비밀분산법과 Diffie-Hellman 문제에 기반한 동적 멀티 대리서명 프로토콜

(Dynamic Multi-Proxy Signature Schemes based on Secret Sharing and Diffie-hellman Problem)

박 소 영 † 이 상 호 ††
(So-Young Park) (Sang-Ho Lee)

요 약 권한 위임은 군대, 기업, 은행 등의 계층 그룹에서 자연스럽게 발생할 수 있다. 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 허용함으로써 대리서명자들이 동적으로 구성될 수 있는 새로운 멀티 대리서명 프로토콜을 제안한다. 한 명의 대리서명자가 아닌 복수의 대리서명자가 모여야만 원 서명자를 대신해 하나의 유효한 대리서명을 생성할 수 있게 함으로써, 보다 강화된 안전성을 제공한다. 대리서명 생성을 위한 권한 위임은 비밀분산법과 Diffie-Hellman 문제에 의해 생성된 위임티켓을 통해, 계층 구조의 상위 계층에서 하위 계층으로 이루어진다. 위임받은 대리서명자 중에서 대리서명에 참여할 수 없는 대리서명자는 다시 자신의 하위 계층의 참가자들에게 개별 위임을 수행함으로써, 대리서명 권한이 반복적으로 위임될 수 있고, 이에 따라 대리서명자 그룹이 동적으로 구성된다.

키워드 : 대리서명, 계층 그룹, 권한 위임, 비밀분산법

Abstract Proxy signatures is a signature scheme that an original signer delegates one's signature capability to a proxy signer, and then the proxy signer creates a signature on behalf of the original signer. Delegation of authority is a common practice in the real world, in particular, it happens naturally in hierarchical groups such as company, bank and army, etc. In this paper, we propose a new dynamic multi-proxy signature scheme allowing repetitive delegations in a hierarchical group. We adopt multi-proxy signatures to enhance the security of proxy signature. In multi-proxy signatures, plural proxy signers can generate a valid proxy signature collectively on behalf of one original signer. In our scheme, the proxy group is not fixed but constructed dynamically according to some situations. Delegations are processed from higher level to lower level in the hierarchy using delegation tickets. When the original signer wants to delegate one's signature authority, the original signer generates a delegation ticket based on secret sharing and Diffie-Hellman problems. The delegation ticket is shared among proxy signers and then all the proxy signers can generate a valid proxy signature collectively by reconstructing the original signer's delegation ticket. If a certain proxy signer can not attend the proxy signature generating protocol, the proxy signer can also delegate repetitively his partial signature authority to the lower level participants, and then the proxies are constructed dynamically.

Key words : Proxy Signature, Hierarchical Group, Delegation, Secret Sharing

1. 서 론

인터넷을 이용한 전자 상거래(electronic commerce)의 활용이 급속도로 증가함에 따라, 개인 프라이버시 및 정보 보안을 위한 암호 기술의 사용이 보편화되고 있고, 특히, 사용자 인증(authorization)을 위한 전자서명(digital signature)이 널리 활용되고 있다. M. Mambo, K.

† 비 회 원 : 이화여자대학교 컴퓨터학과
soyoung@ewha.ac.kr
†† 종신회원 : 이화여자대학교 컴퓨터학과 교수
shlee@ewha.ac.kr
논문접수 : 2003년 4월 17일
심사완료 : 2004년 5월 13일

Usuda와 E. Okamoto에 의해 처음 제안된 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). 또한, 위임받지 않은 대리서명자는 유효한 대리서명을 생성할 수 없어야 하고(unforgeability), 대리서명자는 대리서명 생성 후에 서명 사실을 부인할 수 없어야 한다(undeniability)[1].

권한 위임은 군대, 기업, 은행 등의 계층 그룹에서 계층간에 자연스럽게 발생할 수 있다. B2B 전자 거래 및 전자 서명의 활용 범위가 다양화됨에 따라 이를 반영할 수 있는 보다 안전하고 효율적인 대리서명이 요구된다. 본 논문에서는 계층 그룹에서 반복적 권한 위임을 허용함으로써 대리서명자들이 동적으로 구성될 수 있는 새로운 멀티 대리서명 프로토콜을 제안한다. 본 논문에서의 "동적"이라는 의미는 서명 생성을 위한 서명자 그룹이 상황에 따라 유동적으로 구성될 수 있음을 의미한다. 서명 생성은 복수의 서명자를 가정함으로써 보다 강화된 안전성을 제공한다. 복수의 서명자를 갖는 서명 스킴은 크게 임계 암호(threshold cryptography)[2]를 바탕으로 한 임계 서명 스킴(threshold signature scheme)[3,4]과 멀티 서명 스킴[5,6]으로 구분될 수 있다. 임계 서명은 사전 정의된 임계값 t에 따라서 t명 이상의 서명자가 모이면 하나의 유효한 서명을 생성할 수 있지만, 기본적으로 서명자의 익명성을 보장하므로 생성된 서명으로부터 각 서명자의 신원을 검증할 수는 없다. 반면, 멀티 서명은 임의의 서명자 그룹의 각 서명자들이 자신의 키를 이용하여 부분 서명을 생성하고, 생성된 부분 서명들이 모여 하나의 유효한 서명이 생성되기 때문에 생성된 멀티 서명으로부터 각 서명자의 신원을 확인할 수 있다.

