효율적인 다목적 전환 부인봉쇄 서명 기법

The Efficient Multipurpose Convertible Undeniable Signature Scheme

윤성현, 한군희
천안대학교 정보통신학부

Sung-Hyun Yun(shyoon@cheonan.ac.kr), Kun-Hee Han(hankh@cheonan.ac.kr)

요약

부인봉쇄 서명 기법에서 디지털 서명은 서명자의 동의하에서만 검증 및 부인이 가능하다. 회사 내에서 디지털 서명된 비밀문서가 경쟁 업체에 복제되어 전달되는 경우에, 해당 문서가 일반 서명기법으로 서명되면, 서명자의 동의 없이도 경쟁 업체에서 문서의 진위 여부를 검증할 수 있다. 서명자의 동의하에서만 비밀문서가 검증되기 원한다면, 부인봉쇄 서명 기법의 적용은 필수적이다. 전환 부인봉쇄 서명 기법은 일반 부인 봉쇄 서명 기능과 더불어 부인봉쇄 서명에서 일반 서명으로 필요에 따라서 전환할 수 있는 부가적인 특성을 제공한다. 더 이상 비밀 유지가 필요 없는 부인봉쇄 서명된 문서의 경우에 일반 서명으로 전환하여 공개할 수 있다. 본 연구에서는 El-Gamal 서명 기법에 기반 한 효율적인 다목적 전환 부인봉쇄 서명 기법을 제안한다. 제안한 기법은 부인봉쇄 성질을 만족하며 부인봉쇄 서명을 일반 서명으로 전환할 수 있다. Boyar가 제안한 전환 부인봉쇄 서명 기법과 비교하여 공개키 및 서명 크기가 작으며, 서명 확인 프로토콜에서의 통신 단계 수를 줄였다.

■ 중심어 : | 부인봉쇄 서명 | 전환 부인봉쇄 서명 | 디지털 서명 | 디지털 콘텐츠 보호 |

Abstract

The digital signature can be verified and disavowed only with cooperation of the signer in undeniable signature scheme. A signed confidential document of a company can be copied and delivered to a rival company. If a conventional signature scheme is used to sign the document, it can be confirmed as authentic by verifying the signature without the signer's cooperation. However, if the company doesn't want the document to be verified as authentic by the rival company, it is recommended to use the undeniable signature scheme. Convertible undeniable signature scheme has additional property that the signer can convert undeniable signature to the ordinary one. The document signed by undeniable signature scheme that is no longer confidential can be opened to public use by converting the signature to the ordinary one. In this study, the efficient multipurpose convertible undeniable signature scheme based on El-Gamal signature scheme is proposed. The proposed scheme satisfies undeniable property and can convert undeniable signature to the ordinary one. The number of public keys and signatures are less than those of Boyar's convertible signature scheme. It also reduces the number of communication steps of the signature confirmation protocol.

■ keyword : | Undeniable Signature | Convertible Undeniable Signature | Digital Signature | Contents Security |

접수번호 : #050308-001
접수일자 : 2005년 03월 08일
심사완료일 : 2005년 04월 30일
교신저자 : 윤성현, e-mail : shyoon@cheonan.ac.kr

I. 서 론

부인봉쇄 서명 기법은 서명자의 동의 없이는 서명을 검증할 수 없는 기법이다. 전환 부인봉쇄 서명 기법은 비밀정보의 일부를 공개함으로써 부인봉쇄 서명을 일반서명으로 전환할 수 있는 부가적인 특성을 갖는다. 일반 서명 기법으로 해결할 수 없는 많은 응용에 적용될 수 있는 기법이다.

디지털 콘텐츠를 온라인으로 판매 및 유통하는 모델에서 디지털 콘텐츠 저작자는 본인이 만든 저작물이 중개인에 의해서 고객들에게 올바로 판매되었는지 알 수 있어야 해당 유통 모델을 신뢰할 수 있게 된다. 저작자는 본인의 동의 없이는 고객들이 디지털 콘텐츠를 살 수 없도록 하는 온라인 판매 모델을 필요로 한다. 부인봉쇄 서명 기법으로 만들어진 디지털 저작권은 일반 서명으로 만들어진 디지털 저작권과 비교하여 다음과 같은 특성을 제공한다. 콘텐츠 구매자는 저작권자의 동의 없이는 구매한 콘텐츠의 저작권 정보가 올바른 것인지 확인할 수 없으며, 원 저작자만이 구매자에게 저작권의 진위 여부를 확인시켜줄 수 있다.

