디지털다중서명 방식의 전자계약시스템 적용에 관한 연구

박희운† · 강창구†† · 이임영†

요 약

본 논문에서는 날로 정보화 되는 사회 환경 하에서 다수의 계약자가 계약을 처리할 수 있는 전자계약시스템에서의 위험요소를 분석하고 그에 따르는 디지털 다중 서명의 요구조건을 제시하였으며 지금까지 개발된 기존의 디지털 다중 서명 방식들을 전자계약시스템에 효율적으로 적용하고 새로운 다중 서명 방식을 제안하였다. 또한 제안 방식의 실제 예를 통해 전자 계약 시스템에 적용시켜 보았고, 각 방식별 요구조건 만족도를 검토하여 그 적용성과 효율성을 비교평가 하였다.

A Study on Electronic Contract Systems Using Digital Multisignature

Hee-Un Park†, Chang-Goo Kang†† and Im-Yeong Lee†

ABSTRACT

The multisignature system is a digital contract system which can process multi-party contracts electronically. In this paper, we analyzed various insecure elements involved in general multisignature contract systems and suggest requirements needed for making such systems secure. Based on our analysis, we propose a new secure multisignature method and apply it to the conventional electronic digital contract systems along with several other existing multisignature methods. The applicability and the effectiveness of the newly developed method are demonstrated by comparing how well the suggested security requirements are satisfied by each method.

1. 서 론

통신 기술의 발달과 더불어 컴퓨터의 보급 확산은 우리 생활에 있어 많은 변화와 발전을 주고 있다. 실예로, 손으로 쓴 종이 문서 대신에 E-mail을 통해 서신을 주고받는 것을 보면 그 변화를 실감하게 된다. 그러나 기업간 수출입 계약 체결 및 개인간의 이해 관계가 있는 계약 등에는 현재까지도 번거로이 종이 계약 문서를 들고 다니면서 일일이 계약을 위한 서명을 받아야 하고, 심지어 국제적 협약을 수행하는 데도 일정 회담 장소에 모여 회의를 하는 등의 모습들이 보여 진다. 이런 계약 체계는 상당히 번거로우며 시간 소비가 많은 관계로 편리성과 효율성을 제공하는 새로운 계약 체계를 모색하게 되었다. 그 해결책으로 나온 것이 바로 전자적인 계약 환경을 구축해 전자 문서를 통해 계약을 전자적으로 행하는 것인데 바로 이것을 전자 계약 시스템이라 한다.

전자 계약 시스템은 크게 두 가지로 나뉘어진다. 첫번째 방식은 하나의 계약 문서를 여러 사람들이 돌아가면서 확인한 다음 서명을 수행하는 방식이고, 다른 하나는 여러 계약자들에게 같은 계약 문서를 나눠주고 같은 시간에 계약을 동시에 수행하는 방식이다. 이때 전자 계약 시스템에서는 인감과 같은 역할을 수행하는 디지털 서명이 요구되고, 특히 제 3자

† 순천향대학교 컴퓨터학부
†† 한국전자통신연구원

의 보증 등과 같이 다수 계약자가 관련된 계약을 수행하기 위해서는 디지털 다중 서명이 요구되어 진다.

지금까지 개발된 디지털 다중 서명 방식을 살펴보면 다음과 같다. RSA 공개키 암호시스템을 다중 서명에 적용한 방식으로 Itakura-Nakamura의 다중 서명 방식(Itakura-Nakamura방식)[8]과 Okamoto의 다중 서명 방식 (Okamoto 방식)[9]이 있다. 전자의 방식은 서명 메시지 길이의 증가 및 서명 발생 속도의 문제점을 개선하기 위하여 두개의 큰 소수와 각 서명자에 따른 작은 소수의 곱을 이용하여 RSA 방법을 직접 다중 서명 방식으로 확대 적용한 방식이다. 그리고 후자의 방식은 RSA 방식과 같은 전단사(Bijective) 공개키 암호시스템[2][9]과 일방향 함수(One-Way Function)를 이용하여 서명 메시지의 길이 증가 및 서명자의 순서 제약성을 극복한 방식이다. 그 외에도 서명속도와 키 관리방법을 개선하기 위해 제안된 Fiat-Shamir서명 방식에 근거한 방식으로 Ohta와 Okamoto가 제안한 방식(Ohta- Okamoto 방식)[6]과 Ohta-Okamoto방식에서 통신 횟수를 줄인 Kang-Kim[11] 방식 등이 있다.

본 논문에서는 다수의 계약 참여자들이 동일한 계약문서를 작성하여 보유한 후 실시간적으로 계약문서에 서명을 수행하는 새로운 디지털 다중 서명 방식에 대하여 연구하였고, 제안한 다중 서명 방식을 전자 계약 시스템에 적용시켜 보았다. 또한 전자 계약 시스템에서의 위험요소와 디지털 다중 서명이 갖추어야 할 요구조건을 제시함으로써 향후 연구될 디지털 다중 서명 방식을 검토할 경우 발전적 평가 기준으로서 사용될 수 있으리라 본다.

2. 전자계약시스템에서의 디지털 다중 서명

본 논문에서는 계약참여자 전원이 컴퓨터를 보유하고 있으며, 전자계약을 체결하기 위하여 통신망에 실시간적으로 접속이 가능하다고 가정한다. 또한 계약문서를 작성 완료하거나 미리 작성된 계약문서를 통신망을 통하여 전달받아 계약참여자 전원이 동일한 계약문서를 보유한 후, 계약참여자 전원의 합의하에 디지털 다중 서명을 수행하는 전자계약 시스템을 대상으로 한다.

