Strong Key Insulation을 제공하는 Certificate-less 공개키 암호 시스템*

한상윤[1], 염대현[2], 황용호[2], 이필중[3]

포항공과대학교 정보통신대학원[1], 포항공대대학교 전자전기공학과[2,3]

{syhan, daehyun, yhhwang}@oberon.postech.ac.kr[1,2]

pjl@postech.ac.kr[3]

Certificate-less Public Key Cryptosystem with Strong Key Insulation

Sang Yun Han[1], Dae Hyun Yum[2], Yong Ho Hwang[2], Pil Joong Lee[3]

GSIT[1], Department of EEE[2,3], POSTECH

{syhan, daehyun, yhhwang}@oberon.postech.ac.kr[1,2]

pjl@postech.ac.kr[3]

요 약

S.S.Al-Riyami와 K.G.Paterson에 의해 제안된 Certificate-less 공개키 암호 시스템은 기존 공개키 암호 시스템이 가지는 인증서 관리의 불편함과 ID-based 암호 시스템이 가지는 Key Escrow문제를 동시에 해결해 주었다. 하지만 대부분의 공개키 암호 시스템과 마찬가지로 Certificate-less 공개키 암호 시스템 역시 비공개키의 노출에 대한 문제를 가지고 있다. 따라서 본 논문에서는 기존 Certificate-less 공개키 암호 시스템에 Strong Key Insulation을 제공함으로써 보다 안전한 암호 시스템을 제안한다. 또한 이 시스템은 기존 Key Insulated 공개키 암호 시스템에 비해 계산량을 줄임으로써 보다 효율적인 암호 시스템을 구축할 수 있다.

I. 서론

1984년 A.Shamir는 공개키 암호 시스템이 가지는 인증서 관리의 불편함을 근본적으로 제거할 수 있는 장점을 가지고 있는 ID-based 공개키 암호 시스템(ID-PKC)을 처음 제안하였다.[6] 그 이후 실제적인 ID-based 암호 시스템은 2001년 D.Boneh와 M.Franklin에 의해 제안되어 다양한 암호 시스템에 응용되고 있다.[1] 하지만 ID-PKC는 각 사용자의 비공개키를 PKG(Private Key Generator)가 생성해야 하기 때문에 Key Escrow에 대한 문제를 갖고 있었다. 이 문제를 개선하고자 S.S.Al-Riyami와 K.G.Paterson는 2003년 Certificate-less 공개키 암호 시스템(CL-PKC)을 제안하였다.[2] 이 방법은 마스터키(master key)를 가지고 있는 KGC(Key Generator Center)가 부분적 비공개키를 만들어서 사용자에게 주면 사용자는 자신만이 아는 정보와 결합시켜 실제 비공개키를 생성하게 된다.

공개키 암호 시스템에서 비공개키의 안전한 관리와 생성은 무엇보다도 중요한 요소이다. 실제로

* 본 연구는 대학 IT 연구센터 육성·지원사업과 교육부 두뇌 한국 21사업, Com^{2}MaC-KOSEF의 연구결과로 수행되었음.

사용자의 실수나 안전하지 못한 장치에서의 암호화 및 복호화 수행 과정 등을 통해서 비공개키 노출이 자주 일어나고 있다. 이 비공개키 노출에 대한 피해를 줄이고자 2002년에 Y.Dodis, J.Katz, S.Xu, M.Yung에 의해서 Key Insulated 공개키 암호 시스템(KI-PKC)이 제안되었다.[3][4][5] KI-PKC는 사용자의 비공개키를 Helper(스마트카드 등)의 도움을 받아서 생성하고 각 시간 구간(time period)마다 업데이트한다. 따라서 현재의 비공개키가 노출이 되어도 다른 시간 구간에의 비공개키의 안전성은 유지된다. 또한 KI-PKC에서 사용자의 비공개키와 Helper의 비밀정보(secret value) 모두 노출이 되지 않으면 비공개키의 안전성이 유지가 될 수 있는 것이 Strong KI-PKC이다.

