타원곡선 암호체계를 이용한 인스턴트 메세징 서비스에서의 키 교환 방식

박수영° 박병전 정채영
조선대학교 전산통계학과

Key Exchange Method in Instant Messaging Service Using Elliptic Curve Cryptography

Su-Young Park° Byung-Jun Park Choi-Yeoung Jung
Dept. Computer & Statistics. Chosun University

요 약

컴퓨터와 네트워크의 보급이 일반화되면서 인터넷을 통한 정보전달이 일상 생활처럼 되고 있다. 기존에는 정보를 전달하기 위한 방법이 주로 전자메일에 한정되어 있던 것에 반해, 요즘은 좀 더 즉각적으로 메시지를 전달해주는 인스턴트 메신저를 많이 사용하고 있다. 인스턴트 메신저는 이러한 장점으로 인해 국내에서도 사용자가 급속하게 늘고 있다. 현재 사용하고 있는 대부분의 인스턴트 메신저는 서버에 로그 온 할 때 패스워드를 대칭키 암호기술로 암호화해서 보내지만 패스워드 크래킹 프로그램들이 많이 알려져 있어 전송되는 정보가 제 3자에 의한 암호 해독이 가능하게 된다. 또한 키 분배 및 관리에 있어서 어려움이 있다. 대칭키 암호기술의 어려움을 극복하는 방안으로 제안되었던 공개키 암호기술은 키 분배 및 관리는 편리해졌지만 알고리즘이 더 복잡하고 키의 길이가 상당히 길어 많은 제약이 따르며 처리속도가 오래 걸린다는 단점을 지닌다.[1] 이에 대안으로 제안된 타원곡선 암호체계(Elliptic Curve Cryptography, ECC)는 동일한 키 사이즈를 갖는 다른 암호체계보다 훨씬 강하다고 알려져 있다. 본 논문에서는 ECC를 이용하여 빠르고 효율적이며 높은 안전도를 나타내는 인스턴트 메신저에서의 패스워드 키 교환 방식을 설계한다.

1. 서 론

인터넷 사용인구가 증가하고 인터넷을 이용한 e-비지니스와 서비스가 다양해짐에 따라, 인터넷을 이용한 통신 방법도 매우 다양해지고 있다. 인스턴트 메시징 서비스는 온라인 상에 있는 사용자들이 실시간으로 메시지를 주고 받을 수 있는 서비스이다. 쉽게 생각하면 온라인 상에서 전화와 같이 상대방과 대화를 나눌 수 있는 서비스라 할 수 있다[2].

인스턴트 메신저는 전자메일이 사용자가 메일 서버에 접속하여 메일을 읽어오는 과정을 요하는 비해, 자동적으로 사용자 화면에 메시지를 전달함으로써 보다 간편하고 즉각적인 메시지의 전달을 기대할 수 있다. 인스턴트 메신저는 이러한 장점으로 인해 그 이용자 수가 빠르게 증가하고 있으며, 인터넷의 가장 보편적인 서비스의 하나로 정착하게 될 것이라고 전망된다. 그러나 현재 사용되고 있는 대부분의 인스턴트 메세징 시스템에서 클라이언트가 서버에 로그온 할 때 아이디와 패스워드를 대칭키 암호기술로 암호화하여 전달한다. 그러나 대칭키 암호 알고리즘은 크래킹 툴이 많이 알려져 있어 안전하지 못하다[4]. 본 논문에서는 무선 인터넷 환경에서 안전하고 신뢰할 수 있는 ECC를 이용한 인스턴트 메세징 서비스 시스템에서의 키 교환 방식에 대해 분석하고자 한다. 본 논문의 2장에서는 인스턴트 메세징의 시스템에 대해 알아보고 3장에서는 정보보호 서비스의 근간이 되는 공개키 기반구조에 대해 살펴보고, 4장에서는 타원곡선 암호체계에 대해서 살펴본다. 5장에서는 타원곡선 암호체계를 기반으로 하는 인스턴트 메세징 서비스에서의 키 교환방식을 제안하고, ECC의 안전성을 검증하며, 마지막으로 6장에서 결론을 맺는다.

