情報保護學會論文誌
第13券 第1號, 2003. 2

# EC-KCDSA 부분 은닉서명을 이용한 거스름 재사용 가능한 전자수표지불 시스템

이 상 곤*, 윤 태 은**

# Refunds Reusable Electronic Check Payment System Using an EC-KCDSA Partially Blind Signature

Sang-gon Lee*, Tae-eun Yun**

요 약

본 논문에서는 타원곡선을 이용한 확인서 기반 전자서명 알고리즘(EC-KCDSA : Elliptic Curve - KCDSA)을 기반으로 한 부분 은닉서명 기법을 제안하고, 이를 이용하여 거스름 재사용 가능한 전자수표지불 시스템을 설계한다. 본 논문에서 제안한 부분 은닉서명은 타원곡선 시스템을 사용함으로서 RSA를 사용한 기존 기법보다 향상된 성능을 가진다. 따라서 본 논문에서 제안하는 거스름 재사용 가능한 전자수표지불 시스템은 기존의 것보다 효율적이다. 거스름 수표 발급 시 은행과 고객사이는 데이터 교환을 위하여 일회성 비밀키를 사용하므로 대칭 키 관리가 필요 없다.

ABSTRACT

In this paper, a partially blind signature schemes based on EC-KCDSA is proposed and we applied it to design an electronic check payment system. Because the proposed partially blind signature scheme uses elliptic curve cryptosystem, it has better performance than any existing schems using RSA cryptosystem. When issuing a refund check, one-time pad secret key is used between the bank and the customer to set up secure channel. So the symmetric key management is not required.

**Keyword** : *partially blind signature, electronic payment system, electronic check system, reusable refund*

## Ⅰ. 서 론

전자화폐는 전자상거래에서 지불수단으로 사용하기 위해 개발된 화폐로서, 디지털 정보 형태로 표현되므로 통신망을 통하여 전달 가능하다. 이상적인 전자화폐란 기존의 실물화폐가 가지고 있는 익명성(anonymity), 독립성(independence), 양도성(transferability), 재사용방지(reuse protection), 오프라인(offline) 등의 특성을 지녀야 한다[1].

*David Chaum*[2]이 전자화폐를 처음 소개한 이후 이것에 대한 연구가 많이 이루어졌다. 전자화폐는 화폐로서의 기능상 전자동전(electronic coin)방식[3]과 전자수표(electronic check)방식[4]으로 분류할 수 있다. 전자동전 방식에서는 각 동전이 고정된 액면가를 가지고 있으며, 고객은 지불대금에 맞도록 필요한 개수의 동전을 이용하여 지불한다. 이와는 달리 전자수표 방식에서는 시스템이 정해놓은 고정된 금액의 수표 또는 고객이 원하는 금액의 수표를 인출받아 지불한다. 전자수표는 수표 하나만으로도 지불이 가능하기 때문에 여러개의 동전을 사용해야하는 전자동전방식

* 동서대학교 인터넷공학부(nok60@dongseo.ac.kr)
** 스마트카드테크놀로지(주)(seajack@sct.co.kr)

보다 계산량이나 정보교환량 측면에서 효율적이다[4].

전자수표방식을 사용하는 경우는 수표를 사용하고 난 후의 거스름돈을 처리해야할 필요성이 있다. 거스름돈 처리는 Chaum이 제안한 쿠키통(cookie-jar) 방식[4]과 부분 은닉서명을 이용하는 방식이 있다[6,7]. 부분 은닉서명에서 서명될 메시지는 서명자에게 공개되는 부분과 은닉되는 부분으로 구성되어있다. 공개되는 부분은 전자수표의 액수, 유효기간 등을 표기하고 은닉부분은 수표의 일련번호를 표기함으로서 수표의 익명성을 보장할 수 있으며, 지불과정에서 잔액에 대하여 새로운 일련번호를 부여하고 은행이 서명함으로서 고객은 잔액을 새로운 전자수표로 되돌려 받게 된다. 부분 은닉서명은 M. Abe가 처음 소개하였고[5], RSA 및 Schnorr 서명을 사용한 부분 은닉서명을 제안하였다[6]. 최근에는 RSA를 기반으로한 부분 은닉서명을 사용하여 거스름 재사용 가능한 전자수표시스템이 발표된 바 있다[7]. 하지만 이 시스템은 RSA를 사용함으로써 계산의 효율이 낮다. 특히 Smart Card와 같이 계산 능력이 낮은 장치에서는 실행속도가 느리다.

[8]에서는 서명자와 이용자가 공유하는 공개키를 사용하여 Schnorr 서명 기반의 확률적으로 안전한 부분 은닉서명 기법을 제안하였으며, [9]에서는 EC-KCDSA (Elliptic Curve - KCDSA)[10] 기반의 은닉서명 기법을 제안하였다. 본 논문에서는 [8]과 [9]를 기초로 EC-KCDSA 기반의 부분은닉서명을 제안하고 이를 이용하여 거스름 재사용 가능한 전자수표지불 시스템을 제안한다. 타원곡선 암호시스템을 이용함으로써 RSA를 이용하는 [7] 보다 더욱 효율적인 전자수표지불 시스템을 구현할 수 있게 된다. 본 논문에서 제안하는 EC-KCDSA 기반의 부분 은닉 서명은 서명자와 이용자가 공유하는 공개키를 제거하면 [9]의 완전 은닉서명이 된다.

