스마트 카드에 적용 가능한 비밀분산법을 이용한 키 관리 시스템

손 영 설[†] · 이 동 훈[††]

요 약

다수의 사업자간에 공동 키를 기반으로 서비스를 제공할 경우, 이에 사용되는 마스터 키를 참여 사업자간에 적절하게 분배하여 관리할 필요가 있다. 본 논문에서는 하나의 비밀(secret)을 다수의 참가자에게 분배한 후, 비밀정보를 복원 필요시 참가자 전원 또는 참가자 집단 내에서의 특정 허가된 참가자만이 비밀을 복원할 수 있는 비밀분산법을 이용하여 마스터 키(master key)를 효율적이고 안전하게 관리할 수 있는 비밀분산 시스템을 제안한다. 제안한 시스템은 비밀정보의 안전한 저장과 참가자의 신원 인증을 위해 스마트카드(smart card) 매체를 이용하며, (t, t)과 (k, n)-임계치 비밀분산법을 조합하여 참가자의 소속 그룹(group) 또는 그룹 내에서의 보안권한(security level)에 따라 비밀정보를 분산 및 복원을 가능하도록 한다.

The Key Management System using the Secret Sharing Scheme Applicable to Smart Card

Young Seol Son[†] · Dong Hoon Lee[††]

ABSTRACT

When several service providers want to work together with only one master key, they need to properly distribute the key to participants who come in for the co-work business and then securely manage the distributed keys. This paper describes the system that can efficiently and securely manage the master key on the basis of the secret sharing scheme that can reconstruct original secret information as the necessity of reconstructing original secret arises. The proposed system can distribute secret information to several groups and also redistribute the secret to subgroup in proportion to the participant's security level using smart card-based (t, t)-(k, n)-threshold secret scheme for securely keeping secret information and authentication of participant's identification

키워드 : 비밀분산(Secret Sharing), 스마트카드(Smartcard), 암호(Cryptography), 키 관리(Key Management)

1. 서 론

비밀분산(secret sharing)이란 하나의 비밀정보를 다수의 분산 정보로 부호화하여 해당 참가자(participant)에게 나누어준 후, 특정 부분 액세스 집합만이 최초의 비밀정보를 복원할 수 있도록 하는 암호 프로토콜로써 비밀정보 분배자(dealer)가 참여자에게 분배하는 분배(distribution) 프로토콜과 이러한 참여자의 특정 집단의 비밀정보를 수집하여 원래의 비밀정보를 복원하는 복구(reconstruction) 프로토콜로 나눌 수 있다. 이러한 분산된 비밀정보를 특정 부분집합의 액세스 구조(access structure)를 통해서 문제를 해결하려 했던 것은 Shamir의 비밀분산법[1]에서 찾아볼 수 있다. Shamir는 다항 보간법(polynomial interpolation) 기반의 (k, n)-threshold scheme을 제안하여, 비밀정보의 조각을 분배받은 n명의 참가자들 중에서 임의의 k명 이상이 모이면 비밀정보의 복원이 가능하나, $k-1$명 또는 그 이하의 참가자만으로는 비밀정보를 복원할 수 없도록 하였다. 현실 세계에서 비밀정보를 나눔에 있어서 일반적으로 임의의 참여자보다는 이해 관계자 또는 특정 조직에 속해있는 관계자 등의 특정 집단에 분배하는 것이 보편적이다. 예를 들어, 공인인증 서비스를 제공하는 공인인증기관(CA)의 CA 개인키, 금융 서비스를 제공하는 은행 또는 신용카드사의 현금 카드, 신용카드 등을 관리하기 위하여 사용하는 스마트카드 마스터키, GSM통신과 같은 이동통신에서 가입자 인증을 위하여 사용하는 SIM(Subscriber Identification Module)카드의 인증키[2] 등과 같은 중요한 키에 대한 정보를 취급함에 있어서 특정 보안 책임자 또는 인가자가 관여하게 되며, 이들의 보안 등급에 따라서 분배하는 비밀정보도 달리하여 관리된다.

† 정 회 원 : KT서비스개발연구소
†† 정 회 원 : 고려대학교 정보보호대학원 교수
논문접수 : 2004년 4월 13일, 심사완료 : 2004년 7월 6일

Shamir의 비밀분산법이 제안된 이 후 지금까지 많은 학자와 연구기관에 의해서 다양한 비밀분산법 구성과 연구가 진행되어 왔으며, 이를 실제 환경에 적용하기 위한 노력도 많이 시도되어 왔다[3, 4]. 그러나, 이론적으로 고찰되었던 비밀분산법을 적용하여 실제 서비스 환경에 적합한 비밀분산시스템을 구현하기 위해서는 비밀분산 이론의 중요성과 함께 효율적인 비밀정보의 분산 및 복원을 처리하는 등의 서비스 운영측면이 더욱 고려되어 시스템이 설계되어야 한다. 그렇지만 이러한 서비스 효율성 관점에서의 시스템의 설계는 그렇게 쉬운 일이 아니며, 아직까지 이를 고려한 많은 연구가 이루어지지 않았다. 따라서 본 논문에서는 참가자 전원이 모두 참여함으로써 비밀복원이 가능한 (t, t)-threshold scheme과, n명의 참가자 중에서 k명만 참여해도 비밀복원이 가능한 (k, n)-threshold scheme을 비밀분산법으로 재구성하고, 이에 안전한 저장연산 매체로 사용되는 탬퍼 방지 소자인 스마트 카드를 응용 결합함으로써 보다 실효성이 키 관리 시스템을 설계하였다.

2. 기본 연구

2.1 비밀분산의 개념

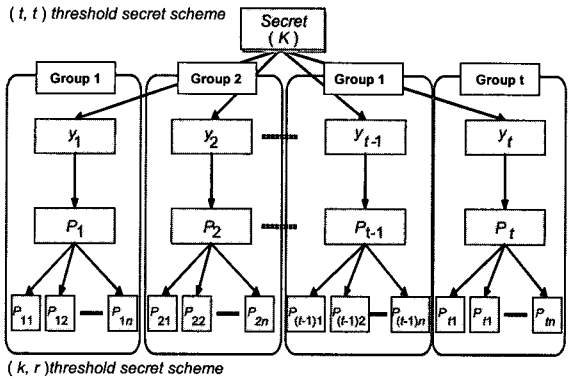
비밀정보 S를 n개의 분산정보 $V=\{V_1, V_2, \cdots, V_n\}$로 분할하여 n명의 참가자 $P=\{P_1, P_2, \cdots, P_n\}$에게 분배자(dealer)가 적절하게 분배한다고 하자. 분산정보 V의 부분집합 $W=\{W_{j1}, W_{j2}, \cdots, W_{jm}\}$또는 분산정보 V를 가진 참가자들의 부분집합 $U=\{U_{i1}, U_{i2}, \cdots, U_{im}\}$으로부터 비밀정보 S가 완전히 복원될 때 W 및 U그룹을 *Qualified access Set* Γ라 하고, 그렇지 않은 그룹을 *Forbidden Access Set* Δ라 한다. Access Set Γ는 *monotone increasing*를 만족하는데 이것은 참가자 P의 부분 집합 U, U′에 대해서 $U\in\Gamma$이고 $U\subseteq U'\subseteq P$이면 $U'\in\Gamma$를 의미한다. 그리고 $\Gamma\cap\Delta=\varnothing$일 경우 (Γ, Δ)는 액세스 구조(access structure)라 하며, $\Gamma\cup\Delta=2^P$일 경우 (Γ, Δ)는 *complete*라 하고 그렇지 않은 경우 *incomplete*라 한다[5]. 액세스 집합 W 및 U에서 하나의 분산 정보(참가자)가 줄어들어 더 이상 Γ의 원소가 되지 못한다면, 이때 W 및 U를 최소집합(minimal set) Γ_0이라 하며, $\Gamma_0\in\Gamma$이다. 어떤 부분 집합 U′가 최소집합 Γ_0를 포함하면 U′는 당연히 액세스 집합이다. Γ_0는 Γ의 *basis*라 하며, Γ는 Γ_0 내에서 부분집합의 상위집합(superset)인 참가자 집합 P의 모든 부분집합으로 구성되어진다. 이때 Γ는 Γ_0의 하나의 함수에 의해서 유일하게 결정되어진다.