이와 같은 전자계약시스템에서는 복수의 계약 참여자에 의해서 전자적으로 계약을 체결하기 때문에 계약자간에 있어서의 다음과 같은 부정의 위험 요소가 있을 수 있다.

위험요소 1 : 서명 위조

계약자가 계약문서에 대하여 자신에게 유리하게 문서를 개조하고 그것에 부가된 다른 계약자의 서명을 위조할 수 있다.

위험요소 2 : 제 3자와 계약체결

계약 당사자 외의 제3자와 결탁하여 정당한 계약자에게 불이익을 주는 계약을 체결할 수 있다.

위험요소 3 : 계약 체결 부인

계약자가 계약문서에 서명을 수행한 후에 그 계약에 참여하지 않았다고 계약 체결을 부인할 수 있다.

위험요소 4 : 계약자 서명의 불법사용

계약자가 전자적으로 수행한 서명은 디지털 데이터이기 때문에 쉽게 복사될 수 있다. 따라서 계약자의 서명을 불법으로 사용할 수 있다.

위험요소 5 : 계약의 고의적 파기

계약자가 전자계약 문서에 서명을 수행할 때 거짓 서명을 수행하여 계약을 무효화시킬 수 있다.

위와 같은 문제점을 고려할 때 전자계약 시스템에 있어서 디지털 다중 서명의 요구조건은 다음과 같다.

요구조건 1 : 검증 가능성(Verifiability)

다중 서명 정보로부터 계약문서가 정당한 계약자들에 의해서 서명 되었다는 것을 계약자는 물론 제3자도 검증할 수 있어야 하고 계약내용이 변경되었을 경우 이를 검증할 수 있어야 한다.

요구조건 2 : 실행 가능성(Viability)

다중 서명 프로토콜이 끝나는 시점에서 각 계약자는 모든 계약 참여자의 서명을 서로 보유할 수 있어야 한다.

요구조건 3 : 부정 조기 검출성(Detectability)

다중 서명 프로토콜 수행 도중에 어떤 계약자가 부정을 행하였을 경우 계약 참여자 전원에 의해서 부정을 조기에 검출 가능하여야 한다.

요구조건 4 : 공통성(Commonness)

계약자가 수행하는 서명 프로토콜은 모든 계약자에 공통적으로 적용되므로, 모든 계약자의 서명 수행 방법은 같아야 한다. 이를 통해 사용자에게 편의성을

제공하게 되고, 효율성을 높일 수 있다.

요구조건 5 : 일반성(Generality)

다중 서명 프로토콜은 두 명의 계약자 즉, point-to-point간에도 그대로 적용 할 수 있도록 호환성을 가져야 한다.

요구조건 6 : 무 순서성(Orderlessness)

다중 서명을 수행하는데 있어서 계약자의 서명 순서가 결정되어져서는 안되며, 임의적으로 다중 서명 생성 및 검증을 할 수 있어야 한다.

단순서명 방식의 안전성이 유지되는 한 다중 서명의 요구조건 1에 의해서 위험요소 1, 2, 4는 제거될 수 있고, 요구조건 2에 의해서 위험요소 3은 불가능하며 또한 요구조건 3에 의해서 위험요소 5를 방지할 수 있다.

3. 기존 다중 서명 방식의 전자계약시스템 적용

3.1 Itakura - Nakamura 방식 적용[7]

이 방식은 RSA 서명 방식[7]에 근거한 것으로서, 요구 조건들 1 ~ 5의 사항은 만족하지만, 랜덤한 값이 작은 서명자부터 서명을 순차적으로 수행하므로 요구 조건 6을 만족하지 못한다.

3.1.1 키 발생 및 배포

단계1 : 키 발급센타는 두 개의 큰 소수 p, q를 선택하고 계약서명자 i에 대하여 작은 소수r_i를 선택한 후 다음과 같이 N_i를 계산한다[2].

$$N_i = p * q * r_i = N_0 * r_i \quad (1)$$

계약 서명자의 r_i는 계약자간에 서로 다르도록 선택하여야 한다.

단계2 : gcd(e, $(p-1)(q-1)(r_i-1)$) = 1을 만족하는 임의의 e를 계산한다.

이때 e는$(p-1)(q-1)(r_i-1)$ 보다 작고 (r_i-1)의 최대값 보다 커야 한다.

단계3 : $e * d_i = 1 \bmod (p-1)(q-1)(r_i-1)$을 만족하는 d_i를 계산한다.

단계4 : e, N_0, r_i는 공개하고 키 발급센타는 p, q를 비밀리 보관하고 계약서명자 i는 d_i를 비밀리에 보관한다.

3.1.2 다중 서명 발생

가. 첫 번째 서명자(서명자 1)의 서명 발생

단계1 : 서명할 계약문서 M에 대하여 자신의 비밀키 d_1으로 다음과 같이 서명을 수행한다.

$$S_1 = M^{d1} \bmod N_1 \quad (2)$$

단계2 : 서명정보 S_1을 모든 서명자들에게 동보전송한다.

나. n번째 서명자(서명자 n)의 서명 발생

단계1 : 앞 서명자로부터 서명정보 S_{n-1}을 수신하면 서명자 n은 앞 서명자의 서명 S_{n-1}에 자신의 서명을 수행한다.

$$S_n = S_{n-1}^{dn} \bmod N_n \quad (3)$$

단계2 : 서명정보 S_n을 모든 서명자들에게 동보전송한다. 만약 서명자가 마지막 서명자 (서명자 m)이면 서명정보 S_m을 동보전송 한다. 이때 S_m이 최종 서명정보가 된다.

