으로부터, 평문 $m \in Z_n$을 쉽게 구할 수 있는 알고리즘이 존재한다. 그러므로, *Class[n]*이 intractable 하다는 것과 모순이다. 따라서 *Class[n]*이 intractable 하면 우리가 제안한 방식은 일방향성을 갖는다. □

정리 3.

*D-Class[n]'*는 개선된 암호 방식의 공개키에 대한 것으로만 제한된 *D-Class[n]*이라고 하자. *D-Class[n]'*와 *D-Class[n]*은 동치(equivalent)이다.

증명 A가 *D-Class[n]*을 깨는 알고리즘이라고 하자. 이 때 이러한 알고리즘은 당연히 *D-Class[n]'*에 대해서도 성립한다. 다른 방향도 성립함을 보이도록 하자. A가 *D-Class[n]'*를 깨는 알고리즘이라

고 하자. [5]의 도움정리 3에 의해 g, $\omega \in Z^*_{n^2}$에 대해, 개선된 방식의 공개키 h에 대한 $\ll\omega\gg_h$, $\ll g\gg_h$의 값을 판별할 수 있다. 이 때 [5]의 도움정리 7에 의해

$\ll\omega\gg_g = \ll\omega\gg_h \ll g\gg_h^{-1} \bmod n$

이 성립하므로 우변의 두 개의 판별된 값으로 좌변의 값을 판별할 수 있다. 따라서 A가 *D-Class[n]*에 대한 판별을 유도할 수 있다. □

위의 정리 3에 의해 공개키의 분산에 관계없이 항상 *D-Class[n]*을 개선된 방식에도 적용할 수 있음을 보였다.

정의 2. *D-Class[n]*이 intractable 하다는 것은 다음을 의미한다.

: 주어진 g, $\omega \in Z^*_{n^2}$와 $x \in Z_n$에 대하여, $x = \ll\omega\gg_g$의 성립 여부를 결정하는 확률 다항식 시간 알고리즘이 존재하지 않는다.

정리 4.

개선된 기본 방식이 어의적 안전성을 만족할 필요충분조건은 *D-Class[n]*이 intractable 한 것이다.

증명 서로 다른 평문 m_1과 m_2 $(0 < m_1, m_2 < n)$가 주어지고, 암호문 C는 m_1과 m_2 중에서 임의로 정해진 평문으로부터 생성되었다고 하자. $m \in \{m_1, m_2\}$에 대하여 $C = g^m r^n \bmod n^2$이다. 확장된 유클리드 알고리즘(Extended Euclidean Algorithm)에 의해, 각각의 $i \in \{1, 2\}$에 대하여,

$$z_i = Cg^{-m_i} \bmod n^2 = g^{(m-m_i)} r^n \bmod n^2$$

이다.

만일 C가 m_1의 암호문이라 하면, z_1은 모듈라 n^2 상의 n차 잉여(n-th residuosity modulo n^2)임을 알 수 있다. 따라서, 개선된 방식이 어의적 안전성을 만족하지 않는다면 *D-Class[n]*은 intractable 하지 않다. 그리고 그 역도 성립한다. □

[5]에서 언급이 없었지만, 어떠한 공격자에 대해서도 안전하기 위해, $g = a + bn \in Z^*_{n^2}$은 $b \in Z^*_n$을 만족해야만 한다. 왜냐하면 $b \in Z_n - \{Z^*_n \cup 0\}$일 때 $\gcd\left(\frac{g-a}{n}, n\right)$는 p 또는 q이므로 n을 소인수분해할 수 있다. 또한 선택 암호문 공격(Chosen Ciphertext Attack : CCA)의 경우 λ 값을 찾는다면 n을 인수분해할 수 있다. CCA는 복호화 오라클(Decryption Oracle)에 접속이 가능하므로 주어진 암호문에 대한 평문을 언제나 구할 수 있다. 공개키 g를 $a + bn$이라 하고, $L(g^\lambda) = l$이라 하자.

$$\begin{aligned}(g + an)^\lambda &= g^\lambda + \lambda g^{-1} an \bmod n^2 \\ &= (1 + ln) + \lambda n \bmod n^2 \\ &= 1 + (l + \lambda)n \bmod n^2\end{aligned}$$

이므로

$$\begin{aligned}m &= \frac{L\{(g + an)^\lambda\}}{L(g^\lambda)} \bmod n \\ &= 1 + \lambda l^{-1} \bmod n \\ \Rightarrow \lambda l^{-1} &= m - 1 \bmod n\end{aligned}$$

이 성립한다. 또한 a', $b' \in Z^*_n$에 대해 $g' = a' + b'n$이라 하고 $L\{(g')^\lambda\} = l'$이라 하자.

$$\begin{aligned}m' &= \frac{L\{(g \cdot g')^\lambda\}}{L(g^\lambda)} = \frac{L(g^\lambda) + L\{(g')^\lambda\}}{L(g^\lambda)} \\ &= 1 + l' \cdot l^{-1} \bmod n \\ \Rightarrow l' l^{-1} &= m' - 1 \bmod n\end{aligned}$$

이 성립한다. 따라서, l^{-1}의 값은 어떤 k, $k' \in Z^n$에 대해

$$l^{-1} = \gcd((m-1) + kn, (m'-1) + k'n)$$

을 만족한다. 그러므로 $\lambda = l(m-1) \bmod n$을 찾을 수 있다. 따라서, 본 논문의 제안 방식과 Paillier의 제안 방식은 CCA에 안전하지 못하므로 두 방식의 안전성은 동치이다.

