디지털 다중서명 방식을 적용한 전자결재 시스템에 관한 연구

박 희 운† · 강 창 구†† · 이 임 영†††

요 약

본 논문에서는 날로 정보화 되는 환경 하에서 다수의 결재권자들이 존재하는 사무실의 전자결재 시스템에 관해 고찰한다. 먼저 전자결재 시스템의 종류를 분류해 보았으며, 지금까지 개발된 기존의 다중서명 방식들을 이용한 전자결재 시스템을 분석하였다. 또한 새로운 다중서명 방식을 제안하여 이 방식을 전자결재 시스템에 적용시킴과 동시에 기존 방식과의 비교 분석을 통해 본 방식의 장점을 살펴보았다.

본 논문에서는 이산 대수 문제의 어려움에 근거한 디지털 다중서명 방식을 이용하여 전자결재 시스템에 적용한 것으로 통신 횟수 및 기능적 측면에서 기존 방식보다 안정적이므로 전자결재 시스템에 적합한 방식이라 하겠다.

A Study on Digital Multisignature Scheme in Electronic Approval Systems

Hee-Un Park† · Chang-Goo Kang†† · Im-Yeong Lee†††

ABSTRACT

In this study, we propose a new multi-party electronic approval system. We classified and analyzed several existing electronic approval systems which use the multisignature method. Based on the analysis, we developed a new multisignature method and then applied it to several existing electronic approval systems. By comparing various aspects of the new and the conventional methods, we were able to demonstrate the effectiveness of the proposed method.

The new method is based on discrete logarithm so that it lowers the complexity requirement involved in electronic communication and rises the ability requirement, hence makes itself suitable to general electronic approval systems.

1. 서 론

현대 사회의 특징 중 하나는 컴퓨터의 광범위한 보급과 디지털 통신망의 급속한 발전에 힘입어 기존과는 다르게 사무실 내의 모든 여건이 바뀌고 있다. 실 예로, 사무 자동화라든가 재택 근무가 실현되고 있으며, 종이 문서를 사용하는 것 대신에 스크린을 통해 전자화된 문서를 취급하는 전자 사무실이 도래한 것이다. 이와 같은 전자 사무실의 특징을 살펴보면, 기존의 종이 문서에서 사용하던 인감이나 사인 대신에 전자 문서의 인증 및 무결성을 위하여 디지털 서명을 사용한다는 점이다. 이와 같이 전자 문서를 대상으로, 전자화된 사무실에서 디지털 서명을 이용하여 결재를 수행하는 시스템을 전자결재 시스템이라 한다.

따라서 전자화된 사무실 안에서 종이를 대신하는 일련의 여건들은 문서의 결재에 있어 고유성과 독창성

† 준 회 원 : 순천향대학교 대학원 전산학과
†† 정 회 원 : 한국전자통신연구원 부호3팀장 책임연구원
††† 정 회 원 : 순천향대학교 컴퓨터학부 교수
논문접수 : 1998년 8월 12일, 심사완료 : 1998년 12월 18일

및 비밀성을 유지할 수 있는 전자결재가 얼마나 중요하게 사용될지를 자명하게 알려 주는 것이며, 향후 이러한 전자결재 시스템의 구현이 절실히 필요한 상태이다.

전자결재 시스템에서는 여러 사람들을 대상으로 하고 있으며, 이들이 생성해낸 전자 문서를 어떻게 주고받을지, 그리고 얼마나 안전하게 처리할지 등의 문제가 발생한다. 특히, 서로의 얼굴을 보지 않고서 모든 결재 행위를 수행하게 되므로, 제 3자에 의한 문서위조, 네트워크 상에서의 정확한 문서 송신 여부, 그리고 수신자의 부정에 따르는 문제 등과 같이 여러 가지 보안 및 안전에 대한 선결 사항들이 필수적으로 처리되어야 한다.

현재 이에 대한 해결 방안으로 각광을 받고 있는 것 중에 하나가 암호학에 기반을 둔 디지털 서명이 있다. 이는 네트워크 상에서 전자 문서의 교환시 발생할 수 있는 사용자 인증과 전자 문서 인증에 효과적인 해결책을 제시하고 있다. 그러나, 기존의 디지털 서명 방식은 오직 양자간의 통신을 기준으로 만들어져 있다. 따라서, 여러 사람을 대상으로 하는 전자결재 시스템을 위해서는 기존의 디지털 서명으로는 부족하게 되었고, 이를 위해서 그 대상을 n명으로 확대한 디지털 다중서명 방식을 요구하게 되었다. 디지털 다중서명 방식은 전자결재 시스템의 결재 방법에 따라 순차적으로 결재를 수행하는 순차적 다중서명 방식과 무 순서적으로 결재를 수행하는 동시 다중서명 방식 등으로 분류할 수 있다.

