겹선형 쌍을 이용한 Threshold 패스워드-인증 키 Retrieval 프로토콜

이송원, 김광조

한국정보통신대학원대학교, 국제정보보호기술연구소

Threshold Password-Authenticated Key Retrieval Protocol Using Bilinear Pairings

Songwon Lee and Kwangjo Kim

International Research center for Information Security(IRIS),

Information and Communications Univ.(ICU), Korea

요 약

본 논문에서는 로밍 사용자를 위한 threshold 패스워드-인증 키 retrieval 프로토콜을 제안한다. 로밍 사용자는 자신의 전용 단말기 이외의 단말기를 이용하여 네트워크에 접근하고자 하는 사용자를 말한다. 본 제안 프로토콜은 로밍 사용자가 자신의 신원정보와 패스워드만을 가지고 원격의 서버들로부터 비밀키를 다운로드 할 수 있도록 한다. 본 논문은 특히, 다중-서버 로밍 시스템의 목적 중의 하나로써, 서버들 중의 일부가 손상되었을 지라도 사용자가 자신의 비밀키를 다운로드 할 수 있는 프로토콜을 제안한다. 이러한 관점에서, 본 논문은 최초의 threshold 패스워드-기반 로밍 프로토콜을 제안하고 있는데, 이를 위하여 (k,n)-threshold scheme을 사용한다. 제안된 scheme은 Weil 쌍이나 Tate 쌍에서 구현될 수 있는 겹선형 쌍에 기반 한다.

I. 서론

인터넷의 급속한 발전으로 사용자는 네트워크에 용이하게 접근할 수 있다. 이를 통하여, 서비스 공급자로부터 특정의 서비스를 받거나 비밀 정보를 사전에 서버에 저장한 후 이를 나중에 다운로드 할 수 있다. 이때, 사용자는 자신이 정당한 사용자임을 서버에게 확인시켜 주어야만 한다. 사용자의 신원(ID)을 검증하기 위하여, 많은 실세계 시스템들은 패스워드-기반의 인증을 사용한다. 그러나 대부분의 사용자 패스워드는 상대적으로 작은 집합 공간에서 선택되고 쉽게 기억될 수 있다는 근본적인 문제점을 가지고 있는데, 이것은 곧 공격자가 패스워드를 쉽게 추측해 낼 수 있음을 의미한다. 로밍 사용자는 자신의 전용 단말기 이외의 단말기를 이용하여 네트워크에 접근하여 자신의 ID와 패스워드만을 가지고 원격의 서버들로부터 비밀키를 다운로드고자 하는 사용자를 말하며, 자신의 비밀정보를 저장하고 있는 스마트 카드 등을 휴대하지 않는다. 스마트 카드는 기밀 정보를 저장하는 중요한 수단으로 사용되지만, 많은 실 환경에서 적용하기 어려운 점이 있는데, 주로 불편함에 기인한다. 예를 들면, 사용자는 스마트 카드와의 통신을 위한 별도의 인터페이스를 필요로 한다. 이러한 관점에서, 강력한 패스워드 기반의 인증 프로토콜들이 제안되고 있으며, Perlman 등[13], Ford 등[6], 그리고 Jablon[9] 등이 제안한 프로토콜이 대표적이다. 본 논문에서는 다중-서버를 이용한 threshold 패스워드 로밍 프로토콜을 제안한다. 기존에 제안된 다중-서버 프로토콜들의 경우, 서버들 중의 일부가 손상된 경우 사용자는 프로토콜을 성공적으로 완료할 수 없다. 즉, 그러한 경우 사용자는 자신의 비밀키를 다운로드 할 수 없게 된다. 본 논문에서 제안하는 프로토콜은

(k,n)-*threshold scheme*을 사용하는데 단지 k개의 정상적인 서버들만을 통하여서 비밀키를 복구할 수 있다. 우리의 scheme은 Weil 쌍이나 Tate 쌍에서 구현될 수 있는 겹선형 쌍에 기반 한다.