사용자 A	공개 정보 g, n	사용자 B
$g \in Z^*_{n^2}$ $r \in Z^*_n$ $m \in Z_n$ $C = g^m r^n \bmod n^2$	C →	$C_\lambda = C^\lambda \bmod n^2$ $g_\lambda = g^\lambda \bmod n^2$ $m = \frac{L(C_\lambda)}{L(g_\lambda)} \bmod n$

그림 1. Paillier의 프로토콜

사용자 A	공개 정보 g, n	사용자 B
$g \in Z^*_{n^2}$ $r \in Z^*_n$ $m \in Z_n$ $C = g^m r^n \bmod n^2$	C →	$C_\lambda = C^\lambda \bmod n^2$ $m = L(C_\lambda)$

그림 2. 개선된 Paillier의 기본 프로토콜

위의 그림 1과 그림 2가 보여주는 것처럼 $L(g_\lambda) \equiv 1 \bmod n$ (혹은 $L(g_a) \equiv 1 \bmod n$)을 만족하는 공개키 $g \in Z^*_{n^2}$을 선택하기 때문에, Paillier 방식의 복호화 작업 부하가 줄어든다. 따라서, 본 논문에서는 Paillier가 제안한 방식을 개선하여 효율성을 높였다.

Ⅳ. 결 론

본 논문에서는 Paillier 방식을 개선한 확률 공개키 암호 방식을 제안하였다. Paillier 방식은 복호화를 시행할 때 암호문 C로부터 얻어진 값 $L(C_\lambda) \in Z^*_n$와 공개키 g로부터 얻어진 값 $(L(g_\lambda))^{-1} \in Z^*_n$의 곱에서 평문을 얻는다. 우리가 제시하는 방식은 Paillier 방식에서 $L(g_\lambda) = 1$을 만족하는 선별된 공개키를 선택함으로써 복호화 과정에서 계산 양을 줄이도록 하였다. 개선된 방식은 Paillier 방식의 관점에서 하나의 특별한 유형이 되므로 이것은 원래의 방식이 갖는 일방향성과 어의적 안전성을 만족시킨다. 또한 개선된 방식은 복호화 시에 계산 양을 줄임으로써, 다량의 암호문을 처리할 때 걸리는 복호화 시간을 줄일 수 있다. 따라서 제시된 방법이 복호화 할 때 효율적이다.

참 고 문 헌

[1] W. Diffie and M. Hellman, "New Directions in Cryptography", *IEEE Transactions on Information Theory*, Vol. IT-22(6), pp. 644-654, 1976.

[2] M. Rabin, "Digitalized Signatures and Public Key Functions as Intractable as Factorization", *MIT Laboratory for Computer Science* TR-212, 1979.

[3] S. Goldwasser and S. Micali, "Probabilistic Encryption", *JCSS* 28, pp. 270-299, 1984.

[4] T. Okamoto and S. Uchiyama, "A New Public Key Cryptosystem as Secure as Factoring", *EUROCRYPTO' 98*, LNCS 1403, pp. 308-318, 1998.

[5] P. Paillier, "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes", *Proc. of EUROCRYPTO' 99*, LNCS 1592, pp. 223-238, 1999.

[6] D. Dolev, C. Dwork and M. Naor, "Non-malleable Cryptography", *Proc. of the 23rd STOC. ACM Press*, New York, 1991.

[7] P. Paillier and D. Pointcheval, "Efficient Public-Key Cryptosystems Probably Secure Against Active Adversaries", *Proc. of ASIACRYPT ' 99*, LNCS 1716, pp. 165-179, 1999.

[8] D.Naccache and J.Stern, "A New Public Key Cryptosystem Based on Higher Residues", *Proc. of 5th ACM Conference on Computer and Communication Security*, ACM Press, pp. 59-66, 1998.

최 덕 환(Dug-Hwan Choi) 정회원

1985년 2월 : 성균관대학교 이학사
1987년 2월 : 성균관대학교 이학석사
1992년 5월 : University of Iowa 대학원 수학과 석사
1998년 12월 : Iowa State University 대학원 수학과 박사

<주관심분야> 암호이론, 부호이론, 조합론

조 석 형(Seok-Hyang Cho) 준회원

1986년 2월 : 이화여자대학교 수학과 이학사
1986년~1998년 : 중앙교육진흥연구소 과장
2001년 2월 : 서울산업대학교 전자계산학과 공학석사
2001년 3월~현재 : 성균관대학교 정보통신공학부 박사 과정

<주관심분야> 암호이론, 부호이론

최 승 복(Seung-Bok Choi) 정회원

1998년 8월 : 연세대학교 통계학과 학사
2001년 8월 : 성균관대학교 전기 전자 및 컴퓨터공학부 공학석사
2001년 7월~현재 : (주) 퓨터시스템 암호체계센터 전임 연구원

<주관심분야> 암호이론, 부호이론

원 동 호(Dong-Bo Won) 종신회원

성균대학교 전자공학과(학사, 석사, 박사)
1978년~1980년 : 한국전자통신 연구소 전임 연구원
1985년~1986년 : 일본 동경공대 객원 연구원
1995년~1997년 : 성균관대학교 교학처장
1996년~1997년 : 국무총리실 정보화추진위원회 자문위원
1999년~2001년 : 성균관대학교 전기전자 및 컴퓨터공학부 학부장
1999년~2001년 : 성균관대학교 정보통신대학원 원장
2002년 : 한국정보보호학회 회장
1982년~현재 : 성균관대학교 정보통신공학부 교수
2002년~현재 : 성균관대학교 연구처장
2000년~현재 : 정통부 지정 정보보호인증기술연구센터 센터장

<주관심분야> 암호이론, 전자상거래