이동환경에서 환불 가능한 타원형 곡선 전자화폐

권 은 경[†] · 조 용 구[††] · 채 기 준[†††]

요 약

브랜드의 카운터 방식 전자화폐 알고리즘(BOCC)은 이동 환경에 적절하지만, 스마트 카드내 금액정보를 공격할 수 있다. 따라서 토큰 데이터에 지불 한계 금액을 삽입함으로써 상한금액을 넘어서 사용하지 못하도록 하고, 상한과 하한 값을 같게 하면 고정금액 토큰이 된다. 또한 온라인 거래에서 더욱 빈번히 발생 가능한 환불성을 추가한다. 기존의 BOCC는 이산대수문제(Discrete Logarithm Problem)에 근거하기 때문에 지수 승을 반복해서 수행하여야 한다. 그런데 제한된 계산 능력을 가진 이동단말의 경우는 계산량을 줄여야 한다. 따라서 타원곡선 알고리즘(ECC)을 적용함으로써 기능은 동일하나 계산량 감소를 얻을 수 있다.

A Refundable Elliptic Curve Electronic Cash in Mobile Environments

Eunkyeong Kwon[†] · Yonggu Cho[††] · Kijoon Chae[†††]

ABSTRACT

BOCC(Brand's Offline Cash with a Counter) is useful in mobile environments, but it has the possibility of attacking amount data in a smart card. To insert the upper & lower limitation of amount into a token data decreases the level of risk. If upper and lower values are same, it means a fixed amount token. Since refund can more often happen in on-line commerce, refundability is added. BOCC is based on Discrete Logarithm Problem, needs exponential computations. But mobile terminals like cell phones have low computational power. As a result, ECC is used to improve the performance supporting same security level.

키워드 : 전자화폐(Electronic Cash), 전자지불(Electronic Payment), 타원형곡선암호화(Elliptic Curve Cryptosystem), 환불성(Refundability), 이동보안(Mobile Security)

1. 서 론

무선 단말기를 이용한 계좌 이체, 증권 거래, 물품 구매, 원격 업무 등의 서비스를 이동 상거래라고 한다. 이동상거래는 웹 중심의 기존 전자상거래에 이동성을 확장한 것 이상의 의미를 갖는다. 전자화폐의 궁극적인 목적은 현재의 화폐를 대신하는 것이다. 그러기 위해서는 익명성, 이중 사용 방지, 복수 전달성, 환불성 등을 지원해야 한다. 본 논문에서는 이동 상거래의 주요 지불수단으로 등장할 스마트 카드를 포함한 이동전화에서의 전자화폐를 제안한다.

단위 금액으로 화폐 데이터를 사용하는 경우에는 금액 정보를 별도로 가질 필요가 없지만, 이동환경에 알맞은 브랜드의 카운터 방식 전자화폐(BOCC : Brand's Offline Cash with a Counter) 알고리즘에서는 화폐의 사용 횟수 별로 하나의 토큰이 사용되면서, 그때 사용하는 금액이 매번 바뀌는 형태이다[1-5]. 그런데 금액의 상한선을 두지 않으면, 카드가 공격 당했을 경우 피해액을 예측할 수 없다. 따라서 금액의 상한선이 필요하며, 이를 포함시키는 방법으로 화폐 데이터 자체에는 포함시키지 않고 상점에서 금액 상한선을 확인하는 방법이 있다. 이는 화폐 데이터에 금액 정보를 별도로 포함하는 것이 아니라 구현이 매우 간편하지만, 모든 사용자와 토큰에 대해 획일적으로 적용해야 하기 때문에 융통성이 매우 떨어진다. 그러므로 최대치와 최소치의 두 가지 금액 정보를 화폐 내에 포함시키는 것이 필요하다. 즉 가변금액 처리를 기본으로 환불성과 효율성을 지원하여 이동환경에 알맞은 전자화폐를 설계하고자 한다.

