通信情報保護學會論文誌
第9卷 第1號, 1999. 3

Blinding ECDSA를 기반으로 한 분할가능 전자화폐 시스템

전 병 욱*, 권 용 진*

Divisible Electronic Cash System based on a Blinding ECDSA

Byeong Wook Jun*, Yong Jin Kwon*

요 약

전자 상거래에 대한 다양한 프로토타입(prototype)이 구현되고 있고, 확대적용의 현실성이 증대되고 있는 작금의 상황을 반영하여 관련 연구가 활발해지고 있으며, 그 중에서 보다 안전하고 효율적인 전자지불방식에 대한 현실적 요구가 증대하고 있다. 전자지불방식의 하나인 전자화폐는 실물 화폐와 유사한 성질들을 만족해야 하며, 이러한 성질들 중에서 필수적인 익명성을 얻기 위한 방법으로는 D. Chaum이 제안한 Blind Signature가 대표적이다. 본 논문에서는 기존의 암호시스템들이 가지고 있는 계산량 등의 문제점을 극복할 수 있는 방식으로써 주목받고 있는 타원곡선 암호시스템 상에서 서명자와 피서명자 간에 은닉 요소(blinding factor)를 교환함으로써 익명성을 제공하는 Elliptic Curve Blind Signature 기법을 제안한다. 또한, 제안 방식을 이용한 전자화폐 프로토콜에서 화폐 잔액에 대한 서명자의 재서명 과정을 통해 화폐의 분할성을 얻는 방법을 제시한다.

Abstract

Recently, various prototypes for electronic commerce are realized and its related researches are active under the present condition which it is increasing for the reality of its extended applications. First of all, actual demands are increasing for more secure and efficient electronic payment systems. Electronic cash, one of the Electronic payment systems, must have several properties like real money. Blind signature scheme by D. Chaum stands for the methods of obtaining privacy. In this paper, we propose a method for obtaining the blind signature based on the Elliptic Curve Cryptosystems, where the crytosystems are known as solving some problems of conventional crytosystems in views of

* 한국항공대학교 통신정보공학과

computation time and key space. Also, we present a method for the divisibility of the electronic cash using our proposal by re-signing spare cash. Thus applying the proposed method, we can develop an efficient electronic payment systems.

Keywords : Blind signature, Elliptic curve, Privacy, Divisibility

Ⅰ. 서 론

전세계적인 인터넷의 보급은 초기의 디지털 정보 전달 및 이용이라는 측면에서 벗어나 현재에는 인터넷 방송, 원격 진료, 전자상거래 등 사회 여러 분야의 정보화를 촉진시키는 역할을 담당하고 있다. 이 중 전자상거래는 기업과 기업간의 거래뿐만 아니라, 기업과 소비자간의 구매 분야에서도 이용되고 있으며 그 사용량이 꾸준히 증가되고 있는 추세이다. 이러한 전자상거래 환경의 활성화를 위해 고려해야 할 사항들 중 큰 비중을 차지하고 있는 대금 결제의 안전성은 계속적인 연구, 개발이 요구되고 있는 분야이다.

인터넷을 통해 대금을 지불할 수 있는 전자지불 시스템은 크게 지불브로커 방식과 전자화폐 방식으로 나눌 수 있다(그림 1). 이 중 전자화폐 방식은 화폐 가치를 디지털 정보의 형태로 저장하여 이를 지불 수단으로 사용하는 것으로써, 그 대표적인 시스템으로는 Digicash사의 E-cash, CyberCash사의 Cyber Cash 등과 같은 네트워크형과 Mondex사의 Mondex 카드, Visa International의 Visa Cash 등과 같은 IC 카드형이 개발되어 있다. 하지만, 이러한 전자화폐를 이용한 지불시스템은 안전성과 신뢰성의 문제로 인해 현재로서는 소액의 대금결제에 적합하며, 거액의 대금 결제를 위해서는 안전성에 대한 계속적인 연구가 필요하다.

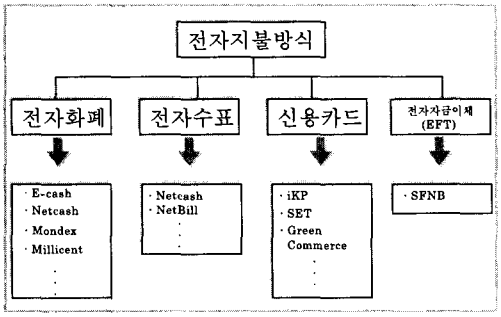


그림 1. 전자 지불 방식의 종류
Figure 1. A classification of Electronic Payment Systems

전자화폐는 그 사용 방식의 특성상 실물 화폐와 유사한 성질을 만족해야 하는데, 그 성질들로는 비의존성(independence), 보안성(security), 익명성(privacy), 오프라인성(off-line), 양도성(transfer-ability), 분할성(divisibility) 등이 제안되고 있다[1](그림 2). 이 외에도 개인의 Privacy를 보장하면서 돈세탁 등의 화폐 부정 사용을 방지하기 위한 조건부 추적가능성에 대한 요구도 또한 제기되고 있다. 상기 성질들 중 분할성이 결여되어 있을 경우, 은행에서 인출한 화폐는 단 한 번만 사용 가능하게 된다. 이러한 문제를 해결하기 위해 제안된 방식으로 이진 트리 구조[1,3,4], 다중 사용 동전[5] 등이 있지만, 전자의 경우는 계층수가 증가함에 따라 계산량이 방대해지는 단점이 있고, 후자의 경우는 정해진 회수만큼만 사용해야 하는 제한을 가지므로, [6,7]에서 Blind signature 기법을 이용한 기본적인 전자지불 프로토콜에 분할성을 부여하는 방법을 제시한 바 있다.

