Okamoto-Uchiyama 확률 공개키 암호 방식의 효율성 개선

(Improvement of Okamoto-Uchiyama Probabilistic Public Key Cryptosystem)

최 덕 환 † 김 현 주 †† 최 승 복 ††† 원 동 호 ††††

(Dug-Hwan Choi) (Hyun-jue Kim) (Seungbok Choi) (Dong-ho Won)

요 약 본 논문은 Okamoto와 Uchiyama가 이산대수 함수만으로 일방향함수를 정의하여 제안한 새로운 확률 공개키 암호 방식을 개선하였다. 평문은 이들 두 이산대수 함수의 모듈라 곱으로부터 구할 수 있는데 두 함수 값 중에서 하나는 주어진 공개키에 종속된 고정된 값을 가진다. 고정된 함수 값이 단위원 1을 갖는 정선된 공개키에 의해 개선이 이루어진다. 왜냐하면 복호화 할 때 계산량을 줄일 수 있기 때문이다. 또한 이러한 성질을 충족하는 공개키를 얻을 수 있는 구체적 방법도 제시한다.

키워드 : 확률 공개키 암호 방식, 이산 대수, 어의적 안전성, p-Sylow 부분군

Abstract We improve a new probabilistic public key cryptosystem, in which the one way function was defined only on the discrete logarithmic functions, proposed by Okamoto and Uchiyama. The plaintexts are calculated from the modular product of two these functions, one of which has a fixed value depending on a given public key. The improvement is achieved by a well-chosen public key assuming an unit element 1 as the fixed function value. Because it is possible to reduce the number of operations at the decryption. Also the concrete method for a public key of our improved scheme is suggested.

Key words : probabilistic public key cryptosystem, discrete logarithm, semantic security, p-Sylow subgroup

1. 서 론

관용 암호 방식에서의 키 관리 문제 등을 해결하기 위해 1976년 Diffie와 Hellman은 암호화키는 공개하고 복호화 키만 비밀로 유지하는 공개키 암호 방식의 개념을 제안하였다[1]. 이후, 소인수 분해 문제나 이산대수 문제에 기반한 여러 공개키 암호 시스템들이 제안되어왔다. 대표적인 것으로 유한 체상에 방정식의 해를 찾는 방법과 인수분해 문제의 어려움을 배합한 RSA-Rabine 방식이 있다. 또한 유한 교환 군에서 이산대수가 교환 법칙을 만족하는 성질과 이산대수 문제가 어렵다는 사실을 이용한 Diffe-Hellman 방식도 대표적인 방식이다. 이외에도 여러 가지 많은 방식들이 제안되었지만 효용성이나 안전성의 문제를 갖고 있기 때문에, 실용적 관점에서 RSA-Rabine과 Diffe-Hellman의 제안만이 여러 분야에 걸쳐서 사용되고 있다.

그러나 Rabine의 방식[2]과 그의 변형된 공개키 암호 방식들은 수동적 공격에 대하여 확률론적으로 안전하다고 알려져 있지만, 암호문으로부터 평문의 어떠한 부분 정보도 유출되지 않는다는 보장을 할 수가 없으며 암호 방식의 비도도 증명되지 않았다는 문제점을 가지고 있다. 이러한 문제를 해결하기 위해 Goldwasser와 Micali는 이차잉여 문제에 기반한 확률 공개키 암호 방식(probabilistic public key cryptosystem)[3]을 제안하였다. 또한 이들은 *어의적 안전성*(semantic security)이

† 비 회 원 : 성균관대학교 전기전자 및 컴퓨터공학과 교수
dchoi@dosan.skku.ac.kr
†† 학생회원 : 성균관대학교 전기전자 및 컴퓨터공학과
hjkim@dosan.skku.ac.kr
††† 비 회 원 : (주)퓨처시스템 암호체계센터 연구원
sbchoi@future.co.kr
†††† 종신회원 : 성균관대학교 전기전자 및 컴퓨터공학부 교수
dhwon@simsan.skku.ac.kr
논문접수 : 2001년 11월 30일
심사완료 : 2002년 5월 8일

라는 새로운 안전성 개념을 소개하여 암호 알고리즘의 안전성을 이론적으로 증명하였다. 어의적 안전성은 IND(Indistinguishability of Encryption)라고도 불리운다. Dolev와 Dwork 그리고 Naor[4]는 *조작불가능성*(non-malleability)이라는 또다른 안전성 개념을 제시하였다. 이러한 두 가지의 안전성 개념들은 어떠한 공격자 유형에 대해서도 조작불가능성이 어의적 안전성을 의미한다는 점에서 서로 연관되어있다[5].

