Journal of KIIT. Vol. 16, No. 7, pp. 67-75, Jul. 31. 2018. pISSN 1598-8619. eISSN 2093-7571 67
http://dx.doi.org/10.14801/jkiit.2018.16.7.67

강한 검증자 지정 은닉 서명 방식의 설계와 분석

김 영 설*

Design and Analysis of a Strong Designated Verifier Blind Signature Scheme

Young-Seol Kim*

이 논문은 2017학년도 동양미래대학교 학술연구과제 연구비 지원에 의하여 연구되었음

요 약

본 논문에서는 강한 검증자 지정 은닉 서명 방식이라는 특수 전자 서명 방식을 제안한다. 검증자 지정 은닉 서명 방식은 검증자 지정 서명과 은닉 서명 방식을 결합한 서명 방식이다. 즉, 제안하는 서명은 검증자 지정 서명의 특성과 은닉 서명의 특성을 모두 가진다. 이 서명에서 오직 검증자로 지정된 주체만 서명의 정당성을 검증할 수 있고, 서명자 생성자는 생성된 서명과 메시지의 연관성에 대해 알지 못하게 된다. 또한, 이전의 연구와는 달리 지정된 검증자는 제3자에게 그 서명의 참임을 납득시킬 수 없다. 본 논문에서는 제안하는 강한 검증자 지정 은닉 서명 방식이 요구하는 안전성에 관한 모든 요구사항에 대해 만족함으로써 안전하다는 것을 보인다.

Abstract

In this paper, we propose special-purpose digital signature scheme, strong designated verifier blind signature scheme. A designated verifier blind signature is a digital signature scheme which combines the properties of designated verifier signature scheme and blind signature. The proposed signature has the advantage of the strong designated verifier and blind signature scheme. In the signature scheme, only designated verifier can prove the validity of a signature and the signer cannot link the own view with the message and signature. And, we show the proposed scheme is secure because the proposed scheme satisfies all signature security properties.

Keywords
digital signature, bind signature, designated verifier signature, public key cryptography

* 동양미래대학교 컴퓨터소프트웨어공학과
- ORCID: https://orcid.org/0000-0002-5384-7008

· Received: Apr. 25, 2018, Revised: Jul. 09, 2018, Accepted: Jul. 12, 2018
· Corresponding Author: Young-Seol Kim
Dept. of Computer Software Engineering of Dongyangmirae University
Tel.: +82-2-2610-5230, Email: youngkim@dongyang.ac.kr

Ⅰ. 서 론

Jakobsson 등은 1996년 검증자 지정 증명 방식이라는 새로운 암호 프로토콜을 제안하였다[1]. 이 방식에서는 증명자가 어떤 명제가 참임을 지정된 검증자에게 확신시킬 수 있으며 그 지정된 검증자가 제삼자에게 해당 명제가 참이라는 것을 증명할 수 없게 할 수 있다. 즉, 지정된 검증자만 해당 명제가 참임을 검증할 수 있다. 이것은, 지정된 검증자만이 메시지에 대한 위조의 서명의 생성이 가능하기 때문이다.

Jakobsson 등은 블랙메일링과 마피아 공격을 방지할 수 있는 새로운 서명 방식인 비-대화형 검증자 지정 증명 방식을 제시하였다[2]-[4]. 그런데 Wang은 Jakobsson 등의 방식에 대해 안전하지 않다고 지적하였는데, 그것은 부정한 서명자가 지정된 검증자를 속일 수 있는 방법이 있기 때문이라고 주장하였다[5]. 그리고, 2003년 Saeednia 등은 이러한 문제를 개선하여 안전하고 강한 검증자 지정 서명 방식을 제안하였다[6]. 이 서명은 제3자가 지정된 검증자의 개인키를 알고 있어도 그 서명의 정당성을 검증할 수 없다.

또 다른 특수 전자 서명으로서, D. Chaum은 1982년에 은닉서명이라는 새로운 서명 방식을 제안하였고[7] 최근까지 그것의 변형 은닉 서명 방식들이 제안되어 왔다[8][9]. 이 서명을 이용하여 사용자는 서명이나 메시지에 대해 아무런 정보도 알려주지 않는 상태에서 자기가 원하는 메시지에 대해 서명자의 서명을 얻을 수 있다. 이러한 은닉서명은 일반적인 전자 서명의 안전성 요구사항인 위조불가능성과 익명성, 불추적성 등을 만족한다.

이 논문에서는 강한 검증자 지정 은닉 서명 방식이라는 전자 서명 방식을 제안한다. 이 서명 방식은 검증자 지정 서명 방식과 은닉 서명 방식을 결합한 형태이다. 따라서 이 서명에서는 서명자가 검증자를 지정하여 지정된 검증자만 서명을 검증할 수 있게 할 수 있고, 검증자는 서명자에게 메시지를 알려 주지 않고 서명을 받을 수다. 그리고 지정된 검증자는 서명을 받은 뒤에 제3자에게 해당 메시지와 서명이 참임을 증명할 수 없게 된다.

