情報保護學會論文誌
第15卷 第6號, 2005. 12

효율성과 사용자의 프라이버시가 개선된 BCP 공개키 암호시스템*

윤 택 영,[1†] 박 영 호,[2] 임 종 인[1‡]
[1]고려대학교 정보보호 대학원, [2]세종 사이버대학교

Improvement in efficiency and privacy on BCP public key cryptosystem*

Taek-Young Youn,[1†] Young-Ho Park,[2] Jong In Lim[1‡]
[1]Graduate School of Information Security(GSIS) Korea University,
[2]Sejong Cyber University

요 약

이중 복호화 기능을 제공하는 BCP 공개키 암호는 Asiacrypt '03에서 Bresson, Catalano와 Pointcheval에 의해서 처음 제안되었고, 이는 Eurocrypt '02에서 Cramer와 Shoup이 제안한 공개키 암호에 기반하고 있다. 기존의 이중 복호화 기법은 Paillier 암호에서 사용되었던 환 Z_{n^2} 위에서 설계되어 있으며, 이때 n은 두 소수 p,q의 곱 $n=pq$ 이다. 본 논문에서는 환 Z_{p^2q} 위에서 이중 복호화 기능을 제공하는 공개키 암호를 제안한다. 본 논문에서 제안하는 공개키 암호는 기존의 것보다 효율적인 암·복호화 연산을 제공한다. 그리고 이전의 이중 복호화 기법이 사용자의 프라이버시 관점에서 취약하다는 점을 보이고 사용자의 프라이버시가 보강된 이중 복호화 기능을 제공하는 공개키 암호를 제안한다.

ABSTRACT

A novel public key cryptosystem that provides a double decryption mechanism is proposed at Asiacrypt '03 by Bresson, Catalano and Pointcheval based on the scheme proposed by Cramer and Shoup at Eurocrypt '02. Previous double decryption scheme is designed based on Z_{n^2} where $n=pq$ for two primes p,q. In this paper, we propose an efficient public key scheme with double decryption mechanism based on Z_{p^2q} for two primes p,q. Our scheme is more efficient than the previous schemes. Moreover, we review the previous schemes in a privacy point of view and propose a privacy enhanced double decryption scheme.

Keywords : *public key cryptosystem, double decryption, semantic security, privacy*

Ⅰ. 서 론

공개키 암호시스템은 암호를 통해서 안전한 통신 서비스를 제공하기 위한 도구로 많은 관심을 받아왔고 많은 연구가 진행되었다. 그러므로 안전한 통신 서비스를 제공하기 위한 도구로써 유용하게 사용될 수 있는 새로운 암호를 구성하는 것은 이론적인 관점에서뿐 아니라 현실적인 관점에도 매우 중요하다.

암호를 설계할 때는 크게 안전성과 효율성을 고려한다. 안전성은 크게 일방향성(one-wayness)과 구분불능성(indistinguishablilty)의 관점을 고려한

접수일 : 2005년 9월 15일 ; 채택일 : 2005년 11월 25일
* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터 육성지원사업의 연구결과로 수행되었음
† 주저자 : taekyoung@cist.korea.ac.kr
‡ 교신저자 : jilim@cist.korea.ac.kr

다. 일방향성은 공개키 암호가 만족해야 하는 가장 기본적인 조건이지만 안전성을 보장하기 위한 충분 조건은 아니다. 근래에는 구분불능성도 공개키 암호가 만족해야 하는 기본적인 안전성의 요건으로 고려되고 있으며 [2]에서 공개키 암호가 구분불능성을 만족해야 이유를 설명하고 있다. 예를 들어, 공개키 환경에서 인증된 키 교환 프로토콜(authenticated key exchange protocol)을 구성하기 위해서는 기반하고 있는 공개키 암호는 IND-CCA2에 해당하는 안전성을 보장해야 된다. 안전성의 두 조건을 만족한다고 해도 효율적이지 않으면 현실적인 의미를 갖지 못한다. 공개키 암호의 단점은 수학적인 연산의 사용으로 인해 많은 계산량이 필요하다는 점이다. 따라서 공개키 암호를 설계함에 있어서 효율성은 안전성만큼 중요한 조건으로 고려된다. 즉, 공개키 암호는 안전성과 효율성을 모두 만족할 수 있도록 설계되어야 한다.

Cramer와 Shoup은 Eurocrypt'02에서 Paillier 암호를 기반으로 표준모델(standard model)에서 구분불능성을 만족하는 공개키 암호를 제안하였다[4]. Bresson 등은 Asiacrypt '03에서 Cramer와 Shoup이 제안한 공개키 암호를 기반으로 이중 복호화 기능을 제공하는 공개키 암호를 제안하였다[1].

기존에 제안된 이중 복호화 기법은 Paillier 암호와 동일하게 환 Z_{n^2}위에 설계되어 있다. Paillier 암호가 사용한 모듈로는 동일한 안전성을 가지는 것으로 알려진 RSA나 ElGamal 공개키 암호가 사용하는 것보다 두 배정도 큰 모듈로를 사용해야 하므로 효율성 측면에서 좋은 특성을 제공한다고 할 수 없다. 마찬가지로 Paillier 암호가 사용한 모듈로를 기반으로 설계된 기존의 이중 복호화 기능을 제공하는 공개키 암호도 효율성 측면에서는 좋은 특성을 갖지 못한다. 그러므로 이중 복호화 기능을 효율적으로 제공할 수 있는 공개키 암호의 개발은 매우 의미 있는 연구주제이다.

Bresson 등은 다음의 두 가지 상황을 동시에 해결할 수 있는 도구로써 이중 복호화 기능을 제공하는 공개키 암호를 제안하였다[1]. 첫 번째는 시스템 관리자가 사용자들의 통신 내용을 확인하고자 할 때 암호문에서 평문을 복원할 수 있는 방법을 제공하는 것이고, 두 번째는 개별 사용자들이 자신의 비밀키를 잃어버렸을 경우에도 자신의 공개키로 암호화된 암호문에서 평문에 대한 정보를 복원할 수 있는 방법을 제공하는 것이다. 두 상황을 동시에 해결하기 위해서는 마스터키(master-key)의 기능을 제공할 수 있는 구조로 설계되어야 한다. [1]에서는 관리자에게만 주어져 있는 모듈로의 인수분해 정보가 마스터키의 역할을 하도록 설계되어 있다. 그러나 이와 같은 설정에서는 관리자가 임의로 선택한 암호문에 대한 평문을 항상 복원할 수 있기 때문에 관리자에 의한 사용자의 프라이버시 침해가 우려된다. 즉, 관리자는 자신의 판단에 의해 모든 사용자의 암호문을 복호화 할 수 있기 때문에 관리자가 악의적으로 사용자의 암호문을 복호화 함으로써 해당 사용자의 프라이버시를 침해할 수 있다. 이러한 이유로 관리자에 의한 사용자의 프라이버시 침해문제를 방지하기 위해서는 관리자에게 주어진 마스터키의 권한을 제한할 수 있는 방법에 대한 연구가 필요하다.

본 논문에서는 환 Z_{p^2q} 위에서 정의된 효율적인 공개키 암호를 제안한다. 제안하는 공개키 암호는 기존의 공개키 암호가 사용한 것보다 작은 모듈로 위에서 모듈로 곱셈이나 지수승과 같은 암호학적인 연산을 수행하기 때문에 3배 효율적인 암·복호화 연산을 제공한다. 특히, 관리자의 경우에는 기존의 것보다 복호화 연산이 4배 정도 효율적이다. 또한 악의적인 관리자에 의해 발생할 수 있는 사용자의 프라이버시 침해문제를 보완할 수 있도록 구성된 이중 복호화 기능을 제공하는 공개키 암호를 제안한다.