본 논문에서는 비밀분산법 및 Diffie-Hellman 문제를 이용하여 원서명자와 대리 서명자간에 보다 효율적으로 권한 위임을 수행할 수 있는 멀티 대리 서명 스킴을 제안한다. 서명자 그룹은 n명의 참가자로 구성된 계층 그룹을 가정한다. 한 참가자가 자신의 서명을 생성할 수 없으면, 하위 레벨 참가자들에게 서명권한을 위임할 수 있고 위임받은 하위 레벨 참가자들은 상위 레벨 참가자를 대신하여 대리서명을 생성할 수 있다. 실질적인 권한 위임은 위임티켓(delegation ticket)[7]의 생성 및 분배를 통해 이루어진다. 원 서명자가 생성한 위임티켓은 비밀분산법(secret sharing scheme)[7]과 Diffie-Hellman 키 교환 프로토콜[8]에 의해 대리서명자들간에 공유되고, 이렇게 공유된 정보를 위임티켓 공유정보라고 한다. 특히, 제안하는 방법에서는 Diffie-Hellman 문제를 이용하여 정보 공유를 위한 안전한 비밀채널에 대한 가정 없이 오픈 네트워크 채널 상에서 대리서명자들이 안전하게 위임티켓 정보를 공유할 수 있다. 각 대리서명자들은 자신의 위임티켓 공유정보와 비밀키-공개키 쌍을 이용하여 부분 대리서명(partial proxy signature)을 생성하고, 생성된 부분 대리서명들이 모두 모이면, 원 서명자의 위임티켓이 복원됨과 함께 하나의 유효한 대리서명이 생성된다.

본 논문에서 제안하는 프로토콜의 또 한가지 주요한 성질은 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 있고, 이에 따라 대리서명자 그룹이 동적으로 구성된다.

본 논문의 2장에서는 관련 연구를 제시하고, 3장과 4장에서 계층 그룹에서 반복적 권한 위임을 허용하는 임계 대리서명 프로토콜에 대해 구체적으로 설명한 후, 5장에서 분석을 하고 6장에서 결론을 맺는다.

2. 관련 연구

Zhang은 임계서명을 바탕으로한 임계 대리서명[9]을 제안하였다. 대리 서명자 그룹 $P=\{P_1, P_2, \ldots, P_n\}$에 대해서, 각 대리 서명자는 자신의 부분 대리 서명 키를 생성하고, 사전 정의된 임계값 t에 대해서, t개 이상의 부분 대리 서명 키가 모이면, 하나의 유효한 대리서명 키가 생성된다. 그러나 Zhang의 스킴은 서명자의 신원 확인성(identifiablitiy)를 제공하지 않는다. 누구라도 t명 이상의 서명자가 모이면 하나의 대리 서명 키를 생성할 수 있기 때문에, 생성된 대리 서명으로부터 서명자의 신원을 확인할 수는 없다. Sun, Lee, Hwang은 Zhang의 스킴을 개선하여 부인 방지 기능을 갖는 임계 대리서명 스킴[10]을 제안하였다. Hwang, Lin, Lu도 개선된 임계 대리서명 스킴[11]을 제안하였으나, 이들 스킴은 취약성을 갖는다[12]. 무엇보다, 위에서 언급된 임계 대리서명 스킴들은 서명 키 생성에 필요한 특정 정보가 참가자간에 비밀스럽게 공유되어야 하기 때문에 참가자간에 안전한 비밀 채널이 있다고 가정한다. 또한, 많은 브로드캐스팅과 공개 정보를 생성하여 유지하여야한다. Lee, Cheon, Kim은 비밀 채널의 사용을 없애기 위해 서명된 보증 정보를 이용한 대리 서명 스킴[13]을 제안하였으며, 본 논문에서 제안하는 스킴도 일종의 수정된 보증 정보를 이용하여 비밀 채널의 가정을 제거하였다.

멀티 서명의 기본 개념은 Itakura와 Nakamura[5]에 의해 처음 소개 되었다. 서명자 그룹 $G=\{P_1, P_2, \ldots, P_L\}$에 대해서, 서명자의 부그룹 $S \subset G$의 모든 서명자들이 모여서 하나의 서명을 생성한다. Micali, Ohta, Reyzin은 Accountable Subgroup Multisignatures(ASM)[6]을 통해 멀티서명 모델을 정형화하였다. 멀티 대리서명은 [14]에서 처음 제안되었고, 그 밖에 여러 다른 멀티 대리서명 스킴들이 [15,16,17]에서 제안되었는데, 제안된 스킴들은 모두 고정된 대리 서명자 그룹을 가정한다. 특히, Lal과 Awasthi의 스킴[16]은 원 서명자가 대리 서명자의 부분 대리서명을 위조할 수 있다는 취약성이 있고, Lin, Wu, Hwang의 스킴[17]은 대리 서명 키 생성을 위해 비밀 채널을 가정한다. 이외에 다른 접근 구조를 갖는 multi-proxy multisignature[18] 스킴과 proxy-multi signature 스킴[19,20,21]들이 제안되었다. multi-proxy multisignature 스킴은 다수의 원 서명자 그룹의 모든 참가자들의 동의 하에 다수의 대리 서명자 그룹에게 대리 서명 권한을 위임하는 프로토콜인 반면, proxy-multi signature 스킴은 다수의 원 서명자 그룹의 동의 하에 한 명의 대리 서명자에게 그들의 서명 권한을 위임하는 프로토콜이다.

