論文94-31A-1-3

전자 계약시스템에서의 디지틀 다중서명 방식

(Digital Multisignature Schemes in Electronic Contract Systems)

姜 昌 求*, 金 大 榮**

(Chang Goo Kang and Dae Young Kim)

要 約

본 논문에서는 전자적인 환경하에서 다수의 계약자가 계약을 처리할 수 있는 전자 계약시스템에서의 위험요소를 분석하고 디지틀 다중서명의 요구조건을 제시하였으며 지금까지 개발된 주요 디지틀 다중서명 방식들을 전자 계약시스템에 효율적으로 적용하고 새로운 디지틀 다중서명 방식을 제안하였다. 또한 각 방식별 요구조건 만족도를 검토하였으며 효율성을 서명처리 속도, 통신 복잡도 및 다중서명 길이 측면에서 분석하고 비교 평가하였다. 본 논문에서 새로이 제안된 다중서명 방식은 Fiat - Shamir 서명 방식에 근거하고 있기 때문에 서명처리 속도면에서 우수하여 실시간 처리가 가능하고, 요구조건 만족도가 높으므로 전자 계약시스템에 적합한 방식이라 할 수 있다.

Abstract

We analyze risks and present the requirements of digital multisignature in electronic contract systems where several persons contract a digital document electronically. We also apply a few digital multisignature schemes that have been developed so far, to the electronic contract system and propose a new digital multisignature scheme based on the Fiat - Shamir scheme.

We investigate how these schemes satisfy with the requirements and evaluate their efficiency in terms of processing speed, communication complexity, and message length. Owing to the high processing speed and the high degree of satisfaction to the requirements, the proposed scheme is suitable for electronic contract systems.

*正會員, 韓國電子通信研究所

(Electronics Telecommucation Reaserch Institut)

**正會員, 忠南大學校 情報通信學科

(Dept. of Elec. Eng., Chungnam Nat'l Univ.)

接受日字 : 1993年 1月 19日

I. 서 론

컴퓨터의 보급확산과 통신기술의 발전으로 종이 문서대신에 디지틀화된 전자문서가 등장하게 되었고, 이러한 전자문서는 전자우편이나 화일전송 등을 이용하여 빠른 시간내에 멀리 떨어진 상대방에게 전달되

고 교환될 수 있게 되었다. 이와 같은 환경하에서는 지금까지의 각종 계약에서 계약참여자들이 서로 만나서 계약문서를 작성하고 서명하는 번거로운 처리가 불필요하게 되었고, 대신 전자적인 계약환경을 구축하여 계약을 전자적으로 처리할 수 있게 되었다. 이것을 전자 계약시스템이라 한다.

전자 계약시스템은 계약처리 방법에 따라 계약 참여자가 계약문서를 전자우편등을 이용하여 순차적으로 회람 하면서 계약문서를 확인하고 서명한 후 다음 계약 참여자에게 전송하는 Off Line형 전자 계약시스템과 계약 참여자가 동일한 계약문서를 보유하고 통신매체를 통하여 실시간으로 계약을 수행하는 On Line형 전자 계약시스템이 있다.[11] 이와같은 전자 계약시스템에 있어서는 인감도장이나 손으로 쓴 서명 대신에 계약자가 각각 자신의 서명을 전자적으로 수행하는 디지틀 서명이 요구되고[2, 5], 또한 계약 보증인을 포함한 다수의 계약 참여자 혹은 다수의 계약자들이 전자계약을 수행하는데는 디지틀 다중서명이 요구된다.

이러한 다중서명에는 두 가지 종류가 있으며 하나는 같은 메세지를 서명자들이 순차적으로 서명을 수행하는 순차 다중서명 방식 (sequential multisignature scheme)이고, 다른 하나는 서명자들이 같은 메세지를 동시에 서명하는 동시 다중서명 방식 (simultaneous multisignature scheme)이다.[6]

지금까지 개발된 디지틀 다중서명 방식으로는 RSA 공개키 암호시스템[7]을 직접 반복하여 다중서명에 적용할 때 서명 메세지 길이의 증가 및 서명발생 속도의 문제점을 개선하기 위하여 두개의 큰 소수와 서명자에 따른 작은 소수의 곱을 이용하여 RSA방법을 직접 확대 적용한 Itakura 와 Nakamura 가 제안한 다중서명 방식(Itakura - Nakamura 다중서명 방식)[8], 서명 메세지의 길이증가 및 서명자의 순서제약을 해결하기 위하여 RSA방식과 같은 전단사 공개키 암호 시스템과 단방향함수를 이용한 Okamoto 가 제안한 다중서명 방식(Okamoto 다중서명 방식)[9], 및 서명 속도와 키 관리 방법을 개선하기 위하여 제안된 Fiat-Shamir 방식[10]에 근거한 방식으로 Ohta와 Okamoto 가 제안한 방식(Ohta-Okamoto 다중서명 방식)[6]과 본 저자들이 제안한 다중서명 방식이 있다.[11, 12]

