論 文

동시성을 갖는 새로운 디지탈 다중서명 방식

正會員 姜 昌 求* 正會員 金 大 榮**

New Digital Multisignature Scheme with Concurrency

Chang Goo Kang*, Dae Young Kim** *Regular Members*

요 약

본 논문에서는 이산대수 문제에 근거한 새로운 1-out-of-n 비대화형 불확정 전송 암호화 프로토콜을 제안하고, 다자간의 공평한 비밀정보 교환방식을 새로이 제안하였으며 이들방식을 이용하여 Fiat-Shamir 서명방식에 근거한 새로운 디지탈 다중서명방식을 제안하고 안전성을 분석하였다.

제안된 디지탈 다중서명방식은 동시성, 실행 가능성 및 부정 조기검출성을 가지고 있으며 다수의 사람이 참여하는 전자계약 서명시스템에 적용될 수 있다.

Abstract

We present an 1-out-of-n noninteractive OT(Oblivious Transfer) protocol based on the Diffie-Hellman assumption and a new fair exchange scheme of secret information among multi-users. Using the noninteractive OT protocol and the fair exchange scheme, we also present a new digital multisignature scheme based on Fiat-Shamir signature scheme and analyze its security.

Owing to its concurrency, viability, and dishonesty detectablility, the proposed digital multisignature scheme is applicable to electronic multi-user contract systems.

I. 개 요

컴퓨터의 보급확산과 디지탈 통신기술의 발전으로 정보화 사회가 도래함에따라 컴퓨터 통신망을 이용하여 많은 업무가 전산화되고 자동처리되고 있다. 이와함께 사무실에서는 종이문서 대신에 디지탈화된 전자문서가 등장하게 되고, 전자문서는 전자우편이나 화일전송등을 이용하여 빠른시간내에 멀리 떨어진 상대방에게 전달되고 교환될 수 있게된다. 이렇게 되면 국가간의 협정서 조인, 기업간의 수출입 계약업무, 개인간의 이해 관계가 있는 계약업무에 있어서 서명은 컴퓨터 통신망을 통해서 이루어지게 될것이다. 이러한 정보화 사회에서는 손으로쓴 서명대신에 디지탈 서명이 요구되고,[1]-[3] 또한 여러사람이 서명을 하여야할때 디지탈 다중서명이 요구된다.[1]-[8]

지금까지는 서명 날인을 할때 주로 특정한 동일한 장소에서 당사자와 직접 만나서 물리적인 식별을 한 후 서로 서명을 수행함으로써 상대가 정당한 서명자인지를 직접 눈으로 확인하고 서명을 동시에 수행할

*韓國電子通信研究所
ETRI
**忠南大學校 情報通信工學科
Chungnam National University
論文番號 : 93-131

수 있었다. 그러나 이러한 동시서명을 통신망을 통하여 수행할때는 서명자를 직접 눈으로 확인할 수가 없게되고 또한 통신망 자체의 특성때문에 아무리 실시간으로 통신을 수행하더라도 서명의 상호 교환이 완벽하게 동시에 수행될 수 없다.

따라서 통신망을 통하여 여러사람이 다중서명을 수행할때 어느 한쪽이 상대에게 먼저 자신의 서명을 보냄으로써 다른 상대는 이 서명을 불법으로 악용할 수 있게되어 서명을 먼저 보낸 서명자가 불이익을 당할 수 있다. 이러한 문제점을 해결하기 위해서는 통신망에서 정당한 서명 당사자간에 서로의 서명을 동시에 교환하도록 하는 동시성을 갖는 디지탈 다중서명방식이 요구되며 이러한 디지탈 다중서명방식이 갖추어야할 특성은 다음과 같다.

첫째, 서명 당사자들이 정직하게 서명 프로토콜을 수행한 후에는 각 서명자는 상대방의 서명을 서로 가질 수 있어야 한다.

둘째, 서명자들은 어느 한쪽의 불이익을 방지하기 위하여 프로토콜 수행시 상대의 서명을 동시에 소유할 수 있도록 서명 교환이 동시에 이루어져야 한다.

세째, 서명의 위조 불가능성으로 일반 디지탈 서명방식에 요구되는 안전성이다. 즉, 각자의 서명은 본인을 제외한 어떠한 사람에 의해서도 위조가 가능해서는 안된다. 서명은 정당한 당사자만이 생성할 수 있어야 하며 모든 서명자들은 서로 상대의 서명을 검증할 수 있어야 한다.

네째, 다중서명 프로토콜 수행도중 어떤 서명자가 부정을 행하였을 경우 다른 서명자에 의해서 이를 조기에 검출할 수 있어야 한다.

위와같은 특성을 갖는 디지탈 다중서명 방식을 구현하기 위해서는 불확정 전송(OT : Oblivious Transfer)기술과 공평한 비밀정보 교환기술이 요구된다.[9]-[11]

본 논문에서는 불확정 전송 기술에 대하여 알아보고 본 다중서명 방식에 요구되는 1-out-of-n 비대화형 OT(NIOT : Non-Interactive OT)를 새로이 제안하고, 다자간의 공평한 비밀정보 교환방식을 새로이 제안하였다.

또한, 새로이 제안된 방법들을 이용하여 Fiat-Shamir의 서명방식에 근거한 새로운 디지탈 다중서명방식을 제안하고 안전성을 분석하였다.

