고속 디지틀 다중서명에 관한 연구

•
홍 성 설, 전 문 석
숭실대학교 전자계산학과

A Study on the High-Speed Digital Multisignature Scheme

•
Seong-Seol Hong, Moon-Seog Jun
Dept. of Computer Science, Soongsil University

요 약

디지틀 서명 분야는 암호학의 주요 응용 분야로서, 그 응용 영역이 상용 시스템까지 확대되고 있는 실정이다. 본 논문에서는 Fiat-Shamir의 서명 방식에 근거한 순차 다중서명 방식을 제안한다. 제안되는 순차 다중서명 방식은 Fiat-Shamir의 서명 방식과 같은 안전성을 가지며, 단순서명 방식을 반복, 적용함으로써 나타나는 서명 속도의 문제를 개선한다.

1. 서 론

컴퓨터 기술 및 통신 기술의 발달은 고도의 정보 통신망을 이룩하는데 지대한 공헌을 하였다. 고도의 정보 통신망의 실현은 인류에게 유용한 정보를 신속하고 정확하게 처리하여 제공할 수 있게 하였다. 그러나, 통신망을 통하여 전송되는 정보는 어떠한 사람이든지 쉽게 접근이 가능하기 때문에 정보의 무단인출, 위조, 파괴의 위험성을 내포하고 있으므로 이러한 위험성을 해결하지 못한다면 개인은 물론 사회 전반에 커다란 영향을 미치게 된다. 따라서, 이러한 정보 보안상의 문제 및 범죄 행위를 사전에 예방하기 위하여 출현한 것이 암호화(cryptography)이다. 암호화는 인가된 사람만이 허가된 정보를 이해할 수 있도록 정보를 변형하는 기법으로 암호화 기법은 오래 전부터 연구되어 왔다.

최근 정보 통신망을 통하여 제공되는 고도 통신망 서비스가 활발히 연구, 개발되고 있으며, 이러한 서비스의 특징은 통신망 상에서 메세지를 이용하여 다양한 형태의 서비스를 제공하기 때문에 메세지 자체에 대한 인증이나 사용자에 대한 인증 문제가 중요하게 대두되고 있다. 인증의 방법에는 여러가지가 있으며, 그 중에서 디지틀 서명(digital signature)은 수기 서명의 효과를 전자적 매체 내에 저장, 전송되는 정보에 대해서 전자적으로 실행하는 새로운 서명 방식이다.

디지틀 서명은 메세지의 송신자가 송신을 부정할 수 없고, 정당한 수신자조차도 메세지의 내용을 위조할 수 없도록 하는 것으로써, 이와 같은 서명의 방식에는 공통키 암호 시스템을 이용하는 방식과 공개키 암호 시스템을 이용하는 방식이 있다. 공통키 암호 시스템을 이용한 디지틀 서명 방식은 서명자와 검증자 간에 공통의 비밀키에 의해서 서명을 생성, 검증하기 때문에 검증자가 서명을 변조하여 새로운 서명 메세지를 생성할 수 있다. 따라서, 공통키 암호 시스템에 의한 서명은 분쟁을 해결하기 어려우므로 서명 방식으로는 효과적이지 못하나, 공개키 암호 시스템의 계산량이 많다는 단점을

보완하기 위한 방법으로서 제안되었다. 이에 반하여, 공개키 암호 시스템을 이용한 디지털 서명 방식은 암호화할 때 사용하는 키(공개키)와 복호화할 때 사용하는 키(비밀키)가 서로 다르게 생성되어 공개키는 공개하고 비밀키만 안전하게 유지하는 방식으로 디지털 서명을 보다 효율적으로 실현할 수 있다.

지금까지 많은 서명 방식들이 개발되었으나, 이들의 대부분은 단순서명(single signature) 방식이었다. 단순서명 방식을 반복함으로써 다중서명에 적용할 수 있으나, 메세지의 길이, 서명 속도 등에서 비효율적이다. 이러한 문제를 해결하기 위해서 Itakura-Nakamura 다중서명 방식, Okamoto 다중서명 방식 등이 제안되었다.

본 논문에서는 Fiat-Shamir의 서명 방식에 근거하고 있으며, 기존의 방식들에 비해 개선된 서명 생성 속도를 가지는 새로운 순차 다중서명 방식을 제안한다. 또한, 제안된 방식과 기존의 접근 방식들의 서명 생성 속도를 비교한다.

