한국군사과학기술학회지 제13권 제4호, pp. 635~641, 2010년 8월

학술논문 정보기술 부문

효율적인 공개키 기반의 디지털 콘텐츠 전송 시스템

Efficient Public Key Broadcast Encryption System

이 문 식*
MoonShik Lee

Abstract

In this paper, we propose an efficient public key broadcast encryption system which can also extend traitor trace and revoke system. Although the proposed system has limited collusion size, the ciphertext size in the system can be sublinear in the number of total users, the private key size is constant, the computational cost can be sublinear and it can support black-box tracing algorithm, therefore, our system can be an option to applications where reducing the ciphertext size, private key size is a top priority. Furthermore, we can also apply our system to military document broadcast system, because it has such an efficient measurement.

Keywords : Cryptography, Broadcast Encryption System, Traitor Tracing, Traitor Trace and Revoke

1. 서 론

일반적인 네트워크상에서 시스템 매니저가 시스템에 가입된 다수의 사용자만이 디지털 콘텐츠에 접근할 수 있고, 비 가입된 사용자는 콘텐츠에 접근할 수 없도록 전송하고자 한다면, 이를 위한 방법으로는 디지털 콘텐츠를 암호화해서, 네트워크상에 전송하는 방법이 있다. 이때, 전송받은 암호화된 콘텐츠를 복호화할 수 있는 키를 가지고 있는 가입된 사용자들은 암호화된 콘텐츠를 복호화 할 수 있고, 복호화 키가 없는 비 가입된 사용자들은 복호화를 할 수 없게 된다. 이러한 전송 시스템을 디지털 콘텐츠 전송 시스템이라 한다.

† 2010년 4월 12일 접수~2010년 7월 12일 게재승인
* 공군사관학교 수학과(Korea Air Force Academy)
책임저자 : 이문식(kafa0443@gmail.com)

디지털 콘텐츠 전송 시스템의 중요한 척도로는 암호문(ciphertext)의 크기(또는 전송량), 개인키(private key)의 크기, 복호화 연산량(computational cost)를 대표적으로 들 수 있으며, 이 중 가장 중요한 것이 암호문의 크기이다. 최근의 연구 결과로는 암호문의 크기는 총 사용자 수, n에 대하여 $\sqrt{n}$ 크기를 갖는 시스템들이 제안되고 있다.

디지털 콘텐츠 전송 시스템의 사용자 중에서 악의적인 목적으로 개인키를 유출하여 콘텐츠를 복호화할 수 있는 키를 만들거나, 가입된 사용자들이 서로 공모하여 복호화 할 수 있는 키를 만들어, 이를 저장한 불법 디코더(pirate decoder)를 만들 수 있는 경우도 있다. 이러한 경우, 그런 불법 디코더를 만들 때 공모한 공모자(traitor)를 추적할 수 있는 디지털 전송 시스템을 공모자 추적 기법(traitor tracing scheme)이라 한다. 또한 공모자를 추적한 이후에 공모자들의 개인키가 저장된 불법 디코더를 시스템에서 제거 시킬 수

있는 기능까지 추가된 시스템을 공모자 추적 및 제거 시스템(traitor trace and revoke scheme)이라 한다.

공개키 기반의 디지털 전송 시스템은 암호문을 만들 수 있는 암호화키가 공개되어 있어서, 시스템의 모든 사용자들이 암호화키를 이용하여, 전송하고자 하는 정보를 암호화하여 네트워크상에 전송할 수 있음으로 모든 사용자들이 data supplier가 될 수 있는 시스템이다.

추적 알고리즘은 불법 디코더를 분해하지 않고 내부에 저장된 키를 추적할 수 있는 black-box tracing 알고리즘을 의미하며, 이는 추적용 암호문을 불법 디코더에 입력하고 나온 출력을 통해서 저장된 키의 소유자를 판별하는 방법이다.