## II. EC-KCDSA 부분 은닉서명

부분 은닉서명은 은닉되는 m과 공개되는 정보 z의 쌍에 대하여 서명자의 서명을 받게되지만 서명자는 서명된 데이터와 m을 연관시키는 것이 계산적으로 용이하지가 않다[6,7]. 일반 은닉서명에서 서명자는 서명 내용을 전혀 알 수 없지만 부분 은닉서명에서 서명자는 z가 서명에 포함된다는 것을 확신할 수 있다. 기존에 발표된 바 있는 EC-KCDSA 기반의 은닉서명기법[9]에 공개정보를 서명에 참여할 수 있도록 수정함으로서 부분 은닉서명을 설계한다.

EC-KCDSA 부분 은닉서명에서 사용하는 공개정보와 사용자 변수는 m을 제외하고 기본 서명방식인 EC-KCDSA와 모두 동일하다.

### 2.1 시스템 변수

- $E(F_{p^m})$ : 유한체 $GF(p^m)$상에 정의된 타원곡선.
- $q$ : $\#E(F_{p^m})$를 나누는 소수. $|q| \geq 160$
- $G$ : 위수 q를 갖는 순환군(cyclic group)을 생성하는 타원곡선 $E(F_{p^m})$의 한 점.
- $h()$ : 충돌 저항성의 해쉬함수. $|h()| \geq 160$
- x : $0 < x < q$인 비공개 서명키.
- y : $y = x^{-1}G$로 계산 되는 서명자의 공개 검증키.
- z : 공개정보 Info의 해쉬코드 h(Info). 길이는 $|q|$.
- m : 서명될 메시지

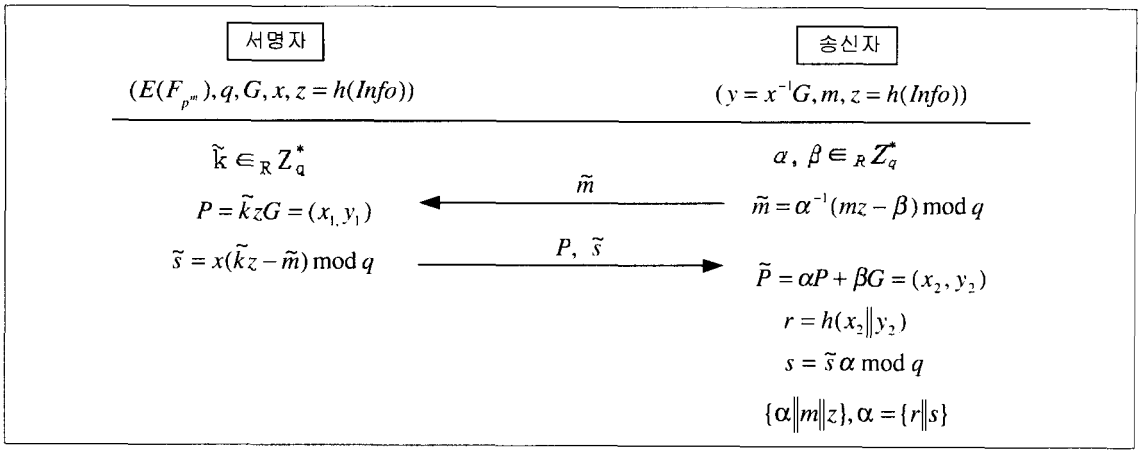
### 2.2 서명 생성 과정

공개되는 데이터를 z라 한다. 이것은 나중에 화폐의 금액이나 유효기간으로 활용될 수 있다. 만약 z가 zero이면 해쉬함수 입력 뒤에 추가 데이터를 사용하여 새로운 값을 생성한다. 서명생성 과정은 아래의 [그림 1]과 같다.

① 메시지 송신자는 $\alpha, \beta \in_R Z_q^*$를 선택한 후 $\hat{m} = \alpha^{-1}(mz - \beta) \bmod q$를 계산하여 서명자에게 보낸다.
② 서명자는 $\hat{k}$를 생성한다. $\hat{k} \in_R Z_q^*$
③ 서명자는 $P = \hat{k}zG$ 와 $\hat{s} = x(\hat{k}z - \hat{m}) \bmod q$를 계산하여 $P, \hat{s}$를 메시지 송신자에게 전송한다.
④ 메시지 송신자는 $\hat{P} = \alpha P + \beta G = (x_2, y_2)$를 계산하여 서명값 $r = (x_2 \| y_2)$를 구한다. 여기서 $x_2 \| y_2$는 타원곡선 위의 점 $(x_2, y_2)$의 좌표 값을 연접(concatenate)함을 의미한다.
⑤ 메시지 송신자는 m에 대한 서명값으로 $s = \hat{s}\alpha \bmod q$를 결정한다.
⑥ 최종적으로 서명된 데이터 $\{\Sigma \| m \| z\}$를 출력한다. 이때 $\Sigma = \{s \| r\}$이다.