II. 기존의 연구 내용

2.1 기존의 공개키 암호

[1]에서 Bresson 등은 Paillier 암호를 변형한 형태로 이중 복호화 기능을 제공하하는 공개키 암호를 제안하였다. [1]에서 제안된 공개키 암호를 BCP 공개키 암호라고 하자. $n=pq$을 안전한-소수 모듈로라고 하자. 즉, 두 소수 p,q는 또 다른 소수 p',q'에 대해서 $p=2p'+1$와 $q=2q'+1$의 형태로 표현된 값이라고 하자. G는 모듈로 n^2에 대한 이차 잉여류의 순환군이라고 하자. $\lambda()$는 chamichael 함수로 소수 p,q의 곱 n에 대해서 $\lambda(n)=lcm(p-1,q-1)$로 정의되는 함수이다. 그러면 $ord(G)=\lambda(n^2)/2=n\lambda(n)/2$ 이다. 위수가 n인 모든 원소는 어떤 $k\in Z_n$에 대해서 $\alpha=1+kn$으로 표현된다. BCP 공개키 암호[1]는 다음과 같이 구성된다.

키생성: 같은 크기의 두 소수 p,q를 선택하고 $n=pq$라고 하자. 임의의 수 $\alpha\in Z_{n^2}$와 $a\in[1,ord(G)]$를 선

택해서 다음을 계산한다: $g=\alpha^2 \bmod(n^2)$와 $h=g^a \bmod(n^2)$. 공개키는 (n,g,h)이고 대응되는 비밀키는 a이다. 두 소수 p,q는 마스터키로 사용되는 비밀키 정보이다.

암호화: 평문 $m\in Z_n$이 주어지면, 난수 $r\in Z_{n^2}$를 선택한다. 그러면 암호문 $C=(A,B)$는 다음과 같이 계산된다: $A=g^r \bmod(n^2)$ 이고 $B=h^r(1+mn) \bmod(n^2)$.

복호화 1: 첫 번째 복호화 방법은 ElGamal 암호와 동일하다. 비밀키 a를 알고 있는 사용자는 다음의 계산을 통해서 평문 m을 복원할 수 있다: $m=(B/A^a-1 \bmod(n^2))/n$.

복호화 2: 두 번째 복호화 방법은 두 소수 p,q를 사용해서 수행된다. [1]의 방법을 사용하면 $g^a \bmod(n^2)$와 $g^r \bmod(n^2)$에서 $a \bmod(n)$과 $r \bmod(n)$을 계산할 수 있다. $ar \bmod(G)=\gamma_1+\gamma_2 n$으로 표기하면, $\gamma_1=ar \bmod(n)$을 만족한다. 이 특성을 사용해서 다음을 계산한다:

$$D=\left(\frac{B}{g^{\gamma_1}}\right)^{\lambda(n)}=\left(\frac{(g^{mr}(1+mn))^{\lambda(n)}}{g^{\gamma_1\lambda(n)}}\right)=1+m\lambda(n)n \bmod(n^2).$$

π를 Z_n^*에서의 $\lambda(n)$의 역원이라고 하면 평문 m은 다음과 같다: $m=((D-1 \bmod(n^2))/n)\pi \bmod(n)$.

[1]에서 제안된 공개키 암호를 분석함으로써 *DLP* (discrete logarithm problem)을 푸는 방법을 제공하는 군에서는 이중 복호화 기능이 제공될 수 있음을 확인할 수 있다. [12]에서 Okamoto와 Uchiyama는 p^2q위에서 *DLP*를 풀 수 있는 특성을 기반으로 공개키 암호를 제안하였다. [12]에서 제안된 공개키 암호를 OU 공개키 암호라고 하자. 이는 이중 복호화 기능을 제공하는 공개키 암호를 설계할 수 있음을 의미하므로 OU 공개키 암호를 살펴보고자 한다.

OU 공개키 암호는 대수적 함수 L에 기반한다. $\Gamma=\{x\in Z_{p^2}^* | x\equiv 1 \bmod(p)\}$라고 하자. $x\in\Gamma$에 대해서 L은 다음과 같다: $L(x)=(x-1)/p$. $x_p=x^{p-1} \bmod(p^2)$. OU 공개키 암호[12]는 다음과 같다.

키생성: k비트의 두 소수 p,q를 선택하고 $n=p^2q$라고 하자. $ord(g^{p-1} \bmod(p^2))=p$를 만족하는 임의의 수 $g\in Z_n$를 선택한다. $h=g^n \bmod(n)$라고 하자. 공개키는 (n,g,h,k)이고 대응되는 비밀키는 (p,q)이다.

암호화: 평문 $m\in[1,2^{k-1}]$이 주어지면, 난수 $r\in Z_n$를 선택한다. 암호문 C는 다음과 같다: $C=g^m h^r \bmod(n)$.

복호화: 우선 $C_p=C^{p-1} \bmod(p^2)$와 $g_p=g^{p-1} \bmod(p^2)$를 계산한다. 그러면 평문 m은 다음과 같이 복원할 수 있다: $m=L(C_p)/L(g_p) \bmod(p)$.

2.2 구분불능성을 제공하는 일반적인 변형기법

구분불능성과 같은 안전성에 대한 개념은 [5,8]에서 처음으로 제안되었다. 그 이후에, 구분불능성과 같은 안전성을 만족하지 않는 공개키 암호를 안전하도록 변환하는 일반적인 변형기법들에 대한 연구가 많이 이루어졌다 [7,15,3,9].

기존에 알려진 일반적인 변형기법 중에서 제안하는 공개키 암호의 안전성을 높이기 위해 Kiltz와 Lee의 KL 변형기법[9]을 사용한다. 변형기법의 제안이 본 논문의 목적이 아니므로 KL 변형기법을 적용할 수 있는 조건과 변형기법의 모델에 대해서 간단히 살펴본다.

Kiltz와 Lee는 ROM(random oracle model)의 환경에서 IND-CCA2 안전성을 만족하는 공개키 암호로 변환하는 일반적인 방법을 제안하였다. 변형방법을 사용하기 위해서는 YCP(Y-computational problem) 형태의 문제를 기반으로 암호가 설계되어야 한다. [9]에서 언급된 바와 같이, RSA나 Diffie-Hellman과 같이 잘 알려진 난제들이 YCP 형태의 문제이다. 본 논문에서는 Diffie-Hellman 문제를 기반으로 설계되어 있으므로 YCP 에 기반해야 한다는 조건을 만족하므로 KL 변형기법을 적용함으로써 안전성을 높일 수 있다.

Kiltz와 Lee가 제시한 일반적인 변형모델은 다음과 같이 구성된다. E^s는 비대칭 암호이고 해쉬함수 G에 대해서 $\kappa=G(f_2(r))$일 때, 변형된 공개키 암호는 다음과 같다: $E_{pk}(m,r)=(f_1(r),E_k^s(m))$. IND-CPA 관점에서 안전한 공개키 암호에 KL 변형기법을 적용하여 IND-CCA2 관점에서 안전한 공개키 암호를 구성하였다. IND-CPA에 안전하게 변형된 공개키 암호를 구성한 것과 동일하게 E^s를 비대칭 암호라고 하고, G,H는 해쉬함수라고 하며 $\kappa=G(f_2(H(m\|r)))$

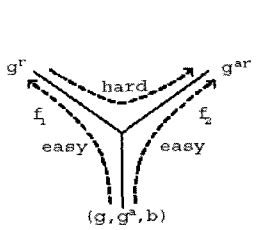


그림 1. YCP: Diffie-Hellman 의 경우

라고 하자. 변환된 공개키 암호는 다음과 같다:

$$E_{pk}(m,r)=(f_1(H(m\|r)),E_k^s(m\|r)).$$

Ⅲ. Z_{p^2q}에서 정의되는 *DHP*와 *DLP*

DHP[6]는 지금까지도 많은 암호를 구성하기 위한 도구로 사용되고 있는 암호학적 프리미티브이다. 제안하는 공개키 암호는 본 논문에서 $p-DHP$라고 정의하는 일종의 *DHP*를 기반으로 설계되어 있다.

