通信情報保護論文誌
第9券 第4號 1999. 12

Meta-ElGamal 기반 메시지 복원 공정 은닉 다중 서명 기법

이형우*

Message Recovery Fair Blind Multi-Signature Scheme Based on Meta-ElGamal Protocol

Hyung-Woo Lee*

요 약

은닉 서명[10]은 서명자의 신분과 메시지 내용에 대한 정보 유출 방지와 함께 익명성 보장을 위해 전자 화폐 시스템에 사용되고 있다. 그러나 완전한 익명성은 전자 화폐에 대한 불법적인 사용 등에 악용될 수 있다. 따라서 필요로 하는 경우 특정 신뢰 센터가 전자 화폐에 대한 공정성을 검증할 수 있어야 한다. 본 연구에서는 Hoster가 제시한 Meta-ElGamal 기법[12]을 분석하여 메시지 복원 기능을 제공하는 공정 은닉 서명 모델에 대해 고찰하고 메시지 복원 기능을 제공하는 개선된 공정 은닉 다중 서명 기법을 제시한다. 본 연구에서 제시하는 기법은 불확정 전송 방식의 특성을 사용하여 신뢰 센터에 의한 공정 검증 및 확인 기능을 제공하는 다중 서명 방식으로 다양한 전자 화폐 시스템에 적용 가능하다.

ABSTRACT

As the blind signature[10] does not reveal any information about the message or its signature, it has been used for preventing the information leakage and for providing the anonymity in secure electronic payment systems. Unfortunately, this perfect anonymity could be misused by criminals as blind signatures prevent linking the withdrawal of money and the payment made by the same customer. Therefore, we should provide publicly verifiable mechanism if it is required for the judge to trace the blackmailed messages. In this paper, we propose a modified blind signature scheme, which additionally provides the role of message recovery after analyzing the existing meta-ElGamal scheme[12] suggested by Horster. And we suggest a new fair blind multi-signature scheme based on the oblivious transfer protocol, with which a judge can publicly verify its fairness and correctness if needed. Proposed scheme can also applicable to the diverse electronic payment applications.

Key word : *Fair Blind Signature, Meta-ElGamal, Oblivious Transfer, Electronic Payment.*

* 천안대학교 정보통신학부, 정보보호 및 전자상거래 연구실

I. 서론

공개키 암호화 방식[1,2]에 기반한 전자 화폐를 구현하기 위해서는 익명성 보장과 이중 지불 방지 기능 등과 같은 안전성이 제공되어야 한다. 그러나, 일반적인 전자 화폐 시스템[3,4,5]인 경우 완전한 익명성을 제공하기 때문에 오히려 악용될 수 있는 소지가 있다. 구체적으로 전자 화폐에서 사용하는 기존의 은닉 서명[10]은 서명자로부터 서명된 메시지에 대한 연관성을 은닉할 수 있는 서명 결과를 생성하므로 전자 화폐 시스템에서 익명성을 제공하는데 사용된다. 그러나 전자 화폐 자체와 이에 대한 서명 결과간의 완전 비연관성을 통해 서명자 신분을 은닉하기 때문에 오히려 전자 화폐에 대한 부정 사용 등과 같이 악용될 수 있다[6,7].

이러한 문제를 해결하기 위해서는 전자 화폐에서 사용하는 은닉 서명 기법이 사용자에 대한 익명성을 제공하면서도 필요할 경우 특정 센터에 의한 검증 및 확인 과정을 제공해야 한다. 결국 전자 화폐에 대해 필요로 하는 경우 공개적인 검증 및 확인 기능을 제공할 수 있는 공정 암호화 시스템[17]에 대한 고찰이 필요하다. 신뢰할만한 센터는 서명자가 생성한 은닉 서명에 대해 필요할 경우에 한해서 어떤 서명자가 생성한 서명인지를 검증할 수 있어야 하고, 이중 사용에 대해 확인할 수 있어야 한다. 이와 같은 특성을 제공하는 공정 은닉 서명(fair blind signature)[18]을 통해 전체 시스템의 신뢰성과 공정성을 향상시킬 수 있다.

본 연구에서는 전자 화폐를 구현하기 위해 필수적인 은닉 서명 기법에 대한 고찰을 통해 개선된 공정 은닉 서명 기법을 제시하고자 한다. 기존의 Meta-ElGamal 기반 은닉 서명 기법[11,12,13,14]을 변형하여 메시지 복원 기능을 지원하는 은닉 서명 모델을 제시한다. 이를 바탕으로 불확정 전송[15,16] 방식(oblivious transfer protocol)의 특성을 사용한 공정 은닉 서명 기법을 제시한다. 제안한 기법은 신뢰 센터에 의한 공정 검증 및 확인 기능을 제공하기 위해 사전 등록 프로토콜을 수행하고 불확정 전송 기법에 기반한 메시지 복원 공정 은닉 서명을 수행한다. 본 연구에서 제시하는 기법은 인터넷 기반 대단위 전자상거래 환경에서 다중 서명자에 의한 은닉 서명을 제공한다. 또한 대단위 분산 컴퓨팅 기반 전자 지불 환경에서 일반 사용자의 전자 화폐에 대해 다중 서명자가 공개 검증 가능한 은닉 서명을 생성할 수 있기 때문에 다양한 응용 분야에 활용 가능하다.

2 장에서는 Meta-ElGamal 기반 메시지 복원 은닉 서명 모델과 일반화 기법을 제시한다. 3 장에서는 메시지 복원 은닉 다중 서명에 대해 고찰하고 이를 바탕으로 4 장에서는 공정 은닉 다중 서명 기법을 제안한다. 5 장에서는 기존의 기법과의 비교 분석 결과를 제시하고 6 장에서는 결론과 향후 연구 방향을 고찰한다.

II. Meta-ElGamal 기반 메시지 복원 은닉 서명

1. 메시지 복원 은닉 서명 모델

Chaum[10]에 의해 제시된 전송자 A와 서명자 B 사이에서의 은닉 서명(blind signature)은 다양한 분야에 접목할 수 있다. 전자 화폐와 관련된 응용 분야에서 메시지 m은 A가 지불할 수 있는 전자 화폐를 의미한다. B에게 전달된 은닉 메시지 m^*과 B에 의해서 생성된 은닉 서명 s^*는 서로 비연관성(unlinkable property)을 지니기 때문에 사용자 A에 대한 익명성을 제공한다. Horster가 제시한 Meta-ElGamal 기법[12]은 이산 대수 문제에 근거하여 메시지에 대해 안전한 은닉 서명을 제공하였다. 본 연구에서는 Horster가 제시한 메타 은닉 서명 기법에 기반하여 메시지 복원 기능을 제공하는 은닉 서명 모델을 제시하고, 공정성을 제공하

는 다중 은닉 서명으로 발전시키고자 한다.

은닉 서명한 메시지에 대한 복원 기능을 제공하는 은닉 서명에 대한 정의는 다음과 같다. 일반적인 은닉 서명 기법과 키 생성 알고리즘은 동일하다. 그러나 대화형 은닉 서명 프로토콜과 검증 알고리즘은 메시지 복원 기능을 제공한다.

【정의1】 메시지 복원 은닉 서명

(SKG, IP_{MR}, Ver_{MR}) .

- SKG - 서명에 필요한 비밀키 및 공개키 (x, y) 를 생성하는 키 생성 알고리즘(signature key generation algorithm).
- IP_{MR} - 서명자와 전송자간의 $(sender(m, y), signer(x))$ 에 해당하고 메시지 복원 기능을 제공하는 대화형 은닉 서명 프로토콜(interactive blind signature protocol). 전송자의 입력은 메시지 m 과 공개키 y 이고 서명자의 입력은 비밀키 x 이다. 서명자는 서명 $s^* = sender(m, y)_{signer(x)}$ 를 전송한다.
- $Ver_{MR}(y, m, s)$ - 서명 검증 알고리즘은 입력 공개키 y , 서명 s 에 대해서 검증 과정에서 메시지 m 과 동일하면 올바른 서명으로 받아들인다.

