ID기반 암호시스템에서의 안전한 키생성 프로토콜

이병천, 양정모, 유승재

중부대학교 정보보호학과

Secure Key Issuing Protocol in ID-based Cryptography

Byoungcheon Lee, Jeongmo Yang, Seungjae Yoo

Department of Information Security, Joongbu University

요 약

ID기반 암호시스템은 인증서를 사용하지 않고 키의 사전분배가 필요 없는 등 여러 가지 장점을 가지고 있으나 키생성기관이 비밀키를 생성하여 사용자에게 제공하기 때문에 비밀키가 키생성기관에게 알려지고 그 결과로 기밀성과 인증성을 제공하기 어렵다는 단점이 있다. 그러므로 안전한 키생성 및 분배의 문제는 ID기반 암호시스템의 실용화를 위해 해결해야 할 매우 중요한 문제이다. 이런 문제를 해결하기 위하여 복수의 키생성기관을 사용하는 방법[2,6]이 제시되었는데 이것은 복수의 키생성기관이 모두 사용자 인증을 해야 하기 때문에 효율성면에서 바람직한 모델이 아니다. 사용자가 자신이 선택하는 비밀정보를 이용하여 키생성기관과의 상호작용을 통해 안전하게 키를 분배하는 모델[1,7]은 결과적으로 ID기반 암호시스템의 특성을 잃어버리게 되는 단점이 있다. 이 논문에서는 복수의 키생성기관을 이용하면서도 사용자 인증의 횟수를 1회로 줄일 수 있는 새로운 안전한 키생성 프로토콜을 제시한다.

I. 서론

전통적인 인증서 기반 공개키암호시스템에서 사용자는 인증기관으로부터 인증서를 발급받아 사용하게 되는데 여기서 중요한 이슈는 인증서 폐지 메커니즘을 운용하는데 많은 비용이 들고 복잡한 계층적 공개키기반구조(PKI)에서는 인증경로 검증에 많은 계산량이 필요하다는 것이다. 1984년 Shamir[10]에 의해 제안된 ID기반 암호시스템은 공개된 사용자정보를 직접 공개키로 사용할 수 있어서 인증과정이 필요 없는 장점이 있다. 반면 키생성기관이 비밀키를 생성하여 사용자에게 제공하기 때문에 비밀키가 키생성기관에게 알려지고 그 결과로 기밀성과 인증성을 제공하기 어렵다는 단점이 있다. 그러므로 안전한 키생성 문제는 ID기반 암호시스템의 실용화를 위해 해결해야 할 매우 중요한 문제이다. 최근 겹선형 암호시스템(pairing-based cryptography)[2,4,5]에 대한 연구가 활발하고 이를 ID기반 암호시스템에 적용하는 연구가 크게 증가하고 있는데 비밀키가 키생성기관에게 노출되지 않는 안전한 키생성 프로토콜이 제공된다면 ID기반 암호시스템의 실용화가 크게 진전될 것으로 예상된다.

이런 문제를 해결하기 위하여 복수의 키생성기관을 사용하는 방법[2,6], 사용자가 선택하는 비밀정보를 이용하여 사용자와 키생성기관간의 상호작용을 통해 안전하게 키를 분배하는 방법[1,7]이 제시되고 있다. 키생성기관의 비밀키를 비밀분산기법을 이용하여 복수의 신뢰기관에게 분산시키는 방법[2]과 사용자가 복수의 키생성기관으로부터 발급받은 비밀키들을 더하여 새로운 비밀키를 생성하는 방법[6]은 키의 노출을 방지할 수 있으나 복수의 신뢰기관이 독립적으로 사용자 신분인증을 해야 한다는 단점이 있다. 키생성에 있어서 사용자 신분인증 문제는 매우 중요하므로 사용자의 물리적인 출석을 요구할 수도 있겠는데 이런 경우 여러 번의 신분

인증을 해야 한다는 것은 큰 부담이 될 수 있다.

한편 Gentry[7]는 사용자가 자신이 선택하는 비밀정보를 이용하여 키생성기관과의 상호작용을 통해서 안전하게 키생성을 수행하는 방법을 제시하였는데 이것은 결국 인증서 기반의 암호시스템이 되어서 ID기반 암호시스템의 장점을 잃어버리게 된다. Al-Riyami[1]의 기법은 이를 새롭게 변형시켜 인증서가 필요 없는 키생성 기법을 제시하였으나 이것 또한 암시적 인증(implicit authentication)만을 제공하는 암호시스템이 되었다.

