제18회 한국정보처리학회 추계학술발표대회 논문집 제9권 제2호 (2002.11)

다중 수신자 지정 서명 방식에 관한 연구

홍종국, 이임영
순천향대학교 정보기술공학부
e-mail:siroe@hotmail.com, imylee@sch.ac.kr

A Study on Digital Multi-Nominative Signature

Jong-kook Hong, Im-yeoung Lee
Division of Information Technology, Soon-chun-hyang University

요 약

통신 단말기 및 네트워크의 발전을 통해 종이로 작성된 각종 공문서 및 서류들이 전자적인 형태로 유통되고 있다. 이러한 문서 중에는 동일한 문서에 관인을 찍어 다수의 수신자에게 발송하는 경우가 종종 있으며, 이와 같이 동일 문서에 서명을 수행하여 다수의 수신자에게 전자적으로 전송해야 할 경우 수신자의 수만큼 전자서명을 수행해야 한다. 이러한 경우 기존의 공개키 암호 방식이나 수신자 지정 서명 방식을 이용하게 되면 연산량 측면에서 서명자에게 많은 부담을 줄 수밖에 없다. 따라서, 본 논문에서는 한번의 서명 수행으로 다수의 수신자에게 효율적으로 전송할 수 있는 다중 수신자를 위한 디지털 서명 방식을 제안한다.

1. 서론

현대 사회의 정보화는 인터넷 및 컴퓨터의 발전을 통해 사용범위가 점점 넓어지고 있다. 특히, 기존의 종이로 된 문서들은 전자적 형태의 문서로 대체되어 가고 있다. 이런 전자 문서의 사용은 전송 및 보관의 용이성과 함께 비용 절감 등과 같은 많은 장점을 제공한다. 그러나 이러한 전자적 형태의 문서는 장점뿐만 아니라 종이문서에서는 나타나지 않는 단점을 가지고 있다.

따라서, 인터넷과 같은 공개통신로를 이용하여 문서를 전달할 경우 문서가 원하는 수신자에게 전송되었는지?, 보내는 송신자가 누구인지?, 전송도중 문서의 내용이 변경되지는 않았는지 확신할 수 없게 된다. 이와 같은 문제점을 해결하기 위해 사용되는 암호학적 기법이 디지털 서명이다. 디지털 서명의 일반적인 특징은 양자간의 통신에 있어 송신자의 신분을 보증하고 메시지의 무결성을 보장한다.

그러나 특정 문서가 개인의 프라이버시와 관계가 있거나 할 경우 서명의 남용을 막기 위하여 특정 수신자를 대상으로 서명을 수행해야 하는 경우가 발생할 수 있다. 이러한 특수한 경우 일반적인 디지털 서명으로는 문제점을 갖게 되고 이를 위해 다양한 특수 디지털 서명 방식이 제안되고 있다.

그중 특정 수신자를 대상으로 서명을 수행하기 위해 수신자 지정 서명 방식이 제시되어 있다. 이 방식은 전자 상거래, 각종 감사, 공증 등 다양한 분야에서 응용할 수 있으며, 더욱 세분화되고 안전성을 요하는 정보화 사회에 있어 그 비중이 커질 것으로 예상된다.

본 논문에서는 기존 양자간 통신의 수신자지정 서명 방식을 n명의 수신자를 대상으로 수행될 수 있도록 확장한 방식을 제안한다. 즉, 동일 문서에 관인을 찍어 다수의 수신자에게 발송하는 경우와 같이 n명의 수신자를 지정하여 지정된 수신자들만이 서명을 검증할 수 있도록 한다.

2. 관련 연구

본 장에서는 다중 수신자지정 서명 방식과 관련한 특수 서명 방식에 대해 고찰한다.

가. 수신자 지정 서명 방식

수신자 지정 서명 방식은 지정된 검증자만이 서명을 확인할 수 있는 방식으로 서명자조차도 서명을 확인할 수 없도록 구성되어 있다. 이러한 특성은 필요시 제 3자에게 서명이 서명자에 의해 발행된 정당한 서명임을 증명할 수 있게 된다. 따라서 이 방식은 서명자의 개인 프라이버시와 관련한 응용에 사용할 수 있다.[1]

1) 시스템 계수

다음은 수신자 지정 서명 방식에서 사용되는 시스템 계수 들이다.

