情 報 保 護 學 會 誌
第 14 券 第 5 號, 2004. 10

Key Encapsulation Mechanism

박 제 홍*, 권 대 성*

요 약

비밀키 암호의 키 관리 문제를 해결하기 위해 제안된 공개키 암호는 효율성이나 제한된 메시지 영역으로 인해, 실제로는 메시지의 암호화에는 비밀키 암호를 사용하고 이때 사용되는 키를 메시지를 보낼 상대방과 안전하게 공유하기 위한 용도로 공개키 암호를 사용하는 하이브리드 형태가 일반적으로 사용된다. 최근 Shoup에 의해 제안된 Key Encapsulation Mechanism (KEM)은 이러한 공개키 암호의 실제 사용 용도를 감안하여 제안된 모델로 Data Encapsulation Mechanism (DEM)과 함께 안전한 하이브리드 공개키 암호를 설계하는 하나의 이론적인 모델을 제시하며, 이를 이용하여 만들어진 하이브리드 암호는 최근의 공개키 암호 표준화 작업에서 하나의 주류로 받아들여지고 있다. 본 논문에서는 최근 공개키 암호의 새로운 적용 방식으로 주목받고 있는 KEM과 함께, 이와 관련된 공개키 암호 표준화 작업에 대해서 구체적으로 알아본다.

Ⅰ. 서 론

1976년 비밀키 암호의 키 관리 문제를 해결하기 위해 Diffie-Hellman에 의해 제안된 공개키 암호는 계산량이 많은 관계로 효율성에 있어서는 비밀키 암호를 대체하지 못하기 때문에 길이가 긴 메시지를 암호화 하는데는 적합하지 않다. 그러므로 현실적으로는 메시지의 암호화에는 비밀키 암호 기법을 사용하고 암호문을 전송받는 상대방과 메시지 암호화에 사용된 비밀키를 안전하게 공유하기 위한 도구로 공개키 암호를 사용하는 경우가 일반적이며, 이를 하이브리드 암호라고 한다. 결국 하이브리드 암호에서는 공개키 암호가 담당하는 부분과 비밀키 암호가 담당하는 부분의 두 부분으로 나눠서 생각해 볼 수 있는데, 공개키 암호 부분은 적절한 비밀키를 생성하고 공개키 암호를 이용하여 이 비밀키를 암호화 하는 역할을 수행하고 비밀키 암호 부분은 임의로 생성된 비밀키를 사용하여 메시지를 암호화 하는 역할을 수행한다. Shoup은 이러한 두 분야를 서로 분리하여 각각에 대한 형식 모델과 안전성 요구조건을 정립하고 각각을 Key Encapsulation Mechanism(KEM)과 Data Encapsulation Mechanism(DEM)이라 명명하였으며[12], 이러한 개념을 도입하여 설계된 하이브리드 형태의 공개키 암호 기법을 KEM-DEM 모델이라 한다. 결국 KEM은 자체적으로 비밀키를 생성하고 그에 대한 암호화를 같이 수행하는 키 관리 면에서의 특화된 기능에 맞춘 기법으로, 일반적인 암호 기법들이 능동 선택 암호문 공격에 대해 구별불가능성(IND-CCA2)을 만족하기 위해 상당한 계산량을 요구하는데 비해 상대적으로 효율적인 방법으로 원하는 안전성을 만족시킬 수 있기 때문에 표준화 작업에서 주목을 받았다. 실제로 2003년 선정작업이 끝난 NESSIE[11]에서는 권고 알고리즘들을 모두 KEM 모델로 선정하였으며, CRYPTREC[7]이나 현재 진행중인 ISO 표준화 작업[8,13]에서도 KEM 기법들이 제안되어 이에 대한 분석작업이 진행되고 있다. 또한 Shoup의 결과[12]이후 제안된 여러 연구 결과들 - Lucks가 Cramer-Shoup 암호 시스템[3]을 2차 잉여류 군 (quadratic residue group)에 적용한 결과[10]나 Dent의 일반화된 변형 기법[4], 그리고 Shoup이 제시한 KEM의 안전성 조건을 약화시켜도 충분히 안전한 KEM-DEM 모델을 만들 수 있음을 보인 Kurosawa-Desmedt의 결과[9] - 은 표준화 작업과는 상관없이 KEM이 기존의 공개키 암호를 적용하는 하나의 연구 분야로 각광을 받기 시작했음을 보여주는 예라고 할 수 있다. 이에 본 논문에서는 KEM에 대해서 소개하고 이와 관련된 최근의 공개키 암호 표준화 작업에