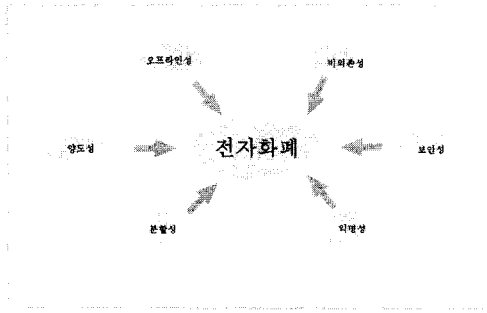


그림 2. 전자 화폐의 요구 사항
Figure 2. Requirements of Electronic Cash

익명성을 제공하는 방법 중 가장 대표적인 것으로는 D. Chaum이 제안한 Blind Signature[2]와 J. Camenisch 등이 제안한 서명 방식[16] 등이 있으며, 이들은 각각 소인수분해와 이산대수문제를 기반으로 하고 있다. 하지만, 소인수분해 문제 및 이산대수문제 등을 기반으로 하고 있는 대부분의 공개키 암호시스템들[8,9,10]은 키분배 문제 해결, 디지털 서명 개념 등의 많은 장점과 함께, 긴 암호화/복호화 시간, 넓은 키 공간(Key space) 등과 같은 구현상의 제한을 가지고 있다. 공개키 암호시스템이 가지는 이러한 단점들은 스마트 카드처럼 작은 계산력과 제한된 양의 메모리를 갖는 디바이스에 적합하지 않으므로, 그 사용 분야에 제약을 받게 하는 원인이 되고 있다.

이러한 공개키 암호시스템의 문제점들은 타원곡선(Elliptic Curve)을 이용한 공개키 암호시스템으로 해결 가능하다. 즉, 타원 곡선 위에서의 이산대수문제는 일반적인 그룹에서 정의되는 이산대수문제보다 더욱 어렵고, 키 공간과 계산량의 문제를 어느 정도 해결할 수 있으므로 스마트 카드 등의 제한된 디바이스에도 적용이 가능하다.

하지만, 타원 곡선에 대한 수학적 연구가 오랜 역사를 가지고 있음에도 불구하고, 암호학적인 접근은 최근들어 적극적인 관심과 연구가 시작되었기 때문에 아직은 더욱 많은 연구가 필요할 것으로 보인다. 타원곡선 이산대수문제를 이용한 은닉서명방식에 대한 연구는 국내에서도 [17]을 통해 발표된 바가 있으나, 현재 표준화가 추진되고 있는 ECDSA를 이용한 완전한 은닉서명방식에 대한 연구는 미흡한 것으로 보인다.

본 논문에서는 타원곡선 디지털 서명에 익명성(anonymity)을 부여하는 방법과 화폐의 분할성을 부여하는 방법을 제시하고, 이를 이용한 전자화폐 프로토콜을 제안하고자 한다. 2장에서는 기존의 타원곡선 암호시스템에 대하여 설명하고, 3장에서는 타원곡선 디지털 서명에서 익명성을 제공하는 타원곡선 Blind Signature를 제안한다. 4장에서는 제안한 서명기법을 기반으로 하여 사용자 익명성 및 화폐의 분할성을 만족하는 전자화폐 프로토콜을 제안하고, 5장에서는 제안 방식의 안전성 및 효율성에 대해 검토한다.

Ⅱ. 타원곡선 암호시스템

1. 타원곡선

1985년, Neil Koblitz[11]와 Victor Miller[12]는 타원곡선 상의 점들에 대한 이산 대수 문제에 기반을 둔 타원곡선 암호시스템(Elliptic Curve Cryptosystem, ECC)을 각자 독립적으로 제안하였다. 이러한 타원곡선 암호시스템은 암호화 방식뿐만 아니라 디지털 서명 방식으로도 사용될 수 있다.

(1) 타원곡선 이산대수문제 (The Elliptic Curve Discrete Logarithm Problem, ECDLP)

q가 소수의 멱승 형태일 때, F_q는 q개의 원소를 포함하는 유한체(finite field)를 의미한다. 실제 응용에 있어서 q는 일반적으로 2의 멱승(2^m) 또는 홀수인 소수(p)가 된다. 이 때, 타원

곡선 이산대수문제는 다음과 같다 : F_q에 대해 정의된 타원 곡선 E, order n의 점$P \in E(F_q)$와 $Q \in E(F_q)$가 주어졌을 때, $Q=dP$를 만족시키는 정수 $d(0 \le d \le n-1)$이 존재한다면 그 값을 구한다.

