효율적인 ID 기반의 Threshold 대리 서명

조원희° 박근수
서울대학교 전기, 컴퓨터 공학부
{whcho°, kpark}@theory.snu.ac.kr

Efficient Identity-based Threshold Proxy Signature

Wonhee Cho° Kunsoo Park
School of Computer Science & Engineering, Seoul National University

요 약

ID기반의 암호 시스템은 사용자의 ID를 공개키처럼 활용하는 시스템[1]이다. ID 기반 threshold 대리 서명(IDTPS)은 이러한 환경에서 사용 가능한 threshold 대리 서명 기법이며, Xu 등[2]에 의해 SOK-IBS[3]를 기반으로 처음 만들어졌다. 본 논문에서는 Cha-Cheon[4]의 서명 기법을 기반으로 하는 효율적인 ID 기반의 threshold 대리 서명을 제안한다. 여기서는 pairing 연산을 적게 사용하고 pairing에 사용되는 군으로 사상되는 해쉬 함수를 적게 사용하기 때문에 이전 기법보다 효율적이면서도 충분한 안전성을 보장하게 된다.

1. 서 론

1.1. 문제 제기

ID 기반의 암호 시스템[1][5]을 사용하는 환경에서, 한 기업의 내부 책임자와 같은 사람들은 자신의 책임하에 서명을 해야 하는 경우가 많다. 그런데 때로는 자신이 직접 서명할 수 없는 상황이지만, 자신의 권한으로 된 서명이 필요한 경우가 발생할 수 있다. 이 때, 자신의 서명 권한을 여러 명에게 나누어 준 뒤, 대리 권한을 받은 사람들 중 일정 수 이상이 서명할 때에만 자신의 서명을 대리하도록 한다면 이러한 문제를 해결할 수 있다.

1.2. 부분적인 문제 해결

이 문제를 해결하기 위해서는 여러 기법들을 사용해야 하는데, 여기에는 threshold 기법, 대리 서명, ID 기반 등이 있다. Shamir[6]에 의해 n명에게 정보를 분배한 뒤, 최소 t명이 참여하면 원래 정보를 복원할 수 있지만, t명 미만으로는 원래 정보를 복원할 수 없는 (t, n) threshold 기법이 소개되었다. 한편, 대리 서명은 Mambo 등[7]에 처음 소개되었으며, 전체 위임과 부분 위임 그리고 위임장에 의한 위임으로 분류된다. 특별히, 위임장에 의한 대리 서명에서, 위임장의 내용을 직접 삽입시킬 수 있는데, 이렇게 함으로써 대리인의 서명 오남용을 방지할 수 있다. 그 후 이 두 기법들을 이용하여 ID 기반의 암호 시스템에서 쓰일 수 있는 ID 기반의 threshold 서명 기법들[12][13]과 ID 기반의 대리 서명 기법들[11]이 만들어졌다. 이 외에도 threshold 대리 서명 기법들[10]이 제안되었지만, 이들 방법은 ID를 기반으로 하지 않는다.

1.3. 이전 연구

2004년 이 문제를 해결한 IDTPS 기법은 Xu 등[2]에 의해 처음으로 소개 되었는데, 이들은 기반이 되는 서명 기법으로 수정된 SOK-IBS 기법[3]을 사용한다. Xu 등의 IDTPS에서는 ID 기반의 암호 시스템 상에서 원서명자가 대리 서명의 권한을 n명에게 나누어 준 뒤, 위임장에 쓰여진 권한 내에서 t 명 이상의 대리 서명자들이 모여 원서명자를 대신하여 서명할 수 있다.

본 논문에서는 SOK-IBS보다 효율적인 Cha-Cheon의 서명 기법[4]을 기반으로 보다 효율적이면서도 충분한 안전성을 보장하는 ID 기반 Threshold 대리 서명 기법을 제안한다.

2. 배경 지식

2.1. Bilinear Map과 안전성의 기반 문제

본 논문에서 사용할 ID 기반 서명은 Pairing을 이용하고 있기 때문에, 이에 관계된 개념[5]을 먼저 살펴 본다.