II. 사전 준비

1. 관련 연구

Perlman과 Kaufman은 비밀키를 안전하게 복구할 수 있는 프로토콜[13]을 제안하였다. Ford와 Kaliski는 패스워드 경화(hardening) 프로토콜을 통하여 공격을 방어할 수 있는 다중-서버를 이용하는 방법[6]을 제안하였다. 경화 프로토콜은 서버와 사용자간의 통신을 통하여 사용자의 패스워드를 강력한 비밀정보로 만들 수 있도록 한다. 또한, Jablon은 패스워드-기반의 다중-서버 로밍 프로토콜[9]을 제안하였는데, 프로토콜을 통하여 사용자는 서버를 인증할 수 있고 자신의 비밀키를 복구할 수 있다. 이상의 프로토콜들은 사용자가 쉽게 기억할 수 있는 패스워드만을 사용하고 있는데, [6]과 [9]는 프로토콜의 목적을 달성하기 위하여 다중-서버를 사용하고 있다. 그러나, 서버들 중에서 일부가 손상된 경우 사용자는 올바른 자신의 비밀키를 얻을 수 없게 되는데, 이것은 키가 올바른지 여부를 사용자가 검증할 수 있는 것과는 별개의 문제이다. 본 논문에서는 이와 같은 문제를 해결하기 위한 하나의 방법을 제시하고자 한다.

우선, 여기에서는 [9]에서 제시된 프로토콜을 간략히 살펴본다.

Parameters. 프로토콜은 Z_p^*에서 위수가 q인 부분군 상에서 작동한다, 여기에서 p, q 그리고 r은 홀수인 소수이며, $p=2rq+1$, $2^{k-1}<p<2^k$, $r \neq q$ 이고 $2^{2j-1}<q<2^{2j}$이다.

Enrollment. 사용자는 패스워드 π를 선택하고, $g_\pi = h(\pi)^{2r}$를 계산하며, 자신의 비밀키 U를 생성한다. 각 $i \in [1,n]$에 대하여, 사용자는 비밀키 공유값 $S_i = g_\pi^{y_i}$을 계산하는데, 임의로 선정된 난수 $y_i \in_R [1,q-1]$을 사용한다. 그리고, 사용자는 자신의 마스터키로서 j-비트의 대칭 키 K_m를 생성하는데, $K_m = h(S_1 \| \cdots \| S_n) \pmod{2^j}$이다. 이를 이용하여 자신의 비밀키를 암호화한다. 즉, $U_K = {}_{K_m}\{U\}$. 또한, 마스터키 검증값 $proof_{PK_m} = h(K_m \| g)$을 생성한다.

1. Client: $\{ID_A, y_i, U_K, proof_{PK_m}\}$를 각 서버 L_i ($i \in [1,n]$)에게 전송한다.
2. Servers: 각 서버는 자신이 관리하는 목록 C_i에 수신된 정보를 저장한다.

Authenticated Retrieval. 등록이 완료된 후 사용자는 필요시 자신의 비밀키를 복구할 수 있는데, 이를 위하여 다음의 절차를 수행한다.

1. Client: 임의의 난수 $x \in [1,q-1]$를 선정한 후, $X = g_\pi^x \pmod{p}$를 계산하며, $\{ID_A, X\}$를 서버에게 전송한다.
2. Servers: 해당 사용자의 C_i로부터 $\{ID_A, y_i, U_K, proof_{PK_m}\}$를 조회하여 $Y_i = X^{y_i}$계산하고, $\{Y_i, U_K, proof_{PK_m}\}$를 클라이언트에게 전송한다.
3. Client: 각 서버 $i \in [1,n]$에 대하여 $S_i = Y_i^{1/x} \pmod{p}$를 계산하고, 마스터키인 $K' = h(S_1 \| S_2 \| \cdots \| S_n)$를 생성한다. 이때, $proof_{PK_m} \neq h(K' \| g)$이면 프로토콜을 중지하고, 그렇지 않으면 비밀키 $U = {}_{1/K'}\{U_K\}$를 구한다.

2. Threshold 암호시스템

비밀키 공유 scheme으로 불리는 Threshold scheme의 개념은 [14]에서 소개되었고, 그 이후로 그러한 scheme에 대한 많은 연구가 수행되어왔다.

(k,n)-*threshold 비밀키 공유 scheme*은 n개의 참여자들 간의 프로토콜인데, 여기에서 *dealer*는 비밀(*secret*)에 관한 부분정보(*share*)를 생성하여 n개의 참여자들에게 배분한다.

- k개미만의 참여자들로 이루어진 임의의 참가자 그룹은 *secret*에 관한 어떠한 정보도 얻어낼 수 없다.
- 적어도 k개의 참여자들로 이루어진 임의의 참가자 그룹은 다항 시간 이내에 *secret*을 계산해 낼 수 있다.

