타원 곡선 암호를 이용한 안전한 메일 기반 전자지불시스템 설계

김성일* · 최문석 · 신병철

*충북대학교

Design of Securer Electronic payment system based on ECC algorithm

Seong Il Kim* · Munsuk Choi · B.C.Shin

Chung Buk National University

E-mail : {onepoet76*, bidulgia}@hotmail.com

요 약

최근에 급속도로 발전해가는 네트워크 망에서 여러 가지 정보들이 서로 교환되고 있다. 이 정보들은 각각의 보안 시스템과 암호화 기법들을 사용하여 보호하려는 연구가 진행되고 있으며, 현재 메일 주소만을 이용하여서도 계좌 이체가 가능한 시스템을 구현하려는 연구가 활발히 진행되고 있다. 그러나 SSL 기반으로 동작하는 메일 시스템에서 악의적인 데이터의 대한 부인과 변조 가능한 방법들이 알려져 있으며 이에 따라 보호되어야할 중요한 정보들이 인가되지 않은 사용자에게 노출될 가능성이 매우 높은 실정이다.

이에 따라, 기밀성, 무결성, 사용자 인증, 부인 방지 등 정보 보호를 위해 한층 더 안정성 있는 전자지불 시스템에 대한 연구가 요구되며, 본 논문에서는 ECC의 안전한 알고리즘에 기반을 둔 안전한 전자지불 시스템을 설계 및 구현하고 기존의 메일 기반 전자 지불 시스템과 성능을 비교 분석하였다.

ABSTRACT

With a great improvement of computers and Network communication skills, we can exchange information quickly. There have been many researches on the subject how to guarantee the information security by security mechanism and cryptography schemes. Nowadays, many people in this area show their interest in money transfer systems between accounts, which can provide a secure mechanism in which people can send money to the legitimate party or person safe. However, we have learned many ways to distort messages and repudiate the malicious activity in mail systems based on SSL mechanism. It is very likely that important information which must be kept in secret is laid exposed to un_authorized user. Accordingly, to provide stronger security service, researches on electronic payment system which can guarantee the security characteristics such as confidentiality, integrity, user authentication, Non-repudiation, are strongly needed. In this paper, we analize the characteristics of the previous researches in this field, and also propose a securer electronic payment system based on ECC algorithm.

키워드

타원 곡선, 메일 기반 전자지불 시스템

Ⅰ. 서 론

인터넷의 급속한 보급한 컴퓨터 네트워크 기술의 비약적인 발전은 사회 각종 분야에 괄목할 만한 변화를 가져 주었다. 인터넷 뱅킹증가와 전자상거래 서비스의 사용자 편의성 증대는 기존의 시장거래 형태를 온라인 거래의 패러다임으로 변화시키고 있다. 전자상거래 서비스는 기능적인 서비스뿐만 아니라 사용자 편의성 극대화를 추구하려는 추세로 발전하고 있으며 최근 메일을 기반으로 전자지불 서비스를 시도하려는 연구가 진행되고 있다.

그러나, 기존의 전자메일 시스템은 기본 표현 방식으로 MINE(Multipurpose Internet Mail

Extensions)을 사용하고 있어 악의적인 의도를 가진 사용자가 메일서버 관리자의 권한을 획득한 경우 해당 메일 서버를 사용하는 이용자의 개인 사생활 정보를 불합적으로 획득 가능하며, 대표적인 전송 프로토콜인 SMTP와 POP3 프로토콜의 경우 전송되는 데이터를 악의적인 사용자가 중간에서 가로채는 경우 쉽게 메시지 변조될 수 있다.

웹메일 시스템을 포함한 인터넷 메일 시스템이 전자상거래에 본격적으로 적용되기 위해서는 반드시 보안 문제에 대한 해결이 필요하다.

전자상거래 상에서 지불 서비스를 성공적으로 운영하기 위하여, 보안기술의 필요성은 이미 널리 인식되고 있으며 인터넷의 발전과 함께 각종 보안 위협이 증가하고 있는 가운데, 금융정보 보호를 위하여 핵심보안 기술 연구에 대한 연구 필요성은성은 한층더 요구되고 있다.

