일방향 해쉬 함수를 이용한 효율적 일회용 대리 서명에 관한 연구

김소진, 박지환
부경대학교 정보보호학과

An Efficient One-Time Proxy Signature Scheme Using One-Way Hash Function

So-Jin Kim, Ji-Hwan Park
Dept of Information Security, PuKyong University

요 약

일회용 대리 서명은 원 서명자를 대신한 정당한 대리 서명자가 메시지에 대한 서명을 오직 한번만 수행하는 기법으로 Huaxiong와 Josef(HJ)는 일방향 해쉬 함수를 이용한 일회용 대리 서명 기법을 제안하였다[1]. HJ 방식은 공개키 암호 방식에 비해 상대적으로 연산속도가 빠르며 효율적이지만, 원 서명자는 사전에 많은 비밀키/공개키 쌍을 생성해야 하고, OT(Oblivious Transfer) 프로토콜[2,3]을 사용함으로 추가적인 계산량의 문제가 발생한다. 따라서 본 논문에서는 HJ 방식의 일회용 대리 서명 방식의 문제점을 지적하고, 이를 개선한 효율적 일회용 대리 서명을 제안한다.

1. 서론

전자 서명은 RSA[4], ElGamal[5]과 같은 공개키 암호 알고리즘을 이용한 메시지(unlimited number of messages)의 서명 방식과 SHA-1나 MD5와 같은 일방향 해쉬 함수를 이용한 한정된 메시지(predetermined number of messages)만을 서명할 수 있는 방식[6~9]으로 구분된다. 특히 일회용 서명(one-time signature)은 주어진 키로 오직 하나의 메시지만 서명하는 것으로 Lamport[6]와 Rabin[7]에 의해 처음 제안되었다. 이후 다양한 일회용 서명 기법들이 연구되었고, 서명의 생성 및 검증에 대한 효율성으로 많은 계산량을 고려해야 하는 응용분야에 이용되고 있다[10~13].

그리고 Huaxiong와 Josef(HJ)는 이를 응용한 새로운 일회용 대리서명 기법을 제안하였다[1]. 일회용 대리 서명(one-time proxy signature)은 원 서명자가 지정한 대리 서명자가 오직 한번만 메시지의 서명을 대신 수행하는 기법이다. HJ 방식은 공개키 암호 방식의 일회용 서명[14,15]에 비해 훨씬 효율적이지만, 사전에 많은 비밀키/공개키 쌍을 생성해야 하고 OT(Oblivious Transfer) 프로토콜의 사용에 따른 추가적인 계산량의 문제가 발생한다.

따라서 본 논문에서는 HJ 방식의 일회용 대리 서명 방식의 문제점을 지적하고, 이를 개선한 일방향 해쉬함수를 이용한 효율적 일회용 대리서명을 제안한다.

2. 관련 연구 - 일회용 대리서명[1]

대리 서명은 원 서명자가 지정한 사람이 원 서명자를 대신해서 서명을 수행하는 방식으로 원 서명자의 계산량을 줄여주는 장점을 가진다.

대리 서명은 다음과 같은 조건을 가져야 한다[16].

- **위조 불능성**

  원 서명자가 지정한 대리 서명자만이 정당한 서명을 생성할 수 있다. 원 서명자를 포함한 제 3자는 대리 서명할 수 없어야 한다.

· 검증 가능성
대리 서명을 확인하는 검증자는 이 서명값이 원 서명자가 지정한 대리 서명자에 의하여 서명되었음을 확인할 수 있어야 한다.

· 신분 확인성
누구든지 대리 서명한 대리자의 신분을 확인할 수 있어야 한다.

· 부인 불가성
원 서명자를 대신하여 서명한 대리자는 이에 대해 부정할 수 없어야 한다.

Mambo[16]는 본인이 부재시 대신 서명을 할 수 있는 대리서명 방식을 최초로 제안하였고, 위임 유형에 따라 완전 위임, 부분 위임, 보증 위임 방식으로 대리 서명을 분류하였다. 이후 다양한 방식으로 개선되었고, KBLK 방식[14]과 KP 방식[15]에서는 대리자가 오직 한번만 메시지의 서명을 수행하여 대리자의 부정을 방지할 수 있는 일회용 대리 서명을 제안하였다. 이러한 대리 서명은 이산대수 문제의 어려움에 기반한 ElGamal 암호방식을 이용하였다. 그리하여 최근 Huaxiong와 Josef에 의해 일방향 해쉬함수를 이용한 효율적 일회용 대리서명 기법이 제안되었다[1].

HJ 방식의 일회용 대리 서명은 다음과 같다.