본 논문에서는 효율적인 공개키 기반의 디지털 콘텐츠 전송 시스템을 제안한다. 제안하는 시스템은 black-box tracing 알고리즘을 지원하는 공모자 추적 및 제거 시스템(traitor trace and revoke scheme)으로 확장할 수 있으므로 다양한 응용분야에서 활용될 수 있다. 또한 제안하는 시스템은 총 사용자 수, n에 대해서 $\sqrt{n}$의 암호문 크기를 가지며, 개인키는 4개를 가지고, 복호화 연산량은 $\sqrt{n}$번의 순환군(cyclic group)에서의 지수승 연산이 필요하므로, 안전성이 검증된 기존의 시스템[2,4]보다도 더욱 효율적인 척도를 가지고 있다.

본 논문에서 제안하는 시스템은 상업적인 분야(위성방송, cable-TV, DVD)에서의 응용성은 물론, 현재 군의 비밀 문서 전송 시스템에 이를 적용할 수 있으며, 장차 미래 전장에서의 통신 환경에 적용할 수 있다. 군의 응용적인 측면은 마지막 절에서 다루기로 한다.

2. 제안하는 디지털 콘텐츠 전송 시스템

가. 구조(Structure)

먼저 제안하는 디지털 콘텐츠 전송 시스템은 다음의 프로토콜로 이루어진다.

1) **Key generation**(n, k, λ) : 입력으로 총 사용자의 수 n, 최대 공모자의 수 k, 시스템 파라미터 λ를 받고, 출력으로는 공개키 PK, n명의 사용자 전체 집합 $U=\{u_1,...,u_n\}$, 그 중에서 사용자 u의 개인키 SK_u를 생성하는 프로토콜이다.

2) **Encryption**$(R, PK; s)$: 입력으로 제거하고자 하는 사용자의 부분 집합 $R(\subset U)$, $|R| \le 2k-1$, 공개키 PK, 세션키 s, 비밀 정보 M를 받고, 출력으로는 R을 제거한 사용자 $U \setminus R$ 들을 위한 세션키의 암호문 Hdr과 비밀 정보의 암호문 $E_s(M)$을 생성하는 프로토콜이다.

즉, 전송하는 암호문은 $C=\{Hdr, E_s(M)\}$이고, E는 DES와 AES같은 블록 암호이다.

3) **Decryption**$(u, SK_u; Hdr)$: 입력으로 사용자의 identity u, 개인키 SK_u, 암호문 $C=\{Hdr, E_s(M)\}$중에서 Hdr를 받고, 출력으로 세션키 s를 복구하고, 이를 통해 $E_s(M)$에서 비밀 정보 M을 복구한다.

4) **TrEncryption**$(X, PK, t; s)$: 입력으로 제거하고자 하는 사용자 부분 집합 $X(\subset U)$, $0 \le |X| \le n$, 공개키 PK, 사용자의 index t, $0 < t <$ n+1, 세션키 s, 비밀 정보 M를 받고, 출력으로는 X를 제거한 사용자 $U \setminus X=\{u_{t+1},...,u_n\}$ 들을 위한 세션키의 암호문 Hdr과 비밀 정보의 암호문 $E_s(M)$을 생성하는 프로토콜이다.

이 프로토콜은 악의적인 사용자들이 자신의 개인키를 유출 또는 공모하여 불법 디코더를 만들었을 때, 디코더의 저장된 키를 찾는 black-box tracing 알고리즘에 필요한 암호문을 만드는 프로토콜이다.

5) **Tracing algorithm** : 불법 디코더를 발견했을 때, 시스템 매니저는 TrEncryption 프로토콜을 이용하여 만든 추적용 암호문을 불법 디코더에 입력하고 나온 출력을 분석하여 불법 디코더내의 저장된 키를 찾는 프로토콜이다. 이를 위해 black-box tracing 알고리즘을 이용한다.

제안된 시스템은 다음 성질을 반드시 만족한다.