G_1과 G_2를 큰 소수 q가 위수인 순환군이라 하자. 여기서 G_1은 덧셈군이며, G_2는 곱셈군이다.

■ bilinear map

함수 $e: G_1 \times G_1 \rightarrow G_2$에 대하여 다음 조건을 만족하는 map을 bilinear map 이라 한다.

- Bilinear: 모든 $P, Q \in G_1$ 와 모든 $a, b \in Z$ 에 대하여 $e(aP, bQ) = e(P, Q)^{ab}$ 가 성립.
- Non-degenerate: map은 $G_1 \times G_1$의 어떤 쌍이라도 G_2의 identity로 보내지 않는다.
- Computable: 어떤 $P, Q \in G_1$에 대해서도, $e(P, Q)$를 효율적으로 계산하는 알고리즘이 존재한다.

■ 안정성의 기반 문제

- 결정 Diffie-Hellman 문제(DDHP) : 주어진 그룹 내의 쌍인 P, aP, bP, cP에 대해 $c = ab$임을 결정하는 문제
- 계산 Diffie-Hellman 문제(CDHP) : 주어진 그룹 내의 쌍인 P, aP, bP에 대해 abP를 구하는 문제
- Bilinear Diffie-Hellman 문제(BDHP) : 주어진 그룹 내의 쌍인 P, aP, bP에 대해 bilinear map e를 이용하여 $e(P, P)^{abc}$를 구하는 문제

특별히, DDHP는 다항 시간 내에 풀 수 있지만, BDHP는 풀기 어려운 성질을 만족하는 군을 gap Diffie-Hellman 군(GDH 군)이라고 하며 Cha-Cheon의 서명에 사용되는 군이다.

2.2. Cha-Cheon의 ID 기반 서명 기법

본 논문에서 제시하는 기법은 Cha와 Cheon이 제안한 ID 기반 서명[4]에 기반하고 있다. 위수가 l인 GDH군의 생성원을 P라 하고 그 위에서의 bilinear map을 e라 할 때, 서명 기법은 네 단계로 이루어지며 그 과정은 다음과 같다.

1) 시스템 구성

난수 $s \in Z/l$ 을 생성하고, $P_{pub} = sP$ 를 계산한다. 다음과 같은 두 개의 충돌 회피 해쉬 함수를 사용한다.

$H_1 : \{0,1\}^* \rightarrow Z/l$, $H_2 : \{0,1\}^* \rightarrow G$

시스템 파라미터는 (P, P_{pub}, H_1, H_2)로 공개하며, 마스터키는 s를 사용한다.

2) 개인키 생성

주어진 ID에 대해, $D_{ID} = sH_2(ID)$를 계산하여 대응하는 ID의 사용자에게 발급한다. 이 때, $Q_{ID} = H_2(ID)$는 공개된 해쉬 함수를 이용하여 쉽게 계산할 수 있으며, 이 값이 공개키 역할을 하게 된다.

3) 서명 생성

서명자는 개인키 D_{ID}와 서명할 메시지 m이 있을 때, 난수 $r \in Z/l$을 선택한 뒤, 다음을 계산한다.

$U = rQ_{ID}$, $V = (r + H_1(m,U))D_{ID}$

m에 대한 서명은 $\sigma = (U,V)$이다.

4) 서명 검증

주어진 서명 $\sigma = (U,V)$에 대하여, e와 $h = H_1(m,U)$를 가지고, $(P, P_{pub}, U + hQ_{ID}, V)$가 타당한 Diffie-Hellman 쌍인지 확인한다. 이는 또한 $e(P,V) = e(P_{pub}, U + hQ_{ID})$를 체크함으로써 확인할 수 있다.

