새로운 디지탈 다중 서명 방식에 대한 고찰

°박희운*, 강창구**, 이임영*

*: 순천향 대학교 **: 한국전자통신연구원

A Study on New Digital Multi Signature Method

Hee-Un Park*, Chang-Goo Kang**, Im-Yeong Lee*

* *Department of Computer Science, Soonchunhyang University*
** *Electronics and Telecommucations Research Institute*

요 약 문

본고에서는 수신된 데이터의 무결성과 데이터에 대한 수신자의 인증을 위해 기존의 디지탈 다중 서명을 분석하여 더욱 향상된 디지탈 다중 서명 방식을 제안하고자 한다.

기존의 디지탈 다중 서명 방식이 ID-based한 특징을 갖는데 비해 제안한 디지탈 다중 서명 방식은 이산 대수에 근거해 계산하고 있다. 이 방식은 형식면에서 더욱 간편하고, 계산적인 면에서 랜덤수를 저장하지 않으므로서 현실적이며 효율적이라 할 수 있다.

I. 서 론

현대 사회의 가장 큰 특징을 기술하라고 한다면, 지금껏 쓰던 종이 문서의 이용에서 탈피해 사회 저변적으로 컴퓨터가 보급 확산 되고 있다는 점을 들 수 있다. 또한, 통신망의 발전을 통해 멀리 떨어진 곳에서도, 움직이는 차량안에서 자신의 의사를 정확하고 신속하게 전달하는 수준에 까지 도달하고 있다. 이와 같이 컴퓨터의 보급 확산과 디지탈 통신망(초고속 통신망)의 급속한 발전은 종래 종이를 사용하여 수행되던 모든 일과를 변혁에 가까울 정도로 변화 시키면서 정보화 사회로 진일보하고 있다. 이러한 정보화 사회로의 발전을 통해 과거에는 생각만으로 그치던 상상들이 실생활에서 이루어 지고 있다. 예를 들어 재택근무, 홈 쇼핑, 인텔리젼트 빌딩, 네트워크를 이용한 각종 행정 서류의 전산화, 군 주요 정보 전달 등등이 그것이다. 그 중 과거의 종이 문서를 대신해 컴퓨터와 디지탈 통신망에서 사용되는 디지탈 문서의 도입은 그 새로운 혁명의 기초가 된다고 해도 과언이 아닐 것이다.

예를 들어 보면, Internet을 이용해서 많은 일들을 할 수 있다. 서로 컴퓨터를 통해 가지고 있는 정보를 디지탈 통신망 등을 이용해 교류도 할 수 있고, 그 밖에도 Internet을 통한 전자 상거래(홈 쇼핑), 전자 메일을 통한 전자 서신 교류, 새로이 쏟아지는 각종 정보를 편리하고, 쉽게 받아 보는 등. 그 예의 열거는 이루 헤아릴 수 없을 정도다. 위 예에서도 살펴보았듯 정보화된 사회에서는 컴퓨터를 통해 각종 정보를 디지탈 문서화 시키고, 이러한 디지탈 문서를 통신망을 이용해 서로 교류하는 모습을 볼 수 있다. 이렇듯 디지탈 문서는 정보화 사회에서 하나의 정보로서 작용하고, 그만큼 중요하게 처리되어야 한다는 것은 자명한 사실일 것이다. 그러나, 이러한 디지탈 문서를 정보화 사회에 도입

함에 있어 어떤 고려 사항이 있을까? 간단히 생각해 본다면, 과연 정보교환의 상대는 누구인가? 자신이 보낸 정보가 정확히 전해졌는가? 정보가 불법적으로 제 3 자에 의해 수정되지는 않았는가? 정말 통신하는 상대방에게 정확하게 정보가 전달되었는가? 등등. 많은 고려 사항을 가지고 있는 것이 현실이다. 이런 현실 속에서 과연 이런 문제들을 해결할 방법은 없는 것인가? 이를 위해 많은 방법들이 존재 할 수 있겠으나 현재는 메세지의 불법적 수정 및 도용을 막을 수 있는 메세지 인증과 통신하는 대상자가 정확한지를 확인하는 사용자 인증 등의 방법들이 제시 되어 있으며, 특히 디지탈 서명과 같은 방법을 통해 메세지 인증과 사용자 인증을 동시에 수행하려 하고 있다. .