따라서 본 논문에서는 CL-PKC가 제공해 주지 못한 비공개키의 노출에 대한 피해를 줄일 수 있는 Strong Key Insulation을 제공하는 Certificate-less 암호 시스템을 제안한다.

II. 본문

1. 정의

1) Admissible pairing

G_1과 G_2를 큰 소수 위수 q를 가지는 가환군이라고 하자. $G_1 \times G_1$에서 G_2로의 함수 $\hat{e}$이 다음과 같은 특징을 가질 때 admissible pairing이라고 한다.

- Bilinear : 모든 $P, Q \in G_1$ 와 $a, b \in Z$에 대해 $\hat{e}(aP,bP) = \hat{e}(P,Q)^{ab}$ 를 만족한다.
- Non-degenerate : $G_1 \times G_1$에 속하는 모든 원소를 G_2의 항등원으로 보내지 않는다.
- Computable : 임의의 $P, Q \in G_1$ 에 대해서 $\hat{e}(P,Q)$를 계산하는 효율적인 알고리즘이 존재한다.

일반적으로 소수 위수 q의 덧셈 군을 G_1이라 하고 동일한 위수 q의 곱셈 군을 G_2라 한다. G_1는 유한체 상의 타원곡선 위의 점으로 구성된 군의 부분 군이고 G_2는 관련된 유한체의 곱셈 군의 부분 군이다.

2) BDH(Bilinear Diffie-Hellman) parameter generator

Security parameter k에 polynomial한 시간 동안 소수 위수를 q를 가지는 G_1, G_2 그리고 admissible pairing $\hat{e}$를 출력하는 랜덤 알고리즘이다.

3) Bilinear Diffie-Hellman Assumption

Bilinear Diffie-Hellman Assumption은 G_1의 원소 P를 임의로 선택하고 Z_q 의 원소 a, b, c를 임의로 선택해서 aP, bP, cP가 주어졌을 때 $\hat{e}(P,P)^{abc}$를 계산하는 것이 어렵다는 가정이다.

2. 제안한 시스템

이 장에서는 Strong Key Insulation를 제공하는 Certificate-less 암호 시스템을 제안한다. 그림 1은 Boneh-Franklin의 시스템[1]에 기반을 둔 새로운 암호 시스템이다.

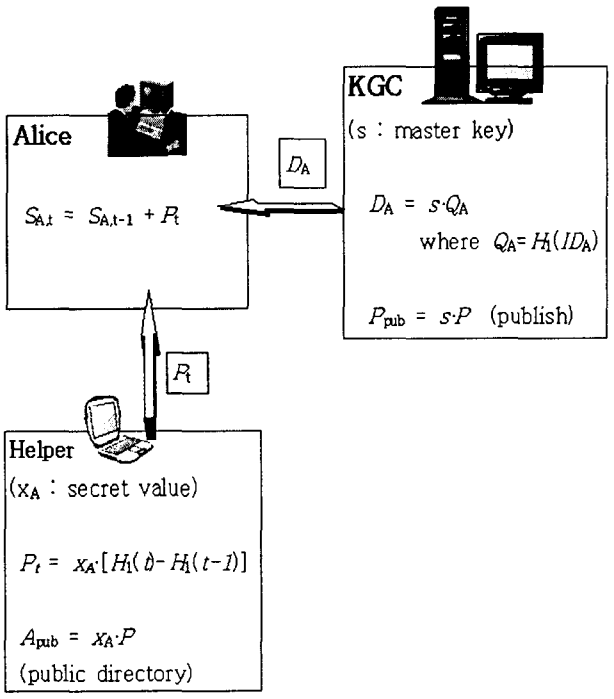

그림 1 CL-PKC with Strong Key Insulation

마스터키 s를 소유하고 있는 KGC는 사용자의 ID를 이용해서 각 사용자에 대한 부분적 비공개키

를 생성한다.

사용자 Alice는 각 시간 구간에 따라 Helper의 도움을 받아서 업데이트된 비공개키를 생성하게 된다.

다음은 제안한 암호 시스템의 각 단계에 대한 상세한 설명이다.

1) 시스템 파라미터 생성

KGC는 다음의 과정을 수행한다.