타원곡선 이산대수문제는 소인수분해 문제나 이산대수문제보다 상당히 어려운 것으로 알려져 있다. 이들을 이용한 암호시스템에서 동일한 암호학적 강도를 가정했을 때 타원곡선 암호시스템의 경우, 다른 시스템들에 비하여 키의 길이가 매우 짧아지는 장점을 갖는다. 예를 들어, 2048-bit의 RSA나 DSA에 비해 300-bit ECC(Elliptic Curve Cryptosystem)의 경우가 더욱 안전한 것으로 알려져 있다[13].

(2) 타원 곡선의 정의

타원곡선은 일반적으로 임의의 유한체 상에서 정의될 수 있으며, 특히 F_{2^n}의 경우 연산 수행에 있어 더욱 효율적이다. 여기에서는 설명을 단순화하기 위해 Z_p(p는 3보다 큰 소수)상에서의 타원곡선에 대해 설명한다.

Z_p에 대한 타원곡선 E는 다음과 같은 형태로 정의된다.

$$y^2 = x^3+ax+b \pmod p$$

여기서, $a,b \in Z_p$는 $4a^3+27b^2 \neq 0$인 상수이며 타원곡선은 무한원점(point at infinity)이라고 하는 원소 O를 포함한다.

타원곡선 E는 적절한 연산을 적용함으로서 abelian 그룹으로 구성할 수 있는데, 일반적인 그룹을 정의하는 것처럼 타원곡선 위의 점에 대해 다음과 같이 덧셈을 정의한다. 단, 모든 연산은 Z_p위에서 정의된다.

1. 모든 점 $P \in E(Z_p)$에 대하여 $P+O = O+P = P$이 성립한다.
2. 만약 $P=(x, y) \in E(Z_p)$이면, $(x, y)+(x, -y) = O$가 된다. (점(x, y)는 $-P$로 표시하고, P의 negative라고 한다.)
3. $P=(x_1, y_1) \in E(z_p)$, $Q=(x_2, y_2) \in E(z_p)$ 라고 할 때, $P+Q=(x_3, y_3)$가 된다. 여기서,

$$x_3 = \lambda_2 - x_1 - x_2$$

$$y_3 = \lambda(x_1 - x_3) - y_1$$

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & P \quad Q\text{일때} \\ \frac{3x_1^2 + a}{2y_1} & P = Q\text{일때} \end{cases}$$

위와 같은 덧셈 규칙은 기하학적으로 잘 설명된다[14]. 타원곡선 E상의 서로 다른 두 점 P와 Q의 합 $R=(x_3, y_3)$는 다음과 같이 정의된다. 첫 번째로 P와 Q를 통과하는 선을 그린다; 이 선은 세 번째 점에서 타원곡선과 교차한다. 이 때, R은 이 점의 x축에 대한 투영(reflection)이다(그림 3). 그림에서 타원곡선은 타원(ellipse)과 무한 곡선(infinite curve)의 두 부분으로 구성된다.

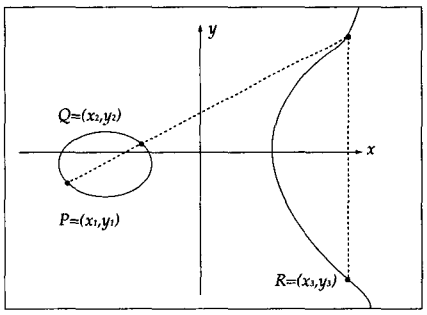


그림 3. 서로 다른 두 점의 덧셈에 대한 기하학적 표시 : P+Q=R

Figure 3. Geometric description of the addition of two distinct elliptic curve points : P+Q=R

$P=(x_1, y_1)$일 때 P의 doubling, $R=(x_3, y_3)$은 다음과 같이 정의된다. 첫 번째로 타원곡선 상의 점 P에 대한 접선(tangent line)을 그린다. 이 선은 두 번째 점에서 타원곡선과 교차한다. 이 때, R은 이 점의 x축에 대한 투영이다(그림 4).

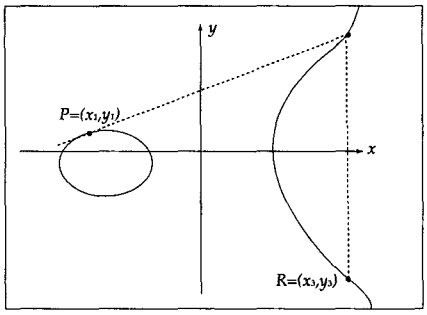


그림 4. 한 점의 doubling에 대한 기하학적 표시 : P+P=R

Figure 4. Geometric description of the doubling of an elliptic curve points : P+P=R

2. 타원곡선 암호시스템

타원곡선 이산대수문제를 기반으로 하는 타원곡선 암호시스템으로는 암호화 방식인 ECES(Elliptic Curve Encryption Scheme)와 디지털 서명 방식인 ECSS(Elliptic Curve Signature Scheme), ECDSA(Elliptic Curve Digital Signature Algorithm), 그리고 키 설정 프로토콜인 ECKEP(Elliptic Curve Key Establishment Protocol) 등이 있다[15].

(1) 시스템 셋업 및 키 생성

시스템 셋업(System Setup)

기초적인 유한체 F_q가 선택된다. F_q상에서 정의된 타원곡선 E와 E에서 order가 소수 n인 점 P가 선택된다. 체 F_q, 타원곡선 E, 점 P 및 order n은 시스템 파라미터를 의미하며, 공개정보이다.