이 서명 방식은 검증자 지정 서명과 은닉 서명의 모든 안전성 요구사항을 만족시킨다. 이 논문에서는 Schnorr의 은닉 서명과[10] Wang의 강한 검증자 지정 대리 서명 방식의[11] 일부분을 이용하였다.

본 논문에서 제안하는 서명 방식은 Kim의 수신자 지정 은닉 서명 방식[12]의 보다 발전된 형태이다. 이전의 검증자 지정 은닉 서명 방식은 지정된 검증자가 제3자에게 자신의 비밀키를 공개하면 서명의 정당성을 납득시킬 수 있는 방식이었다. 따라서 지정된 검증자만이 서명을 확인하는 것이 아니라, 경우에 따라서는 제3자도 서명을 확인할 수 있었다. 본 논문에서 제안하는 강한 검증자 지정 은닉 서명 방식은 위의 약점을 보완하여 지정된 검증자가 자신의 비밀키를 제3자에게 공개하더라도 서명의 정당성을 확신시킬 수 없도록 할 수 있다. 따라서 보다 강한 검증자 지정 은닉 서명 방식이라고 할 수 있다.

본 논문의 구성은 다음과 같다. 1장의 서론에 이어 2장에서 제시하는 검증자 지정 은닉 서명을 위한 여러 계산적인 가정(Computational Assumptions)과 표기법(Notations)을 설명한다. 이어, 3장에서 제시하는 서명 방식과 관련있는 연구를 소개한다. 4장에서는 새로운 형태의 전자 서명인 강한 검증자 지정 은닉 서명을 소개한다. 5장에서는 제시하는 새로운 서명의 안전성을 논하며, 6장에서는 제시하는 서명의 응용으로 모바일 환경에서의 전자 투표 시스템을 제시한다. 7장에서는 제안하는 서명 방식과 이전의 서명 방식의 효율성을 비교 분석한다. 8장에서는 결론을 도출한다.

Ⅱ. 기본 사항

2.1 가정

제안하는 서명 방식의 안전성 증명을 위해 다음과 같이 알려져 있는 여러 계산적으로 해결하기 어려운 문제들을 활용한다. 아래의 가정들에 대한 자세한 기술은 [13][14]를 참조한다.

가정 1: 이산로그(Discrete Logarithm) 가정.

$G_q = < g >$를 위수가 q인 생성원 g에 의해 생성되는 순환적 곱셈군이라고 할 때, 입력 $(g, g^x) \in G_q^2$ $(x \in_R Z_q)$에 대해 무시할 수 없는 확률로 x를 계산하는 확률적 다항식 시간 알고리즘이 존재하지 않는다.

2.2 표기법

본 논문에서 제시하는 서명의 자세한 표기를 위해 다음과 같이 기호를 정의한다.

- p, q: 두 개의 큰 소수, $q \mid p-1$
- g: 위수가 q인 Z_p^*의 생성자
- x_u, y_u: 참가자 U의 비밀키와 공개키, $y_u = g^{x_u}$
- H(): 공개된 암호학적 해쉬 함수
- ||: 문자열 결합

III. 관련 연구

2005년 Guilin Wang은 새로운 검증자 지정 대리 서명 방식을 제안하였다[11]. 이 장에서는 Wang의 서명을 간단히 기술한다. 또한, Schnorr의 은닉 서명 방식에 대해 살펴본다[10][15].

3.1 Wang의 강한 검증자 지정 대리 서명 방식

이 절에서는 Wang의 강한 검증자 지정 대리 서명[11]의 검증자 지정 대리 서명의 생성 부분과 검증 부분만을 살펴본다. 그 내용은 다음과 같다.

<검증자 지정 대리 서명 생성 단계>

대리서명자는 먼저 대리위임장 m_w를 가지고 메시지 m에 서명을 생성하기 위해 다음과 같이 한다. 대리서명자는 먼저 임의의 값 $k \in_R Z_q^*$와 $t \in_R Z_q^*$를 선택하고 다음과 같이 (r, c, s)를 계산한다.

$$\begin{aligned} r &= y_C^k \bmod p, \\ c &= H(m, m_w, r) \bmod q, \\ s &= kt^{-1} - x_P c \bmod q. \end{aligned} \tag{1}$$

그리고 대리 서명자는 지정된 검증자에게 메시지 m과 대리 서명 $\sigma = (m_w, r_P, c, s, t)$를 보낸다.

<대리서명 검증 단계>

대리서명 σ을 증명하기 위해 지정된 검증자는 다음과 같이 한다.

