실용적인 부인방지 전자 서명 기법

곽 남영*, 박 성준**, 류 재철***
* 한국통신 통신망연구소 TMN팀
** 성균관대학교 정보공학과
*** 충남대학교 자연과학대학 컴퓨터과학과

A Practical Undeniable Digital Signature Scheme

Nam-young Kwak*, Sung-Jun Park**, Jea-cheol Ryou***
* TMN Team, Telecommunication Network Research Lab.,
Korea Telecom.
** Department of Information Engineering, Sung Kyun Kwan University
*** Department of Computer Science, College of Natural Sciences
Chungnam National University

ABSTRACT

We propose an undeniable digital signature scheme which is practical since it has less computation and communication overhead than Chaum's one. We expect that this protocol be useful to develop secure systems such as electronic contract system, electronic mail system and electronic cash system.

1. 서론

지금까지 개발된 암호 시스템의 기능은 크게 보호 기능과 인증 기능으로 나눌 수 있다. 보호 기능은 정보가 노출된다 하여도 키를 알 지 못하는 한 정보의 의미를 파악하지 못하게 하여 정보를 보호하는 것이고, 인증 기능은 정보의 전달 상태 또는 통신시 송·수신자간의 상대방 확인 기능을 갖춰 분쟁을 해결할 수 있는 요인을 제공하는 것이다. 인증 기능은 메시지 내용의 변경 유무 및 전달 유무를 확인하는 메시지 인증 기능과 정보의 생성·보관·처리 등의 행위에 관여한 사용자가 맞는가를 확인하는 사용자 인증 기능으로 구분할 수 있다.

이러한 사용자 인증 기능과 메시지 인증 기능은 일상 생활에서 우리가 사용하는 서명이나 인감과 같은 효과를 전자적으로 수행하는 전자 서명을 구현하는데 이용될 수 있다. 일반적으로 서명이나 인감은 개인의 필요성에 의하여 언제든지 발급될 수 있고, 이를 수신한 사람 역시 서명이나 인감의 정당성을 쉽게 확인할 수 있으며 서명의 생성자나 인감의 소유자 이외에는 이 서명이나 인감을 발급할 수 없어야 한다. 따라서 전자 서명은 서명자만이 서명을 생성할 수 있는 유일성, 위조가 불가능한 위조 불가능성, 서명의 진위를 쉽게 확인할 수 있는 진위 확인의 용이성, 자신의 서명을 위조된 것이라고 거부하는 것이 불가능한 거부의 불가능성 등의 요구 사항을 만족하여야 한다.

대부분의 전자 서명은 관용 암호 시스템(Conventional Cryptosystem)에 비해 여러가지 장점을 지닌 공개키 암호 시스템(Public-key Cryptosystem)에 의해 많이 구현되어 적용하는 분야에 따라 여러가지 형태로 변형되어 사용될 수 있다.

예를 들어 정부 기관에서 고시하는 공문서나 공공기관에서 발행하는 각종 증명서, 공개키의 진위 여부를 공증해 주는 공개키 증명서(Public-key Certificate)등과 같은 일반적인 응용에서는 누구나 이를 확인할 수 있도록 하는 것은 필수적이므로 전자 서명이 매우 유용하게 사용될 수 있다.

그러나, 공개키 암호 시스템(Public-key Cryptosystem)을 이용한 전자 서명 방식은 공개키가 모든 사용자에게 공개되기 때문에 통신망에 가입한 사람은 누구든지 메시지의 진위 여부를 확인할 수 있게 되어 필요 이상의 과다한 인증 기회를 제공하게 된다. 이러한 요소는 개인적으로나 상업적으로 민감한 응용 분야에서 임의의 침입자가 전자 서명의 사본을 입수한 경우 이를 확인할 수 있게 되어 서명의 사본이 악용될 수 있는 소지를 제공하게 되며 이로 인해 개인의 이익 또는 사생활이 노출될 가능성이 있게 된다. 또한, 후에 이로 인한 분쟁의 발생시 이를 해결하기 어려운 단점이 존재하게 된다. 따라서 서명의 사본만으로는 서명의 정당성을 확인할 수 없고, 서명의 인증을 위해서는 반드시 서명자의 도움을 받아야 하거나 특정 수신자만이 서명을 확인할 수 있게 하는 방법등에 의해 서명자나 수신자에 대한 부당한 위협 가능성을 줄여 주고 개인의 사생활을 보호할 수 있는 서명 방식이 보다 바람직한 경우가 존재한다.

