情 報 保 護 學 會 誌
第20卷 第2號, 2010. 4

속성기반 암호기술

박 광 용*, 송 유 진**

요 약

인터넷상에서 각종 민감한 데이터들이 공유·유통되어지는 가운데 외부공격자나 내부사용자의 관리 미흡으로 인해 데이터 유출문제가 발생되고 있다. 이를 안전하게 관리하기 암호방식으로 본 논문에서는 ID기반 암호의 확장된 개념의 속성기반 암호방식에 대해 검토한다. 그리고 속성기반 프록시 재암호화 방식도 함께 검토 하였다.

Ⅰ. 서 론

인터넷상의 네트워크를 통해 각종 민감한 데이터들은 공유·유통 되어지고 있다. 각 데이터들은 데이터베이스의 물리적인 장치에 저장된다. 하지만 외부 공격자나 내부 사용자의 관리미흡으로 인해 데이터 유출문제가 발생되고 있는 실정이다. 이러한 유출문제의 위험성을 해결하고자 데이터를 암호화하여 관리할 수 있다.

암호화 방식으로는 공개키 암호방식, ID기반 암호방식, 속성기반 암호방식이 활발히 연구되고 있다. 공개키 암호방식[1]은 현재 일상생활에서 전자서명 등에 사용되고 있으며, ID기반 암호방식[2]은 블랙베리라는 휴대폰에 적용되어 사용되고 있다. 그리고 ID기반 암호의 확장된 개념으로 속성기반 암호[4][10][11] 연구가 이루어 지고 있다.

먼저, 공개키 암호방식(Public Key encryption)은 상호간의 관계 정당성 문제가 발생되어, 이를 해결하기 위한 방법으로 ID기반 암호화 방식(Identity Based Encryption, IBE)이 2001년 Boneh 등에 의해 제안되었다[2]. ID기반 암호방식은 각 개체의 ID나 메일 등을 기초로 공개키가 생성되기 때문에 송신자는 그 정당성을 각자 확인할 수 있게 되어 정당성 문제를 해결할 수 있었다. 그리고 IBE의 개념을 확장한 형태로 Sahai등은 속성 기반암호(Attrubute Based Encryption, ABE)의 개념을 제안[4]하였다.

이 방식을 이용하면 각 개체의 속성(소속, 직무)등을 기초로 암복호화를 실시할 수 있다. ID기반 암호는 ID를 공개키로 이용한다면 속성기반 암호는 각 속성들을 기반으로 암복호화를 실시한다. ID기반암호는 ID와 개체가 1대1관계에 있다면 속성기반 암호는 속성과 개체는 반드시 1대1로 대응할 필요가 없다는 것이다. 그리고 속성 기반 암호는 그 속성에 대해 중복의 권한을 부여할 수 있다. 예를 들어 소속이 (내과)이고 직무가 (의사) 등 두 개의 속성을 가지고 있어야 그 권한을 부여받을 수 있다.

본 논문에서는 암호화 방식 중 속성을 이용한 암호방식에 대해 검토한다. 그리고 프록시 재암호화 기법[3]을 적용한 속성기반 암호방식[5][6]도 검토한다. 프록시 재암호화 기법은 프록시를 통해 암호문을 변환하는 방식으로 기존 공개키 암호화 방식에서는 송신자의 공개키로 암호화된 암호문을 수신자의 비밀키로 복호할 수 있도록 한다. 속성기반 프록시 재암호화 방식에서는 속성의 접근구조를 변경하여 재암호화 함으로써 다른 속성을 가진 개체도 암호문을 복호할 수 있다.

본 논문의 2장에서는 관련연구배경을 알아보고 3장에서는 속성기반암호 방식과 4장에서는 프록시 재암호화를 적용한 속성기반암호방식에 대해 알아보고 5장에서는 결론을 맺는다.

본 연구는 2009년도 정부(교육과기술부)의 재원으로 한국과학재단의 지원을 받아 수행된 연구임.(No. 2009-0083985)

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

Ⅱ. 관련연구배경

2.1 쌍선형 사상

2개의 순회군 G1 와 G2 에 대해 쌍선형 사상 e: G1×G2 → GT (GT는 쌍선형 사상의 출력 공간)는 다음의 성질을 가진다

(1) 쌍선형성(bilinear) : 모든 u∈G1, v∈G2 및 모든 a, b∈Z 에 대해 e(ua, vb) = e(u, v)ab 가 성립된다.