* 국가보안기술연구소 기반기술연구부 ({jhpark,ds_kwon}@etri.re.kr)

대해 정리해 보도록 한다.

Ⅱ. Key Encapsulation Mechanism

1. KEM-DEM 기반 암호의 구성

KEM은 사용자에게 주어진 공개키로 임의의 키를 생성, 이 키를 암호화하고 복호화하는 방식을 제공하는 기법으로 기본적으로 공개키 방식을 이용한다. KEM은 다음의 세 개의 알고리즘으로 구성된다[3].

1. 확률적, 다항식 시간 키 생성 알고리즘 KEM.KeyGen은 안전성 인수 k 를 입력받아 공개키/개인키 쌍 (pk, sk)를 반환한다. 공개키와 개인키의 구조는 특정 기법에 의존한다. 안전성 인수 k에 대해 다음의 확률 공간을 정의할 수 있다.

   $\mathrm{KEM.PKSpace}_k = \{pk : (pk, sk) \leftarrow_R \mathrm{KEM.KeyGen}(1^k)\}$

   $\mathrm{KEM.SKSpace}_k = \{sk : (pk, sk) \leftarrow_R \mathrm{KEM.KeyGen}(1^k)\}$
2. 확률적, 다항식 시간 암호화 알고리즘 KEM.Encap은 안전성 인수 k와 공개키 $pk \in [\mathrm{KEM.PKSpace}_k]$를 입력받아 비밀키 K와 이 키에 대한 암호문인 C를 반환한다. 여기서 K는 길이가 $\mathrm{KEM.KeyLen}(k)$인 비트열이다.
3. 결정적, 다항식 시간 복호화 알고리즘 KEM.Decap은 안전성 인수 k와 개인키 $sk \in [\mathrm{KEM.SKSpace}_k]$, 그리고 암호문 C 를 입력받아, 비밀키 K 나 오류부호 $\perp$를 반환한다.

일반적인 공개키 암호와 마찬가지로, KEM의 경우도 견고성 (soundness)을 만족해야 하는데 이는 KEM의 키 생성 알고리즘 KEM.KeyGen가 입력받은 안전성 인수 k에 대해 $\mathrm{KEM.Decap}(1^k, sk, C) \neq K$인 $(K, C) \in [\mathrm{KEM.Encap}(1^k, pk)]$가 존재하는 공개키/개인키 쌍 (pk, sk)을 무시할 만한 확률로 생성한다는 것을 의미한다.

여기서 보면 KEM은 공개키 암호와 거의 유사하게 동작하며, 단지 그 차이는 KEM의 암호화 알고리즘이 일반적인 공개키 암호 기법의 암호화 알고리즘과는 달리 어떤 특정한 메시지를 입력받는 것이 아니라 임의로 메시지인 비밀키 K 를 직접 생성한다는 점을 알 수 있다. 물론 임의로 키를 생성하고 그것을 암호화 하는 방법은 기존의 일반적인 공개키 암호 기법을 그대로 사용할 수도 있지만 KEM의 경우 보다 효율적으로 원하는 안전성을 만족하도록 설계할 수 있다. [표 1]에서 소개할 RSA-KEM은 이러한 사실을 잘 보여주는 예라 할 수 있다[11].

