다중 ID 기반 암호 스킴

박소영° 이상호
이화여자대학교 컴퓨터학과
soyoung°@ewhain.net, shlee@ewha.ac.kr

A Multiple IDs-Based Encryption Scheme

So-Young Park° Sang-Ho Lee
Dept. of Computer Science and Engineering, Ewha Womans University

요 약

유비쿼터스 환경의 도래와 함께, 사용자는 자신이 가입한 서비스별로 또는 사용자와 연관된 객체별로 서로 다른 ID(가명)를 사용할 수 있다. 기존의 ID 기반 암호 스킴은 하나의 ID에 하나의 독립된 복호키가 부여되기 때문에, ID의 개수가 증가하면 상대적으로 복호키의 개수도 증가한다. 그러나 ID 별로 별도의 복호키를 생성 관리하는 것은 비밀키의 유지 관리에 따른 효율서의 저하를 가져오므로, 서로 다른 ID를 사용하되, 하나의 복호키를 사용하여 ID를 이용한 정보의 기밀성을 제공할 수 있는 방법이 요구된다. 본 논문에서는 사용자가 복수의 ID를 생성하여 사용하되, 각각의 서로 다른 ID로 암호화된 암호문을 단 하나의 복호키를 이용하여 복호할 수 있는 새로운 pairing 기반 암호 스킴을 제안한다.

1. 서 론

Diffie-Hellman이 공개키의 개념을 처음 제시한 이후, 많은 인터넷 기반 보안 분야에서 공개키를 이용한 다양한 암호 시스템들이 개발되어 사용되고 있다. 그러나 공개키 기반 암호 시스템은 공개키 인증을 위한 인증서의 발행 및 인증서 관리에 따른 부가적인 연산을 필요로 하므로, 공개키 기반 암호 시스템의 보편화에 걸림돌이 되고 있다[1]. 1984년 Shamir[2]는 이름이나 메일 주소와 같은 일반적인 ID를 공개키로 사용하는 ID 기반 암호 스킴의 개념을 제시하였다. ID로 부터 공개키를 생성하여 사용하는 것은 공개키 인증에 따른 부가적인 절차를 필요로 하지 않으므로 기존의 공개키 암호 시스템이 갖는 인증서 관리에 따른 비효율성을 극복할 수 있다는 큰 장점을 가진다. 실제적인 ID 기반 암호 스킴은 2001년 Boneh 와 Franklin[3]에 의해 pairing을 이용한 ID 기반 암호 스킴이 처음 제안되었고, 이후 pairing을 이용한 다양한 암호 시스템들이 제안되었다[4-11]. 그러나 Boneh 와 Franklin에 의해 제안된 ID 기반 암호 스킴은 KGC(Key Generattion Center)가 각 사용자의 복호키를 생성하여 건네주므로, KGC에 의한 key escrow 문제를 갖는다.

위의 공개키 및 ID 기반 암호 스킴에서는 하나의 공개키에 대해서 단 하나의 유니크한 비밀키가 할당된다. 즉 공개키와 비밀키 사이에 1:1 매핑 관계가 성립한다. 그러나 인터넷 사용이 증가하고 유비쿼터스 환경의 도래와 함께, 사용자들은 ID를 이용하여 자신을 나타낼 기회를 많이 갖게 되고, 따라서, 자신이 가입한 서비스별로 또는 사용자와 연관된 객체별로 서로 다른 ID 또는 가명을 사용할 수 있다. 실제로 사용자들은 복수의 e-mail 주소를 사용하고 있으며, 웹 상에서 다수의 ID를 사용하여 자신을 나타낸다. 서로 다른 복수의 ID를 사용할 환경이 확대됨에 따라, 기존의 암호 시스템을 그대로 사용하는 경우, ID 증가에 따라 상응하는 비밀키의 개수도 증가하기 때문에, 비밀키 생성 및 유지·관리에 따른 부가적인 기능이 요구된다.