하지만 구매자의 입장에서 보면, 해당 콘텐츠를 구매한 후에 매번 저작권 정보를 확인 받아야지만 사용할 수 있다면 많은 불편이 따르게 된다. 따라서 부인봉쇄 서명된 저작권을 일반 저작권으로 변환할 수 있는 방법이 필요하며, 이러한 경우에 전환 부인봉쇄 서명 기법의 적용은 필수적이다.

본 논문에서는 El-Gamal 서명 기법[2]의 서명식을 변형하여 부인봉쇄 성질을 만족하며 필요에 따라 일반 서명으로 전환할 수 있는 효율적인 전환 부인봉쇄 서명 기법을 제안한다. 기존의 Boyar의 전환 부인봉쇄 서명 기법[4]과 비교하여 서명 크기, 공개키 개수 및 서명확인 단계 수가 적어 실용적이며, 부인봉쇄 다중서명 기법으로의 확장이 용이한 다목적 서명 기법이다.

II장에서는 Chaum의 서명 기법을 통하여 부인봉쇄 성질에 대해서 살펴보고, 동시 이산 대수 문제에 기반 한 Boyar의 서명 기법의 특징 및 한계에 대해서 알아본다. III장에서는 다목적 전환 부인봉쇄 서명 기법에 대해서 제안하며 IV장에서 부인봉쇄 성질을 분석한다. V장에서는 기존 기법과의 차이점 및 제안한 방법의 확장 및 응용에 대해서 고찰하고 VI장에서 결론을 기술한다.

II. 관련 연구

Chaum이 처음 제안한 부인봉쇄 서명 기법[1]과 Boyar가 제안한 전환 부인봉쇄 서명 기법[4]에 대해서 살펴본다. 이산 대수 문제에 근거한 공개키 알고리즘의 안전성은 암호학적으로 안전한 유한체에 기반한다[2]. 유한체 $GF(p)$ 와 군 G_q 에 대한 정의는 다음과 같다.

[정의 1] 암호학적으로 안전한 유한체 $GF(p)$ 와 군 G_q

p 는 큰 소수로 유한체 $GF(p)$ 상에서 법 p 에 대한 이산 대수를 구하는 것이 계산상 불가능할 때 $GF(p)$ 를 암호학적으로 안전한 유한체라 정의한다. $p-1$ 의 인수 중 큰 소수를 q 라 가정하면, 군 G_q 는 $GF(p)$ 의 부분 집합 군으로 위수 q 를 갖는다.

1. 부인봉쇄 서명 기법[1]

서명자는 정의 1로부터 암호학적으로 안전한 유한체 $GF(p)$ 와 군 G_q 를 선택한다. g 는 군 G_q 의 원소로 위수(order) q 를 갖는 생성자이다. 서명자는 Z_q 상에서 비밀키 x 를 선택하고 공개키 $y \equiv g^x \pmod{p}$ 를 계산한다.

1.1 서명 생성 프로토콜

단계 1 : 서명자는 메시지 m 에 대한 부인봉쇄 서명 z 을 생성하고, 메시지와 함께 검증자에게 전송한다.

$$z \equiv m^x \pmod{p},\ m \in G_q$$

1.2 서명 확인 프로토콜

단계 1 : 검증자는 Z_q 상에서 임의의 난수 a, b 를 선택하고 다음과 같이 도전(challenge) w

를 생성한다.

$w \equiv z^a \cdot y^b \pmod{p},\ a,\ b \in Z_q$

검증자는 도전 w 를 서명자에게 전송한다.

단계 2 : 서명자는 다음과 같이 응답(response) R 을 생성한다. x^{-1} 는 법 q 에 대한 x 의 모듈라 곱셈의 역이다.

$R \equiv w^{x^{-1}} \pmod{p},$

$x \cdot x^{-1} \equiv 1 \pmod{q}$

단계 3 : 검증자는 다음 식을 통해서 서명을 검증한다.

$R \equiv m^a \cdot g^b \pmod{p}$: z 는 m 에 대한 올바른 서명이다.

$R \not\equiv m^a \cdot g^b \pmod{p}$: m 에 대한 서명 z 이 잘못됐거나, 서명자가 올바른 서명에 대해서 부인을 하는 경우이다.