최근 Okamoto와 Uchiyama는 RSA-Rabin이나 Diffe-Hellman등과 같은 앞서 제시된 공개키 암호 방식과 전혀 다른 덫문 함수를 제시하였다. p와 q가 소수이고 $n=p^2q$일 때, Okamoto-Uchiyama (O-U) 방식[6]은 Z_n의 *p-실로우 부분 군*(p-Sylow subgroup)에서 정의되는 이산대수 함수를 이용하여 새로운 확률 암호 방식을 제안하였다. 이 방식은 n의 소인수 분해의 어려움에 기초하며, *p-부분 군 가정*(p-subgroup assumption)[6] 하에서 IND-CPA(Indistinguishability of Encryption-Chosen Plaintext Attack)를 만족하지만 조작불가능성은 만족하지 않는다. 하지만 EPOC-3[7]를 이용하면 *조작 가능한*(Malleable) 방식을 조작 불가능한 방식으로 바꿀 수 있다. 또한 Paillier[8]도 새로운 확률 암호 방식을 제안하였는데 이것은 두 개의 소수의 곱으로 이루어진 합성수에 대한 *합성수 잉여류*(composite residuosity class)에 기반을 두었다. 이 방식이 일방향 함수라는 사실과 어의적 안정성을 충족한다는 것이 증명되었다. 조작불가능성을 만족시키지 않지만 [9]에 의해 조작 불가능하게 변환하는 것이 가능하다.

본 논문에서는 공개키를 신중하게 선택한다면 O-U 방식의 안전성 수준을 낮추지 않고서도 복호화 과정에서 하나의 모듈라곱을 제외한 체로 평문을 얻음으로써 계산 양을 줄일 수 있음을 발견하였다. 따라서 제안한 방식은 내용이 많은 메시지의 경우 O-U 방식보다도 더 빠른 복호화 속도를 낼 수 있다. 또한 O-U 방식상의 공개키 집합의 원소를 취함으로서 IND-CPA 안전성을 가지며 일방향성을 만족시킨다.

본 논문의 구성은 다음과 같다. 서론에 이어 2장에서는 O-U 방식을 고찰하고, 3장에서는 개선된 새로운 알고리즘을 제안하며, 4장에서는 제안된 방식의 성질을 설명하고, 5장에서는 결론을 도출하고자 한다.

2. O-U 확률 공개키 암호 방식

O-U 방식과 그 성질들을 소개하고자 한다.

2.1 O-U 방식에대한 고찰

가환 환 $(Z_n,+,\cdot)$위에서 곱셈 군 $(Z^*_{p^2},\cdot)$을 이용한 공개키 암호 방식이다. 이것은 $(Z^*_{p^2},\cdot)$의 p-실로우 부분 군에서 정의된 이산대수 함수 L에 의거한다.

홀수인 소수 p에 대하여

$\Gamma=\{x\in Z^*_{p^2} \mid x\equiv 1 \mod p\}$는 $(Z^*_{p^2},\cdot)$에서의 p-실로우 부분 군이다.

$$L:(\Gamma,\cdot)\to(Z_p,+);\ x\mapsto \frac{x-1}{p}$$

이라고 정의된 함수 L은 모든 $a,b\in\Gamma$에 대하여 조건 $L(a\cdot b)\equiv L(a)+L(b) \mod p$을 만족하는 동형사상이다.

만약에 $x\in\Gamma$와 $m\in Z_p$에 대하여 $y=x^m \mod p^2$이고 $L(x)\neq 0 \mod p$이라면 다음의 식이 성립한다.

$$m=\frac{L(y)}{L(x)} \mod p$$

g를 $(Z^*_{p^2},\cdot)$의 생성자라고 할 때, $g^{p-1}\in\Gamma$이므로 $g^{p-1}=1+pr \mod p^2$인 $r\in Z^*_p$가 존재한다.

$$L(g^{p-1})=\frac{(1+pr)-1}{p}=r \mod p.$$

그러므로 $L(g^*)\neq 0 \mod p$을 만족하는 $g^*=g^{p-1} \mod p^2$를 얻는다.

