通信情報保護學會誌
第9卷 第1號, 1999. 3

확률 공개키 암호에 관한 연구

A Study on the Probabilistic Public-key Encryption

강 주 성*, 박 춘 식*

요 약

본 논문에서는 지금까지 알려진 확률 공개키 암호 방식에 대해서 조사 분석한다. 기존의 결정적(deterministic) 공개키 방식의 문제점을 논하고, 결정적 공개키 방식에서는 이룰 수 없는 강한 안전성 개념들을 소개한다. 그리고 결정적 공개키 방식의 문제점을 보완하고 제시된 안전성 개념을 충족시키는 확률 공개키 암호 방식에 대하여 고찰한다. 또한, 조사한 확률 공개키 방식을 종합적으로 비교 분석한다.

1. 서 론

소인수 분해 문제와 이산 대수 문제 등의 어려움에 안전성 기반을 둔 기존의 공개키 암호 시스템은 비밀키 암호 시스템 사용 시 야기되었던 키 관리 문제를 효과적으로 해결하고 디지털 서명이라는 새로운 기능을 제공하여 암호의 유용성을 증가시켜 왔다. 그러나 단순히 일방향성(onewayness)에만 안전성을 의존하는 기존의 결정적(deterministic) 공개키 방식은 그 안전성에 대한 이론적 증명이 완벽하게 되어 있지 않는 등 몇가지 문제점을 안고 있다. 이러한 문제점을 해결하기 위한 대안으로서 확률 공개키 암호(probabilistic public-key encryption) 방식이 도입되었다.

확률 공개키 암호 방식에서는 같은 메시지일지라도 암호화할 때마다 서로 다른 암호문으로 암호화 된다. 간단히 말해서 확률 공개키 암호 방식은 어떤 안전성 개념에 대하여 증명 가능한 안전성을 확보하기 위해서 랜덤성을 이용하는 방식이다. 본 논문은 이와 같은 확률 공개키 암호 방식에 관해서 종합적으로 조사 분석해 보기 위한 것이다. 이를 위해서 기존 결정적 공개키 방식의 문제점을 살펴보고, 이론적 안전성 개념에 대하여 알아보며, 지금까지 발표된 확률 공개키 암호 방식을 소개 및 비교 분석할 것이다.

이 글은 서론을 포함하여 총 5개의 절로 구성된다. 2절에서는 결정적 공개키 암호 방식의 문제점에 대해서 논하고, 3절에서는 공개키 암호 방식의 엄밀한 정의와 안전성 개념들을 간단히 소개한다. 4절에서는 본 논문의 주제인 다양한 확률 암호 방식에 대하여 조사 분석하며, 5절은 결론부이다.

* 한국전자통신연구원

2. 결정적(deterministic) 공개키 암호 방식의 문제점

트랩도어 일방향 함수(trapdoor one-way function)를 사용하는 결정적 공개키 암호 방식은 안전성 측면에서 다음과 같은 몇가지 문제점을 안고 있다.

첫째, 특별한 메시지 공간에 대해서는 트랩도어 함수의 역함수가 계산 불능이라는 사실을 보장할 수 없다. 메시지 공간이 언어(language)로 한정된 경우나 $M=\{0, 1\}$인 경우는 대부분 역함수를 구하기 쉽다. 예를 들면, 대표적인 공개키 암호인 RSA 방식에서 0과 1은 항상 자기 자신으로 암호화 된다.

둘째, 결정적 공개키 암호에서는 메시지의 모든 정보를 다 숨기지는 못한다. RSA 방식에서 암호문으로부터 평문을 해독하는 문제가 불가능하다고 할지라도 암호문으로부터 평문의 최하위 비트나 최상위 비트 같은 어떤 부분 정보(partial information)를 유추하는 가능성을 배제하지는 못한다. 또한, RSA 방식에서 암호문과 평문의 Jacobi 심볼은 공개지수 e가 홀수이므로

$$\left(\frac{c}{n}\right)=\left(\frac{m^e}{n}\right)=\left(\frac{m}{n}\right)^e=\left(\frac{m}{n}\right)$$

이 되어 항상 일치하게 된다. 이렇게 암호화 과정에서 불변적인 요인이 존재한다는 사실은 안전성 관점에서는 취약한 부분으로 볼 수 있다.