전자지불 방식의 기술적 요인 중에서 보안 문제가 크게 부각되고 있는 인터넷상에서 안전한 전자지불시스템을 구현하는 것은 필수적인 요소이며 이에 따라 본 논문에서는 기존의 메일시스템 기반 전자지불시스템의 성능과 안정성을 분석하고 ECC 알고리즘을 기반으로 한 보다 안전한 전자지불시스템을 설계하였다.

II. 전자지불방식의 기술적 요소

전자지불 시스템에서의 핵심 요소기술로 암호메커니즘, 전자서명(digital signature), 공개키 기반구조, 은닉서명(bind signature)등의 기법들이 요구된다. 보안/안정성은 전자지불 시스템에서 가장 중요한 요소 기술의 하나라 할 수 있다. 전자지불 시스템에서의 보안은 시스템 보안 차원만이 아니라, 거래 정보, 카드 번호 등의 자료자체를 보호(data security)하는 것을 포함한다. 특히 네트워크 환경에서 정보를 주고 받아야 하는 전자지불시스템의 경우, 위조, 부인봉쇄, 이중사용, 돈세탁, 강제적인 전자화폐 인출 등, 각종 위협요소에 직면하고 있으며, 이러 위험으로부터 정보를 안전하게 신뢰 할 수 있게 전달되어야 하는 것이 핵심 요구사항이 된다.

1. 대칭형 암호 알고리즘

암호(Cryptography)는 평문(plaintext)을 해독불가능한 암호문(ciphertext)으로 변형하거나 암호화된 통신문을 복원 가능한 형태로 변환하기 위한 방법을 제공한다. 대칭형 암호 알고리즘은 서로 같은 비밀키를 가지고 암호화/복호화시 사용하며 대표적인 블록 암호 알고리즘은 DES, 3중 DES, RC2, IDEA, FEAL, ICE, AES 등이 있다.

2. 공개키 암호 알고리즘

공개키 암호 알고리즘은 암호용 키와 복호용 키가 서로 다른 키쌍을 지닌 알고리즘으로서 주로 인증 및 디지털 서명 등에 사용되며, 현재는 RSA 방식보다 더 적은 키를 가지고도 높은 안전성을 보장할 수 있는 ECC(Elliptic Curve Cryptography)에 대한 활발한 연구가 진행중이다.

3. 전자 서명(Digital Signature)

컴퓨터 네트워크를 통한 비대면 방식의 전자거래는 대면방식의 기존 거래 방식의 단점을 극복케 한다. 전자거래는 기존 거래 방식의 시간적 · 공간적 제약의 문제점을 해결해 준다. 그러나 전자거래는 많은 장점을 가지고 있음에도 불구하고, 사용자에게 역기능을 제공할 수 있다는 문제점으로 인하여, 보안 요구사항이 먼저 해결되어야만 전자거래의 활성화를 기대할 수 있다.

전저서명은(Digital signature)은 위에 언급된 문제를 해결해 주는 방법으로써 암호(cryptography)기법을 응용해 서명 이후 부인방지(non-repudiation), 적법한 사용자만 정확한 전자서명을 생성가능케하는 위조방지(unforgrable), 문서 변경불가능(authentication), 이후에 재사용 불가능(not reusable) 서비스 등을 제공한다.

4. 공개키기반구조(Public Key Infrastructure)

공개키기반구조(PKI:Public Key Infrastructure)는 인터넷상에서 사용자들간에 민감한 데이터를 안전하게 교환함으로써, 금융 거래를 전자적으로 가능케 하기 위하여 인증서(certificate)를 분배하고 전달하는 시스템이라고 정의 할 수 있다. PKI를 이용하면 기밀성(privacy), 접근제어(access control), 무결성(integrity), 인증(authentication), 부인봉쇄(non-repudiation) 서비스를 제공받을 수 있다.