2.2 스마트카드

본 논문에서 제안하는 비밀분산시스템은 비밀분산에 참여하는 참가자가 비밀정보를 분배받기 위하여 자신의 정당성과 시스템으로의 접근 인가와, 비밀분산 시스템으로부터 분배받은 분산 비밀정보를 안전한 저장과 관리를 위하여 데이터의 저장 및 연산 처리 능력을 가지는 IC(Integrated Circuit) 칩(chip)을 내장한 스마트카드를 사용하게 된다. 데이터의 저장성, 보안성, 휴대성의 특성을 가지는 스마트카드는 이들 특성 중에서도 가장 주목할 기능은 데이터의 보안성이다. 독립된 카드운영체제(COS : Chip Operating System)와 보안 메커니즘을 기반으로 연산기능을 가진 스마트카드는 내부에 탑재된 마이크로프로세서를 이용하여 데이터 암호, 전자서명 등의 암호 연산 및 데이터 접근 제한 기능을 제공함으로써 기밀성(confidentiality), 무결성(integrity), 부인봉쇄(non-repudiation), 인증(authentication) 등의 보안 요구사항을 충족시켜준다. 최근 들어 스마트 카드의 운영체제(COS)는 다중 어플리케이션을 처리가 가능한 형태로 진화하고 있으며, 그 대표적인 운영체제가 자바카드와 멀토스 카드이다. 따라서 본 논문에서 이들 다중 어플리케이션 COS 중에서 자바카드 플랫폼을 기반으로 비밀분산시스템을 설계토록 하겠다. 일반적으로 자바카드는 Native COS 상위에 스마트카드를 위한 최적화되어진 자바 가상머신(VM : virtual machine)을 탑재하고, ISO/IEC 7816[6]에서 정의하는 스마트카드 명령어 처리를 위한 각종 API와 자바언어 해석을 위한 API를 탑재하여 구현된다[7].

3. (t, t)-(k, n)-threshold scheme의 설계

스마트카드 기반의 비밀분산 시스템에 있어서 비밀분산에 참여하는 n명의 참가자가 분배받은 n개의 비밀정보를 모두 제출하여야 원래 비밀정보를 복원할 수 있는 (t, t)-threshold scheme[8], n명의 참가자 중 비밀정보를 분배받은 k명의 참가자가 비밀정보를 제출하면 비밀정보가 복원되는 (k, n)-threshold scheme을 결합하여 비밀분산법을 적용하며, 참가자의 권한 설정 및 비밀정보 저장을 위한 매체로 스마트카드를 사용하여 비밀분산시스템을 설계하며, 전체적인 비밀분산 운영은 아래 (그림 1)과 같다.



(그림 1) (t, t)-(k, n)-threshold scheme

(그림 1)에서 (t,t)-(k,n)-threshold scheme에 참여하는 참가자는 그룹 $G=\{G_1, G_2, \cdots, G_t\}$으로 먼저 구분할 수 있으며, 이 그룹은 비밀정보 K를 복원하기 위한 최소 집합이 된다. 이때 최소 집합의 참가자를 $P=\{P_1, P_2, \cdots, P_t\}$로 하고, 이들을 해당 그룹의 대표자 역할을 가진다. (t,t)-(k,n)-threshold scheme에서 (t,t)-threshold scheme은 이들 P에게 비밀정보 K를 $y=\{y_1, y_2, \cdots, y_t\}$로 분산하여 분배하는 경우에 적용한다.

그리고 해당 그룹은 각각 그룹 내에서 분산받은 비밀정보를 재분산하기 위하여 참가자 $P'=\{\{P_{11}, P_{12}, \cdots, P_{1n}\}\{P_{t1}, P_{t2}, \cdots, P_{tn}\}\}$를 가진다. 이때 참가자 P'에게 비밀정보를 분산할 때 (t,t)-(k,n)-threshold scheme에서 (k,n)-threshold scheme를 적용하게 된다. (t,t)-(k,n)-threshold scheme에 참여하는 참가자 집단은 그룹의 정책에 따라 참가자 P, P'의 인원 수를 조정할 수 있으며, (t,t)-threshold scheme에 참여하는 참가자 P없이 (k,n)-threshold scheme에 참여하는 P'만 둘 수도 있다. P, P'에게 비밀정보를 분산하는 과정은 동일한 비밀분산시스템에서 이루어지게 되며, 이러한 분산정책은 비밀분산 시스템을 구축하는 최초 시점에 정의하여 운영된다.

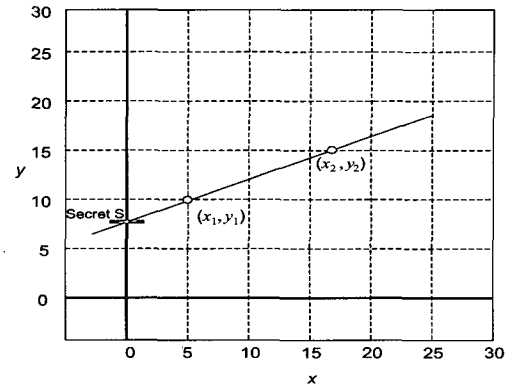
본 절에서는 이런 비밀분산시스템을 위한 (t,t)-threshold scheme과 (k,n)-threshold scheme에 대해서 살펴보며, 참가자 카드에 탑재되는 비밀분산 처리를 위한 카드 어플리케이션의 기능과 특성에 대해서 기술토록 한다.

3.1 (k,n)-threshold scheme

LaGrange Interpolation에 기반한 (k,n)-threshold scheme 구성을 위해 먼저 서로 다른 값 $x_i(1 \le i \le n)$를 선택한다. 2차 평면상에서 주어진 k개의 점 $(x_1, y_1), (x_2, y_2), \cdots, (x_k, y_k)$이 주어졌을 때 모든 i에 대해 $f(x_i)=y_i$인 $(k-1)$차수의 다항식 $f(x)$가 유일하게 존재한다. 비밀분산 시스템이 비밀정보 S을 S_i로 나누고자 할 때 먼저 임의의 $(k-1)$차수의 다항식 $f(x)=a_0+a_1x+\cdots+a_{k-1}x^{k-1}$를 선택할 수 있으며 $a_0=S$인 다항식이어야 한다. 이러한 S_i값 k의 모든 부분 집합(subset)이 주어질 때, 보간법(interpolation)에 의해 다항식 $f(x)$의 계수를 찾아 $S=f(0)$를 구할 수 있게 되며 $(k-1)$의 값을 통해서는 유일한 S를 계산하지 못한다.

