증명가능한 비밀 분산 기법을 이용한 변형된 SE-PKI 키 복구 시스템

이용호, 이임영
순천향대학교 정보기술공학부

Modified SE-PKI Key Recovery System using the Verifiable Secret Sharing scheme

Yong-Ho Lee, Im-Yeong Lee
Division of Information Technology Engineering, Soonchunhyang University

요 약

정보보호를 위한 공개키 기반 구조의 구축은 사용자들에게 많은 이점을 줄 수 있다. 그러나 암호 키의 분실이나 불법적인 사용등의 문제점을 내포하고 있다. 이러한 문제점을 해결할 수 있는 기술로서 공개키 기반 구조와 연동 가능한 키 복구 기술이 있으며, 현재 많은 연구가 진행중에 있다. 기존에 제안되어 있는 방식은 인증기관에게 저장공간을 요구하거나, 인증기관과 위탁기관간의 통신량이 증가하는 문제점을 가지고 있다. 본 논문에서는 이러한 문제점을 지적하고, 이를 해결하는 변형된 SE-PKI 키 복구 시스템을 제안한다.

1. 서론

암호의 사용은 사용자의 정보에 대해 기밀성, 무결성, 인증 등의 정보보호 서비스를 제공해 줌으로써 전자상거래에서 결제등을 가능하게 하고 있다. 이러한 암호의 사용은 우리의 생활을 윤택하게 하는 기능을 가지고 있다. 그러나 이것의 오·남용은 많은 문제점들을 발생시킬 수 있다. 이러한 문제점을 해결하기 위해서는 다음과 같은 요구사항을 만족하는 키 복구 시스템이 요구된다.

- 범죄 수사 등의 합법적인 키 접근 필요성이 있을 경우 적절한 시기에 사용자의 암호문을 복구할 수 있어야 한다.
- 키의 분실이나 손상으로 인해 사용자가 자신의 정보에 접근할 수 없을 경우, 이를 해결해 줄 수 있어야 한다.
- 정당한 키 복구 시스템을 이용하여 부당한 방법으로 키 복구 기능을 우회하면서 비밀 통신을 할 수 없도록 해야 한다.

위에서 알아본 바와 같이 키 복구 시스템은 암호의 오·남용을 해결할 수 있는 방법이다. 그러나 이러한 키 복구 시스템을 현재의 사용자 환경에 도입하기에는 많은 무리가 따르게 된다.

이러한 문제점은 현재 각 나라에서 정보화의 활성화를 위해 구축하고 있는 공개키 기반 구조를 이용하여 해결할 수 있다. 현재 이러한 공개 키 기반 구조에 키 복구 시스템을 도입하는 연구가 다양하게 진행되고 있다.

본 논문에서는 1998년 A. Young등이 제안한 Auto-Recoverable Auto-Certifiable Cryptosystems[1]와 1999년 P. Paillier등이 제안한 Self-Escrowed Public Key Infrastructure[2] 마지막으로 2001년 유희종등이 제안한 다수의 위탁 기관 참여가 가능한 SE-PKI 키 복구 시스템[3]의 문제점들을 알아보고, 이들의 문제점을 해결할 수 있는 변형된 SE-PKI 키 복구 시스템을 제안한다.

2. 기존 방식 분석

본 장에서는 기존에 제안된 방식들을 알아보고 이들의 문제점에 대해 분석해 본다.

2.1 ARC (Auto-Recoverable Auto-Certifiable Cryptosystem)

1998년 A. Young과 M. Yung은 공개키 기반 구조

본 연구는 2001년도 순천향대학교 대학자체 학술연구조성비 지원에 의한 것임

를 이용하여 다수의 위탁 기관이 참여 가능한 키 복구 시스템(ARC)을 제안하였다[1].

2.1.1 시스템 설정

ARC는 키 복구 시스템을 수행하는데 필요한 함수들을 미리 정의하고 있으며, 그 내용은 다음과 같다.

- GEN(poly-time probabilistic Turing Machine)
  - 입력 : 없음, 출력 : (K_1, K_2, P)
  - K_1 : 공개키, K_2 : 비밀키
  - P : 위탁 기관에 의해 K_2가 복구 가능하다는 것을 증명하는 증명서
- VER(poly-time deterministic Turing Machine)
  - 입력 : (K_1, P), 출력 : boolean value
  - P를 이용해 비밀키 K_2가 복구 가능하면 True
- REC(deterministic Turing Machine with a private input)
  - REC_i : REC의 분산된 개체, $1 \le i \le m$
  - 입력 : P, 출력 : k_2의 부분정보 i
  - Turing Machine REC_i들은 협력하여 K_2 복구

2.1.2 수행 과정

ARC는 다음과 같은 과정을 통하여 키 복구를 수행한다.