(1) 메시지 m이 대리위임장 m_w에 적합한지 확인한다. 메시지 m이 대리위임장 m_w에 적합하지 않다면 검증 과정을 더 이상 진행하지 않고, 아니라면 계속한다.

(2) 원서명자와 대리서명자의 신원을 확인하여 대리위임장 m_w에 위배되지 않는지 확인한다. 역시 위배된다면 검증 과정을 멈추며, 그렇지 않다면 계속한다.

(3) r과 대리서명 공개키 y_P를 아래와 같이 계산하여 복구한다.

$$y_P = (y_A y_B)^{H(m_w, r_P)} r_P \bmod p \tag{2}$$

(4) 대리서명 σ가 다음 식을 만족하면 메시지 m에 대한 정당한 대리서명으로 받아들인다.

$$\begin{aligned} &H(m, m_w, \bar{r}) = c, \\ &\bar{r} = (g^s y_P^c)^{t x_C} \bmod p \end{aligned} \tag{3}$$

3.2 Schnorr의 은닉 서명 방식

Schnorr가 제시한 은닉 서명은 아래와 같다[15].

서명자는 $\bar{k} \in_R Z_q^*$를 선택하고 $\bar{r} = g^{\bar{k}} \bmod p$를 계산한다. 그리고 $\bar{r}$을 검증자에게 전달한다. 은닉 서명의 생성을 위하여 검증자는 임의의 수 $\alpha, \beta \in_R Z_q$를 선택하고 $\bar{c} = H(\bar{r} g^{\alpha} y^{\beta}, m) + \beta \bmod q$를 계산하여 서명자에게 $\bar{c}$를 되돌려준다. 서명자는 $\bar{s} = \bar{k} + x\bar{c} \bmod q$를 계산하고 $\bar{s}$를 검증자에게 보낸다. 검증자는 $s = \bar{s} + \alpha \bmod q$와 $c = \bar{c} - \beta \bmod q$를 계산하고 (s, c)를 메시지 m의 은닉 서명으로 삼는다.

다음으로 검증자는 아래와 같이 은닉 서명의 정당성을 검증한다.

$$c = H(g^s y_P^{-c} \bmod p, m) \bmod q \quad (4)$$

Ⅳ. 제안하는 강한 검증자 지정 은닉 서명 방식

이 논문에서 제안하는 강한 검증자 지정 은닉 서명 방식은 어떠한 경우에도 제3자는 서명을 검증할 수 없도록 설계되어 있다. 다시 말해서 지정된 검증자가 자신의 개인키를 공개하는 일이 발생하더라도 지정된 검증자가 아닌 제3자는 서명을 정당성을 확신할 수 없다. 그것은 제3자는 지정된 검증자가 검증식을 만족할 수 있는 또 다른 서명을 시뮬레이션하여 생성할 수 있다는 것을 알기 때문이다.

제안하는 강한 검증자 지정 은닉 서명은 아래와 같은 단계로 구성된다.

- 준비 단계: 서명자 Alice와 지정된 검증자 Bob은 자신들의 개인키와 공개키 쌍을 생성한다. 일반적인 전자 서명 방식의 키 생성 방식으로 이 키들을 생성한다.
- 은닉 단계: 지정된 검증자 Bob은 임의로 은닉 인자를 선택하고 그것을 이용해 메시지를 은닉하여 서명자에게 전달한다.
- 검증자 지정 은닉 서명 생성 단계: 서명자 Alice는 수신한 은닉된 메시지에서 자신의 서명을 생성하고 지정된 검증자에게 다시 보낸다.
- 역은닉 및 검증 단계: 지정된 검증자 Bob은 역은닉 과정을 수행하고 은닉되지 않은 일반적인 서명인 σ를 생성한다. 그리고 메시지 m에 대한 서명 σ의 검증을 수행한다.

제안하는 강한 검증자 지정 은닉 서명은 위의 네 단계로 구성된다. 그리고 제안하는 서명은 앞에서 서술한 것처럼 Wang의 강한 검증자 지정 대리 서명[11]의 일부와 Schnorr 은닉 서명[15]을 이용한다.

상세한 기술에 앞서 Alice와 Bob은 위의 단계 중 준비 단계는 미리 진행하였음을 가정한다. 즉, 자신의 개인키와 공개키 쌍을 생성하여 이미 가지고 있고 하자. Alice의 개인키, 공개키 쌍은 (x_A, y_A)이며 $y_A = g^{x_A} \bmod p$ 관계에 있다. 마찬가지로 Bob도 자신의 개인키, 공개키 쌍인 (x_B, y_B)를 생성하여 가지고 있다고 가정하며 그것은 $y_B = g^{x_B} \bmod p$를 만족한다. 다른 값들도 Wang의 서명[11]과 Schnorr의 서명[15]의 값들과 같다.

