제18회 한국정보처리학회 추계학술발표대회 논문집 제9권 제2호 (2002.11)

Paillier 공개키 암호 방식에 관한 연구

김문정*, 원동호*, 이영수**, 채영도**
*성균관대학교 인증기술연구센터
**성균관대학교 수학과
e-mail:mjkim@dosan.skku.ac.kr

A Study on Paillier Public-Key Cryptosystems

Moon-Jeong Kim*, Dongho Won*, Young-Soo Lee**,Young-Do Chai**
*Authentication Technology Research Center, Sungkyunkwan University
**Dept. of Mathematics, Sungkyunkwan University

요 약

1999년에 Paillier는 합성수 잉여류(composite residuosity class)에 기반을 둔 공개키 암호 방식을 제안하였다. 이는 고차 잉여를 결정하는 것이 계산상 어렵다는 가정 아래 제안된 새로운 확률 암호 방식이다. 현재, 이 새로운 공개키 암호 방식에 대한 안전성 및 변형된 Paillier 암호 방식들에 대한 연구가 다양한 방향에서 진행되고 있다. 요즘, 암호 알고리즘 연구에서, 가장 활발하게 연구되고 있는 Paillier 암호 방식에 대하여 그 내용과 안전성에 대하여 수학적으로 자세히 분석하고, 개선된 Paillier 방식의 안전성과 선택적 암호문 공격에 대하여 분석하였다. 이후, Paillier 방식과 개선된 Paillier 방식의 효율성 및 안전성을 비교한다.

1. 서론

1976년 Diffie-Hellman [2]은 사용자가 복호화 키만 비밀로 보관하고, 암호화키는 공개해도 암호계를 위태롭게 하지 않는 새로운 종류의 암호 방식인 공개키 암호 방식(public-key cryptosystem)을 제안하여 관용 암호 방식의 키 전송 문제를 해결하였다. 이후, 이 방식에 대한 많은 연구에도 불구하고, 안전성이 입증되어 사용 되고 있는 공개키 암호 방식은 극히 드물다. 1999년 Paillier[5]는 합성수 잉여류(composite residuosity class)에 기반을 둔 공개키 암호 방식을 제안하였다. 이는 고차 잉여를 결정하는 것이 계산상 어렵다는 가정 아래 제안된 새로운 확률 암호 방식이다. 소수에 대한 잉여류를 다루는 것과는 대조적으로, 두 개의 소수의 곱으로 이루어진 합성수에 대한 합성수 잉여류에 기반을 두었다. 현재, 이 새로운 공개키 암호 방식에 대한 안전성 및 변형된 Paillier 암호 방식들에 대한 연구가 활발히 진행되고 있다[1][3][4][6]. Paillier 암호 방식은 평문 m을 $E(m,r)=g^m h^n \bmod n^2$, 여기서 g, n 은 공개키이고, h 는 임의의 정수이다. 암호함수 $E(m,r)$는 $E(m,r_1)E(m,r_2)=E(m_1+m_2, r_1r_2)$의 동형 성질을 갖는다. 따라서, Paillier 방식은 유용한 응용들을 가지는데, 예로서, 투표 시스템, 역치 시스템(threshold systems)등이 해당될 수 있다. 이 방식의 일방향성(one-wayness)은 계산적 합성 잉여 문제(computational composite residuosity problem - CCRP)를 공격하는 것만큼 어렵다. 또한, 이것의 어의적 안전성(semantic security)도 증명 되었다. Paillier의 암호 방식은 다양한 구조들로 확장되었다. 한편, 최덕환, 원동호 [1]등은 키 g 의 생성을 변형하여 역수를 취하지 않아도 되는 방식을 제안하였다. Paillier 방식의 복호화 알고리즘은 역수 $L(g^\lambda)^{-1} \bmod n$, 여기서 $n=pq$이고