(그림 2)에서 다항식 $f(x)$는 2개점 (x_1, y_1), (x_2, y_2)에 의해서 유일하게 결정되며, 비밀정보 S는 아래와 같이 표현될 수 있다.

$$S=f(0)=y_2-\frac{(y_1-y_2)}{(x_1-x_2)}(x_0)$$



(그림 2) Shamir's threshold scheme

LaGrange Interpolation에 대한 조건들을 만족시키기 위하여 실 연산을 수행하지 않고 소수 P상에서의 모듈라(modular) 연산을 이용한다. 이때 모듈라 소수 P의 집합 Z_p는 보간법(interpolation) 적용이 가능한 유한체를 형성하게 되며($p > n$), 계수 $(a_0, a_1, \cdots, a_n)$은 $[0, p-1]$의 정수 중 uniform한 분포로 선택되고, 분산 비밀정보 $S_1, \cdots, S_n$의 값들은 모듈라 p상에서 계산한다.

비밀분산 시스템에 참여하는 n명의 참가자를 $P=\{P_1, P_2, \cdots, P_n\}$, 비밀정보 S의 분산 값을 $S=\{S_1, S_2, \cdots, S_n\}$, 그리고 비밀분산 시스템에서 비밀정보를 나누어주는 사람을 분배자(dealer)라 하면 아래와 같은 절차를 통해서 비밀정보를 분산하여 n명의 참가자(Participant)에게 분산하게 된다.

◦ 초기화 단계(Initialization Phase)

분배자(dealer)는 Z_p원소 중 n개의 서로 다른 0이 아닌 원소 x_i를 선택하여 $(1 \le i \le n, p \ge n+1)$ x_i값을 p_i에 분배하고 x_i값을 공개한다.

◦ 비밀분산(Share Distribution) 단계

① 분배자는 비밀정보 $S \in Z_p$를 분배하며, Z_p의 $k-1$개의 원소를 임의로 선택하며 이 값은 $a_1, a_2, \cdots, a_{k-1}$이다.

② $1 \le i \le n$에 대해, $y_i=f(x_i)$를 계산한다.

$$f(x)=a_0+a_1x+\cdots+a_{k-1}x^{k-1} \bmod p$$

$$f(x)=S+\sum_{j=1}^{k-1}a_jx^j \bmod p, a_0=S$$

③ $1 \le i \le n$에 대해서, 분배자는 분산 정보 y_i를 각 참가자 p_i에 분배한다.

◦ 비밀복원(Secret Reconstruction) 단계

비밀정보 S를 복원하기를 원하는 참가자를 $P_{i1}, P_{i2}, \cdots, P_{ik}$라 하고, 이들 참가자는 아래와 같은 분산비밀정보를 알고 있다.

$$yi_j=f(xi_j), 1 \le t \le k$$

상기 식에서 $f(x_i) \in Z_p[x]$는 비밀분산시스템에서 비밀리 선택되어진 아래 식과 같은 $k-1$차 다항식 함수이다.

$$f(x) = a_0 + a_1 x + \cdots + a_{k-1} x^{k-1}$$

그리고 다항식의 계수 $a_0, a_1, \cdots, a_k$들은 Z_p의 은닉 계수이며, $a_0 = S$이다. $yi_j = f(xi_j)$이므로 참가자의 부분집합 B는 k개의 은닉 계수 $a_0, a_1, \cdots, a_k$내에서 k개의 선형 식(linear equation)을 가질 수 있으며, 만약 이들 식이 모두 선형 독립적이라면 유일한 해가 존재하게 되고, 비밀정보 $a_0 = S$는 복원될 수 있다. 유일한 k차 다항식 $f(x)$에 대한 LaGrange Interpolation 공식은 아래와 같이 정의가 가능하다[9].

$$f(x) = \sum_{j=1}^{k} y_{i_j} \prod_{1 \le t \le k,\, t \ne j} \frac{(x - x_{i_t})}{(x_{i_j} - x_{i_t})}$$

$x = 0$으로 치환함으로써 $f(x) = f(0) = S$이 되는 아래 식으로 재정의할 수 있다.

$$S = \sum_{j=1}^{k} y_{i_j} \prod_{1 \le t \le k,\, t \ne j} \frac{x_{i_t}}{(x_{i_t} - x_{i_j})}$$

그리고 위의 식에서 $b_j = \prod_{1 \le t < k,\, t \ne j} \frac{x_{i_t}}{(x_{i_t} - x_{i_j})}$로 정의하면 비밀정보 $S = \sum_{j=1}^{k} y_{i_j} b_j$로 정의할 수 있다.

3.2 (t, t)-threshold scheme

Karnin, Greene, Hellman이 제안한 (t, t)-threshold Scheme[6]은 참가자 집합의 모든 참가자가 분산된 비밀정보를 제출하여야 복원이 되는 방법이다. 이는 서로 이해 관계가 상이한 집단이 상호 공유하는 서비스 매체를 통하여 서비스를 제공하고자 할 때 해당 공유 매체의 비밀정보(예 : 마스터 키)를 서로 분산하여 저장하고자 하며, 아울러 복원시에도 참여 집단의 모든 동의가 이루어진 후 해당 비밀정보를 복원할 수 있도록 하는 것이 필요하다. (t, t)-threshold scheme에서의 비밀정의 분산과 복원과정은 아래와 같다.

• 비밀분산(Share Distribution) 단계

(t, t)-threshold scheme를 사용하는 비밀분산 시스템은 분배하고자 하는 비밀정보 S에 대해서 S보다 큰 임의의 소수 m를 선택한다. 그리고 비밀분산 시스템은 서로 다른 독립적인 $t-1$개의 비밀 조각($y_1, y_2, \cdots, y_{t-1} \in Z_m$)을 안전하게 선택한다. 비밀분산 시스템은 t번째 분산 비밀정보 y_t를 다음 식을 이용하여 계산한다.

$$y_t = S - \sum_{i=1}^{t-1} y_i \bmod m$$

$1 \le i \le t$에 대해, 비밀분산 시스템은 t명의 참여자 집합 $P = \{P_1, P_2, \cdots, P_t\}$에게 상기 과정에서 생성한 해당 y_t값을 분배하여 준다.

• 비밀복원(Share Reconstruction) 단계

(t, t)-threshold scheme기반의 비밀분산시스템에서의 분산된 비밀정보의 복원은 S_i를 가지는 모든 키 집합 $S = Z_m$에 대해서 이루어진다. (t, t)-threshold Scheme에서는 S-hamir의 (k, n)-threshold scheme과는 달리 소수 m을 필수로 하지 않으며, $m \ge w + 1$일 필요가 없다. 비밀분산 시스템은 분산된 비밀정보(y_t)로 비밀정보 S를 복원하기 위하여 다음 식을 통해 계산한다.

$$S = \sum_{i=1}^{t} y_i \bmod m$$

3.3 비밀분산 카드 어플리케이션

본 논문에서 제안하는 비밀분산시스템의 실현을 위해 사용되는 참가자 카드는 자바카드를 기반으로 하며, 해당 카드에는 분산된 비밀정보의 저장 기능과 아래와 같은 기능을 수행할 수 있는 비밀분산 어플리케이션을 개발, 탑재하여 사용한다. 비밀분산 카드 어플리케이션은 자바카드(java card)[10]와 글로벌 플랫폼(global platform)[11] 규격에 준하여 설계되며, 프로그램은 아래와 같은 기능을 가진다.