4.1 제안하는 서명 방식의 은닉 단계

제시하는 서명에서 메시지 m에 대한 검증자 지정 은닉 서명의 생성을 위해 서명자 Alice와 지정된 검증자 Bob은 다음과 같은 프로토콜을 수행한다.

(1) Alice는 임의의 값 $\bar{k} \in_R Z_q^*$와 $t \in_R Z_q^*$를 선택하고 $\bar{r} = g^{\bar{k}} \bmod p$를 계산한다. 다음으로 $(\bar{r}, t)$를 Bob에게 보낸다.

(2) 지정된 검증자 Bob은 메시지 m을 은닉하기 위해 다음과 같이한다. 먼저 Bob은 임의의 값 $\alpha, \beta \in_R Z_q^*$를 선택한다. 여기서 α, β를 은닉 인자라고 부른다. 그리고 Bob은 $r = \bar{r}(g^{\alpha} y_A^{-\beta})^{t x_B} \bmod p$와 $\bar{c} = H(r, m) + \beta \bmod q$를 계산한다. 그리고 Bob은 $\bar{c}$를 Alice에게 되돌려준다.

4.2 제시하는 서명의 검증자 지정 은닉 서명 생성 단계

제시하는 검증자 지정 은닉 서명의 서명 생성 단계는 아래와 같다.

Alice는 Bob으로부터 $\bar{c}$를 수신하면 $\bar{s} = \bar{k} t^{-1} - x_A \bar{c} \bmod q$를 계산한다. 그리고 $\bar{s}$를 Bob에게 보낸다.

4.3 제시하는 서명의 역은닉 및 검증 단계

$\bar{s}$를 전달받으면 지정된 검증자 Bob은 먼저 $s = \bar{s} + \alpha \bmod q$와 $c = \bar{c} - \beta \bmod q$를 계산한다. 최종적으로 Bob은 메시지 m에 대한 서명으로 (s, c, t)를 받아들인다. Bob은 아래의 식이 성립하는지 여부를 확인하여 서명의 정당성을 검증한다.

$$c = H((g^s y_A^c)^{t x_B} \bmod p, m) \bmod q \quad (5)$$

서명이 참이라면 위의 검증식은 아래와 같이 성립한다.

$$
\begin{aligned}
& H((g^s y_A^c)^{tx_B} \bmod p, m) \qquad (6)\\
&= H((g^{(\bar{s}+\alpha)} y_A^{\bar{c}-\beta})^{tx_B} \bmod p, m) \bmod q\\
&= H((g^{(\bar{k}t^{-1}-\bar{c}x_A+\alpha+\bar{c}x_A-x_A\beta)})^{tx_B} \bmod p, m) \bmod q\\
&= H((g^{(\bar{k}t^{-1}+\alpha-x_A\beta)})^{tx_B} \bmod p, m) \bmod q\\
&= H(y_B^{\bar{k}}(g^{\alpha} y_A^{-\beta})^{tx_B} \bmod p, m) \bmod q\\
&= H(\bar{r}(g^{\alpha} y_A^{-\beta})^{tx_B} \bmod p, m) \bmod q\\
&= c \bmod q
\end{aligned}
$$

4.4 제안하는 서명 방식의 서명 시뮬레이션 생성 단계

제안하는 강한 검증자 지정 은닉 서명 방식의 시뮬레이션은 Wang의 검증자 지정 대리 서명[11]의 시뮬레이션과 동일하다. 메시지 m에 대해 Bob은 강한 검증자 지정 은닉 서명을 시뮬레이션의 생성을 위해 $s' \in Z_q$와 $r' \in_R Z_q^*$를 선택한 후 다음과 같이 계산한다.

$$
\begin{aligned}
& r = g^{s'} y_A^{r'} \bmod p, \qquad (7)\\
& c = H(m, r) \bmod q,\\
& l = r' c^{-1} \bmod q,\\
& s = s' l^{-1} \bmod q,\\
& t = l x_B^{-1} \bmod q
\end{aligned}
$$

(s, c, t)는 이제 메시지 m에 대해 시뮬레이션으로 생성된 서명이다. 이것은 다음과 같은 이유로 정당한 서명으로 검증될 수 있다.

$$
\begin{aligned}
(g^s y_A^c)^{tx_B} &= (g^{s'l^{-1}} y_A^c)^{tx_B} \bmod p \qquad (8)\\
&= (g^{s'l^{-1}})^l (y_A^c)^{r'c'^{-1}} \bmod p\\
&= (g^{s'} y_A^{r'}) \bmod p\\
&= r \bmod p
\end{aligned}
$$

위 방식에서 Alice는 지정된 검증자 Bob만이 자신의 개인키 x_B를 가지고 r'로부터 r을 복원할 수 있으며 서명을 검증할 수 있도록 제한받을 수 있다.