지금까지 개발된 디지털 다중서명 방식을 살펴 보면 다음과 같다. RSA 공개키 암호 시스템을 다중서명에 적용한 방식으로 Itakura-Nakamura의 다중서명 방식[8](Itakura-Nakamura 방식)과 Okamoto의 다중서명 방식[9](Okamoto 방식)이 있다. 전자의 방식은 서명 메시지의 길이 증가 및 서명 발생 속도의 문제점을 개선하기 위해 두 개의 큰 소수와 각 서명자에 따른 작은 소수의 곱을 이용하여 RSA 디지털 서명 방식[2]을 직접 확대 적용한 방식이다. 그리고 후자의 방식은 RSA 방식과 같은 전단사(Bijective) 공개키 암호 시스템과 단 방향 함수(One-Way Function)를 이용해 서명 메시지의 길이 증가 및 서명자의 순서 제약성을 극복한 방식이다. 그 외에도 Fiat-Shamir 방식[3,10]에 근거한 방식으로, 서명 속도와 키 관리 방법을 개선시키기 위하여 Ohta와 Okamoto가 제안한 Ohta-Okamoto 다중서명 방식[6](Ohta-Okamoto 방식)과 Ohta-Okamoto 방식에서 통신 횟수를 줄인 Kang-Kim 방식[12] 등이 있다. 또한, 무순차적 동시 결재를 해결하기 위하여 Fiat-Shamir 방식[3,10]에 근거한 방식으로 Brickell-Lee-Yacobi 다중서명 방식[11](Brickell-Lee-Yacobi 방식)과 Brickell-Lee-Yacobi 방식에서 통신 횟수를 줄인 Kang-Kim[12] 방식 등이 있다.

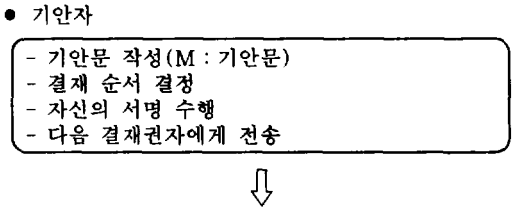
본 논문에서는 기존의 디지털 다중서명 방식들을 전자결재 시스템에 적용시킬 경우 그 종류와 특징을 비교 분석한다. 아울러 이산 대수 문제의 어려움에 근거한 새로운 디지털 다중서명 방식을 제안하여 전자결재 시스템에 적용시켜 보려 한다. 본 방식은 기존의 방식들에 비해 통신 횟수가 적고, 별도의 신뢰된 키 생성 기관(TC : Trusted Center) 및 랜덤수 저장의 필요성을 없앰으로서 효율성을 높이고 있다.[13]

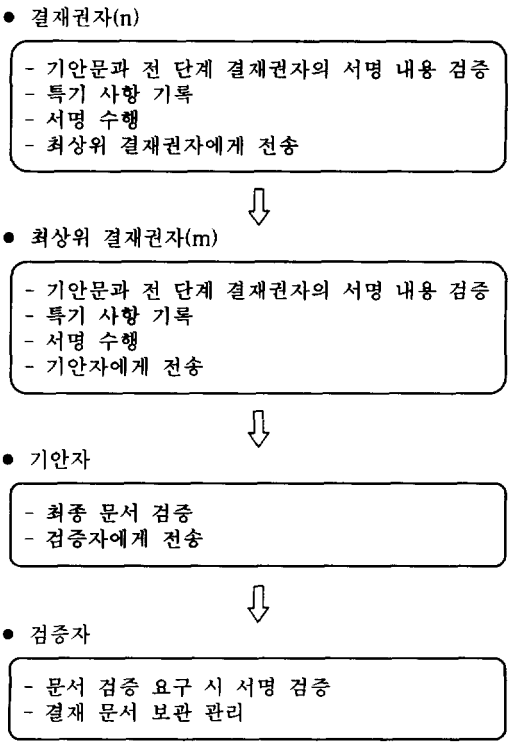
2. 전자결재 시스템의 종류

2.1 순차 전자결재 시스템

순차 전자결재 시스템은 전자적 문서에 대해 기안자가 있고, 여러 상급자의 결재를 요구할 경우 순차적으로 각 직급별 단계를 거쳐 결재를 수행하는 시스템이다. 따라서, 모든 사용자들은 네트워크를 통해 서로의 시스템이 연결되어 있다고 가정한다.

이 시스템을 구성하는데 있어 디지털 다중서명 방식을 사용하며, 특히 모든 사용자들이 서명에 대한 검증이 필요하므로, 결재가 완료된 문서의 경우 기안자가 마지막으로 확인한 후 검증자에게 전송하는 (그림 1)과 같은 순차 전자결재 시스템 모델을 가정하였다.



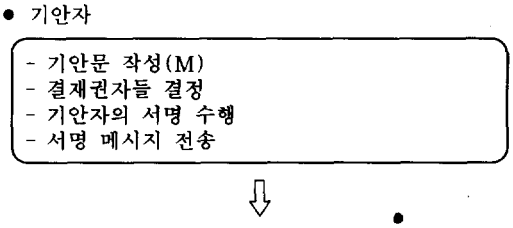


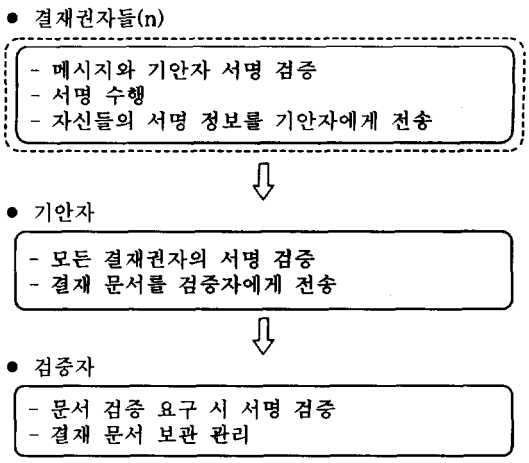
(그림 1) 순차 전자결재 시스템 모델
(Fig. 1) Sequential electronic approval system model

2.2 동시 전자결재 시스템

요즘은 사내의 중요 회의를 네트워크를 통해 원격적으로 수행하고 있는 경우가 있다. 이 때도 역시 디지털 서명을 통해 결재를 수행할 수 있는데 이 경우는 순서와는 상관없이 한 사람이 문서를 작성하여 이 문서에 대해 모든 결재권자가 동시에 결재를 수행한다는 것이 특징일 것이다. 이와 같이 서명자의 순서에 상관없이 결재가 이루어지는 시스템을 동시 전자결재 시스템이라 한다.