[O-U 방식]

n은 소수 p의 제곱과 소수 q의 곱 $(n=p^2q)$이다. 단, $|p|=|q|=k$이다.

$g_p=g^{p-1} \mod p^2$의 위수가 p가 되는 Z^*_n내의 원소 g를 임의로 선택하고 $h=g^n \mod n$이라고 놓는다.

[공개키] (n, g, h, k)

[비밀키] (p, q)

[암호화] m을 평문이라고 놓는다. 이때 m의 범위는 $0<m<2^{k-1}$이다. Z_n의 원소 r을 균일하게 선택한다. 암호문 C는 다음과 같다.

$$C=g^m h^r \mod n$$

[복호화] $C_p=C^{p-1} \mod p^2$일 때 평문은 다음과 같다.

$$m=\frac{L(C_p)}{L(g_p)} \mod p$$

2.2 O-U 방식에 대한 특징

제시된 방식은 실제적이고 provably secure하며 다음과 같은 성질을 갖는다.

1) 제시된 방식은 새로운 것으로 구체적인 유한 부분 군에서 이산대수 함수를 이용하였다.
2) 이것은 확률 암호화 방식이다.
3) 암호화 방식의 일 방향성은 수동적 공격자에 대해 $n=p^2q$를 인수분해 하는 것이 어려운 만큼 안전

하다. 위에서 제시된 방식의 안전성에 관한 증명은 결국 하나의 평문이 임의로 여러 가지 암호문으로 암호화되어질 수 있지만 하나의 암호문은 유일하게 복호화된다는 사실을 이용한 것이다.

4) $p-$ 부분 군 가정이란 r과 r'이 Z_n에서 균일하고 독립적으로 선택될 때 $E(0,r)=h^r \bmod n$과 $E(1,r')=g\,h^{r'} \bmod n$의 계산 결과를 구분할 수 없다는 것이다. 만일 이러한 $p-$ 부분 군 가정이 참 이라면 O-U 방식은 어의적 안전성을 만족하는 것이다.

5) 공개키 암호 방식을 사용하는 가장 실제적인 환경하에서 위에서 제시된 방식의 암호화와 복호화 속도는 타원 곡선 암호 방식보다 약 두 배정도 느리다. RSA방식과 비교할 때 제시된 방식이 암호화 속도는 RSA보다 느리지만 복호화 속도는 RSA보다 더 빠르다.

6) 다음과 같은 준 동형 사상의 성질을 갖는다: 만일 $m_0+m_1<p$라면,

$$E(m_0,r_0)E(m_1,r_1) \bmod n = E(m_0+m_1,r_3)$$

을 만족한다. 이러한 성질은 전자 투표나 다른 암호 방식 프로토콜에 사용된다.

7) 비밀 키를 모르는 사람조차 평문 m을 유지하면서 암호문 $C=E(m,r)$을 다른 암호문 $C'=Ch^{r'} \bmod n$으로 바꿀 수 있고 암호문 C와 C' 사이에 관계는 감출 수 있다.

8) 제시된 방식은 IND-CPA를 만족한다.

위에서 제시된 방식은 능동적 공격자에게 취약하다. 하지만 Bellare-Rogaway의 OAEP와 유사한 방법으로 능동적 공격자에게 안전한 방식으로 수정할 수 있다.

제시된 방식의 6)과 7)의 성질 때문에 조작불가능성의 관점에서 취약하다. EPOC-3를 이용하면 이러한 취약점을 극복할 수 있다.

비록 $n=p^2q$가 $n=pq$보다 인수분해하는데 더 수월한 지는 알려져있지 않더라도 $n=p^2q$을 인수분해하는 특별한 알고리즘들이 연구되었다.

3. 제안하는 암호 방식

Okamoto와 Uchiyama 방식을 개선한 좀 더 효율적인 암호 방식을 제안한다. O-U 방식에서 제안된 방법으로 복호화할 때 계산상의 부하를 줄일 수 있도록 하기 위하여 제안된 공개키가 특정한 성질을 갖는 것들로 선택함으로써 효율성을 증가시켰다.

