2001년 한국정보처리학회 춘계 학술발표논문집 제8권 제1호

표준모델에서 안전성이 증명 가능한 공개키 암호 시스템을 구성하는 일반적인 방법

최승복*, 오수현*, 원동호*
*성균관대학교 전기 전자 및 컴퓨터 공학부
e-mail : sbchoi@dosan.skku.ac.kr

General Construction for Provably Secure Public Key Cryptosystem in the Standard Model

Seung-Bok Choi*, Soo-Hyun Oh*, Dong-Ho Won*
*School of Electrical & Computer Eng., Sungkyunkwan University

요약

암호 기술이 다양화되고 실용화되면서 암호문을 변경할 수 없다는 안전성(CCS)를 만족하는 암호 알고리즘에 대한 필요성이 제기되었고, 최근 몇 년간 안전성이 증명가능한 공개키 암호 방식을 개발하려는 연구가 활발히 진행되어왔다. 지금까지의 연구는 암/복호화시의 효율성 개선과 안전성 증명에 필요한 보다 약한 가정을 사용하려는 방향으로 진행되어왔다. 본 논문에서는 표준모델하에서 기존에 알려진 일방향 함수를 이용하여 적응-선택 암호문 공격에 안전한 공개키 암호 시스템을 구성하는 일반적인 변환 방법을 제안한다. 제안된 방식으로 변환된 공개키 암호 방식은 CCS를 만족할뿐만 아니라 효율적이며 가장 최소화된 가정만을 사용하기 때문에 기존의 어떤 방식들보다 이상적인 변형방식이다.

1. 서론

1976년 Diffie와 Hellman에 의해 공개키 암호 시스템에 대한 개념이 소개된 이후 많은 공개키 암호 시스템이 개발되었으며 공개키 암호 시스템의 안전성을 증명하기 위한 노력은 지속적으로 이루어져왔다. 1984년 Goldwasser와 Micali는 처음으로 증명 가능한 공개키 암호의 안전성 개념을 제안하였다[1]. 그들은 공격자가 주어진 암호문으로부터 평문의 길이 이외에는 평문에 대한 아무런 정보도 얻을 수 없다는 구분불가능성(Indistinguishability:IND)이라는 안전성 개념을 제시하였는데, 그들의 안전성 개념은 수동적 공격자를 모델로 하고있다. 한편, 1991년 Dolev등은 공격자가 주어진 암호문으로부터 해당 암호문의 평문과 관련있는 다른 평문의 암호문을 만들 수 없다는 조작불가능성(Non-Malleability:NM)이라는 능동적 공격자를 모델로 한 안전성 개념을 제시했다[2].

이러한 안전성 개념은 기존의 선택 평문 공격자(Chosen Plaintext Attack:CPA)와 선택 암호문 공격자(Chosen Ciphertext Attack:CCA1), 적응-선택 암호문 공격자(Adaptive Chosen Ciphertext Attack:CCA2) 모델과 결합되어 Bellare등에 의해 체계화되었다[5]. Bellare는 또한 IND-CCA2와 NM-CCA2의 동치성을 증명하였는데 최근에는 이러한 두 안전성 개념을 선택 암호문 공격에 안전한 안전성(Chosen Ciphertext Security:CCS)으로 총칭해서 부르고 있다.

본 논문에서는 기존의 공개키 암호 시스템과 대칭키 암호 시스템을 결합하여 CCS를 만족하며 효율적인 공개키 암호 시스템을 구성할 수 있는 일반적인 변환방법을 소개한다. 그리고, 변환예제로 1998년에 소개된 Okamoto-Uchiyama의 공개키 암호 방식[4]을 제시한다.

2. 기존의 변환 방식과 제안하는 방식과의 비교

1994년 Bellare와 Rogaway는 안전성이 증명가능하고 효율적인 공개키 암호 방식을 발표하였다[3]. 그들의 제안방식은 RSA처럼 trapdoor permutation에 기반하는 암호 방식을 CCS를 만족하는 공개키 암호 시스템으로 변환할 수 있는 방식(OAEP)이다. 그러나, OAEP는 *trapdoor permutation*에 기반한 암호 방식에만 적용할 수 있는 방식이다.