D. Chaum의 부인방지 전자 서명 기법(Undeniable Digital Signature Scheme)[4,5]은 이러한 목적에 의해 제안되었다. 제안된 부인방지 전자 서명 방식은 자신이 발행한 전자 서명이 정당함을 보이는 확인 프로토콜(Confirmation Protocol)과 자신이 발행한 서명을 후에 부인할 수 없도록 하는 부인 프로토콜(Disavowal Protocol)로 구성되어 앞에서 언급한 단점을 없앨 수 있어 많은 응용 분야에 적용될 수 있으나, 응용 분야에 따라서는 서명자의 익명성을 보장하지 못하는 된다.

국내에서의 부인방지 전자 서명에 대한 연구는 임채훈등에 의하여 연구된 수신자 지정 서명 방식[6]과 박성준등에 의해 연구된 의뢰 부인방지 전자 서명 방식[7]이 있다. 수신자 지정 서명 방식은 지정된 수신자만이 서명을 인증할 수 있고, 필요시 제3자에게 그 서명이 자신에게 발행된 유효한 서명임을 증명할 수 있게 하여 수신자에게 발행된 서명의 남용을 통제할 수 있는 서명기법을, 의뢰 부인방지 서명기법은 부인방지 서명기법의 단점인 익명성의 보장을 위한 서명기법을 각각 제안하였다.

이러한 전자 서명의 기능에 관한 사항과 함께 고려되어야 할 요인으로 이러한 프로토콜들이 수행될 때의 계산량과 통신정보량이 있다. 앞에서 언급한 서명 프로토콜들은 정보통신량과 계산량이 많은 상호 동작성을 기본으로 구성하기 때문에 통신망을 통한 전자서명 기법의 실용화에 큰 부담이 된다. 따라서, 본 논문에서는 Chaum에 의해 제안된 부인방지 전자 서명 방식중 프로토콜 동작시 많은 계산량과 통신량을 요구하는 부인 프로토콜을 실용적으로 개선한 프로토콜을 제안하며, 제안된 프로토콜들과 Chaum의 부인 프로토콜들을 비교하여 통신 정보량과 계산량이 감소됨을 보이고 프로토콜의 변경에 따른 변화 성질에 대해 알아 본다.

2장에서는 부인방지 전자 서명 기법들에 대해 알아보고, 3장에서 개선한 부인 프로토콜을 제안하여 이를 기존의 부인 프로토콜과 비교 분석하고, 4장은 결론으로 구성된다

2. Chaum의 부인방지 전자 서명 기법

기존에 제안된 전자 서명 방식들은 검증 프로토콜에서 단지 서명의 정당성 여부만을 확인하는데 비해 1989년 Chaum에 의해 제안된 부인방지 전자 서명 기법은 검증 프로토콜이 확인 프로토콜(Confirmation Protocol)과 부인 프로토콜(Disavowal Protocol)로 구성되어 있다.

확인 프로토콜은 일반적인 검증 프로토콜과 마찬가지로 서명의 정당성 여부를 판단하는 프로토콜로써 이 프로토콜에 의한 검증이 성공하면 아주 높은 확률로 서명이 정당함을 인정하게 된다.

부인 프로토콜은 확인 프로토콜에서 서명의 정당성 확인이 실패했을때 확인하려한 서명이 불법적인 침입자에 의해 만들어진 부당한 서명이었는지 아니면 정당한 서명에 대하여 서명자가 서명을 부인하려는 의도에서 적절치 않은 응답을 하였는지를 구분하기 위한 프로토콜이다.

서명의 검증자는 서명자의 계산 능력이 무한히 큰 경우라고 하여도, 확인/부인 프로토콜을 수행하여 서명의 정당성 여부 및 위의 두 가지 경우 중 어느 경우에 해당하는지를 판단할 수 있게 된다.

신뢰 센터는 소수 $p = 2^n - 1$인 유한체 $GF(2^n)$와 α의 위수가 q인 유한체 상에서의 원시근 α를 사용자들에게 공개한다. 사용자는 임의의 난수 $x \in \{ 1, 2, \cdots\cdots, p-1 \}$를 선택하여 자신의 비밀키로 하고, $v(\equiv \alpha^x \pmod p)$를 계산하여 자신의 공개키로 사용한다. 서명자가 임의의 메시지 m에 대하여 자신의 비밀키를 사용하여 만든 전자 서명의 형태를 $Z(\equiv m^x \pmod p)$라 할 때, 다음의 프로토콜을 이행하여 서명 Z의 정당성 및 부인 여부를 알아낼 수 있다.