2.3. Threshold 대리 서명의 요구 사항

Hwang등[10]은 threshold 대리 서명의 안전성을 위해 요구되는 사항들을 다음과 같이 정리하였다. (1) 원서명자의 비밀키를 알 수 없어야 한다는 Secrecy, (2) 대리 서명자들만이 유효한 대리 서명을 할 수 있어야 한다는 Proxy protected, (3) t명 이상의 사람들만이 합법적인 서명을 만들 수 있어야 한다는 Unforgeability, (4) 한번 유효한 서명이 생성되면 부인할 수 없어야 한다는 Nonrepudation, (5) 일정 시간 동안에만 사용할 수 있어야 한다는 Time constraint 등이 있다. 자세한 내용은 [10]을 참고한다.

3. ID 기반 Threshold 대리 서명

이 절에서는 Cha-Cheon의 서명 기법을 기반으로 하는 (t,n) Threshold 대리 서명 기법을 제시한다. 기본적인 틀은 Xu 등의 IDTPS[2]를 따른다.

3.1. 서명 기법

1) 시스템 구성

Cha-Cheon의 시스템 구성과 같이 (P, P_{pub}, H_1, H_2)를 파라미터로 공개하며 시스템은 마스터키 s를 비밀로 간직한다.

원서명자를 P_0라 하고, $P_i\ (i = 1,\ldots n)$인 n 명의 대리 서명자들 집합을 $PS = \{P_1, P_2, \Lambda, P_n\}$라 한다.

2) 개인키 생성

원서명자 및 대리 서명자들은 자신의 ID에 대응하는 개인키 $D_{ID} = sH_2(ID)$를 발급 받는다.

3) 비밀 분배 정보 생성

n명으로 구성된 대리 서명자들에게 비밀 분배를 위한 정보를 나눈다. 이 정보를 가진 대리 서명자들만이 이후 대리 서명에 참여가 가능하다. 각각의 $P_i \in PS$는 계수가 $a_{ik} \in_R Z_l^*$인 임의의 $(t-1)$ 차 다항식 $f_i(x) = \sum_{k=1}^{t-1} a_{ik}x^k + a_{i0}$을 정한 뒤, $k = 0,\ldots,t$에 대해 $A_{ik} = a_{ik}P$를 계산하여 공개하고, 보안 채널을 통해 다른 모든 대리 서명자 $P_j (j \neq i)$에게 $f_i(j)$를 계산하여 보낸다. P_j는 $f_i(j)P = \sum_{k=0}^{t-1} j^k A_{ik}$ 식이 성립을 확인한 뒤, 자신의 비밀 분배 $r_i = \sum_{k=0}^{t-1} f_k(i)$를 계산한 뒤, $U_i = r_i Q_i$를 공개한다.

4) 대리 권한 분배 생성

원서명자는 대리 서명 권한 및 기간 등을 제시한 위임장 m_w Cha-Cheon 기본 서명 기법을 사용하여 PS에게 전달한 뒤, 권한을 나누어 갖는다.

즉, 원서명자는 $r_w \in Z/l$를 생성하여 다음을 계산한다.

$U_w = r_w Q_o$, $V_w = (r_w + H_1(m_w, U_w))D_0$

이제 위임장 m_w 와 위임 서명 $\sigma_w = (U_w, V_w)$을 각 $P_i \in PS$에게 전달하며, 각 대리 서명자는 다음 식이 성립하는지 확인한 뒤, 다음 단계로 진행한다.

$e(P, V_w) = e(P_{pub}, U_w + H_1(m_w, U_w)Q_o)$

이제 각 대리 서명자는 대리 권한 분배 $ps_i = D_i + \frac{1}{n}V_w \in G$를 생성한다. 그리고 현재의 위임장 m_w에 대한 대리 서명 권한을 나누어 갖기 위해 $b_{ik} \in_R G$를 계수로 갖는 임의의 $(t-1)$ 차 다항식 $g_i(x) = \sum_{k=1}^{t-1} b_{ik}x^k + ps_i$을 정한 뒤, $k = 1,\ldots,t$에 대해 $B_{ik} = e(P, b_{ik})$를 계산하여 공개한다. 이 때, $B_{i0} = e(P, ps_i)$로 계산하여 공개한다.