① BDH parameter generator에 security parameter k를 입력으로 받아 소수 위수 q를 가지는 G_1, G_2 그리고 $\hat{e}$를 생성한다.

② 임의의 생성원 P를 G_1에서 선택한다.

③ 임의의 s를 Z_q에서 선택한 후 $P_{pub} = s \cdot P$를 계산한다.

④ 다음과 같은 해쉬 함수 H_1, H_2를 선택한다.

$H_1 : \{0, 1\}^n \rightarrow G_1$

$H_2 : G_1 \rightarrow \{0, 1\}^n$

여기서 t는 전체 시간 N구간 중에 t번째 구간에 해당하며, 시스템 파라미터는 $<G_1, G_2, \hat{e}, q, P, P_{pub}, H_1, H_2>$이고, s는 KGC의 마스터키이다.

2) 부분적 비공개키 생성

KGC는 다음의 과정을 수행한다.

① Alice의 ID와 H_1을 이용해서 Q_A를 계산한다.

$$Q_A = H_1(ID_A)$$

여기서 ID_A는 Alice의 ID에 해당된다.

② KGC의 마스터키 s를 이용하여 부분적 비공개키 $D_A = s \cdot Q_A$를 구한다.

생성된 D_A를 KGC는 Alice에게 보낸다. Alice는 $\hat{e}(D_A, P) = \hat{e}(Q_A, P_{pub})$ 과정을 통해서 제대로 생성된 D_A임을 알 수 있다.

3) Helper의 비밀정보 생성

Helper는 임의의 x_A를 Z_q^*에서 선택한다. 여기서 x_A는 Helper의 비밀 정보가 된다.

4) 공개키 생성

Helper는 선택된 x_A를 이용하여 $A_{pub} = x_A \cdot P$를 계산하고 공개한다. 여기서 A_{pub}가 Alice의 키라는 확신(Authentication)을 보장하는 인증서가 필요하지 않다. 그러므로 A_{pub}는 누구나 접근 가능한 공개 디렉토리에 저장해 두면 된다.

5) Helper의 키 업데이트

Helper는 시간 구간 t에 따라 Alice의 비공개키 업데이트를 위해 자신의 키를 업데이트 해야 된다.

① t=0 일 때 $P_0 = x_A \cdot H_1(0)$가 된다.

② $1 \le t \le N$ 일 때 $P_t = x_A \cdot [H_1(t)-H_1(t-1)]$을 계산한다.

여기서 $H_1(t-1)$은 전 구간에서 이미 계산해 저장해 놓고 다음 구간에 사용할 수 있기 때문에 실제 계산은 $H_1(t)$만 계산하면 된다. 그리고 계산한 P_t는 Alice에게 안전하게 전달한다.

6) 비공개키 업데이트

Alice는 Helper에게 받은 P_t를 다음 과정을 통해서 t구간의 비공개키 $S_{A,t}$를 생성한다.

① t=0 일 때 $S_{A,0} = D_A + P_0$가 된다.

② $1 \le t \le N$ 일 때는 $S_{A,t} = S_{A,t-1} + P_t$를 계산한다.

7) 암호화

Alice에게 시간 구간 t에 평문 $M \in \{0, 1\}^n$을 암호화하여 보내기 위해서 다음과정을 수행한다.

① 임의의 r을 Z_q^*에서 선택한다.

② 다음과 같은 암호문 $C \in G_1 \times \{0, 1\}^n$를 전송한다.

$$C = [r \cdot P, M \oplus H_2(g^r)]$$

여기서 $g = \hat{e}(P_{pub}, Q_A) \cdot \hat{e}(A_{pub}, H_1(t))$ 이다.