키 생성(Key Generation)

각 Entity는 다음과 같은 동작을 수행한다.

1. 구간 [1, n-1]에서 랜덤한 정수 d를 선택한다.
2. 점 $Q=dP$를 계산한다.
3. Entity의 공개키는 점 Q로 구성된다.
4. Entity의 비밀키는 정수 d이다.

(2) 타원곡선 암호화 방식(ECES)

암호화 절차

(Entity B가 Entity A에게 데이터 M을 보내는 경우) Entity B는 다음의 단계들을 수행한다.

1. A의 공개키 Q를 알아낸다.
2. 데이터 M을 체의 원소 $m \in F_q$으로 표현한다.
3. 구간 [1, n-1]에서 랜덤한 정수 k를 선택한다.
4. 점 $(x_1, y_1) = kP$를 계산한다.
5. 점 $(x_2, y_2) = kQ$를 계산한다.
   만약 $x_2 = 0$이면 단계 3으로 이동한다.
6. $c = m \cdot x_2$ 를 계산한다.
7. 암호화된 데이터 (x_1, y_1, c)를 A에게 전송한다.

복호화 절차

(Entity A가 B로부터 수신한 암호문 (x_1, y_1, c)를 복호하는 경우) Entity A는 다음의 단계들을 수행한다.

1. 자신의 비밀키 d를 사용하여, 점 $(x_2, y_2) = d(x_1, y_1)$를 계산한다.
2. $m = c \cdot x_2^{-1}$ 을 계산함으로서 데이터 m을 복원한다.

(3) 타원곡선 서명 방식(ECSS 및 ECDSA)

ECSS와 ECDSA 방식에서 서명될 메시지는 먼저 고정된 길이의 메시지 다이제스트로 해쉬된 후 서명이 이루어지고, 서명의 검증(Verification)을 위해서는 서명과 원문이 모두 필요하다. ECDSA는 NIST Digital Signature Algorithm(DSA)를 타원곡선 상에서 구현한 것

이다.

ECSS에 대한 서명 생성

(Entity A가 Entity B를 위해 메시지 M에 서명하는 경우) A는 다음의 단계들을 수행한다.

1. 메시지 M을 이진 스트링으로 표현한다.
2. 해쉬값 $e=H(M)$를 계산한다.
3. 구간 [1, n-1]에서 랜덤한 정수 k를 선택한다.
4. 점$(x_1, y_1)=kP$를 계산한다.
5. $r=x_1+ e \mod q$를 계산한다.
6. 비밀키 d를 사용하여 $s=k-dr \mod n$을 계산한다.
7. 메시지 M과 서명(r, s)를 B에게 전송한다.

ECSS에 대한 서명 검증

(Entity B가 메시지 M에 대한 A의 서명(r, s)를 검증하는 경우) B는 다음의 단계들을 수행한다.

1. A의 공개키 Q를 알아낸다.
2. 점$(x_1, y_1)=sP + rQ$를 계산한다.
3. 해쉬값 $e=H(M)$를 계산한다.
4. $r'=x_1+e \mod q$를 계산한다.
5. 메시지 M에 대한 A의 서명을 수락하기 위한 필요충분조건은 $r=r'$이다.

(Notes)

해쉬값 e는 modulo q에 의해 감소되고, 다시 modulo n에 의해 감소된다. 따라서 보안성을 위해 ($H \mod q$) $mod\ n$도 또한 암호학적으로 안전한 해쉬함수가 되도록 하는 해쉬함수 H, q, n이 선택되어야 한다.

ECDSA에 대한 서명 생성

(Entity A가 Entity B를 위해 메시지 M에 서명하는 경우) A는 다음의 단계들을 수행한다.

1. 메시지 M을 이진 스트링으로 표현한다.
2. 해쉬값 $e=H(M)$를 계산한다.
3. 구간 [1, n-1]에서 랜덤한 정수 k를 선택한다.
4. 점$(x_1, y_1)=kP$를 계산하고, $r=x_1 \mod n$으로 설정한다.
5. 비밀키 d를 사용하여 $s=k^{-1}(e+dr) \mod n$을 계산한다.
6. A는 메시지 M과 서명(r, s)를 B에게 전송한다.

만약 $r=0$ 또는 $s=0$이면, 서명 검증에 실패할 것이다. 그러나, k가 랜덤하게 선택된다면 $r=0$ 또는 $s=0$일 확률은 무시할 수 있을 정도로 작다.

ECDSA에 대한 서명 검증

(Entity B가 메시지 M에 대한 A의 서명(r, s)를 검증하는 경우) B는 다음의 단계들을 수행한다.

1. A의 공개키 Q를 알아낸다.
2. 만약 $(r \mod n)=0$이면 서명을 부인한다.
3. 해쉬값 $e=H(M)$를 계산한다.
4. $s^{-1} \mod n$을 계산한다.
5. $u=s^{-1}\ e \mod n$와 $v=s^{-1}r \mod n$을 계산한다.
6. 점$(x_1, y_1)=uP+vQ$를 계산한다.
7. 메시지 M에 대한 A의 서명을 수락하기 위한 필요충분조건은$(x_1 \mod n)=r$이다.