(2) 비퇴화성(non-degenerate) : Gx (x = 1, 2)의 생성원 g∈Gx 에 대해, e(g, g) ≠ 1 이다.

(3) 계산가능성(computable) : 모든 u∈G1, v∈G2 에 대해서 e(u, v)를 계산하는 효율적인 알고리즘이 존재한다.

2.2 Bilinear Diffie-Hellman Assumption(BDH)[7][8]

ID안전성에 근간이 되는 BDH 가정을 검토하면 다음과 같다.

(1) Decisional BDH(Bilinear Diffie-Hellman) assumption
임의에 g, ga, gb, gc∈G , T∈G 를 설정한다. {g, ga, gb, gc, e(g,g)abc }와 {g, ga, gb, gc, T}를, 유의의 다항식 시간내의 알고리즘에 의해 1/2 이상의 확률로 식별할 수 없다.

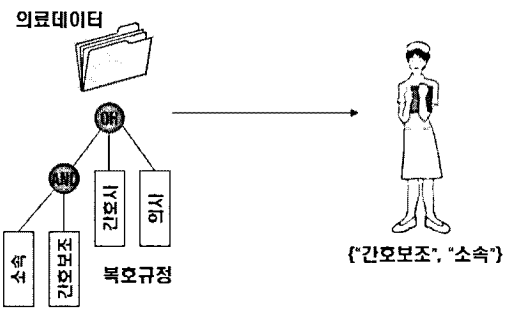
(2) Computational BDH (Bilinear Diffie-Hellman) assumption
임의에 g, ga, gb, gc∈G 를 설정한다. 이 값보다, e(g, g)abc를, 유의의 다항식 시간내의 알고리즘에 의해, 산출할 수 없다. (2) 항의 계산 양적 곤란성의 가정이 성립하면, (1) 항의 합계 산양적 곤란성의 가정도 성립한다.

Ⅲ. 속성기반암호

속성기반 암호는 개체의 속성 정보의 집합과 속성의 접근 구조를 바탕으로 암복호화를 실시하는 방식이다. 여기서 접근 구조[9]란 주어진 속성 집합에 대해 접근을 허가하는지 아닌지를 결정하는 방법이다. 속성집합을 입력하여 접근을 허가하는지 아닌지를 나타내는데 0은 접근 거부, 1은 접근 허가를 돌려주는 함수로 간주한다. 속성 기반암호의 접근구조는 암호화시에 지정하는 CP-ABE(Ciphertext-Policy)와 키생성시 지정하는 KP-ABE(Key-Policy)의 2종류가 있다.

3.1 CP-ABE(Ciphertext-Policy)[10]

CP-ABE는 암호문 생성시 송신자가 접근 구조를 지정하여 수신자의 속성 집합을 바탕으로 복호화를 한다. 예를 들어, [그림 1]에서 개체가 [간호보조], [소속]이라는 속성을 가지고 있을 경우, 송신자는 암호문에 [간호보조이고 소속이라면 복호 가능]이라는 접근구조 만들어 암호화 하면 접근구조를 만족하는 개체만이 복호가 가능하다.



〔그림 1〕 CP-ABE

우선 CP-ABE 암호는 이하의 4개의 알고리즘으로부터 구성된다.

(1) Setup(1^k) : 보안 파라미터 k 를 입력하여 그 값에 대응하는 공개키 PK와 마스터키 MK를 출력하는 알고리즘.

① $G=[p, G, G_T, g\in G, e] \leftarrow \geq n(1^k)$,
$w\in Z_p^*$를 랜덤하게 생성한다.

② 속성 i, $(1 \leq i \leq n)$에 대응하는 랜덤한 $a_i, \hat{a}_i, a_i^*, \in Z_p^*$를 선택한다.

③ $Y=e(g,g)^w$와
$A_i = g^{a_i}, \hat{A}_i = g^{\hat{a}_i}, A_i^* = g^{a_i^*}$ 계산한다.

④ PK는 $\langle Y, p, G, G_T, g, e, (A_i, \hat{A}_i, A_i^*)_{1 \leq i \leq n} \rangle$고
MK는 $\langle w, (a_i, \hat{a}_i, a_i^*)_{1 \leq i \leq n} \rangle$이다.

(2) KeyGen(MK, L) : 마스터키 MK와 속성 집합 L

을 입력하여 접근구조에 대응하는 비밀키 SK_L을 출력하는 알고리즘.

① 속성 집합 $L=[L_1, L_2, ..., L_n]$ 을 입력하여 비밀키를 생성한다.