그러나, 기존에 사용하고 있는 디지탈 서명은 주로 두 사람을 대상으로 하고있다. 따라서, 실 생활에 적용시키려 하다 보면 양자간 디지탈 서명으로는 해결이 불가능한 경우가 발생한다. 그 한 예를 살펴보자. 어느 한 기업의 사무실이 있다고 가정할 때 각 팀별로 상급자와 하급자가 존재할 것이다. 이때 한 문서를 기안 하더라도, 그에 대한 서명자들은 계층적 구조 속에서 여러 명이 있을 수 밖에 없을 것이다. 이와 같은 현실에서 하나의 디지탈 메세지 문서에 대해 여러 사람이 디지탈 서명을 하여야 하는데, 바로 이런 것을 해결하기에는 양자간 디지탈 서명으로는 한계가 올 수 밖에 없을 것이다. 이에 대해, 디지탈 서명에 있어 대상을 두 명에서 n 명으로 확대한 개념의 서명을 생각하게 되었는데 이를 디지탈 다중 서명(Digital Multisignature)이라고 한다. 이런 디지탈 다중 서명 방식은 계층적 구조로 구성되어 있는 일반 회사나 관공서 등의 문서 결재라든가, 일반적인 상거래 계약이나, 화상 회의를 통한 국제 협상에서의 협약서 서약 등에서 사용 될 수 있다.

II. 디지탈 다중 서명 방식

2.1 디지탈 다중 서명의 개념 및 종류

디지탈 다중 서명 방식은 디지탈 서명 방식과는 성격이 약간 다르다. 명명 되어진 것으로부터 알 수 있지만, 디지탈 서명 방식이 양자간의 디지탈 문서를 그 대상으로 하는 반면에 디지탈 다중 서명 방식은 그 개념이 확대되어 두 명 이상의 사용자간에 디지탈 문서를 그 대상으로 하고 있다. 따라서, 디지탈 다중 서명 방식은 시스템의 구성 측면에서, 각각의 서명을 어떻게 수행해야 할지, 어떤 방식을 적용하느냐에 따라 세심한 배려가 요구된다.

다중 서명 방식에는 크게 두 가지의 종류가 있다. 하나는 순차 다중 서명 방식으로 하나의 같은 메세지에 대해 각 서명자가 순차적으로 회람하면서 자신의 디지탈 서명을 수행하는 방식이고, 두 번째는 동시 다중 서명 방식으로 각 서명자에게 똑같은 사본을 나눠주고 같은 시간에 디지탈 서명을 수행 하는 방식이다. 각각의 용도를 살펴보면, 순차 다중 서명 방식은 계층적 구조를 가지고 있는 회사라던가 관공서에서 문서 결재에 사용할 수 있으며, 동시 다중 서명 방식은 여러 사람들이 참여하여 계약을 성립시키는 상거래라던가 다자간 국제 협상시 문서 계약에 많이 사용되리라 본다.

그 종류를 세부적으로 살펴보면, RSA 디지탈 서명 방식을 적용한 Itakura-Nakamura 방식이 있고, 전단사 공개키 암호 시스템과 One-Way 함수를 이용한 Okamoto 방식, Fiat-Shamir 방식에 근거한 Ohta-Okamoto 방식 및 Kang-Kim 방식등의 다중 서명 방식이 있다.

2.2 디지탈 다중 서명의 요구 조건

디지탈 다중 서명 방식은 디지탈 서명 방식과는 사용 성격이 약간 다르기 때문에 디지탈 서명 방식에서 고려하고 있는 사항 이외에 부가적인 조건들이 필요하다. 다음은 디지탈 다중 서명 방식이 갖추어야 할 조건들을 서술한 것이다.

조건 1) 서명문의 길이 고정 :
디지탈 다중 서명 방식은 기본적으로 여러 사람들이 네트워크상에서 자신의 컴퓨터가 연결되어 있다는 가정을 만족한다. 따라서, 속도 및 효율성을 고려해야 함은 자명한 사항이다. 그러므로, 다중 서명의 생성에 참여한 서명자들이 만들어 내는 서명문의 길이는 서명인의 수에 상관없이 고정 되어야 할 것이다.

조건 2) 검증 가능성 :
디지탈 다중 서명은 디지탈 서명 방식을 응용한 것이다. 그러므로, 디지탈 서명 방식에서 고려한 사항은 디지탈 다중 서명 방식에서도 적용되며, 특히 다중 서명 정보로부터 서명된 문서가 정당한 서명 참여자에 의해서 서명되었다는 것을 서명 참여자들은 물론 제 3 자도 검증할 수 있어야 한다.