[표 1] RSA-KEM 의 구조

KEM.KeyGen: 기본적인 RSA 프리미티브의 키 생성방식에 따라 공개키 $pk = (n, e)$와 개인키 $sk = (n, d)$를 계산한다.
KEM.Encap: 공개키 pk 를 입력받은 후, 다음의 과정을 수행한다.
1. 랜덤 정수 $r \in \{0, \cdots, n-1\}$를 생성한다.
2. $C \leftarrow r^e \bmod n$; $K \leftarrow KDF(r)$;
3. (K, C)를 출력한다.
KEM.Decap: 개인키 sk, 그리고 암호문 C 를 입력받은 후, 다음의 과정을 수행한다.
1. $r \leftarrow C^d \bmod n$; $K \leftarrow KDF(r)$;
2. K 를 출력한다.

여기서 KDF는 키 유도 함수 (Key Derivation Function)로 보통 해쉬 함수를 이용하여 만들어지며, 안전성 증명에서는 랜덤 오라클의 역할을 수행하는 것이 일반적이다. RSA-KEM은 기본적인 RSA 프리미티브를 거의 그대로 이용하는 구조로 IND-CCA2 안전성을 만족하는 기존의 RSA-OAEP[2,8,11]에 비해 매우 단순하면서도 KEM에서 요구되어지는 안전성 (소절 2.2 참조)을 만족한다[13].

DEM의 경우 KEM에서 생성된 비밀키를 사용하여 메시지를 암호화하는 기법으로 그 구성은 다음과 같다.

1. 결정적 암호 알고리즘 DEM.Enc는 임의의 길이를 가지는 메시지 m과 사전에 정해진 길이를 가지는 비밀키 K 를 입력받아 암호문 C 를 반환한다.
2. 결정적 복호 알고리즘 DEM.Dec는 암호문 C 와 비밀키 K 를 입력받아 평문 또는 오류부호 $\perp$를 반환한다.

DEM의 경우도 KEM과 마찬가지로 견고성을 만족해야 한다. 즉 모든 유효한 키 K 와 메시지 m 에 대해

$$\mathrm{DEM.Dec}(\mathrm{DEM.Enc}(m, K), K) = m$$

이 성립한다. 또한 DEM은 KEM에서 사용되는 사용자의 공개키를 이용하지 않는다. 본 논문에서는 자세한 DEM의 구조나 안전성에 대한 언급은 생략하도록 한다. 참고로 안전한 하이브리드 암호를 설계하기 위한 적절한

DEM기법의 안전성 요구 조건은 [3]에 소개되어 있으며 [8]에 세 가지 방법이 제시되어 있다. 참고로 이들은 MAC 알고리즘을 기본적으로 사용하며, 블록 암호를 CBC 모드 (Cipher Block Chaining mode)로 사용하거나 KDF와 one-time pad를 조합하는 방식을 이용하여 하이브리드 암호의 안전성과 특징을 만족할 수 있도록 하였다.

만일 각각의 KEM (KEM.KeyGen, KEM.Encap, KEM.Decap) 과 DEM (DEM.Enc, DEM.Dec)이 있고, KEM.KeyLen(k)=Dem.KeyLen(k) 인 경우, 다음과 같이 KEM-DEM 모델을 만들 수 있다. 여기서 DEM.KeyLen은 DEM이 사용하는 비밀키의 길이를 의미한다.

1. 키 생성 알고리즘은 KEM.KeyGen을 사용한다. (pk, sk)← KEM.KeyGen (1^k).
2. 암호화 알고리즘은 다음의 단계를 거친다.
   가. (K, C_1)←KEM.Encap (pk)
   나. C_2←DEM.Enc $_K$(m)
   다. (C_1, C_2)을 출력한다.
3. 복호화 알고리즘은 다음의 단계를 거친다.
   가. K←KEM.Decap (sk, C_1). 만일 $K=\perp$이면 $\perp$를 반환하고 종료한다.
   나. m←DEM.Dec $_K$(C_2). 만일 $m=\perp$이면 $\perp$를 반환하고 종료한다.
   다. m을 출력한다.

이렇게 만들어진 하이브리드 암호는 KEM과 DEM이 각각에서 정의되는 안전성을 만족할 경우 IND-CCA2 안전성을 가지게 된다. KEM과 관련된 안전성 개념은 다음 소절에서 다루도록 한다. 참고로 모든 하이브리드 형태의 공개키 암호가 KEM-DEM 모델인 것은 아니다. NESSIE의 Phase II에서 분석되었던 EPOC-2가 좋은 예라 할 수 있다.