[확인 프로토콜 (그림 2-1)]

① 검증자는 임의의 두 난수 $a, b \in \{ 1, 2, \cdots\cdots, p-1 \}$를 선택하고 V를 계산하여 증명자에게 전송한다.

$$V \equiv m^a \alpha^b \pmod p$$

② 증명자는 임의의 난수 $t \in \{ 1, 2, \cdots\cdots, p-1 \}$를 선택하여 P_1과 P_2를 계산하여 검증자에게 전송한다.

$$P_1 \equiv V \alpha^t \pmod p$$
$$P_2 \equiv P_1^X \pmod p$$

③ 검증자는 자신이 과정 ①에서 선택한 a, b를 증명자에게 전송한다. 증명자는 a, b를 이용하여 V의 정당성을 확인하고 정당하면 t를 검증자에게 전송하고, 정당하지 않으면 증명자는 검증자의 응답이 부당하다고 판단하여 프로토콜을 종료한다.

④ 검증자는 t를 이용하여 과정 ②에서 받은 P_1, P_2의 정당성을 다음과 같이 확인한다.

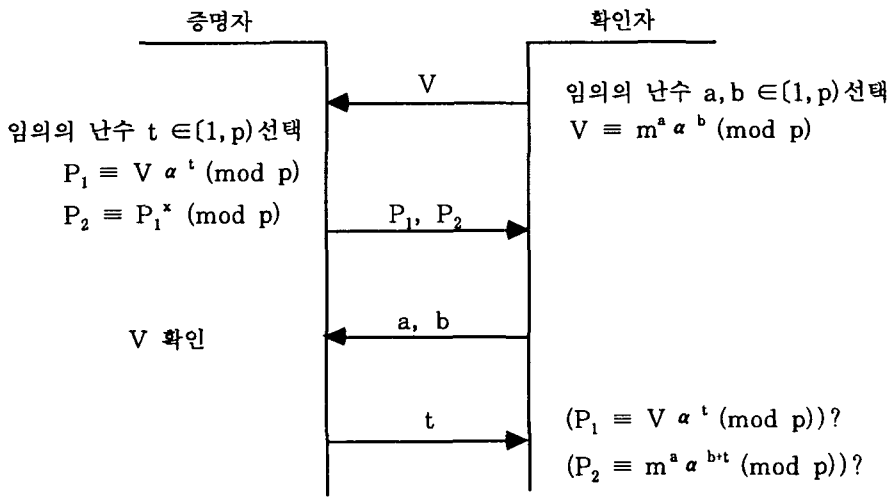
i) t의 정당성 확인

$$\left(P_1 \overset{?}{\equiv} V \alpha^t \pmod p \right)$$

ii) 서명의 정당성 확인

$$\left(P_2 \overset{?}{\equiv} Z^a v^{b+t} \pmod p \right)$$

확인 프로토콜의 과정 ④-i)을 만족하지 않으면 검증자의 응답이 적절하지 않다고 판단하여 프로토콜을 종료하고, 과정 ④-i), ii)를 만족하면 제기된 서명은 정당한 서명으로 받아 들여지게 된다. 만약 과정 ④-ii)를 만족하지 않으면 검증자가 서명을 부인하려는 의도에서 적절치 않은 응답을 하였는지, 제기된 서명이 부당한 서명인지를 판단하기 위한 부인 프로토콜을 수행한다.



<그림 2-1> Chaum의 확인 프로토콜

[부인 프로토콜 (그림2-2)]

① 검증자는 임의의 난수 a ∈ { 1, 2, ····· , p-1 }와 검증수 w ∈ { 0, 1, 2, ····· , k-1 }를 선택하여 V_1, V_2를 계산하여 증명자에게 전송한다.

$$V_1 \equiv m^w \alpha^a \ (\mod p)$$

$$V_2 \equiv Z^w v^a \ (\mod p)$$

② 증명자는 V_1을 x승하면 V_2와 같아지는 성질을 이용하여 trial and error로 w를 결정하고(만일 w를 찾을 수 없다면 임의의 수를 선택), 임의의 난수 t ∈ { 1, 2, ····· , p-1 }를 선택하여 다음을 계산하여 검증자에게 전송한다.

$$P \equiv \alpha^{wt} \ (\mod p)$$

③ 검증자는 자신이 과정 ①에서 선택한 a를 증명자에게 전송하고, 증명자는 a를 이용하여 V_1, V_2의 정당성을 확인하고 정당하면 t를 검증자에게 전송한다.