3.1.3 다중 서명 검증

각 계약 참여자는 다중 서명 수행 도중 앞 서명자들의 서명 정보를 다음과 같이 점검할 수 있다.

$$(...(S_{n-1}^{e} \bmod N_{n-1})^{e}... \bmod N_2)^{e} \bmod N_1 = M \bmod N_1 \quad (4)$$

서명 프로토콜이 완료되면 계약서명자 혹은 제3자는 다중 서명 검증을 다음 식에 의해서 점검할 수 있다.

$$(...(S_m^{e} \bmod N_m)^{e}... \bmod N_2)^{e} \bmod N_1 = = M \bmod N_1 \quad (5)$$

만약 위 식이 만족되면 다중 서명 정보는 유효한 것으로 간주한다.

3.1.4 방식 검토

본 방식은 다중 서명 정보 S_m으로부터 다중 서명 검증식 (5)에 의해 다중 서명을 검증할 수 있으므로 요구 조건 1을 만족하고, 다중 서명 프로토콜이 수행되고 나면 각 계약 서명자는 최종 서명 정보 S_m을 보유할 수 있으므로 요구 조건 2를 만족한다. 또한 다중 서명 프로토콜 수행 도중 계약 서명자가 부정을 행하였을 경우 모든 서명자는 검증식 (4)에 의해 부정이 조기에 검출될 수 있기 때문에 요구 조건 3을 만족한다. 각 서명자는 같은 서명 방법에 의해서 서명을 수행하므로 요구 조건 4를 만족한다. 또한 본 방식은 양자간 계약서명 시스템에서도 그대로 적용 가능하므로 요구 조건 5를 만족한다. 그러나 본 서명 방식은 r_i값이 작은 서명자로부터 서명을 순서적으로 수행

하여야 하므로 요구 조건 6은 만족하지 못한다.

3.2 Okamoto 방식 적용[8]

본 방식은 상기 Itakura-Nakamura방식과 마찬가지로 RSA 서명 방식[7]에 근거하고 있다. 이 방식은 Itakura-Nakamura방식이 가지고 있던 무순서성을 극복하였지만 공통성을 제공하지 못한다는 단점을 가지고 있다.

3.2.1 시스템 기호

다음은 본 방식에서 사용될 기호를 정의한 것이다.

$|N|$: N의 비트 길이

$[S]^L$: S의 ($|S|-L$)개의 최상위 비트. 즉 $|[S]^L| = |S|-L$이다.

$[S]_L$: S의 L개의 최하위 비트. 즉, $|[S]_L| = L$이다.

$L\{S\}$: 상위 ($L-|S|$)개의 '0'비트 패딩을 갖는 S. 즉, $|L\{S\}| = L$이다.

3.2.2 키 발생 및 배포

서명자 i는 공개키 e_i 와 비밀키 d_i를 발생하고 공개키인 e_i와 일방향 해쉬함수 $h_i : X_i * X_i * ... * X_i \dashrightarrow X_i$를 공개하고 비밀키 d_i를 비밀리 보관한다[4].

3.2.3 다중 서명 발생

가. 첫 번째 서명자(서명자 1)의 서명 발생

단계1 : 계약문서 M에 대하여 다음과 같이 서명 S_1과 M_1을 생성한다.

$S_1 = D_{d1}(h_1(M))$(단, D_{d1}는 키 d_1에 대한 복호 함수) (6)

$M_1 = M$ (7)

단계2 : 서명정보(S_1, M_1)와 자신의 식별자 ID_1을 모든 서명자들에게 동보전송 한다.

나. n번째 서명자(서명자 n)의 서명 발생

단계1 : 앞 서명자로부터 서명정보 (S_{n-1}, M_{n-1})을 수신하면 서명자 n은 앞 서명자의 서명정보 (S_{n-1}, M_{n-1})에 자신의 서명을 다음과 같이 수행한다.

만약 $|X_n| > |X_{n-1}|$이면 (8)

$S_n = D_{dn}(|X_n|\{S_{n-1}\})$ (9)

그렇지 않으면

$S_n = D_{dn}(|X_n|\{[S_{n-1}]_{|Xn|-1}\})$ (10)

$M_n = M_{n-1} || [S_{n-1}]^{|Xn|-1}$ (11)

여기서 X_n은 서명자 n의 평문과 암호문의 유한 집합을 나타낸다.

단계2 : 서명정보 (S_n, M_n)와 서명자의 식별자 (ID_1, ...,ID_n)를 모든 서명자들에게 동보전송 한다. 만약 서명자가 마지막 서명자(서명자 m)이면 서명정보 (S_m, M_m)와 (ID_1,..., ID_m)를 모든 계약 참여자에게 동보전송 한다. 이때 최종 다중 서명 정보는 S_m , M_m 과 서명자의 식별자 (ID_1,...,ID_m)이 된다.

3.2.4 다중 서명 검증

다중 서명 프로토콜 수행이 완료되면 각 계약자 및 제 3자는 서명자의 식별자 (ID_1,...,ID_m)로 부터 공개키 e_i(i = 1,2,...,m)를 이용하여 다중 서명 정보 (S_m , M_m)을 다음과 같이 검증한다. 여기서 서명자의 순서는 서명정보에 첨부된 서명자의 식별자 (ID_1,...,ID_m)에 의하여 표시된다.

단계1 : 다음식에 의해서 M_i'와 S_i' (i = 1,2,...,m)을 구한다.

단, $M_m' = M_m$이고, $S_m' = S_m$이다.