메시지 복원 기능을 제공하는 은닉 서명 기법에 대한 일반화 과정을 통해서 공정성을 제공하는 은닉 서명 기법에 대해 고찰하고 이를 공정 은닉 서명으로 발전시킬 수 있다.

2. Meta-ElGamal 기반 메시지 복원 은닉 서명의 일반화 단계

은닉 서명 모델에 기반하여 메시지 복원 기능을 제공하는 서명 기법을 검증할 수 있다. 우선 은닉 서명을 위해 큰 소수 p 와 $q|(p-1)$ 을 만족하는 q 및 법 $p-1$ 에 대한 생성자 $g \in Z_p^*$ 를 공개한 후에 서명자는 랜덤 $w^* \in Z_{p-1}$ 에 대한 은닉 파라메터(blinded parameter) $t^* \equiv g^{w^*} \bmod p$ 를 선택하여 w^* 는 비밀로 하고 t^* 를 전송자에게 전달한다. $Z_q^3 \rightarrow Z_q$ 를 만족하는 변수 m, r, s 에 대해 일반적인 함수의 개념으로 각각 A, B, C 로 설정하였을 경우, 전송자는 임의의 두 수 $\alpha, \beta \in Z_q$ 을 사용하여 메시지 $m \in Z_{p-1}$ 에 대해 $r \equiv m (t^*)^{\alpha} g^{\beta} \bmod p$ 를 계산한다. 다시 서명자는 은닉 파라메터 t^* 에 대해서 아래 수식 (1)과 같이 서명 과정을 수행한다.

$$A^* \equiv x \cdot B^* + w^* C^* \bmod q \qquad (1)$$

이때 x 는 서명자의 비밀키에 해당하고 A^*, B^*, C^* 는 A, B, C 에 대한 은닉 파라메터라 할 때 위 식은 $w^* \equiv C^{*-1}(A^* - x \cdot B^*)$ 로 변형할 수 있다. 메시지에 대한 서명이 (m, r, s) 일 경우 서명에 대한 검증은 아래 수식 (2)와 같이 확인할 수 있다.

$$m \equiv g^{AC^{-1}} y^{-BC^{-1}} r \bmod p \qquad (2)$$

또한 일반적으로 [11]에 의해서 아래와 같은 수식이 성립하므로 다음과 같은 정리를 통해서 수식을 만족하는 α, β 는 유일하다는 것을 증명할 수 있다.

$$\begin{aligned} A &\equiv -\alpha A^* C C^{*-1} - \beta C \bmod q \\ B &\equiv -\alpha B^* C^{*-1} C \bmod q \end{aligned} \qquad (3)$$

【정리】 임의의 (m, r, s) 에 대해 $m \equiv g^{AC^{-1}} y^{-BC^{-1}} r \bmod p$ 를 만족하는 유일한 해 α, β 가 존재한다.

$\alpha, \beta \in Z_q$ 을 아래와 같이 정의하자.

$$\begin{aligned} \alpha &\equiv -BC^* B^{*-1} C^{-1} \bmod q \\ \beta &\equiv (-A + A^* B B^{*-1}) C^{-1} \bmod q \end{aligned}$$

이를 $A^* \equiv x \cdot B^* + w^* C^* \bmod q$ 에 적용하면 수식 (4)와 같다.

$$\begin{aligned} \alpha w^* + \beta &\equiv (-BC^* B^{*-1} C^{-1}) w^* + (-A + A^* B B^{*-1}) C^{-1} \\ &\equiv C^{-1}(-A - B(C^* B^{*-1} w^* - A^* B^{*-1})) \\ &\equiv C^{-1}(-A - B((A^* - x \cdot B^*) B^{*-1} - A^* B^{*-1})) \\ &\equiv C^{-1}(-A + B \cdot x) \bmod q \end{aligned} \qquad (4)$$

$$\begin{aligned} m \cdot t^{*\alpha} g^{\beta} &\equiv m \cdot g^{\alpha w + \beta} \equiv m \cdot g^{C^{-1}(-A + Bx)} \\ &\equiv m \cdot g^{-AC^{-1}} y^{BC^{-1}} \equiv r \bmod p \end{aligned}$$ ■

위 수식을 통해 α 와 β 는 유일하다는 것을 증명할 수 있고, 본 연구에서는 이와 같은 Meta-ElGamal 기반 메시지 복원 은닉 서명에 대한 일반화를 통해 변형된

기법으로 발전시키고자 한다.

III. 메시지 복원 은닉 다중 서명 기법

1. 메시지 복원 은닉 다중 서명 모델

제안한 Meta-ElGamal 기반 메시지 복원 은닉 서명 기법을 은닉 다중 서명으로 확장할 수 있다. 키 생성 알고리즘은 다중 서명자에 해당하는 키를 생성한다. 또한 메시지 복원 기능을 제공하는 대화형 은닉 서명 프로토콜을 은닉 다중 서명으로 확대한다.

메시지 복원 기능을 제공하는 일반화된 메타-메시지 서명을 은닉 다중 서명으로 발전시킬 수 있다. 각 서명자 u_i는 $w^*_{u_i} \in Z_{p-1}$를 만족하는 랜덤수에 대해 $t^*_{u_i} \equiv g^{w^*_{u_i}} \bmod p \ (1 \le i \le k)$ 를 생성하여 전송자에게 전달하게 된다. 전송자는 각 서명자로부터 전달받은 $t^*_{u_i}$에 대해서 $t' \equiv \prod_{i=1}^{k} t^*_{u_i} \bmod p$ 를 계산할 수 있고, 각 개인의 비밀키 $x_{u_i} \in Z_{p-1} (1 \le i \le k)$ 에 대한 공개키 $y_{u_i} (1 \le i \le k)$ 에 대해서 r에 대한 $Z_p^2 \rightarrow Z_p$ 계산을 위한 함수를 d라 할 때 아래 수식 (5)를 만족하는 r과 y를 계산한다.

$$r = d(t', m), \quad y \equiv \prod_{i=1}^{k} y_{u_i} \bmod p \qquad (5)$$

이때 $d^{-1}(r, g^{AC^{-1}} y^{-BC^{-1}}) = m$ 을 만족하는 A, B, C에 대해서 서명자 u_i는 아래 수식 (6)과 같은 서명 파라메터 s_{u_i}를 생성하게 된다.

$$A_i \equiv x_{u_i} B_i + w_i C_i \bmod q \qquad (6)$$

A_i, B_i, C_i는 r과 s_{u_i}로부터 선택되므로, $d^{-1}(r, g^{AC^{-1}} y^{-BC^{-1}}) = m$ 는 다음과 같이 변형할 수 있다.

$$\begin{aligned} & d^{-1}(r, g^{AC^{-1}} y^{-BC^{-1}}) \\ & \equiv d^{-1}(r, g^{AC^{-1}} (\prod_{i=1}^{k} y_i^{BC^{-1}}) \bmod p)) \\ & \equiv d^{-1}(r, g^{AC^{-1}} (\prod_{i=1}^{k} g^{-(A_i - C_i u_i) B_i \cdot BC^{-1}}) \bmod p)) \\ & \equiv d^{-1}(r, g^{AC^{-1}} (\prod_{i=1}^{k} g^{-A_i B_i \cdot BC^{-1}} \prod_{i=1}^{k} t_i^{* C_i B_i \cdot BC^{-1}}) \bmod p)) \end{aligned}$$

만일 C_i와 B_i가 서명 파라메터 s_{u_i}에 의존하지 않는다면, $C = C_i$이고 $B = B_i$가 될 것이다. 따라서 위 식은 다음과 같이 변형할 수 있다.

$$\begin{aligned} d^{-1}(r, g^{AC^{-1}} y^{-BC^{-1}}) & \equiv d^{-1}(r, g^{AC^{-1}} (\prod_{i=1}^{k} g^{-A_i C^{-1}} \prod_{i=1}^{k} t_i^*) \\ & \equiv d^{-1}(r, g^{C^{-1}(A - \sum_{i=1}^{k} A_i)} \prod_{i=1}^{k} t_i^* (\bmod p)) \\ & \equiv d^{-1}(r, t') \equiv m \end{aligned}$$

결국 은닉 다중 서명에서도 메시지 복원 기능을 지원할 수 있다.