조건 3) 부정 조기 검출성 :
디지탈 다중 서명 방식은 여러 서명자를 대상으로 하고 있기 때문에 각각의 서명자들에 대한 서명을 중간 서명자가 언제든지 검증할 수 있어야 한다.

조건 4) 비밀 유지성 :
디지탈 서명방식은 암호학을 그 근간으로 하고있으며, 암호학은 정보에 대한 보호를 그 목적으로 하고 있다. 따라서, 여러 서명자들이 참여하는 디지탈 다중 서명 방식은 중간 혹은, 그 어떤 경우에 있어서도 다중 서명 정보에서 개인의 비밀 정보를 유추해 낼 수 없어야 한다.

조건 5) 공통성 :
서명 참여자들의 혼선을 피하고, 일괄적인 서명 및 검증을 위하여 다중 서명 생성에 참여하는 각 서명자들이 이용하는 서명 프로토콜은 모두 동일해야 한다.

III. 기존의 다중 서명 방식 분석

3.1 Itakura-Nakamura 다중 서명 방식

순차적 서명 방법의 한 예로 RSA 방식을 직접 서명에 적용한 방식이다. 그래서, 상급자의 법 N 이 하급자의 법 N 보다 커야 되는 특징이 있다.

● 키 발생 및 배포

1) 세개의 큰 소수 p, q, r_i를 선택하고, 서명자 i의 직위에 따른 법 N_i를 생성하고, 이것을 공개한다.

$$N_i = p*q*r_i = N_0*r_i$$

(상급자 N이 하급자 N보다 크도록 소수 r_i를 선택)

2) $\gcd(e, (p-1)(q-1)(r_i-1))$
를 만족하는 임의의 상대 소수 e를 선택하고, 공개한다.

(단, $\mathrm{Max}(r_i-1) < e < \mathrm{Min}(p-1)(q-1)(r_i-1)$)

3) $ed_i = 1 \bmod (p-1)(q-1)(r_i-1)$를 만족하는 d_i를 계산하여, 비밀로 한다.

4) e, N_0, r_i는 공개하고, d_i, p, q는 비밀로 보관한다.

◆ 다중 서명 발생

● 서명자 1의 서명 발생

1) 서명자는 계산한 d_1를 가지고 $S_1 = M^{d_1} \bmod N_1$을 계산한다.

2) 서명 메세지 (S_1, M)을 다음 서명자에게 전송한다.

● 서명자 n의 서명 발생

1) 앞 서명자의 서명 메세지를 점검할 수 있으며, 이 단계는 생략 가능 하다.
2) 서명자 n은 앞 서명자의 서명 (S_{n-1})에 다음과 같이 서명한다.

$$S_n = S_{n-1}^{dn} \bmod N_i.$$

3) 서명 메세지 (S_n, M)을 다음 서명자 n+1에게 전송하며,
마지막 서명자는 서명 메세지를 검증자에게 보낸다.

● 다중 서명 검증

검증자는 다음식 $(\ldots (S_m^e \bmod N_m)^e \ldots \bmod N_2)^e \bmod N_1 = M \bmod N_1$ 이 만족하는지 확인하여 검증을 한다.

Ex1) n 이 3 일때의 검증 확인 및 논리

$S_1 = M^{d1} \bmod N_1$
$S_2 = (S1)^{d2} \bmod N_2$
$S_3 = (S2)^{d3} \bmod N_3$
$= \{ (S1)^{d2} \bmod N_2 \}^{d3} \bmod N_3$
$= [\{ (M^{d1}) \bmod N_1 \}^{d2} \bmod N_2]^{d3} \bmod N_3$
$\{(S_3^e \bmod N_3)^e \bmod N_2\}^e \bmod N_1$
$= \{ ([\{ (M^{d1}) \bmod N_1 \}^{d2} \bmod N_2]^{d3e} \bmod N_3)^e \bmod N_2 \}^e \bmod N_1$
$= M \bmod N_1$ (단, $N_3 > N_2 > N_1$)

3.2 Ohta-Okamoto 다중 서명 방식

ID-based 방식인 Fiat-Shamir 방식에 근거한 다중 서명 방식이다.