그런데 검증식을 확인하려면 지정된 검증자의 개인키 x_B를 알아야 한다. 만약 지정된 검증자 Bob이 제3자에게 $(m, (s, c, t))$를 전달하면서 자신의 개인키 x_B를 공개한다 하더라도 지정된 검증자 Bob은 메시지 m에 대해 시뮬레이션 된 서명을 생성할 수 있으므로 제3자는 이것이 정당한 서명임을 확신할 수 없다. 따라서, 지정된 검증자만 서명을 검증할 수 있으며 제3자는 서명을 검증할 수 없게 된다.

Ⅴ. 제안하는 강한 검증자 지정 은닉서명 방식의 안전성 분석

여기에서는 제시하는 서명 방식의 안전성을 논한다. 앞선 연구의 서명 방식들과 비교하여 본 논문에서 제시하는 검증자 지정 서명 방식과 은닉서명 방식의 안전성 요구사항을 모두 만족시킨다는 점에서 차별성과 장점을 가진다.

본 장에서는 이런 여러 안전성 요구사항에 대해 살펴본다.

정리 1. 제안하는 검증자 지정 은닉서명 방식은 위조불가능성을 만족한다.

증명) 첫 번째로, 지정된 검증자의 서명 위조 행위가 불가능함을 보인다. 서명자 Alice가 도와주지 않고 메시지 m에 대한 서명의 위조를 위해 지정된 검증자 Bob은 검증식 $c = H((g^s y_A^c)^{tx_B} \bmod p, m) \bmod q$를 만족시키는 (s, c)를 구해야만 한다. 먼저, Bob이 위의 검증식을 만족하는 서명을 위조하려 한다고 가정한다. 그러나 우리는 $(g^s y_A^c)^{tx_B} = r \bmod p$가 만족함을 알고 있다. 그리고 Bob은 c를 가지고 있으며 s를 계산한다고 하자. 그런데 가정 1에 의해 이것이 계산적으로 불가능한 문제라는 것은 자명하다. 마찬가지로 만약 Bob이 오직 s만 알고 있다고 해도 c를 계산하는 것은 계산적으로 불가능하는 것도 자명하다.

다음으로, 지정된 검증자 Bob이 서명자 Alice의 개인키 x_A를 알려고 시도한다고 가정하자. 그러면 Bob은 $y_A = g^{x_A} \bmod p$를 이용하여 x_A를 계산하던가 $\bar{s} = \bar{k} + \bar{c} x_A \bmod q$로부터 x_A를 계산해야 한다.

그런데 이것은 역시 이산대수문제를 해결해야 한다는 점에서 계산적으로 불가능에 가까운 문제이다.

따라서 지정된 검증자 Bob이 서명을 위조하는 것은 계산적으로 불가능에 가까우며, 지정된 검증자에 비하여 더 적은 정보를 가진 제 삼자가 서명을 위조하는 것은 훨씬 더 어렵다. 그러므로 제안하는 검증자 지정 은닉 서명은 안전성 요구사항 중 위조 불가능성을 만족한다고 할 수 있다.

정리 2. 새로 제안한 검증자 지정 은닉서명 방식은 검증가능성을 제한적으로 만족한다.

증명) 검증자 지정 은닉 서명의 생성과 검증을 위해 지정된 검증자 Bob은 r'로부터 $\bar{r}=(r')^{x_B^{-1}} \bmod p$을 복원한다. 오직 지정된 검증자 Bob만이 자신의 개인키 x_B를 알고 있기 때문에 $\bar{r}$을 복원할 수 있다. 그러므로 제안하는 검증자 지정 은닉 서명은 지정한 주체만 검증가능성을 제한적으로 만족시킨다.

정리 3. 새로 제안한 검증자 지정 은닉 서명은 부인방지 성질을 만족한다.

증명) 제안하는 검증자 지정 은닉 서명에서는 오직 지정된 검증자만이 자신의 개인키를 이용하여 r'에서 $\bar{r}$을 복원할 수 있으며 역은닉 및 검증과정을 수행할 수 있다. 만약 서명 생성 과정에서 서명자가 $\bar{r}$의 이산로그 값인 $\bar{k}$가 아닌 다른 값을 사용한다고 가정하면 지정된 검증자는 그것을 알 수 있고 서명이 거짓임을 알 수 있다. 그러므로 서명자는 자신이 생성한 서명에 대해 추후 부인할 수 없다.

정리 4. 새로 제안한 검증자 지정 은닉서명 방식은 연결불가능성을 만족한다.

제안하는 서명 과정 프로토콜의 은닉성에 대해 증명하기 위하여 임의의 뷰 ν와 임의의 정당한 메시지-서명 $(m,(s,c))$에 대해 오직 유일한 은닉 인자 α,β가 있다는 것을 증명한다.