3.1 공개키

$(Z_{p^2},+,\cdot)$은 단위원 1을 갖는 환이라고 하자. $(Z_p,+,\cdot)$도 또한 단위원 1을 갖는 환이라고 한다. α와 β가 Z_p의 원소일 때 Z_{p^2}의 임의의 원소 z가 $\alpha p+\beta$로 표현되는 것은 자명하다.

정리 1

$z\in Z_{p^2}^*$ 일 때 $z \bmod p$는 Z_p^*의 원소이며 그 역도 또한 성립한다.

증명

($\Rightarrow$) z는 $Z_{p^2}^*$의 원소 이면서 $z \bmod p$가 0 이라고 하자. 이때 $\gcd(z,\ p^2)$은 p 이다. 왜냐하면 z는 αp로 표현된다. 이때 z가 $Z_{p^2}^*$의 원소라는 가정에 모순이 발생한다.

($\Leftarrow$) $z\notin Z_{p^2}^*$ 이고 $z \bmod p$가 Z_p^*의 원소라고 하자. $z\notin Z_{p^2}^*$ 이라는 가정에 의해 p는 소수이므로 $\gcd(z,\ p^2)$은 p 혹은 p^2이므로 $z \bmod p=0\notin Z_p^*$을 만족한다. 이것은 모순이다.

두 개의 집합 사이에 함수 Φ를 다음과 같이 정의한다.

$$\Phi : Z_p\times Z_p^* \to Z_{p^2}^*$$
$$;\ (\alpha,\beta)\ \mapsto \alpha p+\beta.$$

이때 $Z_p\times Z_p^*$과 $Z_{p^2}^*$은 동일한 위수 $p(p-1)$을 갖는 집합들 이다.

함수 $\Phi : Z_p\times Z_p^* \to Z_{p^2}^*$는 전단사 함수이다. (α,β)와 (α',β')이 $Z_p\times Z_p^*$의 원소들이고 $(\alpha,\beta)\neq(\alpha',\beta')$라고 하면 $\alpha p+\beta\neq\alpha' p+\beta'$를 보이는 것은 자명하다. 그러므로 함수 Φ는 단사이다. 이때 $Z_p\times Z_p^*$과 $Z_{p^2}^*$의 위수가 유한하기 때문에 함수 Φ가 전사임은 쉽게 보여진다. 그러므로 $Z_{p^2}^*$의 모든 원소들은 $\alpha p+\beta$라고 표현되고 이때 $\alpha\in Z_p$와 $\beta\in Z_p^*$임을 만족해야 한다.

환 $(Z_{p^2},+,\cdot)$상의 원소 c가 집합 $Z_p^*=\{1,2,\ldots,p-1\}\subset Z_{p^2}^*$의 원소라고 하자. 이때 $c^{p-1}\equiv 1 \bmod p$이므로 $c^{p-1} \bmod p^2$은 Γ의 원소이다. 따라서

$$(\ L(c^{p-1} \bmod p^2)-1\ )\ c \bmod p$$

는 $(Z_p,+,\cdot)$에 속하는 원소이다. 이때 $b\equiv(L(c^{p-1} \bmod p^2)-1)\,c \bmod p$이라고 하면, 정리 1에 의하여 모든 $c\in Z_p^*$에 대해 $g=bp+c$는 $Z_{p^2}^*$에 속한다.

만일 $c=1\in Z_p^*$라면 $b=p-1\in Z_p$이다. 왜냐하면

$$L(c^{p-1}) = \frac{(1+0\cdot p)-1}{p} = 0 \bmod p$$

이기 때문이다. 그러므로 $g\in Z_{p^2}^*$는 $(p-1)p+1$이라는 값을 갖는다. $c\in Z_p^*$가 $L(c^{p-1} \bmod p^2)=1$을 만

족할 때 $g=0\cdot p+c=c$가 된다. 그러므로 각각의 주어진 $c\in Z_p^*$에대해 상응하는 서로 다른 $g\in Z_{p^2}^*$를 구할 수 있다. 따라서 이러한 g의 형식을 갖는 것들은 $p-1$개가 주어질 수 있다. 왜냐하면 각각의 $g\in Z_{p^2}^*$는 $c\in Z_p^*$의 선택에 달려있으므로 요구되어지는 $g\in Z_{p^2}^*$의 갯수는 Z_p^*의 위수 $p-1$과 같다.