최근 Lee[8]는 하나의 키생성기관(KGC, key generation center)과 복수의 키비밀유지기관(KPA, key privacy agent)을 이용하여 사용자 신분인증은 KGC에 의해서 1회만 실시하는 새로운 키생성기법을 제시하였다. 그러나 이 방법에서는 KPA에 의한 모든 계산과정이 직렬적으로 이루어지도록 설계되어 계산적, 통신적 측면에서 단점이 있다. 본 논문에서는 비밀분산기법을 이용하여 병렬적 계산이 가능하도록 개선하여 효율성을 높였다.

본 논문의 구성은 다음과 같다. 2장에서는 새로운 안전한 키생성 프로토콜을 제시한다. 3장에서는 안전성을 분석하고 4장에서는 결론을 맺는다.

II. 새로운 안전한 키생성 프로토콜

본 논문에서는 하나의 키생성기관(KGC)과 n개의 키비밀유지기관(KPA)의 존재를 가정한다. KGC는 사용자의 키생성요청을 받아 사용자의 신분을 인증하고 자신이 서명한 부분키(partial key)를 생성하여 사용자에게 제공한다. n개의 KPA들은 비밀공유기법을 이용하여 어떤 비밀키 s_K를 공유하고 있으며 사용자의 요청을 받아 비밀유지서비스를 제공한다. 프로토콜 메시지들은 사용자가 선택한 비밀정보로 은닉되어 있으며 사용자는 자신만이 가지고 있는 비밀정보를 이용하여 비밀키를 계산해 낼 수 있게 된다.

이 논문에서는 겹선형성에 기반한 암호시스템을 사용한다. G_1은 위수 q를 갖는 덧셈군이라 하고 G_2는 같은 위수 q를 갖는 곱셈군이라 하자. P는 G_1의 생성자이며 겹선형쌍은 $e: G_1 \times G_1 \to G_2$로 표시된다고 하자. 여기에서는 다음과 같은 3개의 해쉬함수를 사용한다.

- $H_1: \{0,1\}^* \to G_1$ (ID 정보로부터 타원곡선상의 포인트를 추출하는데 사용)
- $H_2: G_2 \to \{0,1\}^l$ (여기서 l은 메시지 길이를 나타내며 메시지길이만큼의 해쉬값을 계산해낸다)
- $H_3: \{0,1\}^* \to Z_q^*$ (해쉬값으로 유한체상의 값을 출력)

겹선형암호계에 대한 자세한 내용은 [2,4]를 참조하자.

제안된 키생성 기법은 시스템 구성, 시스템 공개키 생성, 부분키 생성, 키비밀유지서비스, 비밀키 계산의 5개의 단계를 가진다.

Step 1. 시스템 구성 : KGC는 겹선형암호계 $G_1, G_2, P, q, e: G_1 \times G_1 \to G_2, H_1, H_2, H_3$를 생성하여 게시한다.

Step 2. 시스템 공개키 생성 : KGC는 자신의 비밀키 $s_0 \in Z_q^*$를 임의로 선택하고 공개키 $P_0 = s_0 P$를 계산하여 공지한다. n개의 KPA들은 t-out-of-n 비밀분산 프로토콜[9]을 이용하여 공유된 비밀키 s_K를 생성하며 그 결과로 각각의 KPA_i는 자신의 비밀공유값 s_i을 가지고 그에 해당하는 공개값 $P_i = s_i P$를 공개한다. 전체 KPA의 공개키 $P_K = s_K P$를 공개값 P_i들로부터 계산하여 공지한다. KGC는 시스템 공개키로 사용될 $Y = s_0 P_K = s_0 s_K P$를 계산하여 공지한다. 이것의 유효성은 다음과 같이 누구나 검증할 수 있다. $e(Y, P) = e(P_K, P_0)$.