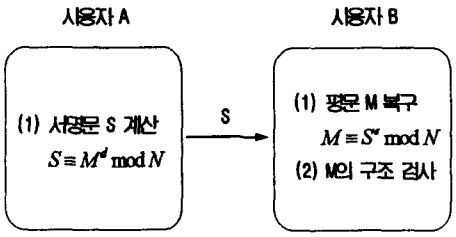
2. 디지털 서명

디지털 서명은 전자적으로 생성된 메세지를 인증하는 방법 중에서 가장 이상적인 메카니즘이다. 이러한 디지털 서명의 목적은 송신자가 자신이 전송한 메세지의 내용을 부인할 수 없도록 하고, 수신자는 수신한 메세지를 위조할 수 없도록 하는 것이다.

2.1 디지털 서명에 관한 기존의 접근 방식

2.1.1 RSA 서명 방식

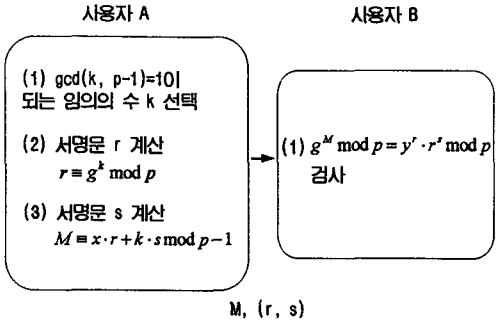
RSA 서명 방식은 정보 보호 기능과 디지털 서명 기능을 동시에 수행할 수 있는 암호 방식으로 널리 이용되고 있다. RSA 서명 시스템은 큰 합성수에 대한 소인수 분해 어려움을 비도로 하고 있다. 이 방식은 비도 측면에서 안정적이라고 평가되고 있지만, 키 값의 지수승을 계산해야 하기 때문에 암호화하는데 많은 시간이 소요된다는 단점을 지니고 있다. RSA 서명 시스템을 구성하기 위한 절차는 <그림 1>과 같다.



<그림 1> RSA 서명 시스템

2.1.2 ElGamal 서명 방식

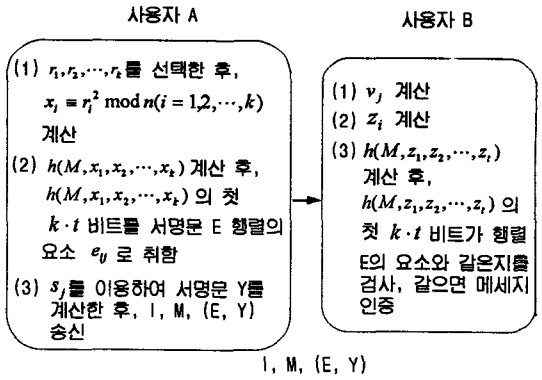
ElGamal은 p가 큰 소수일 경우, GF(P)상에서 이산대수 문제를 해결하는 것이 매우 어렵다는 사실에 기반을 두고 있는 암호 시스템 및 서명 시스템을 제안하였다. ElGamal 서명 시스템에서의 서명문은 한 쌍으로 구성되며, 메세지와 서명문의 관계식을 이용하여 서명문 인증을 수행한다. ElGamal 서명 시스템의 기본 동작은 <그림 2>와 같다



<그림 2> ElGamal 서명 시스템

2.1.3 Fiat-Shamir 서명 방식

Fiat와 Shamir는 ID를 이용하는 개인 식별방식에 기반을 둔 사용자 인증 및 서명 시스템을 제안하였다. Fiat-Shamir의 개인 식별 프로토콜은 ZKIP을 이용하는 매우 안전한 개인 식별 프로토콜이다. 이 서명 시스템은 메세지와 서명문의 관계식을 이용하여 서명문 인증을 수행하며, 기본 동작은 <그림 3>과 같다.