본 논문에서는 전자 계약시스템에서의 위험요소와 디지틀 다중서명이 갖추어야할 요구 조건을 제시하고 지금까지 개발된 다중서명 방식을 이용하여 전자 계약시스템에 효율적으로 적용하였으며, On Line 형 전자 계약시스템에 적합한 새로운 디지틀 다중서명 방식을 제안하였다. 또한 방식별 요구 조건 만족도 및 효율성을 서명처리속도, 통신 복잡도, 및 다중서명 길이 측면에서 분석 비교하였다.

Ⅱ. 전자 계약시스템에서 디지틀 다중서명의 요구 조건

본 논문에서는 계약 참여자 전원이 컴퓨터를 보유하고 있으며, 전자계약을 체결하기 위하여 통신망에 접속되어 실시간으로 계약문서를 작성완료 하거나 미리 작성된 계약문서를 전원이 보유한후 최종적으로 계약문서에 디지틀 다중서명을 수행하는 On Line형 전자 계약시스템을 대상으로하였다. 또한 모든 계약 참여자는 성형의 통신망에 접속되어 있으며 개별 전송 뿐만아니라 bridge node 혹은 MCU등에 의해서 동시정보 전송을 할 수 있으며, 이때 bridge node 혹은 MCU는 동보전송 기능만을 갖는 것으로하였다.

이와 같은 전자 계약시스템에서는 복수의 계약 참여자에 의해서 전자적으로 계약을 체결하기 때문에 계약자간에 있어서의 다음과 같은 부정의 위험요소가 있을 수 있다.

위험요소 1 : 서명위조
계약자가 계약문서에 대하여 자신에게 유리하게 문서를 개조하고 그것에 부가된 다른 계약자의 서명을 위조한다.

위험요소 2 : 제 3 자와 계약 체결
계약 당사자가 아닌 다른 제 3자와 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 불법 사용
계약자가 전자적으로 수행한 서명은 디지틀 데이타이기 때문에 쉽게 복사될 수 있다. 따라서 계약자의 서명을 불법으로 사용할 수 있다.

위험요소 5 : 계약의 고의적 파기
계약자가 전자계약 문서에 서명을 수행할때 거짓 서명을 수행하여 계약을 무효화 시킨다.

위와같은 문제점을 고려하여 볼때 전자 계약시스템에 있어서 디지틀 다중서명의 요구 조건은 다음과 같다.[1]

요구 조건 1 : 검증가능성(Verifiability)
다중서명정보로부터 계약 문서가 정당한 계약자들에 의해서 서명되었다는 것을 계약자는 물론 제3자도 검증할 수 있어야 하고 계약 내용이 변경되었을 경우 이를 검증할 수 있어야 한다.

요구 조건 2 : 실행 가능성 (Viability)
다중서명 프로토콜이 끝난 시점에서 각 계약자는 모든 계약 참여자의 서명을 서로 보유할 수 있어야 한다.

요구 조건 3 : 부정 조기 검출성 (Dishonesty-Detectability)
다중서명 프로토콜 수행도중에 어떤 계약자가 부정을 행하였을 경우 계약 참여자 전원에 의해서 부정을 조기에 검출 할 수 있어야 한다.

요구 조건 4 : 공통성(Commonness)
계약자가 서명을 수행하는 서명 프로토콜은 모든 계약자가 공통이어서 모든 계약자의 서명 수행 방법이 같아야 한다.

요구 조건 5 : 일반성 (Generality)
다중서명 프로토콜은 두명의 계약자 즉, point-to-point간에도 그대로 적용할 수 있도록 호환성을 가져야 한다.

요구 조건 6 : 무 순서성(Orderlessness)
다중서명을 수행하는데 있어서 계약자의 서명순서가 고정되지 않고 임의적이어도 다중서명을 생성 및 검증할 수 있어야 한다.

단순서명 방식의 안전성이 유지되는한 다중서명의 요구 조건 1에 의해서 위험요소 1, 2, 4는 제거될 수 있고, 요구 조건 2에 의해서 위험요소 3은 불가능하며 또한 요구 조건 3에 의해서 위험요소 5를 방지할 수 있다.

본 논문에서는 m명의 서명자가 전자계약 다중서명 시스템에 참여하여 계약 문서에 서명한다고 가정하였으며, 본 논문에 사용되는 기호는 다음과 같이 정의한다.