(Notes)

(a) 해쉬값 e는 modulo n에 의해 감소된다. 따라서 $H \mod n$도 또한 암호학적으로 안전한 해쉬함수가 되도록 해쉬함수 H와 n이 선택되어야 한다.

(b) 서명 생성 단계 4에서 부여된 조건 $r \neq 0$는 보안성에 관한 조건이다. 만약 $r=0$이면, 서명식 $s=k^{-1}(e+dr)$는 비밀키 d를 포함하지 못하게 된다.

(c) 만약 k가 랜덤하게 선택된다면, $r=0$ 또

는 $s=0$일 확률은 무시할 수 있을 정도로 작다.

(4) 타원곡선 키 설정 프로토콜(ECKEP)

ECKEP를 이용하면 Entity A와 B간에 공유 비밀키 K(세션키라고 한다)를 설정할 수 있다. 세션키는 암호화/복호화 뿐만 아니라 인증 등의 응용에 사용될 수 있다.

시스템 셋업

A와 B는 동일한 타원곡선 파라미터 F_q , E, P, n을 사용하고 있다고 가정한다. A는 비밀키 d_A와 공개키 $Q_A = d_AP = (x_A , y_A)$를 갖는다. B는 비밀키 d_B와 공개키 $Q_B = d_BP = (x_B, y_B)$를 갖는다.

1. Entity A는 다음 과정을 수행한다.
   (a) 랜덤한 정수 k_A, $1 \le k_A \le n-1$를 선택한다.
   (b) 점 $(x_1, y_1) = R_A = k_AP$를 계산한다.
   (c) A는 R_A를 B에게 전송한다.
2. Entity B는 다음 과정을 수행한다.
   (a) 랜덤한 정수 k_B, $1 \le k_B \le n-1$를 선택한다.
   (b) 점 $(x_2, y_2) = R_B = k_BP$를 계산한다.
   (c) B는 R_B를 A에게 전송한다.
3. A는 다음 과정을 수행한다.
   (a) 정수 $s_A = k_A + x_1 d_A x_A \bmod n$을 계산한다.
   (b) 세션키 $K = s_A(R_B + x_2 x_B Q_B)$를 계산한다.
4. B는 다음 과정을 수행한다.
   (a) 정수 $s_B = k_B + x_2 d_B x_B \bmod n$을 계산한다.
   (b) 세션키 $K = s_B(R_A + x_1 x_A Q_A)$를 계산한다.

(Notes)

(a) 이 프로토콜은 상호간의 묵시적인 인증을 제공한다.

(b) 이 프로토콜은 키 확인(key confirmation)을 제공하지 않는다.

(c) 이 프로토콜의 또 다른 특징은 non-interactive(두 Entity 사이에서 전송되는 메시지들은 서로 독립적), role-symmetric(전송된 2개의 메시지는 동일한 구조)하다는 점과 암호화 함수, 해쉬 함수 또는 타임 스탬핑 (timestamping)이 요구되지 않는다는 점, 그리고 요구되는 대역폭(bandwidth)이 작다는 점이다.

Ⅲ. 타원곡선 은닉서명

1. ECDSA를 변형한 은닉 서명 방식

D. Chaum, J. Camenisch 등에 의해 제안된 Blind signature 기법은 서명자라고 하더라도 메시지와 서명문을 서로 연관시키지 못하도록 하는 서명 기법이다. 결과적으로 메시지에 서명을 한 서명자는 서명문의 정당성은 검증할 수 있으나 서명된 메시지를 가지고 있는 수신자의 신원은 알 수 없게 된다. 이 프로토콜을 사용한 전자화폐 방식은 은행에서 인출된 전자화폐와 사용자를 연결시키지 못하게 함으로써 사용자의 privacy를 보장하는 데 이용될 수 있다. 본 절에서는 타원곡선 이산대수문제를 기반으로 하는 ECDSA를 변형하여, 사용자의 익명성을 제공하는 Blinding ECDSA를 제안하고자 한다.

키 생성(Key Generation)

키 생성 방식은 2장의 ECDSA와 동일하며, Entity A, B의 공개키는 각각 Q_A, Q_B, 비밀키는 d_A, d_B이고, 공개정보 F_q, E, P, n은 공유한다.

Blinding ECDSA에 대한 서명 생성

(Entity B가 Entity A를 위해 메시지 M에 서명하는 경우) A는 다음의 단계들을 수행한다.

1. 구간 [1, n-1]에서 랜덤한 정수 k_{A1}를 선택한다.
2. 점$(x_1, y_1) = k_{A1} P$를 계산하여 B에게 전송한다.

B는 다음의 단계들을 수행한다.

1. 구간 [1, n-1]에서 랜덤한 정수 k_B를 선택한다.
2. 점 k_B $(x_1, y_1) = (x_2, y_2)$를 계산하여 A에게 전송한다.

A는 다음의 단계들을 수행한다(Blinding 단계).

1. 구간 [1, n-1]에서 랜덤한 정수 k_{A2}를 선택한다.
2. 점k_{A2} $(x_2, y_2) = (x_3, y_3)$를 계산한다.
3. 점$(x_4, y_4) = (x_2, y_2) + (x_3, y3)$를 계산한다.
4. 메시지 M을 이진 스트링으로 표현한 후, 해쉬값 $e = H(M)$를 계산한다.
5. $e' = ex_2x_4^{-1}$를 계산하여 B에게 전송한다.