(1) 사용자는 GEN을 이용해 (K_1, K_2, P)를 생성하고, (K_1, P)를 CA에게 전달한다.
(2) CA는 VER(K_1, P)를 계산하고 K_1에 해당하는 인증서를 생성한다.
(3) EA_i(escrow authorities)는 REC_i(P)에 의해 K_2의 부분정보 i를 계산한다.
(4) 비밀정보를 합쳐 비밀키를 복구한다.

2.1.3 ARC의 문제점 분석

이 방식은 사용자의 비밀키가 위탁기관의 공개키를 이용하여 생성되었음을 증명하는 증명서를 공개키 인증서와 함께 저장해야 하는 저장 공간이 요구된다. 이는 사용자의 개인키를 복구할 때 이 증명서를 이용하기 때문이다. 또한 이러한 문제점 때문에 위탁기관과 인증기관 사이의 통신이 증가한다는 단점도 가지고 있다.

2.2 SE-PKI (Self-Escrowed Public Key Infrastructure)

1999년 P. Paillier와 M. Yung는 ARC의 저장공간 요구와 통신량이 증가되는 문제를 해결하는 SE-PKI 키 복구 시스템을 제안하였다[2].

2.2.1 시스템 설정

SE-PKI는 키 복구 시스템을 수행하는데 필요한 함수들을 미리 정의하고 있으며, 그 내용은 다음과 같다.

- S = <G, E, D>
  - 사용자의 키 생성 알고리즘, 암/복호 알고리즘
  - G는 사용자의 공개/비밀키 (y, x)를 생성
- S′ = <G′, E′, D′>
  - 위탁기관의 마스터 키 생성 알고리즘, 암/복호 알고리즘
  - G′는 위탁기관의 공개/개인키 (Y, X)를 생성
- (y, x)와 (Y, X)는 다음을 만족한다.
  - $y = E'_Y(x)$, $x = D'_X(y)$
- P(Y, x, y)
  - 복구 가능성 검증값으로 복구 가능하면 True

2.2.2 수행 과정

SE-PKI는 다음과 같은 과정을 통하여 키 복구를 수행한다.

(1) 위탁기관은 G′를 이용해 (Y, X)를 생성하고, Y와 CA의 파라메터를 공개한다.
(2) 각 사용자는 $G(Y, 1^k)$를 이용해 $y=E'_Y(x)$을 만족하는 (y, x)를 생성하고, P(Y, x, y)를 이용해 P를 생성한다. 사용자는 (y, P)를 CA에게 전송한다.
(3) CA는 V(Y, y, P)=True인지 확인하고 y에 서명을 붙여 디렉토리에 공개한다.
(4) 수신자의 y를 받아 E를 이용해 메시지를 암호화하고 송신자에게 전송한다.
(5) 송신자는 x를 이용해 D를 수행한다.
(6) 위탁기관은 다음을 이용하여 사용자의 비밀키를 획득한다. $x=D'_X(y)$

2.2.3 SE-PKI의 문제점 분석

이 방식은 ARC에서 요구되었던 저장 공간이 필요없는 새로운 방식을 제안하였고, 이와 더불어 키 복구시 위탁기관과 인증기관 사이의 통신도 감소시키는 이점을 얻었다. 그러나 이 방식은 사용자의 비밀키를 복구할 수 있는 위탁기관의 비밀 정보가 하나의 위탁기관에만 집중되어 있기 때문에 사용자의 프라이버시 침해라는 키 복구 시스템 본래의 논쟁점을 가져오고 있다.

2.3 다수의 위탁기관 참여가 가능한 SE-PKI 키 복구 시스템

2001년 유희종, 최희봉, 오수현, 원동호는 SE-PKI 키 복구 시스템에서 사용자의 비밀 정보가 단일 위탁기관에 저장된다는 문제점을 해결하기 위해 다수의 위탁 기관 참여가 가능한 SE-PKI 키 복구 시스템을 제안하였다[3].

2.3.1 시스템 설정

이 과정은 위탁기관들과 신뢰된 제 3자 간에 이루어지며, 소수 생성 단계, 공개키의 계산 단계, 마스터 개인키의 분산 단계로 나누어진다.