2. 메시지 복원 은닉 다중 서명 기법 (MR-BMS)

본 연구에서는 Meta-ElGamal 방식에 근간한 메시지 복원 은닉 다중 서명을 제시한다. 은닉 다중 서명은 다중 서명자 B_i가 전송자의 메시지 m에 대해서 은닉 서명을 하는 것을 의미한다. 따라서 다중 서명자 B_i는 각기 자신의 공개키와 비밀키 쌍을 가지고 있으며 임의의 난수 $w^*_{B_i} \in Z_q (1 \le i \le k)$ 를 생성한다. 각 서명자는 $w^*_{B_i}$에 대한 $t^*_{B_i} \equiv g^{w^*_{B_i}} \bmod p \ (1 \le i \le k)$ 값을 전송자에게 전달한다.

전송자는 각 서명자 B_i에게 전달할 메시지를 생성하기 위해서, 메시지 m에 대해 해쉬 함수 $m_i = H(m \| y_{B_i}) \ (1 \le i \le k)$ 를 만족하는 m_i를 생성한다. 각 m_i에 대해 전송자는 B_i에게 r_{B_i}와 $m^*_{B_i}$를 전송한다.

$$\begin{aligned} r_{B_i} & \equiv m_i^{-1} (t^*_{B_i})^{\alpha} (y_{B_i})^{\beta} \bmod p \ (1 \le i \le k) \\ m^*_{B_i} & \equiv \alpha^{-1} \cdot (r_{B_i} - \beta) - t^*_{B_i} \bmod q \ (1 \le i \le k) \end{aligned} \qquad (7)$$

각 서명자 B_i는 자신의 비밀키 x_{B_i}를 사용하여 은닉 서명 수식 (8)과 같이 $s^*_{B_i}$를 다음과 같이 생성하여 전송자에게 전달한

다.

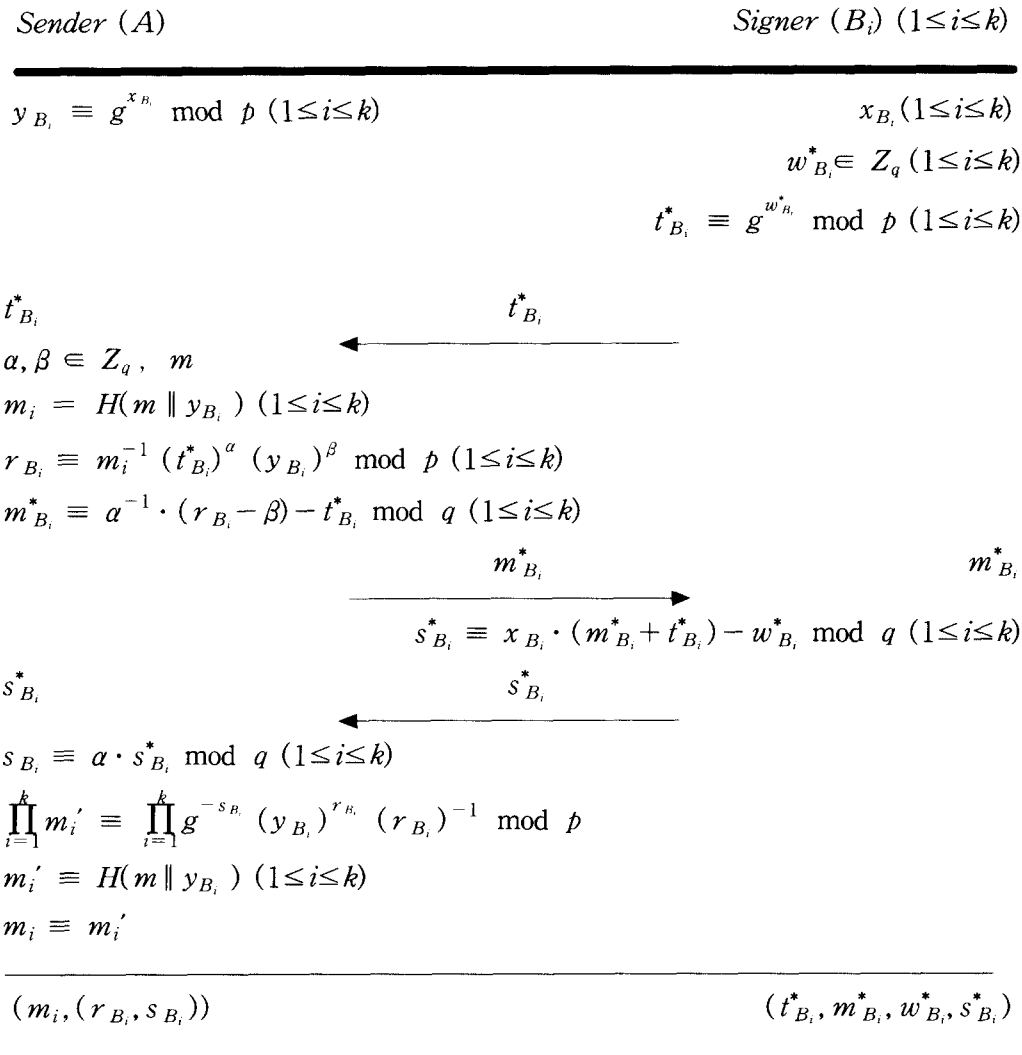
$$s^*_{B_i} \equiv x_{B_i} \cdot (m^*_{B_i} + t^*_{B_i}) - w^*_{B_i} \bmod q (1 \le i \le k) \quad (8)$$

전송자는 아래 수식 (9)와 같이 s_{B_i}를 생성하고 메시지에 대한 검증 단계를 수행한다. 검증 단계는 각 서명자 B_i가 생성한 서명에 대한 확인 단계를 수행하여 m_i'를 계산한다.

$$s_{B_i} \equiv \alpha \cdot s^*_{B_i} \bmod q (1 \le i \le k)$$

$$\prod_{i=1}^{k} m_i' \equiv \prod_{i=1}^{k} g^{-s_{B_i}} (y_{B_i})^{r_{B_i}} (r_{B_i})^{-1} \bmod p \quad (9)$$

각 m_i'에 대해서 해쉬 함수를 적용하여 생성된 $m_i' \equiv H(m \| y_{B_i})$ $(1 \le i \le k)$을 만족할 경우에 대해서 $m_i \equiv m_i'$인 것을 확인할 수 있다. 본 프로토콜은 메시지 복원 기능을 제공하고 다중 서명자에 대한 은닉



(그림 1) 메시지 복원 은닉 다중 서명 기법(MR-BMS)

