계층 그룹에서 반복적 권한 위임을 허용하는 임계 대리서명 프로토콜

박소영° 이상호
이화여자대학교 컴퓨터학과
{soyoung°, shlee}@ewha.ac.kr

Threshold Proxy Signature Schemes allowing Repetitive Delegations in a Hierarchical Group

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

요 약

권한 위임은 일상에서 흔히 발생하는 사건으로서, 특히, 군대, 기업, 은행 등의 계층 그룹에서는 계층간 권한 위임이 자연스럽고 빈번하게 발생한다. 대리서명(proxy signature)은 서명 권한을 위임받은 대리서명자가 원 서명자를 대신하여 유효한 전자서명을 생성하고 검증할 수 있는 전자서명 프로토콜이다. 계층 구조를 갖는 B2B 전자 거래 및 전자서명의 활용 범위가 다양화됨에 따라 이를 반영하는 보다 안전한 대리서명이 요구된다. 본 논문에서는 계층 그룹에서 반복적 권한 위임을 허용하는 새로운 임계 대리서명 프로토콜을 제안한다. 한 명의 대리서명자가 아닌 복수의 대리서명자가 모여 원 서명자를 대신해 하나의 유효한 대리서명을 생성할 수 있게 함으로써, 보다 강화된 안전성을 제공한다. 대리서명 생성을 위한 권한 위임은 위임티켓을 통해 계층 구조의 상위 계층에서 하위 계층으로 이루어지고, 위임받은 대리서명자들 중에서 서명에 참여할 수 없는 대리서명자는 다시 자신의 하위 계층 참가자들에게 개별 위임을 수행할 수 있도록 함으로써, 반복적 권한 위임을 허용한다.

1. 서론

인터넷을 이용한 전자 상거래(e-commerce)의 활용이 급속도로 증가함에 따라, 개인 프라이버시 및 정보 보안을 위한 암호의 사용이 보편화되고 있고, 특히, 사용자 인증을 위한 전자서명(digital signature)이 널리 활용되고 있다. 대리서명(proxy signature)[1]은 서명 권한을 위임받은 대리서명자가 원 서명자를 대신하여 유효한 전자서명을 생성하고 검증할 수 있는 전자서명 프로토콜로서, 다음의 요구조건을 만족해야 한다. 대리서명으로부터 원 서명자의 동의가 있었음을 확신할 수 있어야 하고(verifiability), 대리서명으로부터 대리서명자의 신원을 확인할 수 있어야 한다(identifiability). 위임받지 않은 대리서명자는 유효한 대리서명을 생성할 수 없어야 하고(unforgeability), 대리서명자는 대리서명 생성 후에 서명 사실을 부인할 수 없어야 한다(undeniability)[1].

권한 위임은 일상에서도 흔히 발생하는 사건으로서, 특히, 군대, 기업, 은행 등의 계층 그룹에서는 계층간 권한 위임이 자연스럽고 빈번하게 발생한다. B2B 전자 거래 및 전자 서명의 활용 범위가 다양화됨에 따라 이를 반영할 수 있는 보다 안전하고 효율적인 대리서명이 요구된다. 본 논문에서는 B2B 전자 상거래 환경에서 계층 그룹 내 대리서명을 허용한 전자 문서 계약 등에 활용될 수 있는 안전한 대리서명 프로토콜을 제안한다. 임계 암호(threshold cryptography)[2]를 바탕으로, 복수의 대리서명자가 모여 하나의 유효한 대리서명을 생성할 수 있는 임계 서명 스킴(threshold signature scheme)[3,4]을 통해 강화된 안전성을 제공한다. 대리서명을 위한 권한 위임은 계층 구조의 상위 계층 참가자로부터 하위 계층 참가자로 이루어지고, 위임티켓(delegation ticket)[5]을 통해 실질적인 권한 위임이 수행된다. 원 서명자가 생성한 위임티켓은 비밀분산법(secret sharing scheme)[5]에 의해 대리서명자들간에 공유되고, 이렇게 공유된 정보를 위임티켓 공유정보라고 한다. 특히, 제안하는 방법에서는 Diffie-Hellman 문제[6]를 이용하여 안전한 비밀채널에 대한 가정 없이 대리서명자들이 안전하게 위임티켓 정보를 공유할 수 있다. 각 대리서명자들은 자신의 위임티켓 공유정보와 비밀키-공개키 쌍을 이용하여 부분 대리서명을 생성하고, 생성된 부분 대리서명들이 모두 모이면, 원 서명자의 위임티켓이 복원됨과 함께 하나의 유효한 대리서명이 생성된다. 또한, 대리서명 권한을 위임받은 참가자 중에서 서명에 참여할 수 없는 대리서명자는 다시 자신의 자식 노드에 해당하는 참가자들에게 개별 위임을 수행함으로써, 대리서명 권한이 계층 트리를 따라 단말노드에 해당하는 참가자들에게까지 반복적으로 위임될 수 있다.