1.3 부인 프로토콜(disavowal protocol)

서명자가 생성한 응답 R 이 검증자가 생성한 $m^a \cdot g^b$ 과 다르면 z 가 잘못된 서명이거나 서명자가 올바른 서명에 대해서 부인을 하는 두 가지 경우가 존재한다. 검증자는 부인 프로토콜을 수행해서 서명자의 부정을 검증한다. 단계 1, 2, 3은 서명 확인 프로토콜과 같고 $R \not\equiv m^a \cdot g^b \pmod{p}$ 인 경우에 다음과 같이 단계 4, 5, 6을 수행하여 서명이 잘못된 것인지 서명자가 부정을 하는 것인지 입증한다.

단계 4 : 검증자는 Z_q 상에서 임의의 난수 $c,\ d$ 를 선택하고 다음과 같이 도전 w' 을 생성한다. 검증자는 도전 w' 을 서명자에게 전송한다.

$w' \equiv z^c \cdot y^d \pmod{p},\ c,\ d \in Z_q$

단계 5 : 서명자는 다음과 같이 도전 w' 에 대한 응답 R' 을 생성한다. 검증자에게 응답 R' 을 전송한다.

$R' \equiv w'^{\,x^{-1}} \pmod{p}$

단계 6 : 검증자는 다음 판단식을 생성해서 서명자의 부정을 검증한다.

$(R \cdot g^{-b})^c \equiv (R' \cdot g^{-d})^a \pmod{p}$: 서명 z 가 잘못됨

$(R \cdot g^{-b})^c \not\equiv (R' \cdot g^{-d})^a \pmod{p}$: 서명자가 올바른 서명에 대해서 부인

2. 전환 부인봉쇄 서명기법[4]

Boyar가 제안한 서명 기법에서 서명자의 비밀키 $(x,\ z)$ 와 공개키 $(p,\ q,\ g,\ y,\ u)$ 는 다음과 같이 정의된다. 암호학적으로 안전한 유한체 $GF(p)$ 와 군 G_q 는 정의 1과 같고 g 는 G_q 상에서 정의된 생성자로 위수 q 를 갖는다.

$x,\ z \in Z_q,\ y \equiv g^x \pmod{p}$

$u \equiv g^z \pmod{p},\ m \in G_q$

2.1 서명자의 서명 생성 단계

단계 1 : 서명자는 임의의 난수 t 를 선택한 후 다음과 같이 메시지 M 을 만든다.

$M \equiv g^t \cdot t \cdot z \cdot m \pmod{q}$

단계 2 : M 에 대한 El-Gamal 서명 $(r,\ s)$ 를 생성한다.

$g^M \equiv y^r \cdot r^s \pmod{p}$

단계 3 : $(g^t,\ r,\ s,\ m)$ 를 검증자에게 전송한다.

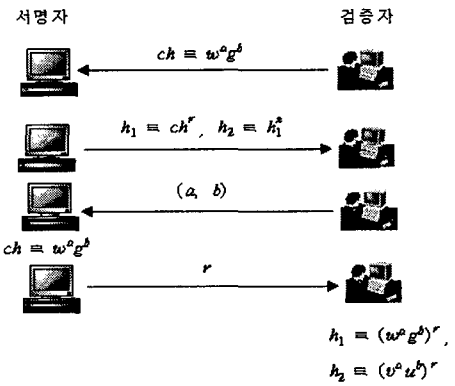


그림 1. 서명 확인 프로토콜

2.2 서명 확인 프로토콜

메시지 m 과 부인봉쇄 서명 $(g^t,\ r,\ s)$ 가 주어졌을 때 서명자와 검증자는 다음과 같이 w 와 v 를 계산할 수 있다.

$$w \equiv g^{t \cdot g^t \cdot m} \pmod{p},\quad v \equiv y^r \cdot r^s \pmod{p}$$

단계 1 : 검증자는 다음과 같이 임의의 난수 $a,\ b$ 를 선택하고 도전 ch 를 생성한다. 서명자에게 도전 ch 를 전송한다.

$$a,\ b \in Z_q,\ ch \equiv w^a \cdot g^b \pmod{p}$$

단계 2 : 서명자는 임의의 난수 r 을 선택해서 다음과 같이 응답 h_1 과 h_2 를 생성한다. 검증자에게 응답 h_1 과 h_2 를 전송한다.

$$h_1 \equiv ch^r \pmod{p},$$

$$h_2 \equiv h_1^z \pmod{p}$$

단계 3 : 검증자는 서명자에게 난수 값 a 와 b 를 전송한다.