(그림 2)는 동시 전자결재 시스템의 모델이다.





(그림 2) 동시 전자결재 시스템 모델
(Fig. 2) Simultaneous electronic approval system model

3. 기존의 다중서명 방식의 전자결재 시스템 적용

3.1 Ohta-Okamoto 방식 적용(순차 다중서명 방식)[6]

본 방식은 결재권자가 특기 사항을 기록할 수 있는 순차 전자결재 시스템을 구성할 때 적용 가능한 방식이다. 그러나 이 방식은 서명 검증을 위해 랜덤수를 별도로 저장해야 하며, 통신 횟수가 늘어나는 특징이 있다. 또한 기능적인 측면에서 중간 서명자의 서명 검증이 불가능하다는 단점을 가지고 있다. 키 생성 절차는 Fiat-Shamir 방식과 동일하며, 키 생성을 위한 별도의 신뢰된 센터(TC : Trusted Center)가 필요하다.

3.1.1 공통키 생성 단계

가. 서명자 1(기안자)

단계 1) 기안자는 랜덤 수 $R_1 \in Z_N$을 선택한다. 여기서 Z_N은 {0, 1, ..., N-1)을 나타낸다. 그리고 다음을 계산한다.

$$X_1 = R_1^2 \bmod N \qquad (1)$$

단계 2) 기안자는 X_1을 다음 서명자에게 전송한다.

나. 서명자 n(결재권자)

단계 1) 서명자 n($2 \le n \le m$)은 앞 서명자로부터 X_{n-1}을 수신하면 랜덤 수 $R_n \in Z_N$을 선택하여 다음을 계산한다.

$$X_n = R_n^2 X_{n-1} \bmod N \quad (2)$$

단계 2) 서명자 n은 X_n을 다음 서명자 n+1에게 전송한다. 만약 서명자가 마지막 서명자(서명자 m)이면 X_m을 기안자에게 전송한다.

3.1.2 다중서명 생성 단계

가. 서명자 1(기안자)의 서명 생성

단계 1) 기안자는 문서를 결재할 사람의 순서를 순차적으로 결정하고, $ID_{cm} = ID_1||ID_2||...||ID_m$을 구성한다. 여기서 ID_1은 기안자의 ID이고, ID_m은 최종 결재권자의 ID이다.

단계 2) 기안자는 다음과 같이 서명을 생성한다.

$$(e_{11}, ..., e_{1k}) = h(M||C_1, ID_{cm}, X_m) \quad (3)$$

$$Y_1 = R_1 \prod_{e_{1j}=1} S_{1j} \bmod N \text{(단, j=1, 2, ..., k)} \quad (4)$$

여기서 C_1은 공란으로 한다.

단계 3) 기안자는 서명 정보($M||C_1, ID_{cm}, X_m, Y_1$)을 다음 서명을 위해 ID_2를 가진 결재권자에게 전송한다.

나. 서명자 n(결재권자)의 서명 생성

단계 1) 서명자 n($2 \le n \le m$)은 서명자 (n-1)로부터 서명 정보($M||C_1||C_2...||C_{n-1}$, ID_{cm}, X_m, Y_{n-1})를 수신하면 문서를 확인하고 지시 사항 C_n을 문서에 추가 기록한 후 다음을 계산한다.

$$(e_{n1}, ..., e_{nk}) = h(M||C_1||C_2||...||C_n, ID_{cm}, X_m) \quad (5)$$

$$Y_n = Y_{n-1} R_n \prod_{e_{nj}=1} S_{nj} \bmod N \text{ (단, j= 1, 2, ..., k)} \quad (6)$$

결재권자 n의 지시 사항이 없으면 C_n은 공란으로 한다.

단계 2) 서명자 n은 서명 정보($M||C_1||C_2||...||C_n$, ID_{cm}, X_m, Y_n)를 다음에 서명할 ID_{n+1}를 가진 서명자에게 전송한다.

단계 3) 서명자가 마지막 결재권자(서명자 m)이면 서명 정보($M||C_1||C_2||...||C_m$, ID_{cm}, X_m, Y_m)를 기안자에게 전송한다.

단계 4) 기안자는 마지막 서명자로부터 ($M||C_1||C_2||...||C_m$, ID_{cm}, X_m, Y_m)을 수신하면 다중서명을 검증하고 이들 정보를 검증자에게 보낸다.

3.1.3 다중서명 검증 단계

가. 중간 서명자 n의 검증

앞 서명자로부터 서명 메시지($M||C_1||C_2||...||C_{n-1}$, X_m, Y_{n-1})을 수신하면 중간 서명자 n은 공개된 법 N과 단방향 함수 f, h를 이용하여 다음 절차에 의해 서명 메시지를 검증한다.

