情 報 保 護 學 會 誌
第19卷 第4號, 2009. 8

ID 기반 암호방식을 이용한 데이터 공유와 권한 관리

박 광 용*, 송 유 진**

요 약

최근 인터넷의 급속한 보급으로 인해 많은 정보가 네트워크를 통해서 전송되고 있는 가운데 보안상의 위험을 고려하여 비밀정보를 암호화하여 전송한다. 본 논문에서는 비밀정보를 안전하게 보내기 위해 ID기반 암호방식을 이용하여 암호화된 데이터의 공유와 권한관리에 대하여 검토하고자 한다.

Ⅰ. 서 론

최근 인터넷의 급속한 보급으로 인해 많은 정보가 네트워크를 통해서 전송되고 있다. 그리고 비밀정보는 보안상의 위험성을 고려하여 암호화되어 전송된다. 암호화 방식은 대칭키 암호방식, 비대칭키 암호방식[1] 및 공개키를 ID로 사용하는 ID기반 암호방식[2]이 있다.

대칭키 암호방식은 암호화를 위해 송신자와 수신자 간에 암호화키 정보를 공유하여야 한다. 이때, 암호화키는 비밀채널을 통해 송신자와 수신자에게 전달된다. 하지만 암호화키를 송/수신자 모두 공유해야 하는 번거로움이 생기게 된다. 따라서 암호화키를 공유하기 위해서 공개키 암호를 사용하는 것이 일반적이다.

공개키 암호방식(Public Key Encryption)[1]은 기존의 대칭키 암호방식과 달리 암호화할 때 사용되는 공개키와 복호화할 때 사용되는 비밀키(복호키)가 서로 다르기 때문에 암호화키를 공개할 수 있어 용이하게 키의 공유가 가능하다. 따라서 수신자는 비밀키 생성기관(PKG, Private Key Generator)를 통해 공개키와 비밀키를 부여받고 인증채널을 이용하여 공개키를 공개한다. 송신자는 공개키로 암호화한 후 수신자에게 비밀정보를 전송하게 된다.

그러나 공개키 암호방식은 공개키와 비밀키를 생성할 때, PKG를 통해 생성됨으로 공개키와 개체의 관계 정당성에 대한 확인이 필요하며 그에 대한 관리가 큰 부하로 발생되고 있다.

이러한 문제를 해결하기 위해 각 개체에 대한 식별자(Identity)를 이용한 방법이 제안되었다[2]. 여기서 식별자란 각 개체를 나타내는 정보를 뜻한다. 즉, ID나 메일, 주소, 소속 및 연령 등 유일하게 특정할 수 있는 것을 말한다. 이러한 식별자를 공개키로 사용함으로써 송신자는 그 정당성을 각자 확인할 수 있게 되어 정당성에 대한 확인이 필요없게 된다. 최근 공개키에 대한 정당성 확인 과정이 필요없이 ID 등의 식별자만으로 간편하게 암호화가 가능한 ID 기반 암호방식[2]이 제안되었다.

ID 기반 암호화 방식(IBE, Identity Based Encryption)은 각 개체의 ID나 메일 등을 기초로 공개키가 생성되기 때문에 키 관리가 용이하다. 즉, 공개키 암호방식과 달리 자신의 ID를 PKG에 한번의 등록으로 비밀키가 생성되고 자신의 ID가 공개키가 되는 것이다. 여기서, ID와 개체는 1대1 관계에 있다. 2001년에 구체적인 방식이 최초로 제안[3]되어 지금까지 많은 연구가 진행되고 있다[12][13][14].

본 논문에서는 ID 기반 암호방식을 이용하여 복호권한을 양도하는 데이터 공유 방식에 대해 검토한다. 복호권한을 양도하는 키는 ID를 기반으로 생성할 수 있다. 그러나 ID만으로 복호 권한을 양도할 수 있으면 누구라도 복호화가 가능하여 데이터의 기밀성을 유지할 수 없다. 따라서 공개키와 쌍이 되는 비밀키와 ID를 기반으로 복호 권한의 양도 키를 생성한다. 이 복호 권한 양도의 기반이 되는 방식은 1998년 Blaze et al.의 「atomic proxy cryptography」이라는 개념이다[8]. 2005년에는

* 동국대학교 전자상거래협동과정 (freemickey@dongguk.ac.kr)
** 동국대학교 정보경영학과 (song@dongguk.ac.kr)

Ateniese et al.의 Proxy Re-encryption 방식이 있다[9]. 이러한 방식들은 암호문의 변환에 관한 방식이지만 본 논문의 방식은 비밀키(복호키)를 재설정하는 방식이다.