● 키 발생 및 배포

서명자 i가 ID_i를 TC(Trusted Center)에 등록한 뒤 TC는 다음 절차에 의해 키 발생 및 배포를 하게 된다.

1) TC에서는 두 개의 큰 소수 p,q를 생성 및 비밀리 유지한다.
2) p,q를 가지고

$$N = p*q$$

인 N을 공개한다.
3) 서명자i에 대하여 S_{ij}를 계산한다.

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

$$I_{ij} = S_{ij}^2 \bmod N$$

4) TC에서는 $(N,f,h,S_{i1},\ldots.S_{ik})$가 기록된 스마트 카드를 발급 배포한다.

◆ 공통키 생성 단계

● 서명자 1

1) 랜덤수 $R_1 \in Z_n$을 선택하고, 다음과 같이

$$X_1 = R_1^2 \bmod N$$

을 계산한다.
2) X_1을 다음 전송자에게 전송한다.

● 서명자n

1) 앞 서명자로부터 X_{n-1}를 수신하면 랜덤수 $R_n \in Z_n$ 을 선택해 자신의 서명 정보

$X_n = R_n^2 X_{n-1} \bmod N$ 을 계산해 낸다.

2) X_n 을 다음 서명자에게 전송, 마지막 서명자일 경우 X_m을 기안자에게 전송한다.

◆ 서명 생성 단계

● 서명자 1의 서명 발생

1) 서명할 사람의 순서를 다음과 같이

$(ID_{cm} = ID_1$(서명자 1)$\| ID_2 \| \cdots \| ID_m$(최종)$)$을 결정한다.

2) 서명 정보

$$Y_1 = R_1 \prod_{j=1}^{k} S_{1j} \bmod N,\ (j=1,2,\ldots,k)$$

를 계산 한 뒤 다음과 같이 서명 $(e_1,\ldots e_k) = h(M, ID_{cm}, X_m, Y_1)$을 생성하여 다음 서명자에게 전송한다.

3) 다음 서명자에게(M, ID_{cm}, X_m, Y_1)을 전송

● 서명자 n의 서명 발생

1) $(M, ID_{cm}, X_m, Y_{n-1})$를 수신하면 자신의 서명 정보를 다음과 같이 계산한다.

$$(e_1,\ldots e_k) = h(M, ID_{cm}, X_m)$$

$$Y_n = Y_{n-1} \prod_{j=1}^{k} S_{nj} \bmod N, (j=1,2,\ldots,k)$$

2) (M, ID_{cm}, X_m, Y_n)을 다음 서명자에게 전송한다.

3) 마지막 서명자는 $(m, ID_{cm}, (e_1,\ldots e_k), Y_m)$ 을 검증자에게 전송한다.

● 다중 서명 검증

법 N과,f ,h,$(m, ID_{cm}, (e_1,\ldots e_k), Y_m)$를 이용해 서명에 대한 검증이 가능하다.

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

$$I_{ij} = f(ID_i, j),\ I = 1,2,\ldots,m,\ j=1,2,\ldots,k$$

2) 다음을 계산한다.

$$Z_m = Y_m^2 \prod_{i=1}^{m} \prod_{j=1}^{k} I_{ij} \bmod N, \quad j=1,2,\ldots,k$$

3) $h(M, ID_{cm}, Z_m)$을 계산하고 다음의 만족 유무를 확인한다.

$$(e_1,..e_k) = h(M, ID_{cm}, Z_m)$$

위 식이 만족하면 메세지는 유효한 것으로 판명한다.

Ex2) n 이 2 일때의 검증 확인

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

검증 요소 $(e_1, \cdots, e_k) = h(M, ID_{cm}, Z_m)$ 인지를 확인한다.

$$Z_2 = Y_2^2 \prod_{i=1}^{2} \prod_{j=1}^{k} I_{ij} \bmod N$$

$$X_2 = R_2^2 X_1 \bmod N$$

$$Y_2 = Y_1 R_2 \prod S_{2j} = (R_1 \prod_{\theta j=1} S_{1j}) R_2 \prod_{\theta j=1} S_{2j} = R_1 R_2 \prod_{\theta j=1} S_{1j} S_{2j} = R_1 R_2 \prod_{i=1}^{2} \prod_{\theta j=1} S_{ij}$$

$$Y_1 = R_1 \prod_{\theta j=1} S_{1j}$$

$$Z_2 = (R_1 R_2 \prod_{i=1}^{2} \prod_{\theta j=1} S_{ij})^2 \prod_{i=1}^{2} \prod_{\theta j=1} I_{ij}$$

$$= R_1^2 R_2^2 \prod_{i=1}^{2} \prod_{\theta j=1} S_{ij}^2 I_{ij}$$

$$= R_1^2 R_2^2 \prod_{i=1}^{2} \prod_{\theta j=1} 1$$

$$= R_1^2 R_2^2$$

$X_2 = R_1^2 R_2^2$. so, $Z_2 = X_2$ 이므로 검증 가능하다.