<그림 3> Fiat-Shamir 서명 시스템

3. 디지틀 다중서명

지금까지의 디지틀 서명 방식은 한 사람이 어떤 메세지에 전자적으로 서명하는 단순서명이었다. 그러나 정보화 사회는 대부분이 계층적인 구조를 가지고 있으며, 작성된 문서는 증명과 승인을 위하여 결재가 요구되며, 이 때 기안자의 서명뿐만 아니라 상급자의 서명이 요구되기도 한다. 또한, 회의 결과를 전자 문서로 작성하고 최종적으로 회의 참석자의 동의를 얻어야 할 때, 참석자 모두의 서명이 요구된다. 이와 같이 동일한 메세지에 여러 사람이 전자적으로 서명하는 것을 디지틀 다중서명(digital multisignature)이라 한다. 이러한 다중서명 방식에는 같은 메세지에 서명자들이 순서적으로 서명하는 순차 다중서명 방식(sequential multisignature scheme)이 있고, 서명자들이 같은 메세지에 무순서적으로 동시에 서명하는 무순차 다중서명 방식(simultaneous multisignature scheme)이 있다. 본 논문에서 제안하는 방식은 순차 다중서명 방식이다.

3.1 디지틀 다중서명에 관한 기존의 접근 방식

기존의 디지틀 다중서명 방식으로는 Itakura와 Nakamura(Itakura-Nakamura 다중서명 방식)가 두 개의 큰 소수와 각 서명자의 직위에 따른 작은 소수의 곱을 이용하여 RSA 방식을 확대한 다중서명 방식을 제안하였으며, Okamoto는 공개키 암호 시스템과 단방향 함수를 이용하는 Okamoto 다중서명 방식을 제안하였다. 그러나, 이들 디지틀 다중서명 방식은 RSA 방식에 근거하고 있기 때문에 서명을 생성하는데 많은 계산량이 요구된다는 단점을 지니고 있다. 또한, Ohta와 Okamoto는 Fiat-Shamir의 서명 방식을 이용하여 순차 다중서명 방식을 제안하였다. 본 논문에서는 같은 방식에 근거하고 있는 Ohta-Okamoto 다중서명 방식에 대하여 언급한다.

3.1.1 Ohta-Okamoto 다중서명 방식

Ohta와 Okamoto는 Fiat-Shamir의 서명 방식에 근거한 다중서명 방식을 제안하였다. 이 방식은 m명의 서명자가 순차 다중서명을 수행하고자 할 때 $(2m-1)$번 통신을 수행해야 하고, 서명자는 첫번째 라운드에서 생성한 난수를 메세지에 직접 서명할 때까지 보관하여야 하며, 첫번째 라운드와 두번째 라운드의 서명 순서가 다른 경우, 중간 서명자는 앞 서명자의 서명을 확인할 수 없게 된다.

4. 새로운 디지틀 다중서명 방식의 제안

본 장에서는 Fiat-Shamir의 서명 방식에 근거하고, 기존의 방식들에 비해 개선된 서명 처리 속도를 가지는 새로운 순차 다중서명 방식을 제안한다. m명의 서명자가 다중서명 시스템에 참여하여 같은 메세지에 서명하고, 검증자는 다중서명된 메세지를 검증한다고 가정한다. 사용되는 기호는 다음과 같이 정의한다.

M = 서명할 메세지
f, h = 공개된 단방향 함수
CO = 압축 함수
ID_i = 서명자 i의 ID 정보
$ID_{cm} = ID_1 \| ID_2 \| \cdots \| ID_m$
k = 보안 변수

제안된 순차 다중서명 방식은 Fiat-Shamir의 서명 방식에 근거하여 두 개의 단방향 함수를 사용하고 있으며, 메세지의 길이 문제를 개선하기 위해서 메세지를 압축하는 하나의 함수를 사용한다.

4.1 키 생성 및 분배

서명자 i가 자신의 개인정보인 ID_i를 키 발급센터(trusted center)에 등록하면, 키 발급센터는 다음 절차에 의해 키를 생성, 분배한다.

1) 키 발급센터는 큰 소수 p, q, r을 임의로 선택하고 그들의 곱 $N = p \bullet q \bullet r$을 계산한다.

2) 키 발급센터는 각 서명자 i에 대해서 $S_{ij}(1 \le j \le k)$를 다음과 같이 계산한다.

$$I_{ij} = f(ID_i, j), j = 1,2,\cdots,k \quad (4.1)$$

$$I_{ij}^{-1} = S_{ij}^2 \bmod N \quad (4.2)$$

3) 키 발급센터는 서명자 i에 대해서 식별을 한 후, $(N, f, h, S_{i1}, \cdots, S_{ik})$가 기록된 스마트 카드를 발급한다.