만약 그것이 참이라면, 서명자의 뷰 ν와 메시지-서명 쌍은 통계적으로 독립 관계에 있어야 하며 그 서명은 은닉성과 연결불가능성을 만족한다고 할 수 있다.

지정된 검증자 Bob은 은닉 인자 α,β를 임의로 선택할 수 있으므로 서명의 은닉성은 아래와 같다. 만약 메시지 m에 대한 서명 (s,c)가 $\bar{k}$, $\bar{r}=g^{\bar{k}} \bmod p$, $r'=y_B^{\bar{k}}$, $\bar{c}$, $\bar{s}=\bar{k}+\bar{c}x_A \bmod q$로 구성된 뷰 ν와 제시한 서명 프로토콜의 수행 중 생성된 것이면 α,β에 대해 아래 수식들이 만족한다.

$$\begin{aligned} &r=\bar{r}(g^{\alpha}y_A^{\beta})^{tx_B} \bmod p, \\ &\bar{c}=H(r,m)+\beta \bmod q, \\ &s=\bar{s}+\alpha \bmod q, \\ &c=\bar{c}-\beta \bmod q \end{aligned} \tag{9}$$

첫 번째와 두 번째 수식에 의하여 $\bar{c}=H(\bar{r}(g^{\alpha}y_A^{\beta})^{tx_B} \bmod p,m)+\beta \bmod q$가 만족한다. 그리고 세 번째, 네 번째 수식에 의하여 은닉 인자 α,β는 유일하게 아래와 같이 정해질 수 있다.

$$\begin{aligned} &\alpha=s-\bar{s} \bmod q, \\ &\beta=\bar{c}-c \bmod q \end{aligned} \tag{10}$$

위의 두 식을 대입하면 다음과 같다.

$$\bar{c}=H(\bar{r}(g^{s-\bar{s}}y_A^{\bar{c}-c})^{tx_B},m)+\bar{c}-c \bmod q \tag{11}$$

그런데 식 (11)은 다음과 같은 이유로 만족하게 된다.

$$\begin{aligned} &H(\bar{r}(g^{s-\bar{s}}y_A^{\bar{c}-c})^{tx_B},m) \\ &\quad = H((g^{x_B\bar{k}}(g^{s-\bar{k}t^{-1}+x_A\bar{c}-x_A\bar{c}+x_Ac})^{tx_B},m) \\ &\quad = H((g^sy_A^{-c})^{tx_B},m) \\ &\quad = c \qquad \text{(검증식에 의하여)} \end{aligned} \tag{12}$$

그러므로 어떤 임의의 뷰 ν와 임의의 정당한 메시지-서명 $(m,(s,c))$에 대해 오직 유일한 은닉 인자 α,β가 있게 된다. 그러면 서명자의 뷰 ν와 메시지-서명 쌍은 통계적으로 독립이라고 할 수 있으며 결과적으로 제시하는 검증자 지정 은닉 서명은 연결불가능성을 만족한다고 할 수 있다.

Ⅵ. 제안하는 수신자 지정 은닉 서명 방식의 모바일 비밀 투표 시스템에의 응용

본 논문에서 제안하는 강한 수신자 지정 은닉 서명은 서명자가 본인이 직접 서명을 확인할 수 없는 상황에서 서명을 생성함과 동시에 해당 서명을 검증하는 검증자를 지정할 수 있다는 특성이 있다. 이를 이용 하여 모바일 전자 투표 시스템에 응용할 수 있다.

투표자의 투표 행위 내용에 관한 비밀이 보장 되어야 하는 모바일 전자 투표 시스템은 다음과 같이 이루어진다. 투표자는 누구에서 투표하였는지 투표 내용을 포함한 메시지를 제안하는 강한 검증자 지정 은닉 서명 방식의 은닉 기능을 이용하여 모바일 단말기를 통해 지역 선거관리위원회에게 보낸다. 그러면 선거관리위원회는 중앙선거관리위원회 메인 센터로 이 메시지를 보낸다. 그러면 메인 센터는 이 메시지들에 서명을 하며 다시 지역 선거관리위원회에게 되돌려준다. 이 때, 메인 센터는 메시지에 오직 서명만을 할 수 있어야 하며 메시지의 내용, 특 투표자가 누구에게 을 알 수 없다. 또한, 센터는 이 메시지와 서명의 검증을 오직 지역 선거관리위원회만이 할 수 있도록 한다.

이러한 모바일 비밀 전자투표 시스템은 다음을 만족시킨다. 첫째, 서명자로서 중앙 메인 센터는 메시지 내용을 알 수 없기 때문에 누가 어떤 내용으로 투표를 하였는지 알 수 없다. 또한, 지정된 검증자인 지역 선거관리위원회만이 이 서명의 검증이 가능하기 때문에 제삼자의 부정을 근본적으로 차단한다.