단계 4 : 서명자는 다음과 같이 도전 ch 를 인증하고, 인증에 성공하면 r 을 검증자에게 전송한다.

$$ch \equiv w^a \cdot g^b \pmod{p}$$

단계 5 : 검증자는 다음과 같이 응답 h_1 과 h_2 를 검증한다.

$$h_1 \equiv (w^a \cdot g^b)^r \pmod{p}$$

$$h_2 \equiv (v^a \cdot u^b)^r \pmod{p}$$

2.3 서명 전환 프로토콜

서명자는 z 를 공개함으로써 모든 부인봉쇄 서명을 일반 서명으로 전환할 수 있다. 특정 서명을 전환하고자 할 경우 t 를 공개한다. t 가 공개되었을 때 서명 검증은 다음과 같다.

$$(u^{m \cdot g^t})^t \equiv y^r \cdot r^s \pmod{p}$$

III. 제안한 전환 부인봉쇄 서명 기법

II 장에서 살펴본 것과 같이 Boyar의 전환 부인봉쇄 서명 기법은 동시 이산대수 문제에 기반하고 있으며, 서명 확인 및 부인 프로토콜의 통신 단계 수가 많아지는 단점이 있다. 다중 서명으로의 확장을 고려할 경우에 서명자 수에 따라 통신 단계 수 및 관리해야 되는 서명 크기 및 개수가 증가하게 되어 확장이 용이하지 않다.

제안한 서명 기법은 El-Gamal 서명 기법[3]의 서명식을 변형하여 Chaum이 제안한 부인봉쇄 성질[1]을 만족하며 부인봉쇄 서명을 일반서명으로 전환할 수 있는 특성을 갖는다. 서명 확인 프로토콜의 통신 단계 수가 2회이며, 서명 크기 및 개수가 Boyar의 기법과 비교하여 작다. 또한, 변형된 El-Gamal 서명식으로부터 부인봉쇄 다중서명 기법으로의 확장이 용이하며, 통신 단계 수가 2회이기 때문에 다중서명 확인을 서명자들 간에 순차적으로 진행할 수 있는 장점이 있다. 식 3.1은 El-Gamal 서명식을 변형한 것으로써 본 논문에서 제안한 전환 부인봉쇄 서명 기법에 적용된다.

$$k \cdot (m_h + s) \equiv x \cdot r \pmod{p-1} \quad (3.1)$$

암호학적으로 안전한 유한체 $GF(p)$ 는 정의 1과 같고 g 는 $GF(p)$ 상에서 정의된 생성자로 위수 $p-1$ 을 갖는다. 서명자의 비밀키 x , 공개키 y 및 서명 대상 메시지 m 은 다음과 같다.

$$x \in Z_{p-1},\ y \equiv g^x \pmod{p},\ m \in Z_{p-1}$$

1. 서명자의 서명 생성 프로토콜

단계 1 : 서명자는 다음 조건을 만족하는 임의의 난수 k 를 선택하고 안전하게 보관한다. 일방향 해쉬 함수 h 를 이용해서 메시지 m 을 해쉬한다. 해쉬값 m_h 가 법 p 에 대한 원시근이 되도록 해쉬 파라미터 hpr 을 조정한다.

$$\gcd(k,\ p-1) = 1,$$

$$m_h = h(m,\ hpr)$$

단계 2 : 난수 k 에 대한 공개 정보 r 을 다음과 같이 생성한다.

$$r \equiv m_h^k \pmod{p}$$

단계 3 : 서명자는 식 3.2를 만족하는 s 를 구한다. k 와 $p-1$ 은 서로소이기 때문에 s 에 대한 유일한 해가 존재한다.

$$k \cdot s \equiv x \cdot r - k \cdot m_h \pmod{p-1} \quad (3.2)$$

단계 4 : 서명자는 검증자에게 메시지 m 과 해쉬 파라미터 hpr , 부인봉쇄 서명 (r, s) 를 전송한다.

2. 서명 확인 프로토콜

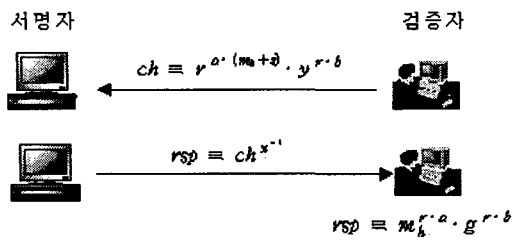


그림 2. 제안한 서명 확인 프로토콜

검증자는 서명 (r, s) 가 메시지 m 에 대한 올바른 서명인지 확인하기 위해서 [그림 2]와 같은 서명 확인 프로토콜을 수행한다.