KEM-DEM 기반 암호의 기본적인 예로는 ElGamal 기법을 들 수 있다[5]. 소수 위수 q를 가지는 순환군 $G=\langle g\rangle$에서 공개키/개인키 쌍은 (h, z)←$G\times Z_q$로, 여기서 $h=g^z$이다. 평문 $m\in G$을 암호화하기 위해 우선 임의의 Z_q의 원소 u를 선택하고 다음을 계산한다.

$$a\leftarrow g^u, \quad b\leftarrow h^u, \quad c\leftarrow b\cdot m.$$

암호문은 $\psi=(a, c)$이다. 개인키를 이용하여 이러한 암호문을 해독하기 위해 $b\leftarrow a^z$, $m\leftarrow c\cdot b^{-1}$를 계산하여 평문 m을 찾을 수 있다. ElGamal 암호의 경우 Diffie-Hellman 키 일치 프로토콜에 기반한 KEM과 modular 곱셈에 기반한 DEM으로 구성된 형태로 볼 수 있다. 물론 ElGamal 기법은 DEM에서 사용자의 공개키 정보를 이용하기 때문에 형식적인 KEM-DEM 모델에 정확하게 맞는 것은 아니지만 KEM-DEM 모델의 특징을 잘 보여주는 구조라 할 수 있다. ElGamal 암호의 선택 평문 공격에 대한 안전성은 DDH 가정과 동등하다는 것은 잘 알려진 사실이다[14]. 중요한 점은 이 안전성은 평문의 암호에서 항상 새로운 키를 생성해야만 보장된다는 점으로, KEM의 경우도 일반적으로 일회성 키를 암호화하는데 사용되며 KEM-DEM 모델의 안전성도 일회성 키에 대해서만 보장된다[11,8]. 이는 KEM과 키 일치 또는 교환 프로토콜과의 차이점을 보여주는 하나의 예라고 볼 수 있다.

2. KEM의 안전성

앞에서 언급한 바와 같이 KEM-DEM 모델의 장점은 KEM과 DEM을 분리해서 생각할 수 있다는 점이다. 특히 KEM과 DEM이 각각의 안전성 요건을 만족하면, KEM-DEM 모델에 대한 증명가능한 안전성을 보장할 수 있다[12]. 그러므로 본 소절에서는 KEM이 가져야 할 안전성 요건에 대해 좀 더 엄밀하게 알아보도록 한다.

안전성의 수준을 결정하기 위한 목표로 여러 가지 개념들이 소개되었는데[1] 여기서는 구별불가능성 (Indistinguishability (IND))에 대해서만 소개한다. 구별불가능성은 공격자가 선택한 두 개의 평문 m_0와 m_1을 임의로 선택하여 생성한 암호문 Enc (m_b) ($b\in\{0,1\}$)을 보고, 그것으로부터 평문을 제대로 찾을 확률이 거의 1/2로 같다는 것이다. 이러한 안전성 목표와 함께 공격자가 어느 정도의 힘을 가질 수 있는가를 나타내는 공격 모델 (attack model)의 형태로는 공격자가 자신이 임의로 선택한 평문을 암호화하여 이루어지는 단순한 선택 평문 공격 (chosen plaintext attack), 여기에다 공격하고자 하는 암호문을 얻기 전까지 임의의 암호문에 대한 평문을 얻을 수 있는 선택 암호문 공격 (chosen ciphertext attack), 그리고 여기에 더하여 공격하고자 하는 암호문을 얻은 후에도 암호문에 대응하는 평문을 얻을 수 있는 능동 선택 암호문 공격 (adaptive chosen ciphertext attack)으로 나눌 수 있다. 암호 시스템에

대한 이러한 안전성 수준은 이러한 안전성 목표와 공격 모델을 결합하여 나타낼 수 있는데, 최근의 안전성에 대한 연구는 대부분이 능동 선택 암호문 공격 모델에서의 구별불가능성 (IND-CCA2)에 초점이 맞춰지고 있다. 이러한 공개키 암호에서의 IND-CCA2 개념은 KEM에 다음과 같이 적용될 수 있다.