B는 다음의 단계들을 수행한다(Signing 단계).

1. $r_B = x_2 \bmod n$을 계산한다.
2. $s_B = k_B^{-1} \{e' + d_B r_B\}$를 계산하여 A에게 전송한다.

A는 다음의 단계들을 수행한다(Unblinding 단계).

1. $r = x_4 \bmod n$으로 설정한다.
2. $s = s_B x_2^{-1} x_4 (k_{A1} + k_{A1}k_{A2})^{-1}$를 계산한다.

Blinding ECDSA에 대한 서명 검증

(Entity A가 메시지 M에 대한 B의 서명(r, s)를 검증하는 경우) A는 다음의 단계들을 수행한다.

1. B의 공개키 Q_B를 알아낸다.
2. $s^{-1} \bmod n$을 계산한다.
3. $u = s^{-1}e \bmod n$와 $v = s^{-1}r \bmod n$을 계산한다.
4. 점$(x_4, y_4) = uP + vQ_B$를 계산한다.
5. 메시지 M에 대한 B의 서명을 수락하기 위한 필요충분조건은$(x_4 \bmod n) = r$이다.

검증식 $uP + vQ_B = (x_4, y_4)$는 다음과 같이 유도될 수 있다.

$$
\begin{aligned}
uP + vQ_B &= s^{-1}eP + s^{-1}rQ_B \\
&= s^{-1}\{s(k_{A1} + k_{A1}k_{A2})k_B - d_B r\}P + s^{-1}rQ_B \\
&\quad (\because s = \{(k_{A1} + k_{A1}k_{A2})^{-1}k_B^{-1}(e + d_B r)\} \\
&= k_{A1}k_B P + k_{A1}k_{A2}k_B P \\
&= (x_2, y_2) + (x_3, y_3) \\
&= (x_4, y_4)
\end{aligned}
$$

참고로, $s = (k_{A1} + k_{A1}k_{A2})^{-1}\ k_B^{-1}(e + d_B r)$에 대한 증명 과정은 다음과 같다.

$$
\begin{aligned}
s &= s_B x_2^{-1} x_4 (k_{A1} + k_{A1}k_{A2})^{-1} \\
&= k_B^{-1}(e' + d_B r_B) x_2^{-1} x_4 (k_{A1} + k_{A1}k_{A2})^{-1} \\
&= k_B^{-1}(e' x_2^{-1} x_4 + d_B r_B x_2^{-1} x_4)\ (k_{A1} + k_{A1}k_{A2})^{-1} \\
&= k_B^{-1}(e x_2\ x_4^{-1} x_2^{-1} x_4 + d_B x_2 x_2^{-1} r)(k_{A1} + k_{A1}k_{A2})^{-1} \\
&= k_B^{-1}(e + d_B r)(k_{A1} + k_{A1}k_{A2})^{-1}
\end{aligned}
$$

제안 방식은 기존 ECDSA의 서명문 생성식 및 검증식을 그대로 유지하면서 사용자의 익명성을 제공하므로, 일단 익명성을 얻은 후에는 재서명 과정을 수행하기 위해 기존 서명식을 그대로 사용할 수 있게 된다.

Ⅳ. 익명성 및 분할성을 갖는 전자화폐 프로토콜

1. 타원곡선 은닉서명을 이용한 분할 가능 전자화폐 프로토콜

이 절에서는 본 논문에서 제안한 타원곡선 은닉서명을 이용하여 사용자 익명성을 제공하고, 지불 프로토콜시 잔액에 대하여 은행의 서

명을 재발급 받음으로써 화폐의 분할성을 부여한 전자화폐 프로토콜을 제안하고자 한다.

인출 프로토콜

(은행은 사전에 화폐의 금액에 대응하는 공개키 및 비밀키의 쌍들을 준비해 둔다.) 고객 A는 다음 단계를 수행한다.

1. 구간 [1, n-1]에서 랜덤한 정수 k_{A1}를 선택한다.
2. 점 $(x_1, y_1) = k_{A1}P$를 계산하여 B에게 전송한다.

은행 B는 다음 단계를 수행한다.

1. 구간 [1, n-1]에서 랜덤한 정수 k_B를 선택한다.
2. 점 k_B $(x_1, y_1) = (x_2, y_2)$를 계산하여 고객 A에게 전송한다.

고객 A는 다음 단계를 수행한다.

1. 구간 [1, n-1]에서 랜덤한 정수 k_{A2}를 선택한다.
2. 점 k_{A2} $(x_2, y_2) = (x_3, y_3)$를 계산한다.
3. 점 $(x_4, y_4) = (x_2, y_2) + (x_3, y_3)$를 계산한다.
4. 화폐일련번호 x_1를 랜덤하게 생성하여 이진 스트링으로 표현한 후, 해쉬 알고리즘을 이용하여 해쉬값 $e_1 = H(x_1)$를 계산한다.
5. $e' = ex_2x_4^{-1}$를 계산한 후, 자신의 ID와 함께 은행에 전송한다.

