論文 95-6-6-16

의뢰 부인방지 서명에 관한 연구

正會員 朴 性 俊*, 李 蒲 英**, 元 東 豪***

Entrusted Undeniable Signature

Sung Jun Park*, Bo Young Lee** and Dong Ho Won*** Regular Members

要 約

본 논문에서는 대화형 영지식 증명시스템을 사용하여 Okamoto, Ohta가 제기한 D. Chaum의 부인방지서명 방식에서 발생하는 거짓말 탐지기 기능 문제를 제3의 재판관 개념을 도입하여 해결하는 새로운 의뢰부인방지서명 방식을 제안한다.

제안한 새로운 의뢰부인방지서명 방식에서는 서명자의 서명문에 대한 부인 프로토콜을 영지식 대화형 증명시스템을 이용하여 제3의 재판관에게만 허용함으로서 거짓말 탐지기 기능 문제를 해결하였다.

ABSTRACT

In this paper, we will propose a new notion of entrusted undeniable signature which overcomes the problem of lie detector in undeniable signature.

The proposed entrusted undeniable signature is a new type of undeniable signature which the signer confirms his(her) signature to any verifier without the help of court but the verifier can't run the disavowal protocol in undeniable signature which only court can run to solve the disputation later. The proposed scheme will be constructed by the combination of undeniable signature and zero-knowledge interactive proof system.

*성균관대학교 정보공학과 박사과정
**한국전산원 연구원
***성균관대학교 정보공학과 교수
論文番號 : 95105-0315
接受日字 : 1995年 3月 15日

1. 서 론

컴퓨터의 급속한 보급과 전기통신기술의 발달로 컴퓨터 통신망이 확산되고 있으며,이에 따라 컴퓨터 통신망에서의 다양한 보안 서비스들에 대한 요구가 확대되고 있다. 그 중에서도 가장 시급하고 중요한 과제가 인증기술이다. 특히 메시지 및 사용자에 대한 인증을 동시에 해결할 수 있는 디지털 서명 기술은 각종 보안 서비스에서 필요 불가결한 도구로 사용되고 있다. 즉 메시지의 출처와 진위여부를 확인할 수 있는 자체 인증기능을 갖는 디지털 서명은 대부분의 응용분야에서는 매우 유용하게 이용된다.

그러나 개인적으로나 상업적으로 민감한 응용들에서는 이러한 자체인증은 필요 이상의 과다한 인증 기능을 제공함으로써 서명의 사본들이 악용될 수 있는 가능성을 높여주게 된다. 따라서 단순한 서명의 사본만으로는 이를 확인할 수 없고 서명의 확인을 위해서는 반드시 서명자의 도움을 받아야 하거나 특정 수신자만이 서명을 확인할 수 있게 하는 방법 등에 의해 서명자나 수신자의 부당한 위협 가능성을 줄여주고 프라이버시를 높여줄 수 있는 서명방식이 보다 바람직한 경우가 있다.[1,7]

이러한 특수한 서명방식 중 하나가 D.Chaum이 제안한 부인방지서명(undeniable signature) 방식이다. D. Chaum의 부인방지서명 방식은 서명자의 도움없이는 서명문을 확인할 수 없는 특징을 가지고 있으며, 서명문의 진위를 확인해주는 확인 프로토콜(confirmation protocol)과 자신의 서명문을 부인하지 못하게 하는 부인 프로토콜(disavowal protocol)로 구성된다.[4,7]

그러나 D. Chaum의 부인방지서명은 자신의 서명문을 부인하지 못하게 하는 부인 프로토콜로 인하여 일종의 거짓말 탐지기 기능을 제공하게 된다. 이와 같은 문제를 해결하기 위하여 T. Okamoto 등이 제안한 non-transitive digital signature가 있다. 그러나 이 non-transitive digital signature은 서명이 문제가 되었을 때 분쟁 해결의 기능이 없어 디지털 서명이라고 할 수 없다.[8]

본 논문에서는 영지식 대화형 증명시스템(ZKIPS : Zero-Knowledge Interactive Proof System)을 사용하여 제3의 재판관 개념을 도입하여 부인방지서명의 특성은 유지하면서 거짓말 탐지기 기능 문제를 해결할 수 있는 의뢰부인방지서명(entrusted undeniable signature) 방식을 제안한다.