4.2 다중서명 생성

4.2.1 서명자 1의 서명 생성

1) 서명자 1은 메세지에 서명할 사람의 순서를 결정하고, $ID_{cm} = ID_1 || ID_2 || \cdots || ID_m$을 구성한다. 여기서, ID_1은 첫번째 서명자의 ID이고 ID_m은 최종 서명자의 ID이다.

2) 서명자 1은 임의의 수 $R_1 \in Z_N$을 선택하고, 다음을 계산한다. 여기서, Z_N은 $\{0,1,\cdots,N-1\}$을 나타낸다.

$$X_1 = R_1^2 \bmod N \quad (4.3)$$

$$(e_{11},\cdots,e_{1k}) = h(M, ID_{cm}, X_1) \quad (4.4)$$

$$Y_1 = R_1 \prod_{e_{1j}=1} S_{1j} \bmod N, j = 1,2,\cdots,k \quad (4.5)$$

3) 서명자 1은 메세지를 압축하여 $CO(M)$을 생성한다.

4) 서명자 1은 $(CO(M), ID_{cm}, X_1, Y_1)$을 다음 서명할 ID_2를 가진 서명자에게 전송한다.

4.2.2 서명자 n의 서명 생성

1) 서명자 n은 서명자 (n-1)로부터 서명 메세지 $(CO(M), ID_{cm}, X_1, \cdots, X_{n-1}, Y_{n-1})$을 받으면 다음의 검증 절차와 같이 앞 서명자들의 서명을 확인한다. 이 절차는 생략될 수 있다.

2) 서명자 n은 서명을 위해서 임의의 수 $R_n \in Z_N$을 선택하고 다음을 계산한다.

$$X_n = R_n^2 X_{n-1} \bmod N \quad (4.6)$$

$$(e_{n1},\cdots,e_{nk}) = h(M, ID_{cm}, X_n) \quad (4.7)$$

$$Y_n = Y_{n-1} R_n \prod_{e_{nj}=1} S_{nj} \bmod N, j = 1,2,\cdots,k \quad (4.8)$$

3) 서명자 n은 $(CO(M), ID_{cm}, X_1, \cdots, X_n, Y_n)$을 다음 서명할 ID_{n+1}을 가진 서명자에게 전송한다. 만약, 서명자 n이 마지막 서명자 즉, 서명자 m이면 $(CO(M), ID_{cm}, X_1, \cdots, X_m, Y_m)$을 검증자에게 전송한다.

4.3 다중서명 검증

4.3.1 서명자 n의 검증

앞 서명자로부터 서명 메세지 $(CO(M), ID_{cm}, X_1, \cdots, X_{n-1}, Y_{n-1})$을 받으면, 서명자 n은 서명 메세지를 다음과 같이 검증한다.

1) 서명자 n은 $X_1, \cdots, X_{n-1}$로부터 다음을 계산한다.

$$(e_{i1},\cdots,e_{ik}) = h(M, ID_{cm}, X_i), i = 1,2,\cdots,n-1 \quad (4.9)$$

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

$$I_{ij} = f(ID_i, j), i = 1,2,\cdots,n-1, j = 1,2,\cdots,k \quad (4.10)$$

3) 서명자 n은 $Y_{n-1}, (e_{11},\cdots,e_{1k}),\cdots,(e_{(n-1)1},\cdots,e_{(n-1)k}), I_{ij}$ 를 이용하여 다음을 계산한다.

$$Z_{n-1} = Y_{n-1}^2 \prod_{i=1}^{n-1}\prod_{e_{ij}=1} I_{ij} \bmod N, j = 1,2,\cdots,k \quad (4.11)$$

4) 서명자 n은 $Z_{n-1} = X_{n-1}$ 을 점검한다. 만약 $Z_{n-1} = X_{n-1}$ 이면, 다중서명 메세지는 유효하다고 간주한다.

