무선환경을 고려한 효율적인 온라인 전자수표시스템

이여진, 유성진, 정일용
조선대학교 전자계산학과

Efficient Online Electronic Check System on Mobile System

Yeo-Jin Lee, Sung-Jin Yoo, Il-Yong Jung
Dept. of Computer Science, Chosun University

요 약

최근 무선 인터넷 시장이 급속한 성장을 하고 있다. 이러한 무선 인터넷상의 실용적인 전자지불 방식이 요구되고 있다. 여러 전자지불방식 중에서 전자수표시스템은 계산량이나 정보교환량 측면에서 전자동전방식보다 효율적인 지불수단이다. 그럼에도 불구하고 수표의 액면가가 제한되어 있고, 대금지불 과정에서 발생하는 거스름의 재사용이 용이하지 않기 때문에 활성화되지 못하고 있다. 이 시스템은 기존의 전자수표 시스템이 가지고 있는 이러한 문제점을 해결하면서 무선환경에 적합하도록 설계된 전자수표시스템이다. 부분은닉서명 기법을 이용하여 수표의 액면가를 임의로 표현할 수 있으며 거스름의 형태가 처음 발행 받은 수표의 형태와 같아 이를 다시 사용할 수 있다. 물론 수표의 익명성이 보장되며, 수표를 사용하고 받은 거스름은 어떤 수표의 거스름인지를 알 수 없게 된다. 또한, 무선인터넷 환경을 고려하여 보다 효율적인 전자수표시스템을 제안한다.

1. 서론

전자화폐는 쓰임새에 따라 분류하는 방법이 다양하다. 이런 분류 가운데 전자동전방식과, 전자수표방식[1,2,3]으로 분류하는 것이 있다. 전자동전방식은 고정된 액면가를 가지며, 지불대금에 맞도록 필요한 개수의 동전을 이용한다. 이와는 달리 전자수표방식은 고객이 원하는 금액의 수표 또는 시스템이 정해놓은 금액의 수표를 인출받아 사용하게 된다. 여러 개의 동전을 사용하는 전자동전방식에 비해 전자수표방식은 하나의 수표를 이용하여 지불이 가능하지만, 거스름에 대한 처리가 복잡하고, 오프라인 형태의 시스템을 만들기가 어렵다. 거스름은 수표의 액면가의 범위 내에서 다양한 금액이 될 수 있으며, 이 새로운 거스름은 재사용이 가능한 형태의 수표가 되어야 한다. 또한, 처음 발행 받은 수표와 거스름으로 받은 수표간에는 어떤 연관관계도 없어야 한다. 이러한 특성들을 고려한 수표시스템을 제안한다. 또한, 최근에 급부상하고 있는 무선 인터넷 환경을 고려하여, 무선인터넷 단말기를 이용한 전자수표 프로토콜을 설계한다.

이 논문의 구성은, 2장에서 기존의 전자수표시스템의 특성과 문제점을 분석하고, 3장에서는 이 논문에서 제안하는 전자수표시스템을 서술한다. 끝으로 결론과 향후 방향에 대해 서술한다.

2. 기존의 전자수표시스템

David Chaum[1]에 의해 1989년 처음 소개된 전자수표시스템은 RSA 은닉서명방식을 이용하여 은행으로부터 은닉서명을 받아 수표를 인출받으며, 고객이 선택한 난수를 수표의 일련번호로 사용한다. 또한, 거스름은 쿠키통에 저장하는 형태를 이용한다. 그 이후 cut-and-choose 기법을 이용한 오프라인 방식의 수표시스템[4]이 소개되며, 1997년 Robert Deng[3] 등이 발표한 온라인 전자수표시스템은 일회성 공개키를 생성하여 일련번호로 사용하지만, 거스름은 쿠키통 방식을 그대로 사용한다. 특히 Deng의 시스템은 온라인 시스템의 문제점을 극복하기 위해 같은 상점과 오프라인으로 다중 지불세션을 가질 수 있는 기능을 제공한다.

3. 제안하는 전자수표시스템

본 연구는 무선인터넷 환경에 적합하도록 연산속도가 빠른 것으로 알려진 타원곡선 알고리즘[7,8]을 적용한 은닉서명 기법인 EC-KCDSA 부분은닉서명 방식[5,6]을 이용하여 전자수표방식에서 문제시되는 거스름에 대한 처리와 익명성을 해결하도록 한다.