(1) 소수 생성 단계

이 단계에서는 Trial Division 방법을 사용하여 공개키 n을 구성하는 수들이 소수인지를 검사한다.

(2) 공개키의 계산 단계

- 위탁기관 A는 n보다 큰 임의의 소수 p와 c_a, $d_a \in Z_p^*$를 선택하고 $x_a = 1$, $x_b = 2$, $x_h = 3$을 설정

하여 $p_{ai} = c_a x_i + p_a$와 $q_{ai} = d_a x_i + q_a$를 계산한 후, p_{ba}, q_{ba}, 와 $r(0) = 0$, $r_i = r(x_i)$인 임의의 이차 다항식 $r(x)$를 선택하여 $Na = (p_{aa} + p_{ba})(q_{aa} + q_{ba}) + r_a$를 계산한다. p_{ab}, q_{ab}, p_{ba}, q_{ba}, r_b를 위탁기관 B에게 p_{ah}, q_{ah}, r_h, N_a를 제 3자 H에게 전송한다.

- 위탁기관 B는 $c_b = (p_{ba} - p_b)/x_a$, $d_b = (q_{ba} - q_b)/x_b$, $p_{bi} = c_b x_i + p_b$, $q_{bi} = d_b x_i + q_b$를 계산한 후, $N_b = (p_{ab} + p_{bb})(q_{ab} + q_{bb}) + r_b$를 계산해 p_{bh}, q_{bh}, N_b를 제 3자 H에게 전송한다.
- 제 3자 H는 $N_h = (p_{ah} + p_{bh})(q_{ah} + q_{bh}) + r_h$와 (x_a, N_a), (x_b, N_b), (x_h, N_h)를 지나는 이차 다항식 $\alpha(x)$를 계산한 후, $\alpha(0)$를 구한다. 여기서 $\alpha(0) = n$이다. H는 계산된 n값을 공개한다.

(4) 마스터 개인키의 분산 단계

위탁기관 A와 B는 아래와 같이 마스터개인키 φ_a와 φ_b를 각각 나누어 갖는다.

- $n = pq = (p_a + p_b)(q_a + q_b)$
- $\varphi(n) = (n - p_a - q_a) - (p_b + q_b)$
- 위탁기관 A의 개인키 : $\varphi_a = n - p_a - q_a$
- 위탁기관 B의 개인키 : $\varphi_b = - (p_b + q_b)$

2.3.2 수행 과정

이 과정은 암/복호 단계와 키 복구 단계로 나누어진다. 여기서, 암/복호와 키 복구는 SE-PKI[2]에서 소개된 SE ElGamal/Paillier Encryption Scheme을 이용해 이루어진다.

2.3.3 다수의 위탁기관 참여가 가능한 SE-PKI 키 복구 시스템의 문제점 분석

이 방식은 위에서 분석했던 ARC와 SE-PKI의 문제점들을 해결하고 있으나, 시스템 설정 과정 중 공개키 계산 단계에서 커다란 문제점을 가지고 있다.

공개키 계산 단계에서 가정했던 사항과 각 기관이 알고 있는 정보를 이용하면 다양한 공격이 가능하다.

우선, 위탁기관 B와 제 3자 H가 공모를 한다고 가정하자. 위탁기관 B와 제 3자 H의 정보를 이용하면 다음과 같은 식을 얻을 수 있다.

$$p_{ab} = 2c_a + p_a \quad (1)$$
$$p_{ah} = 3c_a + p_a \quad (2)$$
$$q_{ab} = 2d_a + q_a \quad (3)$$
$$q_{ah} = 3d_a + q_a \quad (4)$$

- (2)에서 (1)을 뺀다. 결과는 다음과 같다.
  : $c_a = p_{ah} - p_{ab}$ (a)
- (a)와 (2)를 이용하여 p_a를 구한다.
  : $p_a = 3p_{ab} - 2p_{ah}$ (b)
- 같은 방식으로 q_a를 구한다.
  : $q_a = 3q_{ab} - 2q_{ah}$ (c)
- p_a와 q_a를 이용하여 위탁기관 A의 개인키를 유도한다.
  : $\varphi'_a = n - p_a - q_a$

위탁기관 B가 φ'_a를 이용하면, 위탁기관 A의 도움없이 사용자의 키를 복구할 수 있다. 마찬가지로 위탁기관 A와 제 3자 H가 공모를 할 경우, 위탁기관 B의 개인키를 유도할 수 있다.

