타원곡선 암호를 이용한 PDA 기반의 신용카드 결제 프로토콜 설계

유 성 진[†] · 김 성 열[††] · 윤 천 균[†††] · 정 일 용[††††]

요 약

M-Commerce에서 안전한 서비스를 제공하기 위해서는 보안 기능을 갖춘 결제 솔루션이 필수적이다. M-Commerce를 이용하기 위한 사용자의 이동 단말기는 핸드폰, PDA, 스마트폰 등으로 다양화 되어가고 있으며, 이 중에서도 PDA의 인터페이스와 이동 접속은 기존 핸드폰의 유선 인터넷의 정보 의존도가 높은 단점을 극복할 수 있다. 본 논문에서는 타원곡선 암호를 이용하여 PDA 기반의 신용카드 결제 시스템을 설계하였다. 제안된 시스템의 SECURE CARD 모듈은 PDA 단말기 자체에 개인정보, 배송정보, 카드정보를 암호화하여 안전하게 저장함으로써 단말기의 정보입력시에 필요한 불편함을 제거하였다. 또한 프로토콜은 M-Commerce에서 인증, 기밀성, 무결성, 부인봉쇄 서비스 등의 보안기능을 제공하도록 설계되었다.

A Design of Protocol for Credit Card Transaction on PDA Using ECC

Seongjin Yu[†] · Seongyoul Kim[††] · ChunKyun Youn[†††] · Ilyong Chung[††††]

ABSTRACT

In order to provide information services on M-Commerce, a payment solution with security functions should be required. User's mobile terminals for using M-Commerce services are diversifying to cellular phone, PDA, Smart phone etc. Among them, integration of PDA's interface and mobile connection overcomes the weak point of existing cellular phone depending on information via the internet. In this paper, the protocol for a credit card transaction on PDA using ECC is presented. Secure Card module on this protocol encrypts user's information such as private information, delivery information and credit card information and store them on PDA in order to free from inputting information whenever it is used. This scheme also offers security services on M-Commerce including authentication, confidentiality, integration, non-repudiation and so on.

키워드 : 타원곡선 암호(ECC), 신용카드 결제(Credit Card Transaction)

1. 서 론

최근 이동통신망의 급속한 발전과 더불어 PDA 등 소형 정보 단말기의 보급 확대 및 고속데이터전송을 근간으로 하는 IMT-2000의 상용화가 국내뿐 아니라 세계적으로 확대되고 있다. 이러한 흐름에 따라 기존 개인용 컴퓨터 등의 고정 단말기를 기반으로 한 E-Commerce 형태를 벗어나 이제는 이동성(mobility), 휴대성(portability)를 제공하는 새로운 형태의 M-Commerce[1-3]가 보편화되고 있다. 이러한 M-Commerce에서 안전한 서비스를 위해서는 서비스의 특성에 알맞은 무선 결제서비스(Mobile Payment Service)[4]의 연구가 활발하게 진행되고 있다. 현재 무선결제 서비스는 이동통신사를 중심으로 소액결제 서비스가 주로 이루어지고 있으며, 현재 핸드폰 중심의 상거래는 무선 서비스 독자적인 경우보다는 사용자가 유선 상에서 자료를 보고 구매를 결정하는 유선 의존도가 높은 결제방식[5]이다. 이에 반하여 신용카드 기반의 결제구조는 고액결제가 가능하다는 강점을 가지고 있다. 그러나 신용카드 기반 결제구조는 무선 인터넷 인프라가 부족하여 무선결제 시스템에 취약하다는 문제점을 내포하고 있다. 따라서 무선기반 정보제공능력, 고액결제 서비스가 가능한 시스템이 요구된다.

<표 1>은 무선 결제 서비스의 제공능력[6]을 나타내고 있는데 이에 따르면 이동통신사는 무선결제 플랫폼, 과금시스템, 소액결제능력 등에 대해서는 우수하게 나타나고 있으나, 고액결제능력, 신용위험관리, 타 금융서비스와의 연계 등의 부분에서는 다소 미흡한 결과를 보여주고 있다.

† 준 회 원 : 조선대학교 대학원 전자계산학과
†† 정 회 원 : 울산과학대학 컴퓨터정보학부 교수
††† 정 회 원 : 호남대학교 정보기술학부 교수
†††† 종신회원 : 조선대학교 컴퓨터공학부 교수

논문접수 : 2002년 8월 22일, 심사완료 : 2003년 8월 5일

〈표 1〉 무선결제 서비스 제공능력

구 분	이동통신사	은 행	신용카드사
무선결제 플랫폼	●	○	○
과금(빌링)시스템	●	◑	●
소액결제 능력	●	◑	◑
고액결제 능력	○	●	●
신용위험관리	○	●	●
소비자 확보	●	◑	◑
가맹점 확보	○	◑	●
계정관리	○	●	●
타금융서비스와 연계	○	●	◑
자금결제 신뢰감	◑	●	●
● : 우수 ◑ : 보통 ○ : 부족			