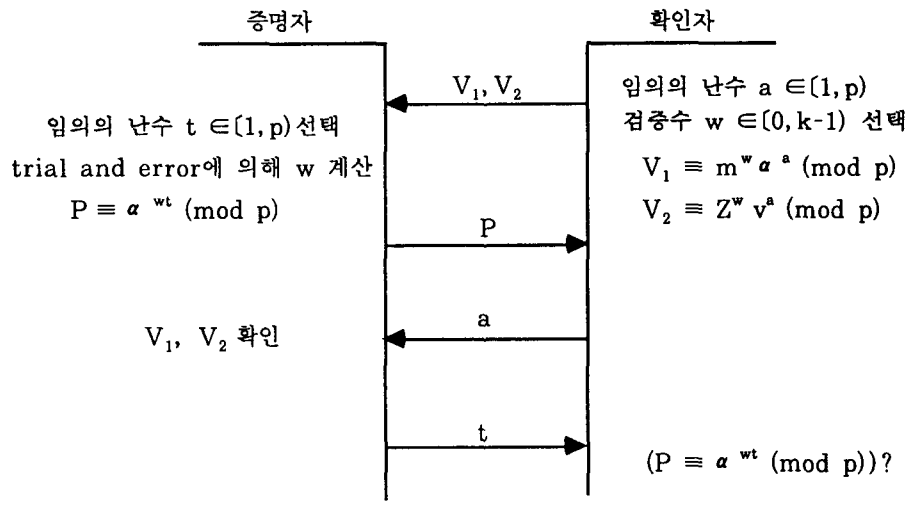
④ 검증자는 다음을 검사하여 제기된 원래의 서명 Z가 정당한지, 아니면 증명자가 거짓을 말하고 있는지 판단한다.

$$(P \stackrel{?}{\equiv} \alpha^{wt} \ (\mod p))$$

과정 ①에서 선택된 검증수 w는 증명자가 검증자를 속일 수 있는 확률을 결정하게 된다. 즉 증명자가 검증자를 속일 수 있는 확률은 k^{-1}이 되며 k의 값은 1024나 2048정도의 값을 사용한다. 제기된 서명 Z에 사용된 x'와 자신의 비밀키 x가 다르다면 과정 ①에서 사용된 검증수 w를 계산할 수 있으나 제기된 서명에 사용된 비밀키가 자신의 비밀키라면 아래의 식에 의하여 w의 값을 결정할 수 없게 된다.

$$((m^x/Z)^w \equiv 1 \ (\mod p))$$

과정 ④의 식이 성립하지 않으면 증명자가 검증자에게 거짓을 말하고 있는 것으로 판정한다. 즉 정당한 서명을 부인하는 것으로 결정한다.



<그림 2-2> Chaum의 부인 프로토콜

3. 제안한 부인방지 전자 서명 기법

3.1. 시스템의 구성

[시스템 초기화]

① 신뢰할 수 있는 센터는 다음의 조건을 만족하는 큰 소수 p, q, w를 선택한다.

- $qw \mid p-1$
- $q^2 \nmid p-1$
- $q,\ w \geq 2^k$
- $qw \geq 2^{512}$

② α의 위수가 q인 Z_p^*상의 원소 α를 선택한다.

$$\alpha^q \equiv 1 \pmod p,\ \alpha \neq 1$$

③ RSA방법에 의하여 센터의 비밀키 d와 공개키 e를 생성한다.

④ 일방향 해쉬 함수 h를 선택한다. h: $Z_p \times Z \in \{ 1, 2, \cdots\cdots, 2^t-1 \}$

⑤ p, α, h, e는 사용자들에게 공개하고 d, q, w를 비밀리에 안전하게 보관한다.

위의 과정에서 q, w의 크기를 결정하는 k의 값은 RSA방법에 의해 선택된 비밀키 d가 소인수 분해되지 않게 하기 위해 140이상의 크기를 요구하며 t는 사용된 해쉬 함수에 의해 그 값이 결정된다.