만약 $|X_i| > |X_{i-1}|$이면

$S_{i-1}' = [E_{ei}(S_i')]_{|Xi-1|}$ (12)

$M_{i-1}' = M_i'$ (13)

그렇지 않으면

$S_{i-1}' = [M_i']_{|Xi-1|\,|Xi|-1} || [E_{ei}(S_i')]_{|Xi|-1}$ (14)

$M_{i-1}' = [M_i']^{|Xi-1|-|Xi|+1}$ (15)

단계2 : 위의 단계 1에서 얻은 S_1'와 M_1'이 다음 식을 만족하면 다중 서명 정보 (S_m , M_m)은 유효한 것으로 간주한다.

$E_{e1}(S_1') = h_1(M_1')$ (16)

다중 서명 프로토콜 수행도중 앞 서명자들의 서명 정보를 위에 기술된 다중 서명 검증식 (12)-(16)에 의해 점검할 수 있다.

3.2.5 방식 검토

본 방식은 다중 서명 정보 S_m, M_m, (ID_1,...,ID_m)으로부터 다중 서명 검증식 (12)-(16)에 의해서 다중 서명을 검증할 수 있으므로 요구 조건 1을 만족하고, 다중 서명 프로토콜이 수행 완료되면 각 계약 서명자는 최종 서명정보 S_m, M_m, (ID_1,...,ID_m)을 보유할 수 있으므로 요구 조건 2를 만족한다. 또한 다중 서명

(12)-(16)에 의해서 부정을 조기에 검출할 수 있으므로 요구 조건 3을 만족한다. 그러나 첫번째 서명자와 그 외 서명자간의 서명방법이 다르므로 요구 조건 4를 만족하지 못한다. 또한 본 방식은 양자간 계약 서명 시스템에 그대로 적용 가능하고, 서명자의 서명 순서가 제약을 받지 않으므로 요구 조건 5와 요구 조건 6을 만족한다.

3.3 Ohta - Okamoto 방식 적용[9]

이 방식은 Fiat-Shamir의 ID-based 서명 방식 [3][10]에 기초하고 있다. 방식의 특성상 키 발급 센터를 가정하고 있으며, 요구 조건들에 대해 효율성을 제공하고 있지만 중간 서명자의 부정을 알아낼 방법이 없다는 단점을 지니고 있다.

3.3.1 키 발생 및 배포

본 방식에서의 키 발생 및 배포 절차는 서명자 i가 자신의 식별 정보인 ID_i를 키 발급센타에 등록하면 키 발급센타는 다음 절차에 의해 키를 발생 배포한다.[10]

단계1 : 키 발급센타(trusted center)는 두개의 큰 소수 p와 q를 선택하고 그들을 비밀리에 유지한다.

단계2 : 키 발급센타는 p와 q의 곱인 $N = p * q$를 공개한다.

단계3 : 키 발급센타는 공개된 일방향 함수 f를 이용하여 각 서명자 i에 대해 다음과 같이 S_{ij}를 계산한다.

$$I_{ij} = f(ID_i, j) \quad (단,\ j = 1,2,...,k) \tag{17}$$

$$I_{ij}^{-1} = S_{ij}^{2} \bmod N \tag{18}$$

단계4 : 키 발급센타는 서명자 i에 대하여 물리적으로 식별한 후$(N, f, h, S_{i1},...,S_{ik})$가 기록된 스마트 카드를 발급 배포한다. 여기서 h는 일방향 해쉬 함수를 의미한다.

3.3.2 다중 서명 발생

가. 공통키 생성 단계

1) 첫 번째 서명자(서명자1)

단계1 : 서명자 1은 랜덤 수 $R_1 \in Z_N$을 선택한다. 그리고 다음을 계산한다.

$$X_1 = R_1^{2} X_0 \bmod N \tag{19}$$

여기서 $X_0 = 1$이다.

단계2 : 서명자 1은 X_1을 모든 서명자에게 동보 전송한다.

2) n번째 서명자(서명자 n)

단계1 : 서명자n은 앞 서명자로부터 X_{n-1}을 수신하면 랜덤 수 $R_n \in Z_N$을 선택하여 다음을 계산한다.

$$X_n = R_n^{2} X_{n-1} \bmod N \tag{20}$$

단계2 : 서명자 n은 X_n을 모든 서명자에게 동보 전송한다. 만약 서명자가 마지막 서명자(서명자 m)이면 X_m을 모든 서명자들에게 동보 전송한다.

나. 서명 생성 단계

1) 첫번째 서명자의 서명 발생

단계1 : 첫 번째 서명자는 다음과 같이 서명을 발생한다.

$$(e_1,...,e_k) = h(M, ID_{cm}, X_m) \quad (단,\ h는\ 일방향\ 해쉬함수) \tag{21}$$

$$Y_1 = Y_0 R_1 \prod_{e_j=1} S_{1j} \bmod N \quad (단,\ j = 1,2,...,k) \tag{22}$$

여기서 $Y_0 = 1$이고 $ID_{cm} = ID_1 || ID_2 || ... || ID_n$은 계약 문서 M상에서 기록된 서명자들의 ID 리스트이다.

단계2 : 첫 번째 서명자는 서명정보 Y_1을 모든 서명자들에게 동보 전송한다.

2) 서명자 n의 서명 발생

단계1 : 서명자 n은 서명자 (n-1)로부터 서명정보 Y_{n-1}를 수신하면 다음을 계산한다.

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

$$Y_n = Y_{n-1} R_n \prod_{e_j=1} S_{nj} \bmod N \quad (단,\ j = 1,2,...,k) \tag{24}$$

단계2 : 서명자 n은 서명정보 Y_n을 모든 서명자들에게 동보 전송한다. 서명자가 마지막 서명자(서명자 m)일 경우에는 서명 정보 Y_m을 서명자들 및 검증자에게 동보전송 한다.