(Fig. 1) Message recovery blind multi-signature scheme

서명 기능이 가능하다. 구체적인 프로토콜 작동 단계는 아래 (그림 1)과 같다.

$$\prod_{i=1}^{k} m_i' \equiv \prod_{i=1}^{k} g^{-s_{B_i}} (y_{B_i})^{r_{B_i}} (r_{B_i})^{-1} \bmod p$$

에 대한 검증 과정은 아래와 같다.

$$\begin{aligned}
&\prod_{i=1}^{k} g^{-s_{B_i}} y_{B_i}^{r_{B_i}} r_{B_i}^{-1} \\
&\equiv \prod_{i=1}^{k} g^{-(\alpha \cdot s^*_{B_i})} \cdot g^{x_{B_i} \cdot r_{B_i}} \cdot m_i \cdot g^{-w^*_{B_i} \cdot \alpha} \cdot g^{-x_{B_i} \cdot \beta} \\
&\equiv \prod_{i=1}^{k} m_i \cdot g^{-\alpha \cdot s^*_{B_i}} \cdot g^{x_{B_i} \cdot r_{B_i}} \cdot g^{-w^*_{B_i} \cdot \alpha - x_{B_i} \cdot \beta} \\
&\equiv \prod_{i=1}^{k} m_i \cdot g^{-\alpha \cdot (x_{B_i} \cdot (m^*_{B_i} + t^*_{B_i}) - w^*_{B_i})} \cdot g^{x_{B_i} \cdot (r_{B_i} - \beta) - w^*_{B_i} \cdot \alpha} \\
&\equiv \prod_{i=1}^{k} m_i \cdot g^{-\alpha \cdot x_{B_i} \cdot (m^*_{B_i} + t^*_{B_i})} \cdot g^{x_{B_i} \cdot (r_{B_i} - \beta)} \\
&\equiv \prod_{i=1}^{k} m_i \cdot g^{-\alpha \cdot x_{B_i} \cdot \alpha^{-1} \cdot (r_{B_i} - \beta)} \cdot g^{x_{B_i} \cdot (r_{B_i} - \beta)} \\
&\equiv \prod_{i=1}^{k} m_i \bmod p
\end{aligned}$$

IV. 제안한 기법

본 연구에서 제시하는 공정 은닉 서명 기법은 신뢰 센터가 필요로 하는 경우에 서명된 메시지에 대한 공개 검증 단계를 수행할 수 있는 기능을 제공한다. 구체적인 공정 은닉 서명에 대한 등록 프로토콜과 메시지 복원 공정 은닉 서명 기법은 다음과 같다.

1. 공정 은닉 서명을 위한 등록 프로토콜 모델

공정성을 제공하기 위해서는 신뢰 센터에 의해서 공개적 검토 가능한 기능을 제공해야 한다. 따라서 전송자 A는 신뢰 센터에 대한 사전 등록 단계를 수행하여 공정 은닉 서명을 위한 비밀 정보를 할당받는다. 전송자는 신뢰 센터로부터 받은 비밀 정보를 사용하여 서명자에게 전달한다. 서명자는 은닉 서명을 수행한다. 서명자에 의해 은닉 서명된 메시지는 다시 전송자에게 전달된다. 등록 프로토콜 RP 는 다음과 같다.

【정의 2】 공정 은닉 서명을 위한 등록 프로토콜 RP

- RP - 전송자와 신뢰 센터간의 $(sender(\delta, y), judge(x))$ 에 해당하고 공정 은닉 서명에 필요한 비밀 정보를 제공하는 대화형 등록 프로토콜.

전송자의 입력은 자신이 생성한 δ 와 신뢰 센터의 공개키 y_J 이고 신뢰 센터의 입력은 자신의 비밀키 x_J 이다. 신뢰 센터는 등록 결과 $v' = sender(\delta, y_J)_{judge(w, x_J)}$ 를 전송한다. 전송자는 v' 에서 공정 은닉 서명에 사용될 정보 v 를 추출한다. 전송자의 δ, v 와 신뢰 센터의 c, v' 는 공정성을 확인할 수 있는 기본 정보에 해당된다. c 는 신뢰 센터에 의한 공개 검증 정보를 포함하고 있다.

2. 메시지 복원 공정 은닉 서명 모델

본 연구에서 제시한 Meta-ElGamal 기반 메시지 복원 은닉 서명 기법을 공정성을 제공하는 은닉 서명으로 확장할 수 있다. 사전 등록 프로토콜을 수행하여 전송자에 해당하는 키를 할당받고 키 생성 알고리즘을 통해 서명자에 해당하는 키를 생성한다. 또한 메시지 복원 기능을 제공하는 대화형 은닉 서명 프로토콜을 기반으로 공정 은닉 검증 기능을 제공한다.

【정의 3】 메시지 복원 공정 은닉 서명 $(RP, SKG, FIP_{MR}, R, FVer_{MR})$.

- SKG - 사전 등록 프로토콜 RP 에 기반하여 공정 은닉 서명에 필요한 비밀키 및 공개키 (x, y) 를 생성하는 키 생성 알고리즘.
- FIP_{MR} - 전송자와 서명자간의 $(sender(v, m, y), signer(c, x))$ 에 해당하고 메시지 복원 기능을 제공하는 대화형 공정 은닉 서명 프로토콜. 전송자의 입력은 등록 단계에서 생성된 v 와 메시지 m 및 공개키 y 이고 서명자의 입력은 공정 프로토콜을 위한 정보 c 와 서명자의 비밀키 x 이다. 서명자는 서명 $s = sender(v, m, y)_{signer(c,x)}$ 를 전송한다.
- R - 은닉 서명에 대해 연관성을 복구할 수 있는 특성을 제공하는 알고리즘. 연관성 정보를 포함하는 $type_I$ 형태의 r_I 과 $type_{II}$ 형태의 r_{II} 를 생성한다.

  r_I - 서명자의 서명 메시지 (m^*, s^*)

로부터 신뢰 센터 J는 서명자의 서명에 해당하는 전송자의 메시지 (m, s)를 연관지을 수 있다.

r_{II} - 전송자의 메시지와 서명 (m, s)에 대해서 신뢰 센터 J는 해당하는 서명자의 서명 (m^*, s^*)를 서로 연관지을 수 있다.

○ $FVer_{MR}(r, y, m, s)$ - 서명에 대한 공정 검증 알고리즘은 입력으로 연관성 정보 r과 공개키 y을 사용하여 해당하는 서명 정보 s와 메시지 m을 공개적으로 검증한다.