2. 부인방지서명

본 장에서는 D. Chaum이 처음으로 제안한 부인방지서명 방식을 설명하고 거짓말 탐지기 기능이 어떻게 사용되는지 알아본다.[4,7]

기존에 제안된 디지털 서명 방식들은 검증 프로토콜에서 서명자의 도움 없이도 서명문의 정당성 여부를 확인할 수 있는 자체인증기능 특성이 있는 반면에, D. Chaum에 의해 제안된 부인방지서명 방식은 자체인증 특성을 배제하여 서명문의 정당성 여부를 확인하고자 할 때 서명자가 개입하도록 하였다.

부인방지서명 방식은 서명자가 자신의 서명문을 검증자에게 확인시켜주는 확인 프로토콜과,후에 서명자가 자신의 서명문을 부인하지 못하게 하는 부인프로토콜로 구성되어 있다. 확인프로토콜은 일반적인 검증 프로토콜과 마찬가지로 서명의 정당성 여부를 판단하는 프로토콜로서 이 프로토콜에 의한 검증이 성공하면 높은 확률로 서명문의 정당함을 인정하게 된다. 또한 부인 프로토콜은 확인하려한 서명문이 불법적인 침입자에 의해 만들어진 부당한 서명문이었는지 아니면 정당한 서명문에 대하여 서명자가 부인하려는 의도에서 적절치 않은 응답을 하였는지를 구분하기 위한 프로토콜로 서명자는 부인 프로토콜에 의해 자신의 서명문을 부인하지 못하게 된다.

D. Chaum의 부인방지서명 방식의 구성방법은 다음과 같다.

신뢰할 수 있는 센터가 소수 P와 유한체 Z_P(GF(P)) 상에서의 원시원소 g를 선택하여 사용자들에게 공개한다. 서명자는 임의의 난수 $x \in_R Z_P$를 선택하여 자신의 비밀키로 하고 $V = g^x \bmod P$를 계산하여 자신의 공개키로 공개한다.

서명자는 자신의 메시지 m를 $Z = m^x \bmod P$로 서명을 하여 검증자에게 전송한다. 그러면 그림 1의 과정으로 검증자는 확인 프로토콜을 실행한다.

〔확인 프로토콜〕

① 검증자는 두 난수 $a,b \in_R Z_P$를 선택하여 T를 계산해서 서명자에게 전송한다.

② 서명자는 임의의 난수 $q \in_R Z_P$를 선택하여 D_1

= Tg^q mod P, $D_2 = D_1^x$ mod P를 계산하여 검증자에게 전송한다.

③ 검증자는 순서①에서 선택한 a,b를 서명자에게 전송한다. 서명자는 a,b로 T의 정당성을 확인하고 정당한 검증자임을 확인하여 q를 전송한다.

④ 검증자는 순서②에서 전송 받은 D_1과 D_2가 $D1 = Tg^q$ mod P와 $D_2 = Z^a V^{(b \cdot q)}$ mod P인가를 확인하여 정당성을 검증한다.

확인 프로토콜 순서 ① - ④의 과정이 정상적이면 서명자의 서명문 Z는 정당한 서명임을 확인할 수 있다.

한편, 서명자가 자신의 서명문을 부인할 때 검증자는 그림 2의 부인 프로토콜을 실행함으로써 서명자가 자신의 서명문을 부인하지 못하게 한다.

〔부인 프로토콜〕

① 검증자는 임의의 난수 $a \in_R Z_P$와 검증수 $s \in \{0,1,\ ,k-1\}$를 선택하여 $T_1 = m^s g^a$ mod P와 $T_2 = Z^s V^a$ mod P를 서명자에게 전송한다.

② 서명자는 T_1^x / T_2를 계산하여 그 값이 1이 아니면 s 값을 계산하여 $q \in_R Z_P$를 선택해서 $Q = g^{sq}$ mod P를 계산하여 검증자에게 전송한다.

③ 검증자는 자신이 선택한 난수 a를 서명자에게 전송한다. 서명자는 T_1과 T_2의 정당성을 확인하고 검증자에게 q를 전송한다.

④ 검증자는 $Q = g^{sq}$ mod P인가를 확인하여 원래의 서명 Z의 정당성을 검증한다. $Q=g^{sq}$ mod P이면 Z는 서명자의 서명이 아님을 확인할 수 있다.