현재 보안측면에서 RSA와 같은 공개키 암호 시스템은 유선상에서 우수한 보안도구로 여겨지고 있으나, 키 사이즈가 너무 크고 처리속도가 느리다는 단점이 있다[7]. 따라서 무선 환경의 낮은 CPU, 적은 메모리의 무선단말기에 적합하지 않은 것으로 판단되고 있다. 이를 보완하기 위해서 무선단말기에 적합한 무선 공개키 기반구조(WPKI)[8-11]의 방향으로 연구가 진행되고 있고 적은 비트수와 빠른 계산 속도를 지원하는 ECC 공개키 암호 시스템[7, 12, 13]에 대한 관심이 증가되고 있다. ECC 공개키 암호 알고리즘의 장점은 첫째로, 다른 공개키 암호 시스템에 비해 가진 큰 장점은 키의 크기가 작다. 둘째로, 전형적인 RSA 시스템에서 사용되는 키의 크기는 1024비트이지만, 같은 보안 수준을 제공하는 ECC 시스템을 구현하기 위해서는 키의 크기가 160비트만 되더라도 충분하다. 셋째로, 계산적인 측면에서도 RSA에 비해 보다 낮은 비용을 요구함으로 많은 비용을 요구하는 소수의 분석과 같은 과정이 ECC에서는 필요치 않다. 넷째로, 소형기기나, 무선기기와 같은 제한된 성능의 시스템에서도 효율적으로 운용이 가능하다는 것이다[14]. <표 2>는 RSA, DSA, ECDSA의 알고리즘들의 속도를 비교[15]한 것이다.

〈표 2〉 알고리즘 속도 비교표

(단위 : msec)

테스트 환경			
CPU : Pentium III 555Mhz, 메모리 : 256MB, OS : x86 Solaris 8			
수 행 결 과			
	DSA	ECDSA	RSA
공개키 크기	1024bit	160bit	1024bit
서명생성	12.8	8.4	50.6
서명검증	28.5	18.8	2.6

본 연구에서는 현재 PDA 시장의 확대에 맞추어 소액결제 방식이 아닌 신용카드 기반의 안전한 고액결제 시스템을 ECC를 기반으로 설계하였다. 또한 모바일 환경을 고려하여 결제 편의성을 갖추도록 하였다.

본 논문의 구성은 2장에서는 무선인터넷 보안에 대하여 기술하고, 3장에서는 SECURE CARD에 대하여 기술하고, 4장에서는 SECURE CARD 기반 프로토콜에 대하여 기술하고, 5장에서는 결론에 대하여 기술한다. 마지막은 참고문헌이다.

2. 무선인터넷 보안

무선인터넷 솔루션은 크게 2가지로 구분할 수 있다. 첫째는 기존 유선 인터넷에서의 프로토콜인 HTTP 기반으로 무선 데이터 서비스를 제공하는 경우이며, 다른 하나는 무선 네트워크 환경에 적합한 새로운 프로토콜을 개발하여 무선 데이터 서비스를 제공하는 방법인 WAP이다. 무선인터넷에서의 정보 보호 서비스는 크게 기밀성, 사용자 인증, 데이터의 무결성, 부인봉쇄 서비스[14]가 있다.

기밀성은 네트워크를 통해 전송되는 데이터는 권한이 부여된 사람만이 내용을 볼 수 있게 하는 서비스이며, 사용자 인증은 메시지를 작성한 사람의 신원을 확인할 수 있게 해주는 서비스이다.

데이터의 무결성은 전송된 데이터가 전송 도중에 변경되었는지 확인할 수 있는 서비스이며, 부인 봉쇄는 송신자가 메시지를 송신한 사실을 부인하거나 수신자가 수신 사실을 부인할 수 없게 하는 서비스이다.

2.1 WAP에서의 보안

WAP 포럼에서는 무선 환경에 적합한 프로토콜을 정의하는 작업을 진행 중인데, 이 가운데 보안 프로토콜은 WTLS (Wireless Transport Layer Protocol)이다. WTLS는 통신을 하는 두 응용프로그램 사이에 안전한 채널을 형성하여 통신 내용의 보안을 보장하는 방법이다. WTLS는 WTP(Transaction Layer)와 WDP(Transport Layer) 사이에서 수행되기 때문에 특정 응용프로그램에 종속되지 않고, WAP를 사용하는 모든 응용프로그램들을 지원한다. WTLS는 기밀성, 사용자 인증, 무결성 등의 보안 서비스를 제공한다[14]. 그러나 WAP에서의 가장 큰 문제점은 종단간 보안을 제공하지 못하고 있다. 종단간 보안에 관련하여 많은 연구가 진행중에 있다[16, 17].

2.2 HTTP에서의 보안

기존 인터넷 표준을 사용하여 무선인터넷을 구현하는 것이 마이크로소프트의 전략이며 이를 위해 이동전화에서 사용할 수 있는 모바일 익스플로러(Mobile Explorer : ME)와 PDA급의 단말기에서 사용할 수 있는 포켓 익스플로러(Pocket Explorer : PE)라는 HTML 브라우저를 만들어 보급하였다. ME와 PE에서는 유선 SSL[18]을 변형시킨 MSSL(Mobile Secure Socket Layer)을 이용한다. MSSL도 유선 SSL과 마찬가지로 부인봉쇄 서비스와 종단간 보안을 완벽하게 지원하지 않는다[14, 19].

