PKI환경에서 ElGamal 방식의 ECC를 이용한 안전한 메신저 설계에 관한 연구

박수영* · 최광미** · 정채영***

A Study on the Design of Secure Messenger Using ECC of ElGamal Method in PKI Environment

Su-young Park* · Kwang-mi Choi** · Choi-yeoung Jung***

이 논문은 2005년도 조선대학교 학술연구비를 지원받았음

요 약

컴퓨터와 네트워크의 보급이 일반화되면서 인터넷을 통한 정보 전달이 일상생활처럼 되고 있다. 기존에는 정보를 전달하기 위한 방법이 주로 전자메일에 한정되어 있던 것에 반해, 요즘은 좀 더 즉각적으로 메시지를 전달해주는 메신저를 많이 사용하고 있다. 현재 사용되고 있는 대부분의 메신저는 자료의 효과적인 관리를 위한 통신의 주체가 되는 각각의 에이젼트들간의 통신과 서버와 에이젼트의 통신에 있어 악의적인 침입에 의한 정보누출이 문제가 되고 있다. 본 논문에서는 메신저의 안전한 통신을 위해 PKI를 이용한 ElGamal 방식의 ECC 이용하여 최대한 안전성이 확보될 수 있고 사용자 그룹 단위의 암호화를 위해 그룹별로 타원곡선과 그 위에 있는 임의의 점을 선택하여 다른 그룹과 구별할 수 있는 안전한 메신저 시스템을 설계하였다.

ABSTRACT

As computers and networks become popular, distributing information on the Internet is common in our daily life. In the past, e-mail has been the primary choice of exchanging information, but messengers are gaining popularity abroad and domestically because of their nature of getting immediate responses. Information leakage by invasion that is enemy of evil in communication of communications division Server and Agent between each agents that become burden of communication for effective administration of data for most of existing messenger is becoming an issue. In this paper, we design a secure messenger system that could be obtained maximum security. It use ECC based on ElGamal methodology using PKI for secure communication. For the message encryption and decryption between the same group users, each group is kept distinct by drawing an elliptic curve and an arbitrary point is chosen on the curve.

키워드

Messenger, PKI(Public Key Infrastructure), ElGamal, ECC(Elliptic Curve Cryptography)

* 조선대학교 컴퓨터통계학과

** 동강대학 컴퓨터인터넷 계열

*** 교신저자

접수일자 : 2006. 3. 23

Ⅰ. 서 론

메신저란 네트워크를 통하여 실시간으로 메시지를 주고받을 수 있는 프로그램을 말한다. 현재 사용되고 있는 대부분의 메신저는 자료의 효과적인 관리를 위한 통신의 주체가 되는 각각의 에이젼트들 간의 통신과 서버와 에이젼트의 통신에 있어 악의적인 침입에 의한 정보누출이 문제가 되고 있다.

따라서, 메신저의 메시지에 대한 보안을 위해서는 메신저를 사용하는 사용자가 많아 복잡한 키(key)를 적절하게 관리할 수 있는 암호화 방식이 요구되고, 안전한 암호화 통신을 위해서 사용자 인증이 필요하며, 실시간으로 메시지의 통신이 이루어지므로 메시지에 대한 암호화 및 복호화 수행 시간이 적게 소요되는 암호화 방식이 필요하다.

본 논문에서는 메신저의 안전한 통신을 위해 PKI를 이용한 ElGamal 방식의 Elliptic Curve Cryptography(이하 : ECC) 사용하여 최대한 안전성이 확보될 수 있게 하였다. 사용자 그룹 단위의 암호화를 위해 제안한 방법은 그룹별로 타원곡선과 그 위에 있는 임의의 점을 선택하여 다른 그룹과 구별할 수 있는 안전한 메신저 시스템을 설계하였다.

논문의 2장에서는 현재 서비스되고 있는 메신저의 특징과 보안위협을 알아보고, PKI의 개요에 대해서 소개한다. 3장에서는 본 논문에서 제안하는 PKI를 이용한 새로운 인증 메신저 시스템을 설명하고, 끝으로 4장에서 결론을 맺는다.

