ECC 기반 무선 인터넷 지불시스템 설계

이정미[0] 김현성 이원호 유기영
경북대학교 컴퓨터 공학과
{jmlee, hskim, purmi}@purple.knu.ac.kr, yook@knu.ac.kr

Design of the ECC-based Payment System in the Wireless Internet

Jung-Mee Lee[0], Hyun-Sung Kim, Won-Ho Lee, and Kee-Young Yoo
Dept. of Computer Engineering, Kyungpook National University

요 약

무선 인터넷 사용자들이 기하급수적으로 증가함에 따라 무선 전자상거래도 활발해져 가고 이에 따라 보안성의 제공도 필수적이다. 게다가 이동 무선 전자상거래에서 사용되는 디바이스들은 속도와, 용량등 성능면에서 많은 제약을 가지고 있다. 따라서, 본 논문에서는 제약이 많은 장치의 특성상 소형 단말기에 적합한 언어인 J2ME를 기반으로 하고, SET프로토콜을 활용한 지불 시스템을 제안한다. 특히, 정보보안을 위해서는 현재 많이 사용되는 RSA알고리즘보다 키 사이즈 및 계산 수행시간 측면에서 유리한 ECC를 적용한다.

1. 서 론

최근 들어 무선 인터넷 사용자가 폭발적으로 증가하고 있다. 이러한 무선 서비스의 가장 큰 특징은 사용자가 시간과 장소에 구애 받지 않는 것이다. 그래서 기존 유선 망 기반의 인터넷 전자상거래에 이어 무선 단말기(휴대폰, PDA 등)를 이용한 전자상거래 또한 점차 증가되고 있다.

현재 대표적인 무선 인터넷 프로토콜로는 WAP을 들 수 있는데, WAP을 이용한 제한된 무선환경에서의 안전한 모바일 전자 상거래를 위해서는 보안문제의 해결이 필수적이다. 그러나 WAP 구조에서는 유무선 환경을 연동해주는 기능을 가진 WAP 게이트웨이에서 데이터가 노출된다는 문제점이 있다. 그리고 무선 단말기는 제한된 용량과 CPU성능, 메모리를 가지는 디바이스라는 특성을 가지고 있다. 따라서 본 논문에서는 이런 단말기의 특성에 적합한 자바언어로서 J2ME를 이용하고, 공개키 암호 시스템으로는 타원곡선 암호 시스템 즉, ECC(Elliptic Curve Cryptosystem)와 SET을 활용한 무선 인터넷용 지불 시스템을 제안한다.

J2ME는 썬에서 휴대폰과 같은 제한된 성능의 하드웨어 환경을 대상으로 개발한 것으로서 플랫폼 독립적이라는 점 이외에도 이식성이 높다는 장점을 가진다[1]. 따라서 단말기상에 소프트웨어적으로 보안모듈을 작성함으로써 하드웨어의 변경 없이 필요에 의한 다운로드가 가능하다. 타원곡선기반 암호 시스템인 ECC는 1985년에 빅터 밀러와 닐 코블리츠가 제안한 것으로 이산대수에서 사용하는 유한체의 곱셈군을 타원곡선군으로 대치한 암호 체계이다. 이러한 타원곡선 암호를 사용함으로써 단말기상에서의 공개키 생성 시간 및 암호화, 복호화 시간을 크게 단축할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 J2ME를 구성하는 MIDP, CLDC 및 ECC에 대하여 살펴보고, 3장에서는 본 논문에서 제시하는 지불 시스템을 설계한다. 끝으로 4장에서 결론을 맺는다.

2. 관련 연구

2.1 J2ME

자바는 플랫폼 성격에 따라서 3가지 Edition 즉, Enterprise Edition과 Standard Edition 그리고 Micro Edition으로 나누어진다. 자바 1.1 버전까지는 일반적인 자바 애플릿이나 응용 프로그램의 개발이 목적이었다. 그러나, 자바 1.2 버전 이상에서는 자바의 용도가 좀 더 다양해지고 자바가 올라갈 수 있는 플랫폼이 다양해져 그 특성에 맞는 자바가 등장하게 되었다. 이에 썬 마이크로 시스템에서는 작고 제한된 성능의 디바이스들을 위하여 동적으로 확장 가능한 네트워크 기반의 어플리케이션을 개발할 수 있도록 하는 J2ME (Java 2 Micro Edition)를 제시하였다.