3.3.3 다중 서명 검증

모든 계약서명자 혹은 제 3자는 다중 서명 정보 $(ID_{cm}, (e_1,..., e_k), Y_m)$에 대하여 공개된 법 N과 일방향 함수 f, h를 이용하여 다음과 같이 다중 서명을 검증할 수 있다.

단계1 : 서명 검증자는 ID_{cm}으로부터 서명자들의 I_{ij}를 계산한다.

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

단계2 : 서명검증자는 Z_m을 다음과 같이 계산한다.

$$Z_m = Y_m^2 \prod_{i=1}^{m} \prod_{e_{ij}=1} I_{ij} \bmod N$$
(단, $j = 1,2,...,k$) (26)

단계3 : 서명검증자는 $h(M, ID_{cm}, Z_m)$을 계산하고 다음 식이 만족하는지를 확인한다.

$$(e_1,..., e_k) = h(M, ID_{cm}, Z_m) \text{ (단, h는 일방향 함수)} \quad (27)$$

만약 식(27)이 만족되면 그 다중 서명 메시지는 유효한 것으로 판명한다.

3.3.4 방식 검토

본 방식은 다중 서명 프로토콜이 수행되고 나면 계약 서명자는 최종 서명 정보 (ID_{cm}, $(e_1,...,e_k)$, Y_m)을 가지게 되고, 또한 이들 정보로부터 다중 서명 검증식 (25)-(27)에 의해서 다중 서명을 검증할 수 있으므로 요구 조건 1과 요구 조건 2를 만족한다. 또한 서명자의 순서가 바뀌어지면 최종 서명 정보 (ID_{cm}, $(e_1,...,e_k)$, Y_m)로부터 다중 서명 검증식 (25)-(27)에 의해서 다중 서명 정보를 검증할 수 있으므로 요구 조건 6은 만족하나, 다중 서명 프로토콜 수행 중에 중간 서명자가 부정을 행하였을 경우에는 이를 조기에 발견할 수 없으므로 요구 조건 3을 만족하지 못한다. 본 방식은 2자간 계약서명 시스템에서도 그대로 적용가능하고 또한 각 서명자가 수행하는 서명 방법이 같으므로 요구 조건 4와 요구 조건 5를 만족한다.

3.4 Kang - Kim 방식 적용[11]

Kang Kim 방식은 상기 방식과 마찬가지로 Fiat-Shamir의 서명 방식에 기초한다. 뿐만 아니라 이 방식은 중간 서명자의 부정을 알아낼 수 있다는 측면에서 모든 요구조건을 만족하고 있다. 그러나, 방식의 특성상 별도의 신뢰된 키 분배 센터를 전제 조건으로 한다.

3.4.1 키 발생 및 배포

본 방식에서의 키 발생 및 배포절차는 Ohta - Okamoto 방식 적용에서와 같다.

3.4.2 다중 서명 발생

가. 첫 번째 서명자(서명자 1)의 서명 발생

단계1 : 첫 번째 서명자는 랜덤수 $R_1 \in Z_N$을 선택한다. 그리고 다음을 계산한다.

$$X_1 = R_1^2 X_0 \bmod N \quad (28)$$

$$(e_{11},...,e_{1K}) = h(M, ID_{cm}, X_1) \text{ (단, h는 일방향 함수)} \quad (29)$$

$$Y_1 = Y_0 \prod_{e_j=1} R_1 S_{1j} \bmod N$$
(단, $j = 1,2,...,k$) (30)

여기서 ID_{cm}은 계약문서 M상에 기록된 서명자들의 ID리스트이고, $X_0 = 1$, $Y_0 = 1$ 이다.

단계2 : 첫 번째 서명자는 서명정보(X_1, Y_1)를 모든 서명자들에게 동보 전송한다.

나. n 번째 서명자(서명자 n)의 서명발생

단계1 : 서명자 n은 서명자(n-1)로부터 서명 정보 X_{n-1}, Y_{n-1}를 수신하면 서명을 하기 위하여 랜덤 수 $R_n \in Z_N$을 선택하고 다음을 계산한다.

$$X_n = R_n^2 X_{n-1} \bmod N \quad (31)$$

$$(e_{n1},...,e_{nK}) = h(M, ID_{cm}, X_n) \quad (32)$$

$$Y_n = Y_{n-1} R_n \prod_{e_j=1} S_{nj} \bmod N, \text{ (단, } j = 1,2,...,k) \quad (33)$$

단계2 : 서명자 n은 서명정보 X_n, Y_n를 모든 서명자에게 동보 전송한다. 만약 서명자가 마지막 서명자 (서명자 m)이면 최종 서명 정보 X_m, Y_m를 모든 서명자들에게 동보 전송한다.

3.4.3 다중 서명 검증

모든 서명자들은 다중 서명 정보(ID_{cm}, $X_1,...,X_m$, Y_m)를 보유하게 되고 $(e_{11},...,e_{1k})$,..., $(e_{m1},...,e_{mk})$을 다음과 같이 계산한다.

$$(e_{i1},...,e_{ik}) = h(M, ID_{cm}, X_i) \text{ (단, } i = 1,...,m) \quad (34)$$

그리고, 다중 서명 검증을 위하여 서명정보 (ID_{cm}, $(e_{11},...,e_{1k})$,...,$(e_{m1},...,e_{mk})$, Y_m)을 저장 보관한다. 그리고 계약자 혹은 제 3자는 다음과 같이 다중 서명을 검증할 수 있다.