셋째, 결정적 공개키 암호 방식에서 고정된 공개키에 대하여 임의의 메시지 m은 항상 같은 암호문 c로 암호화 된다. 이러한 시스템에서는 같은 메시지를 두 번 이상 보내게 되면 이 사실이 쉽게 탐지될 수 있다. 예를 들어서 RSA 방식에서 공개 지수가 l일 때, 같은 메시지를 l명의 수신자에게 보내는 경우 공격자는 쉽게 메시지를 복구할 수 있는 것으로 알려져 있다.

넷째, 기존의 결정적 공개키 방식의 약점으로 안전성에 대한 이론적 증명의 결여를 들 수 있다. 현재까지 RSA 암호 방식을 해독하는 어려움이 큰 수 n을 소인수 분해하는 어려움과 동치인지의 여부는 미해결 문제로 남아있다. 즉, n을 소인수 분해하는 방법 이외의 해독 방법이 존재하는지와 RSA의 해독이 n을 소인수 분해할 수 있다는 사실을 함축(imply)하는지의 여부는 아직까지 밝혀지지 않았다.

이와 같은 몇가지 결정적 공개키 방식의 문제점을 해결하기 위한 대안으로 제시된 것이 확률 공개키 암호 방식이다. 확률 공개키 암호 방식은 결정적 방식과 다르게 어떤 안전성 개념에 대하여 증명 가능하다. 이때 필요한 안전성 개념은 다음 절에서 살펴본다.

3. 공개키 암호 방식의 안전성 개념

확률적 공개키 암호 방식이 기존의 결정적 공개키 암호 방식 보다 더 강한 안전성을 제공한다는 사실을 보이기 위해서는 확률적 공개키 방식이 달성할 수 있는 안전성에 대한 개념 정립이 선행되어야 한다. Goldwasser와 Micali[8]는 의미론적 안전성(semantic security)과 구별불능 안전성(indistinguishable encryption)을 소개하였다. 의미론적 안전성은 Shannon이 정의한 완전 안전성(perfect secracy) 개념을 polynomially bounded시킨 버젼으로 볼 수 있으며, 구별불능 안전성은 의미론적 안전성과 수학적으로 동치인 개념이다. 그리고 이들 안전성 보다 좀 더 강한 개념으로 Dolev, Dwork, Naor[6]는 NM-안전성(non-malleability)을 제안하였다. 한편, Bellare등[1]은 이들 안전성 개념에 공격 관점을 첨가한 정의를 발표하였는데, 공개키 암호 방식에서는 공격을 선택 평문 공격(chosen plaintext attack, CPA), 선택 암호문 공격(chosen ciphertext attack, CCA), 능동적 선택 암호문 공격(adap-

tively chosen ciphertext attack, ACCA)으로 분류한다. 본 절에서는 확률 공개키 암호 방식 소개에 필요한 안전성 개념과 이러한 개념 정의에 기초가 되는 공개키 암호 방식의 엄밀한 정의를 간단히 소개하기로 한다.

정의 1 (공개키 암호 방식)

Π = (K,E,D)가 다음의 조건을 만족할 때 우리는 Π를 공개키 암호 방식(public-key encryption scheme)이라 부른다.

1. 키 생성 알고리즘 K는 확률적(probabilistic) 알고리즘으로 1^n을 입력으로 하여 공개키와 비밀키 쌍 (k_p, k_s)를 출력한다.
2. 암호화 알고리즘 E는 확률적 알고리즘으로 공개키 k_p와 평문 $m \in \{0, 1\}^*$를 입력으로 하여 암호문 c를 출력한다.
3. 복호화 알고리즘 D는 결정적(deterministic) 알고리즘으로 비밀키 k_s와 암호문 c를입력으로 하여 메시지 $m \in \{0, 1\}^*$ 또는 결점있는 암호문을 나타내는 기호 "?" 출력한다.
4. 임의의 평문 $m \in \{0, 1\}^*$에 대하여 $E(k_p, m) = c$인 모든 암호문 c는 $D(k_s, c) = m$를 만족한다.
5. K, E, D는 모두 다항식 시간 안에 계산되는 알고리즘들이다. 여기에서 1^n은 각 비트 값이 모두 1인 n-비트 벡터를 의미하고, 정수 n은 암호 방식의 안전성 파라메타로서의 역할을 한다. 그리고 $E(k_p, m)$는 공개키 k_p로 평문 m를 암호화 하는 것을, $D(k_s, c)$는 비밀키 k_s로 암호문 c를 복호화함을 각각 의미한다.