본 논문은 다음과 같이 구성된다. 2장에서 관련 연구로서 ID 기반 암호방식과 안전성에 대해 알아보고 3장에서는 ID 기반 암호방식을 이용한 데이터 공유와 권한 관리에 대해 검토하고 4장에서 결론을 맺는다.

Ⅱ. 관련 연구

2.1 쌍선형 사상(Bilinear Mapping)

2개의 순회군(Cyclic Group) G_1, G_2에 대해 쌍선형 사상 e: $G_1 \times G_2 \rightarrow G_T$($G_T$는 쌍선형 사상의 출력 공간)는 다음의 성질을 갖는다.

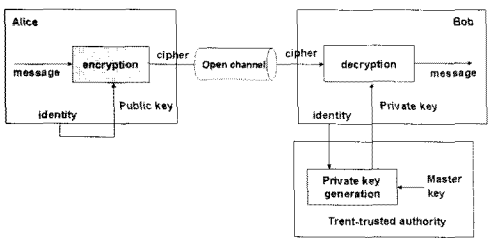
(1) 쌍선형성(bilinear) : 모든 $u \in G_1$, $v \in G_2$ 및 모든 a, $b \in Z$에 대해 $e(u^a, v^b) = e(u, v)^{ab}$가 성립된다.

(2) 비퇴화성(non-degenerate) : G_x (x = 1, 2)의 생성원 $g \in G_x$에 대해 $e(g, g) \neq 1$이다.

(3) 계산가능성(computable) : 모든 $u \in G_1$, $v \in G_2$에 대해서 e(u, v)를 계산하는 효율적인 알고리즘이 존재한다.

2.2 ID 기반 암호방식

ID 기반 암호방식은 암호화시 수신자의 ID를 이용하여 암호화하는 방식으로 암호문 수신자는 PKG로부터 비밀키를 도출하여 복호하는 방식이다[그림 1]. ID 기반 암호방식은 1984년 A. Shamir에 의해 처음 제안되었다[2].



〔그림 1〕 Identity Based Encryption

ID, 이메일, IP주소 등과 같은 사용자의 잘 알려진 정보로부터 사용자의 공개키를 생성한다. 하지만 사용자는 자신의 비밀키를 직접 만들 수 없으며 PKG을 통해 발급받아야만 한다[7]. ID 기반 암호방식은

- 사용자들은 다른 사용자의 공개키를 직접 그 사용자 정보로부터 생성할 수 있고
- 기존 공개키 암호방식과 달리 공개키와 사용자를 연결해 주는 인증서가 필요 없으며
- 시스템 복잡도를 낮추며 공개키 프레임워크의 확립 및 관리와 비용절감 효과가 있다.

2.3 Boneh Franklin의 ID 기반 암호방식[3]

Boneh Franklin의 ID 기반 암호방식은 다음 4가지 알고리즘으로 구성된다.

(1) Setup(k) : 보안 파라미터를 입력하여 그 값에 대응하는 공개 파라미터와 마스터 키를 출력하는 알고리즘

① $[q, G_1, G_2, e] \leftarrow G(k)$, $P \leftarrow G_1$, $s \leftarrow Z_q^*$, $P_{pub} = sP$을 생성한다.

② $H_1 : \{0,1\}^* \rightarrow G_1^*$고 $H_2 : G_2 \rightarrow \{0,1\}^n$이다.

③ params = $\langle q, G_1, G_2, e, n, P, P_{pub}, H_1, H_2 \rangle$, 마스터 키는 s이다.

(2) KeyGen(ID, params, s) : 마스터 키와 수신자의 ID를 입력하여 그 ID에 대응하는 비밀키를 출력하는 알고리즘

① 비밀키 $d_{ID} = sQ_{ID}$를 생성한다. 여기서, $Q_{ID} = H_1(ID)(\in G_1^*)$이다.