J2ME는 CLDC(Connected, Limited Device Configuration)로 정의되는 환경(Configuration)을 사용하여 스펙을 정의하는데, 이와 별도로, 프로파일이라는 개념을 두어 각각의 디바이스에 적합한 API스펙을 정의한다[2,3]. 휴대폰 단말기를 위하여 정의된 프로파일은 MIDP(Mobile Information Device Profile)이다[3]. 그리고 CLDC가상 머신으로는 KVM(K Virtual Machine)을 채택하는데 KVM은 성능에 제약이 있는 모바일 디바이스를 위해 설계된 자바 가상 머신이다. 본 논문에서는 이런 CLDC/MIDP기반 위에 미들릿이라는 애플리케이션 형태로 보안 모듈 및 고객시스템을 개발한다.

2.2 타원곡선 암호체계

본 논문에서는 타원 곡선 공개키 암호 알고리즘으로

ElGamal을 사용하였다. 타원곡선 알고리즘은 무엇보다도 기존의 공개키 암호 알고리즘인 RSA, Diffie-Hellman, DSA, ElGamal보다 작은 사이즈의 키를 사용하면서 비슷한 수준의 보안을 보장해 준다. 게다가 주요 연산이 덧셈이어서 암/복호화측면에서도 유리하다. 이러한 장점으로 인해 타원곡선 알고리즘은 특히, 휴대폰이나 호출기, 스마트카드 같은 휴대형 시스템에 이상적이며, 하드웨어뿐만 아니라 소프트웨어 구현에도 용이하다[4].

타원곡선 공개키 암호방식은 이산대수문제를 기반으로 한 방식이다. 일반 이산 대수 문제와 타원곡선군에서의 이산대수문제를 비교해보면 다음과 같다[5].

● 이산대수문제(Discrete Logarithm Problem)

소수 p에 대한 원시근이 α라 할 경우 $\beta = \alpha^x (mod\ p)$를 계산했을 때 x를 찾는 문제로 소수 p가 매우 클 때는 $x(0 \le x \le p-2)$를 다항식 시간 내에 찾기 힘들다는 것에 근거를 둔 방식이다.

● 타원곡선 이산대수문제(Elliptic Curve Discrete Logarithm Problem)

위수(order)가 n 일 때, P를 타원곡선상의 점이라고 한다면 $Q = xP$, 즉 Q는 P를 x번 더한 값이라 할 때, $x(0 \le x \le n-1)$를 찾기 어려운 것에 근거를 둔 방식이다.

표 1은 DLP와 ECDLP 사이의 차이점을 보여준다.

표 1. DLP와 ECDLP와의 대응관계

표 1구분	DLP	ECDLP
군(Group)	Zp^*	$E(Zp)$
원소	$\{1, 2, \cdots, p-1\}$ 소수 p order q generator α group $\{\alpha^0, \alpha^1, \cdots, \alpha^{(r-1)}\}$	타원곡선상의 점들 (x,y) 와 O order n generator point P group $\{O, P, 2P, \cdots, (n-1)P\}$
연산	modulo p상의 곱셈	점들의 덧셈
키생성	$[1, q-1]$의 구간에서 임의의 정수 u를 택한다. $x = g^u \bmod p$ private key ; u public key ; x	$[1, n-1]$의 구간에서 임의의 정수 d를 택한다. $Q = dP$ private key ; d public key ; Q

3. 무선 인터넷기반 지불 시스템

현재 인터넷상의 전자상거래에서 이용되는 SET기반 프로토콜에서는 공개키 기반 암호화 방식으로 RSA가 사용된다. 그러나 무선 인터넷에서의 전자상거래는 제한된 성능의 단말기에서 주로 이루어지므로 단말기 상에서 수행하기에는 RSA방식보다 ECC방식이 연산수행시간 및 사용되는 키의 길이 등에서 상당히 유리하다. 이 절에서는 타원곡선 공개키 암호 시스템으로서 ElGamal을 쓰고 SET을 활용한 무선 인터넷 기반 지불 시스템을 설계한다.