### 2.3 서명 검증 과정

① 검증자는 서명된 메시지로부터 검증할 메시지 m, 서명의 첫 부분 s, 서명의 두 번째 부분 r과 공개되는 정보 z를 추출한다.




〔그림 1〕 EC-KCDSA 부분 은닉서명 생성과정

② 추출된 정보 중 $0 < s < q$임을 확인한다.

③ 서명자의 공개 검증키 y를 이용하여 $r = h(x_2 \| y_2)$이 성립하는지 확인한다. 이때 $(x_2, y_2) = mzG + sy$이다.

④ ②와 ③의 확인 과정에 이상이 없다면 서명 $\Sigma$는 메시지 m에 대하여 공개 검증키 y와 z에 대응하는 비공개 검증키 x로 서명하였음이 확인된 것이다.

## 2.4 서명의 정확성(correctness)

부분 은닉서명의 정확성 확인을 위해서는 서명자의 공개키와 공유하는 공개키 그리고 서명 메시지 그리고 서명 값을 이용하여 $r = h(x_2 \| y_2)$임을 보이면 된다.

$\hat{P} = (x_2, y_2)$이고 다음의 등식이 성립한다.

$$\begin{aligned}\hat{P} &= mzG + sy \\ &= mzG + \hat{s}\alpha x^{-1}G \\ &= mzG + x(\hat{k}z - \tilde{m})\alpha x^{-1}G \\ &= mzG + \hat{k}z\alpha G - \tilde{m}\alpha G \\ &= mzG + \alpha\hat{k}zG - mzG + \beta G \\ &= \alpha\hat{k}zG + \beta G\end{aligned}$$

위의 식이 성립함은 보임으로서 서명 값 $\{s \| r\}$가 m과 z의 유효한 서명 값임을 의미한다.

## 2.5 서명의 안전성

부분 은닉서명은 부분 은닉성(partially blindness)과 위조 불가능성(non-forgeability)을 만족하면 안전하다[11]. 아래에 부분 은닉성과 위조 불가능성 두 부분으로 나누어 안전성을 설명한다.

### 2.5.1 부분 은닉성(partially blindness)

은닉서명에서는 보통 서명자가 서명 프로토콜을 수행하면서 얻은 정보인 서명자 뷰(V)와 메시지 송신자가 은닉서명을 얻기 위해 생성한 정보사이에 통계적인 독립성이 유지된다.

제안된 부분 은닉서명 프로토콜에서 메시지 서명자의 익명성 보호를 위한 부분 은닉성의 증명을 위해서 서명자의 뷰 $\tilde{m}, P, \hat{s}$와 임의의 유효메시지 서명 값 쌍 $m, r, s$가 주어진 경우, 랜덤하게 선택된 은닉요소인 $\alpha, \beta$의 유일한 값 쌍이 존재함을 보이면 된다. 만약 두 번의 부분 은닉서명을 위하여 설정된 공개정보가 $\text{info}_1 = \text{info}_2$으로 같다고 가정하자. $\{(r_1, s_1)\}$와 $\{(r_2, s_2)\}$가 서명자에게 주어졌다면 $P_i, \hat{s}_i$와 $r_i, s_i$ 사이를 관계짓는 랜덤벡터 $(\alpha, \beta)$가 있다는 것을 보임으로서 부분은닉성은 증명된다[8].

아래의 수식은 서명 프로토콜에서 주어지는 $P_i, \hat{s}_i$와 $r_i, s_i$ 사이의 관계 수식이다.

$$\begin{aligned}r_i &= h(x_{i2} \| y_{i2}) \\ (x_{i2}, y_{i2}) &= \alpha P_i + \beta G = \alpha\hat{k}_i zG + \beta G \\ &= mzG + \alpha\hat{k}_i zG - mzG + \beta G \\ &= mzG + \alpha\hat{k}_i zG - \tilde{m}\alpha G \\ &= mzG + x(\hat{k}_i z - \tilde{m})\alpha x^{-1}G \\ &= mzG + s_i y \\ s_i &= \alpha\hat{s}_i\end{aligned}$$

여기서 *m=message, z=H(info)* 이다.

위의 수식에서 보는 바와 같이 $P_i$, $\tilde{s_i}$와 $r_i$, $s_i$의 값에 관계없이 $\alpha$와 $\beta$가 주어지므로 서명자가 $\{(r_1, s_1)\}$와 $\{(r_2, s_2)\}$를 구분하는 것은 확률적으로 1/2이므로 동전 던지기 확률과 같다. 따라서 제안된 서명시스템은 부분 은닉성을 지니고 있다.