- p : P ≥512 bit인 큰 소수
- q : q | p-1인 큰 소수
- g : 위수가 q인 Z_p상의 원시 원소
- X_A : A의 비밀 서명 정보
- $Y_A \equiv g^{X_A} \bmod p$: A의 공개 검증 정보
- X_{bi} : B_i의 비밀 서명 정보
- $Y_{bi} \equiv g^{X_{bi}} \bmod p$: B_i의 공개 검증 정보

2) 프로토콜

수신자 지정 서명 방식의 전체 흐름은 그림 1과 같다.

서명자 A	공개정보 y_A, y_B, p, q, g	검증자 B
		$y_B \equiv g^{X_B} \bmod p$
$y_A \equiv g^{X_A} \bmod p$		
$r, R \in_R Z_q$		
$K \equiv g^{R-r} \bmod p$	M, K, D, S	
$D \equiv y_B^R \bmod p$	==========>	$h(y_B, K, D, M) =$
$e = h(y_B, K, D, M)$		$(g^S y_A^e K)^{X_B} = D$
$S = r - X_A e \bmod q$		mod p

[그림 1] 수신자 지정 서명 방식 흐름도

3) 특징

이 방식은 지정된 수신자만이 서명을 확인할 수 있기 때문에 제 3자의 요청이 없는 경우 오직 검증자만이 서명자의 신원을 증명할 수 있다. 서명이 수신자의 개인적인 이해 관계나 사생활에 밀접한 관련이 있을 경우 수신자의 동의 없이 서명을 확인할 수 없게 되므로, 특정 수신자에 대한 서명 남용을 방지할 수 있다. 이 방식에서 서명에 대한 안전성은 전적으로 검증자에게 의존한다. 이 방식을 n명의 수신자를 대상으로 확장할 경우 n번의 수신자 지정 서명을 수행해야 한다.

나. 다중 수신자를 위한 Signcryption 방식

본 방식은 메시지 m을 t명에게 보내는 경우를 대상으로 한 방식이다.[2]

1) 시스템 계수

- p : 큰 소수
- q : p-1을 나누는 큰 소수
- g : 위수가 q인 Z_p^*의 원소
- m : 메시지
- H : 일방향 해쉬함수
- KH : keyde 일방향 해쉬함수
- $x_a \in {}_RZ_q^*$: A의 개인키
- $y_a \equiv g^{x_a} \bmod p$: A의 공개키
- $x_i \in {}_RZ_q^*$: i의 개인키 (단, $1 \le i \le t$)
- $y_i \equiv g^{x_i} \bmod p$: A의 공개키
- k : 메시지 암호화 키

2) 프로토콜

다음은 이 방식의 전체 흐름을 나타낸 것이다.

Signcryption 서명자 A	공개정보 y_A, y_i, p, q, g	Unsigncryption 검증자 B
(1) $k \in Z_p^*$ 선택 h = KH_k(m) c = E_k(m, h) 암호화 (2) $v_i \in [1, ..., p-1]$ 선택 $k_i = H(y_i^{v_i} \bmod p)$ 계산 $k_i = k_{i1} \| k_{i2}$ $r_i = KH_{i2}$(m, h) $c_i = EK_{i1}$(k) $s_i \equiv v_i/(r_1+x_a) \bmod q$	(c, c_1, r_1, s_1, ..., c_t, r_t, s_t) ==========>	(c, ci, ri, si) 선택 $ki = H((y_a \cdot g^{ri})^{si \cdot xi} \bmod p)$ $k_i = k_{i1} \| k_{i2}$ k = D_{ki1}(ci) w = m||h = D_k(c) KH_k(m) = h, KH_{ki2}(w) = r_i 이면 받아들인.