Correctness : 제외하고자 하는 사용자 $R(\subset U)$, $|R| \le 2k-1$에 대해서 모든 사용자 $u \in U \setminus R$는 다음을 만족한다.

$$\textbf{Decryption}(u, SK_u; \textbf{Encryption}\ (R, PK; s)) = s$$

나. 안전성(Security)

제안하는 시스템은 다음 security를 반드시 만족해야 한다.

1) **Semantic security** : 시스템에 가입하지 않는 사용자라면 암호문을 통해서 세션키 s를 복구할 수 없어야 하고, 따라서 M을 구할 수 없어야 한다.

2) **Computational secrecy** : k명 이하의 악의적인 사용자가 자신의 개인키를 유출 또는 공모를 하더라도 시스템 매니저가 생성하지 않는 새로운 개인키를 만들 수 없어야 한다.

정의 : 만약 다항식 시간 안에 계산을 할 수 있는 공격자 A가 있어서, 공격자 A가 semantic security와 computational secrecy를 공격할 수 있는 능력이 시스템 파라미터 λ에 대해서 무시할 정도의 능력을 가지고 있다면, 제안하는 시스템은 안전하다.

다. 예비지식(Preliminary)

1) **Discrete Logarithm Problem** : 소수(prime) q ($\approx$ 1024비트)에 대해서 순환군(cyclic group) $Z_q^* = \{1,...,q-1\}$의 생성원을 $g \in Z_q^*$라고 하자. 만약 $b = g^a \pmod q$가 주어졌을 때, a를 구하는 것이 상당히 어렵다는 문제이다.

2) **Decision Diffie-Hellman assumption(*DDH*)** : 순환군 G는 소수 q의 위수를 가지고, g를 G의 생성원이라고 하자. *DDH* 가정은 다음 두개의 ditstributions (g^a, g^b, g^{ab})와 (g^a, g^b, g^c), $a,b,c \in Z_q$을 다항식 시간 안에 구분할 수 있는 확률적인 알고리즘이 존재하지 않는다는 가정이다.

3) **Lagrange interpolation method** : 차수가 z인 다항식 $f(x)$은 $z+1$개의 $(j_0, f(j_0)),...,(j_z, f(j_z))$ 점이 주어진다면 만들 수 있다는 방법으로서 많은 암호학적인 도구로 사용된다. 즉, 먼저 q를 소수라고 하고 차수가 z인 다항식 $f(z)$를 Z_q위에서 정의된 다항식이라 하자. 그러면, 다항식 $f(x)$는 다음과 같이 구해진다.

$$f(x) = \sum_{t=0}^{z} (f(j_t) \cdot \lambda_t(x)),$$

여기서 $\lambda_t(x) = \prod_{\substack{j=0 \\ j \neq t}}^{z} \frac{j_i - x}{j_i - j_t}$, $t = 0,...,z$ 이고,

Lagrange coefficient이다. 또한 위의 방법을 순환군에서 지수 연산으로 자연스럽게 확장할 수 있다. 즉, G를 소수 q의 위수를 갖는 순환군이라 하고, g를 생성원이라 하자.

$z+1$개의 점 $(j_0, g^{f(j_0)}),...,(j_z, g^{f(j_z)})$이 주어진다면 Lagrange interpolation method을 사용하여 $g^{f(x)}$를 다음과 같이 계산할 수 있다.

$$g^{f(x)} = \prod_{t=0}^{z} g^{f(j_t) \cdot \lambda_t(x)},$$

여기서 $\lambda_t(x)$는 Lagrange coefficient이다.

라. 디지털 콘텐츠 전송 시스템 설계

시스템에 사용되는 파라미터(parameter)를 다음과 같이 정의한다. n, k를 각각 총 사용자의 수, 최대 공모자의 수라고 가정하자.