Ⅱ. 비대화형 불확정 전송

2.1 불확정 전송의 분류

불확정 전송(OT)의 기본개념은 1983년 Rabin에 의해서 처음으로 소개되었으며[12] 일반적으로 암호화 프로토콜을 설계하기 위한 기본적인 도구로서 유용하게 쓰이는 서브프로토콜이다. 일상적인 암호화 프로토콜에서 비밀을 보장하면서 그것에 관련한 임의의 정보를 보내야되는 경우 OT 프로토콜은 유용하게 쓰일 수 있다.

OT 프로토콜은 A가 B에게 어떤 비밀을 보내고자 할 때, B가 그 비밀을 1/2의 확률로 취할 수 있게 하고 A는 B가 그 비밀을 취했는지의 여부를 1/2의 확률로 추측할 수 있게 하는 프로토콜이다. 물론 B가 그 비밀을 취했다면, B는 그 비밀의 내용을 알 수 있게 된다.

이 경우는 하나의 비밀에 대해서만 OT를 설명한 것이고 여러 비밀에 대해서도 OT를 확장 적용할 수 있다. 예를 들면 A가 B에게 두개의 비밀중 하나의 비밀만을 B에게 보내고자할 때를 생각해 보자. 이때 B는 1/2의 확률로 둘중의 하나의 비밀만을 취하게 되고 A는 B가 두 비밀 중 어느 비밀을 취했는지를 1/2의 확률로 추측할 수 있게 된다.

OT는 몇개의 비밀에 대해서 적용할 것인가에 따라 하나의 비밀에대한 경우인 일반 OT와 두개의 비밀에 대한 1-out-of-2 OT, n개의 비밀에대한 1-out-of-n OT, 그리고 n개의 비밀중(n-1)개의 비밀만을 불확정 전송할때 (n-1)-out-of-n OT로 분류할 수 있다. 그 중 대표적인 것이 1-out-of-2 OT이다. 이것은 송신자가 2개의 비밀정보 m1, m2를 가지고 있을때 그 가운데 어느 하나만은 수신자에게 정확히 보내지만, 송신자는 수신자가 두개중 어느 비밀정보를 수신하였는지를 알 수 없도록한 프로토콜이다.

또한 OT는 양자간의 정보교환이 대화 형식인지의 여부에따라 대화형 불확정 전송(IOT : Interactive OT)와 비대화형 불확정 전송(NIOT : Non-Interactive OT)로 분류할 수 있다.[13] 대화형 불확정 전송은 송수신자간에 자기의 정보에대한 몇번의 상호교환을 통해 이루어지며 이렇게 프로토콜의 전개가 대화형식으로 진행될때 interactive하다고 하며 이러한 형태를 갖는 OT를 IOT라 한다. NIOT는 프로토콜의 전개가 대화 형식이 아니다. 즉 송신자에 의한 수신자로의 단 한번의 통신만이 존재한다. 이런 경우, 송수신자 간에 통신회수는 급격히 줄어들며 실제의 응용에 있어서 OT를 사용할때 OT에 의한 통신로의 과부하를 줄일 수 있다.

1989년에 Bellare와 Micali는 이산대수(discrete log)문제에 기반한 NIOT를 제안하였으며,[13] 1990년에는 Santis와 Persiano가 이차잉여가설(quadratic residuosity assumption)에 기반한 NIOT를 제안하였다.[14]

본 장에서는 Bellare와 Micali가 제안한 1-out-of-2 NIOT를 소개하고 또한 이산대수문제를 이용한 1-out-of-n NIOT를 새로이 제안하고자 한다.

2.2 1-out-of-2 NIOT

가. 키 발생 방법

키 발급 센타는 임의의 소수 p와 Z_p^*의 생성원 g를 선택하고 이들 p, g와 Z_p^*의 임의의 원소 C를 시스템 내의 모든 사용자에게 공개한다. 그러나 사용자들은 C의 이산 대수를 알지 못한다. 사용자 B는 랜덤하게 $i \in \{0,1\}$을 선택하고 또한 $x_i \in \{0,\ldots,p\text{-}2\}$를 선택한 후 다음을 계산한다.

$$\beta_i = g^{x_i} \bmod p \tag{1}$$

$$\beta_{1-i} = C \cdot (g^{x_i})^{-1} \bmod p \tag{2}$$

그리고 B는 자신의 공개키 β_0, β_1을 공개하고 i, x_i를 비밀리 유지한다. 누구든지 $\beta_0\,\beta_1 = C$를 점검 함으로써 B의 공개키 정보 β_0, β_1이 정확하게 구성 되었는지를 확인할 수 있다.

C의 이산대수가 알려지지 않는한 B는 β_0와 β_1 모두의 이산대수를 알 수 없다. 더구나 공개키 β_0, β_1는 Z_p^*의 원소 쌍들중에 랜덤하게 분포되어 있어서 B가 이산대수를 알고 있는것이 β_0인지, β_1 인지를 다른 사용자가 알 수 없다. 이것이 비대화형 불확정 전송에 결정적인 역할을 한다. 여기서 사용한 방법은 Diffie-Hellman의 비밀키 교환 프로토콜과 유사하며 같은 계산상 복잡성의 가정하에 근거하고 있으며, Diffie-Hellman의 가정은 g^x와 g^y가 주어지고, x와 y가 주어지지 않으면 g^{xy}를계산하기는 어렵다는 것이다.

나. NIOT(S_0, S_1)

A가 B에게(S_0, S_1)의 정보를 비대화형으로 불확정 전송하는 방법은 그림1과 같다.

