공증을 위한 그룹 서명 방식

이덕규, 이임영
순천향대학교 정보기술공학부

Group Signature Scheme for Notary

Deok-Gyu Lee, Im-Yeong Lee
Division of Information Technology Engineering, Soonchunhyang University

요 약

정보화 사회로의 발전을 통해 네트워크상에서 많은 정보들이 공유 및 교환되고 있다. 이들은 네트워크를 전제로 수행되므로, 다양한 형태의 공격의 대상이 되고 있다. 이를 공격에 대응하고 나아가 사용자 및 메시지 인증을 수행하기 위해 각광을 받고 있는 방법 중에 하나로서 디지털 서명을 들 수 있다. 디지털 서명은 크게 일반 서명 방식과 이를 특수한 상황에 이용하기 위한 특수 서명 방식으로 구분할 수 있다. 특수한 상황 중에서 문서에 대해 법적인 효력을 가질 수 있도록 관인을 찍어 각 수신자에게 발송하는 경우가 있으며, 이와 같이 동일 문서에 서명을 수행하여 수신자에게 전자적으로 전송해야 할 경우 전자서명을 수행해야 한다. 하지만 법적인 효율을 가질 수 있도록 하기 위해 한명의 공증인의 의한 서명은 공모의 취약성이 존재하게 된다. 따라서 본 논문에서는 한명의 공증인에 의한 서명 수행이 아닌 여러 공증인에게 키를 생성 분배하여 이를 이용한 서명 수행으로 공모의 취약성을 효율적으로 개선할 수 있는 공증을 위한 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 종이 문서에서는 나타나지 않은 단점을 가지고 있다. 따라서 인터넷과 같은 공개통신로를 이용하여 문서를 전달할 경우 문서가 원하는 수신자에게 전송되었는지?, 보내는 송신자가 누구인지?, 전송도중 문서의 내용이 변경되지 않았는지 확신할 수 없게 된다. 이와 같은 문제점을 해결하기 위해 사용되는 암호학적 기법이 디지털 서명이다. 디지털 서명의 일반적인 특징은 양자 간의 통신에 있어 송신자의 신분을 보장하고 메시지의 무결성을 보장한다. 그러나 특정 문서가 개인의 프라이버시와 관계되는 경우 양측 사용자 사이에 공증인을 두어 서명의 법적 효력을 가질 수 있도록 한다. 이러한 특수한 경우 일반적인 디지털 서명으로는 문제점을 해결할 수 없다. 이를 위해 다양한 특수 디지털 서명 방식이 제안되고 있다. 그 중 공증을 원하는 사용자를 대상으로 서명을 수행하기 위해 공증을 위한 서명 방식이 제시되고 있다. 하지만 기존 공증을 위해 요청자는 공증인에게 서명을 요청해서 수신자에게 전달하였다. 하지만 이때 요청자와 공증인이 공모하여 새로운 메시지를 생성하거나, 새로운 메시지를 생성하여 후에 공증 자체를 부정할 수 있는 등 문제점이 나타날 수 있다. 본 논문에서는 기존 공모의 문제점을 해결하고자 공증자를 여러 명을 둠으로써 발생할 수 있는 공모의 문제점을 해결할 수 있는 방식을 제안한다. 본 논문은 총 4장으로 구성된다. 2장에서는 기존의 디지털 다중 서명 방식에 대하여 살펴본다. 이를 통해 본 논문의 제안 방식이 가져야 하는 고려사항을 살펴보고 제안방식에 대해 기술한다. 마지막으로 본 논문에 대한 분석을 통해 결론을 맺는다.

본 연구는 한국과학재단 목적기초연구 (R05-2003-000-12019-0)지원으로 수행되었음.

2. 관련 연구

본 장에서는 디지털 다중 서명에 대해 고찰한다.