은행 B는 다음 단계를 수행한다.

1. 고객 A의 ID를 확인하고, 고객의 계좌로부터 금액을 인출한다.
2. $r_B = x_2 \bmod n$을 계산한다.
3. 인출 금액에 대응하는 비밀키 d_B를 이용하여 $s_B = k_B^{-1}\{e_1' + d_Br_B\}$를 계산한 후, A에게 전송한다.

고객 A는 다음 단계를 수행한다.

1. $r = x_4 \bmod n$으로 설정한다.
2. $s = s_Bx_2^{-1}x_4(k_{A1} + k_{A1}k_{A2})^{-1}$를 계산한다.
3. 인출 금액에 해당하는 은행의 공개키 Q_B를 알아낸다.
4. $s^{-1} \bmod n$을 계산한다.
5. $u = s^{-1}e_1 \bmod n$와 $v = s^{-1}r \bmod n$을 계산한다.
6. 점 $(x_4, y_4) = uP + vQ$를 계산한다.
7. $(x_4 \bmod n) = r$이면, (r, s)를 정당한 화폐로 받아들인다.

지불 프로토콜

고객 A는 상점 C로부터 상품을 구입한 후 전자화폐 $(x_1, (r, s), e_2)$을 C에게 전달한다. (여기서, $e_2 = H(x_2)$은 대금결제 후 사용될 잔액의 화폐일련번호 해쉬값이다)

상점 C는 다음 단계를 수행한다.

1. 지불된 금액에 해당하는 은행 B의 공개키 Q_B를 알아낸다.
2. 해쉬값 $e_1 = H(x_1)$을 계산한다.
3. $s^{-1} \bmod n$를 계산한다.
4. $u = s^{-1}e_1 \bmod n$와 $v = s^{-1}r \bmod n$을 계산한다.
5. 점 $(x_4, y_4) = uP + vQ_B$를 계산한다.
6. $(x_4 \bmod n) = r$이면, (r, s)를 정당한 화폐로 받아들인다.
7. $(x_1, (r, s), e_2)$을 은행에 보내어 이중사용 유무에 대한 검사를 의뢰한다.

은행 B는 다음 단계를 수행한다.

1. 수신한 전자화폐 $(x_1, (r, s), e_2)$을 데이터베이스에서 검색하여 이중사용여부를 검사하여 정당한 화폐이면 $(x_1, (r, s), e_2)$을 데이터베이스에 추가한다.
2. 잔액에 해당하는 자신의 비밀키 d_B과 화폐일련번호의 해쉬값 e_2을 사용하여 서

명을 한 후, 새로운 전자화폐 (r_B', s_B')을 상점으로 전송한다.

마지막으로, 상점 C는 상품과 잔액 (r_B', s_B')을 고객 A에게 전달한다.

V. 제안 프로토콜의 안전성 및 효율성

1. 타원곡선 은닉서명의 안전성 및 효율성

사용자 A가 선택한 랜덤한 정수 k_{A1}과 k_{A2}를 서명자가 알아내기 위해서는 타원곡선 이산대수문제를 풀어야 하며, 이는 계산량적으로 매우 어려운 문제이다. 결과적으로, 서명자가 원 서명문 (r_B, s_B)와 서명 결과인 (r, s)를 연결하기가 어렵게 된다. 또한, 사용자 A의 입장에서는 서명자의 서명문 s_B가 계산되기 전에 e'을 계산하여야 하므로, 메시지의 해쉬값 e를 위조할 수 없으므로 사용자의 부정행위가 불가능하다.

사용자 익명성을 얻기 위해서는 서명자와 피서명자 간의 은닉 요소(blindign factor) 교환이 이루어져야 하므로, 통신 횟수 및 데이터가 증가되지만, 일단 최초의 화폐발행 단계에서 얻어진 익명성은 이후의 지불과정에서 계속적으로 유지되므로, 지불절차에서는 일반 ECDSA와 같은 성능을 갖게 된다. 결론적으로, 이러한 통신 횟수 및 데이터의 증가로 인한 Overhead는 화폐의 익명성 획득과 Tradeoff 관계에 있다.

본 논문에서 제안한 은닉서명 프로토콜은 타원곡선 디지털 서명 방식으로서 표준화 작업 중에 있는 ECDSA의 서명문 생성식과 검증식을 변경하지 않으면서 익명성을 부여하는 방법을 제시하고 있다. 이러한 점은 실제 응용에 있어서 Blind Signature를 생성하기 위한 별도의 서명 모듈을 설계하지 않고도 기존의 ECDSA 기본 알고리즘에 몇 개의 부가적인 처리를 위한 모듈을 추가하면 된다는 장점을 갖는다. 즉, 일반 서명과 Blind 서명에 대한 모듈을 별도로 설계할 필요없이 단일 서명 모듈을 설계하고, 여기에 Blind 서명에 필요한 몇 가지 처리를 추가하면 된다.

2. 분할가능 전자화폐의 안전성 및 효용성

사용자는 최초의 화폐 인출 과정에서 익명성을 얻게 되므로, 이후의 지불 과정에서는 계속하여 익명성이 유지된다. 따라서, 잔액에 대한 서명을 받는 과정에서는 일반 서명으로 은익 서명을 대신할 수 있다. 제 3 자에 의한 부정행위방지는 지불 과정에서 x_2 대신 $e_2 = H(x_2)$를 사용함으로써 이루어지는데, 제 3 자가 화폐를 가로채더라도 화폐일련번호 x_2을 모르기 때문에 부정사용을 할 수 없게 된다.