단계 1 : A는 y_0, $y_1 \in \{0,\ldots,p\text{-}2\}$를 랜덤하게 선택하고 α_0와 α_1을 다음과 같이 계산하여 B에게 보낸다.

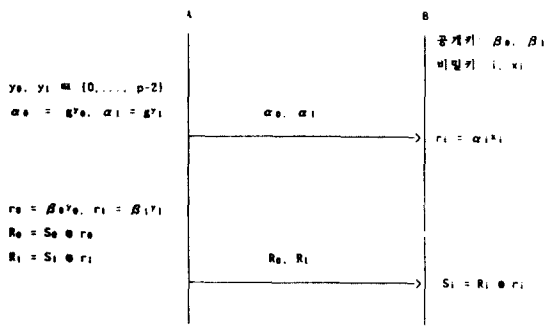

그림 1. (S_0, S_1)의 비대화형 불확정 전송 프로토콜
Fig 1. NIOT(S_0, S_1) protocol

$$\alpha_0 = g^{y_0},\ \alpha_1 = g^{y_1} \tag{3}$$

단계 2 : A는 $r_0 = \beta_0^{y_0}$와 $r_1 = \beta_1^{y_1}$을 계산하고 R_0와 R_1을 다음과 같이 계산하여 B에게 보낸다.

$$R_0 = S_0 \oplus r_0 \tag{4}$$

$$R_1 = S_1 \oplus r_1$$

단계 3 : B는 α_0와 α_1을 수신하면 자신의 비밀키 x_i로 $r_i = \alpha_i^{x_i}$를 계산한다. 그리고 $S_i = R_i \oplus r_i$를 계산함으로써 S_i를 수신하게 된다.
Diffie-Hellman의 가정은 B가 r_{1-i}를 계산하지 못함을 의미한다. 즉 $\beta_{1-i} = g^{x_{1-i}}$ 일 때 $r_{1-i} = g^{x_{1-i}y_{1-i}}$이고 B는 $g^{x_{1-i}}$와 $g^{y_{1-i}}$를 알 수 있으나 x_{1-i}와 y_{1-i}는 알지 못한다. 따라서 B는 r_{1-i}를 계산할 수 없어서 S_{1-i}를 계산할 수 없다.

이렇게 하여 A는 B에게(S_0, S_1) 정보를 불확정하게 전송할 수 있다. 이때 B는 A에게 아무것도 보내지 않았으므로 전송은 비대화형으로 이루어진다.

2.3 1-out-of-n NIOT 제안

사용자 A가 사용자 B에게 비밀 정보 $S_0,\ldots,S_{n-1}$ 중 임의의 한개 정보를 비대화형으로 불확정 전송하는 방식을 다음과 같이 제안한다.

가. 키 발생 방법

키 발급 센타는 임의의 소수 p와 Z_p^* 상의 생성원 g를 선택한다. Z_p^*의 임의의 원소 C_1, $C_2,\ldots,C_{n-1}$를 선택하고 p, g와 함께 시스템 내의 모든 사용자에게 공

개한다. 그러나 사용자들은 $C_1, C_2,\ldots,C_{n-1}$의 이산대수를 알지 못한다. 사용자 B는 랜덤하게 $i \in \{0, 1, 2,\ldots,n-1\}$를 선택하고 또한 $x_i = x_{i1} + x_{i2} + \ldots + x_{i(n-1)}$를 만족하는 xi를 선택한다. 이때 $x_i, x_{i1},\ldots,x_{i(n-1)} \in \{0, 1, 2,\ldots,p-2\}$이다.

그리고 B는 자신의 공개키 $\beta_0, \beta_1,\ldots,\beta_{n-1}$를 다음과 같이 계산하여 공개하고 i, x_i를 비밀리 보관한다.

$$\begin{aligned}
&\cdot \beta_{[i]} = g^{x_i} \bmod p \\
&\cdot \beta_{[i+1]} = C_1 (g^{x_{i1}})^{-1} \bmod p \\
&\cdot \beta_{[i+2]} = C_2 (g^{x_{i2}})^{-1} \bmod p. \\
&\quad \vdots \\
&\cdot \beta_{[i+n-1]} = C_{n-1} (g^{x_{i(n-1)}})^{-1} \bmod p
\end{aligned} \tag{5}$$

여기서 $\beta_{[j]}$의 $[j] = j \bmod n$이다.

누구든지 $\beta_0\ \beta_1 \ldots \beta_{n-1} = C_1\ C_2 \ldots C_{n-1}$를 점검함으로써 B의 공개키 $\beta_0, \beta_1,\ldots,\beta_{n-1}$이 정확하게 구성되어 있는지를 확인할 수 있다. B는 또한 $C_1, C_2,\ldots,C_{n-1}$의 이산대수가 알려지지 않는한 β_i를 제외한 다른 공개키의 이산대수를 알 수 없다.

나. NIOT($S_0, S_1,\ldots,S_{n-1}$)

A가 B에게 $(S_0, S_1,\ldots,S_{n-1})$의 정보를 비대화형으로 불확정 전송하는 방법은 그림2와 같다.