Ⅱ. 공개키 기반구조 개요

2.1. 관련연구

1) 메신저의 특징

ICQ(I Seek You)메신저는 미라빌리스사의 제품으로 인스턴트 메신저의 원조이며, 그 사용자 수도 많다. ICQ 메신저의 특징으로는 사용자가 대화 모드를 선택하여, 현재 자신의 상태를 다양하게 표시할 수 있으며, 대화 모드에는 온라인, 오프라인, 방해금지, 비공개 등으로 모드에 따라서 메시지 수신 방법 등의 차이가 있다[1]. MSN (Microsoft Network)메신저는 마이크로소프트사의 제품으로 메일 서비스 계정으로 메신저에 접속한다. MSN메신저는 접속한 사용자에게 실시간으로 메시지 전송을 할 수 있는데, 수신자가 도착된 메시지를 읽으면, MSN 인스턴트 메시지 창이 뜨게 된다. 인스턴트 메시지 창은 일대일 대화 기능처럼 두 사용자가 주고받는 메시지를 한 화면에 보여주고, 두 사용자간에 일대일 대화를 하는 동안 다른 사람을 초대하여 대화방 기능처럼 사용할 수 있다[2]. AOL(America Online)메신저는 중앙의 BOS서버를 경유하여 한 사용자가 다른 사용자에게 HTML로 작성된 평문 메시지를 전송한다. AOL메신저의 특징으로는 직접적인 연결을 통하여 BOS서버를 경유한 AOL의 이미지 전송, 음성채팅, 게임요청, 파일공유 등이다. AOL메신저는 먼 거리에 있는 사용자에게 게임 프로그램의 실행을 요청할 수 있고, 요청 동안에는 어떠한 직접연결도 설정 될 수 없다[3].

2) 보안 위협

주요 인스턴트메신저 제작회사의 공통적인 보안 위협은 다음과 같다[1][2][3].

- 감염된 파일 전송 : 의도적으로 감염된 파일을 보내거나 또는 자신도 모르는 사이 감염된 파일을 다른 사용자에게 보낼 수 있다.
- 통신 메시지 노출 : 메신저를 이용한 어떤 대화 내용도 암호화되지 않는다.
- 저작권 침해 : 메신저를 통해 완전하게 전송된 많은 파일(복사된 파일, MP3 파일, 복사된 사진 등)이 저작권법에 위배된다.
- 현혹적인 책략 : 바람직하지 않은 일부 인터넷 사용자는 매우 현혹적인 내용으로 개인의 신상 정보는 물론 각종 비밀번호 등의 누설을 유도한다.
- 파일 전송 시 IP 주소 노출 : 파일 전송과 이미지 전송, 음성채팅, 파일공유는 메신저 사용자의 실제 IP 주소를 노출시킬 수도 있다.

2.2. PKI 구조

1) PKI 기본 구성도

시스템 관리에서는 CA(Certification Authority)의 전체 시스템을 관리하기 위해 필요한 기능 즉 관리자의 인터페이스, 시스템 설치, 운영자 정보 관리, 데이터베이스 무결성 확인, 데이터베이스 백업 스케줄 결정, 예외적인 일의 발생 시 회복 등과 같은 기능을 수행한다. 패스워드와 사용자 이름을 해쉬 함수(hashing function)에 적용하여 하나

의 토큰을 생성하고 이 토큰을 데이터베이스에 저장한다. 관리자가 로그인 할 때, 패스워드와 이름을 입력하고 앞에서 실행한 똑같은 해쉬 함수를 이용하여 토큰을 생성하고 데이터베이스에 저장된 토큰과 비교하여 정확한 패스워드인가를 확인한다. 운영자 관리 서비스 모듈은 CA가 설치된 시스템과 독립된 시스템에 설치할 수 있으며, CA와 운영자 관리 서비스 프로그램 사이에 통신 보안이 보장된다. 일반적으로 이것을 지역등록기관이라고 하며, 운영자는 사용자 등록, 삭제, 변경 등을 담당하는 사람이다.