여기서 $\binom{t}{k} \geq 2^b$을 만족하는 자연수인 b, t, k를 정의하고, 두 집합 $T=\{1,2,3,t\}$와 $T_k=\{k\text{-subsets of T}\}$, l-비트의 출력을 갖는 일방향 해쉬함수 $h()$, 그리고 $\{0,1,2,\cdots,2^b-1\}$에서 T_k로의 일대일 대응 함수 $f()$를 사용한다.

가. 원 서명자의 키 생성

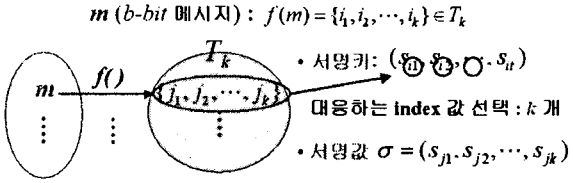
- 원 서명자는 비밀키 A와 공개키 V를 생성한다.
  $A=(s_{ij})_{n\times t}$, $V=(v_{ij})_{n\times t}$
  (s_{ij} : 임의의 l-비트 스트링, $v_{ij}=h(s_{ij})$)

나. 대리 서명자의 서명키 획득

- 원 서명자와 대리자 사이에 OT_1^n(Oblivious Transfer) 프로토콜[3]을 수행하여 대리 서명자는 원 서명자의 A에서 i번째 행(row)의 값을 얻고, 이것은 t개의 대리 서명자의 비밀 서명키들이 된다.
  $i=(s_{i1}, s_{i2}, \cdots, s_{it})$
  이때, 원 서명자는 인덱스 i에 관한 어떠한 정보도 알 수 없다.

다. 대리 서명

- 대리 서명자는 위임받은 서명키(i)를 가지고 b-비트의 m을 서명한다. 먼저 k-비트의 $f(m)$값을 구하고, 이와 대응하는 인덱스의 서명키 k개를 선택한다. 이때 결정된 $(s_{i1}, s_{i2}, \cdots, s_{ik})$값들이 m의 서명값 $\sigma=(s_1, s_2, \cdots, s_k)$이다.



(그림1) 대리 서명값의 생성

라. 서명 검증

- 검증자는 전송받은 $\langle m, \sigma, i\rangle$에서 메시지 m의 $f(m)=\{i_1, \cdots, i_k\}$을 계산하고, $\sigma=(s_1, s_2, \cdots, s_k)$의 각 해쉬값 $h(s_1), h(s_2), \cdots, h(s_k)$을 구하여 $h(s_1)=v_{i1}, \cdots, h(s_k)=v_{ik}$이 성립됨을 확인한다.

HJ 방식은 OT 프로토콜과 일방향 해쉬함수의 안전성에 기반함으로 원 서명자와 대리 서명자의 부정을 방지할 수 있고, 서명의 생성 및 검증에 대한 계산량이 효율적이다. 원 서명자는 대리 서명자가 선택한 비밀키를 $1/n$ 확률로 알아내기 어렵고, 대리 서명자는 위임받은 유일한 서명키를 두 번 이상 사용하면 그 키가 바로 대리자의 키가 됨으로 추적 가능하다. 그러나 한번의 서명 위임을 위해서 원 서명자는 매번 많은 키쌍 ($n\times t$)을 생성해야 하고, 대리 서명자도 l-비트의 비밀키 t개를 저장해야 한다. 게다가 HJ 방식은 공개키 암호 방식의 서명 기법보다 효율적지만, OT 프로토콜에 대한 계산량을 고려하지 않았다. 즉 원 서명자는 $2n$번의 지수 연산, 대리 서명자는 2번의 지수 연산이 필요하다. 그러므로 본 논문에서는 HJ 방식의 문제점을 지적하였고, 이를 개선한 효율적 일회용 대리 서명을 제안한다.

3. 제안 방식

제안 방식은 정당한 서명의 검증과 원 서명자와 대리 서명자의 분쟁을 중재하기 위한 등록 센터를 가정하고, 등록 센터는 등록된 모든 정보를 공개

DB에 저장 및 관리한다. 그리고 원 서명자와 대리 서명자의 원 비밀키/공개키 쌍은 등록센터로부터 생성된 정보이다. 시스템 설정은 다음과 같다.