$\lambda = lcm(p-1, q-1)$이다. 그들은 $g^{\lambda} = 1+n \mod n^2$ 을 만족하는 특별한 공개키 g를 사용한다. 그들의 키 분배는 Paillier의 것과 다르고, 정수론적 이론들도 Paillier의 구조와는 다르다. 그러나, 그들은 키 분배의 일방향성과 어의적 안전성(semantic security)을 증명하진 않았다. 우리는 현재 암호 알고리즘 연구에서, 가장 활발히 연구되고 있는 Paillier 암호 방식에 대하여 그 내용과 안전성에 대하여 수학적으로 자세히 분석하고, 개선된 Paillier 방식에 대하여, 제안자들이 조사하지 않은 안전성과 선택적 암호문 공격에 대하여 분석하였다. 이후, Paillier 방식과 개선된 Paillier 방식의 효율성 및 안전성을 비교, 분석한다.

2. Paillier 암호 방식

정의 2.1 g는 $Z_{n^2}^*$의 원소라 하고, ε_g는 다음과 같이 정의된 함수라 하자.

$$\varepsilon_g : Z_n \times Z_n^* \rightarrow Z_{n^2}^*$$
$$(x, y) \rightarrow g^x y^n \mod n^2$$

ε_g는 g에 의존하는 값이다.

정의2.2 g가 B의 원소라고 가정하자. $\omega \in Z_{n^2}^*$ 에 대하여, $[[\omega]]_g$ 는 $\varepsilon_g(x, y) = \omega$ 를 만족하는 $y \in Z_n^*$ 이 존재하는 유일한 Z_n 안에 있는 정수 x들의 집합이다. 다시 쓰면,

$[[\omega]]_g = !x \in Z_n | \varepsilon_g(x, y) = g^x y^n = \omega \mod n^2$

을 만족하는 $y \in Z_n^*$ 가 존재한다.

정의2.3

$S_n = u < n^2 | u = 1 \mod n = an+1 | a \in Z_n$는 다음을 만족하는 $\mod n^2$에서 정수들의 곱셈 부분군이다. 모든 S_n 의 원소 u 에 대하여, $L(u) = \frac{u-1}{n}$ 은 제대로 정의된 함수이다.

보조정리2.4 $\omega \in Z_n^*$ 와 $g \in B$ 에 대하여,

$$\frac{L(\omega^{\lambda} \mod n^2)}{L(g^{\lambda} \mod n^2)} = \frac{\lambda [[\omega]]_{1+n}}{\lambda [[g]]_{1+n}} =$$

$\frac{[[\omega]]_{1+n}}{[[g]]_{1+n}} = [[\omega]]_g \mod n$ 이다.

< Paillier 암호 방식>

[키 생성] $n = pq$
$\lambda = lcm(p-1, q-1)$

g는 $n | ord_{n^2}(g)$를 만족하는 Z_{n^2}의 원소

[공개키] (n, g)

[비밀키] λ

[m 의 암호화] $m \in 0, 1, \cdots, n-1$, 홀ㅈㅐㅈ
h는 Z_n 에서 임의로 선택
암호문 $c = g^m h^n, \mod n^2$

[c의 복호화]

$m = L(c^{\lambda} \mod n^2)\, L(g^{\lambda} \mod n^2)^{-1}, \mod n$

위 방식이 올바르게 적용된다는 것은 **보조정리2.4** 로부터 쉽게 증명 될 수 있고, 위의 암호문은 덫문(trapdoor) 비밀로 λ (n 의 소인수 분해를 알아야 한다)를 가지는 덫문 함수(trapdoor function) 이다.

정리 2.5 임의의 원소 g 가 위의 조건을 만족할 확률은 $1 - \frac{1}{n}$ 이다.

2.1. Paillier 방식의 안전성

정의2.6 *계산적 합성 잉여 문제* (computational composite residuosity problem) **CCRP**는 주어진 $\omega \in Z_{n^2}^*$, $g \in G_{Pai}$ ㅋㅣㅈㅎ $n \in RSA_{\mod}$ 에 대하여, $[[\omega]]_g$ 를 계산하는 문제이다.