4.3.2 검증자의 검증

검증자가 마지막 서명자로부터 다중서명 메세지 $(CO(M), ID_{cm}, X_1,\cdots,X_m, Y_m)$ 을 수신하면,

$$(e_{i1},\cdots,e_{ik}) = h(M, ID_{cm}, X_i), i = 1,2,\cdots,m \quad (4.12)$$

을 계산하고, 다중서명 검증을 위하여

$$(CO(M), ID_{cm}, (e_{11},\cdots,e_{1k}),\cdots,(e_{m1},\cdots,e_{mk}), Y_m) \quad (4.13)$$

을 보관한다. 다중서명 검증의 절차는 다음과 같다.

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

$$I_{ij} = f(ID_i, j), i = 1,2,\cdots,m, j = 1,2,\cdots,k \quad (4.14)$$

2) 검증자는 Z_m 을 다음과 같이 계산한다.

$$Z_m = Y_m^2 \prod_{i=1}^{m}\prod_{e_{ij}=1} I_{ij} \bmod N, j = 1,2,\cdots,k \quad (4.15)$$

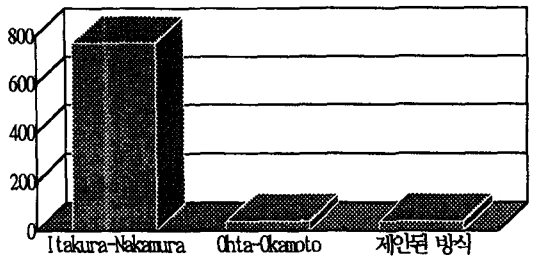
3) 검증자는 다음이 만족되는지를 확인한다.

$$(e_{m1},\cdots,e_{mk}) = h(M, ID_{cm}, Z_m) \quad (4.16)$$

만약 식 (4.16)이 만족되면, 다중서명 메세지는 유효한 것으로 간주한다.

5. 기존의 디지틀 다중서명 방식과 새로운 디지틀 다중서명 방식의 비교

새로이 제안된 다중서명 방식은 Fiat-Shamir 방식에 근거하고 있기 때문에 서명 속도가 RSA 방식에 근거하고 있는 방식보다 빠르고, ID에 근거한 서명 방식이므로 공개키 기록집이 필요없어 키 관리를 단순화할 수 있으며, 서명 순서에 제약이 없다. 서명 처리 속도는 서명자가 서명을 생성하는데 요구되는 처리량으로 평가하였으며, <그림 4>에서 결과를 보이고 있다.



<그림 4> 서명 생성 속도

6. 결 론

암호는 컴퓨터 및 통신망에 신뢰성을 부여할 수 있는 중요한 수단으로 알려져 있다. 디지틀 서명 및 다중서명은 수기 서명의 효과를 전자 문서에 수행할 수 있으므로 최근 전문인뿐만 아니라 일반인에게도 그 중요성이 인식되고 있다. 본 논문에서는 Fiat-Shamir의 방식에 근거한 새로운 디지틀 다중서명 방식을 제안하였으며, 제안된 방식의 특징 및 효율성을 분석하였다. 새로이 제안된 방식은 Fiat-Shamir 방식에 근거하고 있기 때문에 Fiat-Shamir 방식의 장점을 지니고 있으며, 서명 처리 속도의 문제를 개선하였다. 디지틀 다중서명 방식은 정보화 사회에서 필수적인 요소로서 서명 메세지 길이, 서명 처리 속도, 통신 복잡도 등의 효율성을 개선할 수 있는 방식의 연구가 요구되며, 동시에 무순차 디지틀 다중서명 방식에 관한 연구도 병행되어야 할 것이다.

< 참 고 문 헌 >

[1] K. Ohta and T. Okamoto, "A Modification of the Fiat-Shamir Scheme", Crypto '88, 1988.

[2] 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 Vol. 263, 1987.

[3] "현대암호학", 한국전자통신연구소편, 1991.

[4] T. Okamoto, "A Digital Multisignature Scheme Using Bijective Public-Key Cryptosystems", ACM Trans. on Comp. systems, Vol. 6, No.8, 1988.

[5] T. Elgamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", IEEE Trans. on Inform., Vol. IT-31, No. 4. 1985.

[6] W. Diffie and M. Hellman, "New Directions in Cryptography", IEEE Trans. Inform. Theory, Vol. IT-22, 1976.

[7] 염흥렬, "디지틀 서명 방식 고찰", 통신정보보호학회지, 제 3권, 제 2호, 1993.

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