3. SECURE CARD 어플리케이션

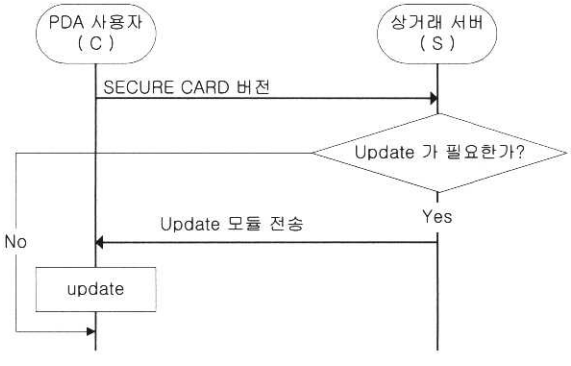
PDA는 이동성이 강한 정보기기로 기존 유선상의 정보기기에 비하여 정보입력 작업이 원활하지 않은 입력 구조를 가지고 있다. 따라서 PDA 기반의 결제 솔루션을 제공하는데 거론될 수 있는 문제가 사용자와의 인터페이스이다. 이동기기의 정보입력 불편의성의 문제를 해결하고 안전한 결제 솔루션을 제공하기 위하여 SECURE CARD를 설계하였다. SECURE CARD는 사용자가 정보를 입력하면 그 정보를 PDA에 저장하여 모든 상거래 서버와 거래할 때 사용할 수 있도록 구성하였다. 또한 PDA 분실시 개인정보 보호를 위해 입력된 정보는 안전한 블록 암호 알고리즘을 이용하여 암호화하여 저장된다.

본 연구에서 제안하는 SECURE CARD는 설치 모듈, 인증 모듈, 거래정보 관리 모듈, 암·복호화 모듈, 지불처리 모듈로 구성된다.

3.1 SECURE CARD 설치 모듈

사용자는 안전한 거래를 위하여 M-Commerce를 이용하고자 할 때 전자 상거래 서버로부터 SECURE CARD 프로그램을 다운받아 설치하여야 한다. 한번 설치가 되면 SECURE CARD는 제휴된 모든 M-Commerce 환경에서 사용이 가능하다. 설치 절차는 (그림 1)과 같이 설치된다.

(그림 1) SECURE CARD 설치

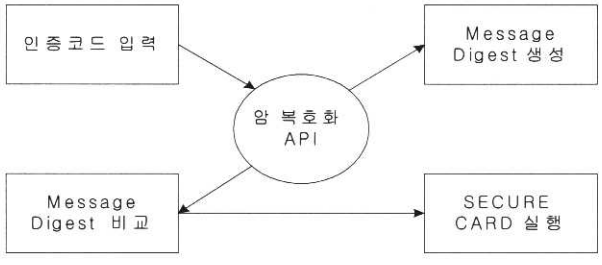


(그림 2) SECURE CARD Update

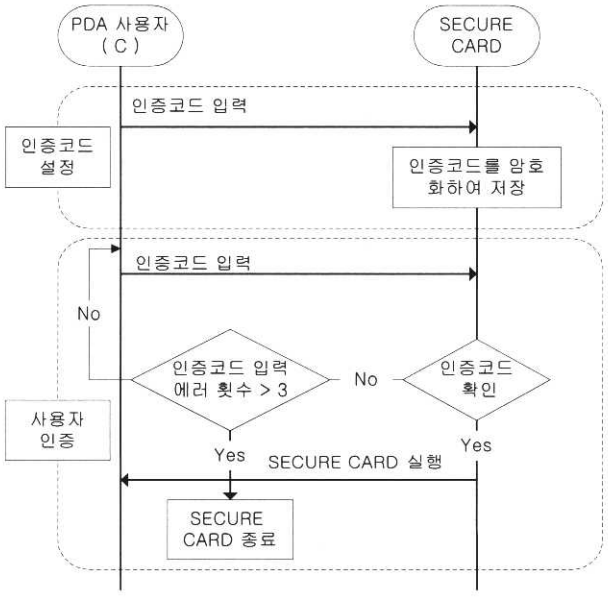
사용자의 PDA에 SECURE CARD가 설치가 되어 있으면 사용자가 상거래서버에 접속할 때 버전을 비교하여 구 버전일 경우 (그림 2)와 같이 자동으로 Update가 되게 된다.

3.2 SECURE CARD 인증 모듈

SECURE CARD 인증 모듈은 SECURE CARD 어플리케이션을 실행할 권한이 있는지를 결정한다. 사용자는 SECURE CARD 설치후 인증코드를 설정하고 인증코드는 암·복호화 모듈에 의해 암호화되어 저장된다. 인증코드 설정 이후의 인증 절차는 이미 저장된 Message Digest와 비교하여 동일한 경우에만 PDA의 SECURE CARD 프로그램을 실행시킨다. (그림 3)은 인증방법을 나타낸 것이고, (그림 4)는 인증모듈의 절차를 표현한 것이다.