따라서, 본 논문에서는 다수의 서로 다른 ID를 생성하여 공개키로 사용하되, 각 ID에 의해 암호화된 암호문을 하나의 복호키를 사용하여 복호화할 수 있는 새로운 pairing 기반 암호 스킴을 제안한다. 사용자는 하나의 마스터 ID와 비밀키를 갖고, 이 마스터 ID를 이용하여 다양한 새로운 ID들을 생성하여, 생성된 ID들을 서비스 별로 또는 객체별로 자신의 공개키로 사용한다. 사용자는 자신의 마스터 ID에 대한 복호키를 생성하고, 이 복호키를 이용하여 각 ID에 의해 암호화된 암호문들을 복호화 한다. 제안된 스킴이 가지는 첫 번째 장점은 각 사용자는 자신의 ID개수에 상관없이 단 하나의 복호키만 유지하면 되므로, 복호키 생성 및 유지·관리에 따른 스토리지 및 신뢰기관과의 키 생성을 위한 연산 오버헤드를 줄일 수 있다. 두 번째는 각 사용자 스스로 자신의 ID를 생성할 수 있다. CA(Certificate Authority)와의 상호 인증 절차 없이 ID를 생성하되, 생성된 ID들은 CA에 의해 인증된 공개키로 사용될 수 있다는 장점을 갖는다.

제안된 스킴은 타원 곡선(elliptic curve)상에서의 Weil pairing과 같은 bilinear map[3]를 기반으로 하고 있으며, 기존의 ID 기반 암호 스킴이 가지는 key escrow 문제를 해결하기 위해 각 사용자는 자신의 비밀키, 공개키 쌍을 갖고 있고, 하나의 CA가 존재한다고 가정한다. 사용자가 선택한 비밀키를 사용하여 복호키를 생성할 수 있도록 하기 위해, Gentry의 CBE(Certificate-Based Encryption) 스킴[7,12]을 바탕으로 다중 ID 기반 암호 스킴을 설계한다.

2장에서 bilinear map에 대해 간략하게 설명하고, 3장에서 다중 ID 기반 암호 스킴에 대해 상세히 기술한다. 4장에서 제안한 스킴의 안전성 및 효율성을 분석하고 5장에서 결론을 맺는다.

2. Bilinear Map

Bilinear map은 Boneh 와 Franklin이 제안한 ID 기반 암호 스킴에서 처음으로 소개되었고, 주로 supersingular curve 상에서의 변형된 Weil pairing 또는 Tate pairing이 사용된다. 본 논문에서 제안하는 프로토콜도 Boneh 와 Franklin이 제시한 paring을 기반으로 하고 있으므로,

bilinear map에 대해서 간략하게 기술한다. G_1은 소수 q에 대해서 오더(order)가 q인 덧셈 그룹이고, G_2는 동일 위수를 갖는 곱셈 그룹이다. 제안한 스킴에서 사용하는 변형된(admissible) bilinear map $e: G_1 \times G_1 \rightarrow G_2$는 다음의 조건을 만족한다.

1. Bilinear : 모든 $Q, W, Z \in G_1$에 대해서, 다음의 조건을 만족하면, $e: G_1 \times G_1 \rightarrow G_2$는 bilinear 하다.

$$e(Q, W+Z) = e(Q, W)e(Q, Z).$$

따라서, 임의의 $a, b \in Z_q^*$에 대해서,

$$e(aQ, bW) = e(Q, W)^{ab} = e(abQ, W)$$

2. Non-degenerate : 그룹 G_1, G_2가 소수 오더를 갖는 그룹이기 때문에, 만약 P가 그룹 G_1의 생성자라면, $e(P, P)$는 그룹 G_2의 생성자이다.
3. Computable : 모든 $Q, W \in G_1$에 대해서, $e(Q, W)$를 계산하는 효율적인 알고리즘이 존재한다.

Pairing 기반 스킴의 안전성은 다음 문제의 어려움에 기인한다.

- Bilinear Diffie-Hellman Problem(BDHP) : 임의의 $a, b, c \in Z_q^*$ 대해서, $\langle P, aP, bP, cP \rangle$가 주어졌을 때, $e(P, P)^{abc} \in G_2$ 를 계산하는 문제이다.

