제 19 회 한국정보처리학회 춘계학술발표대회 논문집 제 10 권 제 1 호 (2003. 5)

공개키 구조 환경에서 기존 디지털 서명 방식의 문제점 보완

송성근*, 윤희용*, 이형수**
*성균관대학교 정보통신 공학부
**전자 부품 연구원 정보시스템 연구센터
e-mail : *{songsk, youn}@ece.skku.ac.kr,
**{hslee}@keti.re.kr

Problem Supplement of Existing Digital Signature Method in Public Key Infrastructure Environment

Sung Keun Song*, Hee Yong Youn*
Lee Hyung Soo**
*School of Information and Communication Engineering, Sungkyunkwan University
** IT System Research Center, Korea Electronics Technology Institute

요 약

인터넷의 급격한 발달로 전자상거래가 우리 생활의 중요한 한 부분을 차지하게 되었다. 이런 전자상거래에서 중요한 한 요소인 기존 디지털 서명 방식에는 몇 가지 문제점을 가지고 있다. 그 중 하나가 악의적인 수신자나 제삼자의 디지털 서명의 재사용 문제점이며, 다른 하나가 서명자의 비밀키 분실 문제이다. 다른 문제점으로 수신자가 서명자의 키가 변경된 후 변경전의 디지털 서명의 검증을 시도하는 경우 검증이 불가능한 문제가 발생한다. 이러한 문제들을 해결할 수 있는 새로운 디지털 서명 방식 및 절차를 제안한다. 이 새로운 디지털 방식은 RSA 와 ElGamal 암호방식을 통합한 것으로 하나의 비밀키의 이에 대응되는 두 개의 공개키를 갖는 구조이다.

1. 서론

최근 인터넷의 급격한 발달은 우리 일상 생활에 많은 변화가 생기게 하는 원인이 되었다. 우리 일상 생활에 변화된 것들이 여러 가지가 있겠지만, 대표적으로 현실 세계에서 물건을 사고, 파는 경제 생활과 금융 관련 일들을 행하는 것을 대표적인 예로 들 수 있다. 예전에는 물건을 사기 위해 소비자가 직접 상점에 찾아가 했고, 금융 관련 일들을 보기 위해 은행을 방문해야만 했다. 그러던 경제 생활들이 인터넷의 발달로 상점이나 은행에 직접 방문할 필요 없이 가정에서나 인터넷에 연결된 컴퓨터가 있는 어디 곳에서든지 물건을 사고, 금융 관련 일들을 행할 수 있게 되었다. 이러한 것을 전자상거래라 하는데, 지금은 미비한 단계이지만 앞으로 급성장하여 실 경제 생활을 대체할 것으로 예상되고 있다.

전자상거래 시장이란 생산자(Producers), 중개인(Intermediaries), 소비자(Consumers)가 디지털 통신망을 이용하여 상호 거래하는 시장으로 실물시장(Physical market)과 대비되는 가상시장(Virtual market)을 의미한다. 전자상거래는 보안성을 기본 바탕으로 하고 있으며 거래인증, 거래보안, 대금결재, 소비자보호, 지적소유권보호 등을 수행하기 위해 암호화 알고리즘을 이용하며, 공개키 암호화 기법인 PKI(Public Key Infrastructure)를 기본 구조하고 있다. 전자상거래에서 중요한 요소 중에 하나가 디지털 서명이다. 이 디지털 서명은 전자상거래에서 거래가 안전하게 성립되기 위해 없어서는 안될 요소이다. 디지털 서명 종류에는 RSA 암호 방식을 이용한 디지털 서명[1], ElGamal 디지털 서명[2], 디지털 서명 표준(DSS : Digital Signature Standard)[3] 등 여러 가지가 있다. 그런데 이런 디지털 서명에는 몇 가지 문제점들이 있다. 그 중 하나가 디지털 서명의 수신자 또는 제삼자의 악용 문제이고, 다른