정의. KEM을 사용하는 암호 시스템과 다음의 게임을 수행하는 공격자 A를 생각해 보자.

1. 시스템은 KEM.KeyGen 알고리즘을 이용하여 임의의 키 쌍 $(pk, sk) \leftarrow \text{KEM.KeyGen}(1^k)$를 생성하고 pk 를 A 에게 전달한다.
2. A 는 임의의 암호문 C 에 대한 복호화를 시스템에 요청하고 시스템은 $\text{KEM.Decap}(1^k, sk, C)$를 A 에게 반환한다.
3. A 가 암호화를 요청하면 시스템은 다음을 계산한다.
   $(K^*, C^*) \leftarrow_R \text{KEM.Encap}(1^k, pk)$;
   $K^+ \leftarrow_R \{0,1\}^l$; $\sigma \leftarrow_R \{0,1\}$;
   만일 $\sigma = 0$ 이면 $K \leftarrow K^*$;
   아니면 $K \leftarrow K^+$.
   여기서 $l = \text{KEM.KeyLen}(k)$이다. 이어 시스템은 (K, C^*)를 반환한다.
4. A 는 C^*와는 다른 암호문에 대한 복호화를 시스템에 요청하며 시스템의 반환값은 단계 2와 같다.
5. A는 $\sigma' \in \{0,1\}$을 반환한다.

공격자의 이점 (advantage)은 공격자의 반환값 σ' 와 σ 가 같아지는 확률로 정의할 수 있으며 KEM의 이점은 임의의 공격자에 대한 이점 중 최대값으로 한다. KEM의 이점이 무시할 수 있을 만큼 작을 때, 이 KEM은 구별불가능이라고 하며 IND-CCA2 모델에서 KEM에 대한 (t, ε, q_D) 공격자는 t 시간 안에 q_D 만큼의 복호화 요청을 할 때 적어도 ε 보다 큰 이점 가지는 확률적 튜링 머신을 의미한다.

결국 KEM의 안전성은 키를 임의로 생성해서 암호화하는 KEM의 특별한 구조에 맞게 정의된 암호문 쌍과 임의의 쌍에 대한 공격자의 구별불가능성에 기반한다. 그러므로 상대적으로 IND-CCA2 안전성을 가지는 일반적인 공개키 암호 기법에 비해 효율적인 방법으로 안전성을 보장해 줄 수 있다.

암호 시스템의 IND-CCA2 안전성을 증명하기 위해서 일반적으로 기반 문제로의 축소 방법을 이용한다. KEM-DEM 기반 암호 기법의 경우 "game hopping" 기법을 이용하여 이러한 기반 문제로의 축소 방법을 실현한다. 이 기법은 IND-CCA2 안전성을 증명하기 위한 공격자와 simulator 사이의 기본적인 게임에서부터 시작하여, simulator가 공격자의 오라클 질의에 대응하는 방법에 대한 규칙을 게임마다 약간씩 변경하면서 공격자가 각 게임에서의 틈을 이용해 암호 시스템에 대한 어떠한 이점도 얻을 수 없도록 함으로써 안전성을 증명할 수 있다는 것이다. 이 기법은 크게 두 가지 중요한 부분으로 나눌 수 있는데 먼저 현재 정의한 게임으로부터 다음 게임의 오류 조건을 정의하는 부분과 두 게임의 차이는 공격자가 기반 문제를 해결하는 능력에 의존한다는 것을 보이는 부분으로 나눠진다. Game hopping 증명 기법에서 중요하게 사용되는 정리는 다음과 같다.

정리. U_1, U_2 그리고 F 를 어떠한 확률공간에서 정의된 사건이라 하자. 만일 사건 $U_1 \wedge \neg F$ 가 발생하면 $U_2 \wedge \neg F$ 가 발생하고 그 반대의 경우도 성립하면 다음이 성립한다.

$$| \Pr[U_1] - \Pr[U_2] | \leq \Pr[F].$$

KEM-DEM 모델에 대한 이러한 증명방법은 [12]에서 처음 도입되어 이후 제안된 여러 KEM-DEM 모델[3,9]의 증명에 적용되었다.