• 비밀분산 카드 어플리케이션의 기능

① 비밀정보소유자의 정당성을 검증하는 CHV기능을 가진다.
② 비밀분산시스템과 상호인증을 통하여 카드의 위/변조를 검증하고 이를 통해 안전하게 비밀정보를 분산 및 복원한다.
③ 비밀분산시스템과 보안채널(secure channel)을 형성하여 안전하게 비밀정보를 카드에 저장하도록 한다.
④ 참가자의 프로파일(profile)파일을 통하여 비밀정보 소유자의 인적정보 및 보안권한을 가진다.
⑤ (t, t)-threshold scheme에서 생성된 분산비밀정보 값, 분배일자, 유효일자 등이 정보를 가진다.
⑥ (k, n)-threshold scheme에서 생성된 분산비밀정보 값, 분배일자, 유효일자 등이 정보를 가진다.
⑦ 상호인증 및 보안채널 형성을 위한 난수 생성 함수와 3DES 알고리즘 기능을 가진다.

• 카드 어플리케이션의 파일정보

스마트 카드 기반의 비밀분산 방법을 구현하기 위하여 카드에 설치된 비밀분산 애플릿은 참가자 파일과 분산 비밀정보 파일을 가지며, 비밀분산에 참여하는 참가자들에게 아래 <표 1>~<표 3>과 같은 정보가 저장된 카드를 발급하여 배포한다.

〈표 1〉 (t, t)-threshold scheme 파일 구조

파일 구조	Linear Variable		파일 크기	Variable
File Access Condition			PIN & KEY	
항 목	Length	Type	Description	
Secret Scheme Type	1	HEX	0×01 : (t, t)-threshold scheme, 0×02 : (k, n)-threshold scheme	
Secret Issuance Date	4	BCD	Secret 분배일자(YYYYMMDD)-비밀정보 분산일자	
Secret Dealer	1	HEX	Secret 분배자로 해당 비밀분산 시스템의 관리주체	
Secret(y_i)	가변	HEX	분산된 비밀정보	
Secret Expiration date	4	BCD	Secret 유효일자, 분산된 비밀정보의 유효기간	

<표 1>은 (t, t)-threshold Secret Scheme를 이용하여 생성한 분산 비밀정보를 저장하기 위한 자바카드 내의 파일 구조를 나타낸다. 해당 파일에 대한 접근은 비밀소유자의 PIN인증과 Key에 의한 상호인증 절차를 수행한 후 가능하다. 즉, (t, t)-threshold Secret Scheme파일은 비밀 소유자의 인증을 통하여 비밀분산시스템에서만 접근이 가능하다.

〈표 2〉 (k, n)-threshold scheme 파일 구조

파일 구조	Linear Variable		파일 크기	Variable
File Access Condition			PIN & KEY	
항 목	Length	Type	Description	
Secret Scheme Type	1	HEX	0×01 : (t, t)-threshold scheme, 0×02 : (k, n)-threshold scheme	
Secret Issuance Date	4	BCD	Secret 분배일자(YYYYMMDD)	
Secret Dealer	1	HEX	Secret 분배자	
$x_i \in Z_p$	가변	HEX	Z_p원소 중 n개의 서로 다른 0이 아닌 원소($1 \le i \le n, p \ge n+1$)	
Secret information(y_i)	가변	HEX	비밀 분산정보($y_i = f(x_i)$)	
Secret Expiration date	4	BCD	Secret 유효일자(YYYYMMDD)	

<표 2>는 (k, n)-threshold Secret Scheme를 이용하여 생성한 분산 비밀정보를 저장하기 위한 자바카드 내의 파일 구조를 나타낸다. 본 파일에 대한 접근 권한은 <표 1>의 (t, t)-threshold Scheme파일과 동일하다.

〈표 3〉 참가자 파일 구조

파일 구조	LF		파일 크기	17Bytes
Access Condition			Card Holder PIN	
항 목	Length	Type	Description	
Organization ID	5	HEX	참여자 소속 기관 ID-비밀분산시스템에 참여하는 사업자(or 그룹)를 나타내는 식별코드	
Participant ID	5	HEX	참가자의 식별 ID-비밀분산 시스템에 참여하는 참가자에게 부여하는 식별자	
Security Level	1	BCD	비밀분산 시스템에 참여하는 참가자의 권한(<표 4> 참조)	
Contact Point	6	BCD	참여자 연락처	
Share Holder PIN	12	HEX	참가자의 비밀번호 비밀소유자의 카드 비밀번호	

비밀분산 시스템에 참여하는 참가자 파일은 참가자의 속성을 나타내는 파일로 비밀분산 시스템은 참가자 그룹간에 합의된 정책에 의하여 참가자의 속성을 정하여 참가자 카드 발급 시점에 이를 정의한다.

〈표 4〉 참가자 권한구분

Group				Sub-Group				구 분
B8	B7	B6	B5	B4	B3	B2	B1	Security Level
0	0	0	1	0	0	0	0	그룹 대표자
0	0	0	0	0	0	0	1	그룹 내 참가자
0	0	0	1	0	0	0	1	그룹 대표자/참가자

4. 비밀정보 분산 및 복원

스마트카드 기반의 비밀분산 시스템은 "참가자(또는 그룹) 등록 신청→참가자 프로파일 및 정책 등록→참가자 카드 발급"을 수행하는 참가자 카드 발급 단계와, "참가자 신원확인→참가자 카드의 정당성 확인→참가자의 접근권한 및 정책 확인→비밀분산 및 저장"을 수행하는 비밀분산 단계와, "참가자 신원확인→참가자 카드의 정당성 확인→참가자의 접근권한 및 정책 확인→분산 비밀정보 판독 및 복원"을 수행하는 비밀복원 단계의 절차로 수행된다.

4.1 정의 및 표기

- P = $\{P_1, P_2, \cdots, P_t\}$: 비밀분산 시스템(SSS)의 참가자
- G = $\{G_1, G_2, \cdots, G_t\}$: 비밀분산 시스템(SSS)에 참여하는 t개의 참여기관.
- CG = $\{CG_1, CG_2, \cdots, CG_t\}$: t개의 참여기관의 참가자 (G_i) 권한을 가지는 스마트 카드
- GP = $\{G_iP_{1i}, G_iP_2, \cdots, G_iP_n\}$: t개의 참여기관 G_i에 속