최근들어 기존의 다양한 공개키 암호 방식에 적용가능한 보다 일반화된 변형 방식들이 소개되었는데, Fusisaki와 Okamoto가 제안한 두 가지 변형방식[6][7]

* 본 연구는 한국과학재단의 목적기초연구(97-0100-13-01-5) 지원사업으로 수행되었음.

과 Pointcheval이 제안한 변형방식[8]은 공통적으로 검증시 재암호화(re-encryption : 수신된 암호문과 복구정보를 이용해 재암호화를 통해 암호문의 변경여부를 검증하는 방식)를 하는 문제점과 IND-CPA를 만족하는 공개키 암호 시스템에만 적용이 가능한 변환 방식이었다. 2001년 발표된 Okamoto와 Pointcheval의 논문에는 암호문의 검증시 재암호화를 하지 않으며 격차-문제(Gap-Problem)라는 계산문제의 어려움을 기반으로 IND-CPA를 만족하는 공개키 암호 방식은 물론 RSA에도 적용가능한 획기적인 방식(REACT)이 소개되었다[10].

본 논문에서 제안하는 방식은 REACT에서 사용한 격차-문제에 기반하고 있기 때문에 대부분의 공개키 암호 방식에 적용 가능하며 REACT와 마찬가지로 하이브리드(hybrid) 방식을 채택했기 때문에 효율적이다. 그러나, REACT가 랜덤 오라클(Random Oracle: RO)을 사용하는 반면, 제안하는 방식은 표준모델(Standard model)을 사용하고 있기 때문에 증명자체는 보다 현실적이다. 따라서, 제안방식은 지금까지 소개된 방식들의 장점만을 취합한 가장 이상적인 변형 방식이다.

<표 1> 제안방식과 기존방식과의 비교

이름	안전성 기반	문제점
OAEP	C-Prob./RO	trapdoor permutation 기반방식에만 적용가능
FO1	D-Prob./RO	re-encryption
FO2	C-Prob./RO	re-encryption
P00	C-Prob./RO	re-encryption
REACT	Gap-Prob./RO	RO 모델사용
CS98	D-Prob./St.	ElGamal에만 적용가능/ 낮은 효율성
ACE	D-Prob./St.	D-H에만 적용가능
제안방식	Gap-Prob./St.	-

※ D-Prob. : Decisional Problem
C-Prob. : Computational Problem
D-H : Diffie-Hellman 키분배 방식
RO : Random Oracle / St. : Standard Model

3. 암호 알고리즘에 대한 안전성 개념

공개키 암호 방식의 기본적인 안전성 개념은 일방향성이다. 일방향성은 공격자가 주어진 암호문으로부터 평문을 찾을 수 없다는 의미를 갖는다.

[정의 1] 일방향성(One-wayness : OW)
t의 수행시간을 갖는 모든 공격자 A에 대해 암호문으로부터 평문을 계산할 확률이 ε보다 작을 때, 공개키 암호 방식은 (t, ε)-OW이다.

$$Adv^{OW}(A) = Pr[(pk, sk) \leftarrow K^{asym}(1^k), m \leftarrow M, r \leftarrow \Omega : A(E_{pk}^{asym}(m;r)) = m] < \varepsilon$$

Goldwasser와 Micali에 의해 정의된 공개키 암호의 안전성 개념(IND^{asym})을 대칭키 암호 방식에 적용한 IND^{sym} 개념을 다음과 같이 정의한다.

[정의 2] 구별불가능성(Indistinguishability : IND^{sym})
t의 수행시간을 갖는 모든 공격자 $A=(A_1, A_2)$에 대해 다음을 만족할 때, 대칭키 암호 방식은 (t, ε)-IND^{sym}이다.

$$Adv^{IND}(A) = 2 \times Pr[K \leftarrow K^{sym}(1^k), (m_0, m_1, s) \leftarrow A_1(K), b \leftarrow \{0, 1\}, c \leftarrow E_K^{sym}(m_b) : A_2(c, s)=b] - 1 < \varepsilon \quad (|m_0| = |m_1| \in \{0,1\}^l)$$

4. 격차-문제와 새로운 공격자 모델

4.1 평문-검사 공격

공개키 암호 방식에 적용가능한 공격자 모델로 평문-암호문 쌍이 유효한지를 결정할 수 있는 평문-검사 공격(Plaintext-Checking Attack:PCA)을 다음과 같이 정의한다.