D. Chaum의 부인방지 프로토콜에서 서명자가 자신의 서명문을 부인할 수 있는 경우는 검증수 s를 정확히 계산할 수 있는 경우인데, 이 확률은 1/k 이 된다. 그러므로 k=1024으로 가정할 경우, 부인 프로토콜을 2회 수행하면 약 100만 분의 1의 확률로 자신의 서명문을 부정할 수 있으며, 부인 프로토콜을 10회 수행하면 자신의 서명문을 부정할 수 있는 확률이 2^{-100}이 된다.

이제 D.Chaum이 제안한 부인방지 서명의 거짓말 탐지기 기능문제에 대하여 알아본다.

어느 기관에 근무하는 공직자가 신문사나 방송 등의 언론기관에 비밀 정보를 제공하고자 할 때, 신원이 밝혀지는 것을 걱정하여 익명을 요구하며 정보를 제공하려는 경우를 생각해보자. 언론기관에서는 허위정보를 보도할 수 없으므로 정보 제공자의 신원을 확인할 필요가 있을 것이고 또한 언론기관은 정보 제공자의 요구대로 그의 신원을 밝히지 않는다고 약속을 할 것이다. 이 경우에도 일반적인 디지털 서명은 적합치 않으며, 만일 정보 제공자가 부인방지 서명을 사용한다고 가정해보자.

정보가 기사화 되고 그 출처를 알아내기 위해 해당기관에서 이를 추적하는 과정에서 이 정보와 관련된 정보

서명자	x : 비밀키 $V=g^x$: 공개키 m^x : 서명문	검증자
	T 〈----------	a,b $\in_R Z_P$ $T=m^a g^b$ mod P
$q \in_R Z_P$ $D_1 = Tg^q$ mod P $D_2 = D_1^x$ mod P	D1,D2 ----------〉	
$T=m^a g^b$ mod P	〈----a,b----	
	q ----------〉	$D_1 = Tg^q$ mod P $D_2 = Z^s V^{b \cdot q}$ mod P

그림 1. D.Chaum의 부인방지서명의 확인 프로토콜

서명자	x : 비밀키 $V=g^x$: 공개키	검증자
	T_1, T_2 〈----------	a$\in_R Z_P$ s$\in\{0,1,\ ,k-1\}$ $T_1=m^s g^a$ mod P $T_2=Z^s V^a$ mod P
s 계산 $q \in_R Z_P$ $Q = g^{sq}$ mod P	Q ----------〉	$D_1 = Tg^q$ mod P
T_1, T_2	〈----a----	$D_2 = Z^s V^{b \cdot q}$ mod P
	----q----〉	$Q=(g^s)^q$ mod P

그림 2. D.Chaum의 부인방지서명의 부인 프로토콜

를 얻었다고 하자. 그러면 그 해당기관에서는 의심이 갈 만한 모든 내부 직원에게 부인 프로토콜을 수행하게 함으로서 정보의 출처를 알아낼 수 있을 것이다. 즉 의심을 받은 사람은 부인 프로토콜을 수행하면 쉽게 자신의 누명을 벗을 수 있고 오히려 이를 거부하는 사람은 자신이 그 정보의 출처임을 시인하는 결과가 될 것이므로 이를 거부할 하등의 이유가 없을 것이다. 따라서 결국 정보 제공자는 신원이 밝혀지게 될 것이므로 이와 같은 응용에서는 부인 방지 서명이 적합치 않음을 알 수 있다.

3. 의뢰부인방지서명

D.Chaum이 제안한 부인방지 서명의 거짓말 탐지기 능 문제를 영지식 대화형 증명 시스템을 이용하여 제3의 재판관 개념을 도입하여 해결할 수 있는 의뢰부인방지서명 방식을 제안한다. D.Chaum의 부인방지 서명방식에서 거짓말 탐지기 기능 문제가 발생하는 것은 결국 검증을 원하는 임의의 검증자가 부인 프로토콜을 수행할 수 있다는 사실에 기인한다. 따라서 거짓말 탐지기 기능 문제를 해결하기 위해서는 임의의 검증자가 부인 프로토콜을 할 수 없고 특정한 자, 예를 들어 분쟁이 발생하였을 때 중재하는 사람 혹은 재판관만이 부인 프로토콜을 할 수 있도록 만드는 것이다. 그러나 디지털 서명의 특성상 확인 프로토콜은 임의의 검증자가 할 수 있도록 해야 한다.