(그림 3) SECURE CARD 인증 방법

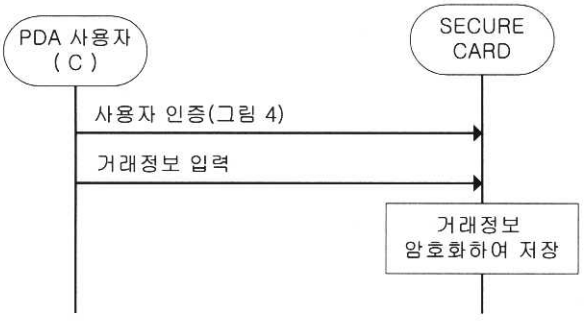


(그림 4) SECURE CARD 인증 모듈

3.3 SECURE CARD 거래정보 관리 모듈

거래정보 관리는 온라인상에서 회원가입 또는 상거래 거래시 필요한 정보의 활용을 위해서 개인정보, 배송정보, 카드정보의 필수 항목을 관리한다. 개인정보에는 ID, 인증코드, 이름, 주민등록번호, E-mail 주소, 전화번호를 필수항목으로 하여 사전에 입력받는다. 배송정보와 카드정보는 다수의 데이터를 입력 받을 수 있어야 한다. 사용자들은 보통 최소 집,

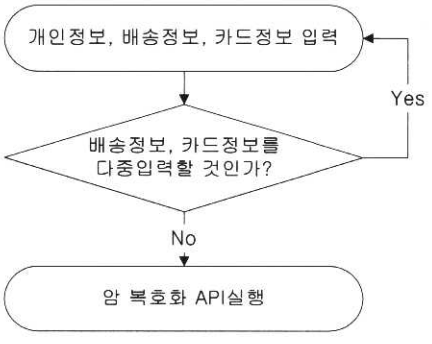
회사 2개의 배송지를 사용하고 카드도 1개 이상을 사용하는 것이 일반적이다. 따라서 사용자는 최종 결제시 SECURE CARD를 실행한 후 다수의 배송지역에서 원하는 배송정보를 옵션에서 선택하게 되며, 그 정보는 유형, 받는 사람, 우편번호, 주소, 전화번호를 필수 항목으로 정하여 입력한다. 사용자는 자신이 소유하고 있는 카드정보도 PDA에 미리 저장한다. 카드에 대한 필수 항목은 카드번호, 유효기간(년, 월)로 설정하였다. (그림 5)은 거래정보 관리를 나타낸 것이다.



(그림 5) SECURE CARD 거래정보 관리

3.4 암·복호화

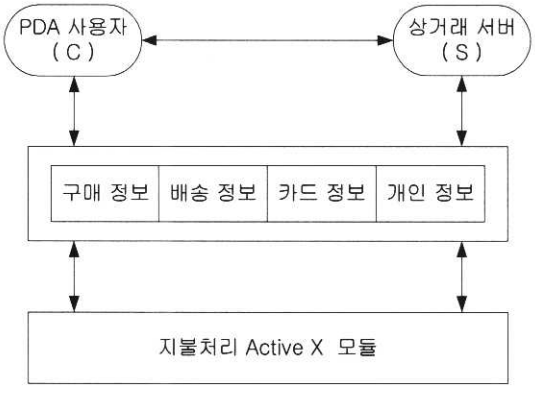
SECURE CARD는 사용자로부터 입력받는 개인정보, 배송정보, 카드정보를 암호화하여 PDA에 저장하며 복호화 작업도 수행한다. 암·복호화 모듈은 다른 암·복호화 알고리즘을 추가적으로 확장할 수 있다. 암·복호화 모듈은 (그림 6)과 같이 입력받은 개인정보, 배송정보, 카드정보를 사용자가 초기에 입력한 인증코드를 이용하여 암·복호화 기능을 수행한다.



(그림 6) 암·복호화

3.5 지불처리 Active X 모듈

사용자가 상품을 구매 요청하는 경우 서비스 제공자는 구매정보를 Active X 컨트롤을 이용하여 PDA 사용자의 SECURE CARD로 전송한다. PDA 사용자는 구매정보를 확인한 다음 자신의 배송정보, 카드정보를 선택하여 Active X 컨트롤을 이용하여 서비스 제공자의 SECURE CARD로 전송한다. 배송정보와 카드정보는 암·복호화 모듈에 의해서 암호화되어 전송된다. 상거래서버도 사용자에게 전달할 데이터가 있을 경우 사용자처럼 Active X 모듈을 이용하여 암호화된 데이터를 전송한다. 지불처리 모듈의 상세 절차는 4장에서 기술한다. (그림 7)은 지불처리 Active X 모듈을 표현한 것이다.