3. 제안 모델

제안하는 스킴은 유한체 상에서의 이산대수 문제의 어려움에 기반한다. 본 절에서는 참가자들의 계층 구조와 위임구조에 대해 설명한 후, 위임받은 대리 서명자 그룹이 하나의 멀티 대리서명을 생성하는 과정과 반복적 원한 위임에 대해서 설명한다. 먼저, n명의 참가자 집합은 $P=\{P_1, P_2, \ldots, P_n\}$이고, 참가자들은 각 참가자들을 노드(node)로 하고 차수(degree)가 2이상인 트리(tree) 형태의 계층 구조를 이룬다고 가정한다. 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, 부트리 T_i의 단말노드들은 다시 $c_{i1}, \ldots, c_{it_i}$로 표기된다. P_i는 위임티켓을 사용하여 자신의 서명 권한을 자식 노드에 해당하는 참가자 $c_{i1}, \ldots, c_{it_i}$들에게 위임할 수 있고, 이 중에서 서명에 참여할 수 없는 대리서명자는 다시 자신의 자식 노드에 해당하는 참가자들에게 개별 위임을 수행할 수 있다. 이와 같이 대리서명 권한은 계층 트리를 따라 단말노드에 해당하는 참가자들에게까지 반복적으로 위임될 수 있고, 대리서명자 그룹이 동적으로 구성된다. 그리고, 최종적으로 권한을 위임받은 모든 대리서명자들이 모이면 하나의 유용한 대리서명을 생성할 수 있다. 다음 그림 1은 계층 구조 및 권한 위임 구조를 표현한 예이다.

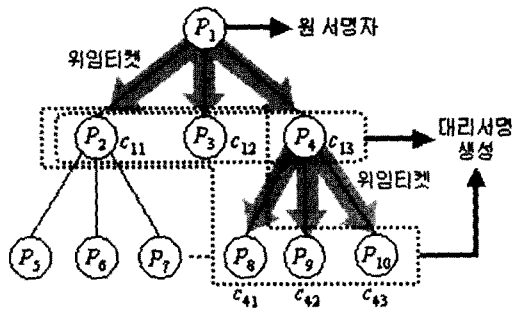

그림 1 계층 구조 및 권한 위임 구조

각 참가자들은 유한체(finite field)상에서의 이산대수 문제[8]에 기반한 비밀키와 공개키 쌍을 보유하고 있고, 모든 참가자들간에는 서로 데이타를 송·수신할 수 있는 네트워크 채널(channel)이 형성되어 있다고 가정한다. 네트워크 채널은 안전하지 않다(insecure)고 가정하며, 도청자(attacker)는 네트워크 채널 상에서 전송되는 모든 정보를 읽을 수 있고 이를 위·변조할 수 있다. 본 프로토콜에서 사용되는 주요 파라미터(parameter)는 다음 (표 1)과 같다.

표 1 주요 파라미터

p, q	매우 큰 두 소수, $\|p\| \geq 512$ bit, $q \mid (p-1)$
g	$g \in Z_p$, $g^{p-1} \equiv 1 \bmod p$, 생성자로서 유한체 $GF(p)$ 상에서의 원시근
$<xp_i, yp_i>$	$xp_i \in Z_p$, $yp_i = g^{xp_i} \bmod p$ P_i의 비밀키-공개키 쌍
t_i	$t_i \geq 2$이거나 $t_i = 0$, P_i의 자식노드 개수(P_i를 대신하는 대리서명자 수)
S_i	P_i가 지정한 대리 서명자 서브 그룹
dk_i	P_i가 권한 위임 시에 발행하는 위임티켓
m	메시지
H	암호학적 일방향 해쉬 함수

4. 멀티 대리서명 프로토콜

n명의 참가자로 구성되는 계층그룹에서 비밀분산법과 Diffie-Hellman 문제를 바탕으로 원 서명자와 대리서명자들이 효율적으로 위임티켓을 생성하여 공유하고, 계층 트리를 따라 반복적 권한 위임을 수행하는 방법을 설명한다. 만약 참가자 P_i가 자신의 서명권한을 위임하고자 하면, 앞 절에서 설명된 계층 구조에 따라서, P_i는 자신의 자식노드에 해당하는 참가자들에게 권한을 위임할 수 있다. 여기서 원 서명자를 P_i라고 하고 자식노드에 해당하는 대리서명자들을 대리 서명자 서브 그룹 $S_i=\{c_{i1},\ldots,c_{it_i}\}$라고 한다. P_i는 위임티켓을 생성하여 $c_{i1},\ldots,c_{it_i}$들에게 서명 권한을 위임하고, $c_{i1},\ldots,c_{it_i}$들은 모두 모여 하나의 유효한 대리서명을 생성할 수 있다. 제안하는 방법은 크게 권한 위임을 위한 위임티켓 생성 단계, 대리서명 생성 및 검증 단계 그리고 반복적 권한 위임 단계로 구분된다. 모든 연산은 유한체 $GF(p)$ 상에서 수행된다. 이후 본 논문의 수식에서 mod p는 생략한다.