또한 [6]에서 제안한 일방향 축적기를 이용한 다중지불세션기능을 이용한다. 일방향 축적기는 준교환성을 만족하는 일방향 함수를 말한다. 준교환성을 만족하는 함수는 함수 $f: X\times X\rightarrow X$가 모든 $x_0, x_1, x_2\in X$에 대해 다음을 만족하는 경우이다.

$$f(f(x_0,x_1),x_2)=f(f(x_0,x_2),x_1)$$

3.1 시스템 설정

은행과 상점은 각각 일반 전자서명을 위한 매우 큰 RSA modulus $n_B=p_Bq_B$, $n_M=p_Mq_M$를 선택하고 RSA 공개키 쌍 (e^B, d^B),($e^M d^M$) 를 생성한다. 또한 은행에는 판매자와 고객의 계좌가 개설되어 있다. 또한, 고객은 지불과정 수행시 일회성 비밀키 KU_{CB}와 KU_{CM}를 생성하여 거래요청서에 은행과 상점 각각의 공개키를 이용해 암호화하여 전송함으로써, 은행과 상점이 고객에게 전송하는 중요한 정보의 암호화에 사용할 수 있다.

표 1. Notation

$E(F_{p^m})$	유한체 $GF(p^m)$상에 정의된 타원곡선
q	$\#E(F_{p^m})$를 나누는 소수 $\lvert q\rvert\geq 160$
G	위수 q를 갖는 순환군 $E(F_{p^m})$을 생성하는 타원곡선 의 한 점
$h()$	충돌 저항성 해쉬함수
x	서명자(은행)의 비공개 검증키 즉, 개인키
$y=x^{-1}G$	서명자(은행)의 공개 검증키 즉, 공개키
$info$	은닉서명시 공개되는 수표에 대한 정보 금액정보(V)와 유효기간(T)으로 구성
$I=h(info)$	$info$의 해쉬코드
N	임의의 난수. 수표의 일련번호 기능
$n=h(N)$	N의 해쉬코드
CK	수표로 사용
C	사용자
M	상점
B	은행
KU_{CB} , KU_{CM}	C가 생성하여 B와 M 각각과 공유하는 일회성 비밀키

3.2 인출 프로토콜

고객은 은행으로부터 (그림 1)에 있는 프로토콜을 이용하여 수표를 인출한다. 고객은 수표의 일련번호 N을 임의로 생성하여 은닉된 서명요청 정보 $\tilde{m}$ 에 은닉요소 α, β을 포함하여 은행에 은닉서명을 요청한다. 은행은 $P, \hat{s}$ 를 생성하여 고객에게 전송하게된다. 이 값을 이용하여 고객은 서명 $\sum$ 을 생성하여, 최종적으로 서명된 정보 CK를 얻을 수 있다. 결국 CK는 최종적인 수표 형태가 된다.

$$CK=\{r \parallel s \parallel n \parallel I\}$$

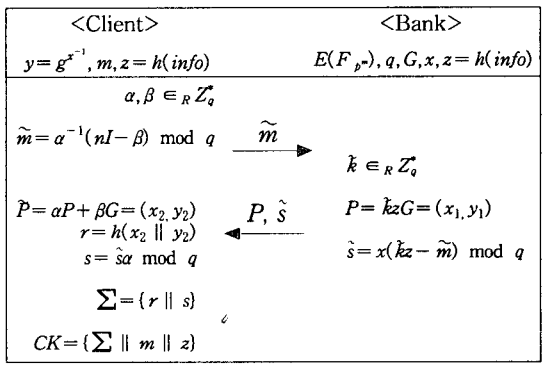

그림 1. 인출 프로토콜

이 수표는 지불과정에서 은행에 전달되어 은행은 자신이 서명한 수표가 맞는지 서명확인 절차를 거치게 된다.