M = 서명할 메세지
f, h = 공개된 단방향 함수
E_{ei} = 키 ei에 의한 공개키 암호함수
D_{di} = 키 di에의한 공개키 복호함수
$|N|$ = N의 비트길이
$[S]^{|L}$ = 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.
$\|$ = 연접 (concatenation)
ID_i = 서명자 i의 ID (이름, 주민등록 번호등)
ID_{cm} = 서명자들의 ID의 연접
즉, $ID_{cm} = ID_1 \| ID_2 \| \cdots, \| ID_m$ 이다.
k = 보안 변수 (security parameter)

Ⅲ. 기존 다중서명 방식의 전자 계약시스템 적용

1. Itakura - Nakamura 다중서명 방식의 적용

1) 키 발생 및 배포

단계 1 : 키 발급 센타는 두개의 큰소수 p, q를 선택하고 계약 서명자 i에 대하여 작은 소수 r_i를 선택한다.

$$N_i = p\ q\ r_i = N_0\ r_i \qquad (1)$$

계약 서명자의 r_i는 계약자간에 서로 다르도록 선택하여야 한다.

단계 2 : $\gcd(e, (p-1)(q-1)(r_i-1)) = 1$을 모든 i에 대해 만족하는 임의의 e를 계산한다. 이때 e는 $(p-1)(q-1)(r_i-1)$의 최소값보다 작고 (r_i-1)의 최대값보다 커야한다.

단계 3 : $e\ d_i = 1 \bmod (p-1)(q-1)(r_i-1)$을 만족하는 d_i를 계산한다.

단계 4 : e, N_0, r_i는 공개하고 키 발급 센타는 p, q를 비밀리에 보관하고 계약 서명자 i는 d_i를 비밀리 보관한다.

2) 다중서명 발생

(1) 첫번째 서명자(서명자1)의 서명 발생

단계 1 : 서명할 계약 문서 M에 대하여 자신의 비밀키 d_1으로 다음과 같이 서명을 수행한다.

$$S_1 = M^{d_1} \bmod N_1 \qquad (2)$$

단계 2 : 서명정보 S_1을 모든 서명자들에게 동보전송한다.

(2) n번째 서명자(서명자 n)의 서명발생

단계 1 : 앞 서명자로부터 서명정보 S_{n-1}을 수신하

면 서명자 n은 앞 서명자의 서명 S_{n-1}에 자신의 서명을 수행한다.

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

단계 2 : 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) 다중서명 검증

각 계약 참여자는 다중서명 수행도중 앞 서명자의 서명정보를 다음과같이 점검할 수 있다.

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

서명 프로토콜이 완료되면 계약 서명자 혹은 제 3자는 다중서명 검증을 다음식에 의해서 점검할 수 있다.

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

만약 위식이 만족되면 다중서명 정보는 유효한것으로 간주한다.

4) 방식 검토

본 방식은 다중서명 정보 S_m으로부터 다중서명 검증식 (5)에 의해 다중서명을 검증할 수 있으므로 요구 조건 1을 만족하고, 다중서명 프로토콜이 수행되고나면 각 계약 서명자는 최종 서명정보 S_m을 보유할 수 있으므로 요구 조건 2를 만족한다. 또한 다중서명 프로토콜 수행도중 계약 서명자가 부정을 행하였을 경우 모든 서명자는 검증식 (4)에 의해 부정이 조기에 검출될 수 있기 때문에 요구 조건 3을 만족한다. 각 서명자는 같은 서명방법에 의해서 서명을 수행하므로 요구 조건 4를 만족한다. 또한 본방식은 2자간 계약서명 시스템에도 그대로 적용 가능하므로 요구 조건 5를 만족하지만 본 서명 방식은 n_i값이 작은 서명자부터 서명을 순서적으로 수행하여야 하므로 요구 조건 6을 만족하지 못한다.

2. Okamoto 다중서명 방식의 적용

1) 키 발생 및 배포

서명자 i는 공개키 e_i와 비밀키 d_i를 발생하고 공개키인 e_i와 단방향 해쉬함수 h_i : $X_iX_iX_i\cdots X_i \cdots \rangle X_i$를 공개하고 비밀키 d_i를 비밀리 보관한다.

2) 다중서명 발생

(1) 첫번째 서명자(서명자1)의 서명 발생

단계 1 : 계약문서 M에 대하여 다음과같이 서명 S_1과 M_1를 발생한다.

$$S_1 = D_{d1}(h_1(M)) \quad (6)$$

$$M_1 = M \quad (7)$$

단계 2 : 서명정보 (S_1, M_1)과 자신의 식별자 ID_1을 모든 서명자들에게 동보전송한다.