다음 장에서는 우리가 제안하고자 하는 scheme을 상세히 기술한다. 제안하는 scheme에서는 (k,n)-*threshold scheme*을 사용하는데, 사용자는 비밀값을 다중 서버들에게 분산시킨다. 이때 서버의 개수는 $n \geq 2k-1$인 것으로 가정한다 [12,10].

3. 겹선형 쌍

동일한 위수 q를 갖는 덧셈군 G_1과 곱셈군 G_2가 있다고 하자. 그러한 그룹 내에서 이산대수문제를 푸는 것이 어렵다고 가정한다. P를 덧셈군 G_1의 생성자라고 하자. 그리고, $\hat{e}: G_1 \times G_1 \rightarrow G_2$을 다음 속성을 만족하는 겹선형 사상이라 하자:

1. Bilinearity: 모든 $P, Q \in G_1$와 모든 $a, b \in Z$에 대하여, $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$ 이다.
2. Non-degeneracy: 모든 $Q \in G_1$에 대하여, $\hat{e}(P, Q) = 1$이면, $P = O$ 이다.
3. Computability: 모든 $P, Q \in G_1$에 대하여, $\hat{e}(P, Q)$를 계산하기 위한 효율적인 알고리즘이 존재한다.

이상의 군 G_1과 G_2를 통하여, 다음과 같은 암호학적 문제를 정의할 수 있다:

· Discrete Logarithm(DL) 문제:

$P, P' \in G_1$가 주어졌을 때, $P = nP'$을 만족하는 정수 n을 구한다.

· Computational Diffie-Hellman(CDH) 문제:

$a, b \in Z_q^*$에 대하여 $(P, aP, bP) \in G_1$가 주어졌을 때, abP를 구한다.

· Decision Diffie-Hellman(DDH) 문제:

$a, b, c \in Z_q^*$에 대하여 $(P, aP, bP, cP) \in G_1$가 주어졌을 때, $c = ab \pmod{q}$인지 여부를 결정한다.

· Gap Diffie-Hellman(GDH) 문제:

CDH 문제는 풀기 어려우나 DDH 문제는 쉬운 문제들의 부류를 말한다.

겹선형 쌍을 구현하기 위하여, Weil쌍 또는Tate 쌍을 이용할 수 있다.

Ⅲ. 제안 방식

본 장에서는 제안하고자 하는 패스워드-기반 threshold 로밍 프로토콜을 설명한다. 프로토콜의 모델을 살펴본 후 상세한 프로토콜을 기술한다.

1. 모델

모델은 [9]에서의 모델과 유사하지만 몇 가지 차이점이 있다.

우선, 우리의 scheme은 threshold 개념을 사용하는데, 사용자는 n개의 서버에 비밀정보를 분산시키는 *dealer*의 역할을 수행한다.

그리고, 제안된 scheme은 사용자의 ID를 사용하는 ID-기반 암호시스템을 사용하는데 Boneh와 Franklin이 제안한 IBE scheme[2]을 예로 들 수 있다. 사용자의 비밀키를 생성하는 TA(Thrusted Authority)가 존재한다고 가정한다.

Enrollment. 사용자는 [14]에서와 유사한 방법으로 (k, n)-*threshold system*을 구성한다.

여기에서 사용자는 자신의 공개키 Q_{ID}를 선정하고 TA로부터 이에 대응하는 비밀키 D_{ID}를 얻은 것으로 가정한다.

사용자는 자신의 패스워드로부터 n개의 비밀 공유 값 Y_i를 산출하여 이로부터 마스터 대칭 키 K_m을 생성한다. 마스터키로 비밀키를 암호화하여 D_K를 얻는다. 마지막으로, 마스터키와 패스워드를 연결한 검증값 V를 생성한다. 사용자는 이상에서 생성한 Y_i, D_K 그리고 V를 자신의 ID와 함께 n개의 서버에게 전송한다. 서버는 이를 수신한 후 저장한다.

Authenticated Retrieval. 사용자가 가용한 임의의 단말기에서 서버로 접속하기를 원할 경우, 사용자는 우선 threshold 프로토콜을 수행하여 자신의 비밀키를 복구한다. 이때에 적어도 k개의 임의의 서버를 선정하며, [14]에서와 같은 방법으로 *Lagrange Interpolation*을 이용한다.

여기에서, 사용자가 사용하고 있는 단말기에는 사용자가 등록 시에 생성한 어떠한 정보도 저장되어 있지 않다는 것을 주목한다.