② $s_i \in Z_p^*$를 랜덤하게 선택하고 $s=\sum_{i=1}^{n} s_i$, $D_0 = g^{w-s}$를 계산한다.$(1 \le i \le n)$

③ 만약에 $L_i = 1$이면 $[D_i, D_i^*] = [g^{\frac{s_i}{a_i}}, g^{\frac{s_i}{r}}]$를 계산하고 $L_i = 0$ 이면

$[D_i, D_i^*] = [g^{\frac{s_i}{a_i}}, g^{\frac{s_i}{a_i}}]$를 계산한다.

④ 비밀키는 $SK_L = \langle D_0, (D_i, D_i^*)_{1 \le i \le n} \rangle$이다.

(3) Encrypt(PK, M, W) : 공개키 PK와 접근구조 W와 평문 M을 입력하여 그 평문에 대응하는 암호문 CT을 출력하는 알고리즘.

① 접근 구조 $W=[W_1, W_2, ..., W_n]$와 평문 $M \in G_T$을 암호화 한다.

② 랜덤 값 $r \in Z_p^*$과 $\tilde{C} = MY^r, C_0 = g^r$ 를 계산한다.

③ 다음을 만족하는 C_i: $W_i = 1, C_i = A_i^r$, $W_i = 0, C_i = \widehat{A_i^r}$, $W_i = *, C_i = A_i^{*r}$를 계산한다$(1 \le i \le n)$.

④ 암호문은 $CT = \langle \tilde{C}, C_0, (C_i)_{1 \le i \le n} \rangle$이다.

(4) Decrypt(CT, SK_L) : 비밀키 SK_L와 암호문 CT을 입력하여 암호문에 대응하는 평문(대응이 없는 경우는⊥)을 출력하는 알고리즘.

① 암호문 $CT = \langle \tilde{C}, C_0, (C_i)_{1 \le i \le n} \rangle$와 비밀키 $SK_L = \langle D_0, (D_i, D_i^*)_{1 \le i \le n} \rangle$를 이용하여 복호화 한다.

$For\ 1 \le i \le n$

$$D'_i = \begin{cases} D_i & \text{if } W_i \neq * \\ D_i^* & \text{if } W_i = * \end{cases}$$

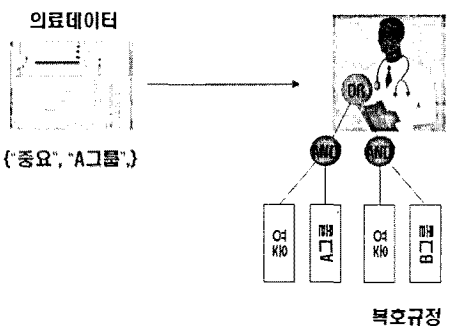
$$\frac{\tilde{C}}{e(C_0, D_0)\prod_{i=1}^{n} e(C_i, D'_i)} =$$

$$\frac{M(e(g,g)^w)^r}{e(g^r, g^{w-s})\prod_{i=1}^{n} e((g^{a_i})^r, g^{\frac{s_i}{a_i}})}$$

$$= \frac{M(e(g,g)^{w\tau})}{e(g^r, g^{w-s})\cdot e(g,g)^{s\tau}} = \frac{M(e(g,g)^{w\tau})}{e(g,g)^{w\tau}}$$

3.2 KP-ABE(Key-Policy)[11]

KP-ABE는 복호 가능한 속성 집합으로 송신자가 암호화 하고 수신자의 키 생성시 자신의 속성 집합에 근거하는 접근구조를 바탕으로 복호화한다. 예를 들어, [그림 2]에서 복호 가능한 속성 집합이 [중요, A그룹]으로 암호화된 암호문을 수신자의 속성 집합에 근거하는 접근구조에 [중요하고 A그룹 이면 복호가능]을 만족하면 복호가 가능하다.



[그림 2] KP-ABE

우선 KP-ABE 암호는 이하의 4개의 알고리즘으로부터 구성된다.

(1) Setup(1^k) : 보안 파라미터 k 를 입력하여 그 값에 대응하는 공개파라미터 PK와 마스터키 MK를 출력하는 알고리즘.

① 속성 $U=\{1, 2, \cdots, n\}$를 정의한다.

② 각각의 속성 $i \in U$에 포함시키고 랜덤한 Z_p로부터 숫자 t_i를 균등하게 선택한다.

③ 랜덤한 Z_p에 y를 균등하게 선택.