결정적 합성 잉여 문제 (decisional composite residuosity problem) **DCRP**는 주어진 $x \in Z_n$, $\omega \in Z_{n^2}^*$, $g \in G_{Pai}$ ㅋㅣㅈㅎ $n \in RSA_{\mod}$ 에 대하여, $x = [[\omega]]_g$ 이 참인지를 결정하는 문제이다.

정리2.7 $n = pq$ 을 소인수분해하는 알고리즘은 CCRP를 풀 수 있게 한다.

그러나, 위 정리의 역이 참인지는 알려져 있지 않다. 즉, CCRP가 모듈라 n을 소인수분해하지 않고 풀려질 수 있는 가능성이 있다.

정리 2.8 Paillier 방식의 일방향성 (one-wayness)은 CCRP를 공격하는 것만큼 다루기 어렵다.

정리 2.9 Paillier 방식의 어의적 안전성은 DCRP를 공격하는 것만큼 어렵다.

3. Paillier 암호 방식

개선된 Paillier 방식과 원래의 Paillier 방식과 다른 점은 크게 두 가지이다. 공개키 g 의 선택과 복호화 알고리즘이다. 개선된 Paillier 방식에서의 공개키 g 들의 집합을 G_{M-Pai} 로 표기하기로 하자. 공개키 g 는 다음 집합에서 선택된다 :

$G_{M-Pai} = g \in Z_{n^2}^* | g^\lambda = 1 + n \mod n^2$

따라서, Paillier 방식의 복호화 과정에서, $L(g^\lambda \mod n^2) = \frac{g^\lambda - 1}{n} = \frac{(1+n)-1}{n} = 1$ 이므로, $L(g^\lambda \mod n^2)$ 의 계산 값은 1이 된다. 결국, 모든 $g \in G_{M-Pai}$ 에 대하여 복호화 과정에서 역수(inversion)를 계산할 필요가 없어졌다.

< 개선된 Paillier 방식 >

[키 생성] $n = pq$, $\lambda = lcm(p-1, q-1)$

$g^\lambda = 1 + n \mod n^2$을 만족하는 $Z_{n^2}^*$의 원소[공개키] (n, g)

[비밀키] λ

[m의 암호화] $m \in 0, 1, \cdots, n-1$, 평문

h는 Z_n에서 임의로 선택한 정수

$c = g^m h^n \mod n^2$

[c 의 복호화] $m = L(c^\lambda \mod n^2)$

정리 3.1 임의의 정수 $g \in Z_{n^2}^*$ 가 집합 G_{M-Pai}에 포함될 확률은 기껏해야 $\frac{1}{\phi(n)}$ 이다.

위 정리에서의 확률 값은 공개키 n 의 비트 길이에서 무시될 수 있는 수이다. 이것은 개선된 Paillier 방식의 안전성을 보장해 주는 중요한 사실이다.

3.1. 개선된 Paillier 암호 방식의 안전성

정리3.2 만약 공개키 g가 단지 공개된 합성수 n에 의해서만 생성될 수 있다면 G_{M-Pai}에 대하여 CCRP를 공격할 수 있다와 필요충분조건은 n을 소인수분해 할 수 있는 것이다. λ을 이용하면 합성수 n 은 소인수분해 된다. 이는 Paillier 방식에서의 **정리 2.7**과 다르게 서로 동치 관계가 성립한다.

따름정리3.3 공개키 g가 단지 공개된 합성수 n에 의해서만 생성되어질 수 있다면 개선된 Paillier 방식이 일방향성이 될 필요충분조건은 n을 소인수분해하는 것만큼 다루기 어렵다.

정리3.4 개선된 Paillier 방식의 어의적 안전성은 그 방식에 따라 DCRP를 공격하는 것만큼 어렵다.

4. 선택적 암호문 공격(Chosen Ciphertext Attack)

개선된 Paillier 암호 방식에 대한 선택적 암호문 공격 (CCA)을 살펴 보겠다. 제안될 개선된 Paillier 방식에 대한 CCA는 합성수 n 을 소인수분해 한다.