#### 2.5.2 위조 불가능성(non-forgeability)

디지털 서명의 공격에 대해서는 [12]에 잘 정의 되있다. 그 중에서 가장 강력한 것은 실제적 적응 선택 메시지 공격(existentially adaptive chosen message attack)으로 알려져 있다. 이것은 공격자가 임의로 선택한 여러 개의 메시지에 대하여 합법적인 서명을 얻을 수 있으며 이것들을 바탕으로 새로운(메시지-서명) 쌍을 위조해 내는 공격이다. D. Pintcheval 등[13]은 이것을 "one-more" 위조라 하였다.

본 논문에서 제안한 서명 알고리듬은 EC-KCDSA에 근간을 두고 있으며, EC-KCDSA는 ElGamal 류의 서명 기법을 따르고 있다. ElGamal 류의 블라인드 서명 기법이 랜덤 오라클 모델 기반 안전성 증명 기법에서 "one-more" 위조에 안전하다고 증명된 바 있다[13,14]. 따라서 본 논문에서 제안한 부분 은닉서명은 "one-more" 위조에 대하여 안전하다고 할 수 있다.

## Ⅲ. 거스름 재사용 가능한 전자수표지불 시스템

이 장에서는 EC-KCDSA 부분 은닉서명을 이용하여 거스름에 대한 문제점을 해결한 온라인 전자수표 지불 시스템을 설계한다.

### 3.1 시스템 설정

은행과 고객 그리고, 판매자의 공개키와 충돌 회피 해쉬함수는 공개되어 있다. 고객이 수표의 일련번호를 받는 방법은 두 가지가 있는데, 첫 번째는 은행으로부터 download하는 방법이다. 고객은 익명의 Proxy Server를 통하여 은행으로부터 언제든지 서명되지 않은 수표의 일련번호를 download 할 수 있다. 익명의 Proxy Server를 사용하는 이유는 은행이 서명되지 않은 수표의 일련번호를 고객과 연결시키지 못하게 하기 위해서이다. 이 방법은 수표의 일련번호들을 은행이 직접 관리하기 때문에 수표의 관리 측면에서 유리하다. 그러나, 일련번호를 download 받기 위한 추가적인 시스템이 필요하다. 두 번째는 고객이 일련번호를 직접 생성하는 방법이다. 이 방법은 추가적인 시스템은 필요 없으나, 은행의 수표관리 차원에서는 유연하지가 못하다. 본 논문에서는 추가적인 시스템을 배제하고 프로토콜 처리단계를 줄이기 위하여 고객이 직접 생성한다고 가정한다. 그리고 은행에는 고객과 판매자의 계좌가 개설되어 있다.

### 3.2 인출 Protocol

고객은 일련번호로 사용할 N을 생성한다. N은 은행의 서명을 받기 전에는 사용할 수 있는 수표의 일련번호로서 인정이 되지 않는다.

#### 3.2.1 사용자 변수

- V : 수표의 액면가.
- T : 수표의 유효기간.
- U : 고객의 계좌정보.
- N : 고객이 생성하는 Random number. 수표의 일련번호로 사용.
- Info : V와 T를 포함하는 공개정보.
- n : n=h(N)으로 계산되는 수표 일련번호의 해쉬코드.
- ch : 지불시 사용될 은행의 서명이 포함된 전자수표.
- z : z=h(Info)로 계산되는 공개정보의 해쉬코드.
- 기타 정의되지 않은 변수는 EC-KCDSA 부분 은닉서명과 동일하다.

#### 3.2.2 인출 Protocol의 세부 절차

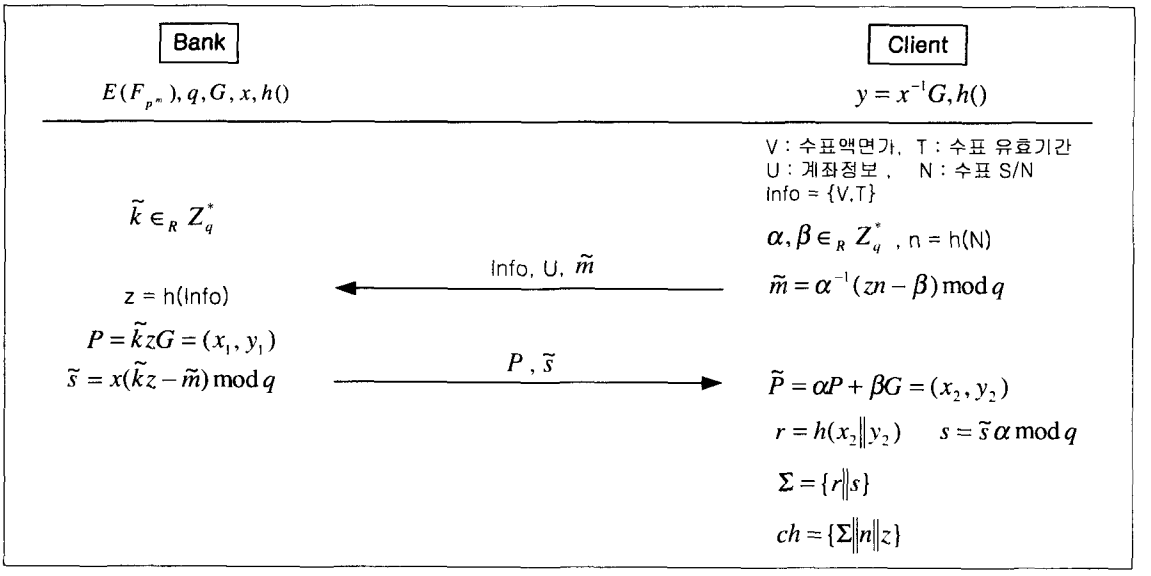
인출 Protocol의 세부 절차는 [그림 2]와 같다.