3.3 Kang – Kim 다중 서명 방식

Ohta-Okamoto 방식과 마찬가지로 Fiat-shamir방식에 근거하고 있다.

● **키 발생 및 배포**

서명자i가 ID_i를 키 발급 센터에 등록하게 되면 TC는 다음과 같은 일 수행하게 된다

1) TC에서는 두개의 큰 소수 p,q를 생성 및 비밀리 유지한다.
2) p,q를 이용해 N = p*q인 N을 계산하여 공개한다.
3) 서명자 i에 대하여 S_{ij}를 계산한다.

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

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

4) TC에서는 $(N,f,h,S_{i1},...S_{ik})$가 기록된 스마트 카드를 발급,배포한다.

◆ **다중 서명 발생**

● **서명자 1의 서명 발생**

1) 서명할 사람의 순서 결정

$$ID_{cm} = ID_1(\text{기안자}) \,||\, ID_2 \,||...||\, ID_m\ (\text{최종})$$

2) 랜덤수 $R_1 \in Z_N$ 을 선택, 여기서 Z_N은 {0,1,....N-1}을 나타냄.
다음과 같은 서명 정보를 생성한다.

$$X_1 = R_1^2 \bmod N$$

$$(e_{11},.....,e_{1K}) = h(M, ID_{cm}, X_1)$$

$$Y_1 = R_1 \prod_{\theta 1 j=1} s_{1j} \bmod N,\ j=1,2,....k$$

3) (M, ID_{cm}, X_1, Y_1)을 다음 서명자에게 전송.

● **서명자 n의 서명 발생**

1) 전단계 서명자로부터 $(M, ID_{cm}, X_1, ...X_{n-1}, Y_{n-1})$을 받으면 검증할 수 있으며, 이 과정은 생략 가능하다.

2) 랜덤 수 Rn ∈ Zn 을 선택하고, 다음의 서명 정보를 계산한다.

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

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

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

3) $(M, ID_{cm}, X_1,...,X_n, Y_n)$을 다음 서명자에게 전송한다.
만약 마지막 서명자일 경우 $(M, ID_{cm}, X_1,...,X_m, Y_n)$을 검증자에게 보낸다.

◆ 다중 서명 검증

● 서명자 n의 검증

$(ID_{cm}, X_1,...,X_{n-1}, Y_{n-1})$ 을 받으면 다음 절차에 의해 검증한다.

1) $X_1,....X_{n-1}$ 로 부터 $(e_{11},...e_{1k}),... (e_{n(n-1)},...e_{(n-1)k})$를 계산.한다.

$$(e_{i1},...e_{ik}) = h (M, ID_{cm}, X_i), I = 1,..., n-1.$$

2) ID_I를 이용하여

$$I_{ij} = f(ID_I, j), I= 1,2,.....,n-1\ j = 1,2,.....,k$$를 계산한다.

3) $Y_{n-1}, I_{ij}, (e_{11},...e_{1k})...(en_{(n-1)},...e_{(n-1)},k)$를 이용해

$$Z_{n-1}=Y_{n-1}^2 \prod_{j=1}^{n-1} \prod_{e_{ij}=1} I_{ij} \bmod N, \quad j=1,2,...,k$$

를 계산하여 $Z_{n-1}=X_{n-1}$이면 유효하다고 판정.

● 검증자의 다중 서명 검증

검증자는 $(M, ID_{cm}, X_1,...X_m, Y_m)$을 받으면 X1,...Xm로 부터

$$(e_{11}, ...,e_{1k})...(e_{m1},...e_{mk})$$ 를 계산한다.

$$(e_{11},...e_{1k}) = h(M, id_{cm}, X_i), \quad I=1,...,m$$

$$(M, ID_{cm}, (e_{11},...e_{1k}),...(en_{(n-1)},...e_{(n-1)k}), Y_m)$$

를 계산해 저장 보관한다.