Step 3. 부분키 생성 : 개인정보 ID를 갖는 사용자는 비밀정보 $x \in Z_q^*$를 임의로 선택한 후

$X = xP$를 계산한다. 비밀정보 x를 이용하여 (ID, X, KGC)에 대해 short signature[5]

$$Sig_x(ID, X, KGC) = xH_1(ID, X, KGC)$$

를 생성한다. 사용자는 KGC에게

$$\langle ID, X, Sig_x(ID, X, KGC)\rangle$$

를 보내고 부분키 생성을 요구한다. KGC는 다음의 과정을 통해 부분키를 사용자에게 제공한다.

① 사용자의 신분인증

② 사용자의 서명으로부터 비밀정보 x의 소유를 확인

③ 사용자의 공개키 생성

$$Q_{ID} = H_1(ID, KGC; KPA_1, \ldots, KPA_n)$$

④ 은닉된 부분키 생성

$$Q'_0 = H_3(P_0, X, s_0 X)s_0 Q_{ID}$$

⑤ 서명 생성

$$Sig_0(Q'_0, ID, X) = s_0 H_1(Q'_0, ID, X)$$

⑥ $\langle Q'_0, Sig_0(Q'_0, ID, X)\rangle$를 사용자에게 전송

사용자는 자신의 비밀정보 x를 이용하여

$$Q_0 = \frac{Q'_0}{H_3(P_0, X, xP_0)} = s_0 Q_{ID}$$

를 계산하고 이것의 유효성을 체크한다.

$$e(Q_0, P) = e(Q_{ID}, P_0)$$

Step 4. 키비밀유지서비스 : Q_0가 유효한 정보이면 사용자는 서명을 이용하여 다음과 같은 확인정보를 생성한다.

$$Sig_x(Q'_0, ID, X) = xH_1(Q'_0, ID, X)$$

사용자는

$$(ID, X, Sig_0(Q'_0, ID, X), Sig_x(Q'_0, ID, X))$$

의 정보를 n개의 KPA들에게 보내고 키비밀유지서비스를 요청한다. 각각의 KPA_i들은 다음의 과정을 통해 키비밀유지서비스를 제공한다.

① KGC의 서명 검증

② 사용자의 서명검증

③ $Q'_i = H_3(P_i, X, s_i X)$를 계산

④ 서명 계산

$$Sig_i(Q'_i, Q'_0, ID, X) = s_i H_1(Q'_i, Q'_0, ID, X)$$

⑤ $\langle Q'_i, Sig_i(Q'_i, Q'_0, ID, X)\rangle$를 사용자에게 전송

Step 5. 비밀키 계산 : 사용자는 각 KPA들로부터 $\langle Q'_i, Sig_i(Q'_i, Q'_0, ID, X)\rangle$를 받으면 다음의 과정을 통해 비밀키를 계산한다.

① KPA_i의 서명을 확인

② Q'_i의 은닉을 해제하여 Q_i를 계산

$$Q_i = \frac{Q'_i}{H_3(P_0, X, xP_0)H_3(P_i, X, xP_i)} \cdot s_i Q_0 \cdot s_0 s_i Q_{ID}$$

③ Q_i의 유효성 확인. $e(Q_i, P) = e(Q_0, P_i)$

④ 자신의 비밀키를 계산

$$D_{ID} = \sum_{i \in I} \delta_{i,I} Q_i = s_0 s_K Q_{ID}$$

여기서 $\delta_{i,I} = \prod_{j \in I, j \neq i} \frac{j}{j - i}$는 Lagrange 계수이고 I는 유효한 Q_i들의 집합이다.

⑤ 계산된 비밀키의 유효성 확인

$$e(D_{ID}, P) = e(Q_{ID}, Y)$$

여기서 n개의 Q_i들의 유효성을 확인하기 위해서는 2n개의 pairing 연산이 필요하다. 그런데 일괄검증(batch verification) 기법[3]을 이용하면 계산량을 크게 줄일 수 있다. 사용자는 20비트 정도의 작은 수 $(t_1, \ldots, t_n)$을 임의로 선택한 후 다음의 수식을 검증한다.

$$e(t_1Q_1+\cdots+t_nQ_n,P)=e(Q_0,t_1P_1+\cdots+t_nP_n)$$

이것을 위해서는 2개의 pairing 연산만이 필요한데 계산량을 n배 줄인 것이다. 이러한 일괄검증 기법에서 부정확한 $(Q_1,\ldots,Q_n)$이 위 검증과정을 통과할 확률은 $2^{-20}<10^{-6}$ 정도로 매우 작다.