[사용자 등록 절차]

① 등록을 원하는 사용자는 임의의 난수 $x \in \{ 1, 2, \cdots, p-1\}$를 선택하여 자신의 비밀키로 하고, 자신의 공개 키 v를 계산하여 사용자의 개인정보와 함께 센터에 제출한다.

$$v \equiv \alpha^x \pmod p$$

② 센터는 사용자의 신원을 검사한 후, 사용자의 공개키 v의 정당성을 검사한다.

$$(v^q \equiv 1 \pmod p) \ ?$$

③ 센터는 사용자의 개인 정보를 이용하여 개인식별 정보 Id를 만들어서 v와 함께 다음의 R을 만들어서 Id와 R을 사용자에게 전송하여 사용자가 등록되었음을 알린다.

$$R \equiv (\alpha^x - Id)^d \pmod p$$

위의 사용자 등록 과정을 거쳐 자신의 비밀키 x를 사용하여 메시지 m에 대한 서명 $Z(= m^x)$가 만들어지게 된다. 서명의 생성자는 자신의 공개키 증명서 R과 개인식별 정보 Id, 서명 Z를 전송하게 된다.

전송된 전자 서명에 대한 검증 프로토콜은 2장에서 소개한 Chaum의 프로토콜과 마찬가지로 확인 프로토콜과 부인 프로토콜로 구성되며 확인 프로토콜은 Chaum의 확인 프로토콜을 그대로 사용하게 되며 부인 프로토콜은 다음과 같이 구성된다.

[부인 프로토콜 (그림 3-1)]

① 검증자는 임의의 난수 a, b, c, d $\in \{ 1, 2, \cdots, p-1 \}$를 선택하여(단, $ad \neq bc$) 증명자의 공개키 v를 사용하여 계산된 V_1, V_2를 증명자에게 전송한다.

$$V_1 \equiv Z^a v^b \pmod p$$
$$V_2 \equiv Z^c v^d \pmod p$$

② 증명자는 임의의 난수 t_1, $t_2 \in \{ 1, 2, \cdots, p-1 \}$를 독립적으로 선택하여 다음의 P_1, P_2, P_3, P_4를 계산하여 검증자에게 전송한다.

$$P_1 \equiv [V_1]^{x^{-1}t_1} \pmod p$$
$$P_2 \equiv [V_2]^{x^{-1}t_2} \pmod p$$
$$P_3 \equiv \alpha^{t_1} \pmod p$$
$$P_4 \equiv \alpha^{t_2} \pmod p$$

③ 검증자는 자신이 과정 ①에서 선택한 난수 a, b, c, d를 증명자에게 전송하고, 증명자는 a, b, c, d를 이용하여 V_1, V_2가 맞는지 틀리는지를 검증한다. 계산된 V_1, V_2의 값이 맞으면, 검증자에게 자신의 난수 t_1, t_2를 전송하고 그렇지 않으면 부인 프로토콜을 종료한다.

④ 증명자의 난수 t_1, t_2를 받은 검증자는 단계 ②에서 받은 P_3, P_4를 이용하여 t_1, t_2의 정당성을 확인한 후, P_1과 P_2를 사용하여 메시지 m에 대한 서명자 응답의 일관성을 검사하고 서명자의 부인 여부를 검사한다.

i) t_1, t_2의 정당성 확인

$$P_3 \overset{?}{\equiv} \alpha^{t_1} \pmod p$$

$$P_4 \overset{?}{\equiv} \alpha^{t_2} \pmod p$$

ii) 서명 Z에 대한 일관성 확인

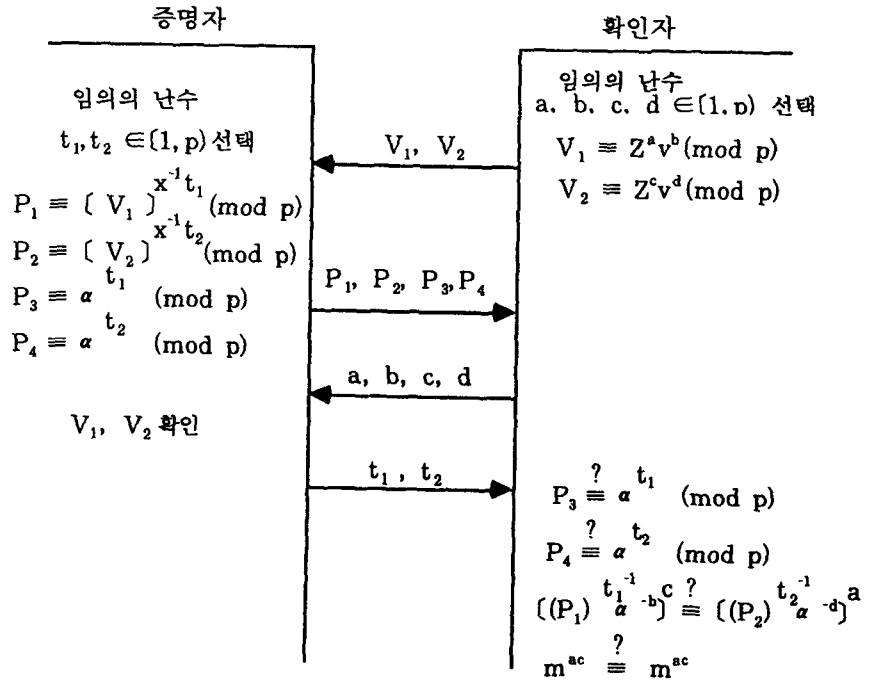
$$[(P_1)^{t_1^{-1}} \alpha^{(-b)}]^c \overset{?}{=} [(P_2)^{t_2^{-1}} \alpha^{(-d)}]^a$$