다음을 만족하는 p($\approx$1024비트), q($\approx$160비트), $q|p-1$, $q \geq n+1$ 인 소수 p, q를 선택한다. 또한 g를 Z_p^*의 생성원, G_q를 Z_p^*의 위수 q를 갖는 부분군이라 하자. 모든 사용자의 집합 $U = \{u_1,...,u_n\}$를 l개의 disjoint한 부분 집합 $U_0,...,U_{l-1}$를 나눈다. 각각의 부분 집합마다 $2k$명의 사용자를 대응시키고, 각 사용자의 index는 다음과 같이 정의한다.

$0 \leq i \leq l-1$에 대해서
$U_i = \{u_t | 2ki+1 \leq t \leq 2k(i+1)\}$, $|U_i| = 2k$

1) **Key generation(n, k, λ)**

시스템 매니저는 사용자들의 개인키를 생성하기 위해 키 생성 다항식을 다음과 같이 정의한다. 먼저, 임의의 $a_0,...,a_{2k-1}, c_0,...,c_{l-1}, b_0,...,b_{2k-1} \in Z_q$를 선택하고 l개의 다항식들 $F_i(x,y) \in Z_q[x,y]$, $0 \leq i \leq l-1$을 다음과 같이 정의한다.

$$F_i(x,y) = A_i(x) + y B(x) \mod q,$$

여기서 $A_i(x) = \sum_{j=0}^{2k-1} a_{i,j} x^j$, $a_{i,j} = \begin{cases} a_j & (j \neq i \mod 2k) \\ c_i & (j = i \mod 2k) \end{cases}$

$$B(x) = \sum_{j=0}^{2k-1} b_j x^j$$

위에서 정의한 다항식을 바탕으로 사용자 $u \in U_i$에 대해서, 임의의 $\alpha_u \in Z_q$를 선택하여 다음과 같은 개인키를 부여한다.

$$SK_u = (i, u, \alpha_u, F_i(u, \alpha_u))$$

또한, 시스템 매니저는 정의한 다항식들의 계수를 바탕으로 다음과 같은 공개키를 공개한다.

$$PK = (g^{a_0}, ..., g^{a_{2k-1}}, g^{c_0}, ..., g^{c_{l-1}}, g^{b_0}, ..., g^{b_{2k-1}})$$

2) **Encryption**$(R, PK; s)$

Data supplier는 비밀 정보 $M \in Z_q$을 암호화하기 위하여 암호문 $C = \{Hdr, E_s(M)\}$을 다음과 같이 만든다.

$m(\leq 2k-1)$명의 사용자들 $R = \{u_{i_1}, ..., u_{i_m}\}$을 제거시키고자 한다면, 먼저 $2k-m-1$개의 $x_{m+1}, ..., x_{2k-1} \in Z_q \setminus U$를 임의로 선택한다. 그리고 $R = \{x_1 := u_{i_1}, ..., x_m := u_{i_m}\}$으로 새롭게 정의하고 각각의 $1 \leq t \leq 2k-1$에 대해서 $g^{B(x_t)}$를 다음과 같이 각각 계산한다.

$$g^{B(x_t)} = \prod_{i=0}^{2k-1} (g^{b_i})^{x^i} = (g^{b_0})(g^{b_1})^{x^1} \cdots (g^{b_{2k-1}})^{x^{2k-1}}.$$

Data supplier는 세션키 $s \in G_q$와 $r \in Z_q$을 임의로 선택하여 암호문 $C = \{Hdr, E_s(M)\}$에서 Hdr을 다음과 같이 계산한다.

$$\left\{ \begin{array}{c} h = g^r,\ h_0 = g^{r a_0}, ..., h_{2k-1} = g^{r a_{2k-1}}, \\ h_{1,0} = g^{r c_0}, ..., h_{1,l-1} = g^{r c_{l-1}}, \\ s \bullet g^{r B(0)}, (x_1, g^{r B(x_1)}), ..., (x_{2k-1}, g^{r B(x_{2k-1})}) \end{array} \right\}$$