III. 안전성 및 효율성 분석

n개의 KPA 중에서 적어도 t개 이상의 KPA가 정직하다면 사용자의 비밀키 D_{ID}는 노출되지 않는다. 비밀정보 x를 가지고 있는 정당한 사용자만이 은닉을 해제하여 비밀키를 계산해 낼 수 있다.

위 프로토콜에서 모든 메시지들은 사용자가 생성한 X값을 이용하여 은닉되어 있으므로 모든 프로토콜 메시지들은 공개게시판 등의 수단을 통해 공개될 수 있다. 이러한 공개적인 작업모델에서 KGC나 KPA들은 불법적인 행위를 하기 어렵다.

이러한 프로토콜을 통해 생성된 비밀키 D_{ID}는 공개키암호화, 전자서명, 키분배 등 기존의 ID기반 암호시스템에 그대로 사용될 수 있다.

제시된 기법에서는 사용자 인증을 KGC에 의해서 1회만 수행하기 때문에 기존의 기법[2,6]들에 비해 효율성이 크게 향상되었다. [8]과 비교하면 사용자와 KPA간의 프로토콜이 병렬적으로 이루어지므로 통신모델상 유리하고 일괄검증기법을 이용할 수 있어서 효율적이다.

IV. 결론

이 논문에서는 하나의 KGC와 n개의 KPA들을 이용하여 사용자가 ID기반 암호시스템의 비밀키를 안전하게 발급받을 수 있는 새로운 프로토콜을 제시하였다. KPA들은 KGC가 생성한 부분키에 대해 서명을 제공함으로써 사용자의 비밀키가 노출되지 않고 발급되도록 하는 역할을 한다.

이렇게 생성된 비밀키는 기존의 ID기반 암호시스템에 그대로 사용될 수 있으며 제안된 안전한 키생성 프로토콜은 ID기반 암호시스템의 실용화를 위한 중요한 핵심기술로 사용될 수 있다.

[참고문헌]

[1] S. Al-Riyami, K. Paterson, “Certificateless public key cryptography”, Advances in Cryptology - Asiacrypt'2003, LNCS 2894, Springer-Verlag. pp. 452-473, 2003.

[2] D. Boneh, and M. Franklin, “Identity-based encryption from the Weil pairing”, Advances in Cryptology - Crypto'2001, LNCS 2139, Springer-Verlag, pp. 213-229, 2001.

[3] M. Bellare, J. Garay and T. Rabin, “Fast Batch Verification for Modular Exponentiation and Digital Signatures”, Advances in Cryptology - Eurocrypt'98, LNCS 1403, Springer-Verlag, pp. 236-250, 1998.

[4] P. Barreto, H. Kim, B. Lynn, M. Scott, "Efficient algorithms for pairing-based cryptosystems", Advances in Cryptology -Crypto'2002, LNCS 2442, Springer-Verlag, pp. 354-368, 2002.

[5] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing", Advances in Cryptology - Asiacrypt'2001, LNCS 2248, Springer-Verlag, pp. 514-532, 2002.

[6] L. Chen, K. Harrison, N. P. Smart, D. Soldera, "Applications of multiple trust authorities in pairing-based cryptosystems", InfraSec 2002, LNCS 2437, Springer-Verlag, pp. 260-275, 2002.

[7] C. Gentry, "Certificate-based encryption and the certificate revocation problem" Advances in Cryptology - EUROCRPYT 2003, LNCS 2656, Springer-Verlag, pp. 272 - 293, 2003.

[8] B. Lee, C. Boyd, E. Dawson, K. Kim, J. Yang and S. Yoo, "Secure Key Issuing in ID-Based Cryptography", In ACSW Frontiers 2004 - Second Australasian Information Security Workshop (AISW2004), volume 26 of Australian Computer Science Communications, pp. 66-74. Australian Computer Society, January 2004.

[9] T. Pedersen, "A threshold cryptosystem without a trusted party", Advances in Cryptology - Eurocrypt'91, LNCS 547, Springer-Verlag, pp. 522-526, 1991.

[10] A. Shamir, "Identity based cryptosystems and signature schemes", Advances in Cryptology - Crypto'84, LNCS 196, Springer-Verlag, pp. 47-53, 1984.