단계 1 : 검증자는 임의의 난수 a, b 를 선택해서 서명자에게 전송할 도전 ch 를 다음과 같이 생성한다.

$$a, b \in Z_{p-1}, \quad m_h = h(m, hpr)$$

$$ch \equiv r^{a\cdot(m_h+s)} \cdot y^{r\cdot b} \pmod{p}$$

단계 2 : 검증자는 서명자에게 도전 ch 를 전송한다.

단계 3 : 서명자는 다음과 같이 응답 rsp 를 생성한다. x^{-1} 는 법 $p-1$ 에 대한 x 의 모듈라 곱셈의 역이다.

$$rsp \equiv ch^{x^{-1}} \pmod{p}$$

단계 4 : 서명자는 검증자에게 응답 rsp 를 전송한다.

단계 5 : 검증자는 식 3.3과 같이 rsp 를 인증해서 서명 (r, s) 가 메시지 m 에 대한 올바른 서명인지 확인한다. 식 3.3이 성립하지 않으면 서명 (r, s) 가 메시지 m 에 대한 올바른 서명이 아니거나 서명자가 부정을 하는 경우이다.

$$rsp \equiv m_h^{r\cdot a} \cdot g^{r\cdot b} \pmod{p} \quad (3.3)$$

부인봉쇄 서명을 일반 서명으로 전환할 경우에 다음과 같이 단계 6, 7, 8이 추가된다. 단계 6, 7을 통해서 서명자는 검증자의 도전을 인증하고 단계 8에서 g^k 을 공개함으로써 검증자에 대한 부인봉쇄 서명을 일반 서명으로 전환한다.

단계 6 : 검증자는 도전값 a, b 를 서명자에게 전송한다.

단계 7 : 서명자는 a, b 를 이용해서 검증자의 도전 ch 를 인증한다.

$$ch \equiv r^{a\cdot(m_h+s)} \cdot y^{r\cdot b} \pmod{p}$$

단계 8 : 서명자는 g^k 을 공개함으로써 검증자에 대한 부인봉쇄 서명을 일반 서명으로 전환한다. 검증자는 다음과 같이 서명 검증을 함으로써 메시지 m 에 대한 디지털 서명을 확인한다.

$$g^{k\cdot(m_h+s)} \equiv y^r \pmod{p}$$

3. 부인 프로토콜

검증자는 응답 rsp 의 인증에 실패할 경우에 서명자가 부정하는 것인지 서명이 잘못된 것인지 확인해야 한다. 단계 1, 2, 3, 4, 5는 서명 확인 프로토콜과 같고 단계 5에서 검증에 실패한 경우에는 다음과 같은 부인 프로토콜이 수행된다.

단계 6 : 검증자는 다음 조건을 만족하는 임의의 난수 c, d 를 선택해서 서명자에게 전송할 도전

ch' 을 생성한다.

$c,\ d \in Z_{p-1},\ a \cdot d \not\equiv b \cdot c \pmod{p-1}$

$$ch' \equiv r^{c \cdot (m_h + s)} \cdot y^{r \cdot d} \pmod{p}$$

단계 7 : 서명자는 검증자에게 다음과 같이 응답 rsp' 을 전송한다.

$$rsp' \equiv ch'^{x^{-1}} \pmod{p}$$

단계 8 : 검증자는 응답 rsp , rsp' 을 이용해서 다음 식을 계산한다.

$$R_1 \equiv (rsp \cdot g^{-r \cdot b})^c \pmod{p}$$

$$R_2 \equiv (rsp' \cdot g^{-r \cdot d})^a \pmod{p}$$

단계 9 : R_1 과 R_2 를 비교하여 서명자의 부정인지 서명이 잘못된 것인지 확인한다.

$R_1 = R_2$: 서명이 잘못된 것이다.

$R_1 \neq R_2$: 서명자가 올바른 서명에 대해서 부인을 하는 경우이다.

IV. 부인봉쇄 성질 분석

제안한 서명 기법의 부인봉쇄 성질에 대해서 분석한다. 정리 4.1과 4.2는 제안한 부인 프로토콜의 정당성을 입증한다. 정리 4.1은 서명자의 부정을, 정리 4.2는 서명이 잘못됐음을 증명한다.

[정의 2] 메시지 m 에 대한 올바른 서명 $(r,\ s)$ 와 잘못된 서명 $(r',\ s)$ 는 다음과 같다.