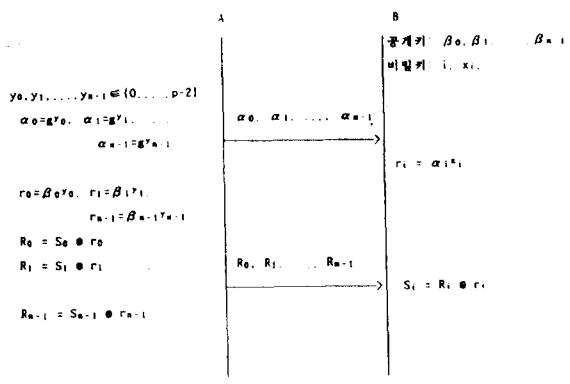

그림 2. $(S_0, S_1,\ldots,S_{n-1})$의 1-out-of-n 비대화형 불확정 전송 프로토콜

Fig 2. 1-out-of-n NIOT($S_0, S_1,\ldots,S_{n-1}$) protocol

단계 1 : A는 $y_0, y_1,\ldots,y_{n-1} \in \{0,\ldots,p-2\}$를 랜덤하게 선택하고 $\alpha_0, \alpha_1,\ldots,\alpha_{n-1}$을 다음과 같이 계산하여 B에게 보낸다.

$$\alpha_0 = g^{y_0},\ \alpha_1 = g^{y_1},\ldots,\alpha_{n-1} = g^{y_{n-1}} \tag{6}$$

단계 2 : A는 $r_0 = \beta_0^{y_0},\ r_1 = \beta_1^{y_1},\ldots,r_{n-1} = \beta_{n-1}^{y_{n-1}}$을 계산하고 $R_0, R_1,\ldots,R_{n-1}$을 다음과 같이 계산하여 B에게 보낸다.

$$\begin{aligned}
&R_0 = S_0 \oplus r_0 \\
&R_1 = S_1 \oplus r_1 \\
&\quad \vdots \\
&R_{n-1} = S_{n-1} \oplus r_{n-1}
\end{aligned} \tag{7}$$

단계 3 : B는 $\alpha_0, \alpha_1,\ldots,\alpha_{n-1}$을 수신하면 자신의 비밀키 x_i로 $r_i = \alpha_i^{x_i}$를 계산한다. 그리고 $S_i = R_i \oplus r_i$를 계산함으로써 S_i 정보를 얻을 수 있다. 앞의 NIOT(S_0, S_1)에서와 같이 Diffie-Hellman의 가정에 의해서 B는 S_i 이외의 다른 송신 정보를 얻을 수 없다. 이와 같이 A는 B에게 1-out-of-n 불확정 전송을 성공적으로 수행할 수 있다. 또한 B는 A에게 아무것도 보내지 않았으므로 전송은 비대화형으로 이루어진다.

Ⅲ. 다자간의 공평한 비밀정보 교환

여러 사람이 각자 비밀정보를 가지고 있고 이들 비밀정보를 서로 공평하게 교환할 수 있는 방법은 암호화 프로토콜에서 중요한 문제이다. 특히 계약 혹은 합의문서에 서명할때 어느 한쪽이 자신의 서명을 먼저 보냄으로써 야기될 수 있는 문제점은 많을 수 있다. 이러한 문제점을 해결하기 위해서 공평한 비밀정보 교환에 관한 연구가 있어 왔다.[15][16] 두 사람간에 있어서 비밀정보의 공평한 교환은 다음과 같은 프로토콜에 의해서 수행될 수 있다. 두 사람 A와 B는 비트길이가 m인 두개의 비밀 정보를 각각 가지고 있을 때 A와 B는 1-out-of-2 OT에 의해 두개의 비밀정보 중 하나의 비밀정보를 불확정 전송한다. A는 B의 두개의 비밀정보중에서 정확히 한개의 비밀정보를 알게되고 B는 A가 자신의 비밀정보들중에서 어떤것을 알고 있는지 모른다. 마찬가지로 B는 A의 비밀정보들중에서 정확히 한개의 비밀정보를 알게되고 A는 B

가 어떤 비밀정보를 알고 있는지 모른다.

이러한 상황에서 A와 B가 서로의 비밀정보를 모두 알려고 할때 다음과 같은 프로토콜을 사용하여 비밀정보를 교환할 수 있다.

- A는 B에게 각 비밀 정보의 첫번째 비트들을 보낸다.
- B는 A에게 각 비밀 정보의 첫번째 비트들을 보낸다.
- 위과정을 m번째 비트들까지 반복한다.

하나의 비밀을 계산하는 것은 비밀공간(m bits 길이의 집합)에서 exhaustive search에 의해서 수행할 수 있다고 가정한다.

만약 A, B 두사람이 정직하게 프로토콜을 따랐다면 서로는 거의 같은 시간내에 서로의 비밀정보를 완전히 얻을 수 있다. 이와같은 프로토콜 수행 과정에서 만약 A가 B에게 k번째 비트들을 보낸후 B가 프로토콜 수행을 중지하면 B는 한 비트의 정보를 이득 보게되어 2대1의 계산상 이득(computational advantage)을 얻게된다. 따라서 B는 하나의 비밀 정보를 계산하기 위해서 2^{m-k}개의 가능한 비밀공간의 부분집합을 조사 하여야 하나 A는 2^{m-k+1} 개의 부분집합에서 조사하여야하므로 A는 두배의 계산이 요구된다.

위와같은 상황에서 이러한 문제를 해결하기 위해 T.Tedrick은 B가 계산상 이득을 일정양까지 줄일 수 있는 방법을 제안하였다.[17] 또한 M명의 사용자간에 공평한 비밀정보 교환을 위해서는 앞에서 기술한 방법을 직접 적용할 수도 있으나 본 장에서는 M명의 사용자간에 공평한 비밀정보 교환방법을 새로이 제안하고자 한다. 여기서 각자는 M개의 비밀정보를 가지고 있다고 가정한다.