$P(k)$를 k 비트의 소수로 구성된 집합이라고 하자. 두 소수 p,q를 $P(k)$에서 선택하고, 지금부터 $n=p^2q$라고 하자. $G_p=\{x\in Z_n|ord(x^{p-1} \bmod (p^2))=p\}$라고 하자. 그러면 $p-DHP$에 대한 정의는 다음과 같다.

정의 1. $p-DHP$는 다음과 같이 정의된다. : g를 G_p의 원소라고 하자. $[1,p-1]$ 범위의 a,b에 대해서 g^a와 g^b가 주어졌을 때, g^{ab}를 찾는 것을 $p-DHP$이라고 한다.

Z_{p^2q}에서의 *DHP*의 어려움과 일반적으로 많이 사용하는 RSA 모듈로에서의 *DHP*의 어려운 정도의 차이에 대해서는 알려지지 않았다. [10]의 분석에서 알 수 있듯이, 생성자의 위수가 소수인 부분군에 대해서 *DHP*를 구성하면 안전하지 않은 것으로 알려져 있지만 생성자의 위수가 소수가 아닌 부분군에 대해서 *DHP*를 구성하면 기존에 알려져 있는 합성수 모듈로위에 구성된 *DHP*에 대한 공격은 적용되지 않는다는 것을 알 수 있다. 그리고 모듈로 p^2q위에서 정의된 *DHP*에 대한 공격은 알려지지 않았고 기존의 다른 공격방법들이 적용되지 않기 때문에 $p-DHP$는 충분히 큰 변수의 선택을 가정할 경우에 안전하다고 할 수 있다. 지수의 크기인 k는 소수 p에 대해서 Z_p에서 정의된 *DHP*에서 160비트의 지수가 사용되는 것을 고려하면 충분한 안전성을 보장할 수 있다.

Conjecture 1. k가 충분히 큰 값으로 선택되면, 모든 PPT(probabilistic polynomial time) 알고리즘 A에 대해서 다음을 만족하는 함수 $negl(k)$이 존재한다.

$$\Pr\left[A(n,A,B)=C \;\middle|\; \begin{array}{c} p,q\leftarrow P(k);n=p^2q; \\ g\leftarrow G_p;\ a,b\leftarrow[1,p-1]; \\ A=g^a \bmod n;\ B=g^b \bmod n; \\ C=g^{ab} \bmod n; \end{array}\right]\le negl(k)$$

지금부터 Z_n^*에서 정의되는 *DLP*인 $p-DLP$를 정의하고 $p-DLP$와 n을 인수분해 하는 것이 동치라는 것을 보이도록 한다.

정의 2. $p-DLP$는 다음과 같이 정의된다: g를 G_p의 원소라고 하자. $[1,p-1]$ 범위의 a에 대해서 g^a가 주어졌을 때, $a \bmod (p)$를 찾는 것을 $p-DLP$이라고 한다.

정리 1. $p-DLP$를 푸는 것은 n을 인수분해 하는 것과 동치이다.

증명) ($\Rightarrow$) n을 인수분해 할 수 있다고 가정하자. $A=g^a \bmod (n)$이 *DLP*에 대한 문제로 주어졌다고 하자. n에 대한 인수분해정보가 주어져 있으므로 다음과 같이 $a \bmod (p)$를 계산할 수 있다:

$$a'=a \bmod (p)=L(A_p)/L(g_p) \bmod (p).$$

($\Leftarrow$) $p-DLP$를 푸는 알고리즘 A가 있다고 가정하자. 임의의 $k\in[2^{k+1},n]$를 선택해서 $g^k \bmod (n)$을 계산한다. A는 $g^k \bmod (n)$에 대해서 $k'=k \bmod (p)$를 계산해준다. $k>p$이기 때문에 $k'\neq k$ 이므로 다음의 식을 통해서 n을 인수분해 할 수 있다: $\gcd(n,k-k')=p$.

Remark 1. 정리 1에서 $p-DLP$를 푸는 것이 n을 인수분해 하는 것과 동치임을 보였다. OU 공개키 암호가 n을 인수분해 하는 것과 동치임이 증명되었으므로[12] $p-DLP$를 푸는 것의 어려움은 OU 공개키 암호의 안전성과 동치이다. 결과적으로 다음과 같은 관계가 만족한다: $p-DLP \Leftrightarrow n$의 인수분해 $\Leftrightarrow$ OU 공개키 암호의 일방향성

Ⅳ. 관리자에 대한 사용자의 프라이버시

일반적으로, 악의적인 관리자는 일반 공격자들과 분리되어 다루어지지 않는다. 그러나 경우에 따라서 시스템 관리자는 다른 행위 주체들보다 많은 능력을 가지고 있다. 그러므로 악의적인 관리자는 일반 공격자들과 나누어 고려해야할 필요가 있다. 이중 복호화 기능을 제공하는 공개키 암호의 경우에 관리자는 인수분해 정보를 마스터키에 해당하는 값으로 보유하고 있다. 따라서 일반 사용자들이 가지고 있는 비밀키 값을 알지 못하더라도 관리자의 판단에 의해 암호문에서 평문을 복원할 수 있다. 결과적으로 일반 사용자들은 악의적인 관리자에 대해서 어떠한 프라이버시도 기대할 수 없다. 본 논문에서는 관리자에 대한 일방향성과 구분불능성에 대해서 정의하고 정의에 따라 제안하는 공개키 암호의 안전성을 분석하고자 한다. 관리자에 대한 일방향성과 구분불능성

에 대한 정의는 다음과 같다.

정의 3. (관리자에 대한 일방향성) 어떤 시스템이 있다고 가정하고, 그 시스템의 관리자가 있다고 하자. s_{sp}는 시스템 관리자만 알고 있는 비밀정보라고 하고 p_{sp}는 일반사용자들도 알고 있는 시스템 공개정보라고 하자. $\Pi=(K,E,D)$는 공개키 암호라고 하자. A를 공개키 암호의 일방향성을 공격하는 악의적인 관리자라고 하면 A의 $Adv^{ow-atk}_{A,\Pi,S_{sp}}$는 다음과 같이 정의된다.

$$Adv^{ow-atk}_{A,\Pi,S_{sp}}(1^k)=\Pr\left[\begin{matrix}A(C,p_k,s_{sp})\\=\mathrm{M}\end{matrix}\;\middle|\;\begin{matrix}(s_k,p_k)\leftarrow K(p_{sp})\,;\ M\leftarrow 0,1^n\,;\\C\leftarrow \mathrm{E}_{sk}(\mathrm{M})\,;\end{matrix}\right]$$

충분히 큰 k와 모든 A에 대해 다음을 만족하는 $negl(k)$ 이 존재하면 Π는 일방향성을 만족한다고 한다: $Adv^{ow-atk}_{A,\Pi,S_{sp}}(1^k)\le negl(k)$.

정의 4. (관리자에 대한 구분불능성) 어떤 시스템이 있다고 가정하고, 그 시스템의 관리자가 있다고 하자. s_{sp}는 시스템 관리자만 알고 있는 비밀정보, p_{sp}는 일반사용자들도 알고 있는 시스템 공개정보라 하고 $\Pi=(K,E,D)$는 공개키 암호라고 하자. A를 구분불능성의 측면에서 공격하는 악의적인 관리자라 하면 A의 $Adv^{ind-atk}_{A,\Pi,S_{sp}}$는 다음과 같이 정의된다.

$$Adv^{ind-atk}_{A,\Pi,S_{sp}}(1^k)=2\Pr\left[\begin{matrix}A(C,p_k,s_{sp})\\=b\end{matrix}\;\middle|\;\begin{matrix}(s_k,p_k)\leftarrow K(p_{sp})\,;\ M_0,M_1\leftarrow 0,1^n\,;\\b\leftarrow 0,1\,;\ \mathrm{C}\leftarrow \mathrm{E}_{sk}(\mathrm{M}_b)\,;\end{matrix}\right]-1$$

충분히 큰 k와 모든 A에 대해 다음을 만족하는 $negl(k)$ 이 존재하면 Π는 구분불능성을 만족한다고 한다: $Adv^{ind-atk}_{A,\Pi,S_{sp}}(1^k)\le negl(k)$.