거짓말 탐지기 기능 문제를 해결할 수 있는 의뢰부인방지서명 방식의 구성은 먼저 부인방지서명 방식에서 사용되는 서명자의 공개키 $V=g^x$를 $V'=(g^x)^r$로 랜덤화하고, 난수 r를 제3의 재판관에게 commitment 방식을 사용하여 공증함으로서 구성할 수 있다. 즉 난수 r를 모르는 검증자는 부인 프로토콜을 하지 못하도록 하고, 후에 서명자가 자신의 서명문을 부인하지 못하게 하기 위하여 자신이 선택한 난수 r를 commitment 방식을 사용하여 제3의 재판관에게 공증함으로서 r를 알 수 있는 제3의 재판관은 부인 프로토콜을 수행할 수 있게 되는 것이다.

또한 확인 프로토콜은 공개키 $V=g^x$를 $V'=(g^x)^r$로 랜덤화하기 위하여 사용한 r과 재판관에게 공증한 r이 같다는 사실을 영지식 대화형 증명 방식을 이용하여 검증자에게 증명한 후 수행하게 함으로써 r를 모르는 임의의 검증자에게도 확인 프로토콜이 가능하도록 한다.

서명에 대한 분쟁이 발생하였을 때 즉 서명문의 서명자를 확인할 때는 랜덤 변수 r를 알고 있는 재판관만이 부인 프로토콜을 수행할 수 있도록 한다. 재판관은 자신의 공개키로 commitment된 r를 비밀키로 찾아 부인 프로토콜을 시작한다.

의뢰부인방지서명 방식은 D.Chaum의 부인방지 서명과 마찬가지로 이산대수 문제를 기반으로 하는 공개키 g^x와 비밀키 x를 선택하고 공개키는 공개한다. 부인 프로토콜을 위한 재판관은 RSA 공개키 시스템을 이용하여 공개키 (e, n), 비밀키 (d, p, q)를 생성하여, 모든 서명자에게 공개키를 공개하고 비밀키는 자신이 비밀리에 보관한다. 서명자는 임의의 난수 $r \in_R Z_P$에 대한 공증방식으로 commitment 방식 $CS(r) = r^e \bmod n$을 사용한다.

평문 m에 대한 서명문이 부인방지서명 방식의 경우 $Z=m^x$이나, 의뢰부인방지서명 방식의 경우에는 $Z=m^{rx}$가 된다. 서명자가 서명문 $Z=m^{rx}$를 생성하여 〈 $CS(r)$, g^{rx}, m^{rx} 〉를 검증자에게 전달한다. 서명문을 확인하기 위한 확인 프로토콜 전에 서명자와 검증자 사이에 영지식 대화형 증명을 통하여 공개키 g^x를 $(g^x)^r$로 랜덤화하기 위하여 사용한 r과 재판관에게 공증한 r이 같다는 사실을 확인시킨다.

영지식 대화형 증명방식으로 자신이 사용한 난수 r를 검증자에게 확인시켜준 서명자는 D.Chaum의 부인방지서명 방식과 동일한 방법으로 확인 프로토콜을 수행하여 서명문의 정당성을 검증자에게 증명할 수 있게 된다.

의뢰 부인방지서명 방식의 전체 과정은 그림 3과 같다.

이제 의뢰부인방지서명 과정의 각 프로토콜을 살펴보자. 〈$CS(r)$, g^{rx}〉에 대한 영지식 대화형 증명방식, 서명문의 확인을 위한 확인 프로토콜, 분쟁 발생시 해결을 위한 부인 프로토콜 순으로 설명한다.

〔영지식 대화형 증명〕

서명자가 $V'=g^{rx} \bmod P$와 $CS(r)$를 검증자에게 전달하였을 때 검증자는 공개키 $V=g^x$를 $V'=(g^x)^r$로 랜덤화하기 위하여 사용한 r과 재판관에게 공증한 r이 같다는 사실을 확인해야 한다. 물론 이때 검증자가 r의 값을 알 수 없게 해야 한다. 이를 위해 영지식 대화형 증명 시스템이 사용된다. 그 과정은 그림 4와 같다.