(그림 7) 지불처리 Active X 모듈

4. SECURE CARD 기반 프로토콜

4.1 개 요

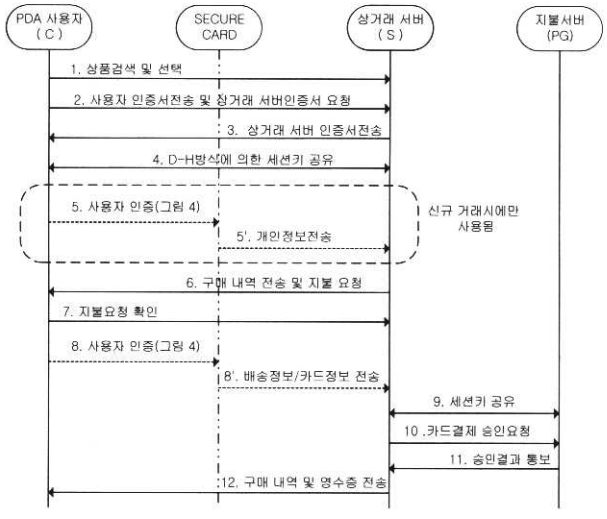
인증서는 신뢰된 인증기관으로부터 발급 받는다. 세션키를 사용하여 거래정보를 암호화할 알고리즘은 안정성이 보장된 블록 알고리즘이라고 가정한다. 사용자는 제안된 프로토콜을 이용하여 M-Commerce를 쉽고 편리하게 사용할 수 있다. 제안된 프로토콜은 <표 3>의 표기법을 따른다.

〈표 3〉 제안된 프로토콜 표기법

표 기	설 명
C	PDA 사용자 고객
S	상서래 서버
PG	지불 게이트웨이
Item	상품
PList	구매 목록
PR	지불 요청
PRA	지불 요청 승인
CI	신용카드 정보(카드번호, 유효기간)
PI	개인 정보(이름, 주민등록번호, 전화번호)
DI	배송 정보(주소, 우편번호)
CAI	신용카드 승인 정보
CR	신용카드 영수증
ID_i	i의 식별자
PK_i	i의 공개키
SK_i	i의 개인키
K_{cs}	C와 S의 공유된 세션키
S_{cs}	C와 S의 공유된 비밀키
A || B	A와 B 데이터의 연접
$E_k[m]$	k를 이용하여 m을 암호화
h{m}	m을 해쉬함수로 수행
$Time_i$	타임스탬프

4.2 PDA 기반 안전한 신용카드 결제 프로토콜

제안된 프로토콜 수행절차는 (그림 8)과 같고, 사용자는 신용카드를 발급 받을 때 비밀번호를 함께 등록한다. 비밀번호는 M-Commerce를 이용할 때 지불서버와 사용자의 비밀키로 사용되어진다. 사각형 점선 부분은 처음 거래하는 상거래 서버에서만 발생하게 된다.



[각 단계별 Transaction 표기]

[단계 1] C → S : Item
[단계 2] C → S : E_{SKauth} [$Time_1$, ID_c, KU_c]
[단계 3] S → C : E_{SKauth} [$Time_2$, ID_s, KU_s]
[단계 4] S ↔ C : EC-DH Key Exchange
[단계 5] C → S : E_{Kcs} [PInfo]
[단계 6] S → C : E_{Kcs} [PList || PR]
[단계 7] C → S : E_{Kcs} [PRA]
[단계 8] C → S : E_{Kcs} [DI || E_{SCPG}[CI] || $Time_3$ || E_{SKc}[h{DI || E_{SCPG} [CI] || $Time_3$}]]
[단계 9] S ↔ PG : EC-DH Key Exchange
[단계 10] S → PG : E_{KSPG} [E_{KCPG} [CI] || $Time_4$ || E_{SKs}[h{E_{KCPG} [CI] || $Time_4$}]]
[단계 11] PG → S : E_{KSPG} [CAI || E_{KCPG} [CR] || $Time_5$ || E_{SKPG} [h{E_{KCPG} [CR] || $Time_5$}]]
[단계 12] S → C : E_{Kcs} [PList || E_{KCPG} [CR] || $Time_6$ || E_{SKs} [h{PList || E_{KCPG} [CR] || $Time_6$}]]

(그림 8) 프로토콜 수행 절차

제안된 프로토콜의 절차를 단계별로 살펴보면 다음과 같다.

[단계 1] 사용자는 상품 검색 및 선택을 하여 상거래 서버와 공유된 세션키로 SECURE CARD를 이용하여 암호화하여 전송한다. 상거래 서버는 세션키를 이용하여 상품 내역을 복호화하고 상품 내역을 확인한다.

[단계 2] 사용자는 인증서에 타임스탬프를 포함하여 상거래 서버에게 전송한다. 인증서에는 타임스탬프, 발급받는 사람의 신원, 발급받는 사람의 공개키로 구성된다.

[단계 3] 상거래 서버는 사용자의 인증서를 검증한다. 합법적인 인증서이면, 상거래 서버는 발급받은 인증서에 타임스탬프를 포함하여 사용자에게 전송한다.

[단계 4] Diffie-Hellman 키 교환 방식을 이용하여 사용자와 상거래 서버와 세션키를 공유한다.