3. 공정 은닉 서명을 위한 등록 단계

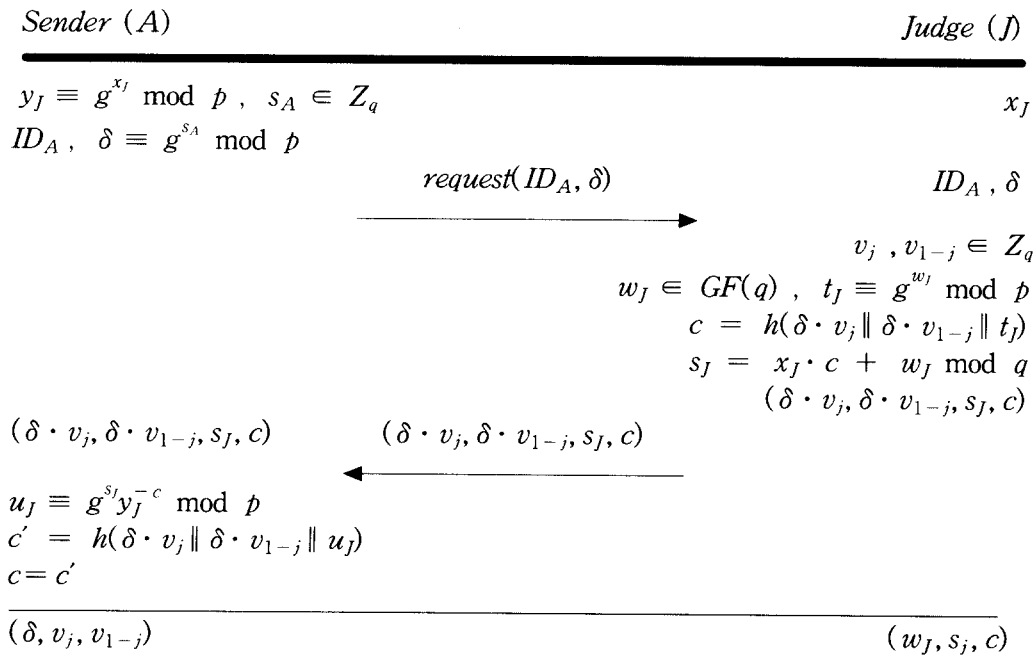
Meta-ElGamal 기반 메시지 복원 은닉 서명 방식에서 공정성을 제공하는 기법으로 발전시킨다. 메시지 복원 기능을 제공하는 은닉 서명 기법에 불확정 전송 방식을 적용하여 공정성 기능을 제공한다. 본 연구에서 제안하는 Meta-ElGamal 기반 메시지 복원 공정 은닉 서명 기법은 우선 신뢰 센터에 대한 등록 단계를 수행한 다음 서명자와의 공정 은닉 서명 단계를 수행한다. 우선 전송자는 신뢰 센터 J에 공정 은닉 서명을 위한 등록 단계를 수행한다. 제안하는 등록 단계에 대한 구체적인 과정은 아래 (그림 2)와 같다.

(증명) $u_J \equiv g^{s_J} y^{-c} \bmod p$ 에 대한 증명

$$u_J \equiv g^{s_J} y^{-c} \equiv g^{x_J \cdot c + w_J} g^{x_J \cdot -c}$$
$$\equiv g^{w_J} \equiv t_J \bmod p$$
$$\therefore c' = h(\delta \cdot v_j \| \delta \cdot v_{1-j} \| u_J)$$
$$= h(\delta \cdot v_j \| \delta \cdot v_{1-j} \| t_J) = c$$

4. Meta-ElGamal 기반 메시지 복원 공정 은닉 서명 기법(MR-FBS)

신뢰 센터에 대한 등록 단계를 거친 후에 전송자와 서명자는 은닉 서명 단계를 수행한다. 본 연구에서는 기존의 은닉 서명 기법에 불확정 전송 기법을 적용하여 공정성을 제공하고자 한다.

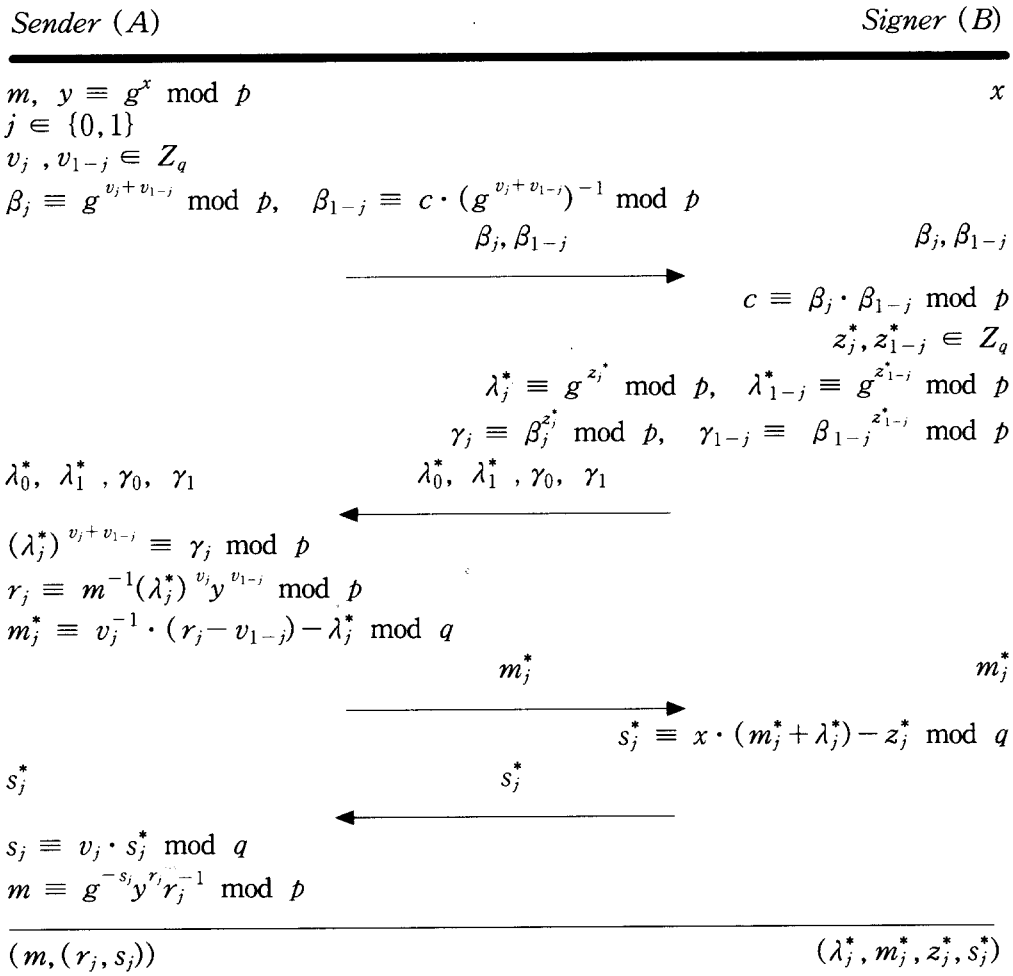


(그림 2) 신뢰 센터 J에 대한 등록 프로토콜
(Fig. 2) Registration protocol on trusted center J

불확정 전송 기법(oblivious transfer: OT)은 A가 B에게 메시지 m 비트를 전달하고자 할 때 $\frac{1}{2}$의 확률로 전달할 경우 A 자신은 어떠한 비트가 전달되었는지 모르는 경우를 의미한다. 구체적으로 A는 B의 공개키 P_B를 사용하여 자신이 가지고 있는 문자열 s_0와 s_1 및 메시지 m을 암호화한 후 B에게 전달한다. B는 자신의 비밀키를 사용하여 복호화 단계를 수행한다. 이때 A는 B가 m 이외에 s_0와 s_1 중에서 어떠한 문자열을 받았는지를 모르는 전송 방식이다. 본 연구에서는 불확정 전송 기법의 특성을 활용하여 신뢰 센터에 의한 공정 검증 기능을 제공하기 위한 하부 구조로 사용한다.

제시하는 불확정 전송 기반 메시지 복원 공정 은닉 서명 기법은 MR-BMS 기법에서 전송자가 등록 단계에서 신뢰 센터로부터 받은 v_j, v_{1-j}를 사용한다. 구체적인 단계는 (그림 3)과 같다.

(증명) $m \equiv g^{-s_j} y^{r_j} r_j^{-1} \bmod p$ 에 대한 은닉 서명 검증.