① 서명자는 랜덤 수 $h \in_R Z_P$를 선택하여 $V_1 \equiv h^e$

서 명 자	x : 비밀키 $V=g^x$: 공개키 CS(r) : commitment	검 증 자
$r \in_R Z_P$	$\langle CS(r), g^{rx}, m^{rx} \rangle$ ——————→	
	$\langle CS(r), g^{rx} \rangle$ 에 대한 ZKIP	
	확인 프로토콜 서명문 : $\langle CS(r), (g^{rx}, m^{rx}) \rangle$	
	부인 프로토콜 ——————→ CS(r)	재판관

그림 3. 의뢰부인방지서명 방식의 전체 과정

서 명 자		검 증 자
$h \in_R ZP$ $V_1=h^a \bmod n$ $V_2=g^{rhx} \bmod P$	V_1, V_2 ——→	
	b ——→	$b \in_R \{0,1\}$
b=0 : R=h b=1 : R=rh	R ——→	b=0 $V_1=R^a \bmod n$ $V_2=g^{rxR} \bmod P$ b=1 $R^a=V_1 r^a \bmod n$ $V_2=(g^x)^R \bmod P$

(t회 반복한다)

그림 4. $\langle CS(r), g^{rx} \rangle$에 대한 영지식 대화형 증명

$\bmod n$, $V_2 \equiv g^{rhx} \bmod P$를 서명자에게 전송한다.

② 검증자는 랜덤 비트 $b \in_R \{0,1\}$을 서명자에게 전송한다.

③ 검증자로부터 전송 받은 b = 0 이면 R = h을 b =1 이면 R = rh을 검증자에게 전송한다.

④ 검증자는 b = 0 을 전송하였을 경우 $V_1 = R^a \bmod p$, $V_2 = g^{rxR} \bmod P$, b =1 을 전송하였을 경우 $R^a = h^a r^a$, $V_2 = (g^x)^{rh}$ 인가를 확인한다.

순서 ① - ④ 을 정상적으로 수행하면 서명자가 공개키 $V=g^x$를 $V'=(g^x)^r$로 랜덤화하기 위하여 사용한 r과 재판관에게 공증한 r이 같다는 사실을 검증자는 확인할 수 있게 된다.

그림 4에서 주어진 프로토콜은 다음에 주어지는 확률론적 튜링 머신인 Simulator M에 의해 영지식 증명시스템임을 쉽게 증명할 수 있다.[9]

〔Simulator M〕

① bit_{i+1} := a random number of {0,1}

② R_{i+1} := a random member of Z_P

③ if $bit_{i+1} = 0$ then

$$V_{1,i+1} := R_{i+1}{}^a \bmod n$$
$$V_{2,i+1} := (g^{rx})^{R_{i+1}} \bmod P$$

else

$$V_{1,i+1} := R_{i+1}{}^a CS(r)^{-1} \bmod n$$
$$V_{2,i+1} := (g^x)^{R_{i+1}} \bmod P$$

④ if $bit_{i+1} = f(V, V', CS(r), H.view_i, V_{1,i+1}, V_{2,i+1})$ then M outputs $V_{1,i+1}$, $V_{2,i+1}$, bit_{i+1}, R_{i+1} and HALT

영지식 대화형 증명이 정상적으로 종료되면 제 삼자 누구도 확인 프로토콜을 수행할 수 있다.

〔확인 프로토콜〕

확인 프로토콜은 서명자가 비밀키 x를 사용하는 대신에 rx를 사용하는 것을 제외하고는 D.Chaum의 프로토콜과 같으며 절차는 그림 5와 같다.

① 검증자는 랜덤 수 $a \in_R Z_P$, $b \in_R Z_P$를 선택하여 $T \equiv m^a g^b \bmod p$를 계산해서 서명자에게 전송한다.

② 서명자는 $D_1 \equiv m^a g^{b \cdot q} \bmod P$와 D_2 $D_1{}^{rx} \equiv \bmod P$를 계산하여 검증자에게 전송한다.

③ 검증자는 서명자에게 순서①에서 선택하였던 a, b를 전송한다.

④ 서명자는 검증자로부터 받은 a, b로 $T \equiv m^a g^b \bmod P$인가를 확인하고 검증자에게 q를 전송한다.

⑤ 검증자는 전송 받은 q로 $D_1 \equiv m^a g^{(b \cdot q)} \bmod P$, $D_2 \equiv Z^a V^{r(b \cdot q)} \bmod P$인가를 확인하여 확인 프로토콜을 검증한다.