제안하는 수신자 지정 은닉 서명 방식은 위의 모바일 비밀 투표 시스템에 완전히 부합한다. 서명자를 중앙 메인 센터로, 지정된 수신자를 지역 선관위로 할 수 있으며 서명자 역할을 하는 투표자들은 단순히 투표 내용을 넣은 메시지를 지역 선관위에게 전달하면 된다.

모바일 전자투표 시스템은 계산량과 전송량의 효율성과 보안성이 매우 중요한 분야로서 이러한 환경에서는 특히 효율적이고 안전성이 검증된 서명 방법을 사용해야 한다. 본 논문에서 제시하는 서명은 안전성과 효율성이 검증되었기 때문에 모바일 환경에 적합하다고 할 수 있다.

Ⅶ. 제안하는 수신자 지정 은닉 서명 방식의 이전 방식과의 효율성 비교 분석 및 비교 평가

이 장에서는 제안하는 강한 검증자 지정 은닉 서명 방식을 이전의 수신자 지정 은닉 서명 방식[12]과 두 가지 경우에 대해 효율성을 비교한다. 첫 번째로는 은닉 단계의 계산량이며, 두 번째는 서명자가 검증자(수신자)를 지정하여 서명을 생성하는 단계의 계산량이다. 이 두 가지 경우에 대해서 연산의 횟수를 비교한 후 실제의 실험 결과를 통해 비교한다. 이 과정을 통해 본 논문에서 제안하는 강한 수신자 지정 은닉 서명이 이전의 수신자 지정 은닉 서명 방식[12]과 비교할 때 보다 효율적임을 보인다. 효율성의 측정과 표기를 위해 다음과 같은 기호를 사용한다.

E: 모듈러 지수승 연산을 수행하는 시간
M: 모듈러 곱셈 연산을 수행하는 시간
I: 모듈러 역수 연산을 수행하는 시간
A: 모듈러 덧셈 연산을 수행하는 시간

(1) 은닉 단계의 계산량 비교

제안하는 강한 검증자 지정 은닉 서명에서 메시지를 은닉하기 위해서는 아래의 식들을 계산하여야 한다.

$$\bar{r} = g^{\bar{k}} \bmod p \tag{13}$$
$$r = \bar{r}(g^{\alpha} y_A^{-\beta})^{tx_B} \bmod p$$
$$\bar{c} = H(r,m) + \beta \bmod q$$

이 과정에 필요한 계산량은 4E+2M이 된다. 같은 방법으로 이전의 수신자 지정 은닉 서명 방식의 은닉 단계의 계산량을 계산해보면 5E+A가 된다. 모듈러 지수승 연산(E)가 모듈러 곱셈 연산(M)과 모듈러 덧셈(A) 연산보다 계산량이 훨씬 크므로 제안하는 강한 검증자 지정 은닉 서명 방식의 은닉 단계가 이전의 수신자 지정 은닉 서명 방식의 은닉 단계보다 효율적이라고 할 수 있다.

(2) 검증자 지정 서명 생성 단계의 계산량 비교

제안하는 강한 검증자 지정 은닉 서명에서 검증자를 지정하여 서명을 생성하기 위해서는 아래의 식들을 계산하여야 한다.

$$\bar{s} = \bar{k}t^{-1} - x_A\bar{c} \bmod q \quad (14)$$

이 과정에서 필요한 계산량은 I+2M+A이다. 같은 방법으로 이전의 수신자 지정 은닉 서명 방식의 은닉 단계의 계산량을 계산해보면 I+2M+2A이므로 이 단계에서도 이전 방식보다 효율적임을 알 수 있다.

다음으로는 실제 실험 데이터를 바탕으로 제안하는 검증자 지정 은닉 서명 방식과 수신자 지정 은닉 서명 방식[12]를 비교 분석한다. 실험은 일반적인 IBM 호환 PC 상에서 제작한 은닉, 서명생성, 역은닉, 검증 단계의 알고리즘을 구현하여 소프트웨어적인 방법을 통해 걸리는 시간을 수치적으로 비교하였다. 의미 있는 실험적 수치를 얻기 위하여 두 가지 모두 일천회의 새로운 서명 생성 및 검증 과정을 수행하였다. 비교 분석 결과는 표 1과 같다.

표 1. 기존 방식과 제안하는 빙식의 성능 비교(단위 초)
Table 1. Performance comparison for existing scheme and proposed scheme (sec)

	Blinding	Signing	Unblinding	Verifying
Proposed Scheme	0.00000112	0.003462	0.000721	0.00742
Previous Scheme	0.00000117	0.004231	0.000914	0.00852

위 표와 같이 제안하는 방식이 기존의 방식보다 효율적임을 알 수 있다. 따라서 제안하는 방식은 기존 방식 대비 장점을 가진다고 할 수 있다.