(그림 3) Meta-ElGamal 기반 메시지 복원 공정 은닉 서명 기법(MR-FBS)
(Fig. 3) Meta-ElGamal based message recovery fair blind signature

$$
\begin{aligned}
& g^{-s_j} y^{r_j} r_j^{-1} \\
& \equiv g^{-(v_j \cdot s^*)} \cdot g^{(x \cdot r_j)} \cdot m \cdot g^{-z_j^* \cdot v_j} \cdot g^{-x \cdot v_{1-j}} \\
& \equiv m \cdot g^{-v_j \cdot s^*} \cdot g^{x \cdot r_j} \cdot g^{-z_j^* \cdot v_j - x \cdot v_{1-j}} \\
& \equiv m \cdot g^{-v_j \cdot (x \cdot (m_j^* + \lambda_j^*) - z_j^*)} \cdot g^{x \cdot r_j} \cdot g^{-z_j^* \cdot v_j - x \cdot v_{1-j}} \\
& \equiv m \cdot g^{-v_j \cdot x \cdot (m_j^* + \lambda_j^*)} \cdot g^{x \cdot r_j - x \cdot v_{1-j}} \\
& \equiv m \cdot g^{-v_j \cdot x \cdot v_j^{-1} \cdot (r_j - v_{1-j})} \cdot g^{x \cdot (r_j - v_{1-j})} \\
& \equiv m \bmod p
\end{aligned}
$$

5. 메시지 복원 공정 은닉 다중 서명 (MR-FBMS)

제시한 공정 은닉 서명을 다중 서명으로 발전시킨다. 전송자가 신뢰 센터에 등록하는 과정은 위에서 제시한 기법과 동일하다. 구체적인 단계는 메시지 복원 공정 은닉 서명 기법과 유사하다. 다만 전송자는 해쉬 함수를 사용하여 메시지를 생성하고, 다중 서명자가 서명을 수행한다. 전송자는 다중 서명된 메시지에 대해 검증하는 과정에서 역시 해쉬 함수를 적용하여 확인한다.

Sender (A)		*Signer* (B_i) $(1 \le i \le k)$
$m,\ y_{B_i} \equiv g^{x_{B_i}} \bmod p$		$x_{B_i} (1 \le i \le k)$
$j \in \{0,1\},\ v_j, v_{1-j} \in Z_q$		
$\beta_j \equiv g^{v_j + v_{1-j}} \bmod p,\ \beta_{1-j} \equiv c \cdot (g^{v_j + v_{1-j}})^{-1} \bmod p$		
	β_j, β_{1-j} $\longrightarrow$	β_j, β_{1-j}
		$c \equiv \beta_j \cdot \beta_{1-j} \bmod p$
		$z^*_{B_i j}, z^*_{B_i 1-j} \in Z_q\ (1 \le i \le k)$
		$\lambda^*_{B_i j} \equiv g^{z_{B_i j}^*} \bmod p,\ \lambda^*_{B_i 1-j} \equiv g^{z^*_{B_i 1-j}} \bmod p$
		$\gamma_{B_i j} \equiv \beta_j^{z^*_{B_i j}} \bmod p,\ \gamma_{B_i 1-j} \equiv \beta_{1-j}^{z^*_{B_i 1-j}} \bmod p$
$\lambda^*_{B_i 0}, \lambda^*_{B_i 1}, \gamma_{B_i 0}, \gamma_{B_i 1}$	$\lambda^*_{B_i 0}, \lambda^*_{B_i 1}, \gamma_{B_i 0}, \gamma_{B_i 1}$ $\longleftarrow$	
$m_i = H(m \parallel y_{B_i})\ (1 \le i \le k)$		
$r_{B_i j} \equiv m_i^{-1} (\lambda^*_{B_i j})^{v_j} y_{B_i}^{v_{1-j}} \bmod p$		
$m^*_{B_i j} \equiv v_j^{-1} \cdot (r_{B_i j} - v_{1-j}) - \lambda^*_{B_i j} \bmod q$		
	$m^*_{B_i j}$ $\longrightarrow$	$m^*_{B_i j}$
		$s^*_{B_i j} \equiv x_{B_i} \cdot (m^*_{B_i j} + \lambda^*_{B_i j}) - z^*_{B_i j} \bmod q$
$s^*_{B_i j}$	$s^*_{B_i j}$ $\longleftarrow$	
$\lambda^{v_j}_{B_i j} \equiv \gamma_{B_i j} \bmod p$		
$s_{B_i j} \equiv v_j \cdot s^*_{B_i j} \bmod q$		
$\prod_{i=1}^{k} m_i' \equiv \prod_{i=1}^{k} g^{-s_{B_i j}} (y_{B_i j})^{r_{B_i j}} (r_{B_i j})^{-1} \bmod p$		
$m_i' \equiv H(m \parallel y_{B_i})\ (1 \le i \le k)$		
$m_i \equiv m_i'$		
$(m_i, (r_{B_i j}, s_{B_i j}))$		$(\lambda^*_{B_i j}, m^*_{B_i j}, z^*_{B_i j}, s^*_{B_i j})$

(그림 4) 메시지 복원 공정 은닉 다중 서명 기법(MR-FBMS)
(Fig. 4) Message recovery fair blind multi-signature

신뢰 센터로부터 전달받은 값 v_j, v_{1-j}에 대해서 전송자는 k 명의 서명자 B_i에게 β_j, β_{1-j}를 전달한다. 각 서명자 B_i는 $c \equiv \beta_j \cdot \beta_{1-j} \bmod p$를 검증하여 신뢰 센터가 생성한 c 값과 동일한지를 확인하고 난수 $z^*_{B_i j}$, $z^*_{B_i 1-j} \in Z_q$를 생성한다. 전체 다중 서명 단계에서 전송자는 서명자 B_i에게 전달할 메시지를 생성하기 위해서 $m_i = H(m \| y_{B_i})$ $(1 \le i \le k)$를 만족하는 m_i $(1 \le i \le k)$를 생성한다. 또한 전송자는 서명자로부터 은닉 서명된 $s^*_{B_i j}$에 대해 아래 수식을 만족하는 m_i'를 생성하고 해쉬 함수에 의한 검증 과정 $m_i' \equiv H(m \| y_{B_i})$ $(1 \le i \le k)$을 수행한다.

$$\prod_{i=1}^{k} m_i' \equiv \prod_{i=1}^{k} g^{-s_{B_i j}} (y_{B_i j})^{r_{B_i j}} (r_{B_i j})^{-1} \bmod p$$

만일 $m_i \equiv m_i'$ 이면 전체 다중 서명은 올바른 은닉 서명이 된다. 구체적인 공정 은닉 다중 서명 과정은 아래 (그림 4)와 같다.

V. 제안한 기법에 대한 분석 및 고찰

1. 제안한 기법의 공정성에 대한 검토

제안하는 기법의 공정성을 확인하기 위해 $type_I$ 형식의 r_I과 $type_{II}$ 형식의 r_{II}에 대해 고찰한다. 신뢰 센터 J는 r_I을 통해 서명자의 서명 메시지 (m^*, s^*)로부터 서명자의 서명에 해당하는 전송자의 메시지 (m, s)를 연관지을 수 있다. 또한 r_{II}를 통해 전송자의 메시지와 서명 (m, s)에 대해서 해당하는 서명자의 서명 (m^*, s^*)를 서로 연관지을 수 있다.