각 대리 서명자들은 다른 모든 대리 서명자 $P_j (j \neq i)$에게 보안 채널을 통해 $g_i(j)$를 계산하여 보낸다. 이를 받은 P_j는 $e(P, g_j(i)) = \prod_{k=0}^{t-1} B_{jk}^{\ i^k}$의 성립을 확인하고, 성립하면 대리 권한 비밀 키 $skp_i = \sum_{k=0}^{n} g_k(i)$를 계산한 뒤, $e(P, skp_i)$를 공개한다.

5) 대리 서명 생성

메시지 m에 대해 원서명자 P_0를 대신하여 대리 서명을 할 t명의 대리 서명자들의 집합을 $PD = \{P_1, P_2, \Lambda, P_t\}$라 하자.

라그랑지 내삽 공식을 적용하여, $\eta_i = \prod_{j \neq i}^{j \in \{1,2,\ldots t\}} \frac{j}{j-i}$에 대해

$U=\sum_{i=1}^{t}\eta_i U_i$ 을 계산한다. 각각의 $P_i \in PD$ 는 대리 서명 작업을 하는 사람에게 자신의 서명 $\sigma_i=(U_i,V_i)$ 을 보낸다. 이 때 U_i,V_i 는 다음과 같다.

$U_i=r_iQ_i,\ V_i=(r_i+H_1(m,U))D_i+skp_i$

비서는 $V=\sum_{i=1}^{t}\eta_i V_i$ 를 계산한 뒤, $\sigma=(U,V)$ 를 생성한 다. 메시지 m 에 대한 t명의 threshold 대리 서명은 다음과 같다. $<m,U_w,m_w,\sigma>$

6) 대리 서명 검증

공개된 키 및 ID를 이용하여, $h_w=H_1(m_w,U_w)$, $h=H_1(m,U)$, $Q_i=H_2(IDi)\in G\ \ (i=0,...,n)$, U , 그리고 $Q=\sum_{i=1}^{t}\eta_i Q_i$ 를 계산한 뒤. 다음식을 통하여 검증한다.

$$e(P,V)=e(P_{pub},U_w+h_wQ_0)e(P_{pub},\sum_{i=1}^{n}Q_i)e(P_{pub},U+hQ)$$

3.2. 정확성

위 서명이 제대로 수행되면 대리 서명 검증식은 성립한다.

$$\begin{aligned}
&e(P,V)=e(P,\sum_{i=1}^{t}\eta_i V_i)\\
&=e(P,\sum_{i=1}^{t}\eta_i skp_i)e(P,\sum_{i=1}^{t}\eta_i(r_i+h)D_i)\\
&=e(P,\sum_{k=1}^{n}\sum_{i=1}^{t}\eta_i g_k(i))e(P,\sum_{i=1}^{t}\eta_i(r_i+h)sQ_i)\\
&=e(P,\sum_{k=1}^{n}g_k(0))e(sP,\sum_{i=1}^{t}\eta_i(r_i+h)Q_i)\\
&=e(P,V_w+\sum_{k=1}^{n}D_k)e(P_{pub},\sum_{i=1}^{t}\eta_i(r_iQ_i+hQ_i))\\
&=e(P_{pub},U_w+h_wQ_0)e(P_{pub},\sum_{i=1}^{n}Q_i)e(P_{pub},U+hQ)
\end{aligned}$$

3.3. 안전성

앞에서 우리는 IDTPS의 요구 사항으로 (1) Secrecy, (2) Proxy protected, (3) Unforgeability,(4) Nonrepudation, (5) Time constraint 를 들었다.

본 서명 기법은 서명 과정에서 existential forgery 공격에 안전한 Cha-Cheon의 서명 기법을 반복해서 사용하고 있으므로, 공개된 정보들만을 가지고는 원서명자의 비밀키를 알아낼 수 없으며(1), 대리 서명자의 비밀키도 알아낼 수 없기 때문에 원서명자라도 대리인을 가장해서 서명할 수 없게 된다(2). 또한 한 번 유효한 서명이 생성되면 부인할 수 없는 특성을 그대로 가지게 된다(4). 한편, 위임장을 포함하고 있으므로 일정 시간만을 사용하도록 제한이 가능하다(5). 그리고 여기서는 t-1차 다항식을 사용하므로, t명 이상이 있을 때에만 다항식이 풀리게 되므로 (3)을 보장하게 된다.