④ PK는 $< T_1 = g^{t_1}, \cdots, T_{|U|} = g^{t_{|U|}}, Y = e(g,g)^y >$고 MK는 $\langle t_1, \cdots, t_{|U|}, y \rangle$이다.

(2) Encrypt(PK, M, γ) : 공개파라미터 PK와 속성집합 T와 평문 M을 입력하여 그 평문에 대응하는 암호문 E을 출력하는 알고리즘.

① 속성 γ의 집합아래 암호화 메시지 $M \in G_2$하고 랜덤값 $s \in Z_p$를 선택한다.

② 암호문은

$E=<\gamma, E'=MY^s, E_i=T_i^{s \cdot q_x(0)}>$이다.

(3) KeyGen(MK, T) : 마스터키 MK와 공개 파라미터 PK을 입력하여 접근구조 A에 대응하는 비밀키 D을 출력하는 알고리즘.

① 만약에 $T(\gamma)=1$이면 복호화가 가능한 사용자에게 키를 출력한다.

② 다음의 비밀값 $D_x = g^{\frac{q_x(0)}{t_i}}$, $i=att(x)$를 사용자에게 준다.

(4) Decrypt(CT, D) : 비밀키 D와 암호문 E을 입력하여 암호문에 대응하는 평문(대응이 없는 경우는 $\perp$)을 출력하는 알고리즘.

① 암호문

$E=<\gamma, E'=MY^s, E_i=T_i^{s \cdot q_x(0)}>$와

비밀키 D, 노드 x의 입력으로 순환 알고리즘 DecryptNode(E, D, x)을 정의한다.

② G_2의 그룹 요소 또는 $\perp$를 출력한다.

③ 만약에 노드 x = LeafNode라면

DecryptNode(E, D, x)=$e(D_x, E_i)$

$= e(g^{\frac{q_x(0)}{t_i}}, g^{s \cdot t_i}) = e(g,g)^{s \cdot q_x(0)}$를 계산하고, $i \in \gamma$이면 $\perp$로 정의한다.

④ $F_z \neq \perp$면

$F_x = \prod_{z \in S_x} F_z^{\Delta i, S'_{f(z)}}$, $S'_x = index(z): z \in S_x$

$= \prod_{z \in S_x} (e(g,g)^{r \cdot q_z(z)})^{\Delta_{i,S'_x}}$

$= \prod_{z \in S_x} (e(g,g)^{r \cdot q_{parent(z)}(index(z))})^{\Delta_{i,S'_x}}$

$= \prod_{z \in S_x} (e(g,g)^{r \cdot q_x(0) \cdot \Delta_{i,S'_x}}$

$= e(g,g)^{s \cdot q_x(0)}$로 계산한다.

Ⅳ. 속성기반 프록시 재암호화

속성기반 Proxy 재암호화 방식은 기존의 Proxy 재암호화(공개키 or ID기반 암호시스템)를 속성기반 방식으로 확장한 개념이다. 즉, 접근제어 환경에서 사용자에게 복호권한을 위임할 수 있도록 한다. 사용자(속성에 의해 식별된)들은 하나의 접근정책에서 다른 접근정책으로 암호문을 재암호화 하는 Proxy를 자유롭게 지정할 수 있다.

4.1 CP-ABPRE[5]

CP-ABPRE 방식은 종전의 CP-ABE방식에서의 접근구조 AS로 암호화된 암호문 C를 다른 접근구조 AS'로 변환하는 Proxy를 지정하여 변경된 접근구조로 암호문 C를 C'로 변환하는 방식이다.

예를 들어 대학교의 개인정보시스템에 대한 어플리케이션 시나리오를 설명한다. 이 시스템에는 학생의 성적에 대한 정보가 있다. 이 정보들은 접근구조 AS ((AGE > 40) ∧ (Tenure))으로 암호화되어 있으며, 정교수 U_1은 접근구조 AS으로 암호화된 암호문 C을 복호할 수 있다. 하지만 정교수 U_1이 휴가중일 때, 성적정보를 복호할 수 있는 교무팀장 U_2가 필요한 경우가 있다. 여기서 교무팀장 U_2는 접근구조 AS'의 암호화된 암호문 C'을 복호할 수 있다.