2. 인스턴트 메세징 시스템 개요

인스턴트 메세징 시스템은 텍스트 메시지를 주고 받고 상대방의 온라인 상태 정보를 알려주던 초기 형태에서 발전하여 최근에는 파일 전송, 음성 메시지, 화상 회의 등 여러 기능이 추가되고 있다. 본 절에서는 인스턴트 메세징 시스템의 기본 개요에 대해서 살펴보고자 한다.

2.1 인스턴트 메세징 시스템 분류

현재 널리 쓰이고 있는 인스턴트 메세징 시스템을 분류해 보면 다음과 같다. 인스턴트 메세징 시스템은 클라이언트/서버 시스템으로 구성되며 우선 사용자가 고유의 정보가 어디에 저장되느냐에 따라서 Network-based 시스템과 Device-based 시스템으로 나눌 수 있고, 클라이언트 사이의 연결 형태에 따라서 Centralized Network, Peer-to-Peer Connection 시스템으로 나눌 수 있다[2].

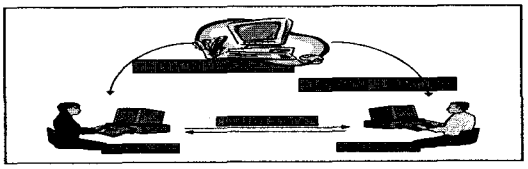

그림 1. Centralized Network

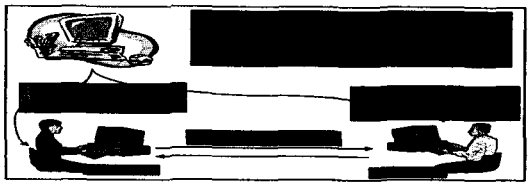

그림 2. Peer-to-Peer Connection

3. 공개키 기반구조

공개키 암호방식은 비 대칭 키 방식이라고 불리기도 하는데, 암호화와 복호화에 사용되는 키가 동일한 관용 암호방식과는 달리 암호화에 사용되는 키와 복호화에 사용되는 키가 서로 다른 것이 특징이다. 제 3자가 중간에 메시지를 가로챈다 하더라도 비밀키를 모르면 암호문을 복호화하여 그 내용을 볼 수 없다.

대칭키 암호 기술은 많은 크래킹 툴이 알려져 있어 안전하지 못하고 키 분배 및 관리에 있어서 어려움이 있다. 대칭키 암호 기술의 어려움을 극복하는 방안으로 제안되었던 공개키 암호 기술은 키 분배 및 관리는 편리해졌지만 알고리즘이 더 복잡하고 키의 길이가 상당히 길어 많은 제약이 따르며 처리속도가 오래 걸린다는 단점을 지닌다.[5] 본 논문에서는 훨씬 짧은 길이의 키를 가지고도 같은 정도의 안전성을 가지며 연산 속도가 훨씬 빠른 ECC(Elliptic Curve Cryptography)를 이용하여 인스턴트 메신저에서의 패스워드 키 교환 방식을 설계한다

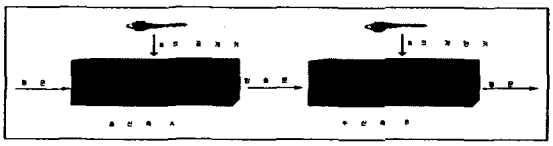

그림 3. 공개키 암호방식에서의 암호화.