3. 제안 방식

본 논문에서는 공개키 기반 구조를 이용하는 기존의 키 복구 시스템들의 문제점들을 지적하였다. 본 장에서는 상기 방식들의 문제점들을 해결하면서 공개키 기반 구조에 적용 가능한 키 복구 시스템을 제안한다.

본 제안 방식은 공개키 기반 구조가 구축되어 사용자들이 서비스를 제공받고 있다는 전제하에서 진행한다.

3.1 시스템 계수

다음은 본 방식에서 사용되는 시스템 계수 및 구성요소를 기술하고 있다.

- p, q : 임의의 큰 소수
- λ : 사용자의 비밀키 복구 정보
- α : 위탁기관이 옳은 키 위탁 정보를 가지고 있음을 확인하는 파라미터
- t_i : 사용자의 비밀키 복구 정보에 대한 i번째 위탁기관의 위탁 정보를 계산하기 위해 사용되는 공개 정보
- f_i : VSS 기법에서 생성되는 다항식의 계수
- EA_i : 사용자가 신뢰하는 위탁기관
- (x, y) : 키 복구를 지원하는 암호화 통신에 사용되는 사용자의 세션키 쌍
- e : ElGamal 암호 프로토콜에서 사용되는 난수

3.2 시스템 프로토콜

3.2.1 키 복구 정보 생성 및 위탁 과정

사용자는 키 복구 정보를 생성한 후, (k, n) threshold VSS(Verifiable Secret Sharing) scheme[4][5]을 이용하여 n개의 위탁기관에 위탁한다.

(1) 사용자는 p, q를 생성하여 $n = pq$와 $g \in Z^*_{n^2}$를 계산한 후 인증기관을 통해 안전하게 공개한다.

(2) 사용자 A는 $\lambda = \mathrm{lcm}(p-1)(q-1)$와 $\alpha = g^{\lambda} \bmod n$을 계산한다.

(3) 사용자는 $f_i \in Z_n$ 인 k개의 난수를 선택하여 다음과 같은 k-1차 다항식을 만들고 계수에 대한 증거값 $(g^{f_i})_{i=0,\ldots,k-1}$을 인증기관을 통해 안전하게 공개한다.
: $f(x) = f_0 + f_1 x + f_2 x^2 + \ldots + f_{k-1} x^{k-1}$, $f_0 = f(0) = \lambda$

(4) 사용자는 공개정보 t_i를 이용하여 $\lambda_i = f(t_i)$를 계산하고, 그 값을 i번째 위탁기관에 안전하게 전송한다.

(5) 각 위탁기관 EA_i는 $\alpha_i = g^{\lambda_i} \bmod n$을 계산하여 인증기관을 통해 안전하게 공개한다.

(6) 키 복구 기관 및 임의의 제 3자는 다음의 식을 통해 각 위탁기관이 옳은 키 위탁 정보를 가지고 있음을 확인한다. 만약 값이 옳지 않을 경우 처음부터 다시 시작한다. α_i는 키 복구 과정에

서 사용되므로 잘 보관해 둔다.

: $\alpha = g^{\lambda 0}$, $\alpha_i = \Pi_{j=0}^{k-1} (g^{f_i})x_i^j$

3.2.2 암/복호화 과정

사용자들은 ElGamal 암호 알고리즘을 이용하여 암/복호화 과정을 수행한다.

(1) 사용자 x<n를 만족하는 x를 선택하고, $y = g^x \bmod n^2$을 계산한다. 이때 (x, y)는 사용자의 비밀/공개키 쌍이 된다.

(2) 사용자 A는 $m<n^2$를 만족하는 평문 m을 다음과 같이 암호화한다.

: 암호문 $c = (my^e, g^e)$, $e<2^{2|n|}$

(3) 수신자가 받은 암호문 c를 (a, b)라고 했을 때, 다음과 같이 복호화 한다.

: $m = a/b^x \bmod n^2$

3.2.3 키 복구 과정

키 복구 기관은 키 위탁 기관들과 협조하여 사용자의 키 복구 정보 λ를 계산한 후, SE-PKI에 제안되어 있는 Paillier's Deterministic Encryption Scheme[2]을 이용하여 사용자의 비밀키를 복구한다.

(1) 키 복구 기관은 공개 정보 t_i를 사용하여 다음 값을 계산한다.