PKI는 공개키에 대응되는 비밀키(private key)를 안전하게 저장하고 특정 공개키와 특정 비밀키가 정확히 연결되도록 한다.

5. 은닉서명(bind signature)

고객이 은행으로 전자화폐를 인출 받고자 할 때, 고객만의 고유번호를 이용하는데, 이 경우에 은행은 고객이 사용한 고유번호를 얻게 되며, 이후 고객이 전자화폐 사용했을 경우 이를 통해 고객의 익명성을 파기함으로써 사용자의 프라이버시를 침해하게 된다. 은닉서명은 이를 막기 위한 기술로써 고객이 고유번호가 무엇인가를 은행이 알지 못하도록 보장한다.

이러한 은닉서명 기법은 82년 D. Chaum에 의해서 발표되었다. 은닉서명 기법은 개인의 사생활 보호를 위해서 발표되었지만, 탈세나 돈세탁과 같은 여러 가지 사회적인 역기능을 발생시켰다.

III. 전자메일 지불 시스템 설계

1. 키 교환 모델

이 논문에서 안전한 키 교환을 하기 위해

ECDH(Elliptic Curve Diffie-Hellman) 알고리즘을 이용한 키 교환 모델로 구현하였으며, 이 모델은 타원 곡선 상에서 이산 대수를 계산하는 난이도를 이용하여 안전한 키 교환을 지원하게 된다.

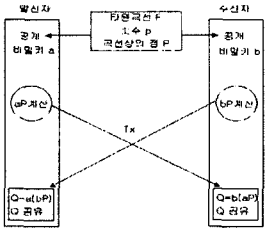

그림 1. ECDH 알고리즘을 적용한 키 교환

① 엘리스와 밥은 각각 정수a와 b를 선택하여 비밀로 간직한다.
② 각각 $aP(\in E)$와 $bP(\in E)$를 계산하여 서로 전송하여 갖는다.
③ 엘리스와 밥은 Q=a(bP)와 Q=b(aP)를 계산하여, Q를 공유

발신자와 수신자가 안전하게 지불 시스템에 사용하는 메일 서로에게 전송하기 전에 안전하게 상호키 교환을 할 수 있다.

2. 메시지 암호 알고리즘

Rijndeal 알고리즘은 AES에 의해서 채택된 관용 암호 알고리즘에 채택된 관용 암호 알고리즘이며, 데이터를 128, 192, 256 비트의 키를 이용한다. 암호화와 복호화에 사용되는 키가 하나이고 속도가 빠르기 때문에 메시지를 암호화하는데 사용될 수 있다. Rijndeal은 아래와 같은 네 부분의 변환 과정에 의해 암호화 및 복호화 과정을 수행한다.

The ByteSub transformation
The ShiftRow transformation
The MixColumn transformation
The Round Key addition

3.EDCSA(Ellipse Curve Digital Signature Algorithm)을 적용한 전자서명

[ECDSA 전자 서명 생성]
① 구간[2,n-2]에서 통계적으로 유일한 수 k를 선택.
② kP = (x_1, y_1)과 r=x1 mod n을 계산.
③ r=o이 아니면 $k_1$mod n 계산
④ $s=k^{-1}\{h(m)+dr\}$mod n을 계산.
⑤ 메시지에 대한 전자서명 : (r, s).

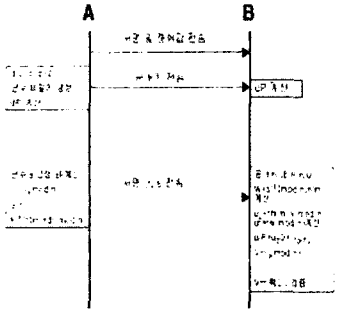

그림 2. ECDSA를 이용한 간단한 서명 모델

[ECDSA 전자 서명 검증]
① 서명 (r, s)검증
② 공개키 (E, P, n, Q)를 획득.
③ r과 s가 구간 [1, n-1]에 있는지 확인
④ $w=s^{-1}$ mod n과 $h(m)$를 계산.
⑤ $u_1=h(m)w$ mod n과 u_2rw mod n을 계산.
⑥ $u_1P+u_2Q=(x_0,y_0)$와 $v=x_0$ mod n을 계산.
⑦ v=r을 확인하여 서명을 검증.