3.3 지불 프로토콜

본 시스템은 단일 지불세션(그림 2)과 한 상점에서 여러 개의 상품을 구입하는 다중 지불세션(그림 3)의 두 가지 지불형태가 있다. 사용자는 지불요청서 O_b에 거스름 수표 정보, 서명확인 정보, 상품정보, 은행과 공유하는 일회성 비밀키 KU_{CB} 등을 포함하여 상점에 전송을 하고, 상점은 이 요청서를 은행에 그대로 전달하게 된다. 은행은 자신의 개인키로 지불요청서를 확인하고, 포함되어 있는 수표정보 CK가 은행 자신이 서명한 정당한 수표인지의 여부를 확인한 후 거스름 수표 생성을 위한 $P', \hat{s}'$를 사용자가 전송해 준 일회성 비밀키를 이용해 판매자를 통해 사용자에게 전달함으로써, 거래 확인은 물론, 임의의 금액의 거스름 수표를 생성할 수 있다. 다중 지불세션 프로토콜 역시 유사한 형태로 이루어지지만, 은행의 확인 없는 오프라인 지불처리를 위해 3개의 난스 N_{BC}, N_{BM}, N_{MC}를 사용한다. 판매자는 고객과의 거래에 대해 스스로 지불이 가능해야 하며, 추후 분쟁 해결을 위해 고객의 지불에 대해 증명이 가능해야 한다.