3) **Decryption**$(u, SK_u; Hdr)$

사용자 $u \in U_i$이고, 제거되지 않은 사용자라면, 즉, $u \notin R$ 이라면, 먼저 $g^{rB(u)}$를 다음과 같이 계산한다.

$$g^{rB(u)} = \left\{ \frac{h^{F_i(u,\alpha_u)}}{h_{1,i}^{u^i} \prod_{j=0}^{2k-1} h_j^{u^j}} \right\}^{1/\alpha_u} = \left\{ \frac{g^{r(A_i(u)+\alpha_u B(u))}}{g^{rA_i(u)}} \right\}^{1/\alpha_u}.$$

$(u, g^{rB(u)}), (x_1, g^{rB(x_1)}), ..., (x_{2k-1}, g^{rB(x_{2k-1})})$의 $2k$개의 점을 통해서 $g^{rB(0)}$를 Lagrange interpolation method를 이용하여 다음과 같이 구한다.

$$g^{rB(0)} = \prod_{i=0}^{2k-1} g^{r\lambda_i B(x_i)} = g^{r \sum_{i=0}^{2k-1} \lambda_i B(x_i)},$$

여기서 $\lambda_i = \prod_{\substack{j=0 \\ j \neq i}}^{2k-1} \frac{x_j}{x_i - x_j},\ 0 \leq i \leq 2k-1,\ x_0 := u.$

그리고 다음과 같이 세션키 $s = \frac{s \bullet g^{rB(0)}}{g^{rB(0)}}$를 구하고, $E_s(M)$에서 비밀 정보 M을 구한다.

만약 사용자 u가 제거되는 사용자라면, 즉, $u \in R$라면, u는 $2k-1$개의 점을 구할 수밖에 없으므로 $g^{rB(0)}$를 구할 수 없고, 따라서 세션키를 구할 수 없다.

4) **TrEncryption**$(X, PK, t; s)$

시스템 매니저는 발견된 불법 디코더내의 키를 찾기 위한 black-box tracing 알고리즘에 필요한 암호문을 다음과 같이 만든다. t명의 사용자들 $X = \{u_1, ..., u_t\}$를 제거시키기 위한 암호문을 다음과 같이 만든다.

먼저 $t = 2kt_1 + t_2,\ 0 \leq t_1 \leq l-1, 1 \leq t_2 \leq 2k$를 만족하는 t_1, t_2 정수를 찾는다. 그리고 세션키 s와 임의의 r을 선택한다.

만약 $t_2 = 2k$ 라면

$0 \leq i \leq t_1$에 대해서 임의로 선택한 $z_i \in Z_q$로 $h_{1,i} = g^{z_i}$를 계산한다. $t_1 < i \leq l-1$에 대해서는 $h_{1,i} = g^{rc_i}$를 계산한다. 그리고 시스템 매니저는 $2k-1$개의 $x_1, ..., x_{2k-1} \in Z_q \setminus U$를 선택하여 $g^{rB(x_j)},\ 1 \leq j \leq 2k-1$를 계산해서 다음 Hdr을 만든다.

$$\left\{ \begin{array}{c} h = g^r,\ h_0 = g^{r a_0}, ..., h_{2k-1} = g^{r a_{2k-1}}, \\ h_{1,0} = g^{z_0}, ..., h_{1,t_1} = g^{z_{t_1}}, h_{1,t_{1+1}} = g^{rc_{t_1+1}}, ..., h_{1,l-1} = g^{rc_{l-1}}, \\ s \bullet g^{r B(0)}, (x_1, g^{r B(x_1)}), ..., (x_{2k-1}, g^{r B(x_{2k-1})}) \end{array} \right\}$$