○ 메시지 m 에 대한 올바른 서명 $(r,\ s)$

$$r \equiv m_h^k \pmod{p}$$

$$k \cdot (m_h + s) \equiv x \cdot r \pmod{p-1}$$

○ 메시지 m 에 대한 잘못된 서명 $(r',\ s)$

$$r' \equiv m_h^{k'} \pmod{p}$$

$$k' \cdot (m_h + s) \not\equiv x \cdot r' \pmod{p-1}$$

$$k' \cdot (m_h + s) \equiv x' \cdot r' \pmod{p-1},\ (x' \neq x)$$

[정리 4.1] 올바른 서명에 대해서 서명자가 부인하는 경우에 부인 프로토콜을 통해서 서명자의 부정을 입증할 수 있다.

(증명) 메시지 m 에 대한 올바른 서명 $(r,\ s)$ 는 정의 2와 같다. 검증자는 다음과 같이 서명 $(r,\ s)$ 에 대한 도전을 생성한다.

$$ch \equiv r^{(m_h + s) \cdot a} \cdot y^{r \cdot b} \pmod{p}$$

서명자는 서명 $(r,\ s)$ 를 부인하기 위해서 다음과 같이 잘못된 응답 r_1 을 생성한다. t 는 Z_{p-1} 상에서 선택된 임의의 정수이다.

$$r_1 \equiv ch^t \equiv m_h^{x \cdot r \cdot a \cdot t} \cdot g^{x \cdot r \cdot b \cdot t} \pmod{p}$$

$$r_1 \not\equiv m_h^{r \cdot a} \cdot g^{r \cdot b} \pmod{p}$$

검증자는 부인 프로토콜을 수행하여 $(c,\ d)$ 에 대한 도전을 생성하고 응답 r_2 를 수신한다.

$$ch' \equiv r^{(m_h + s) \cdot c} \cdot y^{r \cdot d} \pmod{p}$$

$$r_2 \equiv ch'^{\,t} \equiv m_h^{x \cdot r \cdot c \cdot t} \cdot g^{x \cdot r \cdot d \cdot t} \pmod{p}$$

$$r_2 \not\equiv m_h^{r \cdot c} \cdot g^{r \cdot d} \pmod{p}$$

검증자는 서명자의 부정인지 잘못된 서명인지 확인하기 위해서 다음과 같이 R_1 과 R_2 를 계산하고 두 값을 비교한다.

$$R_1 \equiv (r_1 \cdot g^{-r \cdot b})^c \pmod{p}$$

$$\equiv m_h^{x \cdot r \cdot a \cdot c \cdot t} \cdot g^{(x \cdot r \cdot b \cdot t - r \cdot b) \cdot c} \pmod{p}$$

$$R_2 \equiv (r_2 \cdot g^{-r \cdot d})^a \pmod{p}$$

$$\equiv m_h^{x \cdot r \cdot a \cdot c \cdot t} \cdot g^{(x \cdot r \cdot d \cdot t - r \cdot d) \cdot a} \pmod{p}$$

Z_{p-1} 상에서 선택된 난수 $a,\ b,\ c,\ d$ 는 검증자가 생성한 것으로 서명자는 난수 값을 모르므로 R_1 과 R_2 를 같게 할 수 없다. Ⅲ장 3 절의 부인 프로토콜에서

서명자가 올바른 서명에 대해서 부인하는 경우에 R_1 과 R_2 는 서로 다른 값을 갖게 된다. Q.E.D.

[정리 4.2] 서명이 잘못됐음을 부인 프로토콜을 통해서 입증한다.

(증명) 메시지 m 에 대한 잘못된 서명 (r', s) 는 정의 2와 같다.

검증자는 다음과 같이 잘못된 서명 (r', s) 에 대한 도전 ch 를 생성하고 서명자에게 전송한다.

$$ch \equiv r'^{(m_h+s)\cdot a} \cdot y^{r'\cdot b} \pmod{p}$$

서명자는 잘못된 서명 (r', s) 에 대한 응답 r_1 을 생성하고 검증자에게 전송한다.

$$r_1 \equiv ch^{x^{-1}} \equiv m_h^{k'\cdot(m_h+s)\cdot a\cdot x^{-1}} \cdot g^{r'\cdot b} \pmod{p}$$

$$r_1 \not\equiv m_h^{r'\cdot a} \cdot g^{r'\cdot b} \pmod{p}$$

$$(\because\ k'(m_h+s) \not\equiv xr' \pmod{p-1})$$

검증자는 부인 프로토콜을 수행하여 (c, d) 에 대한 도전을 생성하고 응답 r_2 를 수신한다.