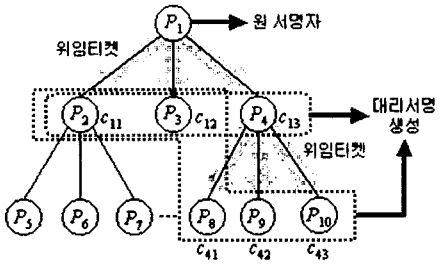
2. 관련 연구

대리서명은 M. Mambo, K. Usuda와 E. Okamoto에 의해 처음 제안되었다[1]. 그러나, 이 MUO 스킴은 원 서명자가 대리서명 키를 생성하여 대리서명자에게 건네주므로, 원 서명자와 대리서명자간 상호 정보 교환(interactive protocol)은 없으나, 부인 방지 기능을 만족하지 않는다. 김승주, 박성준, 원동호는 보증 정보(warrant information)를 이용하여 Schnorr 서명 스킴[7]에 기반한 대리서명을 제안하였고[8], 이는 부인 방지 기능을 갖는다. 보증 정보에 위임 관계가 명백하게 명시되어 있으면, 원 사용자의 대리서명 오용(misuse)을 방지할 수는 있지만, 보증정보 자체에 대한 안전성이 보장되지 않는다. K. Zhang은 MUO 스킴[1]에 부인 방지 기능을 추가하고, 이를 바탕으로 처음으로 임계 대리서명(threshold proxy signature)을 제안하였다[9]. 그러나 원 서명자와 대리서명자간 상호 정보교환을 필요로 하고, 대리서명 생성을 위한 연산량이 비교적 많다. 반복적 권한 위임을 허용하는 대리서명은 아직까지 제안되지 않았다.

3. 제안 모델

본 논문에서 가정하는 계층 구조와 위임구조에 대해 설명한다. n명의 참가자 집합은 $P=\{P_1,P_2,...,P_n\}$ 이고, 참가자들은 각 참가자들을 노드(node)로 하는 차수(degree)가 2이상인 트리(tree)형태의 계층 구조를 이룬다. 계층 트리에서 각 참가자 P_i를 루트로 하고 P_i의 자식노드들을 단말노드(leaf node)로 하는 부트리(subtree)를 T_i라고 한다. T_i는 P_i의 위임구조를 나타내며, T_i의 단말노드들은 다시 $c_{i1},...,c_{it_i}$ 로 표기된다.

P_i는 위임티켓을 사용하여 자신의 서명 권한을 $c_{i1},...,c_{it_i}$ 들에게 위임할 수 있고, 이 중에서 서명에 참여할 수 없는 대리서명자는 다시 자신의 자식 노드에 해당하는 참가자들에게 개별 위임을 수행함으로써, 대리서명 권한이 계층 트리를 따라 단말 노드에 해당하는 참가자들에게까지 반복적으로 위임될 수 있다. 그리고 권한을 위임받은 대리서명자들이 모두 모여야만 하나의 유용한 대리서명을 생성할 수 있다. 다음 (그림 1)은 계층 구조 및 위임 구조를 그림으로 표현한 예이다.