[정의 3] 평문-검사 공격(PCA)
공격자는 임의의 평문과 암호문 쌍을 입력으로 주어진 쌍이 유효하면 1을 출력하고, 그렇지 않으면 0을 출력하는 평문-검사 오라클에 접근할 수 있다.

모든 결정론적 공개키 암호 방식에서 OW-CPA와 OW-PCA는 동치이다. 즉, OW-CPA를 만족하는 모든 공개키 암호 시스템은 OW-PCA를 만족한다[10].

4.2 격차-문제

기존의 계산문제와 결정문제는 다음과 같이 정의할 수 있다.

$f : \{0,1\}^* \times \{0,1\}^* \mapsto \{0,1\}$일 때,

- 계산문제(Computational Problem:CP) : y가 주어졌을때, f(x, y)=1을 만족하는 x를 계산하는 문제
- 결정문제(Decisional Problem:DP) : (x, y)쌍이 주어졌을때, f(x, y)=1인지 아닌지를 결정하는 문제

결정문제는 계산문제로 귀착된다. 즉, 계산문제를 해결할 수 있으면 결정문제를 해결할 수 있다. 그러나, 일반적으로 계산문제를 결정문제로 귀착시키는 것

은 어려우며 이러한 어려움을 기반으로 격차-문제를 정의할 수 있다[9][10].

[정의 4] 격차-문제(Gap-Problem : GP)
y가 주어졌을 때, f(x, y)=1인지 아닌지를 결정할 수 있는 오라클을 이용해 f(x, y)=1을 만족하는 x를 계산하는 문제.

4.3 격차-문제의 예제

공개키 암호 방식의 일방향성을 결정하는 계산문제가 존재하고, 그것으로 귀착시킬 수 있는 결정문제가 정의된다면 격차-문제는 언제나 정의할 수 있다. 다음은 Okamoto와 Uchiyama가 제안한 공개키 암호 방식의 안전성 증명에 사용된 계산문제와 결정문제를 기반으로 정의되는 격차문제에 대한 예제이다.

[정의 5] Okamoto-Uchiyama 문제
$n=p^2q$(p와 q는 큰 소수), $g^{p-1}(\text{mod } p^2)$의 위수가 p인 Z_n^*상의 원소 g, 그리고 $h=g^n(\text{mod } n)$에 대해,

- 계산-OU 문제(C-OU) : (n, g, h, y)가 주어졌을 때, 어떤 $r\in Z_n$에 대해 $y=g^xh^r(\text{mod } n)$을 만족하는 $x\in Z_p^*$를 계산하는 문제
- 결정-OU 문제(D-OU) : (n, g, h, y, x)가 주어졌을 때, 어떤 $r\in Z_n$에 대해 $y=g^xh^r(\text{mod } n)$을 만족하는지 결정하는 문제
- 격차-OU 문제(G-OU) : (n, g, h, y)가 주어졌을 때, 결정-OU 문제에 대한 오라클을 이용해 $y=g^xh^r(\text{mod } n)$을 만족하는 $x\in Z_p^*$를 계산하는 문제

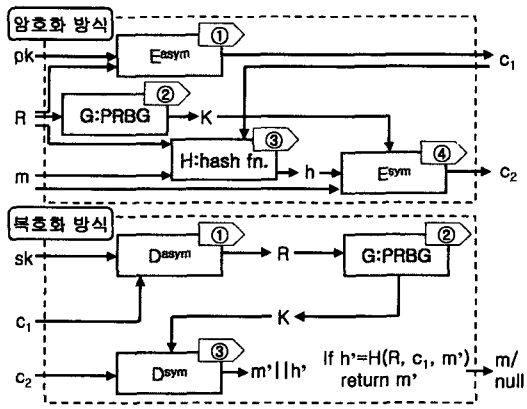
[정의 6] 격차-OU 가정
결정-OU 문제에 대한 오라클에 접근할 수 있는 모든 공격자가 계산-OU 문제를 계산할 수 있는 확률은 무시할 만큼 아주 작다(negligible probability).