우선, 사용자는 임의로 k개의 서버를 선정하여 은닉된 패스워드 정보를 가진 요청 메시지를 선정된 서버들에게 보낸다. 이를 수신한 서버들은 등록 시에 저장된 정보와 수신된 정보를 이용하여 은닉된 응답 메시지를 보낸다. 이때에, 적어도 하나 이상의 서버에서 암호화된 비밀키 D_K와 검증값 V를 응답 시에 함께 전송한다.

사용자는 서버들로부터의 응답메시지를 이용하여 마스터 대칭 키 K_m을 생성한 후 이의 정당성을 검증한다. 마스터키가 정당한 경우, 이를 이용하여 암호화된 비밀키를 복호화 함으로써 원하는 비밀키를 얻는다.

2. 프로토콜

1) Setup

본 단계에서는 Boneh와 Franklin이 제안한 IBE scheme에서와 유사한 과정을 수행한다. 보다 상세한 내용을 원하는 독자는 [6]을 참조할 수 있다. 여기에서 TA는 [6]에서의 비밀키 생성자(PKG)의 역할을 수행하는데 GDH군에 속하는 덧셈군 G_1과 곱셈군 G_2를 선정한다. 이때 이들은 동일한 소수 위수 q를 갖는다. 또한, 겹선형 사상 $\hat{e}: G_1 \times G_1 \rightarrow G_2$, 생성자 $P \in G_1$, 그리고 마스터 비밀키 $s \in_R Z_q^*$를 선정한다. 그리고, TA는 $P_{pub} = sP$를 구하고, 암호학적 Hash함수 $H_1: \{0,1\}^* \rightarrow G_1^*$과 $H_2: G_2 \rightarrow \{0,1\}^n$ (for some n)을 선정한다.

공개 파라미터들은

$\mathbf{params} = \{G_1, G_2, \hat{e}, H_1, H_2, P, P_{pub}\}$이다.

사용자는 TA로부터 자신의 비밀키 $D_{ID} = sQ_{ID}$를 얻는다. 여기에서 $Q_{ID} = H_1(ID)$이다.

2) Enrollment

사용자는 패스워드 π를 선정하고, $R_{ID} = H_1(\pi)$를 구한다. 그리고 다음과 같이 차수 k-1의 다항식을 선정한다.

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

여기에서 $a_0, \cdots, a_{k-1} \in Z_q^*$는 임의의 난수이며, a_0는 사용자의 비밀값이다. 사용자는 자신의 기밀정보를 서버에 등록하기 위하여 그림1의 프로토콜을 수행한다.

Client(A) — **Servers(L_i)**

$y_i = f(i)$
$Y_i = y_i Q_{ID}$
$K = \hat{e}(a_0 R_{ID}, Q_{ID})$
$K_m = H_2(K)$
$D_K = {}_{K_m}\{D_{ID}\}$
$V = H_2(K_m \| P_{pub})$

$\xrightarrow{Q_{ID}, Y_i, D_K, V}$

그림 1: 등록 프로토콜.

클라이언트는 각 서버 L_i ($i \in [1, n]$)에게 $\{Q_{ID}, Y_i, D_K, V\}$를 전송하고, 이를 수신한 서버는 이들을 저장한다.

3) Authenticated Retrieval

비밀키를 복구하기 위하여, 클라이언트는 그림2의 프로토콜을 수행한다. k개의 서버들을 $S = \{L_i | 1 \le i \le k\}$로 나타낸다.

Client(A) — **Servers(S)**

$x \in_R Z_q^*$
$X = xR_{ID}$

$\xrightarrow{Q_{ID}, X}$

Retrieve $\{Q_{ID}, Y_i, D_k, V\}$
$R_i = \hat{e}(X, Y_i)$

$\xleftarrow{R_i, D_K, V}$

$l_i = \prod_{j \in S, j \neq i} \frac{j}{j-i}$ for each i^{th} server
$K' = \prod_{i \in S} R_i^{l_i x^{-1}}$
$K'_m = H_2(K')$
if $V \neq H_2(K'_m \| P_{pub})$, abort.
$D_{ID} = {}_{1/K'_m}\{D_K\}$

그림 2: 키 복구 프로토콜.