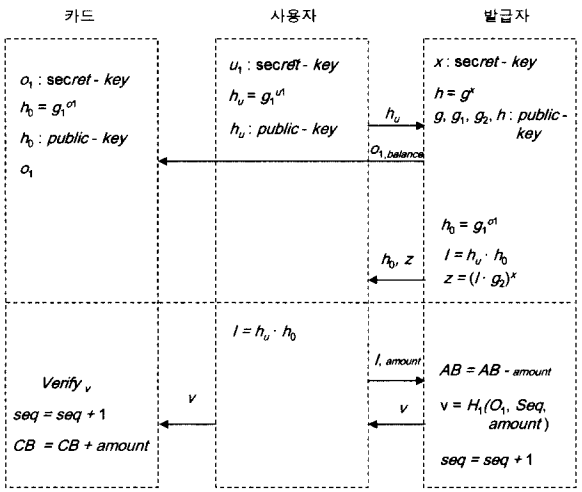
2장에서는 기존의 BOCC 알고리즘을 간략히 소개하고 3장에서는 토큰별로 지불 가능한 금액 상한선과 하한선을 보유하도록 알고리즘을 설계한다. 이를 통해 고정금액과 가변금액의 융통성 있는 혼합을 가능하도록 한다. 4장에서는 사용자와 상점의 부가적인 키 생성을 통해 환불이 가능하도록

† 정 회 원 : 계원조형예술대학 임베디드소프트웨어과 교수
†† 정 회 원 : 영동대학교 임베디드소프트웨어학과 교수
††† 종신회원 : 이화여자대학교 컴퓨터학과 교수
논문접수 : 2004년 2월 4일, 심사완료 : 2004년 4월 26일

한다. 5장에서는 구현에 제약사항을 갖는 이동단말의 상태를 감안할 때 계산량을 대폭적으로 감소시킬 수 있는 타원곡선 알고리즘 적용 방안을 제시한다. 6장에서는 단위함수와 그 집합으로 구분하여 이들의 횟수를 통해 개선된 성능을 예측한다. 일반 이동전화에서의 계산에 의한 성능과 보안용 전용 프로세서를 가진 이동전화에서의 성능을 비교한다. 마지막으로 7장에서 결론을 맺는다.

2. 카운터방식 오프라인 전자화폐(BOCC : Brand's Offline Cash with a Counter)

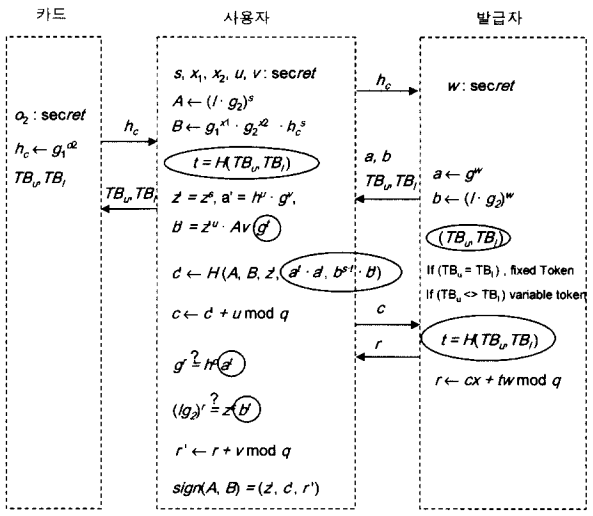
BOCC는 스마트 카드를 이용하여 이중사용 사전검출을 포함하는 카운터방식 오프라인 화폐 프로토콜이다. (그림 1)을 보면, 발급 기관에서 발급 기관과 카드가 공유하는 비밀 키 o_1을 카드에 넣어서 카드를 발급한 후, 그것의 공개키인 h_0를 함께 사용하여 I를 생성한다. 화폐를 발급할 때 카드에서 매번 임시 비밀 키 o_2을 생성하여 사용자에게 해당하는 공개 키 h_c를 제공하고 이것이 화폐 생성과정에 포함되도록 한다. 발급 기관과 은닉서명을 실시하는 과정은 통상적인 절차를 따른다. 실제로 화폐를 지불하는 과정에서는 카드에서 o_1과 o_2을 보유하고 있음을 입증하는 값인 r_1^0을 보내면 사용자는 이를 수신하여 검증한 후 최종적으로 상점에 전달할 r_1, r_2를 계산하게 된다. 카드에서는 o_2을 사용한 후 반드시 삭제하도록 한다. 여기서 o_2가 두 번 사용되면 이중사용이 가능하기 때문이다. 따라서 카드의 연동 없이는 화폐의 발급과 지불이 모두 불가능하며, 카드가 정상적으로 작동된다고 가정하면 이중 사용의 사전방지가 가능해진다.