이 경우 ABPRE로 복호할 수 있는 자격이 주어진 정교수 U_1은 접근구조 AS으로 암호화된 암호문 C을 다른 접근구조 AS'((Admin) ∧¬ (EXP < 10))로 변환하는 프록시를 지정할 수 있게 한다. 프록시는 접근구조 AS으로 된 암호문 C을 접근구조 AS'된 암호문 C'으로 변환한다. 따라서 기존의 접근구조 AS을 만족하는 정교수가 없어도 접근구조 AS', 적어도 10년이상의 근무경력을 가진 교무팀장은 교수의 대리인으로 암호화된 성적정보에 접근할 수 있다[그림 3].

우선 CP-ABPRE 암호는 이하의 6개의 알고리즘으로부터 구성된다[5].

(1) Setup(1^k) : 보안 파라미터 k 를 입력하여 , 공개 파라미터 pp와 마스터 키 mk를 생성하는 알고리즘.

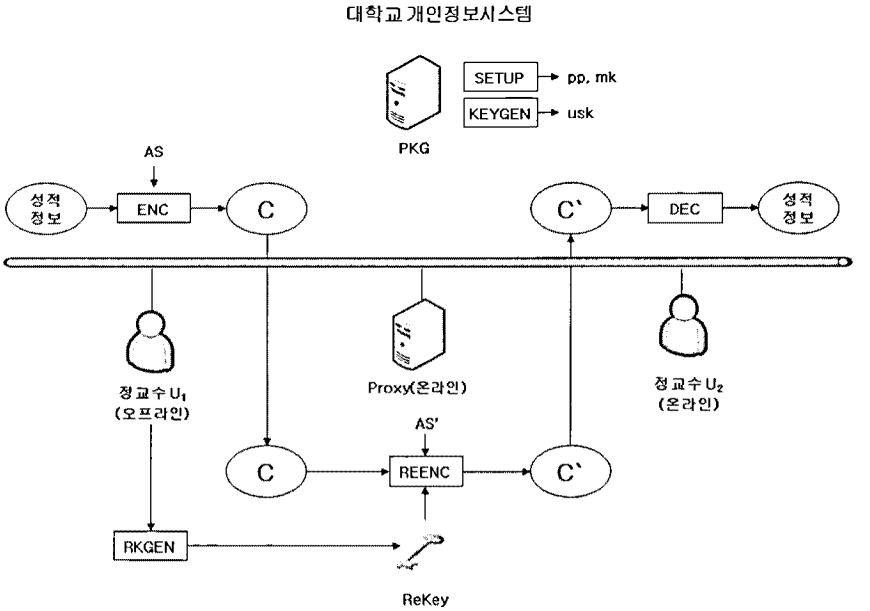
① $y, t_i \in Z_p$ 선택한다. ($1 \leq i \leq$ 3n)

② 생성원 $g, h \in G$을 랜덤하게 선택한다.

③ $Y=e(g,h)^y, T_i=g^{t_i}, T'_i=h^{\frac{1}{t_i}}$ ($1 \leq i \leq 3n$) 정의한다..

④ 공개 파라미터 pp는

$\langle e, gh, Y, T_i, T'_{i_{1 \leq i \leq 3n}} \rangle$이고 마스터키



〔그림 3〕 ABPRE 시스템의 관계(대학교 개인정보 시스템)

mk는 $\langle y, t_{i_{1\le i\le 3n}}\rangle$이다.

(2) KeyGen(S, mk) : 인덱스 집합 S와 마스터키 mk를 입력하여 비밀키 usk를 생성하는 알고리즘.

① 속성의 인덱스 집합을 S로 정의한다.

② $r_1, \ldots, r_n \in Z_p$을 랜덤하게 선택한다.

③ $r = r_1 + r_2 + \cdots + r_n$ 과 $\hat{D} = h^{y-r}$를 계산한다.

④ 만약에 $i \in S$이면 $D_{i,1} = h^{\frac{r_i}{t_i}}$, $D_{i,2} = h^{\frac{r_i}{t_{2n+i}}}$이고

$i \notin S$이면 $D_{i,1} = h^{\frac{r_i}{t_{n+i}}}$, $D_{i,2} = h^{\frac{r_i}{t_{2n+i}}}$이다.

⑤ 비밀키는 $usk = \langle S, (D_{i,1}, D_{i,2})_{i\in N}, \hat{D}\rangle$이다.

(3) Encrypt(AS, m) : 접근구조 AS와 메시지 m을 입력하여 암호문 C를 생성하는 알고리즘.

① 접근 구조 AS, 평문 $m \in G_T$을 정의한다.

② 랜덤 값 $s \in Z_p^*$ 선택한다.

③ $\tilde{C} = m \cdot Y^s$, $\hat{C} = g^s$, $\check{C} = h^s$을 계산한다.