제안된 시스템에 필요한 심볼들은 다음과 같다.

- T, M: 각각 단말기와 상인을 나타내는 식별자
- CA: 인증기관을 나타내는 식별자
- PU_x: 개체 x의 공개키
- PR_x: 개체 x의 비밀키
- $E_y(m)$: 키 y를 사용해 메시지 m을 암호화
- $D_y(m)$: 키 y를 사용해 메시지 m을 복호화

3.1 ElGamal 타원 곡선 암호

그림 1은 Alice가 Bob에게 메시지를 보내는 경우를 가정했을 때 타원곡선 암호시스템에서의 ElGamal 암호과정을 나타낸 것이다. 타원 곡선 암호시스템은 점 P를 x번 더하는 계산이 주를 이룬다. 이를 표기하는 방식은 $Q = xP$ 이다. 그림에서 타원곡선 E와 곡선 위의 점 P는 공개한다고 가정한다.

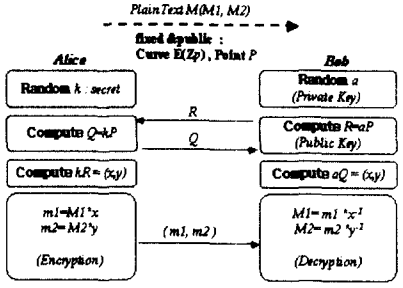

그림 1. ElGamal 프로토콜

3.2 지불 시스템 구조

개방된 네트워크 상에서의 안전한 전자적 거래를 위해서는 신뢰성 있는 데이터 전송 보장, 데이터의 무결성 보장, 그리고 고객과 상인의 신분 인증기능 등을 제공해야 한다. 이를 위해 본 논문에서는 SET프로토콜을 무선인터넷에 확장하여 사용한다[6,7,8].

본 논문에서 제시된 지불 시스템에서 사용되는 프로토콜은 크게 인증서를 획득하는 등록 프로토콜과 대금결제를 수행하는 지불 프로토콜이 있다. 시스템 구성은 고객시스템, 상인 서버 시스템, 인증서버 및 지불 게이트웨이로 구성되고, 전체 시스템 구조도는 그림 2와 같다. 본 논문에서는 지불 게이트웨이와 은행과의 통신은 성공적으로 수행되었다고 가정한다. 그림 2에서 점선으로 표시된 부분은 단말기와 상인 서버 및 인증기관 간의 통신으로서 무선 인터넷 프로토콜을 기반으로 통신이 이루어지고, 실선 부분은 유선 인터넷 환경에서 통신이 이루어지는 부분이다.

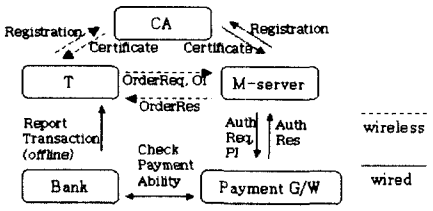

그림 2. 전체 지불 시스템

3.2.1 등록 프로토콜

등록 프로토콜은 고객이나 상인이 공인된 인증기관으로부터 인증서를 획득하는 과정이다. 획득한 인증서는 X.509에 기반한 인증서로서 일련번호, 발행자ID, 인증서 유효기간, 공개키 정보, 그리고 서명 등의 정보를 가진다. 이러한 인증서는 인증기관의 비밀키로 암호화되어 있다. 그림 3은 이러한 등록 프로토콜을 나타낸다.

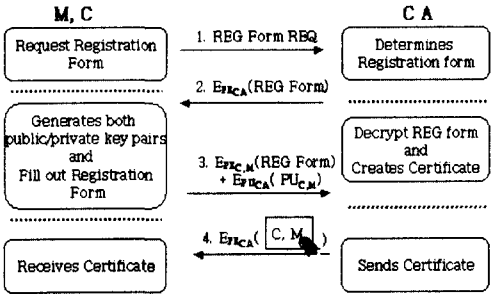

그림 3. 등록 프로토콜

상인 또는 고객은 인증서를 획득하기 위한 등록 초기화 명령을 공인된 인증기관에 보낸다(1). 인증기관은 이에 대한 응답으로 인증기관의 비밀키로 암호화된 등록양식(REG Form)과 인증기관의 인증서를 전송한다(2). 등록양식의 항목으로는 이름, 아이디, 주소지, 요청타입, 카드 번호등이 포함된다. 고객 또는 상인은 등록양식을 채운 후 자신의 비밀키로 암호화한 것과 등록요청자의 공개키를 암호화한 것을 인증기관에 전송한다(3). 인증기관은 메시지의 암호화를 풀고 해당되는 인증서를 생성, 인증기관의 비밀키로 암호화하여 등록 요청자에게 보낸다(4).