4. 타원곡선 암호체계

4.1 타원곡선 암호시스템의 배경

타원 곡선을 이용한 공개키 암호시스템 즉, 유한체 위에서 정의된 타원곡선군에서의 이산대수 문제에 기초한 타원 곡선 암호시스템은 1985년 N. Koblitz와 V. Miller에 의해 처음 제안된 이후 활발히 연구되고 있다[3]. 또한, 타원 곡선을 이용하여 최근 RSA 암호시스템의 근간이 되는 인수분해 문제와 소수성 테스트(primality test)를 위한 효율적 알고리즘을 제공하기도 하였다[4]. 일반적으로 타원곡선에는 불특이 타원곡선과 초특이 타원곡선(supersingular elliptic curve)의 두 가지 종류가 존재하는데, Menezes, Okamoto와 Vanstone에 의해 연구된 결과에서 초특이 타원곡선의 이산 대수 문제가 유한체 위에서의 이산 대수 문제로 바뀔 수 있음이 증명되었다.

ECC는 특정 암호 알고리즘이 아니라, 암호 알고리즘을 구현해 볼 수 있는 수학적인 장소를 제공하고 있는 것으로 RSA, ElGamal등의 알고리즘을 기존의 정수 공간이 아닌 타원 쌍곡선 위에서 구현을 한 것이다[5].

4.2 타원곡선 연사의 기하학적인 이해

4.2.1 실수 위에서의 타원곡선

유한체 $GF(p)$(p>3인 소수)상의 타원곡선은 다음과 같은 Weierstrass 방정식을 만족하는 $GF(p)$상의 모든 점 (x, y)와 가상의 무한원점(point at infinity) O로 구성된다. 실수 위에서 정의된 타원곡선이라 함은 식 4-1의 타원곡선 방정식을 만족시키는 점(x, y)들의 집합이다.

$$y^2 = x^3 + ax + b, (x, y, a, b\text{는 모두실수}) \quad \text{(식 4-1)}$$

여기서 계수들은 다음 조건, $4a^3+27b^2 \neq 0$을 만족시킨다면 이 타원곡선은 실제로 이 타원곡선 상에 존재하지 않는 무한원점(point at infinity) O와 함께 하나의 군을 형성한다. 실수에서 정의된 타원곡선은 계산이 느리고 반올림에 의한 오차로 인하여 계산이 부정확하고 구현하는 원소가 (0, 1)을 사용하므로 암호에는 적당하지 않다. 이런 이유로, 실제 암호학적인 어플리케이션에서의 응용은 주로 정수 유한체 $GF(p)$를 사용하거나 이진 유한체(binary finite field)인 $GF(2^m)$을 사용한다.

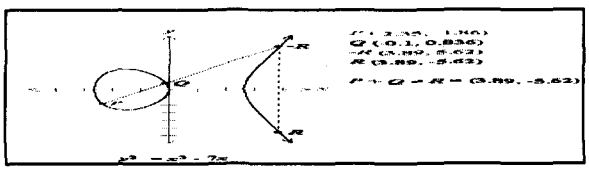

그림 4. 실수 타원곡선 상의 서로 다른 두 점의 덧셈의 예

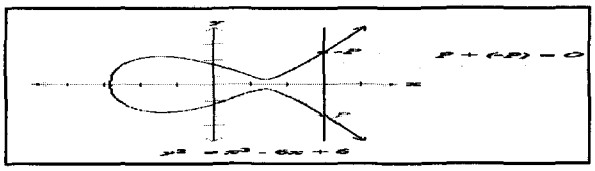

그림 5. 덧셈에 대한 역원과 무한 원점

4.2.2 $GF(2^m)$ 위의 타원곡선

장 특성(field characteristic) 2를 가지는 유한체 $GF(2^m)$상에서 정의된 불특이 타원곡선을 E한다면, E는 다음 방정식을 만족시키는 $GF(2^m)$상의 (x, y)와 실제로 타원곡선 위에는 존재하지 않지만 가상적으로 존재하는 무한 원점 O의 집합이다. 식 4-2

는 유한체 $GF(2^m)$에서의 타원곡선 방정식이다.

$$y^2+xy=x^3+ax^2+b, (a, b\in GF(2^m)) \quad (식\ 4\text{-}2)$$

$GF(2^m)$상에서 정의된 타원곡선 군은 유한 개의 원소을 가지게 되고 반올림에 따른 오름차가 전혀 없기 때문에 이진 컴퓨터 연산에 많이 쓰이게 된다. P와 Q를 타원곡선 E위의 두 점이라 하면 아래 같은 연산 공식이 성립한다.