위 프로토콜의 타당성은 다음과 같이 쉽게 검증될 수 있다.

$$\begin{aligned}
K' &= \prod_{i \in S} \hat{e}(xR_{ID}, y_i Q_{ID})^{l_i x^{-1}} \\
&= \prod_{i \in S} \hat{e}(y_i l_i R_{ID}, Q_{ID}) \\
&= \prod_{i \in S} \hat{e}(f(i) \prod_{j \in S, j \neq i} \frac{j}{j-i} R_{ID}, Q_{ID}) \\
&= \hat{e}(\sum_{i=1}^{k} f(i) \prod_{j \in S, j \neq i} \frac{j}{j-i} R_{ID}, Q_{ID}) \\
&= \hat{e}(a_0 R_{ID}, Q_{ID})
\end{aligned}$$

Ⅳ. 안전성 분석

본 장에서는 우리가 제안한 프로토콜을 안정성 측면에서 간략하게 논한다. 여기에서는 기본적으로 두 가지 유형의 공격과 프로토콜의 강인성(robustness)에 대하여 살펴본다.

우선, 공격자가 R_{ID}에 대한 어떠한 정보도 가지고 있지 않다고 가정할 수 있다. 이때, 프로토콜은 충분한 정보를 제공하지 않음으로써 공격자가 π나 R_{ID}에 대하여 사전 공격을 수행할 수 없도록 하여야 한다. 또한, R_{ID}를 알고 있는 공격자의 경우에, 공격자가 서버에게 정당한 사용자처럼 행사할 수 있어서는 안 되며, π(사전 공격을 하지 않고)에 관한 어떠한 유용한 정보도 알 수 있도록 하여서는 안 된다[4].

강인성 측면에서, 사용자는 π 및 이에 관련된 비밀 정보를 노출시키지 않고 서버들로부터 정당한 비밀키를 획득할 수 있어야 한다.

R_{ID} 또는 π에 대한 공격. 서버들 중에서 일부의 서버(k개미만)가 손상되었고 공격자가 R_{ID}를 획득하였다고 가정하자. 이때, 우리는 π와 마스터 대칭 키 K_m을 보호하는데 관심을 갖는다. 프로토콜의 수행 중에, R_{ID}를 제외하곤 π에 관련된 어떠한 정보도 전송되지 않는다. 이러한 경우, *Discrete Logarithm Problem (DLP)*와 *Computational Diffie-Hellman Problem (CDHP)*를 다항 시간 이내에 풀기가 어렵다고 가정한다면 해당 시간 이내에 어떠한 공격자도 π 그리고 심지어 K_m을 얻을 수 없다.

더욱이, k 개 이상의 서버가 손상되어 사용자가 프로토콜을 성공적으로 완료하지 못하였다 하더라도, K_m은 노출되지 않는다.

강인성[15,12]. 강인성은 $n \geq 2k-1$개의 서버들 중에서 $k-1$개의 서버가 손상된 경우에 주어진 scheme이 성공적으로 완료될 수 있는지를 확인시켜준다. 사용자는 등록 단계에서 threshold scheme을 구성할 때에 Z_q^*에서 균일한 분포도를 갖는 비밀값 a_0를 임의로 선정한다. 따라서, $n \geq 2k-1$개의 서버 중에서 많아야 $k-1$개의 서버를 손상시킬 수 있는 공격자가 존재한다 할지라도, 임의의 k개의 서버들은 Z_q^*에서 균일하게 분포하는 유일한 비밀값을 산출할 수 있다. 손상된 서버는 비밀값에 관련된 어떠한 정보도 얻을 수 없다.

우리는 scheme에 대한 엄밀한 안전성 분석은 향후의 작업으로 남겨둔다.

Ⅴ. 비교 분석

[6]과 [9]에 비교하였을 때, 우리의 scheme은 threshold 미만의 서버가 손상되었을 경우에 견딜 수 있는데, 단지 k개의 정상적인 서버들이 프로토콜에 참여할 수 있다면, 사용자는 자신의 비밀키를 복구할 수 있다.

표1은 [9]와 우리의 scheme을 연산 부하도 측면에서 비교하고 있다. 여기에서 $\mathbf{E}$와 $\mathbf{M}$은 각각 지수연산의 부하와 곱셈연산의 부하를 나타낸다.

표 1: 키 복구 시 클라이언트의 연산 부하.