(2) n번째 서명자(서명자 n)의 서명 발생

단계 1 : 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 $\langle X_n \rangle \mid X_{n-1}$ 이면

$$S_n = D_{dn}\left(\left|{}^{x}{}_{n}\right|\{S_{n-1}\}\right) \quad (8)$$

$$M_n = M_{n-1} \quad (9)$$

그렇지 않으면

$$S_n = D_{dn}\left(\left|{}^{x}{}_{n}\right|\left\{\left[S_{n-1}\right]\left|{}_{x_n}\right|_{-1}\right\}\right) \quad (10)$$

$$M_n = M_{n-1}\left|\left[S_{n-1}\right]\right|^{x}{}_{n}\right|^{-1} \quad (11)$$

여기서 X_n은 서명자 n의 평문과 암호문의 유한 집합을 나타낸다.

단계 2 : 서명정보 (S_n, M_n)와 서명자의 식별자 (ID_1, …, ID_n)을 모든 서명자들에게 동보전송한다. 만약 서명자가 마지막 서명자(서명자 m)이면 서명정보 (S_m, M_m)과 (ID_1, …, ID_m)을 모든 계약 참여자에게 동보전송한다. 이 때 최종 다중서명정보는 S_m, M_m과 서명자의 식별자 (ID_1, …, ID_m)이 된다.

3) 다중서명 검증

다중서명 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 다중서명정보 (S_m, M_m)을 다음과 같이 검증할 수 있다.

여기서 서명자의 순서는 서명정보에 첨부된 서명자의 식별자 (ID_1, …, ID_m)에 의하여 표시된다.

단계 1 : 다음식에 의해서 Mi'와 Si' (i = 1, 2, …, m)을 구한다.

여기서 $M_m' = M_m$이고 $S_m' = S_m$이다.

만약 $\mid X_i \rangle \mid X_{i-1} \mid$ 이면

$$S_{i-1'} = \left[E_{ei}(S_{i'})\right]|_{i-1}| \quad (12)$$

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

그렇지 않으면

$$S_{i-1}' = \left[M_i'\right]|_{xi-1}| - |_{xi}|_{+1}\Big\| \left[E_{ei}\left(S_i'\right)\right]|_{xi}|_{-1} \quad (14)$$

$$M_{i-1}' = \left[M_i'\right]\Big\|^{xi-1}\Big|^{xi}\Big|^{+1} \quad (15)$$

단계 2 : 위의 단계 1 에서 얻은 S_1'와 M_1'가 다음식을 만족하면 다중 서명 정보 (S_m, M_m)는 유효한것으로 간주한다.

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

다중서명 프로토콜 수행도중 앞 서명자들의 서명정보를 위에서 기술된 다중서명 검증식 (12) - (16)에 의거 점검할 수 있다.

4) 방식 검토

본 방식은 다중서명정보 S_m, M_m, (ID_1, …, ID_m)으로부터 다중서명 검증식 (12)- (16)에 의해서 다중서명을 검증할 수 있으므로 요구 조건 1을 만족하고, 다중서명 프로토콜이 수행완료되면 각 계약 서명자는 최종 서명정보 S_m, M_m, (ID_1, …, ID_m)을 보유할 수 있으므로 요구 조건 2를 만족한다. 또한 다중서명 프로토콜 수행도중 계약 서명자가 부정을 행하였을경우 모든 서명자는 검증식 (12) - (16)에 의해서 부정을 조기에 검출할 수 있으므로 요구 조건 3을 만족한다. 그러나 첫번째 서명자와 그외 서명자간의 서명방법이 다르므로 요구 조건 4를 만족하지 못한다. 또한 본 방식은 2자간 계약서명시스템에 그대로 적용가능하고, 서명자의 서명순서가 제약받지 않으므로 요구 조건 5와 요구 조건 6을 만족한다.

3. Ohta-Okamoto 다중서명 방식의 적용

1) 키 발생 및 배포

본 방식에서 키 발생 및 배포 절차는 서명자 i가 자신의 식별정보인 IDi를 키 발급센타에 등록하면 키 발급센타는 다음 절차에 의해 키를 발생 배포한다.

단계 1 : 키 발급센타는 두개의 큰소수 p와 q를 선택하고 그들을 비밀리 유지한다.

단계 2 : 키 발급 센타는 p와 q의 곱인 N = pq를 공개한다.

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

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

$$I_{ij}^{-1} = S_{ij}^2 \bmod N \quad (18)$$

단계 4 : 키 발급센타는 서명자 i에 대하여 물리적 식별을 한 후 (N, f, h, S_{ij},…,S_{ik})가 기록된 스마트 카드를 발급 배포한다.