(3) Enc(params, ID, m) : 공개 파라미터와 수신자의 ID와 평문을 입력하여 그 평문에 대응하는 암호문을 출력하는 알고리즘

① $Q_{ID} = H_1(ID)$와 $r \leftarrow Z_q^*$을 랜덤하게 선택하고 $c = \langle rP, m + H_2(g_{ID}^r) \rangle$를 계산한다. 여기서, $g_{ID} = e(Q_{ID}, P_{pub})$이다.

(4) Dec(params, $c = \langle U, V \rangle$, d_{ID}) : 비밀키와 암호문을 입력하여 암호문에 대응하는 평문(대응이 없는 경우는 $\perp$)을 출력하는 알고리즘

$m = V + H_2(e(d_{ID}, U))$

2.4 ID 기반 암호의 안전성[3][4][6]

ID 기반 암호는 Bilinear Diffie-Hellman (BDH) Assumption 문제를 계산하는 것이 어렵다는 가정하에 랜덤오라클 모델에서 CPA(선택평문공격)에 대해 안전하다는 것이 증명되었다. ID 기반 암호방식의 안전성 근간이 되는 BDH 가정을 검토하면 다음과 같다.

(1) Decisional BDH Assumption

임의로 g, g_a, g_b, $g_c \in G$, $T \in G$를 설정한다. {g, g_a, g_b, g_c, $e(g,g)_{abc}$}와 {g, g_a, g_b, g_c, T}를 다항식 시간내의 알고리즘에 의해 1/2 이상의 확률로 식별할 수 없다.

(2) Computational BDH Assumption

임의로 g, g_a, g_b, $g_c \in G$를 설정한다. 이 값보다 $e(g, g)^{abc}$를 다항식 시간내의 알고리즘에 의해 산출할 수 없다.

ID 기반 암호방식의 안전성을 검토할 때, 일반적인 기준이 되는 안전성 확보 기준, ID의 취약성 유무, 공격의 종류에 대해 설명한다.

안전성을 확보하는 기준으로써 다음의 4가지가 있다.

- One-Wayness(OW) : 암호문으로부터 원래의 평문을 복원할 수 없다
- Semantic Security(SS) : 암호문으로부터 평문의 정보가 1 비트도 노출되지 않는다
- Indistinguishability(IND) : 암호문으로부터 평문의 어떠한 부분 정보도 얻을 수 없다.
- Non-Malleability(NM)[11] : 암호문이 공격자에 의해 조작되더라도 조작된 암호문을 복호화 했을 때 평문과의 어떠한 관계도 찾을 수 없어야 한다.

여기서, 일반적으로 OW ! SS = IND ! NM이다. (! : 왼쪽보다 오른쪽이 안전성이 높음, = : 안전성이 동일함을 의미)

ID의 취약성 유무란, ID 공간상에서 안전성이 파괴되는 ID 존재의 유무를 의미한다. 취약한 ID가 존재하는 경우를 Selective ID(sID), 취약한 ID가 존재하지 않는 경우를 Adaptive ID(ID)라고 한다. 이 경우, sID보다 ID의 안전성이 강하게 된다.

공격의 종류란, 공격할 때 힌트로서 얻을 수 있는 정보의 종류로써 다음의 2가지가 있다.

- 선택평문 공격(CPA) : 임의의 평문에 대응하는 암호문을 얻을 수 있다.
- 선택암호문 공격(CCA) : 임의의 암호문에 대응하는 평문을 얻을 수 있다

ID 기반 암호 등의 공개키 암호에서 CPA의 상황은 분명(공개키를 근거로 임의의 평문에 대한 암호문을 작성) 하기 때문에 최소한 CPA에 대한 안전성은 확보할 수 있고 나아가 현재 가장 강한 공격이라고 생각되는 CCA에 대한 안전성을 만족하는 것이 바람직하다.

ID 기반 암호방식의 안전성을 검토할 때 이들 3종류의 조합으로 안전성을 검토할 수 있다. 예를 들면 IND-ID-CCA 나 NM-sID-CPA 등이다. 여기서, 가장 강하다고 간주되는 조합인 NM-ID-CCA 의 안전성을 만족시키는 방식을 지향해야 하지만 NM-ID-CCA와 IND-ID-CCA의 안전성은 동일하다는 것이 알려져 있기 때문에 ID 기반 암호방식에서는 IND-ID-CCA의 안전성을 달성하는 것이 중요하다.