	Jab01[9]	제안된 scheme
주요 부분	$S_i = R_i^{x^{-1}}$ $K' = h(S_1 \| \ldots \| S_n)$	$S_i = R_i^{l_i x^{-1}}$ $K' = h(\prod_{i \in S} S_i)$
연산 부하	$n\mathbf{E}$	$k(\mathbf{E}+\mathbf{M})$

표1로부터, 키 복구 시에 클라이언트의 연산 부하 측면에서 우리의 scheme이 [9]보다 효율적임을 알 수 있다. 즉, $n\mathbf{E} \geq k(\mathbf{E}+\mathbf{M})$, 여기에서 $n \geq 2k-1$. 이것은 k≥2인 경우, $(k-1)\mathbf{E}-k\mathbf{M} \geq 0$이기 때문이다.

Ⅵ. 결론

본 논문에서는 새로운 threshold 패스워드-기반의 로밍 프로토콜을 제안하였다. 제안된 프로토콜은, off-line 추측에 패스워드를 노출시키지 않고, 로밍 사용자가 원격의 서버로부터 자신의 비밀키를 다운로드 할 수 있도록 한다. 이때, client 단말기는 등록단계에서 생성된 사용자의 어떠한 정보도 가지고 있지 않다.

본 논문은, 다중-서버 로밍 시스템의 목적 중의 하나로써, 서버들 중의 일부가 손상되었을 지라도 사용자가 자신의 비밀키를 다운로드 할 수 있는 프로토콜을 제안하였는데, 이를 위하여 (k,n)-threshold scheme을 사용하였다. 제안된 scheme은 Weil 쌍이나 Tate 쌍에서 구현될 수 있는 겹선형 쌍에 기반 한다.

참고문헌

[1] S.Al-Riyami and K.Paterson, "Certificateless Public Key Cryptography", available at

http://www.ime.usp.br/~rt/cranalysis/CertifLessPKC.pdf, Jul.2003.
[2] D.Boneh and M.Franklin, "Identity-Based Encryption from the Weil Pairing", CRYPTO2001, LNCS 2139, pp.213-229, Springer-Verlag, 2001.
[3] S.Bellovin and M.Merritt, "Encrypted Key Exchange: Password-based Protocols Secure against Dictionary Attacks", Proc.IEEE Symposium on Research in Security and Privacy, May 1992.
[4] S.Bellovin and M.Merritt, "Augmented Encrypted Key Exchange: A Password-based Protocol Secure Against Dictionary Attacks and Password File Compromise", Technical Report, AT&T Bell Laboratories, 1994.
[5] J.Baek and Y.Zheng, "Identity-Based Threshold Decryption", IACR eprint, 2003/164.
[6] W.Ford and B.Kaliski, "Server-Assisted Generation of a Strong Secret from a Password", Proc.9th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprise, IEEE, Jun.14-16, 2000.
[7] F.Hess, "Efficient Identity Based Signature Schemes Based on Pairings", SAC2002, LNCS 2595, pp.310-324, Springer-Verlag, 2003.
[8] D.Jablon, "Strong Password-Only Authenticated Key Exchange", ACM Computer Communications Review, Oct.1996.
[9] D.Jablon, "Password Authentication Using Multiple Servers", CT-RSA2001, LNCS 2020, pp.344-360, Springer-Verlag, 2001.
[10] B.Libert and J.Quisquater, "Efficient revocation and threshold pairing based cryptosystems", PODC'03, pp.163-171, Jul.13-16, 2003.
[11] P.MacKenzie, T.Shirmpton and M.Jakobsson, "Threshold Password-Authenticated Key Exchange (Extended Abstract)", CRYPTO2002, LNCS 2442, pp.385-400, Springer-Verlag, 2002.
[12] T.Pedersen, "Non-interactive and Information theoretic Secure Verifiable Secret Sharing", CRYPTO'91, LNCS 576, pp.129-140, Springer-Verlag, 1992.
[13] R.Perlman and C.Kaufman, "Secure Password-Based Protocol for Downing a Private Key", Proc. 1999 Network and Distributed System Security Symposium, Internet Society, Jan.1999.
[14] A.Shamir, "How to Share a Secret", Communication of the ACM, Vol.22, No.11, pp.612-613, Nov.1979.
[15] D.Vo, F.Zhang and K.Kim "A New Threshold Blind Signature Scheme from Pairings", SCIS2003, Vol.1/2, pp.233-238, Jan.2003.
[16] T.Wu, "The Secure Remote Password Protocol", Proc. 1998 Network and Distributed System Security Symposium, pp.97-111, Internet Society, Jan.1998.