iii) 부인 여부 판단

$$m^{ac} \overset{?}{=} m^{ac}$$

과정 ①에서 V_1, V_2를 계산할 때 서명 Z와 공개키 v를 사용하는 이유는 다음과 같다. 공개키 v에 사용된 비밀키 x는 공개키의 생성자 이외에는 알 수 없으므로 비밀키 x의 역인 x^{-1}를 계산할 수 있는 사용자가 정확히 x^{-1}를 사용하여야 프로토콜을 통과할 수 있도록 하기 위해서 공개키 v를 사용하게 되며 서명 Z는 제기된 서명 Z에 대한 응답의 일관성을 보이기 위해서 사용하게 된다. 임의의 난수 a, b, c, d를 선택하여 각각의 지수승을 하는 이유는 부인 프로토콜에 응하는 서명자가 V_1, V_2를 알 수 없는 형태로 바꾸어 주기 위해서 사용하며 V_1과 V_2 두 개의 메시지를 만드는 이유는 이 두 메시지를 사용하여 응답의 일관성을 확인하기 위해서이다.

과정 ②에서 증명자는 확인자에게서 받은 V_1, V_2를 자신의 비밀키의 역수인 x^{-1}승 하고 이를 다시 임의의 난수 t_1, t_2승 하여 P_1과 P_2를 만들어 준다. 난수 t_1과 t_2로 각각을 지수 연산으로 수행하는 이유는 확인자가 보내온 메시지의 확인이 끝나고 자신이 확인자에게 t_1과 t_2를 전송하기 전까지는 확인자가 임의로 확인할 수 없도록 하기 위함이다. 이 때 사용된 t_1, t_2는 P_3와 P_4의 형태로 공증을 하여 주어 후에 t_1, t_2가 전송되었을 때, 확인자는 P_1과 P_2를 이용하여 정확한 t_1, t_2인지를 확인할 수 있게 된다.



<그림 3-1> 제안된 부인 프롤토콜

과정 ④-i)에서 이루어지는 확인 과정은 앞에서 언급한 바와 같이 증명자에게서 받은 t1, t2의 값이 맞는가 틀리는가를 검사하는 과정이다. 즉, 이미 받은 메시지 P_3, P_4와 자신이 전송받은 t_1, t2를 사용하여 계산한 값과 비교하여 확인한다.

④-ii)는 ④-i)에서 t_1, t_2의 확인이 이루어진 후 메시지 P_1과 P_2에 위의 식과 같은 연산을 행하여 주어 같게 되면 제기된 서명 Z에 대해 증명자의 응답이 일관된다고 판단하게 되고, 같지 않으면 증명자의 응답이 일관되지 않는다고 판단하여 증명자가 자신의 서명을 부인하려는 의도로 결정하게 된다.

④-iii)에서는 ④-ii)에서 응답 메시지의 일관성이 확인된 후 확인자가 원래의 메시지 m에 ac승을 하여 준 후 ④-ii)에서 계산된 값과 비교하여 같으면 증명자가 자신의 서명 Z를 부인하려 한 것으로 판단하게 되고, 다르면 제기된 서명 Z가 원래부터 증명자의 서명이 아닌 것으로 판단하게 된다.

3.2. 제안된 프로토콜의 성질

이 절에서는 본 논문에서 제안한 부인 프로토콜의 성질을 Chaum이 제안한 부인 프로토콜과 비교하여 알아 본다.