5. 제안하는 변환 방식과 안전성

5.1 제안하는 변환 방식

기존의 공개키 암호 방식과 대칭키 암호 방식을 결합한 변환 방식은 다음과 같은 세 개의 알고리즘 $(K^{hy}, E_{pk}^{hy}, D_{sk}^{hy})$으로 구성된다. 여기서, G는 의사 난수 생성기이며 H는 일반적인 해쉬함수이다.

- $K^{hy}(1^k)$: 키 생성 알고리즘
  - 안전성 계수(security parameter) k를 입력으로 공개키와 비밀키쌍 (pk, sk)를 출력한다.
- $E_{pk}^{hy}(m;R,r)$: 암호 알고리즘
  - $c_1 = E_{pk}^{asym}(R;r)$: 공개키 암호 방식으로 랜덤한 입력 값 R을 암호화한다. (r : random coins)
  - K = G(R) : R을 입력으로 대칭키 암호 방식의 세션키 K를 출력한다.
  - H(R, c_1, m) : 검증정보로 사용되며, R과 c_1, m이 해쉬함수의 입력 값이 된다.
  - $c_2 = E_K^{sym}(m \| h)$: 평문 m과 해쉬함수의 결과 값 h를 K를 이용해 대칭키 암호 방식으로 암호화한다.
  (* 결정론적 공개키 암호 방식일 경우, 공개키 암호 방식의 입력 값 r은 null 값을 갖는다.)
- $D_{sk}^{hy}(C)$: 복호 알고리즘 ($C=(c_1, c_2)$)
  - $R = D_{sk}^{asym}(c_1)$: c_1을 복호해서 R값을 찾는다.
  - K = G(R) : 복호된 R을 이용해 세션키 K를 출력한다.
  - $D_K^{sym}(c_2)$: K를 이용해 c_2를 복호한다.
  - $D_K^{sym}(c_2) = m' \| h'$일 때, h'=H(R, c_1, m')를 만족하면 m'(=m)을 출력한다.



<그림 1> 제안하는 변환 방식의 암/복호화 과정

5.2 제안하는 변환 방식의 안전성

제안방식의 가장 큰 특징은, 암호문의 변경여부를 검사하기 위해서 사용된 해쉬함수의 결과 값을 평문과 함께 암호화한다는 것이다. 해쉬함수에 대한 RO가정에 상관없이 IND^{sym}을 만족하는 대칭키 암호 방식에 의해 해쉬함수의 결과 값 자체에 대한 기밀성이 보장되기 때문에, 증명과정에서 필요한 해쉬함수의 RO가정을 제거할 수 있다.

[정리 1]
표준모델과 다음과 같은 가정하에서 제안된 공개키 암호 방식 $(K^{hy}, E_{pk}^{hy}, D_{sk}^{hy})$은 IND-CCA2(=CCS)를 만

족한다.

- 사용된 공개키 암호 방식 (K^{asym}, E^{asym}, D^{asym})가 OW-PCA를 만족한다.
- 사용된 대칭키 암호 방식 (K^{sym}, E^{sym}, D^{sym})가 IND^{sym}을 만족한다.
- 사용된 의사 난수 생성기(PRBG)는 진짜 난수열(truly random)과 구별불가능한 값을 출력한다.

(증명-개요)

제안방식의 IND-CCA2를 깰수 있는 공격자 A=(A_1, A_2)를 가정하고 A를 이용하여 다음과 같은 3개의 알고리즘을 구성할 수 있음을 보인다.

- 알고리즘 B : A를 이용하여 사용된 공개키 암호 방식의 OW-PCA를 깰 수 있는 알고리즘. 즉, IND-CCA2 공격자 A와 결정문제에 대한 오라클을 이용해 계산문제를 해결할 수 있는 알고리즘.
- 알고리즘 C : A를 이용하여 사용된 대칭키 암호 방식의 IND^{sym}를 깰 수 있는 알고리즘. 즉, IND-CCA2 공격자 A를 이용하여 사용된 대칭키 암호 방식의 암호문이 어떤 평문의 암호문인지 구분할 수 있는 알고리즘.
- 알고리즘 D : A를 이용하여 사용된 PRBG의 결과 값과 진짜 난수열을 구분할 수 있는 알고리즘.