하나가 서명자의 비밀키 분실 문제이다. 다른 문제점으로 수신자가 서명자의 키가 변경된 후 변경전의 디지털 서명의 검증을 시도하는 경우 검증이 불가능한 문제가 발생한다[4]. 악용문제점을 해결하기 위해 일반적으로 타임스탬프(Timestamp)을 첨부하는데 이것 또한 문제점을 가지고 있다. 이 문제점은 타임스탬프가 노출되면 수신자나 제삼자가 유효기간 동안 서명자처럼 위장하여 서명문과 서명을 다른 제삼자에게 보낼 수 있다는 점이다. 본 논문에서는 이를 해결하기 위한 방안을 제시한다. 비밀키 분실 문제의 경우는 비밀키의 분실 사실을 서명자가 인지할 때까지 그 피해를 막지 못한다는 것이다. 이 문제 또한 본 논문에서 해결 방안을 모색해 본다. 검증 문제의 경우는 별도의 키 저장기관을 두어 해결하는 방식이 있지만 오버헤드가 크기 때문에 이 논문에서는 인증기관이 사용자의 키들을 기간별로 데이터 베이스(Data Base)화하는 방식을 제안한다.

본 논문의 구성은 다음과 같다. 2 장에서는 PKI 구조에서 기존의 디지털 서명 방식에 대해 알아보고, 3 장에서는 RSA와 ElGamal 디지털 서명 방식에 대해서 알아본 다음 이를 이용한 두 개의 공개키와 하나의 비밀키를 갖는 RSA와 ElGamal 디지털 서명 방식이 통합된 디지털 서명의 키 생성 방식을 제안한다. 4 장에서는 3 장에서 제안한 디지털 서명 방식을 구체화하여 위에서 제시한 디지털 서명의 문제점을 해결할 수 있는 방안을 제안한다. 마지막으로 5 장에서는 결론을 맺는다.

2. 디지털 서명

PKI의 구조는 여러 가지가 있는데 기본적인 구조가 그림 1과 같은 루트(Root) 인증기관(CA : Certificate Authority)를 필두로 한 트리 모양이다.

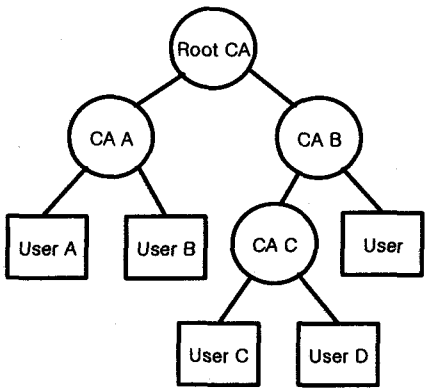

그림 1. PKI 구조

이런 PKI 구조에서 디지털 서명 방식에 대해 알아보면, 사용자 A가 사용자 B에게 디지털 서명문을 보내고자 하는 경우 사용자 A은 서명문 M을 해쉬 함수(H : Hash function)로 압축한 다음 자신의 비밀키로 암호화해서 디지털 서명을 만든 다음 서명문을 임의의 비밀키를 생성해서 암호화하고 그 비밀키를 사용자 B의 공개키로 암호화한 다음 타임스탬프를 첨부해서 사용자 B에게 전송한다. 사용자 B는 서명문을 수신한 경우 인증기관 A로부터 사용자 A의 공개키를 받아 디지털 서명을 복호화하고, 자신의 비밀키로 수신한 비밀키를 복호화하여 이를 이용해 서명문을 복호화한 다음 해쉬함수로 압축하여 디지털 서명을 복호화한 값과 일치하는지를 확인하므로 사용자 A의 서명이 맞는지를 검증한다. 그림 2는 위에서 설명한 디지털 서명 방식을 그림으로 나타내고 있다.

