부인방지를 지원하는 공개키 · 관용키 알고리즘에 기반한 전자 서명 프로토콜

김선희, 이헌길*
강원대학교 전자공학과, *컴퓨터 · 정보통신공학부

A Digital Signature Protocol Supporting Non-repudiation Based on Public-Private Algorithms

Sun Hee Kim, Heon Guil Lee*
Dept. of Electronic Eng., *Div. of Computer, Information and Communications Eng.
Kangwon National University

요 약

기존 전자서명방식의 검증의 남용 문제를 해결하기 위한 방법으로 부인방지 서명방식이 제안되었다. 그러나, 기존의 부인방지 서명방식은 기밀성이 제공되지 않고, 송 · 수신자에게 많은 비밀 정보를 요구하며, 그 정보들을 자주 변경하여야 한다. 또한, 문제 발생 시에 부인 프로토콜을 따로 수행함으로써 많은 작업 시간을 요구한다. 송 · 수신자 사이에 서버를 두는 방법도 제안되었지만 클라이언트 수가 많은 경우 서버는 많은 오버헤드를 가지게 되어 효율적이지 못하다. 본 논문에서는 부인 방지를 위해 송 · 수신자 사이의 Challenge-Response 방식에 기초하여 공개키 · 관용키 알고리즘을 사용한 새로운 프로토콜을 제시한다. 두개의 공개키를 사용하여 검증에 필요한 비밀 정보의 수를 줄였고, 영수증을 통해 부인 프로토콜의 필요성을 없앴을 뿐 아니라, 송 · 수신 부인 방지가 모두 가능하게 하였다. 또한, 관용키 알고리즘으로 원본 메시지를 암호화하여 기밀성을 제공한다.

1. 서론

컴퓨터의 보급과 인터넷 사용이 급증하면서 일반 문서 대신 전자적으로 업무를 처리하는 일이 많아졌다. 전자문서를 이용하면 문서의 작성, 전송, 관리가 효율적이지만 복사와 위조가 쉬워 원본을 구별하기 어렵다[5]. 이를 보완하기 위해 문서의 내용과 출처를 증명해 주는 수단이 필요하게 되었고, 이것이 전자서명이다.

메시지 인증과 사용자 인증 기능을 가진 전자서명은 Diffie와 Hellman이 처음 논의[1]한 이래 많은 전자서명방식들이 개발되었지만 종이 문서의 도장이나 서명을 대신하기에는 부족하다. 공개키 알고리즘[3]만을 사용한 전자서명방식은 검증 정보를 공개함으로써 필요 이상의 과다한 검증 기회를 제공하여, 개인적으로나 상업적으로 중요한 정보에 치명적이다. 또한, 전자서명은 부인 방지 기능이 필요한데, 일반적인 전자서명은 서명의 전송을 통한 송신 부인 방지만을 제공할 뿐 수신 부인 방지는 이루어지지 않는다. 이러한 전자서명의 취약점을 보완하기 위해 제안된 특수 서명 방식 중 하나가 부인방지 서명방식이다.

이 연구는 정보통신부 정보통신분야 우수대학원 지원사업 과제로 수행된 것임

1989년 Chaum과 Van Antwerpen에 의해 처음 소개된 부인방지 서명방식[2]은 서명자의 도움 없이는 서명의 검증이 불가능하기 때문에 사적인 정보의 유출을 방지한다. 또한, 기존의 전자서명방식이 검증 프로토콜에 의해 단지 서명의 정당성만 확인하는데 반해 부인방지 서명방식은 검증 및 부인 프로토콜로 구성되어, 검증 프로토콜을 통해 자신이 발행한 서명의 정당함을 증명하며, 부인 프로토콜로 인해 자신의 서명을 부인할 수 없고, 자신의 서명이 아님을 확인 시켜줄 수 있다.

그러나, Chaum의 부인방지 서명방식은 송 · 수신자 사이에 Challenge-Response 방식에 기초하여 하나의 공개키와 두개의 랜덤 비밀키를 통해 서명을 확인하므로 검증에 많은 정보와 시간이 필요하다. 그리고, 이 정보들은 랜덤 값이므로 새로운 연결을 시도할 때마다 매번 변경되어야 한다. 이것은 문서 교환이 빈번히 이루어지는 송 · 수신자 관계라면 상당히 비효율적이다. 또한, Chaum의 부인방지 서명방식은 검증 프로토콜과

부인 프로토콜을 따로 수행하기 때문에 두 프로토콜 사이의 비밀 정보 공유는 이루어지지 않는다. 이로 인해 문제가 발생했을 때, 부인 프로토콜을 위한 별도의 비밀 정보와 프로토콜을 수행하기 위한 시간이 필요하다. 이를 해결하기 위한 방법으로 송·수신자 사이에 신뢰할 수 있는 서버를 두어 분쟁이 일어났을 경우 서버가 이를 해결해주는 방식이 제안되었다[6, 7]. 하지만, 이 방식은 서버를 유지하는 경비가 필요할 뿐 아니라 서비스를 요청하는 클라이언트의 수가 많은 경우에 서버의 병목 현상에 의해 전체 시스템의 성능이 저하될 수 있다.