서 명 자	rx : 비밀키 $V^r=g^{rx}$: 공개키 $Z=m^{rx}$: 서명문	검 증 자
	T 〈----------	$a\in_R Z_P$, $b\in_R Z_P$ $T\equiv m^a g^b \bmod P$
$q\in_R Z_P$ $D_1\ m^a g^{bq} \bmod P$ $D_2\ D_1^{rx} \bmod P$	D_1, D_2 ----------〉	
$T\ m^a g^b \bmod P$	a, b ----------〉	
	q ----------〉	$D_1\equiv m^a g^{bq} \bmod P$ $D_2\equiv Z^a V^{a(b-q)} \bmod P$

그림 5. 확인 프로토콜

서 명 자	$Z\neq m^{rx}$: 서명문	재 판 관
	T_1, T_2 ----------〉	$s\in_R\{0,1,\ldots,k-1\}$ $a\in_R Z_P$ $T_1\equiv m^a g^a \bmod P$ $T_2\equiv Z^{a/r} V^a \bmod P$
s값을 계산 $q\in_R Z_P$ $Q\ g^{aq} \bmod P$	Q ----------〉	
T_1, T_2 확인	a ----------〉	
	q ----------〉	$Q\equiv g^{aq} \bmod P_1$

그림 6. 부인 프로토콜

순서 ① - ⑤를 실행함으로써 자신의 서명문의 정당함을 확인시킬 수 있다.

검증자는 서명자가 자신의 서명문을 부인할 때, 부인 프로토콜을 재판관에게 요청한다. 재판관은 검증자의 요청에 따라 부인 프로토콜을 수행하기 전에 자신의 비밀키 d로 $(r^e)^d \bmod n$을 계산하여 r를 찾아내고 $Z^{1/r}\neq m^x \bmod n$을 서명자에게 전송한 후 다음 그림 6의 절차로 부인 프로토콜을 수행한다.

〔부인 프로토콜〕

① 재판관은 서명문의 부인을 확인하기 위해 $s\in_R\{0,1,\ldots,k-1\}$와 $a\in_R Z_P$를 선택하여, $T_1\equiv m^a g^a \bmod P$, $T_2\equiv Z^{a/r} V^a \bmod P$를 계산해서 서명자에게 전송한다.

② 서명자는 $Z\neq m^{rx} \bmod P$가 자신의 서명문이 아닐 때 다음의 계산을 통하여 s 값을 구한 후 $Q\equiv g^{aq} \bmod P$를 재판관에게 전송한다.

〔s를 구하는 계산〕

$T_1^x\equiv(m^a g^a)^x \bmod P$이므로 $T_2/T_1^x \bmod P\equiv(Z^{1/r}/m^x)^a \bmod P$.

그런데 서명자는 $Z^{1/r}$를 알고 있으므로, s 값을 구하기 위해 $s=0,1,\ldots,k-1$를 식 $(Z^{1/r}/m^x)^s \bmod P$ $T_2/T_1^x \bmod P$이 만족될 때까지 대입한다.

이 때 위 식을 만족하는 값이 s 값이다.

③ 재판관은 순서①에서 선택한 a를 서명자에게 전송한다.

④ 서명자는 a로 T_1, T_2를 확인하고 q를 재판관에게 전송한다.

⑤ 재판관은 m^{rx}이 서명자의 서명문이 아님을 확인한다.

순서 ① - ⑤과정에서 서명자 자신의 서명문이 아닐 때 재판관이 선택한 s를 구함으로써 자신의 서명문이 아님을 확인할 수 있다. 또한 서명자 자신의 서명문이면 s를 구하지 못해 자신의 서명문이 아니라는 것을 주장할 수 없게 된다.

D. Chaum의 부인방지 프로토콜과 마찬가지로 서명자가 자신의 서명문을 부인할 수 있는 경우는 검증수 s를 정확히 계산할 수 있는 경우인데, 이 확률은 1/k 이 된다. 그러므로 k=1024으로 가정할 경우, 부인 프로토콜을 2회 수행하면 약 100만 분의 1의 확률로 자신의 서명문을 부정할 수 있으며, 부인 프로토콜을 10회 수행하면 자신의 서명문을 부정할 수 있는 확률이 2^{-100}이 된다.

4. 결 론

본 논문에서는 D.Chaum의 부인방지 서명에서 발생하는 거짓말 탐지기 기능을 제3의 재판관 개념을 도입하

여 해결하였다.

서명자는 자신의 비밀키 x와 공개키 $V=g^x$를 임의의 난수 r를 생성하여 rx와 $V'=g^{rx}$로 랜덤화하여 r를 모르는 사람은 부인 프로토콜을 실행하지 못하도록 하였다.