하는 n명의 참가자

- $CGP = \{CG_iP_{1i}, CG_iP_2, \cdots, CG_iP_n\}$: t개의 참여기관 G_i에 속하는 n명의 참가자들이 가지는 스마트 카드
- (t,t)-TSSS : (t,t)-threshold Secret sharing Scheme을 이용하여 비밀분산 및 복원을 수행하는 시스템을 (t,t)-threshold Secret Sharing System
- (k,n)-TSSS : (k,n)-threshold Secret Sharing Scheme을 이용하여 비밀분산 및 복원을 수행하는 시스템을 (k,n)-threshold Secret Sharing System
- 스마트 카드 자원 매니저 : 스마트카드의 삽입/제거에 대한 제어 및 통신채널을 형성하여 직접 APDU의 송수신을 관리함.
- 스마트 카드 인증 모듈 : 비밀소유자가 보유한 스마트카드의 정당성을 검증하기 위한 보안 모듈
- 카드 소지자 검증 모듈(Verifier) : 비밀소유자가 보유한 스마트카드가 본인 것임을 검증하기 위하여 비밀소유자의 비밀번호를 입력받아 소유자 확인을 처리하는 하는 모듈
- 비밀분산/복원 매니저 : 비밀정보의 분산 및 복원에 따라서 스마트카드로부터 판독된 정보 및 비밀분산시스템의 데이터베이스에 기록된 정책파일을 기반으로 분산 및 복원에 따른 절차에 따른 적절한 Secret sharing Scheme의 호출과 정보를 관리하는 모듈
- 참가인 관리자 : 비밀분산 시스템에 참가하는 참가자의 정보 및 권한 등을 저장, 관리하는 관리자
- 비밀분산 정책관리 모듈 : 비밀분산시스템에 참가하는 참가자의 유형에 따른 정책파일 생성, 관리하는 모듈
- 임계치 스킴 매니저 : 참가자의 권한 및 정책, 그리고 분산 및 복원에 따라서 (t,t)-threshold Scheme과 (k,n)-threshold Scheme를 관리, 제어하는 모듈
- $y_i (1 \le i \le t)$: i그룹에서 (t,t)-TSSS에서 분배하는 분산 비밀정보
- $a_{ij} (1 \le i \le n, 1 \le j \le t)$: j그룹에서 (k,n)-TSSS에서 분배하는 분산 비밀정보
- K : (t,t)-TSSS에서 분배하고자 하는 비밀정보
- K_i' : 그룹 i의 (k,n)-TSSS에서 분배하고자 하는 비밀정보

4.2 참가자 카드 발급 단계

비밀분산에 참가하는 참가자는 최초에 비밀분산시스템을 통하여 참가자 모두에게 비밀분산 스마트카드를 발급한다. 카드 발급은 참가자 인적 정보의 등록,상호 간에 협의된 비밀분산 정책등록, 비밀분산 카드 어플리케이션 탑재, 카드 발급 및 등록 과정을 통해서 처리된다.

- 참가자 등록 및 정책 등록

비밀분산 시스템에 참여하는 사업자는 각 사에서 비밀분산 참가자 정보를 비밀분산시스템에 등록한다.

- 비밀분산 시스템 참가자의 인적정보, 그룹 내의 재분산 참가자 수((k,n)-threshold scheme의 k값)
- 해당 참가자의 권한, 해당 참가자의 CHV 인증코드

비밀분산 시스템 신청된 참가자 정보를 기준으로 해당 참가자에 따른 정책을 수립하고, 이를 데이터베이스 등록한다.

- (t,t)-threshold scheme에서 분산된 비밀정보의 재분산 시행여부
- (t,t)-threshold scheme에 참여하는 사업자의 대표자 지정여부
- (k,n)-threshold scheme에 참여하는 참가자중 임계치 k를 만족하는 최소 집합 구성

- 카드 어플리케이션의 탑재 및 발급

스마트카드 관리시스템은 비밀분산 카드 어플리케이션을 각각의 참가자 카드에 설치하고, 해당 참가자의스마트카드 발급을 위하여 아래와 같은 데이터를 해당 데이터 베이스로부터 수집하게 된다.

- 참가자 접근권한 및 참가자 인적 정보 프로파일
- 정책파일에 대한 정보를 가지는 비밀분산 카드 어플리케이션 프로파일
- 스마트카드의 칩 정보 및 사양에 대한 정보를 가지고 있는 카드 프로파일
- 비밀분산 카드 어플리케이션에서의 데이터 암호화를 위한 키 정보를 가지는 키 프로파일
- CHV인증코드의 재시도 횟수

비밀분산 카드 어플리케이션의 발급을 위한 각 프로파일 데이터 수집이 완료가 되면 스마트 카드관리시스템은 비밀분산 카드 어플리케이션과 보안채널을 생성하여 각 프로파일 정보를 스마트카드로 전송한다.

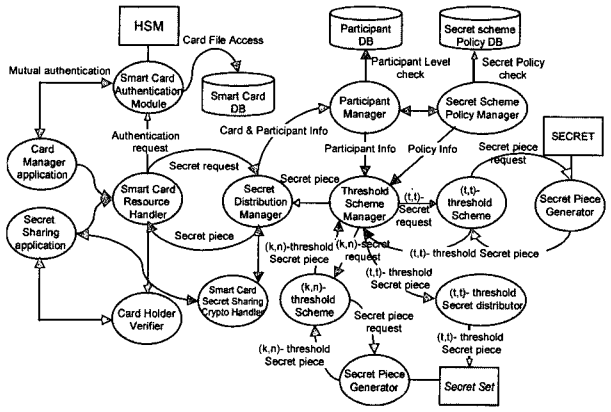
스마트 카드 발급이 완료되면 참가자에게 부여한 참가자 ID, 스마트카드 시리얼번호, 등을 참가자 데이터베이스에 등록한 후 해당 카드를 참여자 $P = \{P_1, P_2, \cdots, P_t\}$에게 각각 분배하여 준다.

4.3 비밀 분산(Secret Distribution)

비밀분산시스템은 비밀분산 시스템에 참가하는 참가자 집합 G와 해당 그룹의 참가자 집합 P에 따라서 각각 다른 threshold Scheme을 적용한다. (t,t)-TSSS에서는 참가자 집합 $G = \{G_1, G_2, \cdots, G_t\}$에게 비밀정보를 분배하게 되며, 각 그룹 참가자의 대표자에게 분산된 비밀정보는 (k,n)-TSSS을 이용하여 다시 해당 그룹의 참가자 집합 $P = \{P_1, P_2, \cdots, P_n\}$에게 분배되게 된다. 이때 (k,n)-TSSS에서 분배하고자 하는 비밀정보(K')는 (t,t)-TSSS에서 분배한 분산비밀정보 y_i가 된다. 이는 최초 비밀정보(K)를 분산함에 있어서 참

가자간의 계층구조(hierarchical structure)를 가지게 되며 그룹 수준에서 참가하는 참가자(G_i)는 해당 그룹의 참가자 집합 $P=\{P_1, P_2, \cdots, P_n\}$의 분산 비밀정보를 모두 가지게 된다. 만약 해당 그룹 참가자(G_i)가 (t,t)-TSSS 시스템에 참여하지 않았다면 G_i그룹 내의 n명의 참여자 G_iP가 모두 참가하여 비밀정보를 분배받아야 한다. 이때 n명의 참가자는 (k,n)-TSSS에 의해서 비밀정보를 분배받게 되며, 해당 그룹 내에서 참가하는 n명의 참가자의 수를 정의하게 된다. 즉, 해당 그룹의 정책이 정의되는 시점에 정의된 정책에 의해서 참가자 카드를 발급받은 n명의 참가자가 참가하게 된다.

(t,t)-(k,n)-TSSS시스템은 (그림 3)에서 정의한 분산처리 과정과 같이 아래 절차로 수행되어진다.



(그림 3) 비밀정보의 분산처리 흐름

◦ Step 1 : 참가자 검증(Participant Verification)

비밀분산시스템(SSS)에 참가하는 참가자는 자신의 스마트카드를 비밀분산시스템에 제출한다. 비밀분산시스템의 스마트 카드 자원 매니너는 삽입된 스마트카드와 통신하며, 카드 소지자 검증 모듈(verifier)은 카드 소지자 검증을 위하여 참가자 자신이 설정한 인증코드(authentication code)를 요구하게 되며, 카드 소지자로부터 받은 비밀번호를 비밀분산 카드 어플리케이션으로 전송하여 확인함으로써 본인의 정당성을 확인한다. 만약, 카드소지자가 제출한 인증코드가 5회 이상 오류가 발생할 경우 비밀분산 카드 어플리케이션은 라이프 사이클 상태를 LOCKED상태로 전환하고 더 이상의 작업을 수행하지 않는다.