단계 1 : 모든 사용자들은 각자 자신이 보유한 M개의 비밀 정보에 대하여 (M-1) 명의 다른 사용자들에게 각각 1-out-of-M OT를 수행하여 하나의 비밀 정보를 각각 불확정 전송한다. 따라서 각 사용자는 자신이 보유한 M개의 비밀 정보중 최대(M-1)개의 비밀정보를 다른 사용자들에게 불확정 전송하게 된다.

단계 2 : 사용자들은 $M \leq 2^{k-1}$을 만족하는 정수값 k를 결정한다. 프로토콜 수행 중지시 중지한 측의 최대 계산상 이득은 $2^{k-1}+1$대 2^{k-1}이 된다.

단계 3 : 각 사용자는 k개 비트로 구성된 2^k 개의 서로 다른 비트 스트링을 생성 저장한다.

단계 4 : 각 사용자는 이들 2^k개의 비스 스트링중에서 자신이 보유하고 있는 M개의 비밀정보중 첫번째 비트부터 k번째 비트까지의 비트 스트링들과 일치하지 않은 비트 스트링을 임의로 선택하여 다른 사용자들에게 다음과 같이 전송한다. "비밀 정보중 첫번째 비트부터 k번째 비트까지의 비트 스트링은 '$X_1 \ldots X_k$'가 아니다."

단계 5 : 각 사용자는 단계 4를 교번하면서 2^{k-1}개의 비트 스트링 만큼 전송한다.

단계 6 : 각 사용자는 자신의 비밀정보가 포함되어 있는 스트링을 포함하여 2^{k-1}개의 스트링만이 남으면 남은 비트 스트링에 각각 '0' 비트와 '1'비트를 추가하여 다시 비트 길이가 k+1인 2^k개의 비트 스트링을 생성 저장하고 단계4, 단계5를 반복 수행한다.

위의 프로토콜 수행중 단계4, 단계5에서 먼저 자신의 메세지를 보낸후 다른 사용자가 프로토콜 수행을 중지하였을 경우 중지한측의 계산상 이득은 한개 스트링을 보내고 중지한 경우 2^k 대 2^k-1, 두개 스트링을 보냈을 경우 2^k-1 대 2^k-2, 다음은 2^k-2대 2^k-3, 이렇게하여 최대 계산상의 이득은 $2^{k-1}+1$ 대 2^{k-1}이 된다.

이것은 서로의 비밀정보를 찾기 위해서 먼저 보낸 사용자가 찾아야 할 비밀공간 대 프로토콜을 중지한 사용자가 찾아야할 비밀공간의 비율이다.

또한 거짓 스트링을 보냄으로써 상대방들이 이를 검출할 확률은 최대(M-1)/M이다. 위에서 제시한 프로토콜은 각자의 비밀정보에서 첫번째, 두번째, 세번째 비트로부터 시작하였으나 보다 좋은 방법을 위해서는 전송될 비트들의 위치를 랜덤하게 선택할 수도 있다. 이렇게 함으로써 어느 한쪽의 최대 계산상의 이들을 $2^{k-1}+1$ 대 2^{k-1}로 줄이면서 비밀정보의 교환을 보다 공평하게 할 수 있다.

Ⅳ. 새로운 디지탈 다중서명방식

본 장에서는 다수의 사람이 동일한 전자문서에 서명하는데 있어서 동시성을 갖는 새로운 디지탈 다중서명방식을 제안하고자 한다.

동시성(Concurrency)은 암호화 프로토콜에서 중

요한 안전 요구사항으로서 다수의 사람들이 서명을 수행할 때 어느 한쪽의 불이익을 방지하기 위해서는 서명을 수행할때 상대의 서명을 동시에 소유할 수 있도록 서명 교환이 이루어져야 한다.

본 논문에서 동시 다중서명시스템에 m명의 서명자가 참여하고 있으며 통신망을 통하여 개별전송 뿐만 아니라 bridge node 혹은 MCU(Multipoint Control Unit)에 의해서 동보 전송을 할 수 있다고 가정하였다.[8] 본 제안 방식은 ID 암호 시스템인 Fiat-Shamir의 디지탈 서명방식[18]을 직접 적용하고 앞에서 제안한 불확정 전송 프로토콜과 비밀정보의 공평한 교환 기술을 이용하여 동시성을 갖도록 하였다.

4.1 키발생 및 배포

본 방식에서의 키종류는 서명에 관련된 키와 비대화형 불확정 전송에 관련된 키가 있으며 이들의 키 발생 및 배포 절차는 다음과 같다.

가. 서명 키 발생 및 배포

서명자 i가 자신의 식별정보인 ID_i를 키 발급센타(trusted center)에 등록하면 키 발급 센타는 다음 절차에 의해 키를 발생 배포한다.

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

단계 2 : 키 발급센타는 p와 q의 곱인 $N=p^*q$를 공개한다.

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

$$I_{ij}=f(ID_i, j),\ j=1, 2,\ldots,k,\ I_{ij}\in QR_N \qquad (8)$$

$$I_{ij}^{-1}=s_{ij}^2 \mod N \qquad (9)$$

여기서 QR_N은 modulus N에 대하여 이차잉여인 집합전체를 의미하고 j는 편의상 1, 2,...,k로 하였다. 또한 f는 단방향 함수이다.

단계 4 : 키 발급센타는 서명자 i에 대하여 물리적 식별을 한후(N, f, h, $s_{i1},\ldots,s_{ik}$)가 기록된 스마트 카드를 발급 배포한다. 여기서 h는 공개된 단방향함수이다.