2.1. 디지털 다중서명

디지털 서명이란 전자적인 정보를 이용하여 디지털 메시지에 서명하는 것으로 메시지 인증과 사용자 인증을 할 수 있어야 한다. 메시지 인증이란 정보가 변경되지 않고 원래의 정보 그대로임을 보증하는 기능이다. 사용자 인증은 사용자 A가 바로 그 A임을 증명하는 기능으로서, 사용자 A가 사용자 B와 협력하여 A가 B에게 A임을 증명할 수 있으나 제 3자인 X는 A로 위장하여 B에게 자신이 A라고 증명할 수 없고 B 또한 제 3자인 D에게 심지어는 자기 자신에게도 A라고 증명할 수 없는 기능이다. 이와 같은 전자서명 기술은 전자문서교환을 위해 중요한 역할을 수행한다. 그러나 대부분의 사무실에서는 계층적인 구조를 가지며 사무실에서 작성한 문서는 기안자 뿐 아니라 상급자들의 서명이 요구된다. 또한 원격회의를 통해 회의결과를 전자문서로 작성하고 최종적으로 회의 참석자들의 동의를 얻어야할 때 참석자들의 서명이 요구된다. 이와 같이 동일한 메시지에 대해 여러 사람이 전자적으로 서명하는 것을 디지털 다중서명(Digital Multi-signature)이라 한다. 서명의 바람직한 특성은 위조하기 어렵고 검증하기 쉬워야 한다. 디지털 서명은 심벌들의 스트링으로 구성되며 이것은 손으로 쓴 서명과는 다르게 서명할 때마다 다르다. 이는 각 디지털서명이 서명하는 메시지의 함수가 되고 timestamp와 함께 사용함으로써 실현 가능하다. 또한 각 서명자에게 유일성을 보장하고 위조를 방지하기 위하여 각 디지털서명은 서명자에게 유일한 비밀키에 의존하는 것이 바람직하다. 검증자는 서명자의 비밀키를 알지 못하더라도 서명을 쉽게 검증할 수 있어야 한다. 이러한 단순서명방법을 기반으로 이루어지는 다중서명 방법은 두 개의 큰 소수와 서명자의 직위에 따라 서명이 이루어지는 Itakura-Nakamura방법, 작은 소수의 곱을 이용하여 RSA 방법을 확대 적용한 Okamoto방법, RSA 방식과 같은 전단사 공개키 암호시스템과 단방향함수로 이루어진 Brickell-Lee-Ya-Cobi방법, Fiat-Shmir 방식에 근거하여 만들어진 Ohta-Okamoto 방법 등이 연구되어있다.

2.2. Okamoto 디지털 다중서명 방법

ID-based 방식인 Fiat-Shamir방식에 근거한 다중 서명 방식이다.