만약 $t_2 \neq 2k$ 라면

$0 \leq i < t_1$에 대해서 임의로 선택한 $z_i \in Z_q$로 $h_{1,i} =$

g^{z_i}를 계산한다. $t_1 \le i \le l-1$에 대해서는 $h_{1,i} = g^{rc_i}$를 계산한다. 그리고 시스템 매니저는 $X' = \{x_1 := u_{t_1,1}, ..., x_{t_2} := u_{t_1,t_2}\} = X \setminus \cup_{i=0}^{t_1-1} U_i$로 X'를 새롭게 정의한다*. 또한 $2k-t_2-1$개의 임의의 x_{t_2+1}, ..., $x_{2k-1} \in Z_q \setminus U$를 선택하여 $g^{rB(x_j)}$, $1 \le j \le 2k-1$를 계산해서 다음 Hdr을 만든다.

$$\left\{ \begin{array}{c} h = g^r,\ h_0 = g^{r a_0}, ..., h_{2k-1} = g^{r a_{2k-1}}, \\ h_{1,0} = g^{z_0}, ..., h_{1,t_1-1} = g^{z_{t_1-1}}, h_{1,t_1} = g^{rc_{t_1}}, ..., h_{1,l-1} = g^{rc_{l-1}}, \\ s \bullet g^{r B(0)}, (x_1, g^{r B(x_1)}), ..., (x_{2k-1}, g^{r B(x_{2k-1})}) \end{array} \right\}$$

5) **Tracing 알고리즘**

Tracing 알고리즘은 악의적인 사용자가 자신의 개인키를 유출 또는 공모해서 복호화 할 수 있는 해적판 디코더를 만들었을 때, 시스템 매니저가 이를 분해하지 않고 암호문을 입력해서 나온 출력을 분석함으로써 저장된 키를 찾는 알고리즘으로써 절차는 다음과 같다.

Step 1. 모든 t, $1 \le t \le n$에 대해서 다음 과정을 반복한다.

Step 1.1. 먼저 $ctr_t = 0$으로 초기화한다.

Step 1.2. $X := \{u_1, ..., u_t\}$를 제거하고자 하는 사용자 집합이라 한다.
$t = 2kt_1 + t_2$, $0 \le t_1 \le l-1$, $1 \le t_2 \le 2k$
를 만족하는 정수 t_1, t_2를 찾는다.

Step 1.3. 다음 과정을 m번 테스트 한다.
(i) 각각의 테스트마다 세션키 s과 r은 임의로 선택한다.
(ii) 암호문 Hdr = **TrEncryption**$(X, PK, t; s)$을 만든다.
(iii) 해적판 디코더에 암호문 Hdr을 입력하고 올바르게 세션키 s를 구하면, $ctr_t \leftarrow ctr_t + 1$로 증가시킨다.

Step 2. 최종적으로 $ctr_{t-1} - ctr_t$가 최대가 되는 정수 t를 찾고, 이때의 사용자 u_t의 개인키가 디코더에 저장되어 있다는 것을 확인한다.

마. 효율성(Efficiency)

제안하는 시스템은 k명 이하의 악의적인 사용자들이 공모를 하더라도 해적판 디코더에 저장된 키를 찾아낼 수 있는 디지털 콘텐츠 전송 시스템이다. 기존에 제시된 시스템과의 제안하는 시스템과의 효율성 비교를 위해서 Naor와 Pinkas가 2000년 Financial Cryptography에서 Lagrange interpolation method를 이용하여 제시한 시스템인 NP00[1] 시스템과 Boneh와 Waters가 2006년 ACM CCS에서 겹선형 사상을 이용하여 제시한 BW06 시스템과 비교하기로 한다. 참고로 BW06[2] 시스템은 지금까지 안전성이 검증된 시스템이지만 암호화 연산량이 $O(\sqrt{n})$번의 지수승 연산과 $O(\sqrt{n})$의 겹선형 사상 연산이 필요하므로 현실적으로 응용되기엔 어려운 시스템이라 할 수 있다.