2) 다중서명 발생

(1) 공통키 생성단계

① 첫번째 서명자 (서명자1)

단계 1 : 첫번째 서명자는 랜덤수 $R_1 \in Z_N$을 선택한다.
그리고 다음을 계산한다.

$$X_1 = R_1^2 X_0 \bmod N \quad (19)$$

여기서 X_0 = 1이다.

단계 2 : 서명자 1은 X_1을 모든 서명자들에게 동보전송한다.

② n번째 서명자 (서명자 n)

단계 1 : 서명자 n은 앞 서명자로부터 X_{n-1}을 수신하면 랜덤수 $R_n \in Z_N$을 선택하여 다음을 계산한다.

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

단계 2 : 서명자 n은 Xn을 모든 서명자들에게 동보전송한다. 만약 서명자가 마지막 서명자 (서명자 m)이면 X_m을 동보 전송한다.

(2) 서명 생성 단계

① 첫번째 서명자의 서명 발생

단계 1 : 첫번째 서명자는 다음과 같이 서명을 발생한다.

$$(e1,\cdots,ek) = h(M, ID_{cm}, X_m) \quad (21)$$

$$Y_1 = Y_0 R_1 \prod_{ej=1} S_{1j} \bmod N,\ j = 1,2,\cdots,k \quad (22)$$

여기서 Y_0 = 1이고, ID_{cm}은 계약문서 M상에 기록된 서명자들의 ID리스트이다.

단계 2 : 첫번째 서명자는 서명정보 Y_1을 모든 서명자들에게 동보전송한다.

② 서명자 n의 서명 발생

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

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

$$Y_n = Y_{n-1} R_n \prod_{ej=1} S_{nj} \mod N, j = 1, 2, \cdots, k \quad (24)$$

단계 2 : 서명자 n은 서명정보 Y_n을 모든 서명자들에게 동보전송한다.
서명자가 마지막 서명자(서명자 m)이면 서명정보 Y_m을 모든 서명자에게 동보 전송한다.

3) 다중서명 검증

다중서명 프로토콜이 수행 완료되면 모든 서명자는 ID_{cm}, (e_1, …, e_k), Y_m을 보유하게 된다. 모든 계약 서명자 혹은 제3자는 다중서명 정보 (ID_{cm}, (e_1, …, e_k), Y_m)에 대하여 공개된 법 N과 단방향 함수 f, h를 이용하여 다음과 같이 다중 서명을 검증할 수 있다.

단계 1 : 서명 검증자는 ID_{cm}으로부터 서명자의 I_{ij}를 계산한다.

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

단계 2 : 서명검증자는 Z_m을 다음과 같이 계산한다.

$$Z_m = Y_m^2 \prod_{i=1}^{m} \prod_{ej=1} I_{ij} \mod N, \ j = 1, 2, \ldots, k \quad (26)$$

단계 3 : 서명 검증자는 $h(M, ID_{cm}, Z_m)$을 계산하고 다음식이 만족되는지를 확인한다.

$$(e1, \cdots, ek) = h(M, ID_{cm}, Z_m) \quad (27)$$

만약 식(27)이 만족되면 그 다중서명 메세지는 유효한것으로 판명한다.

4) 방식 검토

본 방식은 다중서명 프로토콜이 수행 완료되면 각 계약 서명자는 최종 서명정보 ID_{cm}, (e_1, …, e_k), Y_m을 가지게 되고, 이들 정보로부터 다중서명 검증식 (25) - (27)에 의해서 다중서명을 검증할 수 있으므로 요구 조건 1과 요구 조건 2를 만족한다. 또한 서명자의 순서가 바뀌어지면 최종서명정보 ID_{cm}, (e_1, …, e_k), Y_m로부터 다중서명검증식 (25) - (27)에 의해서 다중 서명정보를 검증할 수 있으므로 요구 조건 6은 만족하나, 다중서명 프로토콜 수행중에 중간 서명자가 부정을 행하였을 경우에는 이를 조기에 발견할 수 없으므로 요구 조건 3을 만족하지 못한다. 본 방식은 2자간 계약서명시스템에도 그대로 적용가능하고 또한 각 서명자가 수행하는 서명 방법이 같으므로 요구 조건 4와 요구 조건 5를 만족한다.

Ⅳ. 새로운 다중서명 방식 제안

1. 키 발생 및 배포

본 방식에서 키 발생 및 배포 절차는 서명자 i가 자신의 식별정보인 IDi를 키 발급센타에 등록하면 키 발급센타는 다음 절차에 의해 키를 발생 배포한다.

단계 1 : 키 발급센타는 두개의 큰소수 p와 q를 선택하고 그들을 비밀리 유지한다.

단계 2 : 키 발급 센타는 p와 q의 곱인 N = pq를 공개한다.