(그림 1) 계층 구조 및 권한 위임 구조

각 참가자들은 유한체(finite field) 상에서의 이산대수(discrete logarithm) 문제[6]에 기반한 비밀키-공개키 쌍을 보유하고 있고, 모든 참가자들간에는 서로 데이터를 송·수신할 수 있는 네트워크 채널(channel)이 형성되어 있다. 네트워크 채널은 안전하지 않다(insecure)고 가정하며, 도청자(attacker)는 네트워크 채널 상의 모든 정보를 읽고 위·변조할 수 있다. 본 프로토콜에서 사용되는 주요 파라미터(parameter)는 다음 (표 1)과 같다.

(표 1) 주요 파라미터

p	매우 큰 소수, $\|p\| \geq 512$ bit
g	$g \in Z_p$, $g^{p-1} \equiv 1 \bmod p$, 생성자
$< xp_i , yp_i >$	$xp_i \in Z_p$ $yp_i = g^{xp_i} \bmod p$, P_i의 비밀키-공개키 쌍
t_i	$t_i \geq 2$ 이거나 $t_i = 0$, P_i의 자식노드 개수
dt_i	P_i가 권한 위임 시에 발행하는 위임티켓
m	메시지

4. 임계 대리서명 프로토콜

n명의 참가자로 구성되는 계층 그룹에서 원 서명자 P_i가 자신의 자식노드 $c_{i1},...,c_{it_i}$ 들에게 위임티켓을 생성하여 서명 권한을 위임하고, $c_{i1},...,c_{it_i}$ 들이 대리서명을 생성하는 방법을 설명한다. 제안하는 방법은 크게 위임티켓 생성 단계, 대리서명 생성 및 검증 단계 그리고 반복적 권한 위임 단계로 구분된다. 모든 연산은 유한체 $GF(p)$ 상에서 수행되며, 이후 본 논문의 수식에서 mod p는 생략한다.

4.1 위임티켓 생성

위임티켓은 원 서명자 P_i가 대리서명자를 지정하기 위해 권한 위임 시 임의로 생성하는 정보로서, 위임 정보를 받은 대리서명자 $c_{i1},...,c_{it_i}$ 들은 P_i가 생성한 위임티켓과 동일한 정보를 복원할 수 있다. P_i가 생성하는 위임티켓은 dt_i이고, 이는 비밀분산법에 기반하여 $c_{i1},...,c_{it_i}$ 들 사이에서 공유된다. 각 대리서명자 c_{ij}에게 공유되는 위임티켓 정보를 위임티켓 공유정보 dt_{ij}라고 한다. P_i는 t_i개의 랜덤 값 $rs_1, rs_2, ..., rs_{t_i} \in Z_p$ 를 선택한 다음, $c_{i1},...,c_{it_i}$ 들의 위임티켓 공유정보 $dt_{i1}, dt_{i2}, ..., dt_{it_i}$ 를 다음과 같이 생성한다. yc_{ij}는 c_{ij}의 공개키이다.

$$dt_{ij} = (yc_{ij})^{rs_{ij}}, j = 1,...,t_i$$

결과적으로, P_i가 생성하는 위임티켓 dt_i는 $dt_i = \sum_{j=1}^{t_i} dt_{ij}$ 이고, P_i는 공개 위임 정보 $DT_i = g^{dt_i}$ 를 생성하여 공개한다.

4.2 대리서명 생성 및 검증

원 서명자로부터 위임정보를 건네 받은 대리서명자들은 자신의 위임티켓 공유정보를 생성한 후, Schnorr 서명 스킴[7]에 기반하여 부분 대리서명을 생성한다. 대리서명자 c_{ij}가 자신의 부분 대리서명 $< pa_j, pr_j, ps_j >$을 생성하는 과정은 다음 (표 2)와 같다. $< xp_i, yp_i >$와 $< xc_{ij}, yc_{ij} >$는 각각 원 서명자 P_i와 대리서명자 c_{ij}의 비밀키-공개키 쌍이다.