3.4. 효율성

본 논문이 기반하는 Cha-Cheon의 서명 기법[4]은 이전 연구인 SOK-IBS에 비해, 서명할 때 mapping 하는 시간이 오래 걸리는[5] $H:\{0,1\}^*\rightarrow G$ 대신 $H:\{0,1\}^*\rightarrow Z/l$ 로 가는 간단한 해쉬 함수를 사용하기 때문에 더 효율적이며[8], 검증할 때에도 pairing 연산을 적게 사용[9]하기 때문에 동일한 구조를 갖는 전체 서명 기법에서 더 효율적인 결과를 얻는다.

4. 결론 및 향후 과제

ID 기반의 암호 시스템을 사용하는 곳에서, 자신의 서명 권한을 여러 명의 대리 서명자들에게 분배하는 기술은 매우 유용하다. 본 논문에서는 이를 구현하기 위해 기존의 논문에서 소개된 SOK-IBS를 기반으로 하는 기법보다 충분한 안전성을 보장하면서도 더 효율적인 Cha-Cheon의 서명 기법을 사용함으로써, 더 효율적인 ID 기반의 threshold 대리 서명 기법을 소개하였다. 또한, 비밀키 분배를 위한 계산 이외의 기본 서명 기법은 Cha-Cheon의 서명 기법을 거의 그대로 사용하였으므로, 그 안정성 및 기존 시스템에서의 확장이 용이하다.

5. 참고 문헌

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

[2] J. Xu, Z. Zhang, D. Feng, " Identity Based Threshold Proxy Signature," Cryptology ePrint Archive, Report 2004/250, http://eprint.iacr.org

[3] M. Bellare, C. Namprempre, G. Neven, " Security Proofs for Identity-Based Identification and Signature Schemes," EUROCRYPT 2004, pp.268-286, 2004.

[4] J. C. Cha, J. H. Cheon, "An Identity-Based Signature from Gap Diffie-Hellman Groups," Practice and Theory in Public Key Cryptography - PKC'2003, Lecture Notes on Computer Science 2567, pp. 18-30, 2003.

[5] D. Boneh, M. Franklin, "Identity-based encryption from the Weil pairing," Advances in Cryptology - Crypto'2001, LNCS 2139, pp. 213-229, 2001.

[6] A. Shamir, " How to share a secret," Communications of the ACM 22, pp.612-613, 1979.

[7] M. Mambo, K. Usuda and E. Okamoto, "Proxy signatures for delegating signing operation," Proc. 3rd ACM Conference on Computer and Communications Security, ACM Press, pp.48-57, 1996.

[8] M. C. Gorantla and R. Gangishetti and A. Saxena, " A Survey on ID-Based Cryptographic Primitives," Cryptology ePrint Archive, Report 2005/094, http://eprint.iacr.org

[9] B. Libert and J. Quisquater, " The Exact Security of an Identity Based Signature and its Applications" , Cryptology ePrint Archive, Report 2004/102, http://eprint.iacr.org

[10]M. Hwang, E. Lu, I. Lin, "A Practical (t, n) Threshold Proxy Signature Scheme Based on the RSA Cryptosystem," IEEE Trans. Knowledge and Data Engineering, 15(6), pp.1552-1560, Nov. 2003.

[11] J. Lee, J. Cheon, T. Kim, S. Jin, ``ID-based Proxy Signature Scheme from the Bilinear Map," 한국 정보보호학회 논문지 Vol. 13, No. 2, pp.3-12, 2003.

[12] J. Baek, Y. Zheng. "Identity-Based Threshold Signature Scheme from the Bilinear Pairings," itcc, vol. 01, no. 1, p. 124, International 2004.

[13] X. Chen, F. Zhang, D. M. Konidala, K. Kim, "New ID-Based Threshold Signature Scheme from Bilinear Pairings," INDOCRYPT 2004, pp.371-383, 2004