1) 검증자는 ID를 이용해

$$I_{ij}=f(ID, j), I =1,2,...m, \quad j=1,2,...,k$$ 를 계산한다.

2) Y_m를 이용하여

$$Z_m = Y_m^2 \prod_{j=1}^{m} \prod_{e1j=1} I_{ij} \bmod N, \quad j = 1,2,...k$$

를 계산하여 $(e_{m1},...e_{mk})=h(M, ID_{cm}, Z_m)$ 이면 유효하다고 판단한다.

● 검증에 대한 확인 절차

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

$$= (Y_{m-1}^2 R_m^2 \prod_{e_{mj}=1} S_{mj}^2) \prod_{i=1}^{m} \prod_{e_{ij}=1} I_{ij} \bmod N$$

$$= R_m^2 \cdots R_2^2 R_1^2 \prod_{i=1}^{m} \prod_{e_{ij}=1} S_{ij}^2 I_{ij} \bmod N$$

$= R_m^2 \cdots R_2^2 R_1^2 \bmod N$
$= X_m$.
이므로, $h(M, ID_{cm}, Z_m) = h(M, ID_{cm}, X_m) = (e_{m1}, \cdots, e_{mk})$가 되어
$X_n = R_n^2 Z_{(n-1)}$ 이 성립한다.

IV. 새로운 다중 서명 방식 설계

1) 서명 생성

먼저, 서명에 참가하는 서명자 U_1는 G_N으로부터 랜덤한 요소 $s_1(0<s_1<N-1)$을 선택하여 비밀로 보관하고

$y_1 = g^{s1} \in G_N$을 공개한다.

또 랜덤하게 G_N의 요소 $r_1(0<r_1<N-1)$를 선택하여

$x_1 = g^{r1} \in G_N$ 를 계산한다.

첫번째 서명자 U_1는 해쉬 함수 h를 이용하여

$e_1 = h(x_1, m) \in z_m$ (m : 메세지)을 계산하여

$\sigma_1 = r_1 + s_1 * e_1 \in G_N$

을 생성한다. 문서 m에 대하여 (σ_1, x_1)를 서명 데이터로 한다.

두 번째 서명자 U_2는 공개키 y_1 를 이용하여 문서 m과 서명 데이터 (σ_1, x_1) 에 대한 해쉬 함수 h를 이용하여 $e_1 = h(x_1, m) \in z_m$ 을 계산하여

$g^{\sigma 1} = x_1 * y_1^{e1}$

가 성립하는 가를 검증한다.

두 번째 서명자 U_2는

$x_2 = x_1 * g^{r2} \in G_N, \quad e_2 = h(x_2, m) \in z_m$

을 계산하여

$\sigma_2 = \sigma_2 + (r_2 + s_2 * e_2) \in G_N$

을 생성한다.

두 번째 서명자는 다음 서명자에게 $(\sigma_2, x_2, e_1, e_2, y_1, y_2)$의 다중 서명 데이타를 전송한다.

마지막 서명자 U_n은 G_N으로부터 랜덤한 요소 s_n을 선택하여 비밀로 보관하고
$y_n = g^{sn} \in G_N$ 을 공개한다.

또, 랜덤하게 G_N의 요소 r_n를 선택하여

$x_n = x_{n-1} * g^m \in G_N$ 을 계산한다.

그리고, 해쉬함수 h를 이용하여

$e_n = h(x_n, m) \in z_m$을 계산하고

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

을 생성하여, 최종 검증자에게 . $(\sigma_n, x_n, e_1, e_2, \cdots, e_n, y_1, y_2, \cdots, y_n)$을 다중 서명 데이타로 전송한다.