① 고객은 자신이 인출하고 싶은 만큼의 금액을 정하여 V로 두고, 원하는 수표의 유효기간 T를 결정한다. 여기서 유효기간은 은행에서 고정일을 정한다. Info는 부분 은닉서명 중 공개되는 정보로서 V와 T를 포함한다.

② 고객은 메시지 은닉에 사용할 임의의 $\alpha, \beta$를 $Z_q^*$상에서 선택한 후 $\tilde{m} = \alpha^{-1}(zn - \beta) \bmod q$를 계산하여 자신의 계좌정보 U와 공개정보 Info와 함께 은행으로 전송한다. 이때 z는 공개되어 있는 정보이고, n은 은닉이 되므로 은행이 알지 못한다.

③ 은행은 난수 값 $k$를 $Z_q^*$상에서 랜덤하게 선택하고, 고객으로부터 받은 Info를 충돌회피 해쉬함수를 사용하여 해쉬코드 z=h(Info)를 계산한다.

④ 은행은 $P = kzG = (x_1, y_1)$와 $s = x(kz - \tilde{m}) \bmod q$




〔그림 2〕 인출 Protocol

를 계산하여 $P$와 $\hat{s}$를 고객에게 전송한다.

⑤ 고객은 전송받은 $P$를 이용하여 $\hat{P} = \alpha P + \beta G = (x_2, y_2)$를 계산한다. 고객은 서명 값으로 사용될 $r = h(x_2 \| y_2)$를 계산한다.

⑥ 고객은 두 번째 서명 값 $s = \hat{s}\alpha \bmod q$를 계산하여 서명 데이터인 $\Sigma = \{r \| s\}$를 결정한 후, $\hat{P}$가 $znG + sy$와 같은지를 확인하여 서명을 검증한다.

⑦ 서명이 정상적으로 검증이 되면 지불시 사용할 서명된 수표 $ch = \{\Sigma \| n \| z\}$를 출력한다.

## 3.3 지불 Protocol

### 3.3.1 사용자 변수

- V' : 거스름으로 사용될 수표의 액면가.
- T' : 거스름으로 사용될 수표의 유효기간.
- N' : 고객이 생성하는 Random number로서 거스름으로 사용될 수표의 일련번호.
- Info' : V'와 T'를 포함하는 공개정보.
- I : 고객이 구입할 판매자의 상품 ID.
- M : 판매자의 ID.
- c : 고객으로 표현.
- i : $i = h(I \| Info)$로 계산되는 해쉬코드.
- Price : 상품의 가격.
- j : 고객이 생성한 일회성 비밀키.
- 기타 정의되지 않은 변수는 EC-KCDSA 부분 은닉 서명과 인출 Protocol에서 사용한 것과 동일하다.

### 3.3.2 지불 Protocol의 세부 절차

지불 Protocol의 세부 절차는 [그림 3]과 같으며, 지불 Protocol은 고객이 구입할 상품을 선택한 후 판매자에게 거래요청을 함으로서 시작된다.