Ⅲ. ID 기반 암호방식을 이용한 데이터 공유와 접근 제어

ID 기반 암호방식을 이용하여 복수의 사용자가 기밀 데이터를 효율적으로 공유하는 방식에 대해 검토한다[5].

본 방식은 ID 기반 암호를 사용하여 PKG와 다른 관리자(Adm)를 설정하여 이 관리자가 해당 그룹에서 데이터를 공유하기 위한 공개키 설정과 해당 그룹 각 멤버의 ID를 기반으로 복호 권한을 양도하는 방식이다. 본 방식은 D. Boneh et al.의 ID 기반 암호인 sIBE[4]를 수정한 ID 기반 암호인 mIBE(modified ID Based Encryption)이다.

mIBE를 구성하기 위해 필요한 4가지 기본요소 SEK, MAC, KDF, TCR에 대해 설명한다[10].

(1) SEK(Symmetric Encryption)

- SEK.Enc(암호화 알고리즘) : 대칭 암호화키 K를 이용하여 평문 m $\in \{0, 1\}^*$을 암호화 한다.
  $e_M = SEK.Enc(K, m)$
- SEK.Dec(복호화 알고리즘) : 암호문 e_M을 대칭키 K로 복호화하여 평문을 얻는다.
  $m = SEK.Dec(K, e_M) \in \{0,1\}^*$

(2) MAC(Message Authentication Code)

- 메시지 인증키 k를 이용하여 암호문 $e_M \in \{0,1\}^*$에

대한 tag를 생성한다.

$tag = MAC(k, e_M)$

(3) KDF(Key Derivation Function)

- $v \in G$ 를 만족하는 메시지 인증키 k와 대칭 암호화키 K를 생성한다.

$(k, K) = KDF(v)$

(4) TCR(Target Collision Resistance)

- $TCR: G \times G \rightarrow F_q$

$u_1 = g_1^r, u_2 = g_2^r$ 주워졌을 경우 랜덤 $r \in Z_p$에 대해 $H(u_1, u_2)$가 되는 $H(u_1^*, u_2^*)$을 구하는 것은 어렵다. 여기서, 해시함수 H : G x G -> Zq이다.

3.1 mIBE(modified ID Based Encryption)

(1) mIBE.Setup : 군 G, W, Bilinear map e, SEK, MAC, KDF, TCR 등의 구조를 설정한다.

master secret key : msk.IBE

$= (\rho_1 = g^a, \rho_2 = g^b \in G, a, b, x, y \in F_q)$

master public key : Params

$= (g, h_1 = g^x, h_2 = g^y \in G; c, d \in W,$

$c = e(\rho_1, g) = Z^a, d = e(\rho_2, g) = Z^b)$

여기서, $Z = e(g, g)$

(2) mIBE.Gen : PKG는 mIBE.Setup의 구조를 이용하여 mIBE로 사용하는 키를 생성한다.

- PKG는 msk.mIBE와 Params를 기초로 ID기반 암호 mIBE의 공개키인 ID에 대응하는 비밀키 sk(ID)를 생성하여 안전한 방법(secure channel)으로 ID에 대응하는 사용자에게 분배한다.

$sk(ID) = sk_1, sk_2, sk_3$

$\rho_1 (h_1^{ID} h_2)^r, \rho_2 (h_1^{ID} h_2)^r, g^r$

(3) mIBE.Enc : 공개키 ID, 공개 데이터 Params을 기초로 평문(plaintext) m을 암호화하여 암호문(ciphertext) CM를 작성한다.

$mIBE.Enc(Params, ID, m) = C_M$

$= \{u_1, u_2, e_M, tag\}$

① t를 랜덤하게 선택한 후, u_1과 u_2를 생성한다.

$t \xleftarrow{rand} F_q(random);$

$u_1 \leftarrow g^t; u_2 \leftarrow (h_1^{ID} h_2)^t;$

② u_1, u_2를 TCR요소를 이용하여 α를 생성하고 t를 이용하여 v를 생성한다.