2) 서명 검증

서명 검증자는 다중 서명 데이타$(\sigma_n, x_n, e_1, e_2, \cdots, e_n, y_1, y_2, \cdots, y_n)$를 이용하여 다음 수식이 성립하는가를 확인한다.

$$g^{\sigma_n} = x_n * y_1^{e1} * y_2^{e2} * \cdots * y_n^{en}$$
$$g^{\sigma_1+\sigma_2+\cdots+\sigma_n} = x_1 * x_2 * \cdots * x_n * y_1^{e1} * y_2^{e2} * \cdots * y_n^{en}$$
$$g^{\sigma_1+\sigma_2+\cdots+\sigma_n} = (x_1 * y_1^{e1}) * (x_2 * y_2^{e2}) * \cdots * (x_n * y_n^{en})$$
$$(\because g^{\sigma_i} = g^{ri+si*ei} = g^{ri} * g^{si*ei} = x_i + y_i^{ei})$$

V. 결 론

본고에서는 기존의 다중 서명 방식들을 고찰함으로써 그 특징 및 장단점을 검토해 보았다. RSA 방식에 근거하고 있는 Itakura-Nakamura 서명 방식과 Okamoto 서명 방식은 서명 발생 및 검증시 계산량이 늘어나고, 속도가 떨어지는 단점을 지니고 있다. 그리고, ID-based 한 Ohta-Okamoto 방식은 m 명의 서명자에 대해 2m-1 번 정도의 통신 복잡도를 가지고 있어 이외의 서명 방식에 비해 효율성이 떨어지는 면이 있다. Kang-Kim 방식의 경우에는 서명 길이가 길어진다는 단점이 발생한다.

그러나, Okamoto 방식의 경우에는 Itakura-Nakamura 이 갖고 있던 직급에 따른 비밀키 변동에 대한 제약성을 극복했으며, Otha-Okamoto 방식과 Kang-Kim 방식은 서명의 길이 및 속도에서 안정적인 면을 보이고 있다.

제안된 방식은 서명 순서에 있어 제약성이 없으므로, Itakura-Nakamura 서명 방식의 단점을 극복했으며, 통신 횟수에 있어 m-1 번 정도로 Ohta-Okamoto 방식보다 효율적이다. 뿐만 아니라, 메세지와 비밀키를 일방향 해쉬 함수를 사용해 길이를 고정하였으며 , 초기에 생성한 랜덤수 R 을 저장할 필요가 없으므로 효율적이라 하겠다.

이상을 다음의 표로 정리하였다.

< 표 1 > 각 방식별 장단점 비교

Itakura-Nakamura	직급에 따른 비밀키 변동이 심하다.
Okamoto	순서 변동의 제약성 극복, RSA 에 근거하고 있으므로 속도가 떨어지는 단점 발생
Otha-Okamoto	서명 길이가 짧고 속도가 안정적
Kang-Kim	메세지 길이가 길어 지는 단점이 있으나, 서명 길이 및 속도에서 안정적
제안 방식	순서 변동의 제약성을 극복하였고, 서명의 길이 고정

참고 문헌

[1] D. Chaum and E. van Heyst, " Group Signatures ", Eurocypt '91, pp. 257-265, 1991

[2] K. Itakura and K. Nakamura, " A public-key cryptosystem suitable for digital multisignatures ", NEC J. Res Dev. 71, pp. 1-8, Oct. 1983.

[3] K. Ohata and T. Okamto, " A Digital Multisignature Scheme Based on the Fiat-Shamir Scheme," Proceedings of Asiacrypt '91. pp75-79. 1991.

[4] T. Okmoto, "A Digital Multisignature, Scheme Using Bilective Public-key Cryptosystems, " ACM Trans. On Comp. Systems. Vol. 6, No. 8, pp.432-441, 1988.

[5] A.Fiat and A.Shamir, "How to prove yourself: practical solutions to identification and signature problems, Advances of Cryptology," Proc. Of CRYPTO'86 Springer-Verlag, pp. 186-194

[6] T.Okamoto and K.Ohta, "Divertible Zero-Knowledge Interactive Proofs and Commutative Random Self-Reducible," Advances of Cryptology, Proc. Of EUROCRYPT'89 Springer-Verlag, pp. 134-149

[7] T.P.Pedersen, I.Damgaard, D.Chaum and J.Boyar, "Convertible Undeniable Signatures," Advances of Cryptology, Proc. Of CRYPTO'90 Springer-Verlag, pp. 189-205

[8] C.P.Schnorr, "Efficient identification and signatures for smart cards," Advances of Cryptology, Proc. Of CRYPTO'89 Springer-Verlag, pp. 239-252

[9] 강창구, 김대영, " 전자 계약 시스템에서의 디지털 다중 서명 방식 ", 전자 공학회 논문지, 1993

[10] 강창구, 김대영, " 디지털 다중 서명 방식과 응용에 대한 연구 ", 충남대 학위 논문, pp. 34-74, 1993