4.1 위임티켓 생성

실질적인 권한 위임은 위임티켓의 생성과 분배에 의해 수행된다. 위임티켓은 원 서명자 P_i가 대리서명자 $c_{i1},\ldots,c_{it_i}$를 지정하기 위해 권한 위임 시, 임의로 생성하는 정보이다. P_i가 생성하는 위임티켓은 dt_i로 표기하고, dt_i는 (t, t)-임계 스킴[7]에 의해 t_i개의 위임티켓 공유정보로 나뉘어져서 $c_{i1},\ldots,c_{it_i}$들 사이에서 공유된다. $c_{i1},\ldots,c_{it_i}$들은 대리서명 생성 시에 원 서명자와 동일한 위임티켓을 복원할 수 있다. $j=1,\ldots,t_i$에 대해서, 각 대리서명자 c_{ij}에게 공유되는 위임티켓 공유정보는 dt_{ij}로 표기한다.

P_i는 t_i개의 랜덤 값 $rs_{i1}, rs_{i2},\ldots, rs_{it_i}\in Z_p$를 선택한 다음, $c_{i1},\ldots,c_{it_i}$들의 위임티켓 공유정보 $dt_{i1}, dt_{i2},\ldots, dt_{it_i}$를 다음과 같이 생성한다. 단, yc_{ij}는 c_{ij}의 공개키이다.

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

결과적으로, P_i가 생성하는 위임티켓 dt_i는 $dt_i=\sum_{j=1}^{t_i} dt_{ij}$ 이다. P_i는 dt_i에 해당하는 공개 정보 $DT_i=g^{dt_i}$와 이에 대한 서명 $<R_i, Sig_i>$를 다음과 같이 생성한다.

$$R_i=g^{rs_{i1}+rs_{i2}+\cdots+rs_{it_i}} \mod p,$$

$$Sig_i=H(DT_i, R_i)\cdot xp_i+\sum_{j=1}^{t_i} rs_{ij} \mod q.$$

P_i는 $dt_{i1}, dt_{i2},\ldots, dt_{it_i}$를 대리서명자에게 분배하지 않고 $<DT_i, R_i, Sig_i>$를 공개한다.

4.2 대리서명 생성 및 검증

원 서명자로부터 위임 정보를 건네 받은 대리서명자들은 자신의 위임티켓 공유정보를 생성한 후, Schnorr 서명 스킴[22]에 기반하여 부분 대리서명 $\sigma_{ij}=<pa_j, pr_j, ps_j>$을 생성한다. 각 대리서명자가 생성한 부분 대리서명이 모여 하나의 유효한 대리서명이 생성된다. 대리서명자 c_{ij}가 자신의 부분 대리서명을 생성하는 과정은 다음 (표 2)와 같다. 단, 원 서명자 P_i의 비밀키-공개키 쌍은 $<xp_i, yp_i>$이고, 대리서명자 c_{ij}의 비밀키-공개키 쌍은 $<xc_{ij}, yc_{ij}>$이다.

Diffie-Hellman 키 교환 프로토콜에 기반하여, 각 대리서명자 c_{ij} 들은 자신의 비밀키를 이용하여 자신의 위임티켓 공유정보 dt_{ij}를 생성할 수 있다. 물론, 대리서명자들은 자신이 생성한 위임티켓 공유정보가 정확한 정보인지, 원 서명자가 각 대리서명자에 대해 생성한 것과 동일한지 검증할 수 있다. 제안하는 방법에서는, 각 대리서명자가 주어진 메시지 m에 대해서 부분 대리서명 키가 아닌 부분 대리서명을 생성한다. 따라서, 기존의 방법에서 대리서명자들이 각자의 부분 대리서명 키를 생성한 후 다시 대리서명자들이 단합하여 대리서명을 생성하는 비효율성을 제거하였다. 또한, 각 대리서명자들의 비밀키-공개키 쌍을 이용하여 부분 대리서명을 생성함으로써, 서명에 대한 책임을 지게 되고, 생성된 대리 서명으로부터, 각 대리서명자의 신원을 검증할 수 있다.