키 발생 및 배포는 서명자 i가 ID_i를 TC에 등록한 뒤 TC는 다음 절차에 의해 키 발생 및 배포를 하게 된다. 우선 TC에서는 두 개의 큰 소수 p, q를 생성하고 비밀리에 유지하며, p, q를 가지고 N=p*q인 N을 공개한다. 서명자i에 대하여 S_{ij}에 대하여 다음을 계산한다. l_{ij} =f(ID_i, j), (j=1,2,.....,k), l_{ij}^{-1} =S_{ij}^2 mod N 그리고, TC에서는 (N, f, h, S_{i1},....S_{ik})가 기록된 스마트카드를 발급 배포한다. 다음은 공통키 생성 단계로 서명자 1 랜덤수 $R_1 \in Z_n$을 선택하고, 다음과 같이 $X_1 = R_1^2$mod N계산한다. X_1을 다음 서명자에게 전송하게 되고, 서명자 n은 앞 서명자로부터 X_{n-1}를 수신하면 랜덤수 $R_n \in Z_n$ 을 선택해 다음 $X_n = R_n^2 X_{n-1}$mod N 계산한다. X_n을 다음 서명자에게 전송, 마지막 서명자일 경우 X_m을 첫 번째 서명자에게 전송한다. 서명 생성 단계는 우선 서명자 1의 서명 발생부터 시작 하게 된다. 서명자 1은 서명할 사람의 순서를 결정하고 다음 (ID_{cm}= ID_1(서명자 1의 ID)|| ID_2 ||...|| ID_m(최종 서명자의 ID)) 구성한다. 서명자 1은 다음과 같이 $Y_1=R_1 \prod_{ej=1} S_{1j}$ mod N, (j=1,2,...,k) 서명을 발생한다. 단, e_i의 값은 다음 (e_1,...e_k)= h(M, ID_{cm}, X_m) 같다. 다음 서명자에게 서명 정보(M, ID_{cm}, X_m, Y_1)을 전송한다. 서명자 n의 서명은 서명자(n-1)으로부터 서명 정보(M, ID_{cm}, X_m,Y_{n-1})를 수신하면 다음 (e_1,....e_k) = h(M, ID_{cm}, X_m), $Y_n = Y_{n-1}R_n \prod_{ej=1} S_{nj}$ mod N (j=1,2,....,k)을 계산한다. (M, ID_{cm}, X_m, Y_n)을 다음 서명자에게 전송한다. 마지막 서명자는 (M, ID_{cm}, (e_1,....e_k), Y_m)을 검증자에게 전송한다. 마지막으로 다중 서명 검증은 법 N과,f ,h,(M, ID_{cm}, (e_1,...e_k),Ym)를 이용해 다중 서명에 대한 검증이 가능하다. 우선 검증자는 ID_{cm}으로부터 서명자들의 l_{ij}를 계산한다. l_{ij} = f(ID_j, j), (i=1,2,.....,m , j=1,2,....,k) 그리고 다음 $Z_m=Y_m^2 \prod_{i=1}^{m} \prod_{ej=1} l_{ij}$ mod N (j=1,2,..., k)을 계산한다. h(M, ID_{cm}, Z_m)을 계산하고 다음의 (e_1,..e_k) = h(M, ID_{cm}, Z_m) 만족 유무를 확인한다. 위 식이 만족하면 다중 서명 메시지는 유효한 것으로 판명한다.

3. 공증을 위한 그룹 서명 방식

본 장에서는 공증을 위한 메시지를 사용자들에게 전송함에 있어 효율적으로 디지털 서명을 수행할 수 있는 공증을 위한 그룹 서명 방식을 제안한다. 먼저 이를 위한 고려 사항들을 기술한다.

3.1 공증을 위한 그룹 서명 방식을 위한 고려사항

다음은 공증 서명을 대상으로 하기 위한 고려사항들이다.

서명문의 길이 고정 : 디지털 다중 서명 방식은 기본적으로 여러 사람들이 네트워크상에서 자신의 컴

퓨터가 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 고정되어야 할 것이다.

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

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

3.2 시스템 계수

다음은 본 방식에서 사용되는 시스템 계수를 기술한 것이다.

- p : 소수 $\geq 512bit$ • q : 소수 $\geq 160bit (q \mid p-1)$
- l : 개인키 생성을 위한 랜덤수
- e : 공개 암호화 키 • θ_i : 세션키
- $\gamma_i \in Z_p$: 랜덤수 ◦ $\Gamma = \gamma_1, \cdots, \gamma_k$
- M : 메시지 • k : 예측 사용자의 수
- i : 사용자 $(i = 1, \cdots, k)$ • j : 탈퇴자
- r_i : 랜덤 수 집합 $(r_i \in Z_p) \rightarrow (r_1, \cdots, r_k)$
- $h_i = g^{r_i}$ • a : 랜덤 요소 $(a \in Z_q)$
- $\langle y, h_1, \cdots, h_k \rangle$: 공개키 ◦ $y = \prod_{i=1}^{k} h_i^{a_i}$
  - ◦ a_i : 랜덤수 $(a_i \in Z_q)(a_1, \cdots, a_k)$
- C : 방송 메시지(Broadcast message)
  - ◦ $C = \langle My^{aT}, h_1^a, \cdots, h_k^a \rangle = \langle B, H_1, \cdots, H_k \rangle$
  - ◦ $B = My^a$ ◦ $H_i = \prod_{i=1}^{k} h_i^a$
  - ◦ T : 키 갱신을 위한 인자 $(t_1, \cdots, t_k \in Z_q)$
  - ◦ $T = t_1 \cdot \cdots \cdot t_k$
- o : 보안 파라메타
- b : 사용자가 생성한 공개정보 $(b \in Z_q)$
- Θ, U : 사용자가 등록에 참여하기 위한 사용자 정보
- ζ : 사용자가 임의로 선택한 값
- Ξ : 사용자의 ID를 보관한 값