위 정의 1에 나타난 공개키 암호 방식 Π = (K,E,D)가 어떤 성질을 소유하느냐에 따라서 다음과 같이 안전성 개념을 분류한다.

가. 의미론적 안전성(semantic security)

의미론적 안전성은 Goldwasser와 Micali[8]에 의해 소개된 개념으로서 공개키 암호 방식의 증명 가능한 안전성을 제공하기 위한 효시가 된 정의라고 볼 수 있다. 의미론적 안전성은 암호문으로부터 효율적으로 계산 가능한 것은 모두 단지 평문의 길이만 주어졌을 때에도 효율적으로 계산 가능한 것이라는 사실을 의미한다. 즉, 평문의 길이 이외에 다른 정보가 없다면 암호문은 평문을 유추해 내는 데에 아무런 역할도 하지 못한다는 개념이 의미론적으로 안전하다는 뜻이다. 의미론적으로 안전한 암호 방식을 사용하는 통신로 상에서 암호문을 도청하는 공격자는 평문에 대해서 아무런 정보도 얻지 못한다.

나. 구별불능 안전성(indistinguishability of encryptions)

의미론적 안전성과 함께 암호 방식의 안전성을 판별하기 위한 방법으로 Goldwasser와 Micali[8]가 제안한 개념이 구별불능성(indistinguishability)이다. 임의의 두 평문에 대한 각각의 암호문을 식별해내는 것이 계산적으로 불가능할 때 이 암호 방식은 구별불능성을 소유한다고 말한다. 이 구별 불능 안전성은 의미론적 안전성과 수학적으로 동치라는 사실이 Goldwasser와 Micali에 의해서 증명되었다. 그러므로 구별 불능 안전성과 의미론적 안전성은 개념상 구분할 필요가 없다. 표현의 용이성 때문에 구별 불능 안전성을 많이 사용하는데 공격 관점의 안전성을 결합하여 IND-CPA, IND-CCA, IND-ACCA 등으로 표현한다.

다. NM-안전성(non-malleability)

NM-안전성 개념은 Dolev, Dwork, Naor[6]에 의해서 처음 소개된 것으로 이들의 머리글자를 인용하여 DDN-안전성이라 부르기도 한다. 앞에서 소개했던 의미론적 안전성과 구별불능 안전성 개념의 정의에서와는 다르게 NM-안전

성을 정의할 때는 공격자의 공격 목표가 낮아진다는 것이 큰 특징이다. 이전의 두 안전성 개념에서 공격자의 목표는 주어진 도전 암호문 c로부터 평문 m을 찾아내는 것이었다. 그러나 NM-안전성 개념 정의에 나타나는 공격자의 목표는 도전 암호문 c의 평문 m을 찾는 것이 아니고 단지 그것의 평문이 m과 알려진 방법으로 관계(relation)지워진 어떤 암호문을 얻어내는 것이다. 즉, 다른 안전성 개념에서 보다 공격 성공의 목표치가 약하기 때문에 NM-안전성에서 고려되는 공격자는 그만큼 공격을 쉽게 성공시킬 수 있는 것이다. NM-안전성에 공격 관점의 안전성을 결합한 개념을 NM-CPA, NM-CCA, NM-ACCA 등으로 표현한다.

라. 안전성 개념들 사이의 관계

위에서 언급한 안전성 개념들 사이의 수학적 관계는 Bellare등[1]에 의해서 완벽하게 규명되었는데 그 결과는 그림 1에 잘 나타나 있다. 그림에서 화살표는 수학적 함축성(implication)을 의미하고, 화살표 위의 사선은 이 함축성이 성립하지 않음을 나타낸다. 의미론적 안전성과 구별 불능 안전성은 서로 동치이므로 같은 개념으로 인식하여 그림에서 IND(indistinguishability)로 표현되었다.

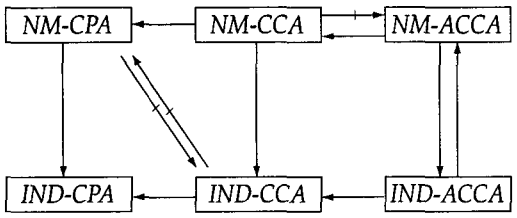

그림 1. 안전성 개념들 사이의 관계

4. 여러 가지 확률 공개키 암호

가. GM(Goldwasser-Micali) 확률 암호

Goldwasser와 Micali[8]가 최초로 제안한 확률적 공개키 암호 시스템으로서 제곱 잉여 문제(quadratic residuosity problem)가 어렵다(intractable)는 가정하에 의미론적으로 안전한 시스템이다.