◦ Step 2 : 참가자 카드 인증

상기 과정이 완료된 카드에서 대해서 비밀분산시스템의 스마트카드관리 시스템은 스마트 카드 관리자(Card Manager)와 비밀분산시스템의 스마트카드 인증 모듈(SAM : Smart Card Secure Authentication Module)과의 상호 인증 절차를 통해서 카드 인증을 수행하게 된다. 카드 인증절차가 완료되면 비밀분산 시스템은 아래와 같은 운영상의 검증 항목을 수행한다.

- 카드로부터 판독된 스마트 카드 일련번호를 이용하여 카드DB에 저장된 해당 ID의 스마트카드의 현재 상태(도난, 분실, 비정상, 정상 등) 등을 확인하여 정상적으로 발급되어 사용 중인 카드임을 검증한다.
- 카드로부터 판독된 참가자의 ID를 통해서 비밀분산시스템의 참가자 DB에 저장된 해당 참가자의 현재 상태(자격정지,퇴사, 정상 등)를 확인한 후 정상 참가자임을 검증한다.
- 상기 2가지 항목의 검증 작업이 실패하였을 경우 비밀분산시스템은 해당 스마트카드를 회수하고 정당한 참가자에 대한 재발급 절차를 수행한다.

◦ Step 3 : 참가자 접근권한 및 정책 확인

비밀분산 시스템의 스마트카드관리시스템은 스마트카드 자원 매니저를 통하여 <표 1>~<표 3>에서 정의한 참가자 파일, (t,t)-threshold scheme 파일, (k,n)-threshold scheme에서 아래와 같은 정보를 읽어온다.

- 해당 참가자의 소속 기관 ID 및 참가자의 ID
- 해당 참가자의 보안 권한

◦ Step 4 : If $P_i \in G_i$, Call (t,t)-TSSS, otherwise Call-TSSS and then (k,n)-TSSS

상기 과정에서 분석된 참가자 보안 권한 <표 4>및 정책을 파일 통해서 비밀분산 시스템의 threshold manager는 다음 2가지 형태의 분산업무를 수행하게 된다.

① $P_i \in G_i$(Security Level = 0×10)

(t,t)-TSSS는 3장 (t,t)-threshold Scheme에서 정의한 절차를 통해서 아래와 같은 분산 비밀정보를 생성한다.

$$y_t = K - \sum_{i-1}^{t-1} y_i \bmod m$$

② $P_i \in G_iP_i$(Security Level = 0×01)

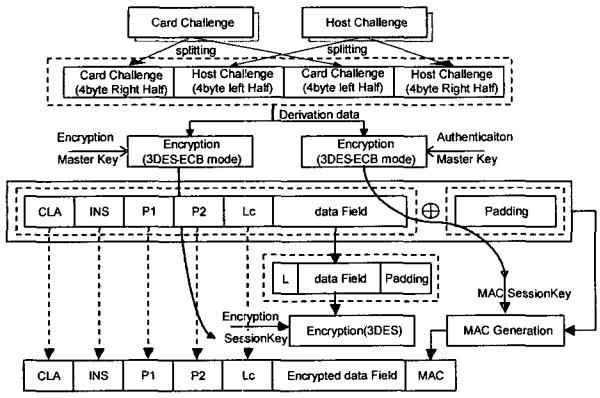
비밀분산시스템(SSS)는 먼저 (t,t)-TSSS시스템을 통하여 y_j을 계산한 후, (k,n)-TSSS를 이용하여 a_i를 생성한다.

$$a_i = f(x_i) = y_i + (b_1 x + \cdots + b_{t-1} x^{t-1}) \bmod p$$

◦ Step 5 : Distribute the Share y_i or a_i to G_i or G_iP_i

상기 과정에서 생성된 참가자(P_i)의 속성에 따라 y_i or a_i이 참가자(P_i)의 스마트 카드에 저장된다. 이때 비밀분산시스템은 참가자의 스마트카드에 threshold secret file의 필드 값을 secure channel을 형성한 후 안전하게 참가자의 스마트카드에 저장하게 된다.

스마트카드 Command APDU구조[12] 형태로 분산 비밀정보의 암호화 및 메시지 인증코드를 생성하여 안전하게 카드로 저장하게 되며, 일련의 절차는 (그림 4)와 같다.



(그림 4) Secure Channel를 위한 Command APDU 구성

4.3.1 데이터 필드 암호화

• Step 1 : 스마트카드에서 생성한 8바이트 난수 값(r_2)을 좌측 4바이트 값(r_{2_LBS}), 우측 4바이트 값(r_{2_MSB})으로, 외부 단말에서 생성한 난수 8바이트 값(r_1)을 좌측 4바이트 값(r_{1_LBS})과 우측 4바이트 값(r_{1_MSB})으로 나누어, $r_{2_MSB} \| r_{1_LBS} \| r_{2_LBS} \| r_{1_MSB}$로 재정렬하여 파생 데이터(R_d)를 생성한다.

$$R_d = r_{2\_MSB} \| r_{1\_LBS} \| r_{2\_LBS} \| r_{1\_MSB}$$

• Step 2 : 상기 과정에서 생성한 파생 데이터(R_d)를 스마트카드에 기 설정된 암호화용 마스터키(K_E)를 이용하여 암호화용 세션 키(S_{E_K})를 생성한다.

$$S_{E\_K} = \text{3DES}(R_d, K_E)$$

• Step 3 : 상기 과정에서 생성한 암호화용 세션 키(S_{E_K})를 이용하여 Command APDU의 데이터 필드(D)를 암호화한다. 이때 데이터 필드의 길이가 8의 배수가 아닌 경우 패딩 규칙에 따라서 '0×00'를 패딩한다.

$$D_e = \text{3DES}(D, S_{E\_K})$$

4.3.2 Command APDU의 MAC생성

• Step 1 : 데이터 필드 암호화의 Step 1과 동일하다.

• Step 2 : 상기 과정에서 생성한 파생 데이터(R_d)를 스마트카드에 기 설정된 MAC생성용 마스터키(K_A)를 이용하여 MAC생성용 세션 키(S_{A_K})를 생성한다.

$$S_{A\_K} = \text{3DES}(R_d, K_A)$$

• Step 3 : 상기 과정에서 생성한 MAC생성용 세션 키(S_{A_K})를 이용하여 Le를 제외한 Command APDU(D') 전체를 암호화한 후 상위 4바이트를 취하여 이를 MAC_4를 사용한다.