본 논문에서는 서버를 사용하는 대신 송·수신자 사이의 Challenge-Response 방식에 기초하고, 공개키·관용키 알고리즘을 사용한 새로운 부인방지 서명방식을 제안한다. 두 개의 공개키를 사용하여 통신이 빈번히 이루어지는 송·수신자 사이에 비밀 정보를 만드는 횟수를 줄이고, 부인 프로토콜 대신 영수증을 사용하여 문제가 발생했을 때 수행해야 하는 송·수신자의 작업량을 줄인다. 그리고, 송·수신자 사이에 합의가 이루어지기 전에 메시지가 노출되는 위험을 피하기 위해 원본 메시지를 관용키 알고리즘으로 암호화하여 메시지의 기밀성을 유지한다.

이 논문의 2장에서는 새롭게 제안한 모델에 관해 설명하고 3장에서는 성능분석 및 평가 그리고 4장에서 결론을 맺는다.

2. 제안한 모델

정당한 사용자 A와 B는 공개키 알고리즘을 사용한다. A와 B의 인증된 공개키 A_{Pu}(A의 공개키), B_{Pu}(B의 공개키)는 공개 디렉토리에 저장되어 있고, A와 B는 각각 자신의 비밀키 A_{Pr}(A의 비밀키), B_{Pr}(B의 비밀키)을 저장한다. 송신자 A가 수신자 B에게 메시지 M을 전송하려 할 때, 본 논문에서 제시하는 프로토콜의 프레임워크는 그림 1에 나타나 있으며, 프로토콜의 각 단계에 대한 자세한 설명은 다음과 같다.

단계 1. 서명의 생성과 전송 (송신자)

- 송신자는 관용키로 사용하기 위해 랜덤 키 A_K를 선택한다.
- 관용키 알고리즘을 사용하여 원본 메시지 M을 A_K로 암호화하여 C를 얻는다. $C = E[M]A_K$
- C를 해싱하여 N을 만든다. $N = H[C]$

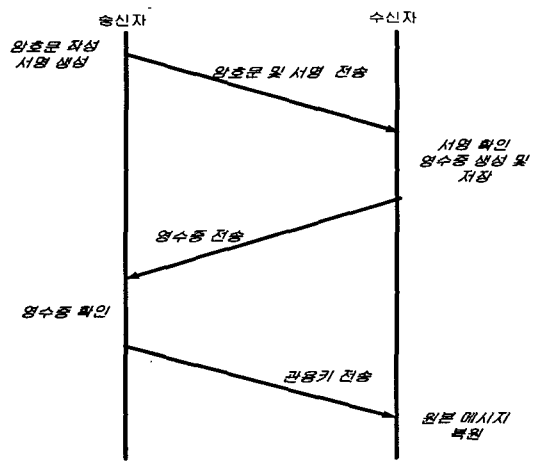

그림 1. 프로토콜 프레임워크

- N을 송신자의 비밀키로 암호화하여 서명 S를 생성한다. $S = E[N]A_{Pr}$
- C와 S를 함께 수신자에게 전송한다.

$$M_A = [\ S\ |\ C\ ]$$

단계 2. 서명 확인 및 송신 영수증 저장 (수신자)

- 수신자는 송신자로부터 받은 M_A'를 S'와 C'로 나눈다. $M_A' = [\ S'\ |\ C'\ ]$
- 서명 S'를 송신자의 공개키로 복호화하여 N'를 구한다. $N' = D[S']A_{Pu}$
- C'를 해싱한다. $H[C']$
- N'와 $H[C']$를 비교한다. 같지 않으면 정당한 사용자가 아니거나 정당한 메시지가 아닌 것으로 생각하고 연결을 끊는다.
- 만약 같다면 정당한 사용자가 보낸 정당한 메시지로 인정하고, 문제 발생 시를 대비하여 이를 영수증으로 보관한다.
- 송신자로부터 받은 N'를 자신의 비밀키로 암호화한 수신 영수증을 송신자에게 전송한다.

$$Receipt = E[N']B_{Pr}$$

단계 3. 영수증 수신 및 메시지 인증 (송신자)

- 송신자는 수신자로부터 받은 영수증 $Receipt$를 수신자의 공개키로 복호화하여 N''를 구한다.

$$N'' = D[Receipt]B_{Pu}$$

- N''과 자신이 처음에 보냈던 N을 비교한다. 같지 않다면 정당한 수신자가 아니거나 메시지가

바뀌었다고 여기고 연결을 끊는다.