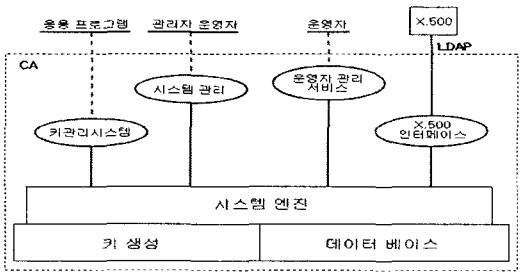


그림 1. PKI의 기본 시스템 구성도
Fig 1. basic system construction of PKI

키 관리 시스템은 응용프로그램(예: 하이브리드 메시징 시스템) 또는 다음 CA로부터의 인증서 요구, 암호화 키 생성 요청 등을 받고 수행하며 그 결과를 요청자에게 전송하고, CA 비밀키와 공개키, 사용자 암호화 키 등을 생성하는 역할을 담당한다. 이 부분은 하드웨어로 구성하는 것이 좋다. 데이터베이스는 운영자와 관련된 정보, 관리자와 운영자가 수행할 수 있는 시스템 모듈과 영역을 정의한 privilege set, 키 history 등을 저장한다. CA의 서명키는 CA 관리자 비밀키에 의해 암호화되며, 다른 중요한 데이터는 운영자 비밀키에 의해 암호화된다. CA 관리자 비밀키와 운영자 비밀키는 각각의 패스워드를 기반으로 시스템이 자동 생성한다. 마지막으로 인증서는 사용자의 신분과 공개키를 연결해주는 문서로 인증기관의 비밀키로 전자 서명하여 생성된다. 인증서의 형식은 1988년 ITU-T가 X.509 초기버전을 공표하고, 1993년에 버전 2를 공표했으며, 1995년 이후로는 ISO/IEC 9594-8의 문서와 동일시되어 공동 개발되었다. 현재 X.509 v3형식은 그림 2과 같다[6].

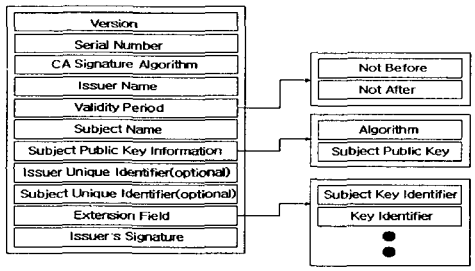


그림 2. X.509 v3
Flg 2. X.509 v3

그림 3 인증기관을 이용한 인증서 발급절차를 보여주고 있다.

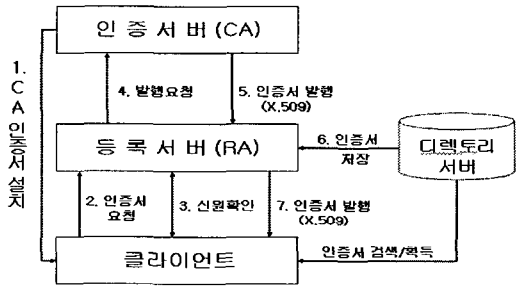


그림 3. 인증서 발급절차
Fig. 3 Issue procedure of Certification

1. 인증서를 신청하는 곳에서는 우선 인증서버의 인증서를 설치해야 한다.

2. 클라이언트는 공개키와 인증서 발급요청서를 등록기관에 보낸다.

3. 접수한 인증 신청을 심사한다.

4. 신원확인에 문제가 없다면, 등록서버는 인증서버에 발행요청을 한다.

5. 인증서버는 공개키와 사용자정보를 이용하여 X.509 인증서를 만들어, 해당 인증서를 등록서버에 전달한다.

6. 등록서버는 모든 신뢰당사자가 이용할 수 있도록 인증기관의 저장소 또는 디렉토리 서버에 저장한다.