단계 1) 서명자 n은 다음과 같이(e_{11}, ..., e_{1k}),..., ($e_{(n-1)1}$, ..., $e_{(n-1)k}$)을 계산한다.

$$(e_{i1}, ..., e_{ik}) = h(M||C_1||C_2||...||C_i, ID_{cm}, X_m)$$
(단, i=1, 2, ..., n-1) (7)

단계 2) 서명자 n은 ID_{cm}으로부터 앞 서명자들의 I_{ij}를 다음과 같이 계산한다.

$$I_{ij} = f(ID_i, j) \text{ (단, i=1,2, ..., n-1, j=1, 2, ..., k)} \quad (8)$$

단계 3) 서명자 n은 다음과 같이 Z_{n-1}을 계산한다.

$$Z_{n-1} = Y_{n-1}^2 \prod_{i=1}^{n-1} \prod_{e_{ij}=1} I_{ij} \bmod N$$
(단, j=1, 2, ..., k) (9)

단계 4) 서명자 n은 다음을 점검한다.

$$Z_{n-1} = X_{n-1} \quad (10)$$

만약 위 식이 성립되면 그 다중서명 메시지는 유효한 것으로 간주한다.

나. 최종 다중서명 검증

기안자 혹은 검증자가 다중서명 메시지($M||C_1||C_2||...||C_m$, ID_{cm}, X_m, Y_m)을 수신하면 공개된 법 N과 단방향 함수 f, h를 이용하여 다음과 같이 문서의 다중서명을 검증한다.

단계 1) 검증자는 다음과 같이 (e_{11}, ..., e_{1k}),..., (e_{m1}, ..., e_{mk})을 계산한다.

$$(e_{i1}, ..., e_{ik}) = h(M||C_1||C_2||...||C_i, ID_{cm}, X_m)$$
(단, i=1, 2, ..., m) (11)

단계 2) 검증자는 ID_{cm}으로부터 서명자들의 I_{ij}를 계산한다.

$$I_{ij} = f(ID_i, j) \text{ (단, i=1, 2,..., m-1, j=1, 2,...,k)} \quad (12)$$

단계 3) 검증자는 Z_m을 다음과 같이 계산한다.

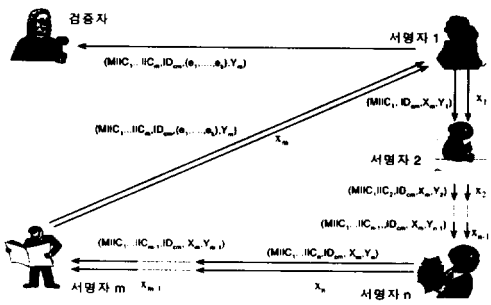
$$Z_m = Y_m^2 \prod_{i=1}^{m} \prod_{e_{ij}=1} I_{ij} \bmod N$$

(단, j=1, 2, ..., k) (13)

단계 4) 검증자는 $h(M||C_1||C_2||...||C_m, ID_{cm}, Z_m)$을 계산하고 다음식이 만족되는지를 확인한다.

$$(e_{m1},..., e_{mk}) = h(M||C_1||C_2||...||C_m, ID_{cm}, Z_m) \quad (14)$$

식 (14)가 만족하면 다중서명 메시지는 유효한 것으로 판명한다. 즉 문서 M에 모든 결재권자의 결재가 완료된 것이다.



(그림 3) Ohta-Okamoto 방식
(Fig. 3) Ohta-Okamoto Scheme

3.2 Brickell-Lee-Yacobi 방식 적용(동시 다중서명 방식)[11]

본 방식은 동시 전자결재 시스템에 적용 가능한 방식으로서 Fiat-Samir 서명 방식에 근거하고 있다. 그러나 서명 검증을 위해 별도의 랜덤수 저장 공간이 필요하며 통신 횟수가 늘어나는 단점을 지니고 있다. [3,10] 키 생성 절차는 Fiat-Shamir 방식과 동일하며, 키 생성을 위한 별도의 신뢰된 센터(TC : Trusted Center)가 필요하다.

3.2.1 키 생성 및 배포 단계

본 방식에서의 키 발생 및 배포 절차는 서명자 i가 자신의 식별 정보인 ID_i를 신뢰할 수 있는 키 발급센터에 등록하면 키 발급센터는 다음 절차에 의해 키를 생성 배포한다.

단계 1) 키 발급센터는 두개의 큰 소수 p와 q를 선택하고 그들을 비밀리에 유지한다.

단계 2) 키 발급센터는 p와 q의 곱인 N=pq를 공개한다.

단계 3) 키 발급센터는 각 서명자 i에 대하여 S_{ij}를 다음과 같이 계산한다.

$$I_{ij} = f(ID_i, j) \text{ (단, } j = 1,2,..., k) \quad (15)$$

$$I_{ij}^{-1} = S_{ij}^2 \bmod N \quad (16)$$

단계 4) 키 발급센터는 서명자 i에 대하여 물리적 식별을 수행한 다음 (N, f, h, S_{i1},..., S_{ik})가 기록된 스마트 카드를 발급 배포한다.

3.2.2 다중서명 생성 단계

가. 서명자 1(기안자)의 서명 생성

단계 1) 기안자는 랜덤 수 $R_1 \in Z_N$을 선택하여 다음을 계산한다.

$$X_1 = R_1^2 \bmod N \quad (17)$$

단계 2) 기안자는 다른 서명자들로부터 X_2, ..., X_m을 수신하면 다음과 같이 X를 계산한다.

$$X = X_1X_2...X_m \bmod N \quad (18)$$

그리고 결재 문서 M에 서명할 서명자들의 식별 정보를 $ID_{cm} = ID_1||ID_2||...||ID_m$과 같이 연접하고, 서명 정보(M, ID_{cm}, X)를 모든 서명자들에게 동보 전송한다. 여기서 ID_1은 기안자의 식별 정보이며, ID_m은 마지막 서명자의 식별 정보를 의미한다.