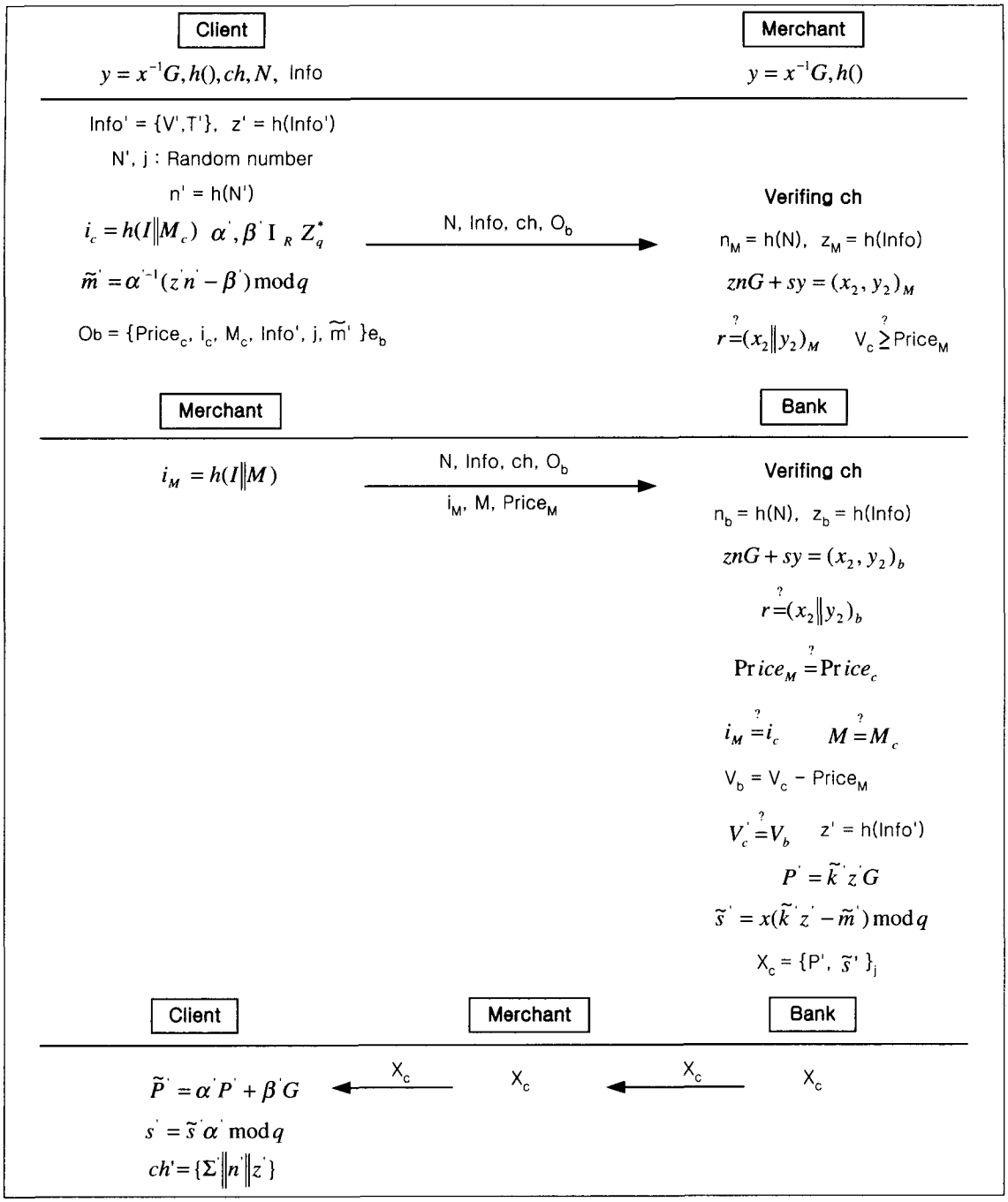
① 고객은 거스름 수표에 사용될 N', $V_c'$, T', Info'를 생성하고, 은행과 사용할 일회용 비밀키 j를 생성한다. 고객은 $n' = h(N')$를 계산하고, 판매자의 ID와 상품 ID $M_c$를 이용하여 $i_c = h(I \| M_c)$을 계산한다.

② 고객은 $\alpha', \beta'$를 $Z_q^*$상에서 랜덤하게 선택한 후 거스름 수표에 사용될 공개정보 z'와 n'를 구하여 $\hat{m}' = \alpha'^{-1}(z'n' - \beta') \bmod q$를 계산한 후 판매자를 통해 은행에 제공될 데이터인 {Price$_c$, $i_c$, $M_c$, Info', j, $\hat{m}'$}를 은행의 공개키로 암호화한 $O_b$를 생성한다.

③ 고객은 N, Info, ch, $O_b$를 판매자에게 보낸다.

④ 판매자는 받은 정보를 이용하여 ch를 검증한다. 먼저, ch에서 r, s, n, z를 추출하여, 고객으로부터 전송 받은 N, Info의 해쉬코드 값은 구하여 n, z와 비교한다. 이상이 없으면 $znG + sy = (x_2, y_2)_M$를 계산한 후 $(x_2 \| y_2)_M$을 계산하여 r과 비교한다. 비교한 값이 같으면 서명된 수표임을 인정한다.

⑤ 수표가 검증이 되면 Info에서 $V_c$를 추출하여 Price$_M$보다 큰 가를 확인한 후 은행에게 {N, Info, ch, $O_b$, $i_M$, M, Price$_M$}을 전송한다. 이때 $i_M$은 판매자




[그림 3] 지불 Protocol

가 계산한 I,M의 해쉬코드이다.

⑥ 은행은 판매자와 같은 방법으로 ch를 검증한다. 검증이 되면 N을 검색하여 정당한 수표의 일련번호인지를 확인한다. 이때 중복사용이라든지 유효기간이 지난 수표이면 거래를 중지시킨다.