서명자는 먼저 자신이 공개키 $V=g^x$를 $Vr=(g^x)^r$로 랜덤화하기 위하여 사용한 r과 재판관에게 공증한 r이 같다는 사실을 영지식 대화형 증명으로 검증자에게 증명하고, 확인 프로토콜을 실행하도록 구성하였으며 재판관과 서명자 사이에는 r를 commitment시켜 r를 알 수 있는 재판관만이 부인 프로토콜을 실행할 수 있도록 구성하였다.

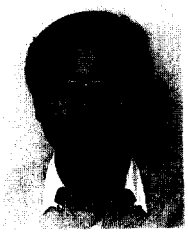
단 이 방식은 영지식 대화형 증명에 소요되는 통신량이 다소 증가하는 불편이 있어 이 통신량을 줄이기 위한 연구가 계속되어야 할 것으로 사료된다. 특히 제3의 재판관 없이도 부인방지서명 방식의 거짓말 탐지기 문제를 해결할 수 있는 프로토콜 연구가 계속되어야 할 것으로 생각된다.

참고문헌

1. 임채훈, 이필중, "상호 신분 인증 및 디지틀 서명기법에 관한 연구," 통신정보보호학회 논문집 제2권 제1호, pp.16-35, 1992.
2. 김승주,박성준,원동호, "수신자 지정서명방식에 관한 고찰," 한국정보처리응용학회 학술발표회 논문집, pp.530-533, 1994년. 10월. 8일.
3. 김승주, 박성준, 원동호, "수신자 지정 서명방식," 한국통신정보보호학회 학술발표회 논문집, pp.24-28, 1994년. 11월. 19일.
4. 곽남영, 박성준, 류재철, "실용적인 부인방지 전자 서명기법," 한국통신정보보호학회 학술발표회 논문집, pp.35-44, 1994년. 11월. 19일.
5. D. Chaum and H. Antwerpen, "Undeniable signature," Proc. Crypto '89, pp.212-216, 1989.
6. D. Chaum, "Zero-knowledge undeniable signature," Proc. Eurocrypt '90, pp.458-464, 1990.
7. J. Boyar, D. Chaum, and I. Damgard, "Convertible undeniable signature," Proc. Crypto '90, pp.195-208, 1990.
8. T. Okamoto and K. Ohta, "How to utilize the randomness of zero-knowledge proofs", Proc. Crypto '90, pp.437-456, 1990.
9. S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of Interactive Proof System," SIAM J. COMPUT. Vol. 18, No. 1, pp.186-208, 1989.
10. 박성준, 이보영, 원동호, "의뢰 Undeniable Signature," 한국통신학회 학술발표회 논문집, pp.47-49, 1994년. 7월. 21일.

元 東 豪(Dong Ho Won) 종신회원

1949년 9월 23일생
1976년 2월 : 성균관대학교 전자공학과 졸업(공학사)
1978년 2월 : 성균관대학교 대학원 전자공학과 졸업(공학석사)
1988년 2월 : 성균관대학교 대학원 전자공학과 졸업(공학박사)
1978년 4월~1980년 3월 : 한국전자통신연구소 연구원
1985년 9월~1986년 8월 : 일본 동경공대 객원연구원
1982년 3월~현재 : 성균관대학교 공과대학 정보공학과 교수
1991년~현재 : 한국통신정보보호학회 편집이사
※주관심 분야 : 암호이론,정보이론



朴 性 俊(Sung Jun Park) 정회원

1960년 10월 29일생
1983년 2월 : 한양대학교 수학과 졸업(이학사)
1985년 2월 : 한양대학교 대학원 수학과 졸업(이학석사)
1985년 1월~1994년 3월 : 한국전자통신연구소 부호기술부 선임연구원
1992년 3월~현재 : 성균관대학교 대학원 정보공학과 박사과정
※주관심 분야 : 암호이론,계산이론,정보이론

李 蒲 英(Bo Young Lee) 정회원

1966년 3월 13일생
1989년 2월 : 성균관대학교 정보공학과 졸업(공학사)
1995년 8월 : 성균관대학교 대학원 정보공학과 졸업(공학석사)
1990년 9월~1993년 10월 : 콜롬버스(주) 전산실
1993년 10월~1995년 5월 : (주)KISC
1995년 7월~현재 : 한국전산원 연구원
※주관심 분야 : 암호이론, 컴퓨터 보안