7. 등록서버는 클라이언트에게 인증서를 발급한다.

8. 발급된 인증서는 인증기관의 정책에 따라 관리된다.

Ⅲ. 안전한 메신저

3.1. PKI를 이용한 키 생성 및 인증서 발급

본 논문에서 제안하는 인증 프로토콜의 전반적인 흐름은 그림 4와 같다.

※ 인증 프로토콜에 사용되는 기호

CA : 인증기관
MS : 메신저 서버
Client A : 사용자 A
Client B : 사용자 B
M : 메시지
ER : 공개키 암호알고리즘 암호
DR : 공개키 복호알고리즘 복호
Z : 압축 알고리즘
KUa : A의 공개키
KUb : B의 공개키
KUs : 서버의 공개키
KRa : A의 개인키
KRb : B의 개인키
KRs : 서버의 개인키
Ks : 세션키
H : 해쉬 알고리즘
Certificate A : A의 인증서
Certificate B : B의 인증서
PSE : 사용자의 정보를 저장하고 있는 국부 메모리

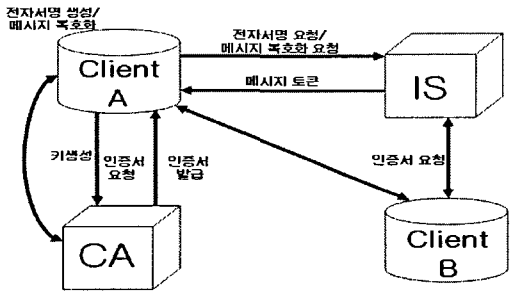


그림 4. 프로토콜 전체 개략도
Fig. 4 Total summary of protocol

3.2. 인증서 신청

CA와 Client A는 세션키를 안전한 방법(out of band)을 통하여 공유하고 있어야한다. Client A는 PSE를 생성하여 세션키로 암호화하여 인증기관에 전송하고. CA는 세션키로 검증 후 인증서를 생성하여 Client A의 공개키로 암호화하여 전송한다.

$$ERKUKs\{PSE\} \quad (1)$$

$$ERKUa\{Certificate\ A\} \quad (2)$$

3.3. 신규등록

신규등록 기능은 사용자로부터 ID와 패스워드 등의 사용자 정보를 입력받아 신규 사용자 등록 작업을 수행하는 기능으로써, 입력된 ID의 중복 여부를 판단하여 모든 입력이 정확하게 이루어지면 Client A는 PSe를 Hash하고 자신의 개인키(KRa)로 암호화하는 하는 고장을 통하여 문서의 지문과 자신의 서명을 한다.

$$ERKRa\{H(PSE)\} \quad (3)$$

그리고 차후에 발생될 전송여부와 변조여부의 시비를 확인할 수 있도록 Hash된 문서(H(PSE))를 보관한다. M, ERKRa{H(PSE)}, Certificate A를 함께 압축하고 세션키(Ks)를 사용하여 관용키 암호화알고리즘으로 암호화한다.

$$EKs\{Z\{M||ERKRa\{H(PSE)||Certifacate\ A\}\}\} \quad (4)$$

세션키(Ks)는 MS의 공개키(KUs)로 암호화 한 후

$$ERKUs(Ks) \quad (5)$$

세션키로 암호화한 문서와 같이 MS에게 전송한다.

$$EKs\{Z\{M||ERKRa\{H(PSE)||Certifacate\ A\}\}\ ||\ ERKUs(Ks) \quad (6)$$

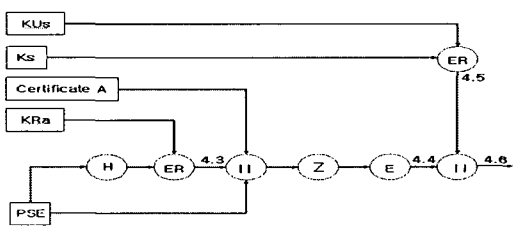


그림 5. 등록 전송전의 암호화 방법
Fig. 5 Cryptography before transmitting registration

그림 6은 MS가 사용자로부터 암호화된 정보를 받아 개인키를 이용하여 해독하는 부분이며 수행과정은 다음과 같다.