3. 다중 ID 기반 암호화 스킴에 대한 설계

본 절에서는 사용자가 다수의 ID를 생성하고, 이를 이용하여 암호화 및 복호화 하는 과정에 대해서 상세하게 설명한다. 먼저, 하나의 CA가 존재한다고 가정한다. 사용자를 Alice라고 했을 때, Alice는 마스터 ID인 ID_{A0}와 자신이 임의로 선택한 비밀키 및 공개키 쌍 $(s_A, P_A = s_A P)$을 갖는다. 시스템은 총 t개의 시간 구간으로 구분되며, CA는 i번째 시간 구간에서 Alice의 공개키에 대한 인증서 $Cert_{Ai}$를 발행한다. 사용자는 자신의 비밀키와 CA로부터 받은 인증서를 이용하여 마스터 ID에 대한 복호키 D_{Ai}를 생성한다. 서로 다른 ID들이 공개키로 사용되는 객체(서비스 또는 사용자 등)를 $Object$로 표기하고, 총 n개의 객체가 있다고 가정한다. Alice는 임의의 객체 $Object_j$에 대해서 ID_{Aj}를 자신의 공개키로 사용한다. k는 안전성 파라미터 (security parameter)이고, IG는 BDH 파라미터 생성자이다.

제안한 프로토콜은 (Gen_{IBE}, Gen_{PKE}, Upd_{cert}, Upd_{dec}, Gen_{Pseud}, Enc, Dec)의 7가지 알고리즘으로 구성되며, 각 알고리즘의 상세 명세는 다음과 같다.

[다중 ID 기반 암호 프로토콜]

1. Gen_{IBE} : CA가 시스템 파라미터를 생성하는 과정은 다음과 같다.
   (a) 소수 q에 대해서, 오더가 q인 두 그룹 G_1, G_2와 변형된 bilinear map $e: G_1 \times G_1 \rightarrow G_2$를 생성하기 위해 k를 입력값으로 해서 IG를 실행한다.
   (b) 임의의 생성자 $P, P_1 \in G_1$을 선택한다.
   (c) 마스터 비밀키 $s_c \in Z_q^*$를 랜덤하게 선택하고, 공개키를 $P_c = s_c P$로 한다.
   (d) 암호학적 해쉬 함수를 다음과 같이 생성한다. 단, m은 평문의 비트 길이이다.

$$H_1: \{0,1\}^* \rightarrow Z_q^*,\ H_2: \{0,1\}^* \rightarrow G_1,$$
$$H_3: G_2 \rightarrow \{0,1\}^n,\ H_4: \{0,1\}^n \times \{0,1\}^n \rightarrow Z_q^*,$$
$$H_5: \{0,1\}^n \rightarrow \{0,1\}^n$$

   시스템 파라미터 $param = \{G_1, G_2, e, n, P, P_1, P_c, H_1, H_2, H_3, H_4, H_5\}$을 생성한다.
2. Gen_{PKE} : 사용자 Alice는 다음과 같이 자신의 마스터 ID와 비밀키 및 공개키 쌍을 생성한다.
   (a) 마스터 ID인 $ID_{A0} \in \{0,1\}^*$를 선택한 후, $Q_A = H_1(ID_{A0})P$로 둔다.
   (b) 비밀키 $s_A \in Z_q^*$를 랜덤하게 선택한 후, $P_A = s_A P$로 둔다.
   (c) (P_A, Q_A)를 CA에게 전송한다.
   (d) Alice는 마스터 ID인 ID_{A0}와 비밀키 s_A를 안전하게 유지·관리 한다.
3. Gen_{Pseud} : Alice는 객체 $Object_j$에 대한 ID_{Aj}를 다음과 같이 생성한다.
   (a) $Object_j$에 대해서 공개키로 사용하기를 원하는 ID인 $ID_{Aj} \in \{0,1\}^*$를 선택한다. 단, $j = 1, \ldots, n$이다.
   (b) $a_j = H_1(ID_{Aj}) / H_1(ID_{A0}) \bmod q$이고, $PK_{Aj} = (s_A / a_j)P$이며 $Com_{Aj} = s_A / a_j H_2(Object_j)$이다.
   (c) Alice는 $(ID_{Aj}, PK_{Aj}, Com_{Aj})$를 $Object_j$에 대한 공개키로 사용한다.
4. Upd_{cert} : 매 시간 구간 $i \geq 0$에서, CA는 Alice의 공개키 P_A에 대한 i번째 인증서를 다음과 같이 발행한다.
   (a) $P_{Ai} = H_2(i, P_c, e(Q_A, P_A))$를 계산한 후,
   (b) $Cert_{Ai} = s_c P_{Ai}$를 계산하여 Alice에게 전송한다.
5. Upd_{dec} : 매 시간 구간 $i \geq 0$에서, Alice는 복호키 D_{Ai}를 다음과 같이 생성한다.