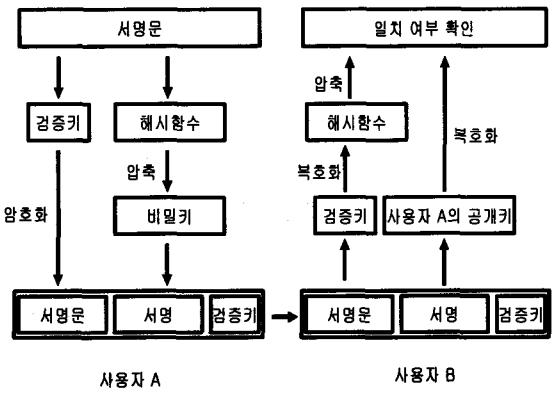

그림 2. 디지털 서명 방식

위에서 설명했듯 이 방식에는 몇 가지 문제점들을 가지고 있다. 그 중 하나가 디지털 서명의 수신자 또는 제삼자의 악용 문제이고, 다른 하나가 서명자의 비밀키 분실 문제이다. 그리고 또 다른 문제점이 서명자의 키가 변경된 후 변경전의 디지털 서명의 검증 문제이다. 이러한 문제점을 해결하기 위해 3 장에서 두 개의 공개키와 하나의 비밀키를 갖는 새로운 디지털 서명 방식을 제안하고 4장에서 구체화한다.

3. 암호화 알고리즘

3.1. RSA 디지털 서명

RSA 공개키 암호 방식은 정보 보호 기능과 디지털 서명기능을 동시에 수행할 수 있는 암호 방식으로 디지털 서명에 널리 이용되고 있다. RSA 디지털 서명은 다음과 같다. RSA 암호 방식과 같이 서명자 A는 충분히 큰 소수 p_A, q_A을 선택하여 $n_A = p_A q_A$을 계산하고 $\phi(n_A) = (p_A - 1)(q_A - 1)$과 서로 소인 K_{Ae}을 선택한다. 다시 유클리드 알고리즘을 이용하여 다음 식을 만족하는 K_{Ad}을 계산한다.

$$K_{Ae}K_{Ad} \equiv 1 \bmod \phi(n_A)$$

K_{Ae}와 n_A은 공개 목록에 등록하여 공개하고 K_{Ad}는 비밀리에 보관한다. 즉, K_{Ae}는 공개키가 되고 K_{Ad}는 비밀키가 된다.

서명 과정을 보면, 서명문 M을 해쉬 함수로 압축 $H = H(M)$ 하고 서명 $S \equiv H^{K_{Ad}} \bmod n_A$를 계산하여 서

명문 M과 함께 사용자 B에게 전송한다.

검증 과정을 보면, 사용자 B는 서명문 M의 해쉬 함수값 $H' = H(M)$ 을 계산하고 서명 S로부터 $H \equiv S^{K_{Ae}} \bmod n_A$ 를 계산한 다음 H와 H' 를 비교하여 서명문 M과 서명 S의 정당성을 검증한다.

3.2. ElGamal 디지털 서명

ElGamal 디지털 서명은 1985년 발표된 디지털 서명으로 그 안정성은 이산 대수 문제를 기반으로 하고 있다.

서명자는 큰 소수 a를 선택하여 집합 Z_a상에서 원시 원소 g를 찾는다. Z_a상의 임의의 원소 X_A을 비밀정보로 선택하여 $y_A \equiv g^{X_A} \bmod a$ 의 공개 정보 y_A을 계산한다. 이 때 y_A가 사용자 A의 공개키 K_e이고, X_A가 사용자 A의 비밀키 K_d가 된다.

서명 과정을 보면, 사용자 A는 $k \in_R Z_{a-1}$을 선정하여 중간값 $R \equiv g^k \bmod a$ 을 계산한다. 서명문 M의 서명 $S \equiv (M - X_A R)k^{-1} \bmod a\text{-}1$ 을 계산하여 사용자 B에게 R, M, S를 전송한다.