4.배달 증명 방식
① 발신자가 배달 증명 요청시 플래그를 붙여 수신에게 전송
② 수신자는 플래그를 확인한 다음, 암호화된 메시지를 비밀키로 서명해 발신자에게 회 신
③ 발신자는 배달증명 요구에 대한 회신 메시지에서 플래그를 확인하여 올바르게 배달되었음을 확인.

IV. 비교분석

이 논문에서 제안한 메일 시스템을 이용한 지불 시스템은 메일 메시지 기밀성, 메시지 무결성, 송신자 인증, 송신자 부인 방지 서비스를 등을 제공하며, 배달증명 서비스를 포함한다.

표 1. ECC과 보안 프로토콜과의 비교

서비스	ECC적용	PEM	MIME	S/MIME
메시지기밀성	제공	제공	제공	제공
메시지무결성	제공	제공	제공	제공
송신자 인증	제공	제공	제공	제공
송신부인방지	제공	제공	제공	제공
배달증명	제공	X	X	X

표 2. ECC적용 메일 지불 시스템과 비교

서비스	ECC적용	범용브라우저	E사	J사
메시지기밀성	제공	제공	제공	제공
메시지무결성	제공	제공	제공	제공
송신자 인증	제공	제공	제공	제공
송신부인방지	제공	제공	제공	제공
배달증명	제공	X	X	X

V. 결 론

전자상거래와 지불시스템의 원활한 운용에 있어 가장 중요한 요소는 안전성과 사용자 편의성이다. 기존의 SSL기반으로 동작하는 시스템에서는 거래 부인, 암호 알고리즘 계산속도 저하, 서버에서의 개인의 정보 누출 가능성에 대한 문제점이 제기되고 있다. 이에 대한 해결책은 공인 인증서에서 몇 개의 인증요소만을 취하여 암호하는 방식으로 타원곡선 암호 알고리즘을 사용함으로서 속도와 안정성면에서 우수한 특성을 볼 수 있다.

기존의 메일 시스템에서 제공하는 기본 보안 서비스를 제공하며, 메시지가 배달증명과, 내용이 변경되었는지 여부에 대한 내용증명 서비스를 제공하는 메일 기반의 전자지불 시스템을 설계하였다.

향후, 메일 기반 서비스 서버에서의 사용자에 대한 DB정보 획득에 있어 침해의 문제 소지가 있으며, 이에 대한 보안대책과 함께 기존의 메일 시스템과 호환성을 유지할 수 있는 지속적인 연구가 요구된다.

참고문헌

[1] 전철우, 이종후, 이상호 "S/MIME을 적용한 안전한 지불 메커니즘 설계", 정보과학회논문지, 29권 제 5호 2002.10

[2] 이원구, 김성준, 이희규, 문기영, 이재광 "타원곡선 암호 시스템을 이용한 보안 메일 시스템의 설계와 구현"

[3] 홍주영, 윤이중, 김대호, "전자우편 시스템의 보호 방식 분석", 통신정보보호학회지 Vol.4 NO2. 1994.6

[4] R Housley, "Cryptograghic Message Syntax(RFC2630)",ITEF, 1999.6.

[5] 이만영, 김지홍, 류재철, 송유진, 염흥열, 이임영, "전자상거래 보안 기술", 생능출판사, 1999

[6] William Stallings, "Cryptography And Network Security: Principle and Practice" second edition.

[7] Scott, "Java Network Programing", O'REILLY, 1997.

[8] B. Ramsdell, "S/MINE Version 3 Certificate Handling(RFC2632)", IETF, 1999.6.