$$ch' \equiv r'^{(m_h+s)\cdot c} \cdot y^{r'\cdot d} \pmod{p}$$

$$r_2 \equiv ch'^{x^{-1}}$$

$$\equiv m_h^{k'\cdot(m_h+s)\cdot c\cdot x^{-1}} \cdot g^{r'\cdot d} \pmod{p}$$

$$r_2 \not\equiv m_h^{r'\cdot c} \cdot g^{r'\cdot d} \pmod{p}$$

$$(\because\ k'(m_h+s) \not\equiv xr' \pmod{p-1})$$

검증자는 서명자의 응답 r_1 과 r_2 를 이용하여 다음 식을 계산한다.

$$R_1 \equiv (r_1 \cdot g^{-r'\cdot b})^c$$

$$\equiv m_h^{k'\cdot(m_h+s)\cdot a\cdot c\cdot x^{-1}} \pmod{p}$$

$$R_2 \equiv (r_2 \cdot g^{-r'\cdot d})^a$$

$$\equiv m_h^{k'\cdot(m_h+s)\cdot a\cdot c\cdot x^{-1}} \pmod{p}$$

R_1 과 R_2 가 같으므로 서명이 잘못됐음을 알 수 있다. Q.E.D.

V. 효율성 분석 및 응용

제안한 서명 기법과 Boyar의 서명 기법[4]을 비교 분석하고 제안한 서명 기법의 확장 및 응용에 대해서 기술한다. 각 서명 기법의 효율성을 통신 단계 수, 서명 크기 및 공개키 크기 측면에서 비교한다.

1. 효율성 분석

표 1. 제안한 서명 기법과 Boyar의 서명 기법 비교

	Boyar의 서명기법	제안한 서명기법
통신 단계 수(서명확인 프로토콜)	4	2
서명 크기	3n	2n
공개키 크기	5n	3n

[표 1]은 제안한 전환 부인봉쇄 서명 기법과 기존의 서명 기법을 통신 단계 수, 서명 크기, 공개키 크기 측면에서 비교 분석한 결과이다. 각 서명 기법에 사용된 법 p 는 n 비트 크기의 큰 소수로 법 p 상에서의 이산 대수 문제가 계산상 불가능 하다고 가정한다.

전환 부인봉쇄 서명 기법은 일반 서명 기법과 달리 서명자의 서명만 가지고는 검증자가 서명의 정당성을 확인할 수 없다. 서명자와 검증자 간에 서명 확인을 위한 도전/응답 프로토콜이 반드시 필요하다. 따라서 서명 확인 프로토콜의 통신 단계 수가 전체 서명 기법의 효율성에 큰 영향을 미치며 통신 단계 수가 적을수록 실용적이다.

서명 확인을 위한 서명자와 검증자 간의 통신 단계 수를 보면 동시 이산 대수 문제에 기반 한 Boyar의 서명 기법[4]이 4 회로 통신 단계 수가 가장 많다. 제안한 서명 기법은 Chaum이 제안한 부인봉쇄 성질을 만족하도록 El-Gamal 서명식을 변형함으로써 Chaum의 서명 기법과 마찬가지로 서명에 대한 도전과 응답의 2 회의 통신

만으로 서명 확인이 가능하다.

공개키 크기를 보면 Boyar의 기법은 서명 전환을 위한 파라미터 z 에 대한 공개값 g^z 이 추가됨으로써 서명 수행을 위해 필요한 공개키 개수가 가장 많다.

제안한 전환 부인봉쇄 서명 기법은 통신 단계 수, 키 크기, 서명 크기 측면에서 Boyar의 기법과 비교하여 효율성이 좋음을 보여준다. Chaum의 기법은 부인봉쇄 서명 기법으로 동일한 메시지에 대해서 항상 동일한 서명을 생성하게 되는 단점이 있지만, 제안한 기법과 Boyar의 기법은 동일한 메시지에 대해서 서로 다른 서명을 생성할 수 있으며, 부인봉쇄 서명을 일반 서명으로 전환할 수 있는 특성을 갖춤으로써, 보다 폭 넓은 영역에 적용될 수 있는 장점이 있다.