[키생성] 각 사용자는 비밀키로 충분히 큰 두 소수 p, q를 생성하고, 공개키로는 두 소수의 곱인 $n=pq$와 모듈러 n으로 제곱 비잉여(quadratic non-residue)이고 Jacobi 심볼값이 1인 $y\in Z_n$를 생성한다. 즉, 공개키는 (n,y)이고, 비밀키는 (p,q)이다.

[암호화] 사용자 B가 A에게 길이가 t인 이진 메시지 $m=m_1\ m_2\ \cdots\ m_t$을 보내고자 한다. A의 공개키가 (n,y)일 때, B는 각 m_i에 대응하는 $x_i\in Z_n$을 선택한 후에

$m_i=1$이면 $c_i=yx_i^2 \bmod n$으로 놓고,

$m_i=0$이면 $c_i=x_i^2 \bmod n$으로 놓는다.

B는 A에게 암호문 $c=(c_1, c_2, \cdots, c_t)$를 보낸다.

[복호화] A는 자신의 비밀키를 사용하여 각 c_i가 모듈러 n에 대해서 제곱 잉여인지를 판별하여 만일 제곱 잉여이면 $m_i=0$으로, 제곱 잉여가 아니면 $m_i=1$로 복호화 한다.

위에서 살펴 볼 수 있는 것처럼 GM 확률 암호의 가장 큰 약점은 메시지 확장이 크게 발생한다는 것이다. 실제로 암호문은 평문에 비해서 그 비트 길이가 $\log n$배 길다.

나. BG(Blum-Goldwasser) 확률 암호

Blum과 Goldwasser[4]가 제안한 확률 암호 시스템은 GM 확률 암호에서와 같은 메시지 확장이 일어나지 않을 뿐만 아니라 RSA 암호 방식 만큼 효과적인 것으로 알려져 있다.

[키생성] 각 사용자는 비밀키로 $4k+3$ 형태의

서로 다른 두 소수 p,q를 선택하고, 공개키로 두 소수의 곱 $n=pq$를 공개한다. 또한, 확장 유클리드 알고리즘을 사용하여 $ap+bq=1$을 만족하는 두 정수 a,b를 구하여 비밀로 간직한다.

[암호화] 사용자 B가 사용자 A의 공개키로 암호화 하는 과정은 다음과 같다.

1. $k=\lfloor \log n \rfloor$, $h=\lfloor \log k \rfloor$로 놓는다.
2. 메시지를 $m=m_1 m_2 \cdots m_t$로 놓는다. 여기서 각 m_i는 길이 h인 이진 스트링이다.
3. 모듈러 n으로 제곱 잉여인 랜덤한 시드(seed) x_0를 선택한다.
4. 1부터 t까지의 각 i에 대해서 다음을 계산한다.
   (1) $x_i=x_{i-1}^2 \bmod n$을 계산한다.
   (2) p_i를 x_i의 하위 h비트라 놓는다.
   (3) $c_i=p_i \oplus m_i$를 계산한다.
5. $x_{t+1} = x_t^2 \bmod n$을 계산한다.
6. 암호문 $c=(c_1, c_2, \cdots c_t, x_{t+1})$를 A에게 보낸다.

[복호화] 암호문 c로부터 메시지 m을 복구하기 위해서 A는 다음을 수행한다.

1. $d_1=((p+1)/4)^{t+1} \bmod (p-1)$을 계산한다.
2. $d_2=((q+1)/4)^{t+1} \bmod (q-1)$을 계산한다.
3. $u=x_{t+1}^{d_1} \bmod p$을 계산한다.
4. $v=x_{t+1}^{d_2} \bmod q$을 계산한다.
5. $x_0=vap+ubq \bmod n$을 계산한다.
6. 1부터 t까지의 각 i에 대해서 다음을 계산한다.
   (1) $x_i=x_{i-1}^2 \bmod n$ 을 계산한다.
   (2) p_i를 x_i의 하위 h비트라 놓는다.
   (3) $m_i=p_i \oplus c_i$를 계산한다.