단계1 : 서명 검증자는 ID_{cm}으로부터 서명자들의 I_{ij}를 계산한다.

$$I_{ij} = f(ID_i, j) \text{ (단, } i = 1,2,...,m,\ j = 1,2,...,k) \quad (35)$$

단계2 : 서명 검증자는 Z_m 을 다음과 같이 계산한다.

$$Z_m = Y_m^2 \prod_{t=1} \prod_{e_j=1} I_{ij} \bmod N \quad (\text{단, } j = 1,2,...,k) \tag{36}$$

단계3 : 서명검증자는 $h(M, ID_{cm}, Z_m)$ 을 계산하고 다음식이 만족되는지를 확인한다.

$$(e_{m1},...,e_{mK}) = h(M, ID_{cm}, Z_m) \tag{37}$$

만약 식(37)이 만족되면 그 다중 서명 정보는 유효한 것으로 판명한다.

3.4.4 방식 검토

본 방식은 다중 서명 프로토콜이 수행되고 나면 계약 서명자는 최종 서명 정보 (ID_{cm} , (X_1,..., X_m), Y_m)을 가지게 된다. 각 계약 서명자는 이들 정보로부터 다중 서명 검증식 (34)-(37)에 의해서 다중 서명을 검증할 수 있으므로 요구 조건 1과 요구 조건 2를 만족한다. 다중 서명 프로토콜 수행 중에 중간 서명자가 부정을 행하였을 경우에는 위의 검증 절차에 의해서 이를 조기에 검출할 수 있으므로 요구 조건 3을 만족하고, 각 서명자가 수행하는 서명방법이 같으므로 요구 조건 4를 만족한다. 또한 본 방식은 양자간 계약서명 시스템에서도 그대로 적용가능하고 서명자의 서명 순서에 제약이 없으므로 요구 조건 5와 요구 조건 6을 만족한다. 따라서 본 방식은 전자 계약 시스템에서의 다중 서명 프로토콜의 요구 조건을 모두 만족한다. 그러나, 이 방식은 서명 수행 특성상 별도의 신뢰된 키 분배 센터를 그 전제 조건으로 삼고 있기 때문에 상기 요구조건과는 별도로 이들 시스템의 안전성은 키 분배 센터의 신뢰도에 의존한다.

4. 새로운 다중 서명 방식 적용

본 논문에서 새로이 적용하고자 하는 디지털 다중 서명 방식은 이산대수에 근거하고 있다. 본 방식은 다중 서명 프로토콜 수행 중에 서명자의 부정이 발생될 경우 조기에 검출할 수 있으며, 계약자들의 순서에 아무런 제약을 받지 않는 특징을 가지고 있다. 따라서 본 논문은 향상된 이러한 특성들을 통해 기존의 방식들이 각각 안고 있던 무순서성, 공통성 및 부정 검출성에 대한 제약사항을 해결하고 있으며, 별도의 신뢰된 키 분배 센터가 필요 없다는 장점이 있다[12].

4.1 발생 및 배포

서명자 i는 랜덤수 $s_i \in Z_p$을 선택하여 비밀로 보관한다. 그리고, 다음을 계산하여 공개한다. (여기서 g, P는 모든 서명자 및 검증자에게 공개된 정보이다.)

$$y_i = g^{si} \bmod P \tag{38}$$

4.2 다중 서명 발생

4.2.1 첫 번째 서명자(서명자 1)의 서명 발생

단계1 : 서명자 1은 랜덤한 수 $r_1 \in Z_p$을 선택하여 다음을 계산한다.

$$x_1 = g^{r1} \bmod P \tag{39}$$

단계2 : 서명자 1은 해쉬함수 h를 이용하여 $e_1 = h(x_1, M)$ (M : 메시지)을 계산하여 다음을 생성한다.

$$\sigma_1 = r_1 + s_1 * e_1 \tag{40}$$

메시지 M에 대하여 (σ_1, x_1)를 서명 데이터로 한다.

단계3 : 서명자 1은 (M, σ_1, x_1)을 모든 서명자에게 동보 전송한다.

4.2.2 서명자들(서명자 i)의 서명 발생(i = 1,...,m)

단계1 : 서명자 i은 계약에 참여한 모든 서명자로부터 서명 정보 (σ_j , x_j)(j=1,..., m, i≠j)를 수신하면 서명 수행을 위하여 랜덤수 $r_i \in Z_p$를 선택하고 다음을 계산한다.

$$x_i = g^{ri} \bmod P \tag{41}$$

단계2 : 해쉬함수 h를 이용하여 $e_i = h(x_i, M)$을 계산하여 다음을 생성한다.

$$\sigma_i = r_i + s_i * e_i \tag{42}$$

단계3 : 각 서명자 i는 모든 서명자에게 (σ_i, x_i)를 다중 서명 데이타로 동보 전송한다.

4.3 다중 서명 검증

모든 서명자들은 다중 서명 데이터(σ_1,..., σ_m, e_1,...,e_m, x_1,...,x_m)를 보유하게 되고, 공개 정보 y_1,y_2,...,y_m과 해쉬함수 h 및 e_1,...,e_m 을 이용하여 다음을 계산한다.

$$x = x_1 * x_2 * ... * x_m \bmod P \tag{43}$$

$$\sigma = \sigma_1 + \sigma_2 + ... + \sigma_m \tag{44}$$

그리고, 다음 수식이 만족하면 그 다중 서명은 유

효한 것으로 판명한다.

$$g^{\sigma} \bmod P = x * y_1^{e1} * y_2^{e2} *...* y_m^{em} \bmod P \quad (45)$$

수식의 증명은 다음과 같다.

$$g^{\sigma 1 + \sigma 2 +...+ \sigma m} \bmod P = x_1 * x_2 *... *x_n * y_1^{e1} * y_2^{e2} *...* y_m^{em} \bmod P$$