두 안전성의 개념은 기존의 일방향성과 구분불능성에 대한 정의와 유사한 형태로 정의되어 있기 때문에 이해하는 것은 어렵지 않다. 두 정의에서 기존의 것과 다른 점은 공격자에게 주어져 있는 정보이다. 악의적인 관리자를 공격자로 가정하고 있기 때문에 비밀 시스템정보인 s_{sp}가 공격자에게 주어져 있는 것을 제외하고 일반적인 공격자를 고려한 정의와 유사하다. 그러므로 이와 같은 환경에서 공격자에게 주어지지 않은 정보는 일반 사용자의 비밀키인 s_k이다.

기존의 이중 복호화 기능을 제공하는 공개키 암호에서 모듈로 n과 생성자 g가 공개 시스템정보에 해당한다. 그리고 모듈로의 인수인 두 소수 p,q가 관리자에게 주어진 비밀 시스템정보에 해당한다. 그런데 공개 시스템정보는 일반 사용자의 공개키와 중복될 수 있다. 예를 들어, 모듈로 n과 생성자 g는 공개 시스템정보이면서 각 사용자의 공개키에 해당된다. 그러나 비밀 시스템정보는 각 사용자의 비밀키와 중복되지 않기 때문에 각 정보에 중복이 발생하는 것은 안전성을 증명함에 있어서 문제가 되지 않는다.

V. 이중 복호화를 제공하는 새로운 공개키 암호

5.1 제안하는 공개키 암호 I

본 소절에서는 효율적으로 이중 복호화 기능을 제공하는 공개키 암호를 제안한다. 제안하는 공개키 암호는 다음과 같다.

키생성: k 비트의 두 소수 p,q를 선택하고 $n=p^2q$라고 하자. $ord(g^{p-1} \bmod (p^2))=p$를 만족하는 임의의 수 $g\in Z_n$를 선택한다. 임의의 $k-1$ 비트의 수 a를 선택하고 $h=g^a \bmod(n)$를 계산한다. 공개키는 (n,g,h,k)이고 대응되는 비밀키는 a이다. 두 인수 p,q는 관리자에게 주어지는 마스터키에 해당하는 정보이고, 관리자만이 알고 있다.

암호화: 평문 $m\in Z_n$이 주어지면, $k-1$ 비트의 난수 r을 선택한다. 그러면 암호문 $C=(A,B)$는 다음과 같이 계산된다: $A=g^r \bmod(n)$이고 $B=h^r m \bmod(n)$.

복호화 1: 첫 번째 복호화 방법은 ElGamal 암호와 동일하게 수행된다. 비밀키 a를 알고 있는 사용자는 다음의 계산을 통해서 평문 m을 복원할 수 있다: $m=B/A^a \bmod(n)$.

복호화 2: 두 번째 복호화 방법은 두 소수 p,q를 사용해서 수행된다. 다음을 계산한다: $h_p=h^{p-1} \bmod(p^2)$와 $g_p=g^{p-1} \bmod(p^2)$. 그러면 다음과 같이 비밀키 a를 복원할 수 있다: $a=L(h_p)/L(g_p) \bmod(p)$. 비밀키 a를 사용해서 첫 번째 복호화 방법과 동일하게 평문 m을 복원할 수 있다: $m=B/A^a \bmod(n)$.

5.2 제안하는 공개키 암호의 안전성 분석

5.2.1 일방향성

제안하는 공개키 암호는 $p-DHP$를 풀거나 $p-DLP$를 풀 수 있으면 해독된다. 일반적으로 DLP가 DHP보다 풀기 어려운 문제이므로 공개키 암호의 안전성은 $p-DHP$의 어려움과 동치임을 보이면 된다.

정리 2. 본 절에서 제안된 공개키 암호의 일방향성은 $p-DHP$의 어려움과 동치이다.

증명) $p-DHP$을 풀 수 있다고 가정하자. 그러

면 $p-DHP$를 푸는 알고리즘 B를 가정할 수 있다. B를 사용해서 공개키 암호의 일방향성을 공격하는 알고리즘 A를 구성하고자 한다. 암호문과 공개키 변수를 각각 $(A=g^r \bmod(n), B=h^r m \bmod(n))$와 (n,g,g^a)라 하자. B는 $(g^a \bmod(n), g^r \bmod(n))$에서 $g^{ar} \bmod(n)$을 계산할 수 있다. 그러므로 B의 능력을 사용하면 다음과 같이 평문을 복원할 수 있다: $m=B/g^{ar} \bmod(n)$. $p-DHP$를 풀 수 있으면 공개키 암호는 일방향성을 만족하지 않는다.

반대로 공개키 암호가 일방향성을 만족하지 않는다고 가정하자. 그러면 주어진 암호문에서 평문을 복원할 수 있는 알고리즘 A를 가정할 수 있다. A를 사용해서 $p-DHP$를 푸는 알고리즘 B를 구성하고자 한다. $g^a \bmod(n)$와 $g^b \bmod(n)$를 $p-DHP$에 대해 주어진 문제라고 하자. 즉, $g^{ab} \bmod(n)$을 계산해야 한다. (n,g,g^a)를 공개키로 설정하고 어떤 $k \in Z_n$에 대해서 $(g^b \bmod(n), g^k \bmod(n))$를 암호문으로 설정하자. k는 어떤 k'에 대해서 $k=ab+k'$로 바꾸어 쓸 수 있다. 그러므로 다음이 만족하는 것을 확인할 수 있다: $g^k = g^{ab+k'} = g^{ab} g^{k'} = g^{ab} m \bmod(n)$. 이때 $m=g^{k'} \bmod(n)$ 이다. 제안된 공개키 암호가 일방향성을 만족하지 않는다고 가정했기 때문에 A는 주어진 암호문 순서쌍 $(g^b \bmod(n), g^k \bmod(n))$의 평문에 해당하는 m을 계산할 수 있다. 즉, B는 A를 사용해서 m을 계산함으로써 $(g^a \bmod(n), g^b \bmod(n))$에 대한 $p-DHP$를 다음과 같이 풀 수 있다: $g^{ab}=g^k/m \bmod(n)$. 그런데 평문 m이 $q-1$의 위수를 가지는 Z_n의 원소일 경우에, m은 G_p에서 구성하는 값을 갖지 않는다. 이와 같은 경우에는 A를 사용해서 $p-DHP$를 풀 수 없다. 그러나 m이 $q-1$의 위수를 가지는 Z_n의 원소로 선택될 확률은 $1/2^k$ 정도이므로, 작은 확률을 제외하고 A를 통해 B를 구성할 수 있다.

5.2.2 구분불능성

[9]에 제안된 일반적인 변형기법을 적용하기 위해서는 공개키 암호가 YCP 형태의 난제를 기반으로 설계되어 있어야 한다. [9]에서 언급되었듯이, DHP도 일종의 YCP이고, 본 논문에서 제안하는 공개키 암호도 DHP의 일종인 $p-DHP$을 기반으로 설계되었기 때문에 Kiltz와 Lee의 변형기법을 적용할 수 있다. 일반적인 변형기법을 적용함으로써 제안하는 공개키 암호가 IND-CCA2의 안전성을 만족하도록 재구성할 수 있다.

H,G를 두 해쉬함수라고 하자. E^s를 대칭키 암호라 하고 $\kappa = G(h^{H(m\|r)} \bmod(n))$라 하자. 변형된 암호는 다음과 같다: $E_{pk}(m,r) = (g^{H(m\|r)} \bmod(n), E_\kappa^s(m\|r))$. [9]에 지적된 것처럼 일회용암호(one-time pad)를 사용함으로써 변형된 공개키 암호의 효율성을 높일 수 있다. 즉, $E_\kappa^s(m\|r) = \kappa \oplus (m\|r)$의 형태로 대칭키 암호를 구성함으로써 효율성을 높일 수 있다.