3.2.2 지불 프로토콜

지불 프로토콜은 등록된 사용자가 상품 주문을 하고, 대금 결제를 하고자 할 때 지불 게이트웨이를 통해 안전한 대금 결제를 수행한다. 지불 프로토콜 과정으로는 지불 초기화 단계, 구매 요청 단계, 지불 승인 단계가 있다. 지불 프로토콜의 전체적인 흐름도는 그림 4와 같다.

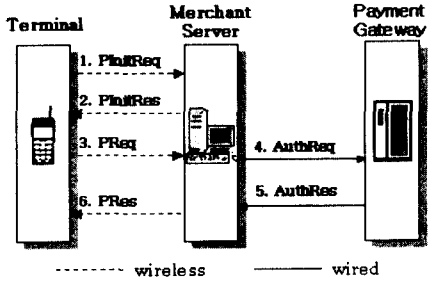

그림 4. 지불 프로토콜

고객은 브라우저를 통해서 물건을 선택하고 지불할 카드를 결정한 뒤에 그림에서처럼 상인에게 지불초기화 요청(PinitReq)을 해서 응답(PiniRes)절차를 거치면 구매요청(PReq)을 한다. 이에 상인은 지불 게이트웨이로 지불에 대한 승인 요청(AuthReq)을 하고 지불 게이트웨이는 은행과 연결하여 결제 가능 여부를 판단한 뒤 지불에 대한 승인(AuthRes)을 하면 상인은 고객에게 구매에 대한 응답을 보낸다.

지불 초기화 응답을 받은 고객은 주문정보(OI)와 지불정보(PI)를 상인에게 보내는데 주문정보는 상인을 위한 정보이고 지불정보는 지불 게이트웨이를 위한 정보이다. 따라서 주문정보는 상인의 공개키로 암호화하고 지불정보는 매입사의 공개키로 암호화하여 전송한다. 각각의 메시지 구성은 표 2와 같다.

표 2. 주문정보와 지불정보 메시지구성

구분	메시지
OI	ID, 상품, 수량, 가격, 사용언어
PI	ID, 카드번호, 카드유효기간,브랜드명

4. 결론 및 향후 연구과제

본 논문에서는 타원 곡선 공개키 암호 시스템으로서 ElGamal을 사용하여 SET을 활용한 무선 인터넷 기반 지불 시스템을 설계하였다. SET프로토콜은 인증기관에서 생성한 인증서를 전송할 때 주고 받음으로써 부인 방지와 상대방의 신원인증을 가능하게 한다. 게다가 메시지는 인증서에서 공개키를 획득하여 타원 곡선 암호화방식으로 암호화 한 뒤 전송하기 때문에 부결성도 제공한다.

향후에는 제안된 시스템을 단말기상에서 시뮬레이션이 가능하도록 구현할 예정이다.

5. 참고 문헌

[1] Java2, Micro Edition, http://java.sun.com/j2me
[2] Connected Limited Device Configuration, http://java.sun.com/products/cldc
[3] Mobile Information Device Profile, http://java .sun. com /products/midp
[4] Certicom, ECC Whitepaper, http://www.cert_icom.ca , 1999
[5] 이혁, 이정규, " 타원 곡선 공개키 암호알고리즘을 이용한 전자지불 시스템" , 공학 기술 논문집 Vol.8 No.1 1999.8
[6] Secure Electronic Transaction Specification, Book 1 : Business Description, Version 1.0, May 31, 1997
[7] Secure Electronic Transaction Specification, Book 2 : Programmer' s Guide, Version 1.0, May 31, 1997
[8] Secure Electronic Transaction Specification, Book 3 : Formal Protocol Definition, Version 1.0, May 31, 1997