[그림 2] 다중 수신자를 위한 Signcryption 방식의 흐름도

3) 특징

메시지 m을 t명의 수신자에게 전송하기 위한 Signcryption 방식이다. 위 프로토콜에서 k를 메시지 암호화에 사용하며 모든 수신자들은 동일한 k를 이

용하여 메시지를 복호화한다. 그러나 k를 얻기 위한 과정은 Signcryption을 한번 수행할 때와 동일하게 이루어지며, 수신자가 t명일 경우 프로토콜의 (1)과정은 한번만 수행되나 (2)과정은 t번 수행하게 되어 Signcryption을 t번 수행하는 경우와 똑같은 연산을 수행한다.

3. 다중 수신자 지정 서명 방식

본 장에서는 하나의 문서를 다수의 수신자에게 전송함에 있어 효율적으로 디지털 서명을 수행할 수 있는 특수 디지털 서명 방식을 제안한다. 먼저 이를 위한 고려사항들을 기술한다.

가. 다중 수신자 지정 서명 방식을 위한 고려사항

다음은 다수의 수신자들을 대상으로 하기 위한 고려사항들이다.

- 오직 송신자가 지정한 수신자들만이 서명을 확인할 수 있다.
- 서명자조차도 자신의 서명을 확인할 수 없다.
- 지정된 수신자들은 필요시 제 3자에게 서명 S가 서명자에 의해 자신에게 발행된 정당한 서명임을 증명할 수 있다.
- 서명자 측면에서 서명 수행시 수신자들의 수와 관계없이 연산 효율성을 제공하여야 한다.

나. 다중 수신자 지정 서명 방식 제안

다음은 본 방식에서 사용되는 시스템 계수를 설명한 것이다.

1) 시스템 계수

- p : 소수 ≥512 bit
- q : 소수 ≥160 bit (q | p-1)
- g : 위수가 q인 Z_p^*의 원소
- n : 지정된 수신자 수
- H : 안전한 일방향 해쉬 함수
- M : 메시지 M
- X_A : A의 비밀 서명 정보
- $Y_A \equiv g^{X_A} \bmod p$: A의 공개 검증 정보
- X_{bi} : B_i의 비밀 서명 정보 (i : $1 \le i \le n$)
- $Y_{bi} \equiv g^{X_{bi}} \bmod p$: B_i의 공개 검증 정보

2) 서명 수행 단계

(1) 서명자는 다음과 같은 정보를 생성한다.

. 큰 소수 p와 q를 생성한 후 이를 공개한다.

. 생성자 g를 계산한다.

: $h \in \{1,...,p-1\}$를 선택한다.

: $g = h^{(p-1)/q} \bmod p$가 되는 g를 계산해 낸다. => g를 공개한다.

(2) 서명자는 자신의 비밀키와 공개키를 생성한다.

. 자신의 일반 서명용 개인키를 생성한다.

: X_A (단, $0 < X_A < q$인 난수)

. 공개키는 다음과 같이 생성한다.

: $Y_A = g^{X_A} \bmod p$

(3) 서명자는 다음과 같이 서명 정보를 생성하여 수신자들에게 전송한다.

. 랜덤 수 r, R을 다음과 같이 생성한 후 K를 계산한다.

: $R, r \in {}_RZ_P$

: $K \equiv g^{R-r} \bmod p$

. 수신자들의 공개키를 이용하여 다음을 계산한다.

: $k_1 = Y_{b1}^{R} \bmod p, .., k_n = Y_{bn}^{R} \bmod p$

. 해쉬 함수를 이용하여 다음을 계산한 다음 서명 정보를 생성한다.

: $e = H(k_1, k_2, ..., k_n \| K \| M)$

: $S \equiv r - X_A^e \bmod p$

. 다음을 수신자들에게 전송한다.

: $(k_1, k_2, ..., k_n, K, S, M)$ => 수신자 B_i

3) 서명 검증 단계

(1) 수신자 B_i는 수신된 정보로부터 다음을 계산한다.

. 전송된 정보로부터 k_i 값을 제외한 k'와 D값을 계산한다.