(그림 1) BOCC 초기설정

3. 가변금액 전자화폐(ECVL : Electronic Cash of Variable Limit)

사용자와 발급 기관간의 초기설정 과정은 기존의 BOCC 알고리즘과 동일하다. 변경 사항은 토큰 발급, 토큰 지불, 예치의 세 과정에서 일어난다. 우선 토큰 발급 과정을 살펴본다. 사용자가 자신의 신분을 인증 받은 후 원하는 종류의 토큰 발급을 신청하게 된다. 사용자의 신용 정보에 따라 가부 여부를 판단하여 허가가 되면 발급 기관은 사용자에게 a, b, TBl, TBu를 보낸다. 사용자는 TBl, TBu를 이용하여 해쉬 값을 계산한다. 이는 c'을 계산하는데 포함시킨다. c'을 이용해 계산된 c가 도전으로서 발급자에게 보내지고 발급 기관은 사용자와 동일하게 TBl, TBu를 이용하여 해쉬 값을 계산한 후 응답 값에 포함시켜서 보낸다. 사용자는 올바른 응답인지를 확인하는 과정에서 토큰 금액의 해쉬 값을 이용한다. 최종적으로 화폐 데이터는 기본의 알고리즘과 동일하게 z', c', r'이 되기 때문에 화폐 데이터 길이에는 변동이 없다. (그림 2)는 화폐 발급 절차를 순서적으로 보여준다. 동그라미 표시 부분이 기존의 BOCC와 차이 나는 부분이다. 여기서 h_u는 $g_1^{u_1}$으로서 사용자의 공개 키에 해당하는 것이고 h^u는 $(g^x)^u$로서 $h = g^x$가 발급기관의 공개 키에 해당한다.



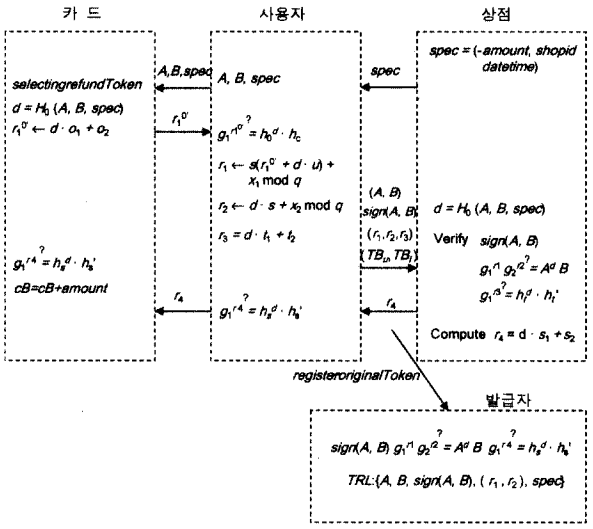
(그림 2) ECVL - 화폐발급

4. 환불가능 가변금액 전자화폐(RECVL : Refundable ECVL)

환불성이란 사용자가 한 상점에서 물건을 환불 시 발급기관의 도움 없이 해당 화폐를 재 사용할 수 있도록 해주는 특성이다. 이를 지원하기 위해서는 다음의 몇 가지 요구

사항이 필요하다. 첫째, 사용자를 검증해야 한다. 본래의 물건을 구매한 사람인지를 확인하는 것이다. 둘째, 상점의 확인을 검증해야 한다. 사용자가 일방적으로 환불을 주장할 수 없도록 조치해야 한다. 셋째, 상점의 불법적인 예치를 방지해야 한다. 환불이 발생한 화폐에 대해서는 예치가 일어나지 않도록 처리해야 한다. 마지막으로 사용자가 발급기관의 도움없이 해당 금액을 간편하게 재사용할 수 있어야 한다. 또한 본래의 화폐 특성인 익명성과 이중사용방지 기능을 동일하게 지원하여야 한다.