MS는 Client A에게서 받은 문서 중 ERKUs(Ks)를 자신의 개인키(KRs)를 사용하여 세션키(Ks)를 구한다.

$$DRKUs\{ ERKUs(Ks)\} = Ks \quad (7)$$

구한 세션키(Ks)를 사용하여 관용키 암호화된 부분을 복호화 한다.

$$DKs\{EKs\{Z\{PSE||ERKRa\{PSE)||CertificateA\}\} \quad (8)$$

사용된 압축을 풀어내고 Certificate A를 통하여 유효한 공개키인지 확인하여 유효하지 않은 인증서이면 재전송을 요구하고 유효한 인증서이면 디렉토리 서버에 저장 후 다음 작업을 수행한다.

클라이언트 a의 개인키(KRa)로 암호화 된 PSE를 인증서 A에 포함되어 있는 A의 공개키를 사용하여 복호화 한다.

$$DRKUa\{ ERKRa\{ H(PSE) \}\} = H(PSE) \quad (9)$$

압축을 풀어낸 문서에 포함된 PSE를 Hash하고 식 4.9에서 나온 H(PSE)과 비교하여 다르면 재전송을 요구하고 같으면 전송도중에 변조되지 않은 것으로 인정한다.

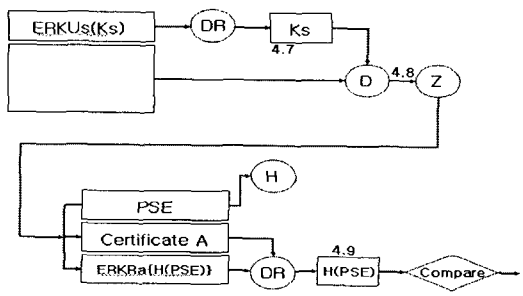


그림 6. 등록 수신후의 복호화 방법
Fig. 6 Decryptography after receiving registration

3.4. ElGamal 방식의 ECC를 이용한 암호화된 대화 기능

사용자 A가 B에게 채팅을 요청하여 상호간의 메시지 송·수신 중에 암호화된 메시지를 전송하는 기능을 수행한다. 인증서에는 각자의 공개키가 들어 있으므로 인증서를 서버로부터 획득하여 서로의 공개키를 확인한 다음 이 공개키를 이용해서 필요한 데이터를 암호화해서 보낸다. 이때 제약사항으로는 채팅하는 사용자가 인증서가 등록된 그룹멤버여야 한다.

Client A와 Client B는 사용할 타원곡선 E와 타원곡선 위의 임의의 점Q를 결정한다. Client B는 자신이 암호문을 전달받기 위하여 자신의 개인키를 이용하여KRbQ를 계산하여 공개한다. 그리고 Client A는 자신의 개인키를 이용하여 KRaQ를 계산하고, 평문 P의 암호문으로 순서쌍 (KRaQ, P+KRa(KRbQ))를 Client B에게 보낸다.

$$\{ KRaQ \,||\, P+KRa(KRbQ) \} \quad (10)$$

또한, Client B는 KRaQ에 자신의 개인키 KRb를 곱하여 KRa(kRbQ)를 구하고 이를 이용하여 P + KRa(KRbQ) - KRb(KRaQ)를 구하여 평문 P를 얻는다.

$$\{ KRaQ \times KRb \} = \{ KRa(KRbQ \} \quad (11)$$

$$\{ P + KRa(KRbQ) - KRb(KRaQ) \} = P \quad (12)$$

ElGamal 방식을 이용하여 암호화 및 복호화를 할 때에는 덧셈연산 및 뺄셈 연산만을 수행하기 때문에 메시지가 증가함에 따라 수행시간이 비례적으로 증가하게 된다.