단계 3) 기안자는 다음과 같이 자신의 서명을 생성한다.

$$(e_1, ..., e_k) = h(M, ID_{cm}, X) \quad (19)$$

$$Y_1 = R_1 \prod_{e_j=1} S_{1j} \bmod N \text{ (단, } j=1, 2,..., k) \quad (20)$$

단계 4) 기안자는 다른 서명자들로부터 Y_2, ..., Y_m을 수신하여 다음과 같이 Y를 계산한다.

$$Y = Y_1Y_2...Y_m \bmod N \quad (21)$$

그리고 다중서명 메시지(M, ID_{cm}, X, Y)을 검증자에게 보낸다.

나. 서명자 i의 서명 발생

단계 1) 서명자 i($2 \le i \le m$)는 랜덤 수 $R_i \in Z_N$을 선택하고 다음과 같이 X_i를 계산하여 기안자에게 전송한다.

$$X_i = R_i^2 \bmod N \quad (22)$$

단계 2) 서명자 i는 기안자로부터 M, ID_{cm}, X를 수신하면 다음과 같이 자신의 서명 Y_i를 생성하여 기안자에게 전송한다.

$$(e_1, ..., e_k) = h(M, ID_{cm}, X) \quad (23)$$

$$Y_i = R_i \prod_{e_{j=1}} S_{ij} \bmod N \quad (단, j=1, 2, ..., k) \quad (24)$$

3.2.3 다중서명 검증 단계

검증자는 기안자로부터 다중서명 메시지(M, ID_{cm}, X, Y)을 수신하면 다음과 같은 절차에 의해 다중서명 메시지를 검증한다.

단계 1) 검증자는 ID_{cm}으로부터 각 서명자에 대한 I_{ij}를 계산한다.

$$I_{ij}=f(ID_i, j) \quad (단, i=1, 2,..., m, j=1, 2,..., k) \quad (25)$$

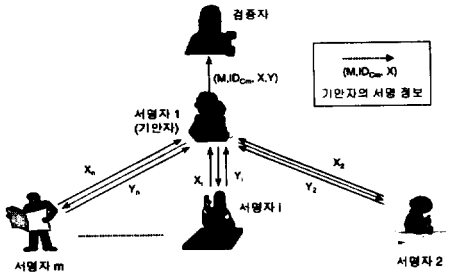
단계 2) 검증자는 M, ID_{cm}, X로부터 $(e_1, ..., e_k)$을 다음과 같이 계산한다.

$$(e_1, ..., e_k) = h(M, ID_{cm}, X) \quad (26)$$

단계 3) 검증자는 Y, $(e_1, ..., e_k)$ 및 I_{ij}로부터 다음과 같이 Z를 계산한다.

$$Z=Y^2 \prod_{i=1}^{m} \prod_{e_{j=1}} I_{ij} \bmod N \ (단, j=1, 2,..., k) \quad (27)$$

만약 Z=X가 만족되면 그 다중서명 메시지는 유효한 것으로 간주한다.



(그림 4) Brickell-Lee-Yacobi 방식
(Fig. 4) Brickell-Lee-Yacobi Scheme

4. 새로운 전자결재 시스템 제안

본 장에서는 이산 대수 문제의 어려움에 근거한 새로운 다중서명 방식을 제안하여 순차 및 동시 전자결재 시스템에 적용하고자 한다.[13] 제안하는 디지털 다중서명 방식은 앞에서 설명하였던 기존의 방식들에 비하여 통신 복잡도 측면에서 보다 안정적이며, 서명 수행시 생성하였던 랜덤수를 별도로 보관할 필요가 없다는 특징을 가지고 있다.[6,11,12,13] 뿐만 아니라 키 생성을 위한 TC가 불필요하고, 중간 서명자의 서명 검증이 가능하다는 장점을 지니고 있다.

4.1 순차 다중서명 방식 적용

제안된 다중서명 방식을 이용하여 서명자가 특기사항을 기록한 후 서명할 수 있도록 순차 전자결재 시스템에 적용한다.

4.1.1 초기 단계

각 서명자(i)는 임의의 랜덤수 $s_i \in Z_p$(단, Z_p = 1, 2, ..., P-1)를 선택하여 비밀리에 보관하고, 다음을 계산하여 공개한다. 여기서 사용되는 랜덤수 g 및 큰 소수 P는 모든 서명자와 검증자에게 공개된 정보이다.

$$y_i = g^{si} \bmod P \quad (단, i = 1, 2, ..., m) \quad (28)$$

4.1.2 다중서명 생성 단계

가. 서명자 1(기안자)의 서명 생성

단계 1) 기안자는 문서에 순차적으로 서명할 사람(결재권자)의 순서를 결정한다.

단계 2) 기안자는 $r_1 \in Z_p$을 선택하여 다음을 계산한다.

$$x_1 = g^{r1} \bmod P \quad (29)$$

단계 3) 기안자는 해쉬 함수 h를 이용하여 문서 M에 대한 해쉬값을 구하고, 다음을 계산한다.

$$e_1 = h(x_1, M||C_1) \ (단, C_1은 공란으로 한다.) \quad (30)$$

$$\sigma_1 = r_1 + (s_1 * e_1) \quad (31)$$

단계 4) 기안자는 $(M||C_1, \sigma_1, x_1, e_1)$을 다음 결재권자에게 전송한다.