(표 2) 대리서명 생성 프로토콜

원 서명자 P_i		대리서명자 c_{ij}
$k_j = dt_{ij} \cdot xp_i + rs_j$ $RS_j = g^{rs_j}$	$< k_j, RS_j, t_i >$ --------->	위임티켓 공유정보 dt_{ij} 생성 $dt_{ij} = (RS_j)^{xc_{ij}} = g^{rs_j \cdot xc_{ij}}$ 생성 후, $g^{k_j} = (yp_i)^{dt_{ij}} \cdot RS_j$ 인가 검증해서 만족하면, 부분 대리서명 $< pa_j, pr_j, ps_j >$ 생성 $a_j \in Z_p$ 랜덤하게 생성 $l_j = a_j + dt_{ij}$ $pa_j = g^{a_j}$ $pr_j = g^{dt_{ij}}$ $ps_j = m \cdot xc_{ij} + l_j$

대리서명자 $c_{i1},...,c_{it_i}$ 들은 자신의 부분 대리서명을 이용하여 대리서명 $< PA, PR, PS >$를 다음과 같이 생성한다.

$$PA = \prod_{j=1}^{t_i} pa_j \ , \ PR = \prod_{j=1}^{t_i} pr_j \ , \ PS = \sum_{j=1}^{t_i} ps_j$$

생성된 대리서명은 각 대리서명자의 공개키와 원 서명자가 공개한 위임티켓 공개정보 DT_i에 의해 다음 등식의 성립 여부로 검증된다.

$$PR = DT_i \quad , \quad g^{PS} = (yc_{i1} \cdots yc_{it_i})^m \cdot PA \cdot PR$$

4.3 반복적 권한 위임

원 서명자 P_i의 대리서명자 $c_{i1},...,c_{it_i}$ 중에서 대리서명에 참여할 수 없는 대리서명자 c_{ij}를 P_j라고 하자. 참가자 P_j는 자신을 루트로 하는 부트리 T_j의 위임구조에 따라 자식 노드에 해당하는 대리서명자들 $c_{j1},...,c_{jt_j}$ 에게 자신의 부분 대리서명 권한을 위임할 수 있다. P_j가 $c_{j1},...,c_{jt_j}$ 들에 대해 생성하는 위임티켓 dt_j는 P_j가 P_i에 대해 생성한 위임티켓 공유정보 dt_{ij}와 동일하다. $c_{j1},...,c_{jt_j}$ 들에 대한 위임티켓 공유정보 생성 과정은 4.1절의 위임티켓 생성과 동일하다. 그러나, P_j는 공개 위임티켓 공유정보 pdt_j를 다음과 같이 추가로 생성하여 dt_j의

공개 정보 g^{dt_i}와 함께 공개한다.

$$pdt_j = dt_j - \sum_{j=1}^{t_i} dt_{jl}$$

각 c_{jl}가 자신의 부분 대리서명을 생성하는 과정은 (표 2)와 동일하다. $c_{j1},...,c_{jt_j}$ 들은 자신의 부분 대리서명 $< pa_{c_{jl}}, pr_{c_{jl}}, ps_{c_{jl}} >$을 생성한 후, P_j의 부분 대리서명 $< pa_j, pr_j, ps_j >$를 다음과 같이 생성함으로써, P_j를 대신하여 대리서명 생성에 참여한다.