$\alpha \leftarrow TCR(u_1, u_2); v \leftarrow c^t d^{t\alpha} = Z^{at} Z^{bt\alpha};$

③ 생성된 v를 KDF요소를 이용하여 메시지 인증키 k와 대칭 암호키 K를 생성한다.

$(k, K) \leftarrow KDF(v);$

④ 메시지 m을 대칭 암호키 K로 암호화 한다.

$e_M \leftarrow SEK.Enc(K, m);$

⑤ 암호화된 e_M은 메시지 인증키 k로 tag를 생성한다.

$output\ C_M = \{u_1, u_2, e_M, tag\}$

따라서, 생성된 암호문 C_M은 다음과 같다.

$output\ C_M = \{u_1, u_2, e_M, tag\}$

(4) mIBE.Dec : 비밀키 sk(ID)를 이용하여 암호문 C_M을 복호 한다.

$mIBE.Dec(sk(ID), C_M) = m$

$\alpha \leftarrow TCR(u_1, u_2);$

$v \leftarrow \dfrac{e(sk_{ID1}, u_1) e(sk_{ID2}, u_1)^\alpha}{e(sk_{ID3}, u_2)^{1+\alpha}}$

$= \dfrac{e(\rho_1 (h_1^{ID} h_2)^r, g^t) e(\rho_2 (h_1^{ID} h_2)^r, g^t)^\alpha}{e(g^r, (h_1^{ID} h_2)^t)^{1+\alpha}}$

$= e(\rho_1, g^t) e(\rho_2, g^t)^\alpha = Z^{at} Z^{bt\alpha} = c^t d^{t\alpha};$

$(k, K) \leftarrow KDF(v);$

$if \quad tag \neq MAC(k, e_M);$

$\quad then\ output\ reject;$

$else$

$\quad m \leftarrow SEK.Dec(K, e_M);$

$output \quad m$

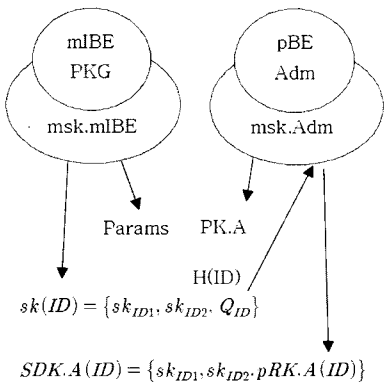
3.2 Proxy를 이용한 데이터 공유 방식

3.2.1 개요

mIBE를 이용한 데이터 공유 방식인 pBE를 검토한다. [그림 2]는 데이터 공유 방식 pBE의 구성을 나타낸다[5].

ID기반 암호방식을 이용해서 mIBE는 PKG에서 사용자 ID에 대응하는 비밀키 sk(ID)를 생성한다. 여기서, pBE는 데이터를 공유하는 그룹에서 PKG와 다른 관리자(Adm)가 설정되어 해당 그룹에서 공유하는 공개키

PK.A를 생성한다. 관리자(Adm)는 PKG가 분배한 비밀키 sk(ID)의 요소를 ID 기반으로 해시함수를 이용하여 Q_{ID}를 기초로 공개키 PK.A의 복호 권한을 양도하는 Proxy-Key pRK.A(ID)를 ID의 사용자에게 분배한다.



〔그림 2〕 Proxy를 이용한 데이터 공유 방식

3.2.2 알고리즘 상세

pBE는 다음의 6가지 알고리즘 {pBE.Setup, pBE.Gen, pBE.Enc, pBE.Der, pBE.Ktr, pBE.Dec}으로 구성된다.

(1) pBE.Setup : ID기반 mIBE의 PKG는 mIBE.Setup에 의해 msk.IBE(master secret key), Params(master public key)를 정하고 mIBE.Gen에 의해 사용자 ID에 대응하는 비밀키 sk(ID)를 생성하여 분배한다.

$$sk(ID)=\{sk_{ID1}, sk_{ID2}, Q_{ID}\}$$
$$=\{\rho_1(h_1^{ID}h_2)^r, \rho_2(h_1^{ID}h_2)^r, g^r\}(r\in Fq)$$

- r은 랜덤값
- Q_{ID}=H(ID)는 hash 함수 H를 사용

$$sk(ID)=\{\rho_1 Q_{ID}^{(xID+y)}, \rho_2 Q_{ID}^{(xID+y)}, Q_{ID}\}$$

비밀키를 이와 같이 설정해 두면 비밀키의 요소 Q_{ID}는 ID를 기초로 취득하는 것이 가능하다. 또한 복호 권한을 양도하기 위해 사용하는 master proxy-key σ = y/x를 작성하여 공개한다.