8) 복호화

수신된 암호문을 $C=[U, V] \in G_1 \times \{0, 1\}^n$ 라고 하면, Alice는 다음과 같이 복호화한다.

$$M = V \oplus H_2[\hat{e}(U, S_{A,t})]$$

3. 계산량 비교

Alice가 시간 구간 t에서 비공개키를 업데이트 하기 위해서 Helper는 $H_1(t-1)$의 값을 이전 구간 $t-1$에서 저장하고 있으므로 전체 계산량은 해쉬 함수 한번, 스칼라 곱셈 한번, 덧셈 두번이 필요하다. 이것은 기존의 KI-PKC보다 효율적이다.[3][5]

만일 Alice에게 자주 보내게 될 경우에는 암호화 과정에서 $\hat{e}(P_{pub}, Q_A)$ 값을 미리 계산해 놓을 수 있기에 단지 pairing 과정이 한번만 필요하다. 복호화 과정 역시 한번의 pairing만 필요하다.

4. 안전성 분석

Bilinear Diffie-Hellman Assumption 하에 만든 본 시스템은 CL-PKC에 기반을 두고 있다. KGC가 부분적 비공개키를 생성하고 사용자가 자신만이 아는 비밀정보를 결합시켜 비공개키를 만들기 때문에 ID-PKC의 Key Escrow 문제를 해결할 수 있다.

일반적으로 Strong Key Insulation을 제공하는 시스템에 대한 공격에는 두 가지가 있다.[5] 하나는 사용자(Alice)에 대한 공격이고 다른 하나는 Helper에 대한 공격이 있다.

먼저 Alice에 대한 공격을 생각해 보자. 비공개키 업데이트 과정에서 $S_{A,t} = S_{A,t-1} + P_t = D_A + x_A \cdot H_1(t)$이므로 공격자가 Alice의 현재 시간 구간의 비공개키 값을 제외한 나머지 $N-1$개의 비공개키를 알아도 Helper의 비밀 정보 x_A를 알 수 없기에 현재 시간 구간의 비공개키를 알 수 없다.

또한, 공격자가 Helper의 비밀정보 x_A을 알 경우에 대해 생각해 보자. 비공개키의 업데이트 과정 $S_{A,t} = D_A + x_A \cdot H_1(t)$에서 Alice에 대한 단 하나의 비공개키도 알지 못하는 공격자는 어떤 시간 구간에서도 사용자의 비공개키를 알 수 없다. 따라서 본 시스템은 Strong Key Insulation을 제공한다.

III. 결론

대부분의 공개키 암호 시스템과 마찬가지로 CL-PKC 역시 비공개키 노출에 대한 문제를 가지고 있다. 본 논문에서는 기존 CL-PKC에 Strong Key Insulation을 제공함으로써 보다 안전한 암호 시스템을 제안하였고, 또한 이 시스템은 기존 KI-PKC에 비해 계산량을 줄임으로써 보다 효율적인 암호 시스템을 구축할 수 있을 것으로 기대된다.

참고문헌

[1] D.Boneh and M.Franklin, "Identity-based encryption from the Weil pairing," Crypto 2001, LNCS 2139, pp.213-229, 2001.

[2] S.S.Al-Riyami and K.G.Peterson, "Certificate -less public key cryptography," Asiacrypt 2003, LNCS, 2003.

[3] Y.Dodis, J.Katz, S.Xu and M.Yung, "Key-insulated public key cryptosystems," Eurocrypt 2002, LNCS 2332, pp.514-532, 2002.

[4] Y.Dodis, J.Katz, S.Xu and M.Yung, "Strong key-insulated signature schemes," PKC 2003, LNCS 2567, pp.130-144, 2003.

[5] M.Bellare and A.Palacio, "Protecting against key exposure: strong key-insulated encryption with optimal threshold," Cryptology ePrint archive 2002/064, http://eprint.iacr.org/, 2002.

[6] A.Shamir, "Identity-based cryptosystems and signature schemes," Crypto 1984, LNCS 196, pp.47-53, 1984.

[7] M.Bellare, A.Desai, D.Pointcheval, and P.Rogaway, "Relations among notions of security for public-key encryption schemes," Crypto 1998, LNCS 1462, pp.26-45, 1998.

[8] M.Girault, "Self-certified publick keys," Eurocrypt 1991, LNCS 547, pp.490-497, 1992.

[9] C.Gentry, "Certificate-based encryption and the certificate revocation problem," Eurocrypt 2003, LNCS 2656, pp.272-293, 2002.