[9]에서는 ElGamal 암호의 안전성이 증명되어 있다. 그리고 증명은 ElGamal 암호가 YCP의 일종인 DHP에 기반하고 있다는 사실에 의해 증명되는 것이므로 동일한 형태로 구성된 공개키 암호에 동일하게 적용된다. 참고로, 대칭 암호는 OTE (one-time encryption) 관점에서 안전한 것으로 가정하고 있다 [9]. 본 논문에서 제안하는 공개키 암호는 $p-DHP$을 기반으로 설계된 일종의 ElGamal 암호이므로 [9]에 제시된 증명을 그대로 적용할 수 있다.

정리 3. $p-DHP$가 풀기 어려운 문제이고, 대칭키 암호 E^s가 OTE 관점에서 안전하면 변형된 공개키 암호는 ROM 환경에서 IND-CCA2 에 안전하다.

5.3 효율성

$|M|$와 $|e|$는 각각 모듈로 M과 지수값 e의 비트사이즈 할 때, 모듈로 M과 지수값 e에 대해서 모듈로 지수승 연산을 수행하는 연산량을 $ME(|M|,|e|)$ 라고 하자. 참고로, $ME(a,b)$ 와 $ME(\alpha a,\beta b)$ 의 연산량의 비율은 $1:\alpha^2\beta$이다. 예를 들어, $ME(a,b)$ 는 $ME(2a,3b)$ 보다 $2^2 \cdot 3 = 12$ 배 정도 효율적으로 연산을 수행한다.

[14]에서 Rene Peralta는 p^2q 형태의 정수와 RSA 정수가 각각 1600비트와 1000비트에서 동일한 안전성을 가진다는 것을 밝혔다. 그러므로 동일한 안전성에서 두 정수를 모듈로로 설계된 공개키 암호의 효율성을 비교하기 위해서는 p^2q 형태의 1600 비트 정수와 1000 비트의 RSA 정수를 비교

표 1. 효율성 비교

암호화 기법	[1]	제안하는 암호
평문의 길이	1000 비트	1600 비트
암호문의 길이	4000 비트	3200 비트
암호화의 계산복잡도	$2ME(2000,1000)$	$2ME(1600,533)$
복호화 1의 계산복잡도	$ME(2000,1000)$	$ME(1600,533)$
복호화 2의 계산복잡도	$2ME(2000,1000)$	$ME(1066,533)$ + $ME(1600,533)$

해야 한다.

본 논문에서는 [1]에서 제안된 이중 복호화 기능을 제공하는 공개키 암호와 효율성을 비교하고자 한다. 기존의 공개키 암호는 표준모델(standard model)에서 증명된 것에 반해 본 논문에서 적용한 방법은 ROM을 기반으로 안전성이 증명되는 것이므로 두 공개키 암호의 기본적인 모델의 효율성을 비교하도록 하며 기본적인 모델은 IND-CCA2의 안전성을 만족하도록 변형되지 않은 공개키 암호를 말한다.

본 논문에서 제안하는 공개키 암호는 기존의 것보다 매우 효율적이다. [1]에서 제안된 기법은 1000 비트의 평문을 전송하기 위해서 4000 비트의 암호문을 생성해야 한다. 그러나 제안하는 공개키 암호에서는 1600 비트의 평문에 대해서 3200 비트의 암호문만을 생성하면 된다. 즉, 평문과 암호문의 비율이 현저히 낮은 것을 확인할 수 있다. 계산량의 측면에서 보면 제안하는 기법은 기존의 것보다 3배 정도 빠른 암호화 연산과 복호화 연상을 제공한다. 특히, 관리자는 기존의 것보다 4배 효율적으로 복호화 연산을 수행할 수 있다.

Ⅵ. 사용자의 프라이버시가 보강된 이중 복호화를 제공하는 공개키 암호

3절에서 제안한 공개키 암호는 기존의 공개키 암호와 마찬가지로 악의적인 관리자에 대한 프라이버시 침해의 우려가 있다. 즉, 관리자는 사용자의 동의 없이도 암호문에서 평문을 복원할 수 있다. 이와 같은 문제를 해결하기 위해서는 관리자의 능력을 제한할 수 있는 기법의 개발이 필요하다. 본 절에서는 관리자의 능력을 제한할 수 있는 기법을 제공함으로써 악의적인 관리자에 대한 사용자의 프라이버시 침해의 문제를 개선하는 공개키 암호를 제안한다.

6.1 제안하는 공개키 암호 Ⅱ

본 소절에서는 사용자의 프라이버시가 보강된 이중 복호화 기능을 제공하는 공개키 암호를 제안한다.

키생성: k 비트의 두 소수 p,q를 선택하고 $n=p^2q$라고 하자. $\mathrm{ord}(g^{p-1} \bmod (p^2))=p$를 만족하는 임의의 수 $g \in Z_n$를 선택한다. 사용자가 관리자에게 복호화 할 수 있는 능력을 허용하는 경우는 다음과 같이 공개키를 생성한다. 임의의 $k-1$ 비트의 수 a를 선택하고 $h=g^a \bmod(n)$를 계산한다. 공개키는 (n,g,h,k)이고 대응되는 비밀키는 a이다. 반대로 사용자가 관리자에게 복호화 할 수 있는 능력을 허용하지 않는 경우는 다음과 같이 공개키를 생성한다. 임의의 t 비트의 a를 선택하고 $h=g^a \bmod(n)$를 계산한다. t는 $t>k$를 만족하는 값으로 선택된다. 공개키는 (n,g,h,t)이고 대응되는 비밀키는 a이다. 두 인수 p,q는 관리자에게 주어지는 마스터키에 해당하는 정보이고, 관리자만이 알고 있다.

암호화: 평문 $m \in Z_n$이 주어지면, t 비트의 난수 r을 선택한다. (사용자가 관리자에게 복호화 할 수 있는 능력을 허용하는 경우에는 $k-1$ 비트의 난수 r을 선택한다.) 암호문 $C=(A,B)$는 다음과 같이 계산된다: $A=g^r \bmod(n)$이고 $B=h^r m \bmod(n)$.

복호화 1: 첫 번째 복호화 방법은 ElGamal 암호와 동일하게 수행된다. 비밀키 a를 알고 있는 사용자는 다음의 계산을 통해서 평문 m을 복원할 수 있다: $m=B/A^a \bmod(n)$.

복호화 2: 두 번째 복호화 방법은 사용자가 관리자에게 복호화 할 수 있는 능력을 허용하였을 경우에만 가능하다. 복호화 방법은 두 소수 p,q를 사용해서 수행된다. 우선 $h_p=h^{p-1} \bmod(p^2)$와 $g_p=g^{p-1} \bmod(p^2)$를 계산한다. 다음과 같이 비밀키 a를 복원할 수 있다: $a=L(h_p)/L(g_p) \bmod(p)$. 그러면 비밀키 a를 사용해서 첫 번째 복호화 방법과 동일하게 평문 m을 복원할 수 있다: $m=B/A^a \bmod(n)$.

Remark 2. 만약에 사용자의 동의가 없으면, 관리자는 비밀 지수를 계산할 수 없다. 관리자가 계산할 수 있는 값은 비밀지수 a에 대해서 $a' = a \bmod(p)$만 알 수 있다. 그러나 충분히 큰 k와 t가 선택되면 a'에서 a를 알아내는 것은 어렵다. 이 문제의 어려움에 대한 논의와 증명은 뒤에서 자세히 다루도록 한다.

Remark 3. 공개키의 소유자가 관리자의 복호화 능력을 제한하더라도 송신자의 선택에 의해 관리자에게 복호화 능력을 제공할 수 있다. 송신자가 관리자의 복호화 능력을 허용하려면 t비트가 아닌 $k-1$ 비트의 난수 r을 선택하면, 관리자는 공개키 소요자의 비밀키 a를 계산한 것과 마찬가지 방법으로 r을 복원함으로써 암호문에서 평문을 복원할 수 있다.