5.3 O-U 방식의 변환예제

앞절에서 정의한 격차-OU 문제가 어렵다는 가정하에서 다음과 같은 보조정리를 얻을 수 있다.

[보조정리 2]

O-U 공개키 암호 방식은 격차-OU 가정하에서 OW-PCA를 만족한다.

O-U 공개키 방식은 다음과 같이 제안된 변형방식에 적용될 수 있다.

G : PRBG, H : 해쉬함수

- $K^{hy}(1^k)$: $n=p^2q$과 $g^{p-1}(\mathrm{mod}\ p^2)$의 위수가 p인 Z_n^* 상의 원소 g, 그리고 $h=g^n(\mathrm{mod}\ n)$을 계산한 후 pk=(n,g,h)와 sk=(p,q)를 출력한다. ($|p|=|q|=k$)
- $E_{pk}^{hy}(m;R,r)$: $R<2^k$과 $r\in Z_n$을 입력으로 $c_1=g^R h^r (\mathrm{mod}\ n)$, $K=G(R)$, $c_2=E_K^{sym}(m \| H(R, c_1, m))$을 계산하고 암호문 $C=(c_1, c_2)$를 출력한다.
- $D_{sk}^{hy}(C)$: $R=L(c_{1p})/L(g_p)(\mathrm{mod}\ p)$, $K=G(R)$, $D_K^{sym}(c_2)=A \| B$를 계산하고 $B=H(R, c_1, A)$를 만족하면 A(=m)을 출력한다. ($c_{1p}=c_1^{p-1}(\mathrm{mod}\ p^2)$, $g_p=g^{p-1}(\mathrm{mod}\ p^2)$, L : 로가리즘 함수(logarithm fn.))

[정리 3]

변환된 O-U 방식은 표준모델에서 격차-OU 가정과 사용된 대칭키 암호 방식, PRBG가 안전하다는 조건하에서 IND-CCA2(=CCS)를 만족한다.

6. 결론

본 논문에서는 기존의 공개키 암호 방식과 대칭키 암호 방식을 이용해 적응-선택 암호문 공격에 안전한 공개키 암호 시스템을 구성할 수 있는 일반적인 변환 방법을 소개하였다. 제안방식은 표준모델에서 격차-문제라는 계산문제에 기반하며 RSA 같은 결정론적 공개키 방식에도 적용이 가능한 효율적이고 최적화된 변형방식이다.

참고문헌

[1] S. Goldwasser and S. Micali, "Probabilistic Encryption", Journal of Computer and System Science, vol 28(2):270-299, April 1984

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

[3] M. Bellare and P. Rogaway, "Optimal Asymmetric Encryption Padding-How to Encrypt with RSA", Proc. of Crypto 94, LNCS 950, pp.92-111, 1994

[4] T. Okamoto and S. Uchiyama, "A New Public-Key Cryptosystem as Secure as Factoring", Proc. of Eurocrypt 98, LNCS 1403, pp.308-318, 1998

[5] M. Bellare, A. Desai, D. Pointcheval and P. Rogaway, "Relations Among Notions of Security for Public-Key Encryption Schemes", Proc. of Crypto 98, LNCS 1462, pp.26-45, 1998

[6] E. Fusisaki and T. Okamoto, "How to Enhance the Security of Public-Key Encryption at Minimum Cost", Proc. of PKC 99, LNCS 1560, pp.53-68, 1999

[7] E. Fusisaki and T. Okamoto, "Secure Integration of Asymmetric and Symmetric Encryption Schemes", Proc. of Crypto 99, LNCS 1666, pp.537-554, 1999

[8] D. Pointcheval, "Chosen-Ciphertext Security for Any One-Way Cryptosystem", Proc. of PKC 2000, LNCS 1751, pp.129-146, 2000

[9] T. Okamoto and D. Pointcheval, "The Gap-Problem : A New Class of Problems for the Security of Cryptographic Schemes", Proc. of PKC 2001, LNCS 1992, pp.104-118, 2001

[10] T. Okamoto and D. Pointcheval, "REACT : Rapid Enhanced-security Asymmetric Cryptosystem Transform", The Cryptographer's Track of the RSA Conference 2001, to appear.