참고로 지금까지 하이브리드 암호의 안전성을 증명하기 위해서는 KEM이 위의 IND-CCA2 안전성을 만족해야 한다는 것이 핵심적인 것으로 인식되었다[3]. 하지만 이 조건이 필수적인 것은 아니라는 결과가 Kurosawa-Desmedt에 의해 최근 밝혀졌다[9]. 이 결과는 Cramer-Shoup 암호 기법[3]에 기반한 약한 안전성을 만족하는 KEM을 이용해 KEM-DEM 모델을 설계하고 이것이 IND-CCA2 안전성을 만족한다는 것을 증명함으로서 KEM의 IND-CCA2 안전성이 KEM-DEM 모델의 IND-CCA2 안전성을 위한 필수조건이 아님을 확인하였다.

Ⅲ. 공개키 암호 표준화 작업

ISO의 표준화 작업에서는 실용적인 암호를 위한 조건으로 임의의 길이를 가지는 메시지를 처리해야 한다는 점을 고려하였고, 이러한 성질을 만족하는 가장 보편적인 형태인 하이브리드 암호에 대해 증명가능한 안전성을 제공하는 일원화된 구조로 KEM-DEM 모델을 채택하여

〔표 2〕 표준화 작업에 제안된 암호 기법들

	암호 기법	NESSIE	ISO	CRYPTREC
DH 기반	ECIES-KEM		○	
	PSEC-KEM	○	○	○
	ACE-KEM	○	○	
RSA 기반	RSA-OAEP		○	○
	RSA-KEM	○	○	
	HIME(R)		○	

그 절차가 진행중에 있다[13,8]. ISO의 표준화 작업에서 KEM-DEM 모델이 제안되어 실제 적용되는 단계 사이에 사업이 진행되었던 NESSIE[11]의 경우 Phase II에 선정된 거의 모든 후보 알고리즘들이 KEM 모델에 적합하게 변경되었으며 최종적으로 선정된 권고 알고리즘들도 모두 KEM 모델들이다. CRYPTREC[7]의 경우는 KEM을 키 교환 알고리즘의 범주로 고려하여 DEM과 함께 사용할 것을 권고하였으며 PSEC-KEM이 유일하게 선정되었다. 물론 이러한 공개키 암호의 표준화 작업들이 하이브리드 형태의 암호만 채택한 것은 아니지만, 그 추세를 보면 하이브리드 방식에 중점을 둔 KEM 방식에 대한 비중이 높다고 볼 수 있다. 현재 NESSIE, ISO 그리고 CRYPTREC에 제안되었거나 제안된 암호 기법 중 KEM 기법으로 제안된 경우를 〔표 2〕에서 정리하였다. NESSIE의 경우는 권고 알고리즘만 표시하였고 RSA-OAEP와 HIME(R)은 KEM 방식은 아니지만 비교를 위해 포함하였다.

참고로 ISO의 경우 제한된 길이의 메시지를 암호화하는데 사용할 수 있는 암호 기법으로 RSA-OAEP와 HIME(R)을 선정하였다. ISO의 RSA-OAEP는 기본적인 OAEP[2]에 기반한 인코딩 방법을 사용하므로 본 논문에서는 같은 범주로 고려하였다.

Ⅳ. 결 론

공개키 암호의 실제 사용 방식을 하나의 모델로 특화시켜 만든 KEM은 그 자체의 효율성과 안전성 및 하이브리드 공개키 암호 설계를 위한 체계화된 구조를 보여준다는 점에서 최근의 표준화 작업에서 큰 비중을 차지하고 있다. KEM은 기존의 공개키 암호를 적용할 수 있는 하나의 연구 분야로 생각해 볼 수 있으며 이와 관련된 여러 가지 암호 이론들, 특히 효율적인 하이브리드 암호 설계를 위한 연구 결과가 점차 증가할 것으로 예상된다.