대리서명자 $c_{i1},\ldots,c_{it_i}$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 대리서명자들의 공개키와 원 서명자가 공개한 위임티켓 공개정보 DT_i에 의해 검증된다. 먼저, 원 서명자의 위임티켓을 다음의 식을 통해 검증할 수 있다.

$$g^{Sig_i}\equiv(yp_i)^{H(DT_i, R_i)}\cdot R_i$$

그리고, 다음의 두 식이 만족하면, 생성된 대리 서명은 정당하다고 검증할 수 있다.

$$PR=DT_i\ ,$$

$$g^{PS}=(yc_{i1}\cdots yc_{it_i})^e\cdot PA\cdot PR$$

4.3 반복적 권한 위임

대리서명 권한은 계층 트리 상에서 하위 계층의 참가자들에게로 반복적으로 위임될 수 있다. 즉, 권한을 위임받은 대리서명자들 중에서 대리서명 생성에 참여할 수 없는 대리서명자는 자신의 부분 대리서명 권한을 자

표 2 부분대리서명 생성 프로토콜

P_i		대리서명자 c_{ij}
$k_j = H(dt_{ij}, S_i) \cdot xp_i + rs_{ij} \bmod q$ $RS_j = g^{rs_{ij}} \bmod p$	$< k_j, RS_j, S_i >$ ---------->	위임티켓 공유정보 dt_{ij} 생성 $dt_{ij} = (RS_j)^{xc_{ij}} = g^{rs_{ij} \cdot xc_{ij}}$ $g^{k_j} \equiv (yp_i)^{H(dt_{ij}, S_i)} \cdot RS_j$ 인가 검증 만족하면, 부분 대리서명 $\sigma_{ij} = < pa_j, pr_j, ps_j >$ 생성 $a_j \in Z_p$ 랜덤하게 생성 $l_j = a_j + dt_{ij} \bmod q$ $pa_j = g^{a_j} \bmod p$ $pr_j = g^{dt_{ij}} \bmod p$ pa_j, pr_j를 S_i에 포함된 모든 다른대리서명자들에게 브로드캐스팅 한 후, PA, PR을 다음과 같이 생성: - $PA = \prod pa_j, PR = \prod pr_j$ for $j = 1, \ldots, t_i$ - $PR \equiv DT_i$ 인가 검증 $e = H(PA, PR, m, S_i)$ $ps_j = e \cdot xc_{ij} + l_j \bmod q$

신의 자식노드에 해당하는 대리서명자들에게 반복적으로 위임할 수 있다. 원 서명자 P_i의 대리서명자 $c_{i1}, \ldots, c_{it_i}$ 중에서 대리서명에 참여할 수 없는 대리서명자 c_{ij}를 P_j라고 하자. 참가자 P_j는 자신을 루트로 하는 부트리 T_j의 위임구조에 따라 자신의 자식 노드에 해당하는 대리서명자들 $c_{j1}, \ldots, c_{jt_j}$에게 P_j의 부분 대리서명 권한을 위임할 수 있다. P_j는 다음의 위임티켓 생성과정을 통해 부분 대리서명 권한을 위임한다.

P_j가 자신의 대리 서명자들에 대한 위임티켓을 생성하기 전에, P_j는 먼저 대리 서명자 그룹 정보 S_j를 자신의 대리 서명자들을 포함하는 $S_j = \{c_{j1}, c_{j2}, \ldots, c_{ij-1}, c_{ij+1}, \ldots, c_{it_i}, c_{j1}, \ldots, c_{jt_j}\}$로 갱신한 후, 기존의 다른 서명자들 $c_{j1}, c_{j2}, \ldots, c_{ij-1}, c_{ij+1}, \ldots, c_{it_i}$에게 전송한다. P_j를 제외한 기존의 다른 서명자들은 서명자 그룹 정보 S_i를 S_j로 수정하기만 하면 된다.

이제 P_j는 자신의 대리 서명자들에 대한 위임 티켓을 생성한다. P_j가 $c_{j1}, \ldots, c_{jt_j}$들을 위해 생성하는 위임티켓 dt_j는 P_j가 P_i에 대해 생성한 위임티켓 공유정보 dt_{ij}와 동일하다. dt_j를 $c_{j1}, \ldots, c_{jt_j}$들 사이에서 공유시키기 위해서, P_j는 t_j개의 랜덤 값 $rs_{j1}, rs_{j2}, \ldots, rs_{jt_j} \in Z_p$를 선택한 다음, $c_{j1}, \ldots, c_{jt_j}$들이 공유할 위임티켓 공유정보 $dt_{j1}, dt_{j2}, \ldots, dt_{jt_j}$를 다음과 같이 생성한다. 단, yc_{jl}는 c_{jl}의 공개키이다.

$$dt_{jl} = (yc_{jl})^{rs_{jl}}, l = 1, \ldots, t_j$$

그리고, P_j는 부가적으로 공개 위임티켓 공유정보 pdt_j를 다음과 같이 생성한다.

$$pdt_j = dt_j - \sum_{l=1}^{t_j} dt_{jl}$$

P_j는 위임티켓 dt_j의 공개 정보 g^{dt_j}를 생성한 후, $< DT_j, pdt_j >$를 서명하여 공개한다.