⑦ 정당한 일련번호이면 은행은 자신의 개인키로 $O_b$를 복호화 한 후 고객과 판매자가 보내온 정보 $Price_c$와 $Price_M$, $i_c$와 $i_M$, $M_c$와 M를 각각 비교한다. 모두 같으면 $V_b$를 계산하여 $V_c'$과 같은지 비교해 본다.

⑧ 은행은 모든 비교에 이상이 없으면 난수 값 $\tilde{k}$를 $Z_q^*$상에서 랜덤하게 선택한 후 $P' = \tilde{k}z'G$를 계산하고, z'=h(Info')를 구하여 $\tilde{s}' = x(\tilde{k}z' - \tilde{m}') \bmod q$를 계산한 후 $P'$와 $\tilde{s}'$를 일회성 비밀키인 j를 사용하여 암호화한다. 이때 암호화된 데이터는 $X_c$이다. 은행은 $X_c$를 판매자를 거쳐 고객에게 전송한다.

⑨ 고객은 $\tilde{P} = \alpha' P' + \beta' G$를 계산하여 서명값 $r' = (x_2' \| y_2')$를 구하고, $s' = \tilde{s}'\alpha' \bmod q$를 계산하여 미리 계산된 r'과 함께 $\tilde{P}' ?= z'n'G + s'y$를 확인하여 서명을 검증한다. 서명이 정상적으로 검증이 되면 은행의 서명이 포함된 거스름 수표인 ch'를 출력하여 보관한다. 이때 $ch' = \{\Sigma' \| n' \| z'\}$이고, $\Sigma' = \{r' \| s'\}$이다. 은행의 서명이 포함된 거스름 수표가 완성이 되면 지불 protocol은 종료된다.

### 3.4 프로토콜의 안전성 및 효율성

#### 3.4.1 프로토콜의 안전성

공개정보를 서명자의 개인키로 서명하므로 서명자만이 서명데이터를 생성 할 수 있다. 그러므로 수표에 있는 공개정보인 V, T 값을 바꾸어 생성된 수표의 액면가, 혹은 유효기간을 위조할 수 없다. 고객과 은행간의 비밀키는 은행의 공개키로 암호화되어 전송되므로 제3자가 네트워 상에 전송되는 정보를 가로채어 수표를 위조하거나 은행에 보내는 데이터에 포함된 비밀키를 알 수 없다. 판매자 또한 은행의 비밀키를 알지 못하므로 고객과 은행과의 비밀키 j를 알지 못한다. 따라서 수표를 위조하거나 임의로 사용하지 못한다. 은행은 지불에 사용된 각 수표에 대한 필요한 정보를 보관하여 수표의 이중사용을 방지할 수 있다.

EC-KCDSA 부분 은닉서명은 완전 익명성을 제공하므로, 고객은 자신의 프라이버시를 보장받고 지불을 할 수 있으며, 고객 이외에는 거스름으로 받은 새로운 수표인 ch'로부터 이전의 수표인 ch를 알 수 없으므로 연결불가능성(untraceability)을 제공한다. 따라서 은행이 신뢰할 수 있는 기관이라고 하면, 사용되는 암호방법들이 안전하므로 본 지불 시스템은 안전하다.

#### 3.4.2 프로토콜의 효율성

기존의 Chaum[4]과 Deng[15]의 전자수표시스템은 수표의 액면가를 표현하는 방법과 거스름으로 받은 쿠키통의 액면가 표현 방법이 다르며 시스템이 정한 고정 금액의 수표만 인출할 수 있다. 또한 쿠키통에 축적된 여러 개의 거스름은 지불에 재사용 할 수 없으며 반드시 은행에 입금해야한다. 하지만, 본 시스템은 수표와 거스름으로 받은 수표는 동일한 형태를 가지고 있으며, 거스름으로 받은 수표도 원래 수표의 형태와 동일하므로 지불에 다시 사용할 수 있다. 또한 고객은 원하는 금액의 수표를 인출할 수 있으므로 수표 액면가의 제약이 없다.

RSA 부분 은닉서명을 이용한 전자수표시스템[7]은 고정되지 않은 금액의 인출이 가능하며 또한, 거스름을 재사용 할 수 있다. 그러나 본 시스템은 다른 공개키 암호 시스템에 비해 연산속도가 빠르고, 짧은 키 길이에 비해 동일한 안전도를 제공하는 ECC(Elliptic Curve Cryptography)를 사용한 EC-KCDSA를 기반으로 하므로 계산비용 측면에서 훨씬 효율적이며, smart card나 무선통신에도 적용 가능하다.