(2) pBE.Gen : 데이터를 공유하는 그룹에 msk.Adm을 이용하여 PK.A를 생성한다.

- msk.Adm
  (master secret key of Administrator)
  $msk.Adm\ \ S\in F_q$ (임의의 string)
- PK.A
  (public key generated by administrator)
  $PK.A=\{g, L\}\in G^2$
  $g\in G, L=h_1^S h_2=g^{xS+y}\in G$

(3) pBE.Enc : mIBE에 대해 ID를 S(=msk.Adm)로 했을 경우 공개키 PK.A로 암호화한다.

$$pBE.Enc(Params, PK.A, m)=C_M$$
$$=\{u_1, u_2, e_M, tag\}$$
$$u_1=g^t, u_2=L^t;$$
$$(m: plaintext;\quad t\in F_q: random)$$

즉, $pBE.Enc(Params, PK.A, m)$
$= mIBE.Enc(Params, S, m)$

(4) pBE.Dec : mIBE에서의 복호 처리와 동일하다. ID를 S(=msk.Adm)로 간주하고 대응하는 비밀키를 sk(S)로 하여 복호화한다.

$$pBE.Dec(sk(S), C_M)=pBE(SDK.A(ID), C_M)$$
$$= mIBE.Dec(sk(ID), C_M)=m$$

3.3 접근 권한 양도

공개키 PK.A로 작성된 암호문 C_M의 복호 권한을 ID의 사용자에게 양도한다. 이 암호문은 비밀키 sk(S)로 복호할 수 있지만 ID의 사용자가 소유하는 비밀키 sk(ID)와는 다르다. 따라서, 관리자 Adm은 비밀키 sk(ID)의 요소 $Q_{ID}=H(ID)$를 취득하여 이 값을 기초로 복호 권한을 양도하는 proxy-key를 생성하여 ID의 사용자에게 분배한다.

(1) pBE.Der (proxy-key의 생성)

사용자(ID)에게 복호권한을 양도하는 키 pRK.A(ID)를 ID, σ, msk.Adm(=S)를 이용하여 생성한다.

$$pBE.Der(S, \sigma, ID)=pRK.A(ID)$$
$$=H(ID)^\tau=Q_{ID}{}^\tau$$
$$\tau=\frac{ID+\sigma}{S+\sigma}$$
$$(\sigma=y/x;\ master\ proxy-key)$$

(2) pBE.Ktr (복호 비밀키의 재설정)

관리자(Adm)의 proxy-key pRK.A(ID)를 기반으로 비밀키 sk(ID)로부터 복호 비밀키 SDK.A(ID)를 재설

정한다.

$$pBE.Ktr(sk(ID), pRK.A(ID)) = SDK.A(ID)$$
$$= \{sk_{ID_1}, sk_{ID_2}, Q_{ID}{}^{\tau}\}$$

SDK.A(ID)는 sk(ID)의 요소 Q_{ID}로 부터 pRK.A (ID)로 재설정된다. 공개키 PK.A로 작성한 암호문 C_M은 재설정된 복호 비밀키 SDK.A(ID)로 복호하는 것이 가능하다. 즉,

$$pBE.Dec(sk(S), C_M) = pBE(SDK.A(ID), C_M)$$
$$= mIBE.Dec(sk(ID), C_M) = m$$

Ⅳ. 결 론

본 논문에서는 공개키 암호방식에서 공개키 정당성의 확인 문제를 해결하기 위해 ID기반 암호를 이용하여 데이터의 공유 및 권한 관리가 가능한 ID 기반 암호방식인 pBE에 대해 검토하였다.

ID 기반 암호방식을 이용한 데이터 공유와 권한 관리는 여러 가지 응용 가능성이 있다. 예를 들면, 의료정보의 권한 관리나 데이터 공유를 위한 응용이 가능할 것이다. 향후, ID 기반 암호방식의 구현을 통한 안전성, 효율성 분석과 응용 가능성에 대한 분석이 필요할 것이다. 또한, 암호문의 변환을 통해 복호 권한을 위임하는 Proxy Re-encryption 방식에 관한 검토 결과를 근간 보고할 예정이다.