- 만약 같다면 정당한 수신자임과 바뀌지 않는 메시지임을 확인하고, 문제 발생 시를 대비하여 이를 영수증으로 보관한다.
- 원본 메시지 복원을 위한 랜덤키 A_K를 수신자의 공개키로 암호화하여 전송한다.

$$Key = E[A_K]B_{Pu}$$

단계 4. 원본 메시지 복원 (수신자)

- 수신자는 송신자로부터 받은 Key를 자신의 비밀키로 복호화하여 랜덤키를 얻는다.

$$A_K = D[Key]B_{Pr}$$

- C를 A_K로 복호화하여 원본 메시지 M을 복원한다. $M = D[C]A_K$

3. 성능분석 및 평가

성능 분석을 위해 각 방식에서 필요로 하는 비밀정보의 수와 송·수신자가 주고받아야 하는 메시지 수, 즉 통신 횟수, 그리고 각 방식에서 사용한 관용키·공개키·해싱 알고리즘의 수행 시간을 비교하였다.

	비밀정보 수	통신횟수	수행시간 (초)
Chaum 모델	200	380	0.86
서버 모델	100	540	0.40
제안된 모델	100	340	0.60

표 1. 전송 문서 100개일 때의 결과

표1은 송신자가 전송하는 메시지의 수가 100개일 때, Chaum 방식과 서버를 사용한 방식, 그리고 본 논문에서 제안한 방식을 비교 분석한 결과이다. 표1에서 볼 수 있듯이 본 논문에서 제안된 방식이 비밀 정보의 수와 통신 횟수가 가장 적다. 서버를 사용한 방식은 공개키 알고리즘의 수행 횟수가 적어 다른 두 방식보다 수행 시간이 적게 나타났으나, 다른 방식에 비해 통신 횟수가 많다. 따라서, 서명확인이나 중재를 요청하는 클라이언트의 수가 많은 경우 서버의 성능이 급격히 저하될 수 있다.

4. 결론 및 향후 과제

본 논문에서는 전자서명의 기본 요구 조건인 부인방지를 제공하기 위해 송·수신자가 대화 형식으로 정보를 교환하여 서명을 검증하는 모델을 제안했다. 이 모델에서는 검증을 위해 필요한 정보의 수를 줄이기 위해 두 개의 공개키를 사용했으며, 부인 프로토콜 대신 영수증을 사용하여 부인 프로토콜을 수행하는데 필요한 정보와 수행 시간을 줄였다. 또한, 관용키 알고리즘을 사용하여 원본 메시지를 암호화함으로써 송·수신자 사이에 합의가 이루어지기 전에 원본 메시지가 노출되는 위험을 피했다.

향후 과제로 서명자가 부재중이거나 서명자가 검증자의 요청을 거부하는 경우에도 서명의 검증이 가능한 방식에 대한 연구가 필요하다.

5. 참고 문헌

[1] W. Diffie and M.E. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, pp. 109-112, 1976.

[2] D. Chaum and H.V. Antwerpen, "Undeniable Signature," *Proc. of Advances in Cryptology CRYPTO'89*, pp. 212-216, 1989.

[3] RSA Laboratories, *PKCS#1: RSA Encryption Standard*, Technical Note, 1993.

[4] Rosario, "RSA-Based Undeniable Signature," *Proc. of CRYPTO'97*, 1997.

[5] 성균관대학교 정보공학과 정보통신보호연구실, *Cryptography*, http://dosan.skku.ac.kr/~sjkim.

[6] 최용환 외, "분산통신망 환경에서 부인방지 서비스를 제공하는 안전한 FTP 설계," 한국정보과학회 학술발표논문집(III), pp. 606-608, 1998.

[7] 장준교 외, "일회성 키를 이용한 전자우편 보안 프로토콜," 한국정보과학회 학술발표논문집 (III), pp. 506-508, 1998.

[8] 류재철, "인터넷 보안 기술," KRNET 특강자료집 T221, pp.163-182, 1999. 6.

[9] D. Chaum, "Designated Confirmer Signature," *Proc of Advanced in Cryptology EUROCRYPTO'94*, pp.189-205, 1994.

[10] J. Boyar, D. Chaum, and I. Damgtare, "Convertible Deniable Signature," *Proc. of CRYPTO'90*, pp.189-205, 1990.