Remark 4. 통신 내용이 사용자의 프라이버시에 크게 지장이 되지 않는 경우에, 사용자는 관리자의 복호화 능력을 허용함으로써 이중 복호화 기능이 제공하는 서비스를 이용할 수 있다.

6.2 안전성

사용자의 프라이버시가 보강된 공개키 암호는 앞에서 설계한 공개키 암호와는 달리 다음과 같이 정의되는 $t-DHP$라는 형태의 문제에 안전성을 기반한다.

정의 5. $t-DHP$는 다음과 같이 정의된다. : g를 G_p의 원소라 하고 t는 $t>k$를 만족하는 값이라 하자. $[1,2^t-1]$ 범위의 두 정수 a,b에 대해서 g^a와 g^b가 주어졌을 때, g^{ab}를 찾는 것을 $t-DHP$이라고 한다.

Conjecture 1. k와 t가 충분히 큰 값으로 선택되면, 모든 PPT 알고리즘 A에 대해서 다음을 만족하는 함수 $negl(k)$이 존재한다.

$$\Pr\left[A(n,A,B)=C \;\middle|\; \begin{array}{c} p,q\leftarrow P(k)\,;n=p^2q\,; \\ g\leftarrow G_p\,;a,b\leftarrow[1,2^t-1]\,; \\ A=g^a \bmod n\,;\ B=g^b \bmod n\,; \\ C=g^{ab} \bmod n\,; \end{array}\right] \le negl(k)$$

직관적으로, 지수가 더 큰 값으로 선택되기 때문에 $t-DHP$가 $p-DHP$보다 풀기 어렵다. $t-DHP$의 어려움을 기반으로 사용자의 프라이버시가 보강된 공개키 암호의 안전성을 증명할 수 있다.

정리 4. 사용자의 프라이버시가 보강된 이중 복호화 기능을 제공하는 공개키 암호의 안전성은 $t-DHP$를 풀기 어려운 것과 동치이다.

증명) 안전성이 기반하는 난제가 $t-DHP$인 것을 제외하면 정리 2와 동일하게 증명되므로 자세한 내용은 생략한다.

정리 4는 프라이버시가 보강된 공개키 암호의 일방 공격자에 대한 안전성에 대한 정리이다. 프라이버시가 보강된 공개키 암호는 관리자에 대해서도 안전하다고 주장하고 있기 때문에, 관리자에 대한 안전성은 따로 구분지어 다루어져야 한다. 관리자는 인수분해 정보를 추가로 보유하고 있으므로 일반 공격자들에게 주어진 문제인 $t-DHP$ 와는 다른 문제로 다루어야 한다. 관리자에 대한 안전성은 t_p-DHP 라는 문제에 기반하고 있는데 t_p-DHP 는 다음과 같이 정의된다.

정의 6. t_p-DHP 는 다음과 같이 정의된다. : g를 G_p의 원소라고 하자. t는 $t>k$를 만족하는 값이라고 하자. $[1,2^t-1]$ 범위의 두 정수 a,b에 대해서 $g^a \bmod(n)$와 $g^b \bmod(n)$가 주어졌을 때, $g^{ab} \bmod(n)$를 찾는 것을 t_p-DHP이라고 한다. 이 경우, $n=p^2q$을 구성하는 인수분해 정보는 공격자에게 주어지는 것으로 가정한다.

관리자에 대한 t_p-DHP의 어려움의 정도를 확인하기 위해서 다음과 같이 t_p-DHP를 단순화 시킬 수 있다. $g\in G_p$와 $[1,2^t-1]$ 범위의 두 정수 a,b에 대해서 (g^a,g^b)를 고려해보자. $a'=a \bmod(p)$, $b'=b \bmod(p)$라고 하면 어떤 두 정수 a'',b''에 대해서 a,b를 다음과 같이 표현할 수 있다: $a=a'+a''p$, $b=b'+b''p$. 그러면 g^{ab}를 다음과 같이 정리할 수 있다: $g^{ab}=g^{(a'+a''p)(b'+b''p)}=g^{a'b'+(a'b''+a''b')p+a''b''p^2}$.

관리자는 인수분해 정보를 알고 있기 때문에 a'와 b'를 계산할 수 있다. 이 정보를 사용해서 $g^{a'},g^{b'}$ 를 계산할 수 있다. 그리고 g^a,g^b 를 알기 때문에 $g^{a''p},g^{b''p}$ 를 다음과 같이 계산할 수 있다:

$$g^a/g^{a'}=g^{a'+a''p}/g^{a'}=g^{a''p},\quad g^b/g^{b'}=g^{b'+b''p}/g^{b'}=g^{b''p}\ .$$

두 값을 사용하면 다음과 같이 $g^{(a'b''+a''b')p}$를 계산할 수 있다: $(g^{a''p})^{b'}\cdot(g^{b''p})^{a'}=g^{a'b''p}\cdot g^{a''b'p}=g^{(a'b''+a''b')p}$. 관리자는 $g^{a'b'}$와 $g^{(a'b''+a''b')p}$를 계산할 수 있기 때문에, t_p-DHP를 푸는 것은 $g^{a''b''p^2}$를 계산하는 문제가 된다:

$$g^{ab}/(g^{a'b'}\cdot g^{(a'b''+a''b')p})=g^{a''b''p^2}.$$

그러므로 관리자에 대한 t_p-DHP는 순서쌍 $(g^{a''p},g^{b''p})$에 대한 DHP와 동치이다. 관리자는 인수분해 정보를 사용해서 비밀지수의 모듈로 p에 대한 값을 계산할 수 있다. 그러나 지수 값이 p의 배수 형태일 경우에는 동일한 방법으로 비밀 지수를 계산할 수 없다. 그러므로 지수 값을 계산하는 방법을 통해서 $(g^{a''p},g^{b''p})$에 대한 DHP를 계산하는 것은 관리자에게도 어려운 문제이다.

관리자는 주어진 모듈로의 인수분해 정보를 알고 있기 때문에, Z_n에서의 DHP를 작은 부분군에서의 DHP로 변환할 수 있고, 이를 통해서 주어진 문제를 쉽게 풀 수 있다. [11]에서 언급되었듯이, 인수분해가 알려져 있는 경우에는 Z_n에서의 DLP와 Z_n의 부분군에서의 DLP가 동일한 안전성을 가진다. 본 논문에서는 Z_n에서의 DHP와 Z_n의 부분군에서의 DHP가 동일한 안전성을 가지고 있다는 것을 정리 5에서 증명하고 있다. 정리 5를 증명하기에 앞서 lemma를 살펴보자.

Lemma 1. 두 소수 p,q에 대해서 $n=p^2q$라고 하자. 그러면 모든 정수 a에 대해서 다음의 관계식이 만족한다: $(\alpha p^2+\beta q)^a=(\alpha p^2)^a+(\beta q)^a \bmod(n)$.