$$D_{Ai} = Cert_{Ai} + s_A(ID_{A0})P_1$$

6. Enc : 매 시간 구간 $i \geq 0$에서, $Object_j$가 Alice의 공개키 (ID_{Aj}, PK_{Aj})를 사용하여 메시지 M에 대한 암호화 과정은 다음과 같다.
   (a) $Q_{Obj} = H_2(Object_j)$를 계산한 후, $e(PK_{Aj}, Q_{Obj}) = e(Com_{Aj}, P)$인지 검증 후, 맞으면 다음을 수행하고 그렇지 않으면 공개키를 거부한다.
   (b) $Q_{Aj} = H_1(ID_{Aj})P$, $S_{Aj} = H_1(ID_{Aj})PK_{Aj}$이고,
   (c) $P_{Ai} = H_2(i, P_c, e(Q_{Aj}, PK_{Aj}))$를 계산하여,

(d) $g = e(S_{Aj}, P_1)e(P_{Ai}, P_c)$를 계산한다.

(e) 랜덤 값 $\sigma \in \{0,1\}^n$를 선택한 후,

(f) $r = H_4(\sigma, M)$로 둔다.

(g) 암호문 $C = \langle U, V, T \rangle$는 다음과 같다.

$$C = \langle U, V, T \rangle = \langle rP, \sigma \oplus H_3(g^r), M \oplus H_5(\sigma) \rangle$$

7. Dec : Alice가 복호키 D_{Ai}를 이용하여 $Object_j$로부터 받은 암호문을 복호화 하는 과정은 다음과 같다.

(a) $V \oplus H_3(e(U, D_{Ai}) = \sigma'$를 계산하고,

(b) $T \oplus H_5(\sigma') = M'$를 계산한 후,

(c) $r' = H_4(\sigma', M')$로 하고, $U = r'P$가 성립하는지 체크한다. (만약 등식이 성립하지 않으면, 암호문을 reject 한다)

(d) M'을 평문으로 출력한다.

단, 여기서 $Q_{Obj_j}, Q_{Aj}, S_{Aj}, e(Q_A, P_A), e(Q_{Aj}, PK_{Aj})$와 $e(S_{Aj}, P_1)$은 전 시간 구간에서 동일하게 사용되는 값이므로, 매 시간 구간에서 이를 재계산해 줄 필요없이, 사전연산을 통해 연산에 대한 오버헤드를 줄일 수 있다.

4. 분석

본 절에서는 제안한 스킴에 대한 안전성을 분석한다. 제안한 스킴의 Enc와 Dec 알고리즘은 Fujisaki와 Okamoto 변환(transformation)[12]을 적용한 Gentry의 CBE 스킴을 따른다. Gentry는 CBE 스킴이 adaptive chosen ciphertext 공격에 안전함을 증명하였으므로[7], 제안한 스킴의 암호 알고리즘에 대한 안전성 증명은 생략한다. 제안한 스킴에서, 암호학적 해쉬 함수의 일방향성과 타원 곡선 상에서의 이산 대수 문제의 어려움에 의해 $Object_j$에 대한 공개키 (ID_{Aj}, PK_{Aj})로부터 Alice의 비밀키 및 마스터 ID를 알아낼 수 없다. 또한, (ID_{Aj}, PK_{Aj})를 알고 있더라도, Alice의 마스터 ID 및 비밀키에 대한 정보 없이는 임의의 ID'에 상응하는 (PK', Com')을 생성할 수 없으므로, 공격자는 유용한 다른 ID 쌍을 생성할 수 없다. CA는 주기적으로 P_{Ai}를 생성하여 Alice의 마스터 ID와 공개키에 대한 인증서를 발행하는데, CA가 생성하는 P_{Ai}에 포함되는 $e(Q_A, P_A)$와 각 $Object_j$에 대한 공개키 (ID_{Aj}, PK_{Aj})에 의해 계산되는 $e(Q_{Aj}, P_{Aj})$가 동일한 값을 가지므로, Alice는 모든 ID쌍에 대한 인증서를 따로따로 받을 필요없이, 마스터 ID와 공개키에 대한 인증서만으로 다른 ID 쌍에 대한 인증까지 수행할 수 있다. 따라서 공개키의 개수가 증가하더라도 인증서 발행 및 인증서 관리에 따른 연산은 증가하지 않으므로, 매우 효율적이다.