BG 확률 암호는 GM 확률 암호와는 다르게 암호문이 평문에 비해서 단지 x_{t+1}의 비트 길이인 상수 만큼만 길기 때문에 메시지 확장이 크게 일어나지 않는다. 또한, 암호화 과정이나 복호화 과정의 속도도 RSA 방식에 비해서 결코 뒤지지 않는 것으로 알려져 있다. 이러한 이유 때문에 BG 확률 암호를 EPE(Efficient Probabilistic Encryption) 방식이라 부르기도 한다[7].

소인수 분해 문제가 어렵다는 가정하에 BM 확률 암호 방식은 의미론적으로 안전하다. 그러나 Rabin 암호 방식과 같이 공개키로부터 비밀키를 찾아내는 선택 암호문 공격에 취약한 것으로 알려져 있다.

다. OAEP(Optimal Asymmetric Encryption Padding) 확률 암호

Bellare와 Rogaway[2]는 RSA 방식에 기반한 확률 암호인 OAEP 방식을 제안하였다. 이들은 공개키 암호 방식의 증명 가능한 안전성을 위해서 랜덤 오라클(random oracle) 모델을 처음으로 제안하였는데, 이 모델에서는 안전성을 증명할 때 랜덤한 이상적인 오라클이 존재한다는 가정을 전제한다. 랜덤 오라클은 구현상에서는 일방향 해쉬 함수 같은 유사 랜덤 함수로 대치된다.

[키생성] 각 사용자는 RSA 방식에서와 같은 공개키 (n,e)와 비밀키 (p,q,d)를 생성한다. 그리고 $H:\{0,1\}^{k_0} \rightarrow \{0,1\}^{k_1+l}$과 $G:\{0,1\}^{k_1+l} \rightarrow \{0,1\}^{k_0}$는 랜덤 함수이다.

[암호화] $m(|m|=k_0)$를 평문이라 하자. 그러면 먼저 임의의 $r(|r|=k_1)$을 랜덤하게 선택한다. 그리고

$$y=(m||0^l) \oplus H(r),\ z=r \oplus G(y),$$
$$C=(y||z)^e \bmod n$$

일 때, 암호문은 C가 된다.

[복호화]

$$X=C^d \bmod n,\ Y=[X]^{k_0+l},$$

$R=[X]_{k_1} \oplus G(Y)$

일 때, $[Y \oplus H(R)]_l = 0^l$ 인가를 판별하여 이것이 성립하면

$m=[Y \oplus H(R)]^{k_0}$

를 출력하고, 성립하지 않으면 암호문을 기각한다.

OAEP 확률 암호는 랜덤 오라클 모델에서 RSA 문제가 어렵다는 가정 하에 가장 강한 개념인 IND-ACCA sense의 안전성을 제공한다. 이 증명을 위해서 Bellare와 Rogaway는 평문 인식성(plaintext awareness)이라는 안전성 개념을 도입하였다. Dolev, Dwork, Naor[6]는 의미론적 안전성보다 강한 개념인 NM-안전성을 만족시키기 위하여 영지식 증명을 이용한 확률 암호를 제안했지만 이는 극히 비현실적인 것이었다. 그러나 OAEP 확률 암호는 IND-ACCA와 NM-ACCA는 동치 개념이므로 현재까지 알려진 암호중 안전성이 가장 좋으며, RSA 암호의 이용 형태로서 표준적 위치를 차지하고 있다. 실제로 OAEP 방식은 신용 카드에 기인한 SET(Secure Electronic Transaction) 등에 이용되고 있다.

라. EPOC(Efficient Probabilistic Public-key Encryption) 확률 암호

Okamoto와 Uchiyama[9]는 안전성이 증명 가능하고 효율적인 공개키 암호 방식을 제안하였다. 이 방식의 일방향성은 $n=p^2q$의 소인수 분해가 어렵다는 사실에 기반하고, p-부분군 가정 하에서 IND-CPA sense의 안전성을 제공한다. 최근에 Okamoto[10]는 이 시스템을 안전성 측면에서 약간 개선시킨 EPOC 확률 암호를 제안하였다.

[키생성] $p,q(|p|=|q|=k)$는 서로 다른 소수이고, $n=p^2q$라 하자. 그리고 $g \in Zn$ 는 $g_p=g^{p-1} \bmod p^2$의 차수(order)가 p인 정수이며, $h=h_0^n \bmod n$ $(h_0 \in Z_n^*)$라고 하고, H: $\{0,1\}^* \rightarrow \{0,1\}^{2k+c}$ ($c>0$: 상수)와 G:$\{0,1\}^* \rightarrow \{0,1\}^l$ 은 랜덤한 함수라 하자. 이때, 공개키는 (n,g,h)이고, 비밀키는 (p,q) 이다.