정리 2

$c\in Z_p^*$이고 $b\equiv(L(c^{p-1}\bmod p^2)-1)c\bmod p\in Z_p$를 만족한다고 하자. $Z_{p^2}^*$의 원소 g가 $bp+c$라는 형태를 갖는다고 하자. 이때 $g^{p-1}\equiv 1+p \bmod p^2$ 이다.

증명

가정에 의해서, c는 Z_p^*의 원소이며 b는 c의 값에 영향을 받는다. g는 $Z_{p^2}^*$의 원소이고 집합 $Z_{p^2}^*$는 가환 환 $(Z_{p^2},+,\cdot)$의 부분 집합으로 간주할 수 있으므로 다음의 식은 환의 이항정리에 의해 성립함을 보일 수 있다.

$$\begin{aligned}(bp+c)^{p-1} &\equiv c^{p-1}+(p-1)bc^{p-2}p \bmod p^2\\ &\equiv 1+\left(\frac{c^{p-1}-1}{p} \bmod p\right)p+(p-1)bc^{p-2}p \bmod p^2\\ &\equiv 1+\left(\frac{c^{p-1}-1}{p}-bc^{p-2} \bmod p\right)p \bmod p^2\\ &\equiv 1+p \bmod p^2.\end{aligned}$$

마지막 단계가 성립하는 이유는 다음과 같다.

$$\begin{aligned}\frac{c^{p-1}-1}{p}-bc^{p-2} &\equiv \frac{c^{p-1}-1}{p}-\left(\frac{c^{p-1}-1}{p}-1\right)c^{p-1} \bmod p\\ &\equiv \frac{c^{p-1}-1}{p}-\frac{c^{p-1}-1}{p}c^{p-1}+c^{p-1} \bmod p\\ &\equiv \frac{c^{p-1}-1}{p}(1-c^{p-1})+c^{p-1} \bmod p\\ &\equiv 1 \bmod p\end{aligned}$$

왜냐하면 Z_p^*의 임의의 원소 c에 대하여, $c^{p-1}\equiv 1 \bmod p$ 이기 때문이다.

정리 2에 의해서, $L(g_p)=L(g^{p-1} \bmod p^2)=1$이다. 따라서 $0\le m<p$의 범위를 만족하는 평문 m은 정리 2에서 주어진 g를 이용하면 다음과 같은 방법으로 구할 수 있다.

$$\begin{aligned}m &= L(1+mp \bmod p^2) \bmod p\\ &= L((g^m h^r)^{p-1} \bmod p^2) \bmod p\end{aligned}$$

이러한 사실을 우리는 효율적인 복호화를 위하여 사용하고자 한다.

환동형사상에 의해 우리가 제안하고자 하는 방식의 공개키 $g\in Z_{p^2q}^*$를 구할 수 있다. z_1에 대해 $p-1$개의 원소가 존재하고 z_2에 대해서는 q개의 원소가 존재할 수 있으므로 결국 우리가 제안하고자 하는 방식은 $(p-1)q$개의 공개키가 존재할 수 있다.

3.2 제안하는 방식

이산대수 함수 L에 기초하고 O-U 방식을 개선한 구체적인 방식을 소개하고자 한다.

두 개의 큰 소수 p와 $q(|p|=|q|=k)$를 선택하고, $n=p^2q$라고 하자. $g\in Z_{p^2q}^*$는 $L(g_p)=L(g^{p-1} \bmod p^2)=1$을 만족하는 것이다. 이때 $\gcd(p,q-1)=1$와 $\gcd(q,p-1)=1$을 만족한다.

[O-U 방식의 개선]

Z_p^*의 원소 c와 방정식 $b\equiv\left(\frac{c^{p-1}-1}{p}-1\right)c \bmod p$을 만족하는 Z_p의 원소를 b라고 하자. 방정식 $g=bp+c \bmod p^2$를 만족하는 Z_n^*의 원소를 g라고 한다. $h\equiv g^n \bmod n$이라고 정의한다.