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

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

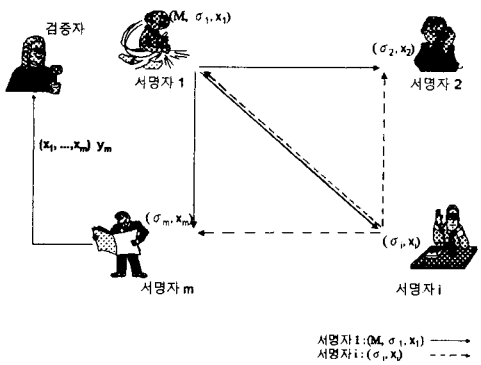


그림 1. 제안된 방식 적용

4.4 방식 검토

본 방식은 다중 서명 프로토콜이 수행되고 나면 계약 서명자는 최종 서명 정보 (σ_1,..., σ_m, e_1,...,e_m, x_1,...,x_m)를 가지게 되고, 또한 이들 정보로부터 다중 서명 검증식 (43)-(45)에 의해서 다중 서명을 검증할 수 있으므로 요구 조건 1과 요구 조건 2를 만족한다. 다중 서명 프로토콜 수행 중에 중간 서명자가 부정을 행하였을 경우에는 위의 검증 절차에 의해서 이를 조기에 검출할 수 있으므로 요구 조건 3을 만족하고, 각 서명자가 수행하는 서명방법이 같으므로 요구 조건 4를 만족한다. 또한 본 방식은 2자간 계약서명 시스템에서도 그대로 적용가능하고 서명자의 서명 순서에 제약이 없으므로 요구 조건 5와 요구 조건 6을 만족한다. 따라서 본 방식은 전자 계약 시스템에서의 다중 서명 프로토콜의 요구 조건을 모두 만족한다. 이와 함께 본 제안 방식은 별도의 신뢰된 키 분배 센터가 필요하지 않게 되므로, 별도로 키 분배 센터에 대한 신뢰도를 평가하지 않아도 된다는 장점을 가지고 있다.

4.5 적용 예

이 절에서는 다중 서명 방식에 대한 실질적 전자계약의 적용 예를 들어 살펴본다. 서명 참여자를 3명이라 한다면 g값으로 425, P값을 1131이라고 가정하자. 그리고, 각 서명자는 자신들의 서명 정보를 다음과 같이 생성했다고 가정하자.

	r_i	s_i	e_i	y_i(공개정보)
서명자 1(U_1)	754	653	241	185
서명자 2(U_2)	351	263	324	926
서명자 3(U_3)	425	324	796	625

가. 서명 발생

첫 번째 서명자(U_1)는 다음과 같이 서명을 생성한다.

$$x_1 = (425)^{754} \bmod 1131 = 763$$
$$\sigma_1 = 754 + (653 * 241) = 158127$$

서명 데이타 정보 (763, 158127)를 모든 서명자에게 동보 전송한다.

두 번째 서명자 (U_2)는 다음과 같이 서명을 생성한다.

$$x_2 = (425)^{351} \bmod 1131 = 677$$
$$\sigma_2 = 351 + (263 * 324) = 85563$$

서명 데이타 정보 (677, 85563)를 모든 서명자에게 전달한다.

세 번째 서명자 (U3)는 다음과 같이 서명을 생성한다.

$$x_3 = (425)^{425} \bmod 1131 = 224$$
$$\sigma_3 = 425 + (324 * 796) = 258329$$

서명 데이타 정보 (244, 258329)를 모든 서명자에게 전달한다.

나. 서명 검증

각 서명자 및 검증자는 모든 서명이 끝나면 각 서명자들로부터 받은 서명 데이타 정보를 통해 다음과 같이 검증한다.

$$x_1 * x_2 * x_3 = 763 * 677 * 224 = 469 \pmod{1131}$$
$$\sigma_1 + \sigma_2 + \sigma_3 = 158127 + 85563 + 258329 = 502019$$
$$(425)^{502019} \bmod 1131 = 469 * (185)^{241} * (926)^{324} * (625)^{796} \bmod 1131 = 302$$

따라서 계산된 값은 302가 되므로, 수행된 전자 계약은 검증된다.

5. 요구 조건 만족도 비교 분석

Itakura - Nakamura 방식은 RSA 방식을 직접 반복 적용시 발생하는 서명 메시지의 길이 증가 및 서명 발생 속도의 문제점을 해결하였고, 다중 서명 메시지의 블록 수와 길이가 증가되지 않는다는 장점을 가지고 있다. 그러나 이 방식을 전자 계약시스템에 적용할 경우 최초 서명자의 법 N은 나중 서명자의 법 N보다 항상 작아야 하기 때문에 서명 순서가 제약받게 되어 무순서성을 만족하지 못한다.

Okamoto 방식은 Itakura - Nakamura 방식의 서명 순서가 제약받는다는 단점을 개선하였으며 다중 서명 메시지의 길이를 단순 서명 메시지의 길이와 거의 같게 하였다. 또한 일방향 함수를 사용함으로써 다중 서명 발생 및 검증을 효율적으로 처리 할 수 있도록 하였으며 RSA뿐만 아니라 어떠한 전단사 공개키 암호 시스템으로도 구성할 수 있다. 그러나 이 방식을 전자 계약시스템에 적용할 경우 첫 번째 서명자와 그 외의 서명자간의 서명 방법이 다르기 때문에 서명자간의 공통성을 갖지 못한다.

Fiat - Shamir방식에 근거하고 있는 Ohta - Okamoto 다중서명 방식은 서명자간의 공통성을 가지고 있으나 서명자 순서가 다를 경우 서명자의 부정을 조기에 검출할 수 없다는 문제점을 가지고 있다.