[암호화] $m(|m|=l)$을 평문이라 하자. 그러면 $r(|r|=k-1)$을 랜덤하게 선택하고,

$C_1 = g^r h^{H(m\|r)} \bmod n$, $C_2 = m \oplus G(r)$

일 때, 암호문은 (C_1, C_2)가 된다.

[복호화]

$C_p = C_1^{p-1} \bmod p^2$, $r = \dfrac{L(C_p)}{L(g_p)} \bmod p$,

$m = C_2 \oplus G(r)$

을 계산한다. 여기에서 $L(x) = \dfrac{x-1}{p}$ 이다.

다음으로 $C_1 = g^r h^{H(m\|r)} \bmod n$이 성립하는 지를 판별하여 성립하면 m을 출력하고, 성립하지 않으면 암호문을 기각한다.

EPOC 확률 암호는 OAEP 확률 암호와 비슷하게 랜덤 오라클 모델 하에서 가장 강한 안전성 개념인 IND-ACCA sense의 안전성이 보장된다. Okamoto의 소속 연구소인 일본의 NTT는 OAEP 방식을 표준안으로 채택한 공개키 표준화 그룹인 P1363에 이 EPOC 방식을 투고해 놓은 상태이다.

마. Cramer-Shoup 확률 암호

Cramer와 Shoup[5]는 최근에 ElGamal 암호 방식을 개량한 실질적인 확률 암호를 제안하였다. 이 방식은 DDH(Decision Diffie-Hellman) 가정이 참이고 유니버설 일방향 해쉬 함수를 이용할 수 있다는 전제 하에 IND-ACCA sense의 안전성이 보장된다. 그리고 속도는 ElGamal 방식에 비해서 약 두배 정도 느

린 것으로 알려져 있다.

[키생성] p,q 는 $q|(p-1)$인 큰 소수라 하고, g_1, g_2는 차수(order)가 q인 Z_p^* 의 원소라 하자. Z_p^*로부터 임의로 x_1, x_2, y_1 , y_2, z를 선택한다. 그리고

$c = g_1^{x_1} g_2^{x_2} \bmod p$, $d = g_1^{y_1} g_2^{y_2} \bmod p$,
$h = g_1^{z} \bmod p$

를 계산하고, H는 유니버설 일방향 해쉬 함수라 하자. 공개키는 (p,q,g_1, g_2,c,d,h)이고, 비밀키는 (x_1, x_2, y_1, y_2, z)이다.

[암호화] $m(0 < m < q)$이 평문일 때, 임의의 $r \in Zq$ 를 선택하고,

$u_1 = g_1^r \bmod p$, $u_2 = g_2^r \bmod p$, $e = h^r m \bmod p$, $\alpha = H(u_1, u_2, e)$, $v = c^r d^{r\alpha} \bmod p$

를 계산한다. 암호문은 (u_1, u_2, e, v)이다.

[복호화]

$u_1^{x_1+y_1\alpha}\ u_2^{x_2+y_2\alpha} \equiv v \bmod p$

가 성립하는지를 판별한 후에 성립하면

$m = e/u_1^z \bmod p$

를 출력하고, 성립하지 않으면 암호문을 기각한다.

OAEP와 EPOC 확률 암호가 랜덤 오라클 모델 하에서 IND-ACCA sense의 안전성을 보장하는 반면 Cramer-Shoup 방식은 유니버설 일방향 해쉬 함수의 존재성을 가정하지만 랜덤 오라클 모델이 아닌 표준 모델에서 IND-ACCA sense의 안전성을 만족한다는 것이 큰 특징이다.

지금까지 살펴본 확률적 공개키 암호 방식들을 개괄적으로 비교하여 정리해 보면 다음 표 1과 같다. 표 1에서 QRP(Quadratic Residuosity Problem)는 홀수인 합성수 n이 주어졌을 때 Jacobi 심볼이 1인 정수 a가 모듈러 n으로 제곱 잉여가 되는지를 결정하는 문제이고, RSAP(RSA Problem)는 RSA 공개키가 주어졌을 때 암호문으로부터 평문을 찾아내는 문제를 의미하며, DDH(Decision Diffie-Hellman)는 소수 p, 생성원 $\alpha \in Z_p^*$, $\alpha^a \bmod p$, $\alpha^b \bmod p$가 주어졌을 때, $\alpha^{ab} \bmod p$ 를 결정하는 문제이다.