증명) $(\alpha p^2+\beta q)^a$는 다음과 같이 표현할 수 있다: 만약 $i\neq 0,a$ 이면, $p^2|(\alpha p^2)^i$와 $q|(\beta q)^{a-i}$가 만족하므로 $(\alpha p^2)^i(\beta q)^{a-i}=0 \bmod(n)$이다. 그러므로 다음의 식이 만족하는 것을 알 수 있다:

$$(\alpha p^2+\beta q)^a = {}_aC_a(\alpha p^2)^a(\beta q)^0 + {}_aC_0(\alpha p^2)^0(\beta q)^a. \\ = (\alpha p^2)^a + (\beta q)^a \bmod(n)$$

Lemma 2. 두 소수 p,q에 대해서 $n=p^2q$라고 하자. 그러면 모든 정수 a에 대해서 다음이 만족한다:

$$(p^2(p^{-2}\bmod(q)))^a = p^2(p^{-2}\bmod(q))\bmod(n),$$
$$(q(q^{-1}\bmod(p^2)))^a = q(q^{-1}\bmod(p^2)) \bmod(n).$$

증명) $l=p^2(p^{-2}\bmod(q))\bmod(n)$ 이라고 하자. lemma를 증명하는 것은 $l^2=l \bmod(n)$ 임을 보이는 것과 같다. $l^2=l \bmod(n)$는 다음과 같이 다른 형태로 확인해 볼 수 있다: $l^2=l \Leftrightarrow l^2-l=0 \Leftrightarrow l(l-1)=0 \bmod(n)$. 그러므로 $l^2=l \bmod(n)$는 $l(l-1)=0 \bmod(n)$를 보임으로써 증명할 수 있다. $l=p^2(p^{-2}\bmod(q))\bmod(n)$ 이므로 $l(l-1)$는 다음과 같이 표현할 수 있다:

$$l(l-1)=p^2(p^{-2}\bmod(q))(p^2(p^{-2}\bmod(q))-1) \bmod(n).$$

$l(l-1)=0 \bmod(n)$인 것은
$p^2(p^{-2}\bmod(q))=0 \bmod(p^2)$이고
$p^2(p^{-2}\bmod(q))-1=0 \bmod(q)$인 것을 통해 쉽게 확인할 수 있다.

정리 5. $n=p^2q$의 인수분해에 대한 정보는 알려져 있다고 하자. 그러면 Z_n에서 정의된 *DHP*를 푸는 것의 어려움은 Z_{p^2}와 Z_q에서 정의된 *DHP*를 모두 푸는 것의 어려움과 동치이다.

증명) Z_{p^2}와 Z_q에서 정의된 *DHP*를 모두 풀 수 있는 알고리즘 A가 있다고 가정하자. A를 이용해서 Z_n에서 정의된 *DHP*를 풀 수 있다. $(g^a \bmod(n), g^b \bmod(n))$를 문제로 주어지는 Z_n에서 정의된 *DHP*에 대한 순서쌍이라고 하자. 인수분해 정보가 알려져 있으므로 $(g^a \bmod(p^2), g^b \bmod(p^2))$와 $(g^a \bmod(q), g^b \bmod(q))$를 계산할 수 있다. A는 두 순서쌍 $(g^a \bmod(p^2), g^b \bmod(p^2))$와 $(g^a \bmod(q), g^b \bmod(q))$에서 $g^{ab} \bmod(p^2)$ 와 $g^{ab} \bmod(q)$를 계산할 수 있다. $\gcd(p^2,q)=1$을 만족하므로 CRT(중국인의 나머지 정리: Chinese Remainder Theorem)을 사용하면 $g^{ab} \bmod(n)$을 계산할 수 있다.

반대로, Z_n에서 정의된 *DHP*를 푸는 알고리즘 B가 있다고 가정하자. 그러면 B를 사용해서 Z_{p^2}와 Z_q에서 정의된 *DHP*를 풀 수 있다. g를 생성자라 하고 $(g^a \bmod(p^2), g^b \bmod(p^2))$를 문제로 주어지는 Z_{p^2}에서 정의된 *DHP*에 대한 순서쌍이라고 하자. Z_q에서 정의된 *DHP*를 푸는 것에 대해서도 일반성을 잃지 않기 때문에 Z_{p^2}에 대해서만 살펴보도록 한다. 주어진 문제에 대해서 다음과 같이 x,y,z를 구성할 수 있다:

$$z=(g \bmod(p^2))q(q^{-1}\bmod(p^2))+p^2(p^{-2}\bmod(q))\bmod(n),$$
$$x=(g^a \bmod(p^2))q(q^{-1}\bmod(p^2))+p^2(p^{-2}\bmod(q))\bmod(n),$$
$$y=(g^b \bmod(p^2))q(q^{-1}\bmod(p^2))+p^2(p^{-2}\bmod(q))\bmod(n).$$

Lemma 1와 Lemma 2에 의해서 $z^a \bmod(n)$ 와 $z^b \bmod(n)$ 을 다음과 같이 표현할 수 있다:

$$\begin{aligned} z^a &= ((g \bmod(p^2))q(q^{-1}\bmod(p^2))+p^2(p^{-2}\bmod(q)))^a \bmod(n) \\ &= ((g \bmod(p^2))q(q^{-1}\bmod(p^2)))^a + (p^2(p^{-2}\bmod(q)))^a \bmod(n) \\ &= (g \bmod(p^2))^a(q(q^{-1}\bmod(p^2)))^a + (p^2(p^{-2}\bmod(q)))^a \bmod(n) \\ &= (g \bmod(p^2))^a q(q^{-1}\bmod(p^2))+p^2(p^{-2}\bmod(q))\bmod(n) \end{aligned}$$

$$\begin{aligned} z^b &= ((g \bmod(p^2))q(q^{-1}\bmod(p^2))+p^2(p^{-2}\bmod(q)))^b \bmod(n) \\ &= ((g \bmod(p^2))q(q^{-1}\bmod(p^2)))^b + (p^2(p^{-2}\bmod(q)))^b \bmod(n) \\ &= (g \bmod(p^2))^b(q(q^{-1}\bmod(p^2)))^b + (p^2(p^{-2}\bmod(q)))^b \bmod(n) \\ &= (g \bmod(p^2))^b q(q^{-1}\bmod(p^2))+p^2(p^{-2}\bmod(q))\bmod(n) \end{aligned}$$

$x=z^a \bmod(p^2)$이고 $x=z^a \bmod(q)$이므로 $x=z^a \bmod(n)$임을 알 수 있으며 $y=z^b \bmod(n)$ 가 된다. B는 $(z^a \bmod(n), z^b \bmod(n))$에서 $z^{ab} \bmod(n)$를 계산할 수 있다. 그러므로, $g^{ab} \bmod(p^2)$는 다음과 같이 계산할 수 있다: $(z^{ab} \bmod(n)) \bmod(p^2) = g^{ab} \bmod(p^2)$. Z_q에서 정의된 *DHP*도 마찬가지의 방법으로 계산할 수 있다.

정리 5에서 증명되었듯이, t_p-DHP 의 안전성은 Z_{p^2}와 Z_q에서 정의된 *DHP*를 계산하는 것과 같다. 그러나 $t-k$가 작으면, t_p-DHP 는 관리자에 대해 안전하지 않다. 이는 관리자는 인수분해 정보를 알고 있기 때문에 $a=a'+a''p$ 로 표현된 a에 대해서 a'를 알 수 있고, $t-k$비트 정도의 크기에 해당하는 a''만이 비밀정보로 남겨지기 때문이다. 이때, $t-k$의 크기가 작으면 a''가 전수조사 형태의 공격을 통해서 분석된다. 그러므로 t_p-DHP 이 안전하기 위해서는 Z_{p^2}와 Z_q에서 정의된 *DHP*가 안전하고, $t-k$가 전수조사 형태의 공격에 안전하도록 t,k가 선택되어야 한다.

Conjecture 3. $\sum_{i=0}^{a} {}_aC_i(\alpha p^2)^i(\beta q)^{a-i} \bmod(n)$ k와 t가 충분히 크면, 모든 PPT 알고리즘 A에 대해서 다음을 만족하는 함수 $negl(k)$이 존재한다.

$$\Pr\left[A(p,q,A,B)=C \;\middle|\; \begin{array}{c} p,q \leftarrow P(k); n=p^2q; \\ g \leftarrow G_{\hat{p}}\ a,b \leftarrow [1,2^t-1]; \\ A=g^a \bmod n;\ B=g^b \bmod n; \\ C=g^{ab} \bmod n; \end{array} \right] \leq negl(k)$$

t_p-DHP 가 안전하다고 가정하면 사용자의 프라이버시가 보강된 이중 복호화 기능을 제공하는 공개키 암호는 관리자에 대한 안전성을 보장한다. 관리자에 대한 충분한 안전성을 획득하기 위해서는 t,k가 충분히 큰 값으로 선택되어야 하기 때문에 앞에서 소개한 효율성 측면만 고려된 제안된 공개키 암호에 비해서는 t,k의 크기가 크다. 사용자에 대한 안전성을 증명하는 정리 6은 안전성이 t_p-DHP에 기반하고 있다는 것을 제외하면 정리 4와 동일하게 증명된다.