본 논문에서 제안한 부인 프로토콜은 x의 값을 { 1, 2, ····· , p-1 }상에서 선택하여 공개키 ($v \equiv a^x \pmod p$)를 계산하여 사용되어 공개키가 주어 졌을 때 x를 구하는 것이 이산대수 문제라는 사실에 기반을 두어 프로토콜의 안전성을 이산대수 문제에 근거하여 사용한다. Chaum의 부인 프로토콜 역시 이와 같은 이산대수 문제에 안전성의 근거를 두고 있다.

제안된 부인 프로토콜과 Chaum의 부인 프로토콜을 같은 수준의 안전도(약 2^{-256}정도)를 주었을 때의 특징은 다음과 같으며, 그 밖의 안전도에서도 유사한 결과를 얻을 수 있다.

Chaum의 프로토콜은 부인방지를 위한 난수 w를 선택하여 이를 trial and error 방식에 의하여 증명자가 w의 값을 계산하여 확인자에게 다시 보내주는 방법을 적용하고 있는데, 이 부인 프로토콜의 부인 가능성은 난수 w의 선택 범위에 의해 결정된다. 예를 들어, w가 { 0, 1, ... , k-1 } 사이에서 선택된다면 부인 프로토콜에서 속일 수 있는 확률은 k^{-1}가 된다. 그러므로 2^{-256}정도의 안전도를 유지하기 위해서는 k의 값이 2^{256}정도가 되어야 한다. 그러나 이렇게 큰 값으로 k 값을 정하면 부인 프로토콜 수행시 k값을 계산하기 위한 과정에서 증명자가 정당함에도 불구하고 정확한 k를 계산해 내지 못하게 되므로 프로토콜이 효율적으로 동작할 수 없게 된다. 때문에 k의 값은 1024나 2048정도의 작은 값을 사용하여 빠른 시간안에 정확한 응답을 할 수 있도록 정해 주게 되며, k의 값과 요구되는 안전도 수준에 따라 계산량과 통신 정보량이 유동적으로 변하게 된다.

예를 들어 k의 값을 1024라 가정하고 전체 부인 프로토콜에서 정당한 서명을 부인할 수 있는 가능성이 2^{-256}정도가 요구될 때, 프로토콜상에서의 요구되는 계산량과 통신 정보량을 살펴보면 다음과 같다.

Chaum의 부인 프로토콜을 한번 수행할 때 부인 가능성이 2^{-10}이므로 2^{-256}정도의 확률을 요구하게 되면, 프로토콜을 약 25번 정도 수행하여야 요구되는 수준의 부인방지 가능성을 만족하게 된다. 이 때의 계산량과 통신 정보량을 계산하면 다음과 같은 결과를 얻을 수 있게 된다. Chaum의 부인 프로토콜을 한 번 수행할 때의 계산량은 큰 수(2^{100}이상)를 지수승하는 연산이 7번이고 작은 수(2^{100}이하)를 지수승하는 연산이 약 516번 정도의 연산을 하여야 한다. 이를 25번 정도 반복 수행하여야 하므로 전체 연산량은 큰 수의 지수 연산수는 175번 수행하고 작은 수의 지수 연산은 12,900번 정도 수행하여야 한다. 통신 정보량은 프로토콜을 한 번 수행할 때 두 라운드(통신하는

A와 B가 서로 메시지를 한 번씩 주고 받은 상태)의 메시지 교환이 필요하므로 이를 25번 수행하면 50라운드의 메시지 교환이 필요하게 된다.

그러나, 제안된 부인 프로토콜은 임의의 검증수를 선택하지 않고 교환되는 메시지에 의한 일관성 확인이 이루어지게 되므로 부인 프로토콜을 단 한 번만 수행하면 된다. 이에 따라 요구되는 계산량과 통신 정보량은 다음과 같다. 제안된 프로토콜에서 요구되는 계산량은 큰 수의 지수 연산을 17번 요구하게 되며, 통신 정보량은 두 라운드의 메시지 교환만으로 가능하게 된다.

위의 예를 통해 알아 본 것과 같이, k의 값이나 요구되는 안전도 수준에 따라 약간의 차이는 있지만 제안된 프로토콜이 실제 응용에 있어 매우 효율적임을 알 수 있다. k 값과 요구되는 안전도 수준의 변화에 따른 Chuam의 부인 프로토콜과 제안된 부인 프로토콜의 통신 정보량과 계산량의 변화는 <표 3-1>, <표 3-2>와 같다.