참 고 문 헌

〔1〕 M. Bellare, A Desai, D. Pointcheval, P. Rogaway, "Relations among notions of security for public-key encryption schemes", *Advances in Cryptology - CRYPTO'98*, Lecture Notes in Comput. Sci. 1462, pp. 26-46, 1998.

〔2〕 M. Bellare, P. Rogaway, "Optimal asymmetric encryption padding - How to encrypt with RSA", *Advances in Cryptology -EUROCRYPT'94*, Lecture Notes in Comput. Sci. 950, pp. 92-111, 1994.

〔3〕 R. Cramer, V. Shoup, "Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack", *SIAM J. Comput.*, 33(1), pp. 167-226, 2003.

〔4〕 A.W. Dent, "A designer's guide to KEMs", *Cryptography and Coding*, Lecture Notes in Comput. Sci. 2898, pp. 133-151, 2003.

〔5〕 T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms", *IEEE Trans. Info. Theory*, 31, pp. 469-472, 1985.

〔6〕 R. Gennaro, V. Shoup, "A note on an encryption scheme of Kurosawa and Desmedt", Cryptology ePrint Archive, Report 2004/196, 2004.

〔7〕 Information-technology Promotion Agency, Telecommunications Advancement Organization of Japan, "*CRYPTREC Report 2002*", 2003.

〔8〕 International Organization for Standardization, "*ISO/IEC CD 18033-2, IT Security techniques - Encryption algorithms - Part 2: Asymmetric cipher*", 2004.

〔9〕 K. Kurosawa, Y. Desmedt, "A new paradigm of hybrid encryption scheme", *Advances in Cryptology - CRYPTO 2004*, Lecture Notes in Comput. Sci. 3152, pp. 426-442, 2004.

〔10〕 S. Luck, "A variant of the Cramer-Shoup cryptosystem for groups of unknown

order", *Advances in Cryptology - ASIACRYPT 2002*, Lecture Notes in Comput. Sci. 2501, pp. 27-45, 2002.

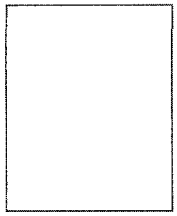
[11] B. Preneel, A. Biryukov, E. Oswald, B. van Rompay, L. Granboulan, E. Dottax, S. Murphy, A. Dent, J. White, M. Dichtl, S. Pyka, M. Schafheutle, P. Serf, E. Biham, E. Barkan, O. Dunkelman, M. Ciet, F. Sica, L. Knudsen, H. Raddum, "NESSIE security report (NESSIE Deliverable D20, version 2.0)", 2003.

[12] V. Shoup, "Using hash functions as a hedge against chosen ciphertext attack", *Advances in Cryptology - EUROCRYPT 2000*, Lecture Notes in Comput. Sci. 1807, pp. 275-288, 2000.

[13] V. Shoup, "A proposal for an ISO standard for public key encryption (version 2.1)", Cryptology ePrint Archive, Report 2001/112, 2001.

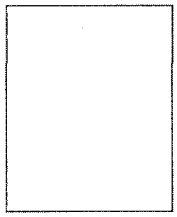
[14] Y. Tsiounis, M. Yung, "On the security of ElGamal based encryption", *Advances in Cryptology - ASIACRYPT 2000*, Lecture Notes in Comput. Sci. 1431, pp. 117-132, 1998.

〈著 者 紹 介〉



박 제 홍 (Je Hong Park)
정회원

1998년 2월 : 경북대학교 수학과 졸업
2000년 2월 : 한국과학기술원 수학과 석사
2004년 2월 : 한국과학기술원 수학과 박사
2004년 3월~현재 : 국가보안기술연구소 연구원
관심분야 : 암호이론



권 대 성 (Daesung Kwon)
정회원

1992년 2월 : 서울대학교 수학과 졸업
1994년 2월 : 서울대학교 수학과 석사
1999년 2월 : 서울대학교 수학과 박사
2001년 3월~현재 : 국가보안기술연구소 선임연구원
관심분야 : 암호이론