신뢰 센터가 $type_I$ 형태로 검증하는 과정은 다음과 같다. 신뢰 센터는 s_j^*와 s_j가 $s_j \equiv v_j \cdot s_j^* \bmod q$ 인 관계이고 m_j^*와 m은 다음 수식과 같은 관계성을 갖기 때문에 서명자의 메시지 (m^*, s^*)에 대해서 전송자의 메시지 (m, s)를 연관지을 수 있다.

$$\because\ m \equiv r_j^{-1} (\lambda_j^*)^{v_j} y^{v_{1-j}} \bmod p,$$

$$r_j \equiv v_j \cdot (m_j^* + \lambda_j^*) + v_{1-j} \bmod q$$

$$\therefore\ m \equiv (v_j \cdot (m_j^* + \lambda_j^*) + v_{1-j})^{-1} (\lambda_j^*)^{v_j} y^{v_{1-j}} \bmod p$$

$$\begin{aligned} s_j &\equiv v_j \cdot s_j^* \bmod q \\ &\equiv v_j \cdot (x \cdot (m_j^* + \lambda_j^*) - z_j^*) \bmod q \\ &\equiv v_j \cdot (x \cdot (v_j^{-1} \cdot (r_j - v_{1-j})) - z_j^*) \bmod q \\ &\equiv x \cdot (r_j - v_{1-j}) - v_j \cdot z_j^* \bmod q \end{aligned}$$

신뢰 센터가 $type_{II}$ 형태로 검증하는 단계는 다음과 같다. 신뢰 센터는 전송자와 관련된 메시지 (m, s)에 대해서 m_j^*와 s_j^*는 다음과 같이 변형할 수 있다.

$$m_j^* + \lambda_j^* \equiv v_j^{-1} \cdot (r_j - v_{1-j}) \bmod q,$$

$$s_j^* \equiv x \cdot v_j^{-1} \cdot (r_j - v_{1-j}) - z_j^* \bmod q$$

결국 신뢰 센터는 s_j^*에 대해 서명자 자신의 비밀키 x와 난수 z_j^* 및 신뢰 센터가 생성한 v_j, v_{1-j}를 사용하여 검증 가능하다. $s_j^* \equiv v_j^{-1} \cdot s_j \bmod q$ 이므로 전송자의 메시지와 서명 (m, s)에 대해서 해당하는 서명자의 서명 (m^*, s^*)를 서로 연관지을 수 있다. 물론 $type_{II}$ 형태의 검증 단계는 서명자가 선택한 비밀 정보에 대해 신뢰 센터가 미리 알고 있을 경우에 가능하다.

2. 제안한 공정 은닉 서명 기법에 대한 분석

Stadler-CC 및 Stadler-FS 기법[18,19]의 안전성은 소인수분해 문제의 어려움에 근간하고 있으며 RSA[2] 기법의 안전성 및 Fiat-Shamir[8] 기법의 안전성에 기반한 공정 은닉 서명 기법이다. Stadler-FS 기법인 경우 메시지 복원 방식으로 변형할 수 있으나 공정성 측면에서 $type_I$ 형태의 확인 기능만을 제공한다.

Meta-ElGamal 기반 MR-BMS 기법은 ElGamal[9] 기반 이산 대수 문제의 어려움에 근거하고 있으며 전송자가 발생한 메시지에 대해 다중 서명자가 서명할 수 있고 전처리 및 공정성을 제공하는 은닉 서명으로 발전시킬 수 있다. 결국 MR-BMS 기법은 Nyberg-Rueppel 기

법[24]에서 제공하는 메시지 복원 방식을 Meta-ElGamal 은닉 서명 기법과 결합하여 발전시킨 것이다. 제시한 메시지 복원 은닉 다중 서명 기법은 기존의 Meta-ElGamal 기반 은닉 서명과 유사한 성능을 나타내면서 메시지 복원 기능을 제공한다.

또한 MR-FBS 기법인 경우 이산 대수 문제의 어려움에 근거하고 있다. 또한 제안한 기법인 경우 메타-ElGamal 기법의 안전성 및 특성을 나타낸다. 그러나 MR-FBS 기법에서 적용한 불확정 전송 기법인 경우 신뢰 센터에 대한 사전 등록 단계를 수행하고 키 생성 단계 및 은닉 파라메터 생성 단계에서 적용된다. 따라서 제안한 기법은 불확정 전송 기법을 은닉 서명 단계에서 반복적으로 적용한 Stadler-FS 기법보다 계산량 및 전송량 측면에서 효율적이다. 제안한 기법은 신뢰 센터에 의해 $type_I$과 $type_{II}$ 형태의 검증 과정을 제공한다. 구체적인 특성 비교 결과는 아래 [표 1]과 같다.

[표 1] 은닉 서명 기법의 특성 비교
[Table 1] Property comparison on blind signatures

기법 / 비교 항목	Stadler-CC	Stadler FS	MR-BMS	MR-FBS	MR-FBMS
근본 안전성 기반	RSA 소인수분해	Fiat-Shamir 소인수분해	ElGamal 이산대수	ElGamal 이산대수	ElGamal 이산대수
메시지 복원	불가	변형가능	제공	제공	제공
공정 암호화 시스템 (fair cryptosystem)	판정불가	변형가능	변형가능	변형가능	변형가능
공정 은닉 다중 서명 (fair blind multisignature)	판정불가	변형가능	변형가능	변형가능	제공
추가 공정 암호화 기법	Cut-and-Choose	Oblivious Transfer	-	Oblivious Transfer	Oblivious Transfer
공정성 적용 단계	서명단계	서명단계	-	초기단계	초기단계
비밀 공유 기법	불가	변형가능	변형가능	변형가능	변형가능
공정성 확인 형태	I / II	I	-	I / II	I / II

본 연구에서 제시한 기법은 비밀 공유 기법(secret sharing)[22]의 변형이라 생각할 수 있다. 서명자는 자신의 서명에 대한 부분 분할을 통해서 검증자에게 전달한다. 이때 부분 서명 s_i를 신뢰할만한 중간자 B_i에게 전달한다. B_i는 서명에 대한 검증이 필요할 경우 공개적으로 증명 가능하다. 메시지 복원 기능을 제공하는 공정 은닉 다중 서명 기법인 MR-FBMS 역시 동일한 특성을 제공한다. α를 은닉 서명 단계에서의 추가적인 계산량에 해당하는 상수라 정의할 때 제안한 기법과 기존 기법에 대한 성능 분석 결과는 아래 [표 2]와 같다.

[표 2] 은닉 서명 기법의 성능 비교
[Table 2] Performance comparison on blind signatures

기법 / 비교 항목	Stadler-CC	Stadler-FS ($|d| = k'$)	MR-BMS	MR-FBS	MR-FBMS ($M = k$)
대화형 반복 회수	4	$1 + 2k'$	3	4	$4k$
서명 전처리 가능성	가능	불가	가능	가능	가능
전송 단계 처리 1024비트 mod 곱셈 연산수	$300 + \alpha$	$550,000 + \alpha$	$300 + \alpha$	$300 + \alpha$	$(300 + \alpha)k$
서명 단계 처리 1024비트 mod 곱셈 연산수	$1,650 + \alpha$	$830,000 + \alpha$	$300 + \alpha$	$300 + \alpha$	$(300 + \alpha)k$
검증 단계 처리 1024비트 mod 곱셈 연산수	$60 + \alpha$	$90 + \alpha$	$300 + \alpha$	$300 + \alpha$	$(300 + \alpha)k$

메시지 복원 기능을 제공하는 MR-FBMS 기법은 서명을 수행하는 전송자와 서명자 사이에서 전송자는 자신의 전자 화폐에 해당하는 메시지 내용을 서명자에게 공개하지 않으면서 서명자에 의해 전자 서명을 수행하는 방식이다. 이때 전송자는 서명자가 서명한 은닉 서명에 대한 확인 과정에서 자신이 생성한 메시지와 동일한 메시지를 복원하게 된다. 따라서 메시지 복원 기능을 제공하지 않는 일반 서명 기법보다 소액 전자 지불 방식(micropayment)에서의 전자 화폐 금액 관리 방식에 유리하다. 왜냐하면 복원된 메시지가 전자 화폐 금액을 바로 생성하기 때문에 잔액에 대한 정산 방식에 카운터 기법을 적용할 수 있다. 결국 메시지 복원 기법은 계산량 및 복잡도 측면에서 개선된 전자 화폐 지불 시스템을 제공할 수 있다. 특히 스마트 카드(smart card)에 기반한 소액 지불 시스템인 경우 효율적이다.