타원 곡선를 이용한 키 교환은 아래와 같은 방법을 이루어진다. 우선 소수 p 와 $y^2 \equiv x^3 + ax + b(\text{mod } p)$에 대한 타원형 곡선 인자 a와 b를 선택한다. 이것은 Ep(a, b)의 타원형 그룹을 정의한다. 다음으로 Ep(a, b)에서 생성점 G = (x1, y1)를 선택한다. G의 선택에서 중요한 기준은 nG = O에 대한 n의 가장 작은 값이 매우 큰 소수이다. Ep(a, b)와 G는 모든 참여자에게 알려진 암호 시스템의 인자이다.

1. C는 n보다 적은 SK_c를 선택한다. 이것은 C의 개인키이다.
2. C는 공개키 $PK_c = SK_c \times G$를 생성한다. 공개키는 Ep(a, b)에서의 점이다.
3. S는 C와 유사하게 개인키 SK_s를 선택하고 공개키 PK_s를 계산한다.
4. C는 비밀키 $K = SK_c \times PK_c$를 생성한다.
5. S는 비밀키 $K = SK_s \times PK_s$를 생성한다.

$SK_c \times PK_s = SK_c \times (SK_s \times G) = SK_s \times (SK_c \times G) = SK_s \times PK_s$

(그림 9) Diffie-Hellman 키교환

[단계 5] Secure Card가 실행되고, 사용자에 의해 입력된 인증코드가 정확하면 상거래 서버와 공유한 세션키로 SECURE CARD를 이용하여 암호화한 개인정보를 전송한다. 상거래 서버는 세션키를 이용하여 개인 정보를 복호화하여 저장한다.

[단계 6] 상거래 서버는 구매정보와 지불요구를 사용자와 공유된 세션키로 SECURE CARD를 이용하여 암호화하여 전송한다. 사용자는 세션키를 이용하여 복호화하고 구매 정보와 지불요구가 맞는지 확인한다.

[단계 7] 사용자는 지불 요청 승인을 상거래 서버와 공유된 세션키로 SECURE CARD를 이용하여 암호화 하여 전송한다. 상거래 서버는 세션키를 이용하여 복호화 하고 확인한다.

[단계 8] 사용자는 SECURE CARD에 사용자 인증코드를 입력하고 인증코드가 정확할 때만 상거래 서버로 배송정보와 카드정보를 전송 할 수 있도록 한다. 사용자는 배송정보, 사용자와 지불 게이트웨이와 공유된 비밀키로 암호화된 신용카드 정보, 타임스탬프, 이 3가지 정보를 해쉬 함수를 수행한 결과에 개인키로 서명한 정보를 상거래 서버와 공유된 세션키로 Secure Card를 이용하여 암호화하여 전송한다. 이렇게 함으로써, 중요정보에 대한 기밀성, 무결성, 부인봉쇄 서비스를 제공한다.

[단계 9] Diffie-Hellman 키 교환 방식을 이용하여 상거래 서버와 지불 게이트웨이와 세션키를 공유한다. 세

션키 공유절차는 (그림 9)와 같다.

[단계 10] 상거래 서버는 사용자와 지불 게이트웨이와 공유된 비밀키로 암호화된 카드정보, 타임 스탬프를 상거래 서버와 지불 게이트웨이와 공유된 세션키로 SECURE CARD를 이용하여 암호화하여 전송한다. 카드 정보는 상거래 서버는 알지 못하고 사용자와 지불 게이트웨이만 볼수 있도록 하였다.

[단계 11] 지불 게이트웨이는 신용카드 승인 정보, 사용자와 지불 게이트웨이의 비밀키로 암호화된 영수증, 타임스탬프를 상거래 서버와 지불 게이트웨이와 공유된 세션키로 SECURE CARD를 이용하여 암호화하여 전송한다.

[단계 12] 상거래 서버는 구매 내역, 사용자와 지불 게이트웨이의 비밀키로 암호화된 영수증, 타임스탬프를 상거래 서버와 사용자와 공유된 세션키로 SECURE CARD를 이용하여 암호화하여 전송한다.

4.3 제안된 프로토콜 보안 서비스 분석

지금까지 유선 환경에서 사용되어온 SSL(Secure Socket Layer)의 단점은 부인봉쇄 서비스와 종단간 보안[18-20]을 지원하지 않는다. 무선 환경에서 앞으로 사용될 WTLS는 종단간 보안[16, 17, 21]을 지원하지 않으며, 무선 환경의 SSL은 유선과 마찬가지로 부인봉쇄 서비스와 종단간 보안[19]을 지원하지 않는다. 그러나 본 논문에서 제안한 프로토콜을 이용하여 모바일 전자상거래를 이용한다면 종단간 보안, 기밀성, 인증, 무결성, 부인봉쇄 서비스 등을 제공받을 수 있다. 기존 방법들과 비교하면 <표 4>와 같다. 또한 무선 환경에 적합하게 정보 입력의 불편함을 해소하기 위하여 거래 정보를 PDA에 암호화하여 저장하였다.

종단간 보안은 [단계 8]과 [단계 10]에서 볼 수 있듯이 사용자와 지불서버만이 공유하는 비밀키로 암호화하여 상거래 서버에 전달되기 때문에 상거래 서버에서는 볼 수가 없고 사용자와 지불서버만이 신용카드 정보를 알 수가 있다.