토큰을 발급 받는 과정에서 금액의 상한과 하한선이 음수인 경우는 환불용 토큰을 의미하도록 한다. 사용자와 상점은 지속적으로 사용하는 한 쌍의 비밀 키와 공개 키를 갖는다. 이를 사용자용으로 *ownerid*로 하고, 상점용으로 *shopid*로 한다. 이 *ownerid, shopid*는 사전에 분배된 상태라 가정한다. 공개 키를 각각의 고유번호로 이용하는 것도 가능하다. 또한 트랜잭션별로 다시 한 쌍의 비밀 키와 공개 키를 생성한다. 사용자용으로 *tokenid*라 하고, 상점용으로 *transid*라 한다. 정상구매 절차에서 서로의 *tokenid, transid*를 전달받는다. 사용자는 구매 정보와 상점의 공개 키를 상점은 사용자 정보와 사용자의 공개 키를 함께 저장하도록 한다. 환불 가능 기간 내의 환불 절차는 (그림 3)과 같다. 우선 금액 데이터는 음수가 되어야 한다. 즉 금액이 사용자 카드에 가산됨을 의미한다. 사용자는 자신이 이전 토큰을 사용한 사용자임을 입증하기 위해 r_3을 부가적으로 전달한다. r_3는 사용자의 *ownerid, tokenid*의 비밀 키를 이용해 계산된다. 따라서 상점은 미리 보관한 *tokenid*를 이용하여 검증 가능하다. 또한 d를 계산 내에 포함시키기 때문에 정확한 금액 데이터를 보장할 수 있다. 상점은 r_4를 계산하여 사용자에게 보내면 사용자는 본래 토큰을 지불한 곳과 같은 상점임을 검증할 수 있다. 즉 미리 보관한 *transid*를 이용하면 된다. 이렇게 서로간의 검증이 확인되고 나면 사용자는 즉시 발급 기관에 폐기된 토큰을 등록해야 한다. 이때 본래 사용된 토큰 정보와 상점으로 받은 r_4를 포함하여 발급 기관으로 전송하면, 발급 기관에서는 토큰이 올바른 지와 상점에서 환불을 서명하였는지를 함께 검증한 후 성공하면 TRL(Token Revocation List)에 등록하게 된다. 사용자가 환불에 사용한 토큰을 등록할 필요가 없다. 금액 정보가 음수이기 때문에 단지 토큰 정보만으로 환불용이라는 것이 증명된다. 상점에서 예치하는 과정에서, 만약 구매에 사용한 토큰을 발급 기관에 전송하면, 발급 기관은 해당 토큰을 TRL에서 발견하여 예치되지 않는다. 그리고 환불 토큰을 발급 기관에 전송하면, *spec*내 음수 금액을 보고 예치를 중지한다. 만약 사용자가 *spec*내 양수 금액을 전송한다면, 올바르지 않은 토큰으로 판명된다. 즉 발급자의 안전성이 보장된다. 또한 사용자와 상점의 안전성은 부가적으로 추가된 t_1, s_1에 의해 보장된다. 즉 원래의 토큰을 지불한 사용자의 검증과, 환불을 합의한 상점의 검증이 이를 통해 이루어진다.



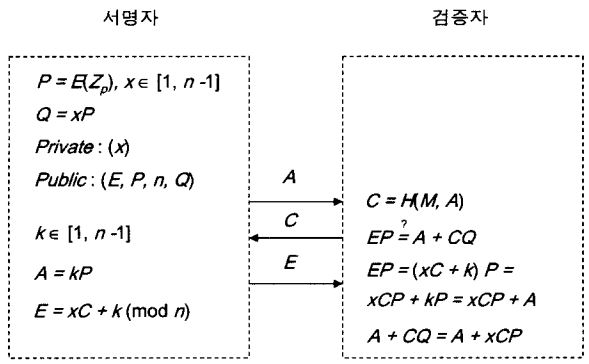
(그림 3) RECVL 환불

5. 환불가능 타원형곡선 가변금액 전자화폐 (REECVL : Refundable Elliptic curve ECVL)