단계 3 : 키 발급센타는 각 서명자 i에 대하여 Sij를 다음과 같이 계산한다.

$$I_{ij} = f(ID_i, j), \ j = 1, 2, \cdots, k \quad (28)$$

$$I_{ij}^{-1} = S_{ij}^2 \mod N \quad (29)$$

단계 4 : 키 발급센타는 서명자 i에 대하여 물리적 식별을 한 후 (N, f, h, S_{ij}, …, S_{ik})가 기록된 스마트 카드를 발급 배포한다.

2. 다중서명 발생

1) 첫번째 서명자의 서명 발생

단계 1 : 첫번째 서명자는 랜덤수 $R_1 \in Z_N$을 선택한다.
그리고 다음을 계산한다.

$$X_1 = R_1^2 X_0 \mod N \quad (30)$$

$$(e11, \cdots, e1k) = h(M, ID_{cm}, X_1) \quad (31)$$

$$Y_1 = Y_0 R_1 \prod_{e1j=1} S_{1j} \mod N, j = 1, 2, \cdots, k \quad (32)$$

여기서 X_0 = 1, Y_0 = 1 이고, ID_{cm}은 계약문서 M상에 기록된 서명자들의 ID리스트이다.

단계 2 : 첫번째 서명자는 서명정보 (X_1, Y_1)를 모든서명자에게 동보 전송한다.

2) n번째 서명자(서명자 n)의 서명 발생

단계 1 : 서명자 n은 서명자 (n-1)로부터 서명정보 X_{n-1}, Y_{n-1}를 수신하면 서명을 하기 위하여 랜덤수 $R_n \in Z_N$을 선택하고 다음을 계산한다.

$$X_n = R_n^2 X_{n-1} \mod N, \quad (33)$$

$$(en1, \cdots, enk) = h(M, ID_{cm}, X_n) \quad (34)$$

$$Y_n = Y_{n-1} R_n \prod_{enj=1} S_{nj} \mod N, \ j = 1, 2, \cdots, k \quad (35)$$

단계 2 : 서명자 n은 서명정보 (X_n, Y_n)를 모든 서명자에게 동보전송 한다. 만약 서명자가 마지막 서명자 (서명자 m)이면 (X_m, Y_m)를 동보전송한다.

3. 다중서명 검증

다중서명 프로토콜이 수행 완료되면 모든 서명자들은 계약문서 M과 계약문서상의 ID_{cm} 및 다중서명정보 (X_1, …, X_m, Y_m)를 보유하게되고 다음과같이 (e_{11}, …, e_{1k}), …, (e_{m1}, …, e_{mk})을 계산한다.

$$(ei1,\cdots,eik) = h(M, ID_{cm}, X_i), i = 1,\cdots,m \qquad (36)$$

그리고 다중서명 검증을 위하여 서명정보(ID_{cm}, (e_{11}, …, e_{1k}), …, (e_{m1} ,…, e_{mk}), Y_m)를 저장 보관한다. 계약자 혹은 서명검증자는 다음과 같이 다중서명을 검증할 수 있다.

단계 1 : 서명검증자는 ID_{cm}으로부터 서명자들의 I_{ij}를 계산한다.

$$I_{ij} = f(ID_i, j),\ i = 1,2,\cdots,m,\ j = 1,2,\cdots,k \qquad (37)$$

단계 2 : 서명검증자는 Z_m을 다음과 같이 계산한다.

$$Z_m = Y_m^2 \prod_{i=1}^{m} \prod_{cj=1} I_{ij} \bmod N,\ j = 1,2,\ldots,k \qquad (38)$$

단계 3 : 서명검증자는 h(M, ID_{cm}, Z_m)을 계산하고 다음식이 만족되는 지를 확인한다.

$$(em1,\cdots,emk) = h(M, ID_{cm}, Z_m) \qquad (39)$$

만약 식 (39)이 만족되면 그 다중서명 정보는 유효한것으로 판명한다.

4. 방식 검토

본 방식은 다중서명 프로토콜이 수행되고나면 계약서명자는 최종서명정보 ID_{cm}, X_1, …, X_m, Y_m을 가지게되고, 또한 이들 정보로부터 다중서명 검증식 (37) - (39)에 의해서 다중서명을 검증할 수 있으므로 요구 조건 1과 요구 조건 2를 만족한다. 다중서명 프로토콜 수행도중 중간 서명자가 부정을 행하였을 경우에는 위의 검증 절차에의해서 이를 조기에 검출할 수 있으므로 요구 조건 3을 만족하고, 각 서명자가 수행하는 서명방법이 같으므로 요구 조건 4를 만족한다. 또한 본 방식은 2자간 계약서명시스템에도 그대로 적용가능하고 서명자의 서명 순서에 제약이 없으므로 요구 조건 5와 요구 조건 6을 만족한다. 따라서 본 제안방식은 전자 계약시스템에서의 다중서명 프로토콜의 요구 조건을 모두 만족한다.