검증 과정을 보면, 사용자 B는 공개키 y_A로 다음 식의 성립 여부를 조사한다.

$$y_A^R R^S \equiv g^M \bmod a$$

3.3. 새로운 디지털 서명의 키 생성

위에서 알아본 RSA와 ElGamal 디지털 서명 방식을 혼합하여 두 개의 공개키와 한 개의 비밀키를 갖는 새로운 디지털 서명 방식을 만들 수 있다. 먼저 RSA 암호 방식에서 p와 q를 선택하여 n을 계산한 다음 ElGamal의 큰 소수 a를 n과 비슷한 값의 소수로 선택한다. 다음 Euler 함수 값 $\phi(n) = (p-1)(q-1)$ 과 서로소인 K_e을 선택하고, 다시 유클리드 알고리즘을 이용하여 다음 식을 만족하는 K_d을 계산한다.

$$K_e K_d \equiv 1 \bmod \phi(n)$$

그 후, ElGamal에서 Z_a상의 임의의 원소 X_A을 K_d로 하여 $y_A \equiv g^{K_d} \bmod a$ 의 공개 정보 y_A을 계산한다. 이 때 K_d가 가입자의 하나의 비밀키가 되고 K_e가 하나의 공개 암호화 키인 K_{e1}, y_A가 다른 하나의 공개 암호화 키인 K_{e2}가 된다.

4. 새로운 디지털 서명 방식

3 장에서 제안한 새로운 디지털 서명의 키 생성 방식을 이용한 새로운 디지털 서명 방식은 다음과 같다. 우선 표기법을 살펴 보면 다음과 같다.

- K_d : 사용자 비밀키. 사용자만 비밀리에 보관
- K_{e1} : 사용자 공개키. 인증기관에 비밀리에 보관됨. 일반에 공개되지 않음
- K_{e2} : K_{e1}와 또 다른 공개 암호화 키. 인증기관에 보관되며 일반에 공개됨.
- K_v : 서명문을 암호화하는데 사용되는 비밀키. 대칭 형 암호방식 사용.
- n, a, g: 공개 정보. 인증기관에 보관됨.
- A_{RSA} : RSA 암호화 알고리즘
- $A_{ElGamal}$: ElGamal 암호화 알고리즘

새로운 디지털 서명 방식에서는 PKI 구조의 변화는 없다. 사용자 A가 사용자 B에게 디지털 서명문을 보내고자 하는 경우 사용자 A은 서명문을 해쉬함수로 압축한 다음 여기에 타임스탬프와 유효기간을 첨부하여 자신의 비밀키인 K_{Ad}로 K_{Ae1}와 일치하는 알고리즘 A_{RSA}으로 암호화해서 디지털 서명을 만든다. 그림 3은 디지털 서명의 구조를 나타내고 있다.

그림 3. 디지털 서명의 구조

그리고 서명문을 임의의 비밀키 K_v을 생성하여 암호화한다. 이 비밀키는 사용자 A의 비밀키로 암호화하고 인증기관으로부터 사용자 B의 공개키 K_{Be2}을 받아 다시 암호화한 다음 사용자 B에게 M, S와 함께 전송한다.

사용자 B는 서명문을 수신한 경우 인증기관으로부터 사용자 A의 공개키를 받아 자신의 비밀키와 함께 수신된 비밀키 K_v을 복호화해서 서명문을 복호화 한다. 이 때 사용자 A가 자신의 비밀키로 K_v을 암호화를 했기 때문에 복호화된 K_v로 서명문이 이상 없이 복호화 되면 사용자 A로부터 송신된 서명문이라는 것을 확인할 수 있다. 그림 4는 위의 과정을 나타내고 있다.