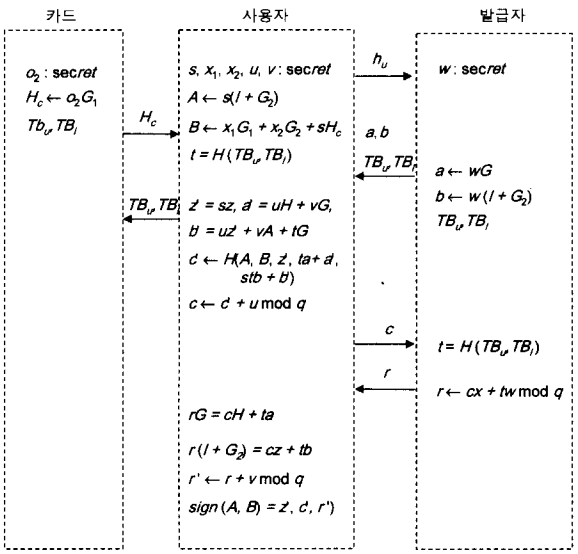
이제까지 제안된 알고리즘은 계산 및 저장 능력의 제한을 갖는 스마트 카드와 이동전화에서의 성능을 보장하기 어렵다. 먼저 동일한 기능을 제공하면서 우수한 성능을 지원해주는 ECC(Elliptic Curve Cryptography)에 대해 살펴본다. ECC는 차세대 암호화 기법 중의 하나로 다른 암호화 기법보다 적은 키 비트 수로도 신뢰성있는 암호화가 가능하다는 장점이 있다[6-8]. RSA로 1024비트 키 암호화한 것과 ECC 160비트 키를 갖는 시스템이 같은 안전도를 가진다[9].

(그림 4)와 같이 타원곡선을 이용한 온닉서명에서 P, Q는 ECC 곡선 상에 두 점이다. 비밀 키에 해당하는 상수 x, k는 n-1보다 적은 수이며 상수와 곡선상의 점간의 곱셈은 ECC 곡선 상의 점을 상수만큼 반복해서 더하는 것과 같은 결과이다. C = H(M, A)에서 M은 서명하고자 하는 메시지에 해당하고, A는 곡선상 좌표이므로 해쉬에서는 x좌표 만을 이용한다. 수신자측에서 증명하는 과정에 덧셈과 곱셈의 분배법칙이 성립하기 때문에 위와 같은 변환이 도출된다. 이러한 기본 원리를 이용하여 RECVL에서 기존 이산대수

문제를 타원형 곡선 이산대수문제형식으로 변경하는 것이 가능하다. (그림 5)는 타원 곡선 이산대수문제를 적용하여 변경된 화폐발급 절차를 보여준다.



(그림 4) 타원곡선을 이용한 은닉서명



(그림 5) REECVL - 화폐 발급

6. 검 증

BOCC와 RECVL에서 가장 시간을 많이 차지하는 부분은 지수승이므로 그 횟수를 이용하여 성능을 비교하고자 한다. 지수승은 exp, 공통적인 키 검증 집합은 verify, 키 생성은 kGen이다. 다음의 <표 1>은 지수승과 공통적인 검증집합의 횟수를 비교한 것이다. 환불성은 BOCC에 없는 기능이므로 비교 대상에서 제외하였다. 인출 부분에서 이동전화의 지수승 회수는 3회 많은 것을 볼 수 있고 지불 절차에서는 상점과 이동전화가 각각 1회 키 생성 횟수가 많은 것을 볼 수 있다. 예치과정은 기존과 동일하다. 단위 지수승의 계산 시간을 실험에 의해 알아낸 후 증가하는 횟수에 대한 증가 정도를 예측할 수 있다.

<표 1> 지수승 횟수 비교(시간 복잡도)

스키마	인 출				지 불					
	발급자	이동전화		카드	상 점		이동전화			카 드
기능	exp	exp	verify	exp	exp	kGen	exp	verify	kGen	exp
BOCC	2	**11**	**2**	1	7	0	**0**	**1**	**0**	0
RECVL	2	**14**	**2**	1	7	1	**0**	**1**	**1**	0

실험 환경은 Intel Pentium 4, 1.60GHz, 512MB RAM를 가진 PC이다. DH와 ECDH의 단위시간을 계산하면 <표 1>을 이용하여 BOCC, RECVL, REECVL를 모두 계산할 수 있다. exp는 단위 지수승 또는 타원형의 포인트 연산이고, kGen은 키 생성 시간을 의미한다. verify는 상대방으로부터 인증데이터를 얻어서 검증하는 단위계산 집합을 의미한다. 즉 DH에서 exp, verify, kGen 단위 시간 계산을 하고 ECDH에서 mul, verify, kGen 단위 시간 계산을 한 후 DH 단위 시간을 이용해서 BOCC & RECVL 인출과 지불 시간을 계산하고 ECDH 단위 시간을 이용해서 EBOCC & REECVL 인출과 지불 시간을 계산하는 것이다. (그림 6)을 보면 REECVL는 BOCC에 비해 지불절차에서 약 68% 개선되었음을 알 수 있다.