개선된 Paillier 방식에 대한 CCA는 다음과 같이 적용된다. 우선 공개키 g 를 $g+n$ 으로 바꾸고, 공개키 $g+n$ 과 임의의 정수 $h \in Z_n$ 을 이용하여 평문 m을 암호화 한다. 이때, 공격자는 복호화 알고리즘으로부터 $L((g+n)^\lambda, \mod n^2)$을 주는 비밀키 λ를 복구할 수 있다. 따라서, 합성수 n 은 소인수분해 된다. CCA는 다음과 같이 요약 된다.

[암호문의 생성]

1. 임의의 정수 $h \in Z_n$ 을 선택한다.
2. 공개키 g를 $g+n$으로 바꾼다.
3. $c = (g+n)^m h^n \mod n^2$ 을 계산한다.

[복호화 알고리즘]

$m' = L(c^\lambda)$.

[n 의 소인수분해]

1. $\lambda = g(m' m^{-1} - 1) \mod n$ 을 계산한다.
2. λ 를 이용하여 n을 소인수분해 한다.

정리 4.1 위의 선택적 암호문 공격(CCA)은 합성수 n 을 소인수분해 한다.

G_{M-Pai} 는 특별히 선택되는 공개키이므로 개선된 Paillier 방식에 대한 선택적 암호문 공격(CCA)은 효과적이다. 공격자는 키 g 가 조건 $g^\lambda = 1 + n \mod n^2$ 을 만족한다는 것을 안다. 이와 반대로, Paillier 방식에서의 공개키 g 는 그런 조건을 만족하지 않고, 알려지지 않은 임의의 정수 $r \in Z_n$ 에 대하여 $g^\lambda = 1 + rn \mod n^2$ 을 만족한다. 공격자들은 비밀키 λ 뿐만 아니라 임의의 정수 r 도 추측해야 한다. 우리는 CCA는 Paillier 방식에는 적용될 수 없음을 안다. 여기서 개선된 Paillier 방식과 원래의 Paillier 방식과의 안전성의 틈이 생긴다.

5. Paillier방식과 개선된 Paillier방식의 비교,검토

Paillier 방식에서는 n의 정보만 있으면 $g = 1 + n$ 또는 Z_{n^2}의 임의의 원소로 공개키 g를 선택할 수 있다. 그러나 개선된 Paillier 방식에서 $g^\lambda = 1 + n \mod n^2$ 을 만족하는 g를 선택할 확률은 매우 작아 공개키 n 의 길이에서 무시될 수 있다. 이는 개선된 Paillier 방식의 안전성을 보장해 주는 중요한 사실이다. 더구나, 우리는 공개키를 생성할 수 있는 알고리즘이 합성수 n을 소인수분해 할 수 있다는 것을 증명하였으므로

	Paillier 방식	개선된 Paillier 방식
공개키 g	$n \mid ord_{n^2}(g)$ 인 Z_{n^2}의 원소	$g^{\lambda}=1+n \mod n^2$ 인 $Z^*_{n^2}$의 원소
g의 선택 확률	$1-\frac{1}{n}$	$\frac{1}{\phi(n)}$
g의 생성	Z_{n^2} 의 임의의 원소 또는 $g=1+n$	g의 생성은 n의 소인수분해만큼 어렵다
m의 암호화	$c=g^m h^n, \mod n$	$c=g^m h^n, \mod n^2$
c의 복호화	$m=L(c^{\lambda} \mod n$	$m=L(c^{\lambda} \mod n^2)$, 복호화 과정에서 매우 효율적
CCRP	n의 소인수분해와 충분조건	n의 소인수분해와 필요충분조건
일방향성	CCRP 공격과 충분조건	n의 소인수분해와 필요충분조건
어의적 안전성	Paillier 방식에 대한 DCRP와 충분조건	개선된 Paillier 방식에 대한 DCRP와 충분조건
CCA	해당 없음	n을 소인수분해