: $k' = \prod_{j=1}^{n} k_j$ [단, $i \neq j$]

: $D \equiv k_i \cdot k' \bmod p$

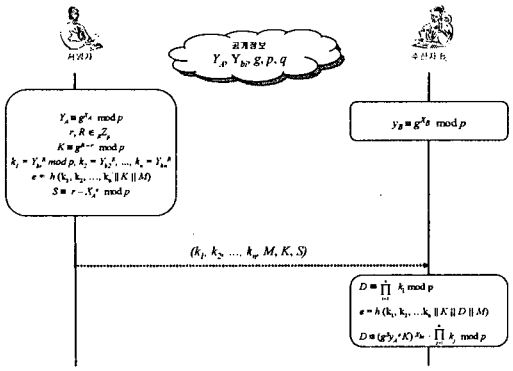
. 해쉬함수를 이용하여 e값을 계산한다.

: $H(k_1, k_2, ..., k_n \| K \| M) = e$

(2) 생성된 e을 통해 다음 수식이 만족한다면 서명은 유효하다고 판단한다.

: $D \equiv (g^S \cdot Y_A^e \cdot K)^{Xbi} \cdot k' \bmod p$

그림 1은 제안 방식에 대한 계략적인 흐름도를 나타낸 것이다.



[그림 3] 제안 방식 흐름도

4) 서명 프로토콜 검증

서명 프로토콜 검증은 다음과 같은 과정을 통해 그 유효성을 입증할 수 있다.

$$\begin{aligned} D &= (g^S \cdot Y_A^e \cdot K)^{Xbi} \cdot (k') \bmod p \\ &= (g^r \cdot g^{-X_A^e} \cdot g^{X_A^e} \cdot g^{R-r})^{Xbi} \cdot k' \bmod p \\ &= (g^R)^{Xbi} \cdot k' \bmod p \\ &= g^{R \cdot Xbi} \cdot k' \bmod p \\ &= Y_{bi}^R \cdot k' \bmod p \\ &= D \end{aligned}$$

4. 제안방식 고찰

본 방식의 연산량에 있어 지수승을 고려하여 n명의 수신자를 가정할 때, 서명 수행에서 n+2번의 지수승과 검증과정에서 3n번의 지수승을 필요로 한다. 기존의 방식을 n번 수행한다면 총 6n번의 지수승 연산을 필요로 하게 된다. 통신량에 있어서는 n명의 수신자를 위한 메시지 전송은 항상 n명에게 전달되어야 하기 때문에 기존 방식을 n번 수행할 때와 동일하다.

수신자들은 자신의 서명 검증 정보 X_{bi}를 이용하여 서명을 검증할 수 있으며, 이를 모르는 제 3자는 서명 검증이 불가능하다.

5. 결론

정보화 사회를 거치면서 많은 부분들이 전자화되어 가고 있으며, 전자화된 문서들은 인터넷과 같은 공개된 통신로를 이용하기 때문에 송신자 인증 및 전송되는 데이터의 무결성 보장 등과 같은 기능들을 만족해야 한다. 이러한 기능들은 디지털 서명을 통해 제공할 수 있다.

본 논문에서는 기존의 양자간 통신에서의 수신자 지정 서명 방식을 n명의 수신자를 대상으로 확장하였으며, 연산량에 있어 기존 방식을 n번 수행했을 때 보다 지수승 연산에 있어 효율적인 방식을 제안하였다. 제안된 방식은 동일 문서를 다수의 수신자에게 전송함에 있어 효율성과 안전성을 제공할 것이다. 현재 제안된 특수 서명 방식들을 응용하여 서명자의 익명성을 보장할 수 있는 서명 방식에 대한 연구가 필요하다.

참고문헌

[1] S. J. Kim, S. J. Park and D. H. Won, "Nominative Signatures," Proc. ICEIC'95, pp.II-68 ~ II-71, 1995.

[2] Y. Zheng. "Signcryption and it's applications in efficient public key solutions," in Proceedings of 1997 Information Security Workshop(ISW'97), Berlin, New York, Tokyo, 1997, Lecture Notes in Computer Science, Springer-Verlag.

[3] C. Boyd, "Digital Multisignatures," Cryptography and Coding, H.J. Beker and F.C. Piper, eds, Oxford : Clarendon Press, 1989, pp.241-246.

[4] 최용락, 소우영, 이재광, 이임영, "컴퓨터 통신 보안", 2001. 2. 28, 도서출판 그린

[5] 이임영, "전자상거래 보안 입문", 2001, 생능출판사