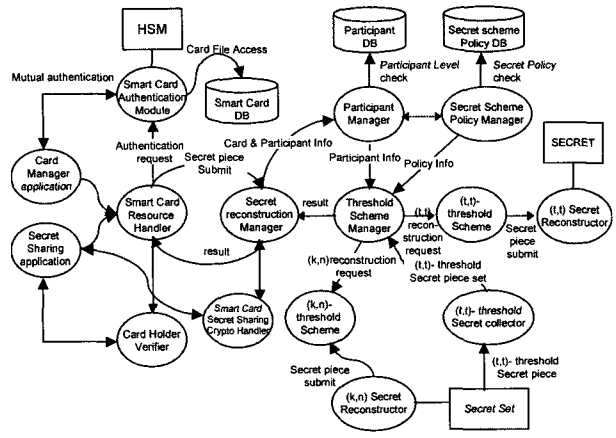
$$D' = CLA \| INS \| P1 \| P2 \| Lc \| Data$$
$$\text{MAC}_4 = \text{3DES}(D', S_{A\_K})$$

4.3.3 Command APDU의 전송

비밀분산 시스템(SSS)는 분산된 비밀정보(데이터 필드의 영역 값)를 스마트 카드로 전송시 상기 데이트 필드 암호화 과정을 통해서 암호화되며, Command APDU 전송시 상기 MAC생성 과정을 통해서 생성된 MAC_4 값을 붙여서 스마트 카드로 전송하게 된다. 이를 통해서 비밀분산시스템과 스마트카드는 상호간의 통신에 있어서 암호성, 무결성, 인증, 등의 암호특성을 만족시킨다.

4.4 비밀복원 단계(Secret Reconstruction)

비밀정보의 분산 및 복원은 비밀분산에 참가자 집합이 최초로 설정한 분산정책에 의하여 행하여 진다. 분산된 비밀정보의 복원에 있어서도 분산시 적용했던 정책을 통해서 복원을 행하게 된다.



(그림 5) 비밀정보의 복원처리 흐름

예를 들어, 유형 2의 경우를 살펴보도록 하자. G_1그룹은 그룹 대표 참가자 G_1없이 G_1의 하부 참가자 집합(G_1P_1, G_1P_2, G_1P_3)에게만 비밀정보를 분산하며, G_2그룹은 그룹 대표 참가자 G_2와 G_2의 하부 참가자 집합 (G_1P_1, G_2P_2, G_2P_3) 모두에게 비밀정보를 분산하며, G_3그룹은 그룹 대표 참가자(G_3)만 참여하는 정책을 수행하고 있다.

(t, t)-(k, n)-TSSS시스템은 (그림 3)에서 정의한 복원처리 과정과 같이 아래 절차로 수행되어진다.

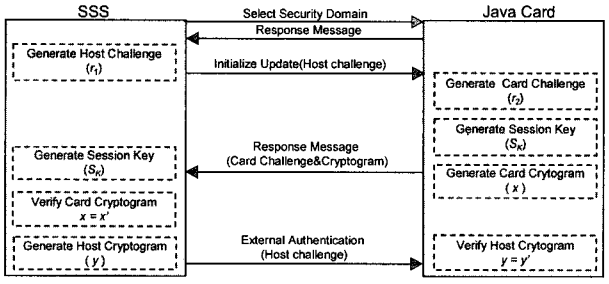
• Step 1 : 비밀 소유자 검증(Share Holder Verification)

Distribution Phase에서 수행했던 것과 동일하게 참가자의 개인 비밀번호(PIN)를 입력받아 참가자 카드의 정당한 소유자임을 확인하다.

• Step 2 : 비밀 소유자 카드 인증(The authentication of Share Holder's smart card)

Distribution Phase에서 수행하였던 것과 동일하게 비밀분산 시스템과 참가자의 스마트카드는 상호인증을 통하여 참가자 카드의 위/변조 및 현재 카드 상태를 확인하다. 이는 비밀분산에 참여한 후 회사 및 그룹의 정책에 의하여 해당

참가자의 카드의 자격을 정지하거나, 분실 및 도난으로 인하여 카드 상태를 변경할 수 있으므로 이를 검증한다.
비밀분산 시스템과 자바카드와의 상호 인증을 위한 절차는 아래 그림과 같이 비밀키 암호 기반의 상대인증 방식을 진행되며 상세한 절차는 아래와 같다[1, 3].



(그림 6) 카드와 비밀분산시스템과의 상호인증

① 비밀분산 시스템(SSS)은 난수(r_1)를 생성해서 카드로 송신하다.
② 자바카드는 난수(r_2)를 생성한 후 수신받은 r_1과 조합하여 자바카드내에 마스터 키(M_k)를 이용하여 세션 키 $S_k = 3DES(r_1 \| r_2, M_k)$를 생성한다.
③ 상기 과정에서 생성된 S_k를 이용하여 카드는 $x = 3DES(r_2 \| r_1, S_k)$를 생성하여 SSS로 송신하다.
④ *SSS*는 상기 과정에서 수신한 난수(r_2)를 이용하여 세션키 S_k를 생성한 후 검증 데이터 $x' = 3DES(r_2 \| r_1, S_k)$를 생성하여 수신된 x와 비교하여 자바카드를 인증한 후 SSS의 Cryptogram $y = 3DES(r_1 \| r_2, S_k)$를 생성하여 카드로 송신하다.
⑤ 자바 카드는 검증 데이터 $y' = 3DES(r_1 \| r_2, S_k)$를 생성한 후 수신된 y와 비교하여 SSS를 인증함으로써 상호간의 인증을 수행한다.

◦ Step 3 : Share Holder Privilege & Secret Sharing Policy Check

비밀분산 시스템은 참가자의 카드로부터 읽은 정보 파일을 분석하여 해당 참가자의 보안 권한을 파악하게 되며, 또한 비밀분산을 위한 정책 파일을 확인한다. 비밀분산시스템은 <표 4>의 참가자의 보안권한을 판독하여 해당 비밀정보 파일<표 1>, <표 2>의 유효기간을 확인하며, 또한 <표 3>의 참가자 파일(참가자 ID)을 판독하여 해당 참가자가 비밀정보 분산에 참가한 사람인지를 확인한다.

◦ Step 4 : If $P_i \in G_i$, Call (t, t)-TSSS, otherwise Call (t, t)-TSSS and then (k, n)-TSSS

분산된 비밀정보의 복원은 (k, n)-TSSS를 통하여 K'를 복원한 후 (t, t)-TSSS를 수행하여 비밀정보 K를 복원한다.

① $\forall P_i \in G_i$

비밀정보 복원에 참여하는 참가자 집합이 모두 G_i에 속할 경우 비밀분산 시스템은 (t, t)-TSSS을 통하여 비밀정보(K)를 복원하게 된다.

$$k = \sum_{i=1}^{t} y_i \bmod m$$

② $P_i \in G_i P_i$

비밀정보 복원에 참여하는 참가자 집합이 $G_i P_i$에 속할경우 비밀분산시스템은 (k, n)-TSSS를 먼저 호출하여 G_i에 분배한 비밀정보(K')를 우선 복원한다.

$$k' = \sum_{j=1}^{t} y_i \prod_{1 \le k \le t, k \ne j} \frac{x_{i_k}}{(x_{i_k} - x_i)}$$

참가자 집합 $G = \{G_1, G_2, \cdots, G_t\}$에 분배된 비밀정보 집합 $K' = \{K'_1, K'_2, \cdots, K'_t\}$을 (k, n)-TSSS를 이용하여 복원한 후 상기 과정의 (t, t)-TSSS를 호출하여 최초 비밀정보 K를 복원한다.

5. 비밀분산 시스템의 분석

(t, t)-(k, n)-비밀분산법을 이용한 스마트카드 기반의 비밀분산시스템은 아래와 같은 특성을 가진다.