이제, 갱신된 S_j에 포함된 모든 대리서명자들이 모여 멀티 대리 서명을 생성한다. S_j에 포함되는 각 대리서명자 c_k는 4.2절의 표 2에 설명된 것과 동일한 방법으로 자신의 부분 대리서명 $< pa_k, pr_k, ps_k >$를 생성한다. 모든 대리서명자들은 먼저 자신의 위임티켓 공유정보를 생성한 후, 자신의 비밀 랜덤 값을 선택하여 pa_k와 pr_k

를 생성한다. 그런 다음, pa_k와 pr_k를 S_j의 다른 대리 서명자들에게 전송한 후, PA와 PR을 생성한다. 그러나, 반복적 권한 위임에서는 PA와 PR를 다음과 같이 생성한다.

$$PA = \prod_{k \in S_j} pa_k \ , \quad PR = \left(\prod_{k \in S_j} pr_k \right) \cdot g^{pdt_j}$$

마지막으로, 모든 대리 서명자들은 갱신된 서브 그룹 정보 S_j를 이용하여 표 2에 기술되어 있는 대로 ps_k를 생성하여 부분 대리 서명을 완성한다. 결국, 갱신된 대리 서명자들이 생성한 멀티 대리 서명은 $<PA, PR, PS>$이고, $PS = \left(\sum_{k \in S_j} ps_k \right) + pdt_j$이다.

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 $c_{j1}, \ldots, c_{jt_j}$들이 모여 원 서명자 P_i의 대리서명을 생성할 수 있고, 생성된 대리서명은 대리서명에 참가한 대리서명자들의 공개키를 이용하여 검증할 수 있다. 권한 위임은 위와 같은 방법으로 단말 노드의 참가자들에게까지 반복적으로 위임될 수 있고, 대리서명자들이 동적(dynamic)으로 구성될 수 있다.

5. 분 석

제안하는 방법은 기존의 대리서명 프로토콜이 만족해야 하는 안전성과 부인 방지기능[1]을 만족함과 동시에 반복적 권한 위임을 허용하고, 다수의 대리서명자를 가정함으로서 대리서명의 안전성이 보다 강화되었다. 권한 위임을 위한 위임티켓 생성 및 전송 단계에서는 Diffie-Hellman 문제[8]를 이용함으로써, 참가자들간 안전한 비밀 채널의 가정 없이, 원 서명자와 대리서명자가 동일한 위임티켓 정보를 공유한다. 프로토콜 수행의 각 단계에서 원 서명자 및 대리서명자들은 상호간의 위임 정보 및 서명 정보를 검증할 수 있으므로, 오용 및 악의적인 사용을 발견하고 방지할 수 있다.

제안하는 프로토콜의 기본적인 안전성은 매우 큰 소수에 대한 유한체 상에서의 이산대수 문제의 어려움[8]에 근거한다. 원 서명자 P_i와 대리서명자 $c_{i1}, \ldots, c_{it_i}$들은 Diffie-Hellman 키 교환 방식에 따라 동일한 위임티켓 공유정보를 공유하므로, 원 서명자는 위임 사실을 부인할 수 없고, 원 서명자로부터 위임 정보 $RS_j = g^{rs_{ij}}$를 받지 않은 대리서명자들은 정당한 위임티켓 $dt_{ij} = (RS_j)^{xc_{ij}} = g^{rs_{ij} \cdot xc_{ij}}$을 생성할 수 없다. 또한 악의적인 대리서명자들이 원 서명자의 위임티켓을 위조하는 것도 불가능하다. 대리서명자들이 악의적으로 모두 단합하여 임의의 랜덤 값 $rs_1', \ldots, rs_{t_i}'$을 선택하고 $RS_1', \ldots, RS_{t_i}'$를 생성하여, 이로부터 새로운 위임티켓 공유정보 $dt_{ij}' = (RS_j')^{x_{c_{ij}}}$를 생성할 수 있다하여도, 원 서명자의 비밀키를 모르기 때문에 새롭게 생성한 위임티켓 공유정보에 상응하는 $k_1', \ldots, k_{t_i}'$를 생성할 수 없으므로 위임티켓의 위조가 불가능하다. 즉, 악의적인 대리서명자들이 임의로 위임티켓을 위조하여 사용했을 경우, 원 서명자에 의해 발행된 위임티켓이 아님이 검증될 수 있다. 정당한 대리서명자들은 자신이 생성하는 위임티켓의 정확성을 원 서명자 P_i의 공개키를 이용하여 등식 $g^{k_j} = (yp_i)^{dt_{ij}} \cdot RS_j$ 의 성립 여부로 검증할 수 있다.

각 대리서명자들의 부분 대리서명 $< pa_j, pr_j, ps_j >$은 Schnorr 서명 스킴[22]에 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 대리서명자가 생성한 부분 대리서명 $< pa_j, pr_j, ps_j >$는 각 대리서명자들의 공개키 yc_{ij} 및 공개 위임티켓 공유정보 $pr_j = g^{dt_{ij}}$를 이용하여 등식 $g^{ps_j} = (yc_{ij})^e \cdot pa_j \cdot pr_j$의 성립 여부로 검증될 수 있다. 위임받은 모든 대리서명자들의 부분 대리서명이 모여야만 정당한 하나의 대리서명 $< PA, PR, PS >$가 생성될 수 있고, 생성된 대리서명은 다음의 등식을 만족한다.

$$PA = \prod_{j=1}^{t_i} pa_{c_{ij}} \ , \quad PR = \prod_{j=1}^{t_i} pr_j = DT_i = g^{dt_i} \ ,$$

$$PS = \sum_{j=1}^{t_i} ps_j = e(x_{c_{i1}} + \cdots + x_{c_{it_i}}) + (a_1 + \cdots + a_{t_i}) + dt_i$$

생성된 대리서명은 각 대리서명자의 공개키와 원 서명자가 공개한 위임티켓 공개정보 DT_i에 의해 검증될 수 있다. 그러나, dt_i는 (t, t)-임계 스킴에 의해 대리서명자들에게 공유되므로, 부분 대리서명이 하나라도 부족하게 되면, 원 서명자가 생성한 위임티켓 dt_i를 완전하게 복원할 수 없기 때문에, 검증 가능한 정당한 대리서명을 생성할 수 없다[7].