기밀성은 안전한 세션키 교환이 필수적인데 세션키 교환은 [단계 4]와 같이 Diffie-Hellman의 변형된 타원곡선을 이용하여 세션키를 안전하게 교환한다. 이렇게 교환된 세션키를 이용하여 [단계 5]부터 전송되는 모든 데이터를 안전하게 암호화하여 다른 사용자의 도청으로 보호한다.

인증은 1차적으로 무선 단말기의 분실에 대비하여 (그림 3)과 같이 PDA 자체에서 일방향 함수를 이용하여 인증코드를 암호화하여 저장하고, (그림 4)와 같이 인증코드가 정확히 입력되었을 때 개인 정보를 볼 수가 있게 된다. 2차적으로 (그림 4)와 같이 전자상거래시 거래정보를 전송하기 전에 인증코드 확인 절차를 거쳐 상거래 서버로 거래 정보를 전송하게 된다. 그리고 사용자와 상거래 서버간의 인증은 [단계 2]와 [단계 3]에서와 같이 신뢰된 인증기관으로부터 발부 받은 인증서를 서로 교환하여 서로 인증이 가능하다.

무결성은 거래 정보가 변경 되었을때 확인 할 수 있는 방법이다. 제안된 프로토콜에서는 중요 정보에 대하여만 해쉬 함수를 수행하여 불필요한 오버헤드를 줄였다. 즉, 신용카드 정보와 결제에 대한 데이터인 [단계 8], [단계 10], [단계 11], [단계 12]에서 해쉬 함수를 사용하였다.

부인봉쇄는 거래 정보를 개인키로 서명함으로써 이루어지는데 기존의 유선에서 사용하는 공개키 암호 시스템을 M-Commerce에서 사용하면 연산 속도가 오래 걸리는 단점이 있다. 제안된 프로토콜에서는 타원곡선 암호 시스템을 이용하여 M-Commerce에 적합한 서명을 하여 부인봉쇄 서비스를 제공한다. 또한 모든 거래 정보에 서명을 하지 않고 [단계 8], [단계 10], [단계 11], [단계 12]과 같은 중요한 데이터에만 서명을 함으로써 불필요한 오버헤드를 줄였다. 각각이 단계들은 기밀성, 무결성, 부인봉쇄 서비스를 제공하고 재전송 공격으로부터 안전하다.

5. 결 론

M-Commerce 환경에서 데이터 서비스를 원활하게 제공하면서 정보보호 기술을 만족하기 위해서는 안전한 전자상거래 시스템 설계가 중요하다. 기존의 공개키 암호 시스템은 M-Commerce에 적합하지 않았지만, 적은 비트 수와 빠

〈표 4〉 제안된 프로토콜의 특징 비교

항 목	SSL[18, 20]/[19]	WTLS[9]/[17, 21]	MSSL[14]	AIP 기반[16]	제안 방식
부인봉쇄 서비스	X/O	O/O	X	O	O
기 밀 성	O/O	O/O	O	O	O
인 증	O/O	O/O	O	O	O
무 결 성	O/O	O/O	O	O	O
하드웨어 필요성	불필요	불필요	불필요	스마트카드 필요	불필요
정보입력 불편의성	•	해결안됨	해결안됨	해결안됨	해결
사용 프로토콜	HTTP	WAP	HTTP	독립적	독립적
종단간 보안	X/X	X/O	X	O	O

른 계산 속도를 보장하는 타원곡선 공개키 암호 시스템으로 인하여 M-Commerce에서 공개키 암호 시스템이 사용 가능하게 되었다. 제안된 프로토콜에서는 M-Commerce에 적합한 타원곡선 암호 시스템을 이용하여 PDA 기반의 신용카드 결제 시스템을 설계하였다. 세션키 교환에서는 Diffie-Hellman의 키 교환 기법을 이용하였고, 타원곡선 암호 알고리즘과 안전한 블록암호 알고리즘을 이용하여 거래 정보의 기밀성, 무결성, 인증, 부인봉쇄 서비스 등을 갖춘 안전한 M-Commerce 프로토콜을 설계하였다. 제안된 프로토콜의 장점은 종단간 보안이 가능하며, SSL에서 지원하지 않는 부인봉쇄 서비스를 지원한다. 또한 PDA를 이용하여 거래를 할 때 정보 입력의 불편의성을 극복할 수 있게 설계하였고, 단말기 분실시 개인정보를 보호하기 위해여 인증 모듈이 1차 사용자 인증을 하고, M-Commerce시 다시 2차 인증을 한다. 또한 중요한 정보만을 선택적으로 전자 서명 및 해쉬 함수를 수행함으로써 불필요한 오버헤드를 줄였고 타임스탬프를 이용하여 재전송 공격으로부터 안전하다.

따라서 본 논문에서 제안된 프로토콜에 의해 PDA의 정보입력 인터페이스의 단점을 극복할 수 있고, 안전한 M-Commerce가 가능하게 설계되었다. 이를 통해 신용카드 결제 서비스의 모바일 전자상거래 활성화에 기여할 수 있을 것으로 기대된다.

참 고 문 헌

[1] 이재규 외 3인, "전자상거래원론", 범영사, 2000.