3.3 프로토콜

1) 공증인 등록 및 키 분배 단계

공증인 등록은 TC(Trusted Center)가 관할하며, 소속에 등록 및 키를 분배 받기 위해서는 다음과 같은 일련의 과정을 거친다.

Step 1. TC는 공증인의 정보 획득을 위한 값을 생성하여 공개한다.

$$\gamma_i \in \Gamma, \ (\gamma_1, \cdots, \gamma_k)$$

Step 2. 공증인은 공개된 정보 Γ과 자신의 ID를 이용하여 다음의 값을 계산한다.

$$ID_i = (\Xi_i)^{\gamma_i} (\mathrm{mod}\ n)$$

Step 3. 공증인은 생성된 값을 이용하여 다음의 값을 계산한다.

$$\Xi_i \equiv (ID_i)^{1/\gamma_i} (\mathrm{mod}\ n), \quad U \equiv \Xi_i \cdot \zeta (\mathrm{mod}\ n)$$

$$\Theta \equiv \zeta^b (\mathrm{mod}\ n)$$

Step 4. 공증인은 생성된 값(Θ, U)를 TC에게 전송한다.

Step 5. TC는 제공받은(Θ, U)를 이용하여 공증인 정보 ID_i를 획득한다. Θ로부터 ζ을 추출하면 추출한 값을 이용하여 Ξ_i를 얻는다. 얻은 Ξ_i값을 이용하여 ID_i값을 획득한다.

$$\Theta \equiv \zeta^b (\mathrm{mod}\ n) = \zeta, \quad U \equiv \Xi_i \cdot \zeta (\mathrm{mod}\ n) = \Xi_i$$

$$\Xi_i \equiv (ID_i)^{1/\gamma_i} (\mathrm{mod}\ n), \quad ID_i \equiv (\Xi_i)^{\gamma_i} (\mathrm{mod}\ n)$$

Step 6. TC는 공증인 i의 정보를 이용하여 ID_i열을 선택하고 다음을 계산한다.

$$h_i \equiv g^{\gamma_i} \bmod q$$

작성한 값에 해당하는 공개키 열을 생성한다.

$$\langle y, h_1, \cdots, h_k \rangle$$

Step 7. TC는 생성된 값 h_i를 이용하여 공개키를 작성한 후 이를 바탕으로 개인키를 계산한다.

$$\theta_i = \left(\prod_{i=1}^{k} r_i a_i \right) / \left(\prod_{i=1}^{k} r_i \gamma_i \right) \bmod q$$

Step 8. TC는 생성된 개인키 d_i에서 θ_i를 스마트카드를 발급한다. $d_i = \theta_i \cdot \gamma_i / \gamma_i$

2) 그룹 공증 서명 수행 단계

Step 1. TC는 공증자를 선택하고 이를 전체 공증자에게 제공한다.

Step 2. 공증자는 순서에 따라 서명을 수행하게 된다. 우선 공증자 1의 서명 수행은 메시지 M에 대하여 자신의 비밀키 θ_i를 가지고 다음을 계산한다.

$$S_1 = M^{\theta_i} \bmod n$$

step 3. 서명 메시지 (S_1, M)을 다음 공증자에게 전송한다.

Step 4. 공증자의 순서에 따라 마지막 공증자 n의 서명을 수행한다. 이때 앞 공증자의 서명 메시지를 점검할 수 있으며, 이 단계는 생략 가능하다.

step 5. 공증자 n은 앞 공증자의 서명 (S_{n-1})에 자신

의 서명을 서명한다.

$$S_n = S_{n-1}^{\theta_n} \bmod n$$

Step 6. 서명 메시지 (S_n, M)을 다음 공증자 $n+1$에 전송하며, 마지막 공증자는 서명 메시지를 요청자에게 전송한다.