[$GF(2^m)$상의 점 덧셈 연산 알고리즘]

◎ $P\neq Q$이면, $P+Q=R(x_3, y_3)$이고, x_3, y_3의 값 은 다음과 같다.

$$x_3=\lambda^2+\lambda+x_1+x_2+a,$$
$$y_3=\lambda(x_1+x_3)+x_3+y_1$$
$$\lambda=\left(\frac{y_1+y_2}{x_1+x_2}\right).$$

타원곡선 암호 시스템의 안전도는 타원곡선 상에서의 이산대수 문제의 복잡성에 근거한다. 즉, 타원곡선 $E(GF(2^m))$위의 점 P 와 $Q=k\cdot P$가 주어졌을 때, k를 지수 함수 시간 내에 구하기가 불가능하다는 것이다[6].

4.3 구 현

타원곡선 암호시스템은 타원곡선 위의 점 P을 x번 더하는 계산이 주를 이룬다. 즉, $Q=xP$을 구하는 덧셈 연산은 모듈러 곱셈을 통해 이루어진다. 주요 공개키 암호시스템은 효율적인 모듈러 곱셈에 의존하고 있으며, 타원곡선은 소수 P 의 값이 서로 다른 시스템보다 작기 때문에 그 효율성이 뛰어나다 할 수 있다. 즉, 타원곡선 암호시스템의 안전도는 타원곡선 이산대수 문제에 의존하고 있으며, 그 효율성은 xP 빠른 계산에 달려 있다.

5. ECC를 이용한 인스턴트 메시징 서비스에서의 키 교환 방법

5.1 프로토콜

타원곡선 E와 $P(\in E)$를 공개하고, 메시지 $M=(ID_x, PWD_y)(\in F_{2_m}\times F_{2_m})$이라 가정하자.

<Client(인스턴트 메세징 사용자)가 Sever에 로그인 할 때>

[Sever]

임의로 정수 a를 선택

kP를 계산하여 공개

[Client]

임의로 정수 k를 선택

점 kP와 점 $k(aP)=a(kP)=(x, y)$를 계산

$x, y \neq 0$ 이면,

$(kP, IDx, PWDy)$를 Server에게 보낸다.

<ID, PWD를 확인하기 위하여(Server)>

1) $a(kP)=(x,y)$를 계산

2) $\frac{IDx}{x}=ID, \frac{PWDy}{y}=PWD$를 계산

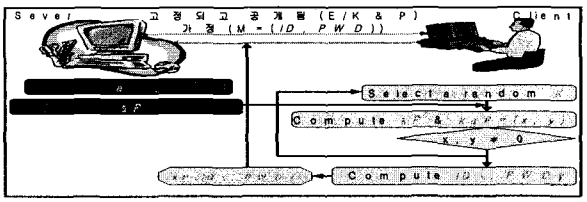

그림 6. Client가 Sever에게 ID, PWD를 보내는 과정

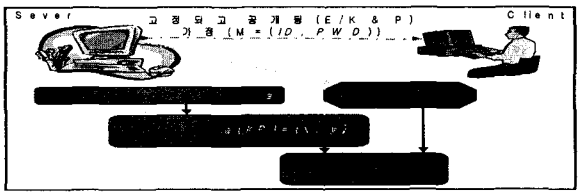

그림 7. ID, PWD를 얻는 과정

5.2. 안전성

공개키 암호시스템의 이론적 안전도를 조사하기 위해서는 먼 시스템을 공격하는 데 있어 그 시스템의 기반이 되는 수학적 문제를 푸는 것이 요구되는가를 분석한다.