[공개키] (n, g, h, k)

[비밀키] (p, q)

[암호화] m을 평문이라고 놓는다. 이때 m의 범위는 $0<m<2^{k-1}$이다. Z_n의 원소 r을 균등하게 선택한다. 암호문 C는 다음과 같다.

$$C\equiv g^m h^r \bmod n$$

[복호화] $C_p\equiv C^{p-1} \bmod p^2$일 때 평문은 다음과 같이 얻는다.

$$m=L(C_p)$$

4. 제안하는 방식의 특징

제안한 스킴은 O-U 방식의 특성과 마찬가지로 일 방향성을 만족하고 어의적 안정성을 갖는다. 더욱이 효율성 측면에서는 O-U 방식보다 더 낳은 결과를 갖는다.

일방향성

정리 3

제안하는 방식이 일 방향성을 갖는다는 이야기는 $n=p^2q$의 소인수분해가 어렵다는 말과 동치이다.

증명

($\Rightarrow$) 제안한 방식에 대한 반대과정을 실행할 수 있는 오라클이 존재한다고 가정하자. 즉 주어진 암호문으로부터 평문을 계산할 수 있다고 하자. η는 $\eta\ge 2^{k-1}$을 만족한다고 하고 암호문 $C=g^\eta \bmod n$가 주어지면, 오라클은 메시지 $m<2^{k-1}$을 산출한다. 그러면 $\gcd(\eta-m,n)$은 p, p^2 또는 pq가 될 것이다. 왜냐하면 $\eta\equiv m \bmod p$이기 때문이다. 그러므로 n을 소인수분해할 수 있다.

($\Leftarrow$) $n=p^2q$의 소인수분해가 쉽다면 비밀키 (p,q)를 얻을 수 있다. 이때 주어진 암호문으로부터 평문을 계산할 수 있다. 그러므로 일 방향성을 만족하지 못한다.

IND-CPA

3.2에서 우리가 제안한 공개키는 O-U가 제안한 방식

의 공개키중에서 특별한 성질을 만족하도록 선택된 것들이다. 그리고 원래의 O-U 방식에서 복호화할 때 평문을 얻기 위한 계산에서 우리의 공개키를 선택하면 고정된 값 $L(g_p) \bmod p$가 항상 단위원 1을 가지므로 결국 우리가 제안한 방식은 O-U 방식의 특별한 유형임을 의미한다. 따라서 O-U 방식이 $p-$부분군 가정하에서 IND-CPA를 만족한다면 우리가 제안한 방식 또한 같은 가정하에서 IND-CPA 안전성을 충족하여야 한다. 왜냐하면 개선된 제안 방식이 $p-$부분군 가정하에서 IND-CPA를 만족하지 못한다고 하면 이 방식은 O-U 방식의 한가지 유형에 대해 IND-CPA를 만족시키지 못하는 것이므로 결국 O-U 방식이 IND-CPA하지 못하다는 것을 의미한다.

효율성 비교

표 1과 표 2는 각각 O-U 프로토콜과 본 논문에서 제안한 O-U방식을 개선한 프로토콜을 나타낸 것이다. 각 프로토콜에 사용된 평문의 길이가 길다고 하자. O-U 방식은 메시지를 복호화하기 위해 두 번의 모듈라멱승과 한번의 모듈라곱이 필요하지만 제안한 암호 방식은 복호화 과정에서 하나의 모듈라멱승만으로 평문을 얻음으로써 계산량을 줄였다. 따라서 O-U 방식보다도 더 빠른 복호화 속도를 낼 수 있다.

O-U 방식에서 고정된 값 $L(g_p)^{-1} \bmod p$을 미리 계산하여 복호화 속도를 줄였다고 가정하더라도 그 값이 1이 아니라면 제안한 암호방식보다 복호화 속도가 빠르지는 못하다. 왜냐하면 각각의 암호 블록 단위당 그 고정된 값을 항상 곱하여 평문을 계산하여야 하기 때문이다. 하지만 제안한 암호방식에서 공개키는 항상 $L(g_p)=1$을 만족하기 때문에 모듈라곱 만큼 연산 횟수를 개선한다. 표 3은 각 프로토콜을 이용할 때 예상되는 사용자 B의 평균 계산량을 비교한 것이다. 단, 여기서 M($|p|$)는 길이가 $|p|$인 두 숫자들의 모듈라곱에 대한 평균 계산량을 의미한다.