5.1 비밀정보의 분산 가중치 부여(Weight Management)

비밀분산 시스템(*SSS*)을 현실 시스템에서 구현할 때 실제로 참여자의 직위나 참여자들의 관계에 의해서 해당 참여자에게 적절하게 가중치(W)를 부여하여 비밀정보를 분산하여야 한다. 그러나 일반적인 비밀분산 시스템에서는 분배하고자 하는 참여자(P)의 보안 권한이나 직위 여부에 따른 가중치(W)를 판단하는 방법이 실제로 시스템을 운영하는 운영자(operator) 또는 배분자(dealer)가 대면(face-to-face) 또는 서류 확인 등의 절차를 통해서 참여자(P)의 신원 및 권한을 확인하여야 했다. 그러나, 스마트카드 기반의 비밀분산 시스템은 비밀분산을 협의한 참여자의 특성에 따라서 최초에 참여자의 특성에 따른 비밀정보 접근 권한(access condition)을 부여한 스마트 카드를 사전 발급함으로써 비밀정보 분산시 참여자가 제출한 스마트카드의 정보를 판독하여 능동적으로 해당 참여자의 권한에 따라 적절하게 비밀정보를 조정하여 참여자에게 분산할 수 있다.

5.2 접근권한의 부여

스마트카드 기반의 비밀분산 시스템은 비밀분산에 참여하는 참여자의 카드소지자 정당성을 확인하기 위하여 스마트카드에서 제공하는 카드소지자 인증방법(CHV : Card Holder Verification)으로 최초 발급시 참여자(P)가 직접 설정한 인증코드(authentication code)를 비밀분산 및 비밀복원 단계에서 직접 입력하도록 요구한다. 카드소지자의 인증단계가 수행된 후 비밀분산시스템은 스마트카드 자체의 위/변조 및 분실/도난 여부를 검증하기 위하여, 비밀분산시스템과 스마트카드가 상호인증을 수행하며, 인증이 완료된 카드에 대해서 최초 발급시 등록된 스마트 카드 ID및 참여자의 정보를 통해서 카

드 상태를 점검하게 된다. 이를 통해서 정상적인 정당한 스마트카드에 대해서만 비밀분산 및 복원에 참여할 수 있도록 권한을 부여하게 된다. 또한 비밀분산 시스템은 비밀분산소지자의 보안 프로파일을 판독하여 해당 보안권한의 따라서 분배하고자 하는 비밀정보를 조절함으로써 해당 비밀정보에 대한 접근권한도 통제하게 된다.

5.3 분산의 효율성(Distribution Efficiency)

비밀분산자와 분산정보 소유자간에 많은 통신 교환 및 주기적인 비밀정보 Refreshment가 필요한 검증 가능한 비밀분산법(verifiable secret sharing scheme)[14]의 경우 스마트카드 기반의 비밀분산 시스템은 분산자 정보 소유자와 네트워크를 통한 원격 통신을 통하여 효율적으로 비밀정보를 재분산할 수 있도록 하며, VSSS(Verifiable Secret Sharing Scheme)에서 참여자에게 분배하는 분산정보와 함께 분배하는 분산정보 소유자가 분배받은 분산정보를 직접 검증하기 위하여 필요한 정보를 스마트 카드를 통해서 분배하며, 분산정보 소유자는 자신이 소유한 스마트카드의 연산기능을 통해서 직접 검증할 수 있도록 한다.

6. 결 론

본 논문에서는 Shamir가 제안한 (k, n)-threshold Secret Sharing Scheme[1]과 Karnin, Greene, Hellman이 제안한 (t, t)-threshold secret sharing Scheme[6]를 혼용한 비밀 분산법에 분배자와 비밀정보 소유자간의 신뢰성과 분산된 비밀정보의 안정성을 위해 탬퍼 방지 소자(tamper-resistance device)인 스마트카드를 결합한 비밀분산 시스템을 제안하였다. 제안한 시스템은 디지털 커버전스(digital convergence)가 가속화되고 융합 서비스가 출현하는 시장 환경에서 제휴 사업자간 또는 동일 조직 내의 비밀정보를 분산하여 관리하는 키 관리 시스템에 매우 유용하게 응용될 수 있을 것이다. 또한 임계치(threshold)의 적절한 선택하여 비밀분산법을 운영함으로써 참가자간의 이해관계와 상황에 따라 계층적 비밀분산(hierarchical secret sharing scheme) 관리와 참가자간의 상호 합의에 의한 비밀분산 시스템 운영할 수 있는 등의 유연한 시스템 운영방안을 마련할 수 있다.

향후 보다 실용적이고 효율적인 비밀분산 시스템 설계를 위한 다양한 비밀분산법(verifiable secret scheme, multi-threshold secret sharing scheme,등)의 응용연구와 스마트카드 내에서 직접 비밀분산이 가능한 비밀 분산시스템 설계에 연구할 것이다.

참 고 문 헌

[1] Shamir A, "How to Share a Secret," Comm. Of the ACM, 22, pp.612-613, 1979.

[2] Digital Cellular Telecommunication Systems Phase 2+, Specification of Subscriber Identification Module-(SIM-ME) interface, GSM 11.11, ETSI.

[3] Ahmet M.Eskicioglu, "A Key Transport Protocol Based on Secret Sharing-Applications to Information Security," IEEE Transactions on Consumer Electronics, Vol.48, No.4, pp. 816-824, November, 2002.

[4] D. Catalano and R. Gennaro. "New and Efficient Protocols for Verifiable Signature Sharing and Other Applications," Journal of Computer and System Sciences, Vol61, No.1, pp.51-80, August, 2000. Preliminary version in the proceedings of CRYPTO'98, Springer-Verlag LNCS 1462, pp.105-120.

[5] E. F Brickell and D.R. Stinson, "Some Improved Bounds on the information Rate of Perfect Secret Sharing Schemes," Journal of cryptology, Vol.5, pp.153-166, 1992.

[6] ISO/IEC 7816-4, identification cards-integrated circuit(s) cards with contacts-interindustry commands for interchange, 1995.

[7] Java Card 2.1.1, Sun Microsystems, 1998.

[8] E. D. karnin, J. W. Greene and M. E. Hellman, "On Secret Sharing Systems," IEEE Transaction on Information Theory, v.IT-29, pp.35-41, 1983.

[9] Douglas R. Stinson, "Cryptography theory and Practice," CRC Press, Inc, pp.330-331, 1995.

[10] Sun microsystems, java card API 2.1 Application Programming Interface, 1998.

[11] Global platform, http://www.globalplatform.org/.

[12] ISO/IEC 7816-4, identification cards-integrated circuit(s) cards with contacts-interindustry commands for interchange, "5.3. APDU message structure," pp.7-10, 1995.

[13] Global Platform, Open Platform Card Specification Ver.2.1, pp.(10-1)-(10-2), June, 2001.

[14] M. Stadler, "Publicly Verifiable Secret Sharing," Advances in Cryptography-Eurocrypto96, LNCS, Vol.1070, pp.190-199, Springer-Verlag, 1996.

손 영 설

e-mail : sonys@kt.co.kr

1995년 부산외국어대학교 컴퓨터공학과(학사)

2004년 고려대학교 정보보호대학원(공학석사)

1995년~현재 KT 서비스개발연구소 재직 중

관심분야 : 정보보호, 암호 프로토콜, 스마트카드, RFID, 네트워크 보안, 전자지불

이 동 훈

e-mail : donghlee@korea.ac.kr

1984년 고려대학교 경제학과

1987년 Oklahoma Univ. 전산학과 석사

1992년 Oklahoma Univ. 전산학과 박사

1993년~2001년 고려대학교 전산학과 교수

2001년~현재 고려대학교 정보보호대학원 교수

관심분야 : 암호이론, 암호 프로토콜, 정보이론