$$pa_j = \prod_{l=1}^{t_j} pa_{c_{jl}} \quad , pr_j = \left(\prod_{l=1}^{t_j} pr_{c_{jl}} \right) \cdot g^{pdt_j} \quad , ps_j = \left(\sum_{l=1}^{t_j} ps_{c_{jl}} \right) + pdt_j$$

pr_j는 P_j가 공개한 g^{dt_j}와 동일하고, ps_j는 pa_j 및 pr_j와 $c_{j1},...,c_{jt_j}$ 들의 공개키로 검증될 수 있다. 결과적으로, 원 서명자 P_i의 위임을 받은 대리서명자 중에서 P_j가 다시 권한 위임을 수행하면, P_i의 자식 노드들 중에서 P_j를 제외한 나머지 자식 노드들과 P_j의 자식노드 $c_{j1},...,c_{jt_j}$ 들이 모여 P_i의 대리서명을 생성할 수 있고, 생성된 대리서명은 모든 대리서명자들의 공개키에 의해 검증된다. 권한 위임은 위와 같은 방법으로 단말 노드의 참가자들에게까지 반복적으로 위임될 수 있다.

5. 분석

제안하는 방법의 기본적인 안전성은 매우 큰 소수에 대한 유한체 상에서의 이산대수 문제의 어려움에 근거한다. 원 서명자 P_i와 대리서명자 $c_{i1},...,c_{it_i}$ 들은 Diffie-Hellman 키 교환 방식에 따라 동일한 위임티켓 공유정보를 공유하므로, 원 서명자는 위임 사실을 부인할 수 없고, 위임 정보 $RS_j = g^{rs_j}$를 받지 않은 대리서명자들은 정당한 위임티켓 공유정보 $dt_{ij} = (RS_j)^{xc_{ij}} = g^{rs_j \cdot xc_{ij}}$ 을 생성 할 수 없다. 또한 악의적인 대리서명자들이 원 서명자의 위임티켓을 위조하는 것도 불가능하다. 대리서명자들이 악의적으로 모두 단합하여 임의의 랜덤 값 $rs_1',...,rs_{t_i}'$ 을 선택하고 $RS_1',...,RS_{t_i}'$ 를 생성하여, 이로부터 새로운 위임티켓 공유정보 $dt_{ij}' = (RS_j')^{x_{c_{ij}}}$ 들을 생성할 수 있다 하여도, 원 서명자의 비밀키를 모르기 때문에 새롭게 생성한 위임티켓 공유정보에 상응하는 $k_1',...,k_{t_i}'$ 를 생성할 수 없으므로 위임티켓의 위조가 불가능하다. 즉, 악의적인 대리서명자들이 임의로 위임티켓을 위조하여 사용했을 경우, 원 서명자에 의해 발행된 위임티켓이 아님이 검증될 수 있다.

각 대리서명자들의 부분 대리서명 $< pa_j, pr_j, ps_j >$은 위임티켓 공유정보와 함께 Schnorr 서명 스킴에 기반하여 생성되므로, 비밀키를 모르는 원 서명자 및 위임받지 않은 다른 참가자들은 대리서명자를 가장하여 대리서명에 참여할 수 없고, 대리서명자 또한 부분 대리서명 생성 사실을 부인할 수 없다. 각 대리서명자의 부분 대리서명 $< pa_j, pr_j, ps_j >$는 대리서명자들의 공개키 yc_{ij} 및 공개 위임티켓 공유정보 $pr_j = g^{dt_j}$에 의해 등식 $g^{ps_j} = (yc_{ij})^m \cdot pa_j \cdot pr_j$ 의 성립 여부로 검증될 수 있다. 그리고, 부분 대리서명이 하나라도 부족하게 되면, 원 서명자의 위임티켓이 제대로 복원되지 않으므로, 모든 대리서명자들의 부분 대리서명이 모여야만 정당한 하나의 대리서명 $< PA, PR, PS >$이 생성된다.

각 대리서명자의 부분 대리서명권한은 다시 하위 계층의 참가자들에게 반복적으로 위임될 수 있다. 그러나 이 경우에는 공개 위임티켓 공유정보를 부가적으로 생성해야 하므로, 반복 위임의 회수가 증가할수록 공개 위임티켓 공유정보의 개수도 증가한다. 공개 위임티켓 공유정보는 위임받은 대리서명자들이 상위 대리서명자의 위임티켓 공유정보를 복원할 수 있기 위한 부가 정보로써, 공개 위임티켓 공유정보만으로는 위임티켓에 대한 어떠한 정보도 획득할 수 없다.