나. 불확정전송 키 발생 및 공개

단계 1 : 키 발급센타는 큰 소수 r와 Zr* 상의 생성원 g를 선택하고 Zr* 상의 임의의 원소 C_1, $C_2,\ldots,C_{m-1}$을 선택한 후 이들을 시스템 가입자에게 공개한다.

단계 2 : 서명자 i는 랜덤하게 $k\in\{0, 1, 2,\ldots,m-1\}$을 선택한다. $x_k=x_1+x_2+x_3+\ldots+x_{m-1}$를 만족하는 x_k를 선택한다. 여기서 모든 x는 $\in\{0, 1,\ldots,r-2\}$이다. 사용자 i는 k와 x_k를 비밀리 보관한다.

단계 3 : 자신의 공개키 β_i, $\beta_{i1},\ldots,\beta_{i(m-1)}$를 다음과 같이 계산하여 공개한다.

$$\begin{aligned}
\beta_{ik}&=g^{x_k} \bmod r\\
\beta_{i(k+1)}&=C_1(g^{x_1})^{-1} \bmod r\\
\beta_{i(k+2)}&=C_2(g^{x_2})^{-1} \bmod r\\
&\vdots\\
\beta_{i(k+m-1)}&=C_{m-1}(g^{x_{m-1}})^{-1} \bmod r
\end{aligned} \qquad (10)$$

여기서 β_{in}의 n은 모듈러 m에 대한 값이다.

4.2 다중서명 수행절차

본 제안 방식의 다중서명 수행절차는 그림3과 같다.

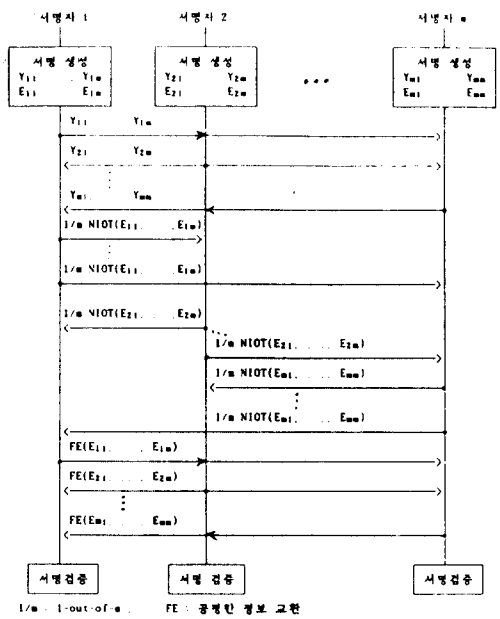

그림 3. 제안된 디지탈 다중서명 방식의 서명 수행절차
Fig 3. Procedure of the proposed digital multisignature scheme

가. 서명 생성 단계

본 디지탈 다중서명 시스템에 참여한 모든 서명자는 다음과 같이 각자의 서명을 생성한다.

단계 1 : 서명자 n은 랜덤수 $R_{n1},\ldots,R_{nm} \in Z_N$을 선택한다. 여기서 Z_N은 {0, 1,...,N-1}을 나타낸다. 그리고 다음을 계산한다.

$$X_{n1} = R_{n1}^2 \mod N \qquad (11)$$

$$X_{n2} = R_{n2}^2 \mod N$$

$$\vdots$$

$$X_{nm} = R_{nm}^2 \mod N$$

단계 2 : 서명자 n은 서명할 메세지 M에 대하여 자신의 서명을 다음과 같이 생성한다. 여기서 ID_{cm}은 메세지 M에 서명할 사람들의 ID의 연접이다. 즉, $ID_{cm} = ID_1 \| ID_2 \| \ldots \| ID_m$ 이다.

$$E_{n1} = (e_{n11},\ldots,e_{n1k}) = h(M, X_{n1}, ID_{cm}) \qquad (12)$$

$$E_{n2} = (e_{n21},\ldots,e_{n2k}) = h(M, X_{n2}, ID_{cm})$$

$$\vdots$$

$$E_{nm} = (e_{nm1},\ldots,e_{nmk}) = h(M, X_{nm}, ID_{cm})$$

$$Y_{n1} = R_{n1} \prod_{e_{n1j}=1} S_{nj} \mod N \qquad (13)$$

$$Y_{n2} = R_{n2} \prod_{e_{n2j}=1} S_{nj} \mod N$$

$$\vdots$$

$$Y_{nm} = R_{nm} \prod_{e_{nmj}=1} S_{nj} \mod N$$

여기서 j = 1, 2,...,k이다.

나. 서명 정보 공개 전달 단계

단계 1 : 서명자 1은 자신의 서명 정보 $Y_{11},\ldots,Y_{1m}$을 다른 서명자들에게 동보전송하여 전달한다.

단계 2 : 다중서명 시스템에 참여한 다른 모든 서명자들도 자신들의 서명정보를 위의 단계 1 과같이 전달한다. 이때 서명자 순서는 상관없다.

다.($E_1,\ldots,E_m$)의 불확정 전송단계

단계 1 : 서명자 1은 서명자 2에게 II장에서 기술한 1-out-of-m NIOT를 이용하여 자신의 $E_{11},\ldots,E_{1m}$중 하나를 불확정 전송한다. 이때 서명자 2는 서명자 1로부터 얻은 E_{1k} 정보로부터 Y_{1k}를 검증하고 부정이 검출될시 이를 모든 서명자들에게 알리고 프로토콜 수행을 중지한다.