표 1. 확률 공개키 암호 방식의 비교

확률 암호 방식	안전성	정수론 가정	특 징
GM (Goldwasser-Micali)	의미론적 안전성 (semantic security)	QRP	비효율적 (메시지 확장이 큼)
BG(EPE) (Blum-Goldwasser)	의미론적 안전성 (semantic security)	Factoring	효율적 CCA에 약점
OAEP	IND-ACCA	RSAP	랜덤 오라클 모델
EPOC	IND-ACCA	Factoring	랜덤 오라클 모델
Cramer-Shoup	IND-ACCA	DDH	유니버설 일방향 해쉬 함수 존재성 가정

5. 결 론

확률적 공개키 암호 방식이 추구하는 안전성은 다소 현실적이지 못하며 이론적인 면이 강하다. 즉, 공격자의 능력을 현실적이지 못한 측면에서 가정하여 안전성을 논하고 있는 듯하다. 그러나 공격자의 능력이 상상외로 향상될 수 있음을 고려한다면 이러한 안전성 관점의 연구가 결코 지나치다고만 생각할 수는 없다. 실제로 RSA 암호 방식의 표준으로 사용되어온 PKCS #1(Ver. 1)의 안전성이 문제가 되었는데[3], 이에 대한 대안으로 OAEP 확률 암호가 채택된 사실은 시사하는 바가 크다.

참고문헌

[1] M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway, "Relations among notions of security for public-key encryption schemes", Advances in Cryptology-CRYPTO'98 LNCS 1462, Springer-Verlag, 1998, 26-45.

[2] M. Bellare and P. Rogaway, "Optimal asymmetric encryption", Advances in Cryptology-EUROCRYPT '94, LNCS 950, Springer-Verlag, 1995, 92-111.

[3] D. Bleichenbacher, "Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS #1", Advances in Cryptology-CRYPTO'98, LNCS 1462, Springer-Verlag, 1998, 1-12.

[4] M. Blum and S. Goldwasser, "An efficient probabilistic public-key encryption scheme which hides all partial information", Advances in Cryptology-CRYPTO'84, LNCS 196, Springer-Verlag, 1985, 289-299.

[5] R. Cramer and V. Shoup, "A practical public-key cryptosystem provably secure against adaptive chosen message attack", Advances in Cryptology-CRYPTO'98, LNCS 1462, Springer-Verlag, 1998, 13-25.

[6] D. Dolev, C. Dwork, and M. Naor, "Non-malleable cryptography", Proceedings of the 23rd Annual ACM Symposium on Theory of Computing, 1991, 542-552.

[7] S. Goldwasser and M. Bellare, "Lecture Notes on Cryptography", MIT Lab. Computer Science. 1997.

[8] S. Goldwasser and S. Micali, "Probabilistic encryption", Journal of Computer and System Sciences, 28, 1984, 270-299.

[9] T. Okamoto and S. Uchiyama, "A new public-key cryptosystem as secure as factoring", Advances in Cryptology-EUROCRYPT'98, LNCS 1403, Springer-Verlag, 1998, 308-318.

[10] T. Okamoto, "Provable security of practical public-key encryption schemes", Proceedings of JWIS'98(Japan-Singapore), 67-73.

□ 著者紹介

강 주 성

1989년 2월 고려대학교 이과대학 수학과 (학사)
1991년 2월 고려대학교 대학원 수학과 (이학석사)
1996년 2월 고려대학교 대학원 수학과 (이학박사)
1997년 12월 - 현재 한국전자통신연구원 선임연구원

※ 주관심분야 : 암호이론

박 춘 식

광운대학교 전자통신과 (학사)
한양대학교 대학원 전자통신과 (석사)
일본동경공업대학 전기전자공학과(암호학 전공, 공학박사)
1989년 10월 - 1990년 9월 일본동경공업대학 객원 연구원
1982년 12월 - 현재 한국전자통신연구원 책임연구원
1999년 한국통신정보보호학회 국제협력이사, 종신회원

※ 주관심분야 : 암호이론, 정보이론, 통신이론