V. 요구 조건 만족도 및 효율성 분석

1. 요구 조건 만족도

전자 계약시스템에서의 요구 조건에 대하여 앞에서 기술한 다중서명 방식들의 만족도는 표 1과 같다.

표 1. 다중서명 방식별 요구 조건 만족도
Table 1. Degree of satisfaction to the requirements.

요구조건 / 적용방식	검증 가능성	실행 가능성	부정조기 검출성	공통성	일반성	무순서성
Itakura-Nakamura 다중서명 방식	0	0	0	0	0	X
Okamoto 다중서명 방식	0	0	0	X	0	0
Ohta-Okamoto 다중서명 방식	0	0	X	0	0	0
제안된 다중서명방식	0	0	0	0	0	0

Itakura - Nakamura 다중서명 방식은 RSA 방법을 직접 반복 적용시 서명 메세지의 길이 증가 및 서명 발생속도의 문제점을 해결하였고, 다중서명 메세지의 블럭수와 길이가 증가되지 않는다는 장점을 가지고 있으나 이 방식을 전자 계약시스템에 적용시 나중 서명자의 법 N이 앞 서명자의 법 N보다 항상 커야하기때문에 서명 순서가 제약받게되어 무순서성을 만족하지 못한다.

Okamoto 다중서명 방식은 Itakura-Nakamura 다중서명 방식의 서명 순서가 제약받는다는 단점을 개선하였으며 다중서명 메세지의 길이를 단순 서명 메세지의 길이와 거의 같게하였다. 또한 단방향 해쉬 함수를 사용함으로써 다중서명 발생 및 검증을 효율적으로 처리할 수 있도록 하였으며 RSA뿐만아니라 어떠한 전단사 공개키 암호 시스템으로도 구성할 수 있다. 그러나 이 방식을 전자 계약시스템에 적용시 첫번째 서명자와 그외 서명자간의 서명 방법이 다르므로 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 없다. 본 논문에서 새로이 제안

된 다중서명 방식은 전자 계약시스템에서의 다중서명 방식의 요구 조건을 모두 만족한다.

2. 서명처리 속도

서명처리 속도는 서명자가 서명을 발생하는데 요구되는 처리량으로 평가하였다. 단방향함수 f, h는 모듈라 곱셈에 비하여 훨씬 빠르므로 모듈라 곱셈의 수만으로 계산하였다. 서명자가 서명을 생성하는데 소요되는 모듈라 곱셈수는 표 2에서와 같이 RSA에 근거한 Itakura-Nakamura 다중서명 방식과 Okamoto 다중서명 방식은 1.5 | N | 번의 모듈라 곱셈이 요구되고, Ohta-Okamoto 다중서명 방식과 본 논문에서 제안한 새로운 다중서명 방식은 (k/2 + 3) t번의 모듈라 곱셈이 요구된다. 여기서 t는 비도를 높이기 위한 다중 서명의 반복 횟수를 의미한다.

표 2. 다중서명 방식별 효율성 비교
Table 2. The comparison of efficiency.

항 목 \ 방 식	Itakura-Nakamura 다중서명방식	Okamoto 다중서명방식	Ohta-Okamoto 다중서명방식	제안된 다중서명방식
서명처리속도 (모듈라 곱셈수)	1.5 |N|	1.5 |N|	(k/2 + 3) t	(k/2 + 3) t
다중서명 길이 (비트)	|N|	|M|+ |N|	m|ID|+kt+|N|	m |ID| + k t m + |N|
통신 회수	m	m	2m	m

예를 들면, k = 72이고, t = 1이고, | N | = 512일 때 모듈라 곱셈수는 Ohta-Okamoto 다중서명 방식과 새로이 제안된 다중서명 방식은 39번이 요구되고, Itakura-Nakamura 다중서명 방식과 Okamoto 다중서명 방식은 768번의 모듈라 곱셈이 요구된다. 따라서 Fiat-Shamir방식에 근거하고 있는 제안된 다중서명 방식은 서명자가 서명을 발생하는 서명 처리속도면에서 RSA에 근거한 방식보다 훨씬 효율적이라 할 수 있다.

3. 통신 복잡도

통신 복잡도는 m명의 서명자가 전자 계약시스템에 가입되어 계약문서에 서명한다고 할때 다중서명을 수행하는데 있어서 요구되는 서명자들의 정보 전송회수의 합으로 평가하였다. 또한 동보전송은 bridge node혹은 MCU에 의해서 동시에 전송되는 것으로 간주하여 전송 회수를 1회로 계산하였다. 표 2에서와 같이 Itakura-Nakamura 다중서명 방식, Okamoto 다중서명 방식, 제안된 다중서명 방식은 m번의 정보전송으로 다중서명을 수행할 수 있으나, Ohta-Okamoto 다중서명 방식은 2m번의 정보전송이 요구된다.