제안하는 프로토콜은 대리서명 생성을 위한 반복적 권한 위임을 허용한다. 서명 권한을 위임받은 대리서명자들 중에서 대리서명에 참여할 수 없는 대리서명자는 다시 자신의 서명 권한을 계층 트리 상의 자식 노드 참가자들에게로 위임할 수 있으며, 이 경우 상위 대리서명자는 자신의 부분 대리서명권한을 하위 대리서명자들에게 위임한다. 즉 위임받은 하위 대리서명자들은 상위 대리서명자의 위임티켓 공유정보를 복원함으로써 상위 대리서명자의 부분 대리서명 역할을 대신한다. 상위 대리서명자의 위임티켓 공유정보는 비밀분산법에 기반해서

하위 대리서명자들에 의해 공유되고, 이러한 위임과정은 최하위 계층의 참가자들에게까지 반복적으로 수행될 수 있다. 그러나 위임받은 대리서명자가 다시 반복적 권한 위임을 수행하는 경우에는 공개 위임티켓 공유정보를 부가적으로 생성하므로, 반복 위임의 회수가 증가할수록 공개 위임티켓 공유정보의 개수도 증가한다. 공개 위임티켓 공유정보는 위임받은 대리서명자들이 상위 대리서명자의 위임티켓 공유정보를 복원할 수 있기 위한 부가정보로, 공개 위임티켓 공유정보만으로는 위임티켓에 대한 어떠한 정보도 획득할 수 없다.

다음 (표 3)은 기본 대리서명 스킴, 임계 대리서명 스킴, Lin, Lu, Hwang의 멀티 대리서명 스킴과 본 논문에서 제안한 멀티 대리서명 스킴을 간략히 비교한 표이다.

제안된 스킴은 공개 네트워크 채널 상에서, 한 사람의 대리 서명자를 가정하는 기본 대리서명 스킴의 서명 길이와 검증 시간을 벗어나지 않는 범위에서 대리서명자의 신원을 확인 할 수 있으며, 대리서명자들이 동적으로 구성되는 멀티 대리서명 스킴이다. (표 3)에서 서명 길이와 검증 시간 항목은 한 명의 서명자를 가정하는 기본 대리 서명의 서명 길이와 검증 시간을 1로 두었을 때, 상대적인 값을 나타낸 것이다. α값은 서명자의 수에 따라 증가하는 값이나, 지수 연산을 기본 연산인 1로 하였을 때, 이 보다는 훨씬 작은 값이다. 각 서명자는 자신의 키를 이용하여 부분 대리서명을 생성한 후, 이들을 모아 대리서명을 생성하므로, 임계 대리서명과 같이 대리서명 키를 생성한 다음, 다시 생성된 키를 이용하여 서명을 생성하는 부가 연산을 피할 수 있다.

6. 결 론

인터넷을 통한 전자상거래의 활성화와 함께 개인 프라이버시 및 정보 보안이 주요 문제로 부각됨에 따라, 안전한 전자상거래를 위한 다양한 암호 기술들이 요구되고 있다. 공개키 기반 구조를 이용한 전자서명은 사용자 인증을 위한 기본 암호 기술 중의 하나로써, 현재 가장 보편적으로 사용되고 있다. 전자서명의 이용 분야가 다양화됨에 따라, 이를 응용한 여러 암호 기술이 요구되며, 이 중의 하나가 대리서명이다.

본 논문에서는 계층 그룹에서 반복적 권한 위임을 허용함으로써 대리서명자 그룹이 동적으로 구성되는 임계 대리서명 프로토콜을 새롭게 제안하였다. 계층 그룹 내에서 계층간 권한 위임을 통해 대리서명이 수행되고, 대리서명은 복수의 대리서명자가 모여야만 생성할 수 있도록 함으로써, 대리서명의 안전성을 강화시켰다. 제안하는 방법은 대리서명이 만족해야 하는 기본적인 안전성 및 부인 방지 기능을 만족한다. 권한 위임은 비밀분산법과 Diffie-Hellman 문제에 의해 생성된 위임티켓을 통해 이루어지며, 원 서명자와 대리서명자들은 동일한 위임티켓 정보를 공유한다. 즉, 위임받은 대리서명자들은 모두 모여야만 원 서명자와 동일한 위임티켓을 복원할 수 있고, 이로부터 정당한 대리서명을 생성할 수 있다. 특히, 제안하는 방법에서는 Diffie-Hellman 문제[8]를 이용하여 원 서명자와 대리서명자가 보다 안전하고 효율적으로 위임티켓을 생성하고 공유한다. 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 Transaction 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," in Advances in Cryptology-EUROCRYPT '96, LNCS 1070, 1996.