참고문헌

[1] W. Diffie and M. E. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, vol. IT-22, no. 6, pp. 644-654, Nov. 1976.

[2] A. Shamir, "Identity-based cryptosystems and signature schemes," Proc. of Crypto'84, LNCS 196, pp. 47-53, 1984.

[3] D. Boneh and M. Franklin, "Identity based encryption from the weil pairing," Proc. of Crypto'01, LNCS 2139, pp. 213-229, 2001.

[4] D. Boneh and X. Boyen, "Efficient selective-id secure identity based encryption without random oracles," Proc. of Eurocrypt'04, LNCS 3027, pp. 223-238, 2004.

[5] 扇 裕和, "IDベース暗号をもとに構成した公開鍵の合成方式とアクセス管理," The 2009 Symposium on Cryptography and Information Security Otsu, Japan, pp. 20-23, Jan. 2009.

[6] D. Boneh and X. Boyen, "Secure identity based encryption without random oracles," Proc. of Crypto'04, LNCS 3152, pp. 443-459, 2004.

[7] 김광조, 김진, 여운동, "ID 기반 암호시스템," 2005 tech-issue energing s&t report, KISTI, 한국과학기술정보연구원, 2005.

[8] M. Blaze, G. Bleumer and M. Strauss. "Divertible protocols and atomic proxy cryptography," Proc. of Eurocrypt'98 LNCS 1403, pp. 127-144, 1998.

[9] G. Ateniese, K. Fu, M. Green and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," In Network and Distributed System Security Symposium, pp. 29-44, 2005.

[10] R. Genaro and V. Shoup, "A note on an encryption scheme of Kurosawa and Desmedt," IACR ePrint archive 2004/194, 2004

[11] Danny Dolev, Cynthia Dwork, and Moni Naor, "Non-malleable cryptography," Proc. of the twenty-third annual ACM symposium on Theory of computing, pp. 542-552, 1991.

[12] D. Boneh, X. Boyen, and E. Goh, "Hierarchical identity based encryption with constant size ciphertext," Proc. of Eurocrypt'05, LNCS 3494, pp. 440-456, 2005.

[13] J. Horwitz and B. Lynn, "Toward hierarchical identity-based encryption," Proc. of Eurocrypt' 02, LNCS 2332, pp. 466-481, 2002.

[14] C. Gentry and A. Silverberg, "Hierarchical id based cryptography," Proc. of Asiacrypt'02, LNCS 2501, pp. 548-566, 2002.

〈著者紹介〉

박 광 용 (Kwangyong Park)

학생회원

2008년 2월: 동국대학교 전자상거래학과 졸업
2008년 3월~현재: 동국대학교 석사과정(전자상거래 기술전공)
<관심분야> 암호이론, 데이터베이스 보안, 유비쿼터스 프라이버시 보호

송 유 진 (Youjin Song)

정회원

1982년 2월: 한국항공대학교 전자공학과 학사
1987년 8월: 경북대학교 대학원 석사
1995년 3월: 일본 Tokyo Institute of Technology(동경공업대학) 정보보호학과 박사
1988년~1996년: 한국전자통신 연구원 선임연구원
2003년~2005년: 미국 University of North Carolina at Charlotte 연구교수
2006년 7월~8월: 일본 정보보호대학원대학(IISEC) 객원교수
1996년~현재: 동국대학교 정보 경영학과/대학원 교수
2005년~현재: 동국대학교 부설 전자상거래연구소 소장
1998년~현재: 한국정보보호학회 이사
2006년~현재: 국제e-비즈니스학회 이사
2006년~현재: 한국사이버테러정보전학회 이사
2001년: ICISC2001 운영위원장
2003년: 하계CISC2003 프로그램위원장
2006년: CISC-S2006 공동 프로그램 위원장
2007년: 한국정보시스템학회 추계학술발표대회 공동 조직위원장
<관심분야> Secret Sharing, Privacy Protection, 전자상거래 응용보안 (Location Privacy, 디지털컨텐츠 보호, SCM/CRM 보안 등), Context Aware Application Security