: $a_i = \Pi \frac{t_m}{t_m - t_i}$

(2) 키 복구 기관은 α_i와 a_i를 이용하여 Lagrange 보간 다항식을 이용하여 다음과 같이 키 복구 정보 λ를 복구한다.

: $\lambda = \sum_{i=1}^{k} a_i \lambda_i$

(3) 키 복구 기관은 λ와 Paillier's Deterministic Encryption Scheme을 이용하여 다음과 같이 사용자의 비밀키를 복구한다.

: $x = \frac{L(y^\lambda \bmod n^2)}{L(g^\lambda \bmod n^2)} \bmod n$

3.3 제안 방식 분석 및 비교

3.3.1 ARC의 문제점 해결

제안 방식에서는 인증기관이 공개정보를 저장하고는 있으나, 단지 임의의 제 3자가 확인만 하는 것으로써 통신량의 증가는 없으며, 제 3자의 수정등 불법 행위를 방지하는 역할을 수행한다.

3.3.2 SE-PKI의 문제점 해결

제안 방식에서는 증명가능한 비밀 분산 기법을 적용하여 다수의 위탁기관 참여 뿐만아니라, 사용자가 신뢰하는 위탁기관을 선택할 수 있는 서비스를 제공한다.

3.3.3 다수의 위탁기관 참여가 가능한 SE-PKI 키 복구 시스템의 문제점 해결

제안 방식에서는 키 복구 정보를 사용자가 생성하고, 증명가능한 비밀 분산 기법을 적용하여 위탁기관에 전달함으로서, 위 방식에서 발생하는 문제점을 근본적으로 해결하고 있다.

3.4 각 방식별 비교 분석

다음은 공개키 기반 구조에 적용 가능한 키 복구 시스템의 요구 사항에 기초하여 기존 방식과 제안 방식을 비교 분석한 결과이다.

표1. 각 방식별 비교 분석

대상 / 항목	ARC	SE PKI	SE PKI 개선	제안 방식
인증기관의 추가지연 통신량	많음	없음	없음	없음
시스템의 안전성	O	O	X	O
시스템의 효율성	X	X	X	O
위탁기관 선택유무	X	X	X	O
위탁기관의 부정 및 공모	불가능	불가능	가능	불가능
키 복구시 필요한 위탁기관 수	참여 위탁기관 전체	1	참여 위탁기관 전체	n개중 k개

4. 결론

암호 사용의 증가와 함께 오·남용에 따른 부작용 또한 증가하고 있다. 이러한 부작용을 해결하기 위한 기술로써 키 복구 시스템이 연구되고 있으나 현재의 암호 사용자 환경에 도입하기에는 많은 문제점을 가지고 있다. 최근 이러한 문제점을 해결하기 위해 공개키 기반 구조를 이용하려는 연구가 진행중에 있다.

본 논문에서는 PKI와 연동가능한 키 복구 시스템으로 제안된 ARC와 SE-PKI 키 복구 시스템 그리고 다수의 위탁 기관 참여가 가능한 SE-PKI 키 복구 시스템에 대하여 고찰하였다. 또한 기존 방식의 문제점을 해결하는 새로운 키 복구 시스템을 제안함으로써 향후 공개키 기반 구조하에서 필수적으로 제공되야 할 키 복구 서비스에 대한 방향을 제시할 수 있으리라 기대된다.

[참고문헌]

[1] A. Young, M. Yung, "Auto-Recoverable Auto-Certifiable Cryptosystmes", Advanced in Cryptology-Eurocrypto'98, Springer-Verlag, pp.17-31, 1998

[2] P. Paillier, Moti Yung, "Self-Escrowed Public Key Infrastructures", Proceedings of ICISC'99, 1999

[3] 유희종, 최희봉, 오수현, 원동호, "다수의 위탁 기관 참여가 가능한 SE-PKI 키 복구 시스템", 통신정보보호학회논문지, 제 11권, 제 1호, 2001

[4] T.P.Pedersen, "Distributed provers with application to undeniable signatures", Advances in Cryptology-Eurocrypt'91, pp.222-242, 1991

[5] 김종흠, 심상규, 이필중, "안전하고 공정한 키 위탁 시스템의 제안", 한국통신정보보호학회 종합학술발표회 논문집, Vol.10, No.1, 2001

[6] 이임영, 이재광, 소우영, 최용락, "컴퓨터 통신 보안", 도서출판 그린, 2001

[7] 최용락, 소우영, 이재광, 이임영, "통신망 정보 보호", 도서출판 그린, 1996