Kang Kim 방식 역시 Fiat Shamier방식에 근거한다. 이 방식은 Ohta-Okamoto의 단점으로 지적되었던 중간 서명자의 부정을 검출할 수 있게 함으로서 상기 요구조건들을 모두 만족하고 있다. 그러나, 이 방식은 그 전제 조건으로 신뢰된 키 분배 센터(TC)를 고려하고 있다.

이에 대해 제안된 방식은 순차 다중 서명 방식의 요구 조건을 모두 만족한다. 이산대수에 근거하고 있는 제안된 서명 방식은 서명자간에 공통성을 지니고 있으며, 서명자의 순서와 관계없이 서명이 가능하고 부정조기 검출성 및 일반성을 가지고 있다. 실제 적용 예에서 보았듯이 충분히 그 성능을 발휘하고 있으며, 모든 요구 조건 사항을 만족하고 있다고 볼 수 있다. 뿐만 아니라, 이 방식은 별도의 키 분배 센터를 필요로 하지 않는다는 장점을 가지고 있다. 다음은 전자 계약시스템에서의 각 다중 서명 방식들의 요구 조건에 대한 만족도를 표로 구성한 것이다.

6. 결 론

본 논문에서는 정보화 사회에 걸맞은 계약체결 시스템을 구성하기 위해 다중 서명 방식을 적용시켜 보았다. 먼저 효율적이고 신속하게 처리할 수 있는 전자 계약 시스템에 있어서 위험요소를 분석하였고 그에 따르는 다중 서명 방식의 요구조건을 제시하였다. 그리고 지금까지 개발된 기존의 디지털 다중 서명 방식들을 전자 계약 시스템에 적용하고 검토하였다. 이를 토대로 전자 계약 시스템에 적합한 새로운 다중 서명 방식을 제안하였으며, 각 방식별 전자 계약 시스템의 요구조건 및 만족도를 검토하였다. 본 논문에서 제안한 새로운 다중 서명 방식은 Itakura-Nakamura방식과는 달리 직급에 따른 키 변동이 없으며, Okamoto 방식이 가지고 있던 중간 사용자의 부정을 막을 수가 있었다. 또한 새로이 제안한 다중 서명 방식은 요구 조건을 모두 만족하며, 별도의 신

표 1. 전자 계약시스템에서의 다중서명 방식별 요구 조건 만족도

요구조건 / 방식	검증성	실행성	부정 검출성	공통성	일반성	무순서성	TC의 불필요성
Itakura-Nakamura방식[7]	○	○	○	○	○	×	○
Okamoto방식[8]	○	○	○	×	○	○	○
Kang-Kim방식[11]	○	○	×	○	○	○	×
Ohta-Okamoto방식[9]	○	○	○	○	○	○	×
제안 방식	○	○	○	○	○	○	○

뢰된 키 분배 센터가 필요하지 않기 때문에 다수의 계약자가 참여하는 전자 계약 시스템에 적합하다 할 수 있겠다.

본 논문에서 제안한 다중 서명 방식을 전자 계약 시스템에 적용할 경우, 각 서명자 중 누군가가 모든 서명 정보를 수신한 뒤 서명을 거절한다면 오직 자신은 모든 서명 정보를 얻지만 그 외의 다른 서명자는 최종 서명을 얻지 못하게 되는 불합리성이 생길 수 있다. 따라서 이러한 문제를 해결하기 위한 다자간 서명 동시 교환이 필요하고 이러한 동시성 문제를 해결할 다중 서명 프로토콜에 관한 연구가 필요하리라 본다.

참 고 문 헌

[1] T.Tanaka and K.Nakao, "Mutual Digital SignatureScheme 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 Crypto Systems 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] 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.

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

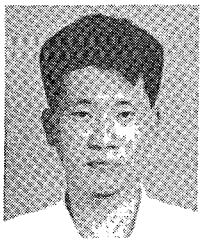
[8] T.Okamoto, "A digital Multisignature Scheme Using Bijective Public-Key Cryptosystems," ACM Trans. on Comp. Systems, Vol.6, No.8, pp.432-441, 1988.

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

[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.

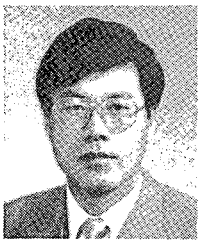
[11] 강창구, 김대영, "새로운 순차 및 동시 다중 서명 방식," 한국통신정보보호학회논문지, 제2권, 제1호, pp.36-44, 1992.

[12] 박희운, 강창구, 이임영, "새로운 디지털 다중 서명 방식에 대한 고찰," 한국통신정보보호학회 종합학술발표회 논문지, 제7권, 제1호, pp.101-110, 1997.



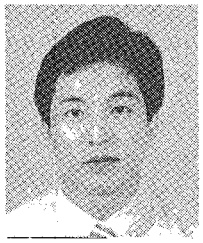
박 희 운(朴 喜 雲)

1997년 순천향대학교 전산학과 졸업
1997년~현재 순천향대학교 전산학과 대학원
관심 분야 : 암호이론, 컴퓨터 보안



강 창 구(姜 昌 求)

1975년 한국항공대학 항공전자공학과 졸업(공학사)
1986년 충남대학교 대학원 전자공학과(공학석사)
1993년 충남대학교 대학원 전자공학과(공학박사)
1979년~1982년 한국공군 기술장교
1987년~현재 한국전자통신연구원 부호3팀장 책임연구원
관심분야 : 운영체제, 분산처리체제, 컴퓨터통신보안



이 임 영(李 壬 永)

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