3) 서명 검증 단계

Step 1. TC는 요청자의 공증 그룹에 대한 공개키 값을 형성하고 이를 요청자에게 전송한다.

$$\Theta_n = (\theta_1 \cdot \theta_2 \cdot \cdots \cdot \theta_n)$$

Step 2. 요청자는 공개키 값을 받아 서명의 검증을 실시하여 만족하는 확인한다.

$$U^{\theta_n} = \left(\prod_{i=1}^{k} H_i^{r_i} \right), \qquad M^{\left(\prod_{i=1}^{n} \theta_i \right) \cdot -\theta_n} \bmod n = M$$

3.4 제안 방식 고찰

기존의 특수 디지털 서명 방식들을 고려할 경우, 본 방식은 다음과 같은 특징을 보유하고 있다.

(1) 키 분배 시, 다양한 키 생성이 가능하므로 안전성 및 효율성에서 효과를 거둘 수 있다.

(2) 오직 지정된 공증자만이 서명을 확인할 수 있기 때문에 안전한 공증 서비스가 가능하다.

(5) 공증자의 신원 확인이 필요할 경우, 신뢰된 요소의 판단에 따라 신원을 검증할 수 있으므로, 익명성 제어가 가능하다

(6) 수신자 신원 확인 시 TC의 허가를 통해서 수행되므로, 공정성을 보장하고 있다.

이러한 특징들은 서명자의 익명성을 제공할 뿐만 아니라 수신자를 지정할 수 있음으로서, 안전성과 비밀성을 동시에 제공하고 있다. 또한 환경을 고려하여 TC의 허가를 통해 익명성 제어가 가능하므로 공정성을 확보하고 있다.

4. 결론

정보화 사회를 거치면서 많은 부분들이 전자화 되어 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. 특히 특수 디지털 서명 방식의 종류를 살펴보면서, 이들의 특성들을 간략히 고찰하였다.

본 논문에서는 기존의 공증인을 통한 서명에서 발생할 수 있는 문제점을 해결하면서 효율적인 공증 서명 방식을 제안하였다. 이를 통해 향후 더욱 안전하고 신뢰할 수 있는 네트워크 정보 교류에 일조하리라 판단된다. 또한 현재 제안된 많은 서명 방식들의 연구를 통해 더욱 효율적이고, 안전한 특수 디지털 서명 방식의 연구가 필요하리라 판단된다.

[참고문헌]

[1] S. J. kim, S. J. Park and D. H. Won, "Nominative Signature,"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, Germany, 1997, Lecture Notes in Computer Science, Springer-Verlag

[3] "Specification for a Digital Signature Standard," NIST, FIpS XX. Draft, August 1991[1].

[4] C. Schnorr, "Method for identifying subscribers and for generating and verifying electronic signatures in a data exchange system,"US patent #4,995,082, Feb. 1991.

[5] D. Chaum, "Undeniable Signature Systems," U.S. Patent #4,914,689, 3 Apr 1990.

[6] S. J. Park, K. H. Lee and D. H. Won, "An Entrusted Undeniable Signature," Proceedings of the 1995 Japan-Korea Workshop on Information Security and Cryptography, Inuyama, Japan, 24-27 Jan 1995, pp. 120-126.

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

[8] D. Chaum, "Blind Signature Systems," US. Patent #4,759,063, 19 Jul 1988.

[9] M. Mambo, K. Usuda, and E. Okamoto, "Proxy Signatures," Proceedings of the 1995Symposium on Cryptography and Information Security (SCIS 95), Inuyama, Japan, 24-27 Jan 1995, pp. B1.1.1-17.

[10] D. Chaum, "Group Signature," Advances in Cryptology -EUROCRYPT 91 Proceedings, Springer-Verlag, 1991, pp.257-265.

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

[12] 박희운, 이임영, "공정한 그룹 기반 수신자 지정 서명," 한국통신학회 하계종합학술발표회, Vol.23 No.2, 1861~1864, 2003