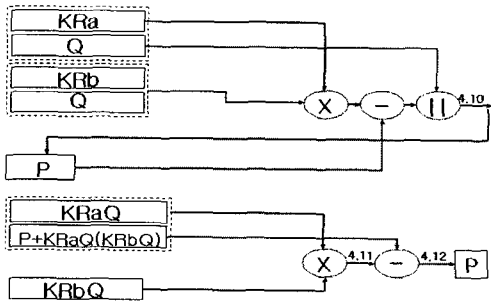


그림 7. 암호화 된 대화 기능
Fig 7. encrypted conversation

Ⅳ. 결 론

본 논문에서는 서버와 클라이언트환경에서 PKI를 이

용한 사용자 인증을 소개하고, 서버로부터 획득한 인증서에 공개키를 사용하여 ElGamal 방식의 타원곡선암호(ECC)알고리즘을 이용한 안전한 메신저 시스템을 소개하였다.

인스턴트 메신저에서 사용자는 메신저에 등록하기 위하여 개인 신상에 관한 정보 및 인증서를 서버에 전송한다. 사용자는 서버에 접속하여 상대방의 인증서를 요청하고 유효한 인증서인지 확인한다. 유효한 인증서이면 타원곡선 E와 타원곡선 위의 임의의 점Q를 선택하여 암호화 통신을 시작한다. 타원곡선 암호는 각기 다른 타원곡선의 위의 점을 임의로 선택하여 소그룹 단위로 설정하고, 소그룹별로 등록된 사용자들만 서로 통신할 수 있는 환경도 제공할 수 있다. 또한 타원곡선 암호 알고리즘을 이용함으로써 공개키 암호 방식의 단점인 연산처리 속도를 향상시킬 수 있다.

향후 연구과제로는 인증서에 대한 활용성을 증가시키기 위해서는 전자정부를 위한 공개키 기반구조 영역과 민간 분야를 위한 공개키 기반구조 영역간의 상호 연동을 위한 인증서 정책이 개발되어야 한다.

참고문헌

[1] ICQ, http://www.icq.com

[2] MSN, http://www.dreamseurity.com/products

[3] AOL, http://www.aim.com

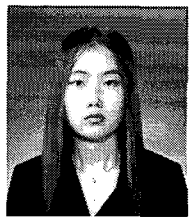
[4] R. Housley, W. Ford, W. Polk., D. Solo, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, RFC2495, January 1999

[5] R. Housley, W. Polk, Representation of Key Exchange Algorithm(KEA) Keys in Internet X.509 Public Infrastructure Certificates, RFC 2528, March 1999

[6] S. Boeyen, T. Howes, P. Richard, Internet X.509 Public Key Infrastructure Operational Protocols-LDAPv2, RFC 2559, April 1999

[7] C. Adams S. Farrell, Internet X.509 Public Key Infrastructure Certificate Management Protocols, RFC 2510, March 1999

저자소개

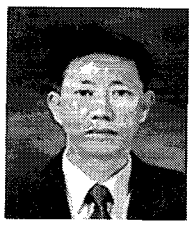


박 수 영(Su-Young Park)

2001년 조선대학교 전산통계학과 이학사
2003년 조선대학교 전산통계학과 이학석사
2005년 조선대학교 전산통계학과 박사수료
※관심분야: 정보보호, 신경망, 신경망, 인공지능, 멀티미디어, Bioinformatics

최 광 미(Gwang-MI Choi)

2003년 조선대학교 전산통계학과 이학박사
2002년~2006년 현재 동강대학 컴퓨터인터넷계열 초빙전임강사
※관심분야: 정보보호, 신경망, 인공지능, 디지털컨텐츠, Bioinformatics



정 채 영(Chai-Yeoung Jung)

1983년 조선대학교 공학사
1986년 조선대학교 공학석사
1989년 조선대학교 공학박사
1986~현재 조선대학교 자연과학대학 컴퓨터통계학 교수
※관심분야 : 정보보호, 신경망, 인공지능, 멀티미디어, Bioinformatics