6. 결론

본 논문에서는 계층 구조를 갖는 B2B 전자 상거래에 적합한 안전한 대리서명 프로토콜을 새롭게 제안하였다. 계층 그룹 내에서 계층간 권한 위임을 통해 대리서명이 수행되고, 복수의 대리서명자가 모두 모여야만 정당한 대리서명을 생성할 수 있도록 함으로써, 대리서명의 안전성을 강화시켰다. 제안하는 방법은 대리서명이 만족해야 하는 기본적인 안전성 및 부인 방지 기능을 만족하며, 반복적 권한 위임을 허용한다. 권한 위임은 위임티켓의 생성을 통해 이루어지며, 위임받은 대리서명자들은 자신의 비밀키와 위임티켓 공유정보를 이용하여 부분 대리서명을 생성하고, 생성된 부분 대리서명이 모두 모이면 원 서명자와 동일한 위임티켓이 복원되어, 하나의 정당한 대리서명이 생성된다. Diffie-Hellman 문제를 이용하여 복수의 대리서명자들이 비밀 채널을 통한 공유정보의 전송 없이 위임티켓을 공유할 수 있게 함으로써, 보다 실용적인 프로토콜을 제안하였다. 또한, 계층 구조 내에서 반복적 권한 위임을 허용함으로서 대리서명자들이 동적으로 구성될 수 있다. 그러나, 권한 위임이 반복적으로 수행되는 경우에는 공개 위임티켓 공유정보가 부가적으로 생성되므로, 부가정보의 생성 없이 보다 효율적으로 반복적 권한 위임을 허용할 수 있는 방법이 요구된다.

[참 고 문 헌]

[1] M. Mambo, K. Usuda and E. Okamoto, "Proxy Signature: Delegation of the Power to Sign Message," IEICE Trans. Fundamentals, vol. E79-A, no. 9, pp. 1338-1353, 1996.

[2] Y. Desmedt, "Threshold Cryptography," European Trans. on Telecommunications and Related Technologies, vol. 5, no. 4, pp. 35-43, 1994.

[3] R. Gennaro, S. Jarecki, H. Krawczyk and T. Rabin, "Robust Threshold DSS Signatures," Advances in Cryptology-EUROCRYPT '96, LNCS 1070, 1996.

[4] C. Li, T. Hwand and N. Lee, "(t,n)-Threshold Signature Scheme based on Discrete Logarithm," Advances in Cryptology-EUROCRYPT '94, 1995.

[5] 송영원, 박소영, 이상호,"트리형태의 계층 구조에 적용가능한 비밀분산법의 설계", 한국정보과학회 논문지, 제29권 4호, pp. 161-168, 2002.

[6] W. Diffie and M. E. Hellman, "New Directions in Cryptography," IEEE Trans. on Information Theory, vol. IT-22, no. 6, pp. 644-654, 1976.

[7] C. P. Schnorr, "Efficient Signature Generation for Smart Cards," Advances in Cryptology-CRYPTO '89, pp. 239-252, 1990.

[8] S. Kim, S. Park and D. Won, "Proxy Signatures, Revisited," Proceeding of ICICS '97, LNCS 1334, pp. 223-232, 1997.

[9] K. Zhang, "Threshold Proxy Signature Schemes," Proceeding of 1st International Information Security Workshop, pp. 191-197, 1997.

[10] J. L. Camenisch, J. M. Prveteau and M. A. Stadler, "Blind Signatures based on the Discrete Logarithm Problem," Advances in Cryptology-EUROCRYPT '94, pp. 428-432, 1994

[11] K. Zhang, "Nonrepudiable Proxy Signature Schemes based on Discrete Logarithm Problem," Manuscript, 1997.