④ $W_i = 0, C_i = \widehat{A_i^r}$, $W_i = *, C_i = A_i^{*r}$를 계산한다 $(1 \le i \le n)$.

⑤ AS가 $+d_i$이면 $C_i = T_i^s$이고

$-d_i$이면 $C_i = T_{n+i}^s$

$C_i = T_{2n+i}^s$이다.

⑥ 암호문은 $C = < AS, \tilde{C}, \hat{C}, \check{C}, (C_i)_{i\in N} >$다.

(4) RKExtract(usk, AS) : 비밀키 usk와 접근구조 AS를 입력하여 재암호화 키 rk를 생성하는 알고리즘.

① $d \in Z_p$를 랜덤하게 선택한다.

② $\nu = g^d, \hat{D}' = \hat{D}$를 정하고 ξ 는 $AS\nu$의 암호문이다.

③ 만약에 $i \in S$이면

$$D'_{i,1} = D_{i,1} \cdot (T_i')^d, D'_{i,2} = D_{i,2} \cdot (T_{2n+i})^d$$

$i \notin S$이면

$$D'_{i,1} = D_{i,1} \cdot (T'_{n+i})^d, D'_{i,2} = D_{i,2} \cdot (T'_{2n+i})^d$$

④ 재암호화 키는

$rk = < S, AS, (D'_{i,1}, D'_{i,2})_{i\in N}, \hat{D}, \xi >$이다.

(5) Re-encryption : 재암호화 키 rk와 암호문 C의 입력으로 재암호화된 rk에 인덱스 집합이 암호문 C의 접근구조를 만족하면 재암호화문 C'을 생성, 만족하지 않으면 reject하는 알고리즘.

① AS가 $+d_i$이면

$E_i = e(C_i, D'_{i,1}) = e(g^{t_i s}, h^{\frac{r_i+d}{t_i}})$
$= e(g,h)^{s(r_i+d)}$ 이며,
$-d_i$이면

$E_i = e(C_i, D'_{i,1}) = e(g^{t_{n+i} s}, h^{\frac{r_i+d}{t_{n+i}}})$
$= e(g,h)^{s(r_i+d)}$

$E_i = e(C_i, D'_{i,2}) = e(g^{t_{2n+i} s}, h^{\frac{r_i+d}{t_{2n+i}}})$
$= e(g,h)^{s(r_i+d)}$ 이다.

② $\hat{C}, \hat{D}'$을 사용하여 $\overline{C} = e(\hat{C}, \hat{D}') \prod_{i \in N} E_i$
$= e(g,h)^{ys+nds}$ 을 만든다.

③ 암호문은 $C' = < AS', \tilde{C}, \overline{C}, \check{C}, \xi >$
$C'_{re} = < AS', \tilde{C}, \overline{C}, \check{C}, \xi' >$이다.

(6) Decrypt(usk, C) : 비밀키 usk와 암호문 C을 입력하여 인덱스 집합이 암호문 C의 접근구조를 만족하면 메시지 m을 생성하고 만족하지 않으면 reject하는 알고리즘.

① AS가 $+d_i$이면

$E_i = e(C_i, D_{i,1}) = e(T^s, h^{\frac{r_i}{t_i}})$
$= e(g,h)^{sri}$ 이며,
$-d_i$이면

$E_i = e(C_i, D_{i,1}) = e(T^s_{n+i}, h^{\frac{r_i}{t_{n+i}}})$
$= e(g,h)^{sri}$,

$E_i = e(C_i, D_{i,2}) = e(T^s_{2n+i}, h^{\frac{r_i}{t_{2n+i}}})$
$= e(g,h)^{sri}$ 이다.

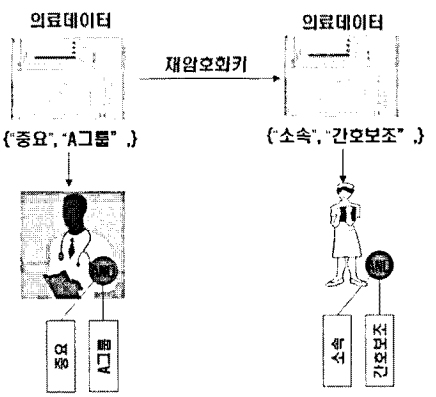
② 암호문 $C' = < AS', \tilde{C}, \overline{C}, \check{C}, \xi >$과 비밀키 $usk = \langle S, (D_{i,1}, D_{i,2})_{i \in N}, \hat{D} \rangle$를 이용하여 복호화 한다.