4. 다중서명의 길이

본 논문에서는 다중서명 길이를 계약문서의 다중서명을 검증하기 위해서 서명자가 보관하여야 하는 서명정보의 양으로 계산하였다. 서명자 수가 m명일때 표 2에서와 같이 Itakura-Nakamura 다중서명 방식은 N 비트, Okamoto 다중서명 방식은 (| M | + | N |)비트가 저장되어야 하고, Ohta-Okamoto 다중서명 방식은 {m | ID | + k t + | N | }비트, 제안된 다중서명 방식은 {m | ID | + k t m + | N | }비트가 저장되어야 한다. Ohta-Okamoto 다중서명 방식과 새로이 제안한 다중서명 방식은 보안 레벨 변수 k t에 따라 서명길이가 달라진다.

Ⅵ. 결 론

본 논문에서는 정보화 사회에서의 계약체결을 보다 효율적이고 신속하게 처리할 수 있는 전자 계약시스템에 있어서 위험요소를 분석하고 다중서명 방식의 요구 조건을 제시하였다. 또한 지금까지 개발된 주요 디지틀 다중서명 방식을 전자 계약시스템에 적용하고 검토하였으며 전자 계약시스템에 적합한 새로운 다중서명 방식을 제안하고, 각 방식별 전자 계약시스템의 요구 조건 만족도를 검토하였으며 효율성을 서명 처리속도, 통신복잡도 및 다중서명 길이 측면에서 분석하고 비교 평가하였다.

본 논문에서 새로이 제안된 다중서명 방식은 Fiat-Shamir 방식에 근거하고 있기 때문에 Fiat-Shamir 방식의 모든 장점을 가지고 있으며 Itakura-Nakamura 다중서명 방식과 Okamoto 다중서명 방식보다 서명처리 속도면에서 우수하고, Ohta-Okamoto 다중서명 방식보다 다중서명 길이는 증가되나 통신 복잡도 문제를 해결하였다. 또한 새로이 제안된 다중서명 방식은 요구 조건을 모두 만족하므로 다수의 계약자가 참여하는 전자 계약시스템에 적합한 디지틀 다중서명 방식이라 할 수 있다.

본 논문에서는 모든 서명자가 정직하게 다중서명 절차를 수행한다고 가정하였다. 그러나 마지막 서명자가 다른 서명자들의 서명 정보를 전달 받은후 자신의 서명 정보를 전달하지 않을 경우, 마지막 서명자는 모든 서명자의 다중서명을 가지게 되나 다른 서명자는 계약 참여자 전원의 다중서명을 얻을 수 없게

되어 불이익을 받게된다. 따라서 이러한 문제를 해결하기 위해서는 다자간의 서명 동시교환이 요구되고, 이러한 동시성 (concurrency) 문제를 해결할 수 있는 다중서명 프로토콜에 관한 연구가 요구된다.

參考文獻

[1] T.Tanaka and K.Nakao, "Mutual digital signature scheme on on-line electronic contract wywtem," 일본정보통신학회 기술연구보고서, ISEC 91-46, pp. 19-25, 1991.

[2] D.W.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.C. Guillou and J.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.L. 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] 강창구, 김대영, "순차적 다중서명 방식," 한국통신학회 하계 종합학술발표회 논문집, pp. 31-35, 1992.

[12] 강창구, 김대영, "새로운 순차 및 동시 다중서명 방식," 한국통신정보학회논문지, 제2권 1호, pp.36-44, 1992.

著者紹介

姜 昌 求(正會員)

1957年 3月 1日生. 1979年 2月 한국항공대학 항공전자공학과 (공학사). 1986年 2月 충남대학교 대학원 전자공학과(공학석사). 1993年 8月 충남대학교 대학원 전자공학과(공학박사). 1979年 ~ 1982年 한국공군 기술장교. 1987年 ~ 현재 한국전자통신연구소 부호기술부 책임연구원.

金 大 榮(正會員)

1952年 5月 28日生. 1975年 2月 서울대학교 공과대학 전자공학과 (B.S). 1977年 2月 KAIST 전기 및 전자공학과 (M.S). 1983年 2月 KAIST 전기 및 전자공학과 (Ph.D). 1978年 ~ 1981年 독일 RWTH Aachen, UNI Hannover 공대 연구원. 1987年 ~ 1988年 미국 University of California Davis 분교 객원연구원. 1983年 ~ 현재 충남대학교 정보통신공학과 교수.