또한 본 연구에서 제시한 메시지 복원 공정 은닉 다중 서명 기법인 경우 기본적인 은

닉 서명 기능을 제공하면서도 필요로 하는 경우에 신뢰 센터에 의해서 공개적으로 전자 화폐에 대한 공정성을 확인할 수 있다. 따라서 일반 소액 지불 시스템 뿐만아니라 일반적인 전자 화폐 시스템에서의 상호 신뢰성을 더욱 향상시킬 수 있다.

VI. 결론

본 연구에서는 Chaum이 제시한 기법[10]에 기반한 일반적인 은닉 서명 기법의 문제점[6,7]을 개선하기 위해서 이산 대수 문제의 어려움에 근거한 Meta-ElGamal 기반 은닉 서명 기법[11,12]을 변형하고 불확정 전송[15,16]의 특성을 이용한 메시지 복원 공정 은닉 다중 서명 기법을 제시하였다.

Meta-ElGamal 기법에 대한 일반화 단계를 통해 메시지 복원 기능을 제공하는 은닉 서명 모델을 분석하였다. 또한 신뢰 센터에 의해 공개 검증 가능하도록 하기 위해 공정 암호화 기법을 도입한 은닉 서명 기법을 제시하였다. 본 연구에서 제시하는 기법은 대단위 분산 컴퓨팅 기반 전자 지불 환경에서 일반 사용자의 전자 화폐에 대해 다중 서명자가 공개 검증 가능한 은닉 서명을 생성할 수 있었다. 또한 기존의 공정 은닉 서명 기법[18,19]과 달리 신뢰 센터에 대한 사전 등록 단계를 수행한 후 불확정 전송 기법을 은닉 서명의 초기 단계에 적용하여 전체 성능을 향상시켰다. 또한 $type_I$ 및 $type_{II}$ 형태의 공정성 확인 기능을 제공하여 필요로 하는 경우 신뢰 센터에 의해 공개 검증할 수 있다. 본 연구에서 제시한 기법은 카운터 기반 정산 방식과 결합하고 소액 지불 방식을 접목하여 스마트 카드 기반 오프-라인 전자 지불 시스템으로 발전 가능하다.

참 고 문 헌

[1] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, Vol. IT-22, No. 6, pp. 472-492, Nov. 1976.

[2] R. L. Rivest, A. Shamir and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM*, Vol. 21, No. 2, pp. 120-126, 1978.

[3] D. Chaum, A. Fiat, M. Naor, "Untraceable electronic cash," Advances in Cryptology - Crypto'88, Lecture Notes in Computer Science, Springer-Verlag, pp.319-327, 1990.

[4] S. Brands, "An Efficient Off-line Electronic Cash System Based on The Representation Problem," Technical Report CS-R9323, CWI, 1993.

[5] S. Brands, "Untraeable Off-line Cash in Wallets with Observers," Advances in Cryptology - Crypto'93, Lecture Notes in Computer Science, Vol. 773, Springer-Verlag, 1994.

[6] B. von Solms, D. Naccache, "On blind signatures and perfect crimes," Computers and Security, Vol. 11, No. 6, pp.581-583, 1992.

[7] E. F. Brickell, P. Gemmell, D. Kravitz, "Trustee-based tracing extensions to anonymous cash and the making of anonymous change," In Symposium of Distributed Algorithms (SODA), 1995.

[8] A. Fiat, A. Shamir, "How to Prove Yourself: practical solutions of identification and signature problems," Advances in Cryptology - Crypto'86, Lecture Notes in Computer Science, Vol. 263, Springer-Verlag, 1987.

[9] T. ElGamal, "A Public Key Cryptosystem and a Signature Scheme based on Discrete Logarithms," *IEEE Transactions on Information Theory*, Vol. IT-30, No. 4, pp. 469-472, Jul. 1985.

[10] D. Chaum, "Blind Signatures for Untraceable Payments," Advances in Cryptology - Crypto'82, Lecture Notes in Computer Science, Springer-Verlag, pp.199-203, 1983.

[11] Patrick Horster, Holger Petersen, "Meta Message Recovery and Meta Blind signature schemes based on the discrete logarithm problem and their applications," Advances in Cryptology - Asiacrypt'94, Lecture Notes in Computer Science, Springer-Verlag, 1994.

[12] Patrick Horster, Markus Michels, Holger Petersen, "Meta-ElGamal signature schemes," Proc. 2nd ACM conference on Computer and Communications security, Fairfax, Virginia, Nov. 2-4, 1994.
[13] Patrick Horster, Markus Michels, Holger Petersen, "Efficient blind signature schemes based on the discrete logarithm problem," Technical Report TR-94-6-D, University of Technology Chemnitz-Zwickau, Dept. of Computer Science, 1994.
[14] Patrick Horster, Markus Michels, Holger Petersen, "Meta-Multisignature schemes based on the discrete logarithm problem," Technical Report TR-94-12-F, University of Technology Chemnitz-Zwickau, Dept. of Computer Science, 1994.
[15] M. Rabin, "How to exchange secrets by oblivious transfer," Technical Reports TR-81, Harvard Aiken Computation Laboratory, 1981.
[16] Mihir Bellare, Silvio Micali, "Non-Interactive Oblivious Transfer and Applications," Advances in Cryptology - Crypto 89, Lecture Notes in Computer Science, Vol. 435, Springer-Verlag, 1989.
[17] S. Micali, "Fair Cryptosystems," Technical Reports MIT/LCS/TR-579-b, 1993.
[18] Markus Stadler, Jean-Marc Piveteau, Jan Camenisch, "Fair Blind Signature," Advances in Cryptology - Eurocrypt'95, Lecture Notes in Computer Science, Vol. 921, Springer-Verlag, 1995.
[19] Jan Camenisch, Jean-Marc Piveteau, Markus Stadler, "An Efficient Electronic Payment System Protecting Privacy," Advances in Cryptology - Eurocrypt'94, Lecture Notes in Computer Science, Vol. 875, Springer-Verlag, 1994.
[20] N. Asokan, Victor Shoup, Michael Waidner, "Optimistic Fair Exchange of Digital Signature," IBM Technical Report RZ 2973, 1997.
[21] Holger Petersen, Guillaume Poupard, "Efficient Scalable Fair Cash with Off-line Extortion Prevention," Technical Report LIENS-97-7, 1997.
[22] Markus Stadler, "Publicly Verifiable Secret Sharing," Advances in Cryptology - Eurocrypt'96, Lecture Notes in Computer Science, Springer-Verlag, pp.190-199, 1996.
[23] Alfred J. Menezed, Paul C. van Oorschot, Scott A. Vanstone, Handbook of Applied Cryptography, *CRC Press*, 1996.
[24] K. Nyberg, R.A. Rueppel, "A New Signature Scheme Based on the DSA Giving Message Recovery," 1st ACM Conference on Computer and Communication Security.

著者紹介

이 형 우(Hyung-Woo Lee) 정회원

1994년 2월 : 고려대학교 컴퓨터학과 졸업
1996년 2월 : 고려대학교 컴퓨터학과 이학석사
1999년 2월 : 고려대학교 컴퓨터학과 이학박사
1999년 3월~ 현재 : 천안대학교 정보통신학부 전임강사

〈관심분야〉 암호학, 정보보호, 전자서명, 멀티미디어, 네트워크