모듈러 P에서의 소인수 분해 문제와 이산대수 문제는 일반적으로 Sub-exponential time 알고리즘이 알려져있다. 이 알고리즘의 수행시간은 상수 C 에 대하여 $O(\exp((c+o(1)))(\ln n)^{1/3}(\ln \ln n)^{2/3})$이다. 타원곡선 이산 대수 문제를 위한 최상의 알고리즘은 완전지수 복잡도 알고리즘이며, 수행시간은 $O(\sqrt{P})$이다. 이것은 타원곡선 이산대수문제가 소인수분해 문제나 이산대수문제보다 어렵다는 것을 의미한다.

완전지수 복잡도 알고리즘은 타원곡선 암호시스템과 RSA를 깨는 알려진 최상의 알고리즘으로 그 수행시간을 비교하여 보면 그림 4와 같고 표 1는 CertiCom에서 제시한 자료로서 같은 안전도를 갖는 RSA/DSA와 타원곡선에 대한 도메인 변수의 크기를 비교해 놓은 것이다[7].

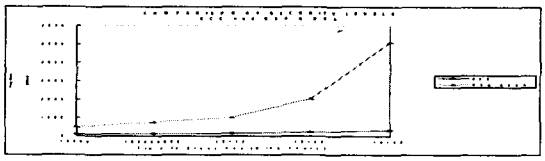

그림 8. 안전도 수준 비교

Time to break in MIPS year	RSA/DSA (bits)	ECC (bits)	RSA vs. ECC key
10^4	512	106	5:1
10^8	768	132	6:1
10^{11}	1024	160	7:1
10^{20}	2048	210	10:1
10^{78}	21000	600	35:1

표1. 같은 안전도에 따른 도메인 변수의 크기 비교

6. 결 론

IDC 보고서에 따르면 2003년 현재 전세계적으로 1억 3천명 정도가 무료 인스턴트 메세징 서비스를 사용하고 있으며 이중에 8천만명 정도는 매일 인스턴트 메세징 서비스를 이용하고 있는 것으로 나타났고 앞으로 인스턴트 메신저의 사용은 앞으로 점점 늘어날것으로 전망된다. 인스턴트 메세징 서비스가 보다 활성화되기 위해서는 안전성 및 신뢰성을 보장할 수 있는 정보보호가 필요하다. 본 논문에서는 처리 속도가 빠르고 비트당 안전도가 타 공개키 시스템보다 효율적인 ECC
에대해 살펴보고 인스턴트 메세징 서비스에 적용할 수 있는 방법을 고찰해보았다. 또한 이 방법의 보안 수준을 완전지수복잡도 알고리즘을 이용하여 RSA 및 DSA를 깨는데 걸리는 수행시간과 도메인 변수 크기를 비교하였다. 결과적으로 기존의 아이디 패스워드 암호화 방식으론 안전하지 못하며, ECC를 이용한 방법이 안전하다는 것을 볼 수가 있었다. 따라서, 가까운 미래에 ECC를 이용한 인스턴트 메신저가 주류를 이룰 것으로 예상된다.

더 나아가, 인스턴트 메세징 서버와 클라이언트 사이의 통신을 위해서 침입탐지 시스템을 무사 통과할 수 있도록 설계된 점에 대한 보완 방법도 강구 되어야 할 것이다.

참고문헌

[1] http://www.idata.co.kr/199907/solution/218.htm
[2] Gartner report. "Manage resks of free IM usage to gain business value," TechRepublic Inc., 2001.11.16.
[3] 서광식, 김용태, 임종인, 김창한, 수론과 암호학, 경문사, 1998.
[4] D. Chundnovsky and G. Chundnovsky, "Squences of numbers generated by addition in formal guoups and new primality and factoring test," Advances in Applied Mathematics, 7, PP. 385-434, 1087.
[5] A.J. Menezes and S. A. Vanstone, "Elliptic Curve cryptosystems and their implementation, Journal, on Crytology, PP 209-224, Autumn, 1998.
[6] ECC Totorial, http://www.certicom.com/resources/ecc_toturial/ecc_toturial.html, 2001.
[7] Insoo Lee, "Analysis on Elliptic Curve Public Cryptosystems", KISA, December, 1998.