## Ⅳ. 결 론

본 논문에서는 EC-KCDSA에 기반으로 하여 부분 은닉서명을 제안하였다. 또한 제안한 부분 은닉서명을 이용하여 거스름 재사용 가능한 전자수표지불 시스템을 설계하였다. 부분 은닉서명을 사용함으로서 지불 과정에서 발생하는 거스름에 대해 익명으로 새로운 수표를 발행할 수 있다. 그리고 제안된 전자수표지불 시스템은 서명 시 공개되는 정보를 수표 액면가로 사용함으로서 액면가에 제한이 없이 원하는 액수를 발급 받아 사용할 수 있다. 거스름 수표 발급 시 은행과 고객사이의 데이터는 일회성 비밀키를 사용하므로 계산의 비용을 절감할 수 있다. 무엇보다도 이 전자수표지불 시스템은 EC-KCDSA 부분 은닉서명을 사용하므로 기존의 RSA 암호방법보다 키의 길이가 짧고 계산비용을 절감할 수 있으므로, Smart Card를 사용한 전자상거래에도 응용되어 질 수 있다.

## 참 고 문 헌

[1] 이만영 외 5인, "전자상거래 보안기술", *생능출판사*, 1999.

[2] David Chaum, "Blind Signature for Untraceable Payments," *Advances in Cryptology - Crypto'82*, pp. 199~203, 1982.

[3] David Chaum, Amos Fiat, and Moni Naor, "Untraceable Electronic Cash", *Advances in Cryptology - Crypto'88*, LNCS 403, Springer Verlag, pp. 319~327, 1988.

[4] David Chaum, "Online Cash Checks", *Advances in Cryptology - Eurocrypt'89*, LNCS 434, Springer Verlag, pp. 288~293, 1989.

[5] M. Abe and E. Fujisaki. "How to date blind signatures," In K.Kim and T. Matsumoto, editors, *Advances in Cryptology - ASIACRYPT '96*, LNCS 1163, Springer-Verlag, pp. 244~251, 1996.

[6] Masayuki Abe and Jan Camenisch, "Partially Blind Signature Schemes," *Proc of the 1997 Symp. on Cryptography and Information Security Workshop*, 1997.

[7] Sangjin Kim, Ihwa Choi, Heekuck Oh, "Refunds Reusable Online Electronic Check System," *Journal of KIISC VOL.11, No.1*, 2001, pp. 73~85. 2001.2.

[8] M. Abe and T. Okamoto, "Probably Secure Partially Blind Signature," *Advances in Cryptology* - Crypto 2000, LNCS 1880, Springer Verlag, pp.271~286, 2000.

[9] Moonseog Seo and Kwangjo Kim, "Blind Signature Schemes based on KCDSA and EC-KCDSA", *CISC '99*, Vol. 9, No. 1, pp. 141IV150, 1999. 11.6.

[10] C. H. Lim and P. J. Lee, "A Study on the Proposed Korean Digital Signature Algorithm", *Advances in Cryptology - ASIACRYPT '98*, LNCS 1514, Springer-Verlag, pp. 175~186, 1998.

[11] A. Juels, M. Luby, and R. Ostrovsky, "Security of Blind Digital Signatures", *Advances in Cryptology-CRYPTO '97*, LNCS 1294, Springer-Verlag, pp. 150~164, 1997.

[12] S. GoldWasser, S. Micali, and R. Rivest, "Digital Signature Schemes Secure Against Adaptive Chosen-Message Attacks", *SIAM Journal of Computing*, vol. 17, No 2, pp.281,308, April, 1988.

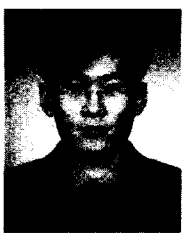
[13] D. Pintcheval, J. Stern, "Provably Secure Blind Signature Schemes", *Advances in Cryptology-ASIACRYPT '96*, LNCS 1163, Springer-Verlag, pp. 252~265, 1996.

[14] D. Pintcheval, J. Stern, "Secure Proofs for Signature Schemes", *In Advances in Cryptology-EUROCRYPT '96*, LNCS 1070, Springer-Verlag, pp. 387~398, 1996.

[15] R. H. Deng, Y. Han, A. B. Jeng, and Teow-Hin Ngair, "A New On-Line Cash Check Scheme", *Proc. of the 4th ACM conf. on Computer and Communications Security*. pp.111-116, 1997.

## 〈著者紹介〉

**이 상 곤 (Sang-gon Lee) 종신회원**
1986년 2월 : 경북대학교 전자공학과 졸업
1988년 2월 : 경북대학교 전자공학과 석사
1993년 2월 : 경북대학교 전자공학과 공학박사
1991년 3월~1997년2월 : 창신대학교 정보통신과 조교수
1997년 3월~현재 : 동서대학교 인터넷공학부
<관심분야> 암호이론, 네트워크보안, Java 기술, 부호기술



**윤 태 은 (Tae-eun Yun) 정회원**
2000년 2월 : 동서대학교 정보통신공학부 졸업
2002년 2월 : 동서대학교 대학원 정보통신공학과 석사
2002년 2월~현재 : 스마트카드테크놀로지(주) COS 개발팀 연구원
<관심분야> 네트워크보안, COS, Java 기술