$$\frac{\tilde{C} e(\nu, \check{C})^n}{\overline{C}} = \frac{m \cdot e(g,h)^{ys} \cdot e(g^d, h^s)^n}{e(g,h)^{ys+nds}} = m$$

4.2 KP-ABPRE[6]

KP-ABPRE방식은 종전의 KP-ABE방식에서 키 생성시 수신자의 속성에 근거하는 접근구조로 송신자의 암호문을 복호할 수 있다. 이때, 다른 접근구조를 가진 수신자가 암호문을 복호하기 위해서는 송신자가 복호 가능한 속성을 통해 암호화된 암호문 C를 Proxy를 통하여 다른 접근구조 AS'로 변경하기 위한 재암호화 키 $rk_{AS \to AS'}$를 출력하여 암호문 C를 입력으로 암호문 C'로 변환하는 방식이다. 이렇게 하면 변경된 암호문 C'로 다른 접근구조를 가진 수신자가 암호문을 복원할 수 있게 된다.

예를 들면 [그림 4]에서 의료데이터 정보를 얻기 위해서는 [중요, A그룹] 이라는 접근구조를 만족하여야 한다. 하지만 [소속, 간호보조]의 접근구조에는 만족하지 못하므로 의료데이터를 얻을 수 없다. 이때, 재암호화 키를 이용하여 [중요, A그룹]의 속성으로 암호화된 암호문을 [소속, 간호보조]의 속성으로 재암호화 하여 접근구조 [소속, 간호보조]를 가진 사람도 의료데이터를 열람 할 수 있게 된다.



[그림 4] KP-ABPRE

우선 KP-ABPRE 암호는 이하의 6개의 알고리즘으로부터 구성된다[6].

(1) Setup(1^k) : 보안 파라미터 k와 System 파라미터에 의해 메시지 공간 M과 암호문 공간 C를 기술하는 알고리즘.

① 속성 $U = \{1, 2, \cdots, n\}$를 정의한다.

② 각각의 속성 $i \in U$에 포함시키고 랜덤한 Z_p로부터 숫자 t_i를 균등하게 선택한다.

③ 랜덤한 Z_p에 y를 균등하게 선택.

④ PK는
$< T_1 = g^{t_1}, \cdots, T_{|U|} = g^{t_{|U|}}, Y = e(g,g)^y >$고 MK는 $\langle t_1, \cdots, t_{|U|}, y \rangle$이다.

(2) KeyGen(MK, T) : 보안 파라미터 1^k의 입력으로 공개키 PK와 비밀키 SK를 출력하는 알고리즘.

① 만약에 $T(\gamma)=1$이면 복호화가 가능한 사용자에게 키를 출력한다.

② 다음의 비밀값 $D_x = g^{\frac{q_x(0)}{t_{q_x}}}$ where $i=att(x)$를 사용자에게 준다.

(3) Encrypt(PK, M, γ) : 속성 γ_1의 집합과 메시지 M을 통하여 암호문 C_1를 출력하는 알고리즘.

① 속성 γ_1의 집합아래 암호화 메시지 $M \in G_2$하고 랜덤값 $r \in Z_p$를 선택한다.

② 암호문은 $C=<\gamma, E=MY^r, E_i = T_i^{r_{i\in\gamma}}>$이다.

(4) RKExtract(γ_1, γ_2) : 비밀키 sk와 속성 γ_2의 집합의 입력으로 단방향성의 재암호화키 $rk_{1\to 2}$를 출력하는 알고리즘.

① 재암호화 키는

$RK_1^{A\to B} = t'_1/t_1, RK_1^{A\to B} = t'_2/t_2,$ 이다

$\cdots, RK_{|\gamma|}^{A\to B} = t'_{|\psi|}/t_{|\psi'|},$

(5) Re-encryption : 재암호화 키 $rk_{1\to 2}$과 암호문 C_1의 입력으로 재암호화된 암호문 C_2나 "부인"을 출력하는 알고리즘.

① γ_2은 수신자의 속성과 $s \in Z_p$의 집합이다.

② 재암호화된 암호문은

$C_2 = (\gamma', E' = MY^{rs},$ 이다.

$\left\{E_i = ((T_i^r)^{RK_i^{A\to B}})^s\right\}_{i\in\gamma})$

(6) Decrypt(E, D, x) : 비밀키 SK와 암호문 C_2을 입력하여 암호문에 대응하는 평문(대응이 없는 경우는⊥)을 출력하는 알고리즘.