VI. 결 론

본 논문에서는 기존의 공개키 암호방식을 바탕으로 하는 전자화폐의 단점인 계산량 및 키 공간 문제을 보완하기 위해 타원곡선 암호방식에 기반을 둔 타원곡선 은닉서명을 제안하고, 이를 이용한 전자화폐 프로토콜을 제안하였다. 제안한 타원곡선 은닉서명은 피서명자의 익명성을 보장하며, 그 안전성은 ECDLP의 안전성에 기반을 두고 있다. 또한 본 논문에서 제안하고 있는 전자화폐 프로토콜은 은닉서명 기법을 통해 고객의 익명성을 보장하는 동시에 화폐의 분할성도 제공할 수 있다. 따라서, 본 논문의 결과는 중요성이 증대되고 있는 스마트카드 등의 이동휴대단말에 응용할 수 있을 것으로 생각된다. 앞으로의 연구 방향으로는 화폐의 부정사용을 막고, 고객에게 제한된

익명성을 제공할 수 있는 Fair Cryptosystem에 대한 연구와 화폐의 처리를 보다 효율적으로 하기 위한 Off-line성 등에 대한 연구가 요구된다.

참고 문헌

[1] T. Okamoto and K. Ohta, "Universal Electronic Cash", Advance in Cryptology- Crypto'91, Lecture Notes in CS, Springer -Verlag, pp32-37, 1992

[2] D. Chaum, "Blind signature for untraceable payments", Crypto'82, pp199-203, 1982

[3] T. Eng, and T. Okamoto, "Single-Term Divisible Electronic Coins", Preproceedings of Eurocrypt'94, pp.313-328, 1994

[4] T. Okamoto, "An Efficient Signature Generation by Smart Cards", Journal of Crypt. Vol 4, No.3, pp.161-174, 1991

[5] N. Ferguson, "Extensions of Single-Term Coins", Advances in Cryptology-Crypto'93, Lecture Notes in CS, Springer-Verlag, pp.292-301, 1994

[6] 전병욱, 권용진, "전자화폐의 분할성에 관한 연구" 전자정보통신공학논문지, 제4권 제1호, pp.131-136, 1998년 4월

[7] 전병욱, 권용진, "Blind Signature를 이용한 분할이용가능 전자화폐" 한국정보과학회 '98 춘계 학술발표 논문집, 제 25 권, 1호, pp735-737, 1998

[8] T. ElGamal, "A public key cryptosystem and a signature scheme based on the discrete logarithm", IEEE Trans. Vol. 31, No. 4, pp469-472, 1985

[9] M. O. Rabin, "Digitalized Signatures and Public Key Functions as Intractable as Factorization", Technical Report, MIT/ LCS/TR212, MIT Lab, Computer Science, Cambridge, Mass. 1979

[10] R. L. Rivest, A. Shamir, L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", Com- munications of the ACM, Vol. 21, No. 2, pp120-126, 1978

[11] N. Koblitz, "Elliptic curve cryptosystems", Mathematics of Compu- tation, number 48, pp203-209, 1987

[12] V. S. Miller, "Use of elliptic curves in cryptography", Advances in Cryptology - Proceedings of CRYPTO'85, Springer Verlag Lecture Notes in Computer Science 218, pp417-426, 1986

[13] A Certicom Whitepaper, "Remarks on the security of the elliptic curve cryptosystem", September, 1997

[14] D. B. Johnsom, A. J. Menezes, "Elliptic Curve DSA(ECDSA): An Enhanced DSA", A Certicom Whitepaper, 1997

[15] WORKING DRAFT, IEEE P1363 STANDARD, November, 1995

[16] J. Camenisch, J. M. Piveteau, M. Stadler, "Blind Signature Based on the Discrete Logarithm Problem", Proc. Eurocrypt 94, pp428-432.

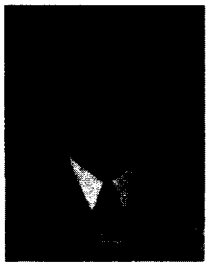
[17] 윤중철, 임종인, 서광석, 서창호, "타원곡선의 이산로그문제에 기반을 둔 Blind signature", 한국통신정보보호학회 종합학술발표논문집, 제 7 권, 1호, pp111-119, 1997

□ 著者紹介

전 병 욱

1997년 한국항공대학교 통신정보공학과 (학사)
1999년 한국항공대학교 대학원 통신정보공학과 (공학석사)
1999년 ~현재 (주)신테크 EC보안팀 전임연구원

※ 주관심분야 : 정보보호, 네트웍 보안



권 용 진

1986년 한국항공대학교 항공전자공학과 (학사)
1990년 일본쿄토대학 대학원 정보공학과 (공학석사)
1994년 일본쿄토대학 대학원 정보공학과 (공학박사)
1994년 ~ 현재 한국항공대학교 통신정보공학과 조교수

※ 주관심분야 : 정보보호, 암호이론, 알고리즘 개발