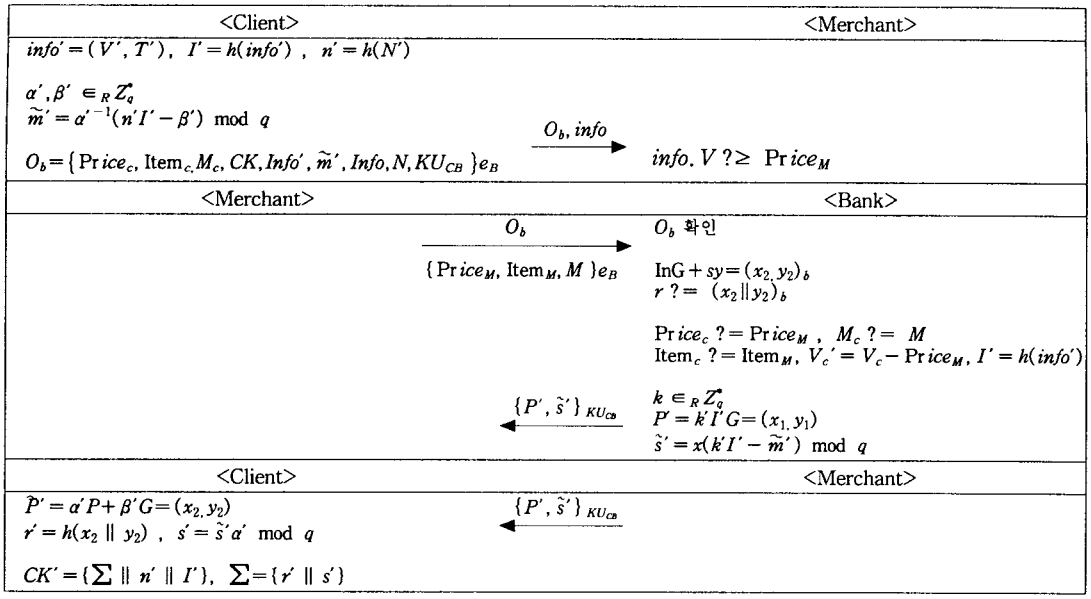

그림 2. 단일 지불 세션 프로토콜

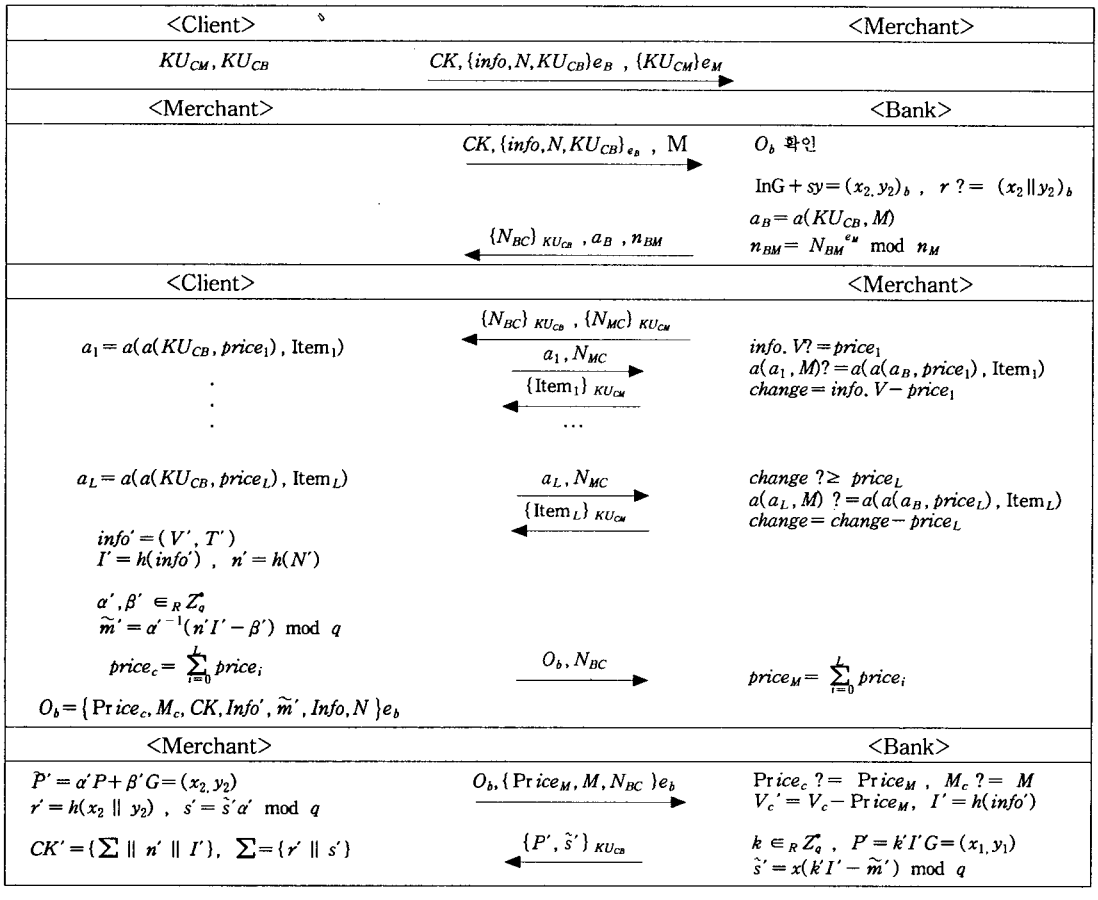

그림 3. 다중 지불 세션 프로토콜

4. 결론

본 시스템은 부분은닉서명방식을 이용하여 거스름 문제를 해결하게된다. 대금지불과정에서 발생하는 차액에 대해 새로운 수표를 발행하여 재사용이 가능하게 된다. 즉, 고객에 대한 익명성은 보장하면서 임의의 액면가를 가진 수표의 인출이 가능함은 물론, 액면가 한도내에서 임의의 금액을 가진 거스름 수표 생성이 가능하게 된다. 또한, RSA와 같은 일반 전자서명방식에 비해 빠른 연산속도를 지닌 ECC를 이용한 전자서명방식을 사용하여, PDA와 같은 무선인터넷 환경에 적합한 시스템이 된다.

[참고문헌]

[1] David Chaum, "Online Cash Checks", EuroCrypt'89, Springer Verlag, LNCS434, pp.288~293, 1989.

[2] David Chaum, Bert Boer, Eugene Heyst, Stig Mjoelsnes, and Adri Steenbeek, "Efficient Offline Electronic Checks", Eurocrypt'89, Springer Verlag, LNCS 434, pp.294~301, 1989.

[3] Rober H. Deng, Yongfei Han, Albert B. Jeng, and Teow-Hin Ngair, "A New On-Line Cash Check Scheme", Proc. of the 4th ACM Conf. on Computer ad Communication Security, pp.111~116, 1997.

[4] David Chaum, Bert Boer, Eugene Heyst, Stig Mjoelsnes, and Adri Steenbeek, "Efficient Offline Electronic Checks", Eurocrypt'89, Springer Verlag, LNCS 434, pp.294~301, 1989.

[5] 윤태은·이상곤, "KCDSA 및 EC-KCDSA를 기반으로한 부분 은닉서명", 한국정보보호학회 CISC2001, 2001.

[6] 김상진·최이화·오희국, "거스름의 재사용이 가능한 온라인 전자수표시스템", 한국정보보호학회논문지 제 11권 제 1호, 2001.

[7] 이동훈·황효선·임채훈, "타원곡선 암호의 기초와 응용", (주)퓨쳐시스템 암호체계센터 Technical Report. 2001.

[8] 이동훈·임채훈, "타원곡선 암호의 표준화 동향", (주)퓨쳐시스템 암호체계센터 Technical Report, 2001.