Ⅷ. 결 론

이 논문에서 우리는 새로운 서명 방식인 강한 검증자 지정 은닉 서명 방식을 제안하였다. 이러한 서명 방식은 기존의 약한 검증자 지정 은닉 서명 방식을 개량하여 지정된 검증자의 일탈 행위를 방지할 수 있는 서명 방식을 제안하였다는 면에서 의미를 가진다. 또한, 제시하는 서명 방식은 검증자 지정 서명 및 은닉 서명의 안전성 요구사항에 대해 모두 만족시킨다는 점에서 안전하다고 할 수 있으며 기존 방식들과 비교하여 차별성을 가진다고 할 수 있다. 더불어, 제안하는 서명 방식은 기존의 서명 방식과 비교할 때 계산량 면에서 효율적이다.

따라서 우리가 제안하는 강한 검증자 지정 은닉 서명은 모바일 환경과 같은 효율성이 크게 중요한 환경에 적합하다고 할 수 있다. 제시하는 서명 방식은 위조불가능성, 제한적인 검증가능성, 부인방지, 연결불가능성의 여러 안전성 요구사항들을 모두 만족시킨다.

References

[1] M. Jakobsson, K. Sako, and R. Impagliazzo, "Designated verfier proofs and their applications", In: EUROCRYPT'96, Springer-Verlag, LNCS, Vol. 1070, pp. 143-154, May 1996.

[2] Y. Desmedt and M. Yung, "Weakness of undeniable signature schemes", In: EUROCRYPT'91, Springer-Verlag, LNCS, Vol. 547, pp. 205-220, Apr. 1991.

[3] M. Jakobsson, "Blackmailing using undeniable signatures", In: EUROCRYPT'96, Springer-Verlag, LNCS, Vol. 950, pp. 425-427, May 1994.

[4] Y. Desmedt, C. Coutier, and S. Begnio, "Special uses and abuses of the Fiat-Shamir passport protocol", In: Crypt'87, Springer-Verlag, LNCS, Vol. 293, pp. 21-39, Aug. 1987.

[5] G. Wang, "An Attack on not-interactive designated verifier proofs for undeniable signatures", Cryptology ePrint archive, http://eprint.iacr.org/2003/243/, Nov. 2003.

[6] S. Saeednia, S. Kremer, and O. Markowitch, "An efficient strong designated verifier signature scheme", ICISC'03, Lecture Notes in Computer Science, Springer Berlin, Vol. 2971, pp. 40-54, Nov. Nov. 2003.

[7] D. Chaum, "Blind signatures for untraceable payments", Crypto '82, pp. 199-203, Plenum Press, pp. 199-203, Jan. 1983.

[8] Young-Seol Kim, "Design and Analysis of a Proxy Blind Signature Scheme with Revocation Protocol", Journal of KIIT, Vol. 11, No. 7, pp. 105-112, Jun. 2013.

[9] Young-Seol Kim, "Design of a New Secure Proxy Blind Signature Scheme", Journal of KIIT, Vol. 9, No. 11, pp. 115-126, Nov. 2011.

[10] C. Schnorr, "Efficient signature generation by smart cards", Journal of Cryptography, Vol. 4, No. 3, pp. 161-174, Mar. 1991.

[11] G. Wang, "Designated-Verifier Proxy Signature Schemes", In: Security and Privacy in the Age of Ubiquitous Computing (IFIP/SEC 2005), Springer, pp. 409-423, May 2005.

[12] Young-Seol Kim and Hyun Sook Rhee,, "Design and Analysis of a Designated Verifier Blind Signature Scheme", Journal of KIIT, Vol. 12, No. 1, pp. 193-200, Jan. 2014.

[13] D. Boneh, "The decision Di±e-Hellman problem", In: Pro-ceedings of the Fhird Algorithmic Number Theoty Sym-posium(ANTS'98), Springer-Verlag, LNCS, Vol. 1423, pp. 48-63, Jun. 1998.

[14] F. Bao, R. H. Deng, and H. Zhu, "Variations of Diffie-Hellman problem", In: Information and Communications Security(ICICS 2003), Springer-Verlag, LNCS, Vol. 2836, pp. 301-312, Oct. 2003.

[15] C. Schnorr, "Security of blind discrete log signatures against interactive attacks", In: Information and Communications Security (ICICS'01), Springer-Verlag,, LNCS, Vol. 2229, pp. 1-12, Nov. 2001.

저자소개

김 영 설 (Young-Seol Kim)

2000년 8월 : 서강대학교 컴퓨터공학과(공학사)
2003년 2월 : 서강대학교 컴퓨터공학과(공학석사)
2008년 2월 : 서강대학교 컴퓨터공학과(공학박사)
2008년 3월 ~ 2012년 2월 : 삼성전자(주) 책임연구원
2012년 3월 ~ 현재 : 동양미래대학교 컴퓨터소프트웨어공학과 조교수