단계 2 : 서명자 1은 서명자 3,...,서명자 m에게도 각각 위의 단계 1과 같이 수행하여 자신의 $E_{11},\ldots,E_{1m}$ 중 하나를 불확정 전송한다.

단계 3 : 다른 서명자들도 위의 단계 1, 단계 2를 수행하여 각자 자신의 m개 정보중 하나의 정보를 다른 서명자들에게 각각 불확정 전송한다.

라.($E_1,\ldots,E_m$)의 공평한 정보교환 단계

단계 1 : 각 서명자(서명자 n)는 자신의 비밀정보 $(E_{n1},\ldots,E_{nm})$에 대하여 III장에서 기술한 공평한 비밀정보 교환방법을 이용하여 서로 교번하면서 상호간의 비밀정보들을 공평하게 교환한다.

단계 2 : 이때 부정이 검출되면 이를 모든 서명자에게 알리고 프로토콜 수행을 중지한다.

이렇게 함으로써 각 서명자는 다른 서명자들의 서명정보$(Y_{11},\ldots,Y_{1m}),\ldots,(Y_{m1},\ldots,Y_{mm}),(E_{11},\ldots,E_{1m}),\ldots,(E_{m1},\ldots,E_{mm})$을 모두 가지게 된다.

4.3 다중서명 검증

위의 다중서명 프로토콜 수행에서 모든 서명자가 정직하게 수행하였다면 모든 서명자는 서명정보$(Y_{11},\ldots,Y_{1m}),\ldots,(Y_{m1},\ldots,Y_{mm}),(E_{11},\ldots,E_{1m}),\ldots,(E_{m1},\ldots,E_{mm})$을 모두 가지게 되고, 다중서명 검증은 다음과 같이 수행한다.

다중서명 검증자는 다음을 계산한다.

$$I_{ij} = f(ID_i, j) \qquad (14)$$

$$Z_{it} = Y_{it}^2 \prod_{e_{itj}=1} I_{ij} \mod N \qquad (15)$$

$$E_{it} = h(M, Z_{it}, ID_{cm}) \qquad (16)$$

여기서 i, t = 1, 2,...,m, j = 1, 2,...,k이다.

모든 서명자의 서명 정보에 대해서 위의 검증식이 모두 만족되면 다중서명은 유효한것으로 간주한다.

만약 모든 서명자가 위의 프로토콜을 정직하게 따랐다면 정의에 의해서 $I_{ij}^{-1}=S_{ij}^2 \bmod N$ 이고 Z_{it}는 다음과 같이 X_{it}가 된다.

$$\begin{aligned} Z_{it} &= Y_{it}^2 \prod_{e_{ij}=1} I_{ij} \mod N \\ &= R_{it}^2 \prod_{e_{ij}=1} S_{ij}^2 I_{ij} \mod N \\ &= R_{it}^2 \mod N \\ &= X_{it} \mod N \end{aligned} \tag{17}$$

V. 안전성 분석

본 논문에서 제안한 디지탈 다중서명방식에 대한 안전성을 분석해본다. 본 방식에서의 다중서명은 Fiat-Shamir의 서명방식을 직접 적용하였기 때문에 Fiat-Shamir 방식과 같이 안전하다고 할 수 있다. 불확정 전송 단계에서 1-out-of-m NIOT를 이용하였기 때문에 각 서명자는 다른 서명자의 m개의 비밀정보 중 하나만을 소유할 수 있고 나머지 비밀 정보에 대한 안전성은 $C_1, C_2, \ldots, C_{m-1}$의 이산대수 문제의 어려움에 달려 있기 때문에 Diffie-Hellman의 가정과 같이 안전하다. 이 단계에서 서명자 n은(m-1)명의 다른 서명자에게 각각 1-out-of-m NIOT를 수행함으로써 서명자 n은 다른 서명자들에 대해서 자신의 m개 정보 $(E_{n1},\ldots,E_{nm})$ 중 최대(m-1)개 정보를 불확정 전송하게 되는 것이다. 따라서 서명자 n은 자신의 m개 정보중 다른 서명자들이 어떤 정보를 가지고 있는지를 알 수 없다. 또한 서명자 n은 이미 자신의 서명정보 $Y_{n1},\ldots,Y_{nm}$을 모두 전달하였기 때문에 이 단계에서 부정을 할 경우 다른 서명자에 의해서 조기에 검출될 수 있다. 또한 프로토콜의 전개가 대화형식이 아니고 송신자는 수신자에게 단 한번의 통신으로 불확정전송을 수행함으로써 통신 회수를 급격히 줄일 수 있다.

공평한 정보교환 단계에서 서명정보를 한 비트씩 교환하지 않고 III장에서와 같이 스트링으로 교환함으로써 어느 한쪽이 한꺼번에 서명을 보냄으로써 받는 불이익을 감소 시켰다. 따라서 어느 서명자가 손해볼 수 있는 계산상의 이득을 미리 정해둔 k 값에 따라 최대$(2^{k-1}+1)$대 2^{k-1}로 하였다. 상대방이 거짓 스트링을 보냄으로써 그 거짓 정보에 대한 부정이 검출될 확률은 최대(m-1)/m이다.

이 단계에서 모든 서명자가 정직하게 프로토콜을 수행하였다면 모든 서명 참여자는 상대방의 서명을 동시에 상호 교환할 수 있게 되어 상대방의 서명정보를 모두 얻게된다.