2. 확장 및 응용

제안한 전환 부인봉쇄 서명 기법은 Ⅲ장에서와 같이 El-Gamal 서명식을 변형하여 부인봉쇄 성질을 만족하도록 한 것으로써, [표 1]에서와 같이 통신 단계 수를 줄인 효율적인 서명 방법이다. 따라서 여러 서명자의 서명을 필요로 하는 다중서명 방식으로 확장할 경우에 서명 확인 단계에서 서명자들과 검증자 간에 도전/응답 프로토콜을 순차적으로 한 번만 수행하면 된다. 부인봉쇄 다중서명은 서명자 모두의 동의 없이는 서명을 확인할 수 없는 방법으로, 디지털 콘텐츠에서의 공동 저작권 보호 기법으로 적용될 수 있다. 다중서명 생성 프로토콜을 통해서 디지털 콘텐츠에 대한 공동 저작권을 생성하고 저작권 정보를 워터마킹한다. 온라인을 통하여 공동 저작된 디지털 콘텐츠 배포 시에 다중서명 확인 프로토콜을 이용하여 모든 저작자들의 동의 하에서만 워터마킹된 저작권을 검증할 수 있도록 함으로써, 공동 저작자들에게 공통의 권리를 보장할 수 있다. 저작자들 간에 분쟁 발생 시에는 부인 프로토콜을 통해서 저작자의 잘못인지 저작권 정보가 잘못된 것인지 확인할 수 있다.

Ⅵ. 결 론

본 논문에서는 El-Gamal 서명식을 변형하여 부인봉쇄 성질을 만족하고 부인봉쇄 서명을 일반 서명으로 전환할 수 있는 디지털 서명 기법을 제안하였다. 제안한 전환 부인봉쇄 서명 기법은 동일한 메시지에 대해서 서로 다른 서명을 생성할 수 있으며 기존의 Boyar의 기법과 비교하여 서명 확인 프로토콜에서의 통신 단계 수, 공개키 크기 및 서명 크기를 줄인 효율적인 프로토콜이다. 제안한 서명 기법의 부인봉쇄 성질에 대해서 분석하였으며 부인봉쇄 다중서명으로의 확장 및 응용에 대해서 기술하였다.

참 고 문 헌

[1] D.Chaum, "Undeniable Signatures," Advances in Cryptology, Proceedings of CRYPTO'89, Springer-Verlag, pp.212-216, 1990.

[2] W.Diffie and M.E.Hellman, "New Directions in Cryptography," IEEE Transactions on Information Theory, Vol.IT-22, No.6, pp.644-654, 1976.

[3] T.Elgamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Transactions on Information Theory, Vol. IT-31, No.4, pp.469-472, 1985.

[4] I.B.D.J.Boyar, D.Chaum and T.P.Pedersen, "Convertible Undeniable Signatures," Advances in Cryptology, Proceedings of Crypto90, pp.189-205, 1991.

[5] M. M. P. Horster and H. Petersen. Blind multisignature schemes and their relevance for electronic voting. Proceedings of COMPSAC'95, pp.149-155, 1995.

[6] T. P. Pedersen, "Distributed provers with applications to undeniable signatures," Advances in Cryptology, Proceedings of Eurocrypt'91, LNCS 547, pp.221-242, 1991.

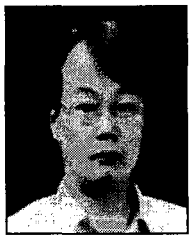
[7] P. S. M. Hellman, "An improved algorithm for computing logarithms over gf(p) and its cryptographic significance," IEEE Transactions

on Information Theory, IT-24:106.110, 1978.

[8] S.H.Yun, and S.J.Lee, "An electronic voting scheme based on undeniable blind signature scheme," Proceedings of IEEE 37th carnahan conference on Security Technology, pp.163-167, 2003.

저 자 소 개

윤 성 현(Sung-Hyun Yun) 정회원



- 1992년 2월 : 고려대학교 컴퓨터학과(이학사)
- 1994년 2월 : 고려대학교 컴퓨터학과 일반대학원(이학석사)
- 1997년 2월 : 고려대학교 컴퓨터학과 일반대학원(이학박사)
- 1998년 3월~2002년 2월 : LG 전자/정보통신 중앙연구소 선임연구원
- 2002년 3월~현재 : 천안대학교 정보통신학부 조교수

<관심분야> : 콘텐츠 보호, 전자상거래, 정보보호

한 군 희(Kun-Hee Han) 종신회원

- 1989년 2월 : 충북대학교 컴퓨터공학과(공학사)
- 1994년 8월 : 경남대학교 컴퓨터공학(공학석사)
- 2000년 8월 : 충북대학교 컴퓨터공학과(공학박사)
- 1989년 1월~1994년 12월 : 대우정보시스템 연구원
- 1995년 3월~2000년 12월 : 대천대학 전기전자컴퓨터학부 조교수
- 2001년 3월~현재 : 천안대학교 정보통신학부 조교수

<관심분야> : 콘텐츠보호, 웹시스템 개발