나. 서명자 n의 서명 생성

단계 1) 서명자 n(2≤n≤m)은 서명자 (n-1)로부터 서명 정보$(M||C_1||C_2||...||C_{n-1}, \sigma_{n-1}, x_{n-1}, e_1, ..., e_{n-1})$을 수신하면 검증 절차에 의해 앞 서명자들의 서명을 확인한다. 만약 앞 서명자들의 서명을 확인하고 싶지 않다면 이 검증 절차는 생략할 수 있다.

단계 2) 서명자 n은 앞 서명자로부터 수신한 문서를 확인하고 지시 사항 혹은 특기 사항 C_n을 추가로

기록한 다음, 다음과 같이 서명을 생성하여 결재권자(n+1)에게 전송한다. 특기 사항이 없으면 C_n은 공란으로 한다.

$$x_n = x_{n-1} * g^m \bmod P \quad (32)$$

$$e_n = h(x_n, M||C_1||C_2||...||C_n) \quad (33)$$

$$\sigma_n = \sigma_{n-1} + (r_n + s_n * e_n)$$

만약 서명자 n이 마지막 결재권자이면 기안자에게 서명$(M||C_1||C_2||...||C_n, \sigma_n, x_n, e_1, ..., e_n)$을 전송한다.

단계 3) 기안자는 마지막 서명자(서명자 m)로부터 $(M||C_1||C_2||...||C_m, \sigma_m, x_m, e_1, ..., e_m)$을 수신하면, 다중서명 검증 단계에 의해 다중서명을 검증하고, $(M||C_1||C_2||...||C_m, \sigma_m, x_m, e_1, ..., e_m)$을 검증자에게 보내어 문서를 관리 하도록 한다.

4.1.3 다중서명 검증 단계

최종 검증자는 다중서명 데이터$(M||C_1||C_2||...||C_m, \sigma_m, x_m, e_1, ..., e_m)$이용하여

$$g^{\sigma m} = x_m * y_1^{e1} * y_2^{e2} * ... * y_m^{em} \quad (34)$$

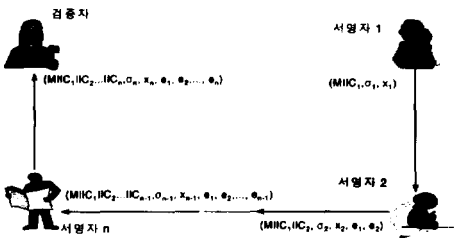
을 계산하여 확인되면, 순차 전자결재는 검증되었다고 판단한다.

다음 식을 통해 식 (34)가 성립됨을 알 수 있다.

$$g^{\sigma 1+\sigma 2+...+\sigma m} = x_1 * x_2 * ... * x_m * y_1^{e1} * y_2^{e2} *...* y_n^{em}$$

$$g^{\sigma 1+\sigma 2+...+\sigma m} = (x_1 * y_1^{e1}) * (x_2 * y_2^{e2}) *...* (x_m * y_m^{em})$$

$$(\because g^{\sigma i} = g^{ri+si*ei} = g^{ri} * g^{si*ei} = x_i * y_i^{ei})$$



(그림 5) 제안된 순차 전자결재 시스템
(Fig. 5) The proposed sequential electronic approval system

4.2 동시 다중서명 방식 적용

제안된 다중서명 방식을 이용하여 동시 전자결재 시스템에 적용한다. 이때, 모든 결재권자들의 시스템은 동보 전송이 가능한 네트워크로 결합되어 있다고 가정한다.

4.2.1 초기 단계

각 서명자 i는 임의의 랜덤수 $s_i \in Z_p$(단, Z_p = 1, 2, ..., P-1)를 선택하여 비밀리에 보관하고, 다음을 계산하여 공개한다. 여기서 사용되는 랜덤수 g 및 큰 소수 P는 모든 서명자와 검증자에게 공개된 정보이다.

$$y_i = g^{si} \bmod P \quad (단,\ i = 1, 2, ..., m) \quad (35)$$

4.2.2 다중서명 생성 단계

가. 서명자 1(기안자)의 서명 생성

단계 1) 기안자는 랜덤수 $r_1 \in Z_p$을 선택하여 다음을 계산한다.

$$x_1 = g^{r1} \bmod P \quad (36)$$

단계 2) 기안자는 해쉬 함수 h를 이용하여 문서 M에 대한 해쉬값을 구하고, 다음을 계산한다.

$$e_1 = h(x_1, M) \quad (37)$$

$$\sigma_1 = r_1 + (s_1 * e_1) \quad (38)$$

기안자는 (M, σ_1, x_1)를 모든 서명자(결재권자)에게 동보 전송한다.

나. 서명자 i(결재권자)의 서명 생성

단계 1) 서명자 $i(2 \le n \le m)$는 기안자로부터 서명 메세지 (M, σ_1, x_1)을 수신하면 먼저 기안자의 서명 메세지를 검증한다. 서명자들이 서명자 1의 메시지를 검증하고 싶지 않으면 이 검증 절차는 생략할 수 있다.

단계 2) 랜덤한 수 $r_i \in Z_p$를 선택하여 다음을 계산한다.

$$x_i = g^{ri} \bmod P \quad (39)$$

단계 3) 해쉬 함수 h를 이용해 $e_i = h(x_i, M)$을 구하여 다음을 계산한다.

$$\sigma_i = r_i + (s_i * e_i) \quad (40)$$

단계 4) 서명자 i는(M, σ_i, x_i)를 기안자에게 전송한다.