〈표1〉 시스템 설정

· $h()$: 공개된 일방향 해쉬 함수 (l-비트) $h: \{0,1\}^* \rightarrow \{0,1\}^l$ · m: 메시지 (b-비트 binary code) · σ: m의 서명값 (u-비트 binary code) · K: 비밀키 공간 (l-비트의 binary code) · $\binom{t}{l} \geq 2^b$을 만족하는 k, b, l 정의 · 원 서명자: A - 원 비밀키: $x_A \in K$ - 원 공개키: $h(x_A)$ · 원 대리 서명자: B - 원 비밀키: $x_B \in K$ - 원 공개키: $h(x_B)$

가. 대리 서명 요청

- 원 서명자는 대리 서명자에게 $\langle m, s_A, H_A \rangle$을 전송하여 서명을 요청한다.

① $k_A \in K$

$s_A = h(x_A \| k_A)$, $H_A = h(m \| s_A \| h(x_B))$

② $h(s_A \| x_A \| h(x_B))$을 등록 센터에 등록한다.

나. 서명키 생성 및 대리 서명

- 대리 서명자는 $\langle m, s_A, H_A \rangle$을 이용하여 위임 정보을 인증하고, 대리 서명값을 생성한다.

① $H_A = h(m \| s_A \| h(x_B))$

위의 식이 성립되지 않으면 수행을 중단하고, 이때, s_A의 정당성은 등록센터에서 확인 가능하다.

② t개의 대리 서명키를 다음과 같이 생성한다.

$s_{B_i} = h(x_B \| s_A \| i)$, $1 \leq i \leq t$

③ 다음을 계산하여 메시지를 서명한다.

(a) $w = h(m)$

$= (a_1 a_2 \cdots a_l)$, $a_i \in \{0,1\}$, $1 \leq i \leq l$

(b) $z = w \| c = (a_1 a_2 \cdots a_t)$ $1 \leq i \leq t$

여기서 c는 $w = (a_1 a_2 \cdots a_l)$의 a_i 값이 0인 비트 수의 합(binary code)이다.

z는 t-비트 즉, $t = (l + \lfloor \lg l \rfloor + 1)$이다.

(c) $z = (a_1 a_2 \cdots a_t)$에서 a_i의 값이 1인 각 위치를 선택하여 이와 동일한 인덱스의 s_{B_i}를 서명값으로 결정한다.

$s_i = s_{B_j}$, $1 \leq j \leq u$

$\sigma = (s_1, s_2, \cdots, s_u)$

④ m, σ를 검증자에게 전달한다.

다. 서명 검증

- 서명 검증자는 수신된 $\langle m, \sigma \rangle$을 검증하여 서명을 인증한다.

① m으로 다음을 계산하고, a_i=1인 인덱스와 대응하는 공개값과 서명값을 비교한다.

(a) $w' = h(m) = (a_1 a_2 \cdots a_l)$

(b) $z' = w' \| c' = (a_1 a_2 \cdots a_t)$

(c) $v_i = h(s_i)$, $1 \leq i \leq u$

② 위의 수식이 성립하면, 정당한 서명값으로 인증한다.

4. 제안 방식의 안전성 분석 및 비교

▶ 안전성

[정리1] 원 서명자만이 위임 정보를 생성할 수 있다.

$s_A = h(x_A \| k_A)$

- 일방향 해쉬함수를 이용하여 위임 정보를 생성함으로 역함수 $h^-()$을 구할 수 없으면 s_A를 계산할 수 없다.

[정리2] 원 대리 서명자만이 대리 서명을 할 수 있다.

$s_{B_i} = h(x_B \| s_A \| k_{B_i})$, $1 \leq i \leq t$

- s_A는 지정된 대리 서명자만이 사용할 수 있게 등록센터에 $h(s_A \| x_A \| h(x_B))$을 등록함으로 제 3자는 s_A를 이용한 대리 서명을 할 수 없다.
- 일방향 해쉬함수를 이용하여 서명키를 생성함으로 h^-을 구할 수 없으면 s_{B_i}를 계산할 수 없고, 서명도 불가능하다.
- 원 서명자를 포함한 제 3자가 m'의 서명을 위조한다면, 공개된 $\sigma = (s_1, s_2, \cdots, s_u)$값을 이용할 것이다. 그러므로 m'는 m보다 0의 비트를 많이 가져함으로 $c' > c$, c'는 1의 비트를 가진다. 이 경

우, m의 적어도 하나의 0 자리에 m'는 1을 가지게 되어 공개된 u개의 서명값으로는 위조가 불가능하다.

[정리3] 대리 서명자의 서명이 일회성임을 보장한다.

- 동일한 서명키 s_{B_i}를 두 번 이상 사용하면, $u+1$개 이상의 서명키가 노출됨으로, 제 3의 서명자들이 서명을 위조할 수 있게 된다. 그러므로 대리 서명자는 서명키를 하나의 메시지에 한번만 사용해야 한다.