[2] Nam-Je Park, You-Jin Song, "M-Commerce Security Platform based on WTLS and J2ME," ISIE2001, 2001.

[3] Lyytinen, K., "M-commerce - mobile commerce : a new frontier for E-business," Proceedings of the 34th Annual Hawaii International Conference on System Sciences, 2001.

[4] 김선형 외 2인, "이동 통신 시스템에서의 효율적인 소액 지불 기법", 춘계학술발표논문집, 한국정보과학회, 2002.

[5] 임수철 외 3인, "M-Commerce를 위한 고액 지불 시스템", 춘계학술발표논문집, 한국정보처리학회, 2002.

[6] Forrester Research, "Mobile Payment's Slow Start," May, 2001.

[7] H. X. Nel, Doris Baker, "보안과 암호화 모든 것", 인포북, 2001.

[8] Gunter Horn, Bart Preneel, "Authentication and Payment in Future Mobile Systems," ESORICS, LNCS 1485, 1998.

[9] Wireless Application Protocol Wireless Transport Layer Security, WAP Forum, April, 2001.

[10] Wireless Application Protocol Public Key Infrastructure Definition, WAP Forum, Oct., 2000.

[11] 정여석, 김수진, 서인석, 서상원, 원동호, "무선 PKI 기술 및 서비스 동향에 관한 연구", 한국정보처리학회 추계학술발표대회, 한국정보처리학회, 2002.

[12] 최용락 외 3인 공역, "컴퓨터 통신 보안", 도서출판 그린, 20001.

[13] M. Aydos, B. Sunar and C. K. Koc., "An elliptic curve cryptography based authentication and key agreement protocol for wireless communication," end International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications, Dallas, Texas, October, 1998.

[14] 무선인터넷백서 편찬위원회, "무선인터넷 백서", 소프트뱅크 미디어, 2000.

[15] http://www.kisa.or.kr, 한국정보보호진흥원.

[16] 임수철, 강상승, 이병래, 김태윤, "무선인터넷에서의 종단간 보안을 제공하는 신용카드 기반의 지불 프로토콜", 한국정보과학회논문지, 한국정보과학회, 2002.

[17] Eun-Kyeong Kwon, Yong-Gu Cho, Ki-Joon Chae, "Integrated transport layer security : end-to-end security model between WTLS and TLS," Proceedings of the 15th International Conference on Information Networking, 2001.

[18] A. Freier, P. Karlton, P. Kocher, "The SSL Protocol version 3.0," Internet Draft, Nov., 1996.

[19] 유성진, 김성열, 정일용, "안전한 통신서비스를 제공하는 향상된 SSL기반 정보보호 시스템의 설계", 한국통신학회논문지, 한국통신학회, 2000.

[20] 박지철, 한명진, 이경현, "Session Resume의 기한 연장을 이용한 SSL/TLS Handshake 프로토콜의 성능개선", 한국정보과학회 추계학술발표대회, 한국정보과학회, 2002.

[21] 최진규, 이헌길, "WAP환경에서 안전한 종단간 보안을 제공하는 TLS-Plus 프로토콜", 한국정보과학회 춘계학술발표대회, 한국정보과학회, 2002.

유 성 진

e-mail : desktop@teachiworld.com

1998년 조선대학교 전자계산학과(학사)

2000년 조선대학교 대학원 전자계산학과 (이학석사)

2000년~현재 조선대학교 대학원 전자계산학과 박사과정

관심분야 : 정보보안, 분산 시스템, 전자상거래

김 성 열

e-mail : green@mogent.net

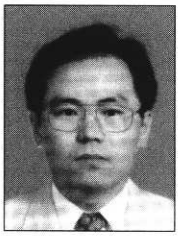
1994년 조선대학교 전자계산학과(학사)

1996년 조선대학교 대학원 전자계산학과 (이학석사)

2000년 조선대학교 대학원 전자계산학과 (이학박사)

2002년~현재 울산과학대학 컴퓨터정보학부 전임강사

관심분야 : 정보보안, 분산 시스템, 전자상거래



윤 천 균

e-mail : chqyoun@honam.ac.kr

1982년 인하대학교 전자공학과(학사)

1997년 포항공과대학 정보통신학과(공학석사)

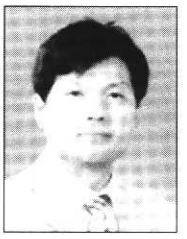
2003년 조선대학교 전자계산학과(이학박사)

1982년~1998년 포항종합제철(주) 과장

1998년~2002년 호남대학교 정보기술원 조교수

2003년~현재 호남대학교 정보기술학부 조교수

관심분야 : Network, 정보가전, 생산관리시스템, 공장자동화 시스템



정 일 용

e-mail : iyc@mail.chosun.ac.kr

1983년 한양대학교 공과대학(학사)

1987년 City University of New York (전산학석사)

1991년 City University of New York (전산학박사)

1994년~현재 조선대학교 컴퓨터공학부 부교수

관심분야 : 네트워크 보안, 전자상거래, 분산 시스템 관리, 코딩이론, 병렬 알고리즘