4.2.3 다중서명 검증 단계

가. 서명자 1(기안자)의 검증 및 서명 정보 전송

단계 1) 기안자는 결재권자들로부터 받은 서명 메시지 $(M, \sigma_i, x_i)(2 \le i \le m)$와 해쉬 함수를 이용하여 구한 e_i에 대하여 다음과 같이 검증한다.

$$g^{\sigma i} \bmod P = x_i * y_i^{ei} \bmod P \qquad (41)$$

위 식이 만족되면 그 메세지는 유효한 것으로 간주한다.

단계 2) 기안자는 서명자 i로부터 받은 서명 정보를 이용하여 다음을 계산한다.

$$\sigma'_m = \sigma_1 + \sigma_2 + \ldots + \sigma_m \qquad (42)$$

$$x'_m = x_1 \cdot x_2 \cdot \ldots \cdot x_m \qquad (43)$$

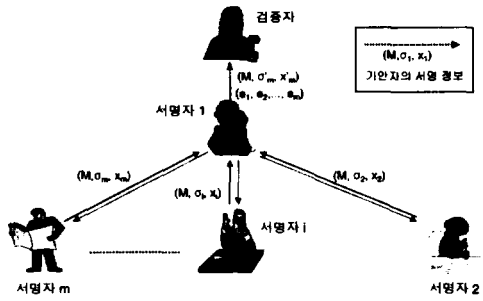
단계 3) 기안자는 (M, σ'_m, x'_m) 및 $(e_1, e_2, \ldots, e_m)$을 검증자에게 전송한다.

나. 서명자 i(결재권자)의 검증

서명자 i는 기안자로부터 받은 서명 정보(M, σ_1, x_1)에 대하여 다음과 같이 검증한다.

$$g^{\sigma 1} \bmod P = x_1 \cdot y_1^{e1} \bmod P \qquad (44)$$

위의 식이 만족되면 그 메세지는 유효한 것으로 간주한다.



(그림 6) 제안된 동시 전자결재 시스템
(Fig. 6) The proposed simultaneous electronic approval system

다. 검증자의 검증

최종 검증자는 기안자로부터 다중서명 정보(M, σ'_m, x'_m)과 해쉬 함수를 이용하여 다음과 같이 다중서명을 검증한다.

$$g^{\sigma' m} = x'_m \cdot y_1^{e1} \cdot y_2^{e2} \cdot \ldots \cdot y_m^{em} \qquad (45)$$

계산이 확인되면, 동시 전자결재는 검증되었다고 판단한다.

4.3 기존 방식과의 비교 분석

본 절에서는 기존의 디지털 다중서명 방식들과 새로운 제안 방식을 전자결재 시스템에 적용할 경우, 그 효율성에 대해 비교 분석해 본다.

기존의 Ohta-Okamoto 방식을 순차 전자결재 시스템에 적용 시켰을 경우 각 결재권자는 서명 정보를 송·수신하기 위해 네트워크에 2회 접속하게 되므로 통신 횟수는 2회가 되며, Brickell-Lee-Yacobi 방식을 동시 전자결재 시스템에 적용 시켰을 경우에는 통신 횟수가 3회 정도가 된다. 또한 Ohta-Okamoto 방식의 경우에는 중간 서명자가 서명을 검증할 수 없다는 문제점을 안고 있었다. 상기 설명되었던 기존 방식들 모두 키 생성을 위해서 별도의 신뢰된 센터(TC)가 필요하고, 각 결재권자가 서명 생성을 위해 만들었던 랜덤수를 검증 단계에서 사용하기 위해 별도로 보관해야하는 번거로움이 있다.

새로이 제안한 다중서명 방식을 순차 전자결재 시스템에 적용 시켰을 경우 각 결재자는 서명 정보 송·수신을 위해 네트워크에 1회 접속하게 되므로 통신 횟수는 1회가 되며, 동시 전자결재 시스템에 적용시킬 경우 통신 횟수는 2회 정도가 된다. 또한 기존 방식들과는 달리 키 생성을 위한 별도의 신뢰된 센터(TC)와 서명 생성시 사용했던 랜덤수를 별도로 보관할 필요가 없다는 장점을 가지고 있다. 동시에 Ohta-Okamoto 방

〈표 1〉 각 방식별 효율성 비교
〈Table 1〉 Comparison of the efficiency on each method

항목 \ 방식		통신 횟수	중간서명자 검증성	랜덤수 저장	TC 필요성
순차 전자 결재 시스템	Ohta-Okamoto 방식	2회	불가능	필요	필요
	제안 방식	1회	가능	불필요	불필요
동시 전자 결재 시스템	Brickell-Lee-Yacobi 방식	3회	가능	필요	필요
	제안 방식	2회	불가능	불필요	불필요

식에서는 불가능했던 중간 서명자의 서명 검증이 가능하기 때문에 효율적이라 할 수 있다. 다음은 각 방식별 효율성에 대하여 비교 정리한 것이다.

5. 결 론

본 논문에서는 새로운 디지털 다중서명 방식을 제안하여 전자결재 시스템에 적용시켜 보았다. 먼저 전자결재 시스템을 순차 전자결재 시스템과 동시 전자결재 시스템으로 분류하여 모형화 하였고, 기존 방식(Ohta-Okamoto 방식 및 Brickell-Lee-Yacobi 방식)을 분석하였다. 그리고 새로이 제안한 다중서명 방식을 결재권자가 특기 사항을 기록할 수 있도록 순차 결재 시스템 및 동시 전자결재 시스템에 적용하였다.