그런데 실제 이동전화나 스마트 카드의 경우에 어느 정도 성능이 감소되는 지 예측할 필요가 있다. 다음의 <표 2>는 일반 PC와 ARM 프로세서에서 계산된 성능 비교치이다 [㈜장미디어]. 여기서 시스템1은 Intel Pentium II 350MHz, Microsoft Windows 2000, 시스템2는 Intel StrongArm 1110 206MHz, Microsoft Windows CE 3.0를 의미한다.

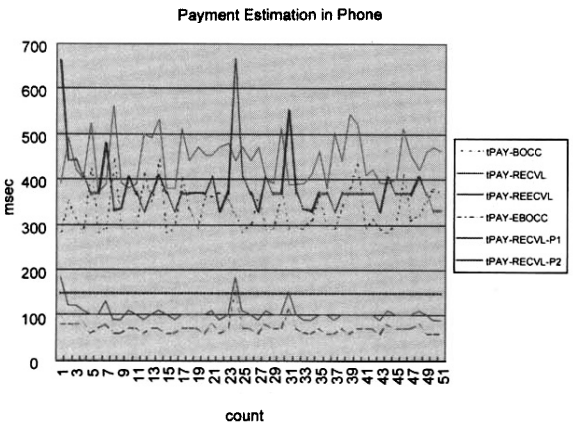
<표 2> 시스템별 성능 비교

	ECDSA 160bit		
	Key generation	signature	validation
시스템1	0.006	0.006	0.012
시스템2	0.011	0.011	0.023

그런데 본 논문의 실험 PC 사양과 위의 <표 2>의 PC 사양이 다르고 또한 테스트 환경도 다르기 때문에 이를 그대로 이용할 수가 없다. 인텔의 사양 별 성능 비교 자료(www.intel.com)를 이용하면 1GHz와 500MHz간의 정수 계산력은 상대적으로 1.96배가 감소한다고 나온다. 이러한 상대적 수치를 본 논문의 실험 PC와 <표 2>의 시스템1과의 차이로 계산하고, 다시 시스템1과 시스템2간의 차이인 1.87배 감소를 본 논문의 실험 PC의 다음 단계 계산에 적용하면 최종적으로 <표 2>의 시스템2와 같은 사양에서 예측되는 결과가

계산된다. 이 수치에 의하면 (그림 6)에서 tPAY-REECVL-P1와 같이 BOCC와 유사한 수준으로 상당히 낮은 성능을 예측할 수 있다.

그러나 최근 대부분의 이동전화와 스마트 카드의 시스템 구성도를 살펴보면 보안용 코프로세서와 같은 전용 보안 엔진의 탑재를 통해 상당히 높은 수준의 성능을 보장해 준다고 명시되어 있다. 그런데 특히 "SecurCore(20MHz)"를 채택한 경우에, 타원형 곡선의 경우 192비트 DH계산도 100ms 이하를 보장해 준다고 한다. 즉 더 시간이 많이 소요되는 검증의 경우가 100ms라면 상대적인 기준치를 적용해서 키 생성의 경우는 48ms로 예측할 수 있다(<표 2>의 시스템2의 비교치를 이용하여 나누기 2.1 적용함). 즉 이 값은 보안용 전용 프로세서를 탑재한 경우에 해당한다. (그림 6)의 tPAY-REECVL-P2(평균148ms)와 같이 당초의 tPAY-REECVL보다 약간 낮은 성능이므로, 실제로 이동전화나 스마트 카드 적용에 문제가 없음을 알 수 있다.



위부터 RECVL, REECVL-P1, BOCC, REECVL-P2, REECVL, EBOCC 순서임.