개선된 Paillier 방식에서의 공개키들은 n의 소인수분해를 알지 못하고는 생성될 수 없다. 한편, 개선된 Paillier 방식에서는 특별히 $g^{\lambda}=1+n \mod n^2$을 만족하는 g를 선택하였기 때문에 복호화 과정에서 $L(g^{\lambda} \mod n^2)=\frac{g^{\lambda}-1}{n}=1, \mod n^2$이므로 역수를 취할 필요가 없다. 이는 복호화 시에 계산량을 크게 줄일 수 있게 하여 다량의 암호문의 처리에 매우 효율적이다. CCRP와 일방향성의 관계에서 볼 때, Paillier 방식보다 개선된 Paillier 방식에서 일방향성이 잘 보장된다는 것을 알 수 있다. 한편, 개선된 Paillier 방식에서 어의적 안전성에 대하여 DCRP와 필요조건이 되는 것을 보이는 것은 남겨진 문제이다. 우리는 개선된 Paillier 방식에 대한 선택적 암호문 공격(CCA)을 제안했는데, 이 CCA는 복호화 알고리즘에 대한 단지 한번의 추측으로 생성될 수 있다. 그러나 Paillier방식에서는 비밀키 λ와 임의의 정수도 추측해야하므로 CCA는 적용되지 않는다. 따라서, 개선된 Paillier 방식에서 원시원소의 안전성을 주의해야한다.

6. 결론

우리는 현재 암호 알고리즘 연구에서, 가장 활발히 연구되고 있는 Paillier 암호 방식에 대하여 그 내용과 안전성에 대하여 자세히 분석하였다. Paillier는 합성잉여류 문제가 풀기 어려운 것에 기반을 두어 Paillier 암호 방식을 제안하였는데, 이는 일방향성과 어의적 안전성을 갖는다는 것을 증명해 보았다. 우리는 또한 최덕환, 원동호[1] 등에 의해 제안된, 개선된 Paillier 방식을 분석해 보았고, 그들이 증명하지 않은 안전성에 관한 몇 가지를 조사해 보았다. 첫째, 공개키 g가 단지 공개 정보 n에 의해서만 생성되어질 수 있다면 개선된 Paillier 방식의 일방향성은 n을 소인수분해하는 것과 동치 조건임을 보였다. 둘째, 공개키를 생성할 수 있는 알고리즘이 합성수 n을 소인수분해 할 수 있다는 것을 증명했다. 따라서 Paillier 방식의 공개키들은 단지 공개된 합성수 n의 정보로부터만 생성될 수 있었으나, 개선된 Paillier 방식에서의 공개키들은 n의 소인수분해를 알지 못하고는 생성될 수 없다. 셋째로, 우리는 개선된 Paillier 방식에 대한 선택적 암호문 공격을 제안했다. 이 CCA는 복호화 알고리즘에 대한 단지 한번의 추측으로부터 생성될 수 있다. 이런 공격은 Paillier 방식에 대하여는 알려져 있지 않았다. 이들 분석을 기초로 하여, 우리는 Paillier 방식과 개선된 Paillier 방식의 효율성 및 안전성을 비교해 보았다.

참고문헌

[1]D. H. Choi, S. Choi, and D. Won, "Improvement of probabilistic public-key Cryptosystem using discret logarithm", ICISC 2001, LNCS 2288, pp.72-80, 2002.

[2] W. Diffie, and M. Hellman, "New directions in cryptography", IEEE Transactions on Information theory, Vol. IT22, pp.664-654, 1976.

[3] I. Damgard, and M. Jurik, "A generalization, a simplication and some applications of Paillier's probabilistic public-key system", PKC2001, LNCS 1992, pp.119-136, 2001.

[4] S. Galbraith, "Elliptic curve Paillier schemes", to appear in Journal of Cryptology, 2001.

[5] P. Paillier, "public-key Cryptosystem based on composite degree residuosity classes", Eurocrypt'98, LNCS 1592, pp 223-238, 1999.

[6] P. Paillier and D. Poincheval, "Efficient public key cryptosystems probably secure against active adversaries", Asiacrypt'99, LNCS1716, pp.165-179, 1999.