표 1 O-U 프로토콜

사용자 A	공개정보 g, n	사용자 B
$C=g^m h^r \mod n$	C ---------->	$C_p=C^{p-1} \mod p^2$ $g_p=g^{p-1} \mod p^2$ $m=\frac{L(C_p)}{L(g_p)} \bmod p$

표 2 제안하는 프로토콜

사용자 A	공개정보 g, n	사용자 B
$C=g^m h^r \mod n$	C ---------->	$C_p=C^{p-1} \mod p^2$ $m=L(C_p)$

표 3 사용자 B의 평균계산량

$\|p\|$	O-U 프로토콜	제안하는 프로토콜
512	768 + M(512)	768
1024	1536 + M(1024)	1536
2048	3072 + M(2048)	3072

5. 결 론

본 논문에서는 O-U 방식을 개선한 확률 공개키 암호 방식을 제안하였다. O-U 방식은 복호화를 시행할 때 암호문 C로부터 얻어진 값 $L(C_p) \in Z_p^*$와 공개키 g로부터 얻어진 값 $L(g_p) \in Z_p^*$의 곱에서 평문을 얻는다. 우리가 제시하는 방식은 O-U 방식에서 $L(g_p) = 1$을 충족하는 선별된 공개키를 취함으로서 그 공개키가 복호화 과정에서 계산량을 줄이도록 하였다. 개선된 방식은 O-U 방식의 관점에서 하나의 특별한 유형이 되므로 이것은 원래의 방식이 갖는 일방향성과 어의적 안전성을 만족시킨다. 또한 복호화시에 계산량을 줄임으로서, 개선된 방식은 많은 암호문을 처리할 때 걸리는 복호화 시간을 우리의 공개키와 다른 것을 사용했을 때보다 줄일 수 있다. 따라서 제시된 방법이 복호화할 때 효율적이다.

참 고 문 헌

[1] W. Diffe and M. Hellman, *New Direction in Cryptography* IEEE Tranctions 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, 2, pp. 270-299. 1984.

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

[5] M. Bellare, A. Desai, D. Pointcheval and P. Rogaway, *Relations Among Notions of Security*

for Public-Key Encryption Schemes Advances in cryptology-Proc. of CRYPTO'98, Lecture Notes in Computer Science, Vol. 1462, pp. 26-35, Springer-Verlag. 1998.

[6] T. Okamoto and S. Uchiyama, *A New Public-Key Cryptosystem as secure as Factoring* Proc. of EUROCRYPTO'98, pp. 309-318. 1998.

[7] T. Okamoto and D. Pointcheval, *Efficient Public-Key Encryption (ver. 3)* Submission to P1363a, available on http://grouper.ieee.org/groups/1363/submission.html. 2000.

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

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

최 덕 환

1985년 2월 성균관대학교 수학과(학사). 1987년 2월 성균관대학교 수학과(석사). 1992년 5월 University of Iowa 수학과(석사). 1998년 12월 Iowa State University 수학과(박사). 1999년 1월 ~ 1999년 12월 Iowa State University에서 Temporary Assistant Professor. 2000년 9월 ~ 현재 성균관대학교 전기전자 및 컴퓨터공학과 연구조교수. 관심분야는 암호이론, 부호이론, 조합론

김 현 주

1991년 2월 세명대학교 수학과(학사). 1997년 2월 서강대학교 수학과(석사). 1999년 2월 ~ 현재 성균관대학교 전기전자 및 컴퓨터공학과 박사과정 재학 중. 관심분야는 암호이론

최 승 복

1998년 8월 연세대학교 통계학과(학사). 2001년 8월 성균관대학교 전기전자 및 컴퓨터공학과(석사). 2001년 7월 ~ 현재 (주)퓨쳐시스템 암호체계센터 연구원. 관심분야는 정보보호, 암호이론, 네트워크 보안

원 동 호

성균관대학교 전자공학과(학사, 석사, 박사). 한국전자통신연구소 전임연구원. 일본동경공대 객원 연구원. 성균관대학교 교학처장, 전기전자 및 컴퓨터공학부장, 정보통신대학원장, 국무총리실 정보화추진위원회 자문위원. 한국정보보호학회 이사, 부회장, 수석부회장. 현재 성균관대학교 전기전자 및 컴퓨터공학부 교수. 한국정보보호학회 회장. 정통부지정 정보보호인증기술연구센터 센터장. 관심분야는 암호이론, 정보시스템 보안