기존의 다중서명 방식을 전자결재 시스템에 적용할 경우 통신 횟수가 많았으며, 별도로 키 생성을 위한 신뢰된 센터(TC)와 랜덤수를 저장해야 하는 번거로움이 있었다. 또한 Ohta-Okamoto 방식의 경우에는 중간 서명자의 서명 검증이 불가능하다는 문제점을 가지고 있었다.

일반적으로 정보화 된 사무실 환경에서 전자결재 시스템을 구축할 경우 서명 정보를 송·수신하기 위해 네트워크에 접속하는 횟수가 늘어난다면 그만큼 번거로운 일이 될 것이며, 수신된 서명 정보를 검증하기 위해 랜덤수를 별도로 저장해야 한다면 메모리 측면에서도 그만큼 손해가 될 것이다. 이에 대해 새로이 제안된 다중서명 방식은 기존의 방식들에 비해 네트워크 접속 횟수가 적고, 별도로 랜덤수를 저장할 필요가 없다는 장점을 가지고 있다. 또한 별도의 신뢰된 키 생성 기관(TC)이 필요 없을 뿐 아니라 중간 서명자의 서명 검증이 가능한 효율적인 방식이다.

상기 사항들을 고려해 볼 때 새로이 제안한 디지털 다중서명 방식은 전산화된 통신망으로 구축된 사무실 환경에서 전자결재 시스템에 효과적으로 적용될 수 있으리라 본다.

참 고 문 헌

[1] T.Tanaka and K.Nakao, "Mutual Digital Signature Scheme on Online Electronic Contract System," 일본정보통신학회 기술연구보고서, ISEC 91-46, pp.19-25, 1991.

[2] D.Davies, "Applying the RSA Digital Signature to Electric Mail," IEEE Computer, pp.55-62, Feb. 1983.

[3] A.Shamir, "Identity-based Cryptosystems and Signature Schemes," Proceedings of Crypto'84, Lecture Notes in Computer Science 196, pp.47-53, 1985.

[4] T.Okamoto and A.Shiraishi, "A Fast Signature Scheme Based on Quadratic Inequalities," Proceedings of the IEEE Symposium and Privacy, IEEE, pp.123-132, 1985.

[5] L.Guillou and J.Quisquater, "A Paradoxical Identity-Based Signature Scheme Resulting from Zero-Knowledge," Proceedings of Crypto'88, 1988.

[6] K.Ohta and T.Okamoto, "A Digital Multisignature Scheme Based on the Fiat-Shamir Scheme," Proceedings of Asiacrypt'91, pp.75-79, 1991.

[7] R.Rivest, A.Shamir and L.Adleman, "A Method for Obtaining Digital Signatures and Public-key Cryptosystems," Communication of the ACM, Vol.21, No.2, pp.120-126, 1978.

[8] K.Itakura and K.Nakamura, "A Public-key Cryptosystem Suitable for Digital Multisignature," Nec J.Res.Dev.71, pp.1-8, 1983.

[9] T.Okamoto, "A Digital Multisignature Scheme Using Bijective Public-Key Cryptosystems," ACM Trans. on Comp. Systems, Vol.6, No.8, pp.432-441, 1988.

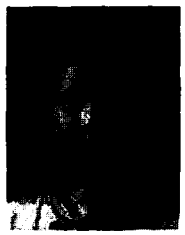
[10] A.Fiat and A.Shamir, "How to prove yourself: Practical Solutions to Identification and Signature Problems," Advances in Cryptology-Crypto'86, Lecture Notes in Computer Science 263, pp.186-199, 1987.

[11] E.Brickell, P.Lee and Y.Yacobi, "Secure Audio Teleconference," Advances in Cryptology-Crypto'87, Lecture Notes in Computer Science 293, pp.418-426, 1988.

[12] 강창구, 김대영, "새로운 순차 및 동시 다중서명 방

식", 한국통신정보보호학회논문지, 제2권, 제1호, pp. 36-44, 1992.

[13] 박희운, 강창구, 이임영, "새로운 디지털 다중서명 방식에 관한 고찰", 한국통신정보보호학회 종합학술발표회 논문지, 제7권, 제1호, pp.101-110, 1997.



박 희 운

e-mail : heeun@ai-cse.sch.ac.kr

1997년 순천향대학교 전산학과 졸업

1997년~현재 순천향대학교 전산학과 대학원

관심분야 : 암호이론, 컴퓨터 보안

강 창 구

e-mail : cgkang@etri.re.kr

1979년 한국항공대학 항공전자공학과 졸업(공학사)

1986년 충남대학교 대학원 전자공학과(공학석사)

1993년 충남대학교 대학원 전자공학과(공학박사)

1979년~1982년 한국공군 기술장교

1987년~현재 한국전자통신연구원 부호3팀장 책임연구원

관심분야 : 암호이론 및 응용기술, 컴퓨터보안

이 임 영

e-mail : imylee@asan.sch.ac.kr

1981년 홍익대학교 전자공학과 졸업

1986년 일본 오오사카대학 통신공학과(석사)

1989년 일본 오오사카대학 통신공학과(박사)

1989년~1994년 한국전자통신연구원 선임연구원

1994년~현재 순천향대학교 컴퓨터학부 교수

관심분야 : 암호이론, 정보이론, 컴퓨터 보안