5. 결론 및 향후 연구 과제

본 논문에서는 pairing을 이용한 다중 ID 기반 암호 스킴을 새롭게 제안하였다. 제안된 스킴에서, 각 사용자는 다양한 복수의 ID들을 생성할 수 있고, 생성된 ID들은 다양한 암호 시스템에서 사용자의 공개키로 사용된다. 반면에 사용자는 ID의 개수와 상관없이 단 하나의 복호키만을 생성하여 유지·관리하고, 서로 다른 ID에 의해 암호화된 암호문들을 복호화 할 수 있다. 서로 다른 ID들에 대해서 동일한 하나의 복호키가 사용되기 때문에, 복호키의 유지·관리를 위한 안전성이 더욱 요구되는데. 이는 주기적인 복호키 갱신을 통해서 해결 가능하며, 기존의 ID 기반 암호 스킴에서 foward secrecy를 만족하는 비밀키 갱신 프로토콜[13]을 제안된 스킴에 적용시킴으로써 해결될 수도 있으나, 보다 효율적인 복호키 갱신 방안에 대한 연구가 향후 필요하다.

참고문헌

[1] P. Gutmann, "PKI: It's not Dead, Just Resting," IEEE Computer, vol. 35, no. 8, 2002, pp. 41-49.

[2] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes, Advances in Cryptology - Crypto'84, LNCS 0196, 1984, pp. 47-53.

[3] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," Advances in Cryptology - Crypto'01, LNCS 2139, 2001, 213.

[4] S. Al-Riyami and K. Paterson "Certificateless Public Key Cryptography," Advances in Cryptology - Asiacrypt'03, LNCS 2894, 2003, pp. 452-473.

[5] P. Barreto, H. Kim, B. Lynn and M. Scott, "Efficient Algorithms for Pairing-based Cryptosystems," Advances in Cryptology - Crypto'02, LNCS 2442, 2002, pp. 354-368.

[6] J. C. Cha and J. H. Cheon, "An Identity-Based Signature from Gap Diffie-Hellman Groups," Proc. of PKC'03, LNCS 2567, 2003, pp. 18-30.

[7] C. Gentry, "Certificate-Based Encryption and the Certificate Revocation Problem," Advances in Cryptology - Eurocrypt'03, LNCS 2656, 2003, pp. 272-293.

[8] F. Hess, "Efficient Identity-Based Signature Schemes based on Pairings," Proc. of SAC'02, LNCS 2595, 2003, pp. 310-324.

[9] B. Lee, C. Boyd, E. Dawson, K. Kim, J. Yang and S. Yoo, "Secure Key Issuing in ID-based Cryptography," Proc. of AISW'04, vol. 32, 2004.

[10] K. Paterson, "Cryptography from Pairings: A Snapshot of Current Research," Information Security Technical Report, vol. 7, no. 3, 2002, pp. 41-54.

[11] N. P. Smart, "An Identity-Based Authenticated Key Agreement Protocol based on the Weil Pairing," Electronic Letters, vol. 38, no. 13, 2002, pp. 630-632.

[12] E. Fujisaki and T. Okamoto, "Secure Integration of Asymmetric and Symmetric Encryption Schemes," Advances in Cryptology - Crypto'99, LNCS 1666, 1999, pp. 537-554.

[13] Y. Hanaoka, G. Hanaoka, J. Shikata and H. Imai, "Identity-Based Encryption with Non-Interactive Key Updates, 2004.