정리 6. 사용자의 프라이버시가 보강된 이중 복호화 기능을 제공하는 공개키 암호의 관리자에 대한 안전성과 t_p-DHP의 안전성은 동치이다.

일반 공격자와 악의적인 관리자에 대한 프라이버시가 보강된 공개키 암호의 일방향성은 각각 $t-DHP$와 t_p-DHP에 안전성을 두고 있다. 두 문제는 일종의 YCP이므로, [9]에 제안된 일반적인 변형기법을 적용함으로써 IND-CCA2의 안전성을 만족하도록 변형할 수 있다. 프라이버시가 보강된 공개키 암호의 변형된 모델은 다음과 같다. H,G를 두 해쉬함수라고 하자. E^s는 대칭키 암호라 하고 $\kappa = G(h^{H(m\|r)} \bmod(n))$라 하자. 변형된 공개키 암호는 다음과 같다: $E'_{pk}(m,r) = (g^{H(m\|r)} \bmod(n), E^s_\kappa(m\|r))$. 구분불능성에 대한 증명은 정리 3과 동일하다.

정리 6. $t-DHP$ 가 풀기 어려운 문제이고, 대칭키 암호 E^s가 OTE 관점에서 안전하면 변형된 공개키 암호는 ROM 환경에서 IND-CCA2 관점에서 안전하다. 특히, IND-CCA2 관점에서의 관리자에 대한 안전성은 t_p-DHP 가 어려운 문제라는 것에 기반한다.

Remark 5. [9]에서 제안하는 방법은 YCP라는 형태의 문제를 기반으로 설계된 공개키 암호를 IND-CCA2 에 안전하도록 변환하는 기법이다. YCP라는 형태의 문제는 계산적인(computational) 문제이고 관리자는 인수분해에 대한 정보를 통해서도 t_p-DHP 를 풀 수 없는 것을 증명했으므로 인수분해를 알고 있는 관리자에 대해서도 제안하는 공개키 암호의 변형된 모델은 IND-CCA2의 안전성을 가진다.

제안하는 공개키 암호는 관리자에 대해서도 일방향성과 구분불능성을 만족하기 때문에 프라이버시 관점에서 기존의 것보다 보강되었다고 할 수 있다. 일반 사용자가 관리자에 대한 프라이버시의 침해를 방지하고 싶은 경우에는 이중 복호화 기능의 사용을 포기하는 대신 자신의 프라이버시를 보호할 수 있다. 프라이버시를 보호하면서 이중 복호화 기능을 제공받을 수는 없지만 사용자가 이중 복호화 기능의 사용 여부를 선택함으로써 자신의 프라이버시를 보호할 수 있기 때문에 기존의 공개키 암호보다 관리자에 대한 프라이버시의 관점에서 안전하다. 제안하는 공개키 암호는 변수 t에 따라 관리자와 일반 공격자에 대한 안전성이 다르다. 즉, 두 종류의 공격자에 대한 안전성이 다르다. 그러나 충분히 큰 t,k를 선택함으로써 관리자에 대한 충분한 안전성을 획득할 수 있다.

Ⅵ. 결 론

본 논문에서는 이중 복호화 기능을 제공하는 기존의 공개키 암호보다 효율적인 공개키 암호를 제안하였고, 그 공개키 암호를 기반으로 관리자에 대한 사용자의 프라이버시가 보강된 이중 복호화 기능을 제공하는 공개키 암호를 제안하였다.

참 고 문 헌

[1] Emmanuel Bresson, Dario Catalano, and David Pointcheval, "A Simple Public-Key Cryptosystem with a Double Trapdoor Decryption Mechanism and Its Applications", ASIACRYPT 2003, LNCS 2894, pp. 37-54, Springer-Verlag, 2003.

[2] Mihir Bellare, Anand Desai, David Pointcheval, and Phillip Rogaway, "Relations Among Notions of Security for Public-Key Encryption Schemes", CRYPTO'98, LNCS 1462, pp. 26-46, Springer-Verlag, 1998.

[3] Joonsang Baek, Byoungcheon Lee, and Kwangjo Kim, "Provably Secure Length-Saving Public-Key Encryption Scheme under the Computational Diffie-Hellman Assumption", ETRI Journal, Volume 22, Number 4, December 2000.

[4] Ronald Cramer, and Victor Shoup, "Universal Hash Proofs and a Paradigm for Adaptive Chosen Ciphertext Secure Public-Key Encryption", EUROCRYPT 2002, LNCS 2332, pp. 45-64,

Springer-Verlag, 2002.

[5] D. Dolev, C. Dwork, and M. Naor, "Non-malleable cryptography", Proceedings of the 23rd Annual Symposium on Theory of Computing, ACM, 1991.

[6] W. Diffie, and M. E. Hellman, "New Directions in Cryptography", IEEE Transactions on Informaion Theory, 22(6), 644-654, 1976.

[7] Eiichiro Fujisaki, and Tatsuaki Okamoto, "How to Enhance the Security of Public-Key Encryption at Minimum Cost", PKC'99, LNCS 1560, pp. 53-68, 1999.

[8] S. Goldwasser, and S. Micali, "Probabilistic encryption", Journal of Computer and System Science, Vol.28, No.2, pp.270-299, 1984.

[9] Eike Kiltz and John Malone-Lee, "A General Construction of IND-CCA2 Secure Public Key Encryption", Cry ptography and Coding 2003, LNCS 2898, pp. 152-166, 2003.

[10] Wenbo Mao, and Chae Hoon Lim. "Cryptanalysis in Prime Order Subgroups of Z_n^*", ASIACRYPT'98, LNCS 1514, pp. 214-226, 1998.

[11] A.J. Menezes, P.C. Oorschot, and S.A. Vanstone, "Handbook of Applied Cryptography", CRC Press, Inc, (1999).

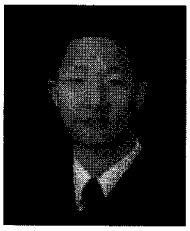
[12] Tatsuaki Okamoto, Shigenori Uchiyama, "A New Public-Key Cryptosystem as Secure as Factoring", EUROCRYPT '98, LNCS 1403, pp. 308-318, Springer-Verlag, 1998.

[13] Pascal Paillier, "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes", EUROCRYPT'99, LNCS 1592, pp. 223-238, Springer-Verlag, 1999.

[14] Rene Peralta, "Report on Integer Factorization", available at http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/doc/1025_report.pdf, 2001.

[15] David Pointcheval, "Chosen-Ciphertext Security for any One-Way Cryptosystem", Proceedings of PKC'2000, LNCS 1751, pp. 129-146, 2000.

〈著者紹介〉



윤 택 영 (Taek-Young Youn) 정회원
2003년 2월: 고려대학교 수학과 이학학사
2005년 2월: 고려대학교 정보보호대학원 정보보호학과 공학석사
2005년 3월~현재: 고려대학교 정보보호대학원 정보보호학과 박사과정
〈관심분야〉 암호 이론, 정보보호 이론, 암호 프로토콜, 부채널 공격

박 영 호 (Young-Ho Park) 정회원
1990년 2월: 고려대학교 수학과 이학사
1993년 2월: 고려대학교 수학과 이학석사
1997년 2월: 고려대학교 수학과 이학박사
2002년 3월~현재: 세종 사이버 대학교 조교수
〈관심분야〉 정수론, 공개키 암호, 암호 프로토콜, 부채널 공격

임 종 인 (Jongin Lim) 정회원
1980년 2월: 고려대학교 수학과 학사
1982년 2월: 고려대학교 수학과 석사
1986년 2월: 고려대학교 수학과 박사
1999년 2월~현재: 고려대학교 정보보호대학원 원장, CIST 센터장
〈관심분야〉 암호 이론, 정보보호 정책