그러나 Chaum의 부인 프로토콜은 정보의 교환시에 비밀 정도에 대한 어떠한 정보의 유출이 없이 그 타당성만을 보이는 영 지식성(Zero-knowledge)을 만족하는 프로토콜인데 비해, 제안된 프로토콜은 서명 Z에 대한 일관성 확인시에 메시지 m에 x^{-1}승한 값에 대한 정보를 일 부분 누출하게 되기 때문에 영 지식성을 만족하지는 못한다.

	안전도 수준	2^{-512}		2^{-256}		2^{-128}	
	k	2^{10}	2^{20}	2^{10}	2^{20}	2^{10}	2^{20}
Chaum의 부인 프로토콜		100라운드	50라운드	50라운드	24라운드	24라운드	12라운드
제안된 부인 프로코콜		2라운드	2라운드	2라운드	2라운드	2라운드	2라운드

<표 3-1> 제안된 부인 프로토콜과의 통신 정보량 비교

	안전도 수준	2^{-512}		2^{-256}		2^{-128}	
	k	2^{10}	2^{20}	2^{10}	2^{20}	2^{10}	2^{20}
Chaum의 부인 프로토콜	큰수의 지수 연산	350	175	175	84	84	42
	작은 수의 지수 연산	25,800	25,700	12,900	12,336	6,192	6,168
제안된 부인 프로토콜	큰수의 지수 연산	17	17	17	17	17	17
	작은 수의 지수 연산	0	0	0	0	0	0

<표 3-2> 제안된 부인 프로토콜과의 계산량 비교

4. 결론

본 논문에서는 Chaum에 의해 제안된 부인방지 전자 서명 프로토콜을 수행할 때, 서명의 부인방지를 위해 사용되는 부인 프로토콜이 많은 계산을 수행하여야 하고 많은 수의 메시지를 교환하는 단점을 없앤 매우 실제적인 부인 프로토콜을 제안하였다. 제안된 프로토콜은 이산대수 문제에 그 안전성의 근거를 두고 있으며 기존의 부인 프로토콜보다 계산량과 메시지의 교환량을 현저하게 줄여 실제 응용에 적합한 프로토콜임을 보였다. 그러나 제안된 프로토콜은 기존의 부인 프로토콜이 갖는 영 지식성을 만족하지는 않는다.

본 논문에서 제안된 프로토콜은 사용자의 익명성 보장, 재사용 검출, 현금의 분할 사용등의 요구 사항을 갖는 기존의 종이 화폐의 기능을 수행하는 전자 현금(Electronic Cash) 시스템, 전자 계약(Electronic Contract) 시스템, 전자 우편(Electronic Mail) 시스템 등을 개발하는데 이용될 수 있을 것이다.

향후에는 본 논문에서 제안된 부인 프로토콜을 영 지식성이 만족하면서 현재의 효율을 유지할 수 있는 프로토콜에 대한 연구 및 확인 프로토콜과 부인 프로토콜을 한 단계의 프로토콜로 처리할 수 있는 프로토콜에 대한 연구와 부인방지 서명 기법과 수신자 지정 서명 기법을 이용하여 부인방지 서명 기법에서의 서명자의 익명성을 보장하며 좀 더 단순하고 빠른 서명 기법에 대한 연구가 계속 이루어져야 할 것이다.

[참고 문헌]

[1] Y. Desmedt, M. Yung, "Weakness of Undeniable Signature Schemes", EURO-CRYPT '91, pp. 205-220, 1992.

[2] D. Chaum, "Security without Identification: Transaction Systems to Make Big Brother Obsolete", Communication of the ACM vol. 28 no. 10, pp.1030-1044, OCT. 1985.

[3] D. Chaum, "Some Weakness of : Weakness of Undeniable Signatures", EURO-CRYPT '91, pp. 554-556, 1992.

[4] D. Chaum, "Zero-Knowledge Undeniable Signature", Crypto '90, pp. 458-464, 1991.

[5] D. Chaum, H. V. Antwerpen, "Undeniable Signatures", EURO-CRYPT '89, pp. 212-216, 1990.

[6] 임채훈, 이필중, "상호 신분 인증 및 디지틀 서명 기법에 관한 연구", 통신정보보호학회논문집 제2권 제1호, 1992.

[7] 박성준, 이보영, 원동호, "의뢰 undeniable signature", 94년 하계종합학술발표논문집, pp.47-49, 1994.