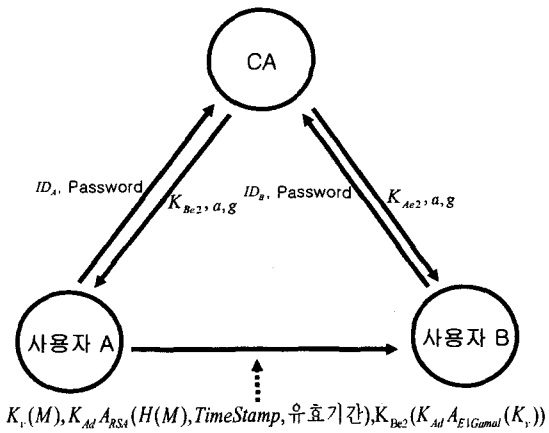

그림 4. 새로운 디지털 서명 방식

서명문 무결성(Integrity) 및 디지털 서명 검증 방법은 다음과 같다. 사용자 B는 서명문의 해쉬 함수값과 사용자 A의 디지털 서명을 인증기관에게 전송한다. 그러면 인증기관은 사용자 A의 공개키인 K_{Ae1}으로 디지털 서명을 복호화하여 해쉬 함수값과 비교하여 그 결과를 사용자 B에게 전달한다. 그림 5는 디지털 서명 검증 방법을 나타내고 있다.

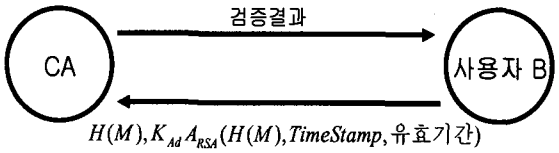

그림 5. 디지털 서명 검증 방법

지금까지 새로운 디지털 방식에 대해 알아 보았다. 이 디지털 서명 방식은 서론에서 제기한 문제들을 해결할 수 있다. 사용자 A는 디지털 서명을 K_{Ad} 을 이용하여 RSA 암호화 방식으로 암호화하기 때문에 사용자 B는 사용자 A의 공개키인 K_{Ae2}로 디지털 서명의 타임스탬프와 유효기간을 볼 수 없을 뿐만 아니라 서명문에 대한 사용자 A의 디지털 서명이 맞는지를 확인할 수 없다. 다만 사용자의 공개키인 K_{Ae2} 을 이용하여 서명문 M이 사용자 A에게서 전송된 사실만 알 수 있을 뿐이다. 디지털 서명의 검증은 오직 인증기관에서만 할 수 있다. 따라서 사용자 B의 디지털 서명의 재사용을 차단할 수 있으며, 또한 디지털 서명에 대해 검증을 제삼자인 인증기관이 수행하므로서 사용자간의 분쟁을 차단할 수 있다.

사용자 A의 비밀키 분실 문제의 경우는 디지털 서명 과정에서 필요한 사용자 B의 공개키를 인증기관으로부터 받을 때, 추가 정보 ID 및 패스워드를 기입하게 하므로서 제삼자가 사용자 A의 비밀키는 알아도 인증기관에 가입된 ID 및 패스워드를 모르면 디지털 서명을 할 수 없게 하므로서 비밀키 분실에 대한 피해를 최소화 할 수 있다.

각 비밀키 및 공개키의 안전성을 고려해 일정기간마다 키를 변경한다. 만일 키가 변경된 후 변경되기 이전의 디지털 서명을 인증기관에 검증을 요구하면 검증이 불가능한 문제가 발생한다. 이러한 문제점을 해결하기 위해 인증기관이 각 사용자의 공개키를 데이터 베이스화하여 보관하므로서 이러한 문제점을 해결할 수 있다.

5. 결론

지금까지 새로운 디지털 방식에 대해서 알아 보았다. 이 논문에서 RSA와 ElGamal 방식의 결합 예만 들었는데, RSA와 DSS와도 결합해서 같은 방식의 디지털 방식을 만들 수 있다. 이 논문에서 제안한 새로운 디지털 방식은 기존의 몇 가지 문제점을 해결할 수 있다. 그러나 몇 가지 미비점을 가질 수 있다. 좀더 연구를 해서 미비점을 찾아내어 보완 발전 시킬 것이며, 많은 응용 분야에 적용해 볼 예정이다.

참고문헌

[1] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems", Communications of the ACM, 21(2):120-126, February 1978.

[2] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms", IEEE Trans. Info. Theory, IT 31, 1985.

[3] Digital Signature Standard (DSS). FIPS PUB 186, 1994.

[4] Petros Maniatis and Mary Baker, "Enabling the Archival Storage of Signed Documents", In Conference on File and Storage Technologies, Monterey, California, USA, 28-29 January 2002.