(그림 6) 지불 소요시간 비교

7. 결 론

BOCC의 안전도를 높이기 위해 금액 정보를 화폐에 포함시킨 ECVL, 일정 기간 내에 온라인 환불이 가능한 RECVL, 지수승 계산량의 부담을 줄여서 이동 단말에서의 구현을 가능하도록 이산대수문제를 타원 곡선 이산대수문제로 변경한 REECVL를 제시하였다. 실험과정에서 첫째 PC에서의 BOCC, RECVL, REECVL를 비교하여서 REECVL는 BOCC에 비해 인출 64%, 지불 68% 개선되었음을 알게 되었다. 실제로 이동전화 또는 스마트 카드는 보안을 위한 전용 프로세서 및 엔진을 탑재하게 되면 REECVL과 거의 유사한 성능을 유지하므로 전자화폐의 기본 요구 사항인 프라이버시, 익명성, 이중사용방지는 그대로 보장하면서 부가적으로 환불성을 지원하며 이동환경에서 성능이 보장됨을 검증하였다.

참 고 문 헌

[1] S. Brands, "Off-line Cash Transfer by Smart Card," CWI Report CS-R9455, 1994.

[2] S. Brands, "Electronic Cash on the Internet," Symposium on Network and Distributed System Security, Feb., 1995.

[3] S. Brands, "Restrictive Blinding on Secret-Key Certificates," CWI Report CS-R9509, 1995.

[4] S. Brands, "Off-line Electronic Cash Based on Secret-Key Certificates," Proceedings of the Second International Symposium of Latin American Theoretical Informatics (Latin '95), Apr., 1995.

[5] S. Brands, "Untraceable Off-line Cash in Wallets with Observers," In Advances in Cryptology-Proc. of CRYPTO '93, LNCS, Springer-Verlag, Vol.773, pp.302-318, Aug., 1994.

[6] A. Juristsic and A. J. Menezes, "Elliptic Curves and Cryptography," Certicom Corp, ECC White papers, http://www.certicom.com.

[7] A. J. Menezes, "Elliptic Curve Public Key Cryptosystems," Kluwer Academic Publishers, Boston, MA, 1993.

[8] D. B. Johnson and A. J. Menezes, "Elliptic Curve DSA (ECDSA) : An Enhanced DSA," Certicom Corp, ECC White papers, http://www.certicom.com.

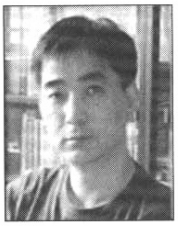
[9] A. K. Lenstra and E. R. Verheul, "Selecting Cryptographic Key Size," The 3rd Workshop on Elliptic Curve Cryptography(ECC'99), Nov., 1999.

[10] N. Ferguson, "Single Term Off-line Coins," Advances in Cryptology Proc. of Euro-crypt '93(Lecture Notes in Computer Science), Springer-Verlag, pp.318-328, 1993.

[11] T. P. Pederson, "Electronic Payments of Small Amounts," Cambridge Workshop on Security Protocols, Vol.1189, pp.59-68, 1997.

권 은 경

e-mail : ekkwon@kaywon.ac.kr
연세대학교 전산과학과 학사
연세대학교 대학원 전자계산전공 석사
이화여자대학교 대학원 컴퓨터학과 박사
현재 계원조형예술대학 임베디드소프트웨어과 조교수
관심분야 : 이동보안, mobile IP, Creative Embedded System



조 용 구

e-mail : ygcho@youngdong.ac.kr
광운대학교 전자통신과 학사
광운대학교 대학원 전자통신과 석사
광운대학교 대학원 전자통신과 박사
현재 영동대학교 임베디드소프트웨어학과 부교수
관심분야 : 이동보안, 경영학, Creative Embedded System

채 기 준

e-mail : kjchae@ewha.ac.kr
1982년 연세대학교 수학과(이학사)
1984년 미국 Syracuse University 컴퓨터학과(이학석사)
1990년 미국 North Carolina State University 컴퓨터공학과(공학박사)
1990년~1992년 미국 해군사관학교 컴퓨터학과 조교수
1992년~현재 이화여자대학교 컴퓨터학과 교수
관심분야 : 네트워크 보안, 인터넷/무선통신망/고속통신망 프로토콜 설계 및 성능분석