이에 비해 제안하는 시스템은 NP00 시스템과 비슷한 효율성을 갖지만 공모자를 추적하는데 있어서 black box tracing 알고리즘을 사용할 수 있는 장점을 가지고 있으며, BW06 시스템과는 공모자의 수에 제한이 있지만 개인키의 크기가 상대적으로 적은 특징을 가지고 있다. 제안하는 시스템의 암호문 크기는 $O(k+l)$이므로, 만약 $k = \sqrt{n}$으로 정의한다면, 암호문의 크기는 $O(\sqrt{n})$이 된다.

Table 1. 효율성 비교(exp : 순환군에서의 지수승 연산, pairing : 겹선형 사상 연산을 의미)

시스템	암호문 크기	개인키 크기	복호화 연산량
NP00	$O(\sqrt{n})$	$O(1)$	$O(\sqrt{n})$ exp
BW06	$O(\sqrt{n})$	$O(\sqrt{n})$	3 pairing
제안 시스템	$O(\sqrt{n})$	$O(1)$	$O(\sqrt{n})$ exp

시스템	최대 공모자의 수	Black-box tracing
NP00	limited k	No
BW06	unlimited	Yes
제안 시스템	limited k	Yes

* 표기의 간편성을 위하여 $u_{i,j} := u_{2ki+j}$를 의미한다

바. 안전성(Security)

제안하는 시스템은 다음과 같이 semantic security와 computational secrecy를 만족한다.

정리 1 : 만약 Decision Diffie-Hellman assumption이 어렵다고 가정한다면, 제안하는 시스템은 semantic security를 만족한다.

증명 : 엄밀한 증명 대신 개략적인 증명으로 대신한다. 먼저, 제안 시스템이 semantic secure하지 않다고 가정하면, 공격자는 임의의 세션키 s_0, s_1을 선택하고, 이를 암호문을 만드는 오라클에게 전달한다. 오라클은 두개의 세션키중 어느 하나를 가지고 암호문을 만들고, 이를 공격자에게 전달한다. 만약 공격자가 암호문을 만들 때 사용한 세션키를 맞출 수 있는 확률이 1/2+ϵ만큼 된다면, 이를 이용해서 Decision Diffie-Hellman assumption을 1/2+ϵ의 확률로 구별 할 수 있다. 따라서 DDH 문제가 어렵기 때문에 제안하는 시스템은 semantic secure 하다.

정리 2 : 만약 Discrete Logarithm Problem이 어렵다고 가정한다면, k명 이하의 악의적인 사용자들이 공모한 집합 $X=\{x_1,...,x_k\}$이 자신의 개인키를 유출하여 새로운 개인키 $SK_u \notin \{SK_{x_1}, ..., SK_{x_k}\}$를 만들 수 없다.

증명 : 공격자 A_1을 k개의 공모자들의 개인키를 가지고 새로운 개인키를 만드는 알고리즘이라고 하고, A_2를 Discrete Logarithm Problem을 푸는 알고리즘이라고 하자. 먼저 A_2가 존재한다면, 당연하게 A_1을 구현할 수 있다. 따라서 A_1이 존재하면, A_2를 구현할 수 있다는 것을 증명하면 된다. 즉, A_1이 존재한다면 A_1을 subroutine으로 해서 A_2의 존재를 보일 수 있다. 자세한 증명은 생략한다.

3. 군의 응용분야

가. 비밀 정보 전송 시스템

제안하는 디지털 콘텐츠 전송 시스템은 군의 비밀 정보 전송 시스템에 다음과 같이 적용할 수 있고, 본 절에서는 적용 가능성에 초점을 맞추어 다음과 같이 간략히 설계한다. 이를 위해, 군 본부를 시스템 매니저라고 하고 예하 부대를 사용자라고 한다.