표 3 기존 스킴과의 비교

구분	기본 대리서명 스킴	임계 대리서명 스킴	Lin, Lu, Hwang의 멀티 대리서명 스킴	제안한 멀티 대리서명 스킴
기본 요구사항 (위조 및 부인 방지)	O	O	O	O
대리서명자 확인	O	X	O	O
서명 길이	1	1	1	1
서명 검증 시간	1	1	$1 + \alpha$	$1 + \alpha$
네트워크 채널	공개 채널	비밀 채널 필요	비밀 채널 필요	공개 채널
서명자 그룹	-	고정	고정	동적
서명 생성 방식	대리서명 키 생성	대리서명 키 생성	부분 대리서명 생성	부분 대리서명 생성

[4] C. Li, T. Hwand and N. Lee, "(t, n)-Threshold Signature Scheme based on Discrete Logarithm," in Advances in Cryptology-EUROCRYPT '94, 1995.
[5] K. Itakura and K. Nakamura, "A Public-Key Cryptosystem Suitable for Digital Multisignatures," NEC Research and Development, (71), pp. 1-8, 1983.
[6] S. Micali, K. Ohta and L. Reyzin, "Accountable-Subgroup Multisignatures," Proceeding of ACM Conference on Computer and Communications Security, pp. 245-254, 2001.
[7] 송영원, 박소영, 이상호, "트리형태의 계층 구조에 적용가능한 비밀분산법의 설계", 한국정보과학회 논문지 (컴퓨터 시스템 및 이론), 제29권 4호, pp. 161-168, 2002.
[8] W. Diffie and M. E. Hellman, "New Directions in Cryptography," IEEE Transaction on Information Theory, vol. IT-22, no. 6, pp. 644-654, 1976.
[9] K. Zhang, "Threshold Proxy Signature Schemes," Proceeding of 1st International Information Security Workshop, pp. 191-197, 1997.
[10] H. Sun, N. Lee and T. Hwang, "Threshold Proxy Signatures," Proceeding of IEE - Computers and Digital Techniques, vol. 146, no. 5, pp. 259-263, 1999.
[11] M. Hwang, I. Lin and E. J. Lu, "A Secure Nonrepudiable Threshold Proxy Signature Scheme with Known Signers," Informatica, vol. 11, no. 2, pp. 137-144, 2000.
[12] S. Hwang and C. Chen, "Cryptanalysis of Nonrepudiable Threshold Proxy Signature Schemes with Known Signers," Informatica, vol. 14, no. 2, pp. 205-212, 2003.
[13] J. Lee, J. Cheon and S. Kim, "An Analysis of Proxy Signatures: Is a Secure Channel Necessary?," Proceeding of CT-RSA 2003), LNCS 2612, pp. 68-79, 2003.
[14] S. Hwang and C. Shi, "A Simple Multi-Proxy Signature Scheme," Proceeding of the Tenth National Conference on Information Security, Hualien, Taiwan, pp. 134-138, 2000.
[15] X. Chen, F. Zhang and K. Kim, "ID-Based Multi-Proxy Signature and Blind Multisginature from Bilinear Pairings," Proceeding of KIISC conference 2003, pp. 11-19, 2003.
[16] S. Lal and A. Awasthi, "A New Multi-Proxy Signature Scheme for Partial Delegation with Warrant," http://www.gfcr.org/ecryp/old/multi.pdf.
[17] C. Lin, T. Wu and J. Hwang, "Multi-Proxy Signature Schemes for Partial Delegation with Cheater Identification," Institute of Information Management, NCTU.
[18] S. Hwang and C. Chen, "New Multi-Proxy Multi-Signature Schemes," Applied Mathematics and Computation, Vol. 147, pp. 55-67, 2004.
[19] S. Hwang and C. Chen, "A New Proxy Multi-Signature Scheme," International Workshop on Cryptology and Network Secrity, Taipei, Taiwan, pp. 199-204, 2001.
[20] H. Sun, "On Proxy (Multi-) Signature Schemes," 2000 International Computer Symposium, Chiayi, Taiwan, pp. 65-72, 2000.
[21] L. Yi, G. Bai and G. Xiao, "Proxy Multi-Signature Scheme: A New Type of Proxy Signature Scheme," Electronic Letters, Vol. 36, No. 6, pp. 527-528, 2000.
[22] C. P. Schnorr, "Efficient Signature Generation for Smart Cards," in Advances in Cryptology-CRYPTO '89, pp. 239-252, 1990.

박 소 영
1998년 2월 이화여자대학교 컴퓨터학과 학사. 2000년 2월 이화여자대학교 컴퓨터학과 석사. 2000년 3월~현재 이화여자대학교 컴퓨터학과 박사과정. 관심분야는 정보보호, 암호프로토콜, 암호 알고리즘

이 상 호
정보과학회논문지 : 시스템 및 이론
제 31 권 제 6 호 참조