VI. 결 론

본 논문에서는 암호화 프로토콜을 설계하는데 있어서 중요한 불확정전송 프로토콜에 대해서 알아보고 동시성을 갖는 디지탈 다중서명방식에 필요한 1-out-of-n NIOT를 이산대수 문제에 근거한 새로운 방식을 제안하였다. 또한 서명정보의 상호교환에 있어서 도중에 프로토콜을 중지 하였을 경우 상대방의 계산상 이득을$(2^{k-1}+1)$대 2^{k-1}로 줄일 수 있는 다자간의 공평한 비밀정보 교환방식을 새로이 제안하였다.

제안된 암호화 프로토콜을 이용하여 m명이 다중서명 시스템에 가입하여 서명을 수행할 때 동시성을 갖는 새로운 디지탈 다중서명방식을 제안하고 안전성을 분석하였다. 본 제안된 방식의 특징은

첫째, Fiat-Shamir 서명방식을 직접 이용하였으므로 Fiat-Shamir 서명방식과 같이 안전하고 또한 그의 장점을 모두 가지고 있으며

둘째, 다중서명 시스템에서 한쪽의 불이익을 방지할 수 있는 동시성을 가지고 있으며

세째, 서명자들이 정직하게 서명 프로토콜을 수행 완료하면 각 서명자는 다른 서명자들의 서명을 모두 소유할 수 있고

네째, 다중서명 프로토콜 수행도중 부정을 행하였을 경우 이를 조기에 검출할 수 있다.

이와같은 특징으로 본 논문에서 제안된 방식은 전자계약시스템 등 동시성이 요구되는 각종 서명시스템에 효율적으로 적용될 수 있을것으로 사료되며, 앞으로 연구로서는 m명이 가입한 다중서명 시스템에서 서명자 한 사람이(m-1) 서명자에게(m-1)-out-of-m NIOT를 수행할 수 있는 효율적인 방법과 안전성, 통신량 감소등 효율성을 향상시킬 수 있는 동시 다중서명방식에 관한 연구가 요구된다.

참 고 문 헌

1. 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.

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. K.Ohta and T.Okamoto, "A Digital Multisignature Scheme Based on the Fiat-Shamir Scheme," Proceedings of Asiacrypt'91, pp.75-79, 1991.
5. K.Itakura and K.Nakamura, "A Public-key Cryptosystem Suitable for Digital Multisignature," NEC J.Res, Dev.71, pp.1-8, 1983.
6. T.Okamoto, "A Digital Multisignature Scheme Using Bijective Public-Key Cryptosystems," ACM Trans. on Comp. systems. Vol.6, No.8, pp.432-441, 1988.
7. 강창구, 김대영, "순차적 다중서명 방식," 한국통신학회 하계종합학술발표회 논문집, pp.31-35, 1992.
8. 강창구, 김대영, "새로운 순차 및 동시 다중서명 방식," 한국통신정보보호학회 논문지, 제2권 1호, pp.36-44, 1992.
9. R.Peralta, R.Berger, T.Tedrick, "A Provably Secure Oblivious Transfer," Proceedings of Eurocrypt'84, pp.379-386, 1984.
10. A.Yao, "How to Generate and Exchange Secrets," Proceedings of 27th FOCS, pp.162-167, 1986.
11. T.Tedrick, "How to Exchange Half a Bit," Proceedings of Crypto'83, pp.147-151, 1983.
12. J.Halpern and M.O.Rabin, "A logic to Reason about Likelihood," Proceedings of the 19th ACM Symposium on Theory of Computing, pp.310-319, May, 1983.
13. M.Bellare and S.Micali, "Non-interactive Oblivious Transfer and Applications," Proceedings of Crypto'89, pp.547-557, 1989.
14. A.De Santis and G.Persiano, "Public-Randomness in Public-Key Cryptography," Proceedings of Eurocrypto'90, pp.46-62, 1990.
15. M.Blum, "How to Exchange Secret Keys," ACM Trans. Comput. System, pp.175-193, May, 1983.
16. S.Even, O.Goldreich, A.Lempel, "A Randomized Protocol for Signing Contracts," Comm. ACM, Vol.28, No.6, pp.637-647, June, 1985.
17. T.Tedrick, "Fair Exchange of Secrets," Proceedings of Crypto'84, pp.434-438, 1984.
18. A.Fiat and A.Shamir, "How to prove yourself : Practical Solution to Identification and Signature Problems," Advances in Cryptology-Crypto'87, Lecture Notes in Computer Science 263, pp.186-199, 1987.

姜 昌 求(Chang Goo Kang) 정회원
1957년 3월 1일생
1979년 2월 : 한국항공대학 항공전자공학과 졸업(공학사)
1986년 2월 : 충남대학교 대학원 전자공학과(공학석사)
1993년 8월 : 충남대학교 대학원 전자공학과(공학박사)
1979년~1982년 : 한국공군 기술장교
1987년~현재 : 한국전자통신연구소 부호기술부 책임연구원

金 大 榮(Dae Young Kim) 정회원
1952년 5월 28일생
1975년 2월 : 서울대학교 공과대학 전자공학과(B.S)
1977년 2월 : KAIST 전기 및 전자공학과(M.S)
1983년 2월 : KAIST 전기 및 전자공학과(Ph.D)
1978년~1981년 : 독일 RWTH Aachen, UNI Hannover 공대 연구원
1987년~1988년 : 미국 University of California Davis 분교 객원연구원
1983년~현재 : 충남대학교 정보통신공학과 교수