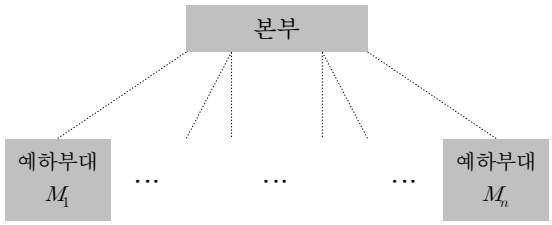

Fig. 1. 비밀 정보 전송 시스템

1) **Key generation** : 본부는 공개키 PK와 예하부대마다 해당 부대키 $SK_{M_1}, ..., SK_{M_n}$을 생성하고 이를 저장한 디코더를 배포한다.

2) **Encryption** : 본부 또는 예하부대는 제거하고자 하는 부대 $R=\{M_1,..., M_m\}$을 선택하고 비밀 정보 또는 보안성이 높은 문서 M을 암호화한 암호문 $C=\{Hdr, E_s(M)\}$을 계산하고 전송한다.

3) **Decryption** : 암호문 $C=\{Hdr, E_s(M)\}$을 전송받은 부대는 R에 포함되지 않는다면, 해당 부대키를 이용하여 세션키를 복호화하여 M을 얻는다.

위의 시스템을 구현하기 위해서, 예를 들어서 총 사용자 n=2^{16}, 최대 공모자 k=2^8으로 설정하면, 제안 시스템의 암호문의 크기는 $4k+l$개이고, l=$n/2k$이므로 2Mbyte가 필요하고, 개인키의 크기는 4Kbyte가 필요하다. 또한 복호화에 필요한 연산량은 대략 2^{20}번 지수승의 modulo 곱셈 연산이 필요하므로 쉽게 구현할 수 있을 것이다. 더욱이 군내의 분야에 응용하기 위해서 최대 공모자의 수를 k=2^8로 설정했지만, 군내의 경우, 비교적 사용자들에 대한 공모 가능성이 상업적인 분야의 공모 가능성보다 현저히 떨어질 수 있으므로 k를 낮게 설정한다면, 제안하는 비밀 정보 전송 시스템은 매우 효율적이라 할 수 있다.

4. 결 론

본 논문에서는 공모자 추적 및 제거 시스템으로

확장할 수 있는 디지털 콘텐츠 전송 시스템을 제안하였다. 제안된 시스템은 비록 공모자들의 수에 제한이 있는 시스템이지만, 기존에 제시된 안전성이 검증된 시스템보다 개인키의 크기가 매우 작으면서, 해적판 디코더를 분해하지 않고 저장된 키를 찾는 black-box tracing 알고리즘을 지원하는 장점을 가지고 있으며, 암호화 연산량과 복호화 연산량이 효율적인 시스템이다.

따라서 공모자들의 수가 제한적인 환경 또는 개인키의 크기와 암호화 및 복호화 연산량이 적은 환경의 응용분야에 쉽게 적용될 수 있는 시스템이라고 할 수 있다. 또한 제안된 시스템은 군내에서의 비밀 정보 전송 시스템에 적용함으로써 기존의 문서화된 비밀 정보의 열람, 관리, 폐기 등의 문제를 보다 쉽게 해결할 수 있는 장점을 가진다고 할 수 있다.

References

[1] D. Boneh, A. Sahai and B. Waters, Fully Collusion Resistant Traitor Tracing with Short Ciphertexts and Private Keys, EUROCRYPT 2006, LNCS 4004, pp. 573～592, 2006.

[2] D. Boneh and B. Waters, A Fully Collusion Resistant Broadcast, Trace and Revoke System, ACM Computer and Communications Security pp. 89～98, 2006.

[3] T. Matsuhita and H. Imai, A Public Key Black-Box Traitor Tracing Scheme with Sublinear Ciphertext Size against Self-Defensive Pirates, ASIACRYPT 2004, LNCS 4307, pp. 260～275, 2004.

[4] M. Naor and B. Pinkas, Efficient Trace and Revoke Schemes, FC 2000, LNCS 1692, pp. 1～20, 2001.