▶ HJ 방식과의 비교

HJ 방식의 원 서명자는 매번 최대 $n \cdot t \cdot l$-비트의 비밀키/공개키 쌍을 생성해야 하고, 대리 서명자도 $t \cdot l$-비트의 비밀키를 저장해야 한다. 그리고 OT 프로토콜에 대한 원 서명자는 $2n$번의 지수 연산, 대리 서명자는 2번의 지수 연산이 필요하다. 그러나 제안 방식의 원 서명자는 고정된 l-비트의 원 비밀키/공개키 쌍으로 매번 l-비트의 위임 정보를 생성함으로 더 효율적이다. 또한 제안 방식은 OT 프로토콜을 수행하지 않으므로 지수 연산을 하지 않고, 서명 위조에 대한 안전성을 확보한다.

5. 결론

디지털 서명은 네트워크 상의 통신 상대방을 인증하고 메시지의 무결성을 보장하여 송·수신자간의 분쟁을 해결할 수 있는 전자 서명 방식이다. 이것은 일반적으로 공개키 암호 시스템을 기반하기 때문에 무선 환경에 그대로 적용하는 것은 사용자 단말기의 제한된 용량(메모리, CPU 파워, 인터페이스 등)으로 효율적이지 못하다는 문제점이 제기되고 있다. 그리하여 이를 해결할 수 있는 대리 서명 방식이 적용될 수 있다.

본 논문에서는 일방향 해쉬 함수를 이용한 효율적 일회용 대리 서명방식을 제안하였다. 제안 기법은 원 서명자의 키 사이즈를 줄이고, OT 프로토콜을 사용을 배제하여 HJ 방식을 개선한 방식이다. 그러므로 서명의 생성 및 검증에 대한 효율성으로 많은 계산량을 고려해야 하는 응용분야에 적용 가능하다.

참고문헌

[1] Huaxiong Wang and Josef Pieprzykm, "Efficient One-Time Proxy Signatures", Advances in Cryptology - ASIACRYPT 2003, LNCS, 507-522

[2] M.Rabin, "How to Exchange Secrets by Oblivious Transfer", Technical Report TR-81, Harvard University, 1981

[3] W-D.Tweng, "Efficient 1-out-n Oblivious Transfer Schemes", PKC 2002, LNCS, 159-171

[4] R.L.Rivest, A Shamir and L.Adleman, "A Method for Obtaining Digitial Signatures and Public Key Cryptosystems", Communication of ACM 1978

[5] T.ElGamal, "A Public Key Cryptosystem and a Signature Scheme Secure Based on Discrete Logarithm", IEEE Transactiona on Information Theory, 1985, 469-472

[6] L.Lamport, "Constructing Digital Signatures from a One Way Function", Technical Report CSL-98, SRI International, 1979

[7] M.Rabin, "Digital Signatures, Foundations of Secure Communication, Academic Press", 1978

[8] L.Reyzin and N.Reyzin, "Better than BiBa: Short One-Time Signatures with Fast Signing and Verifying", Information Security and Privacy, ACISP 2002, LNCS, 144-153

[9] P.Rohatgi, "A Compact and Fast Hybrid Signature Scheme for Multicast Packet Authentication", ACM conference on Computer and Communication Security, 1999

[10] M.Abdalla and L.Reyzin, "A New Forward-Secure Digital Signature Scheme", Advacnes in Cryptology-ASIACRYPT 2000, LNCS, 116-129

[11] C.Dwork and M.Naor, "An Efficient Existentially Unforgeable Signature Scheme and Its Applications", Advances in Cryptology-CRYPTO 1994, LNCS, 234-246

[12] H.Kim, J.Baek, B.Lee and K.Kim, "Secret Communication with secrets for mobile agent using one-time proxy signature", The 2001 Symposium on Cryptography and Information Security, Oiso, Japan

[13] A.Perrig, "The BiBa One-Time Signature and Broadcast Authentication", ACM conference on Computer and Communication Security, 2001

[14] 김희선, 백준상, 이병천, 김광조, "대리 서명을 이용한 모발일 에이전트의 안전성 강화 방법", 한국정보보호학회, 종합학술발표논문집, Vol.10, No.1, pp.424-437, 2000

[15] 김소진, 박지환, "이동 통신 환경에 적합한 일회용 대리 서명 방식", 정보처리학회 논문지, 제 10-C권, 제5호, 2003

[16] M. Mambo, K. Usuda and E. Okamoto, "Proxy signature," Proceedings of ICEIC '95, 1995