① 첫 번째 단계의 암호문

$c_{\psi_1} = (\gamma_1, E' = MY^r, \{E_i = T_i^r\}_{i\in\gamma_1})$와

재암호화키 $RK_1^{A\to B} = t'_1/t_1, RK_1^{A\to B} = t'_2/t_2,$

$\cdots, RK_{|\gamma|}^{A\to B} = t'_{|\psi|}/t_{|\psi'|}$가 주어진다.

② 주어진 첫 번째 암호문과 재암호화키로 두 번째 단계의 암호문인

$C_{\psi_2} = (\gamma', E' = MY^{rs}, \left\{E_i = (T_i^{rs})^{RK_i^{A\to B}}\right\}_{i\in\gamma})$

$= (\gamma', E' = MY^{rs}, \{E_i = (T_i'^{rs})\})$을 얻게된다.

③ 만약에 노드 x = LeafNode라면

DecryptNode(E, D, x)=$e(D_x, E_i)$

$= e(g^{\frac{q_x(0)}{t_i}}, g^{s\cdot t_i})$

$= e(g,g)^{s\cdot q_x(0)}$를 계산하고, $i\in\gamma$이면 ⊥로 정의한다.

④ $F_z \neq \perp$면

$F_x = \prod_{z\in S_x} F_z^{\Delta i, S'_x(0)}$, $S'_x = index(z): z\in S_x$

$= \prod_{z\in S_x} (e(g,g)^{r\cdot q_z(0)})^{\Delta_{i,S'_x}}$

$= \prod_{z\in S_x} (e(g,g)^{r\cdot q_{parent(z)}(index(z))})^{\Delta_{i,S'_x}}$

$= \prod_{z\in S_x} (e(g,g)^{r\cdot q_x(0)\cdot\Delta_{i,S'_x}}$

$= e(g,g)^{s\cdot q_x(0)}$로 계산한다.

V. 결 론

본 논문에서는 ID기반 암호의 확장된 개념으로 속성기반 암호방식에 대해 검토해보았다. 기존의 ID기반 암호에서는 식별할 수 있는 아이디나 e-mail 등 하나의 속성으로 암호화 하였다. 하지만 속성기반 암호방식은 다수의 속성을 이용한 접근구조라는 개념을 적용하여 접근구조의 속성을 만족해야만 데이터의 복원을 가능하게 하였다.

본 연구의 결과로 속성기반 암호는 새로운 응용의 가능성을 나타내는 것으로 생각된다. 예를 들어 의료정보의 권한 관리나 데이터의 접근제어의 응용에 대한 가능성을 볼 수 있다. 따라서 향후 과제로써는 실제 속성기반 암호의 구현을 통한 안전성 및 효율성 분석과 응용가능성에 대한 정량적 분석이 필요할 것으로 보인다.

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

[3] M. Mambo and E. Okamoto, "Proxy cryptosystems: Delegation of the power to decrypt ci-

pertext," IEICE Trans. Fund Electronics Communications and Computer Science, 1997.

[4] A. Sahai and B. Waters, "Fuzzy identity- based encryption," Proc. of Eurocrypt'05, LNCS 3494, pp. 457-473, 2005.

[5] X. Liang, Z. Cao, H. Lin and Jun Shao, "Attribute Based Proxy Re-encryption with Delegating Capabilities," ASIACCS 2009, Sydney, Australia, 10-12 March 2009. ACM, pp. 276-286, 2009.

[6] GUO Shanqing, ZENG Yingpei, WEI Juan and XU Qiuliang, "Attribute-Based Re- Encryption Scheme in the Standard Model," Wuhan University Journal of Natural Sciences, Vol.13 No.5, pp. 621-625, 2008.

[7] 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.

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

[9] A. Beimel, "Secure schemes for secret sharing and key distribution," PhD thesis, Israel Institute of Technology, Technion, Haifa, Israel, 1996.

[10] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," Proc. ACM Conference on Computer and Communications Security (CCS), pp. 456-465, 2007.

[11] V. Goyal, O. Pandey, A. Sahai and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," Proc. of ACM CCS'06, pp. 89-98, 2006.

〈著者紹介〉

박 광 용 (Kwangyong Park)
학생회원

2008년 2월: 동국대학교 전자상거래학과 졸업
2008년 3월~현재: 동국대학교 석사과정(전자상거래 기술전공)
<관심분야> 암호이론, 데이터 베이스 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 프로그램 위원장
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