타원 곡선을 이용한 전자 서명 알고리즘 연구

전 용 준*, 전 문 석, 이 철 희
숭실대학교 전자계산학과 대학원

A Study of Digital Signature Using The Elliptic Curve.

Jun, Yong-June* · Jun, Moon-Seog · Lee, Chul-Hee
Dept. of Computer Science, Soongsil University

요 약

타원 곡선 암호 시스템은 기존의 암호 시스템에 비해 단위 비트당 키 길이가 작으며, 속도가 빠르다는 장점을 가지고 있으므로 이러한 장점을 이용하여 휴대 통신 기기에 적용할 수 있다. 이에 본 논문에서는 타원 곡선에 대한 사항에 대하여 살펴 보며, 이산 로그 문제에 기반한 전자 서명 알고리즘인 *ElGamal* 스킴을 타원 곡선에 사용한 타원 곡선 전자 서명 구현 방안을 제시하고자 한다.

1. 개 요

타원 곡선은 대수학적으로나 기하학적으로 지난 150여년 동안 심오한 연구를 지속해 왔었다. 그래서 타원 곡선에 대한 이론은 매우 풍부하며 이론적으로도 심도 깊다. 타원 곡선을 암호화 시스템에 처음 제시 한 것은 1985년에 워싱턴 대학의 닐 코블리츠(Neal Koblitz)와 IBM의 빅터 밀러(Victor Miller)이다. 타원 곡선 암호는 타원 곡선이라는 수학 곡선을 암호화에 이용한 기술을 말한다. 공개키 암호는 이용하는 수학 이론에 따라 소인수 분해(IFP)의 형과 이산 대수문제(DLP)의 형으로 분류되는데 타원 곡선은 이산 대수 문제에서도 타원 곡선의 이산 대수문제(EC DLP)의 형태라고 볼수 있다. 공개키 암호는 암호화하는 키와 해독하는 키가 서로 다른 암호 방식으로 한 개의 키를 공개하고 다른 키는 비밀로 하기 때문에 불특정 다수와의 암호 통신이나 전자 서명 등에서 사용된다. 지금까지 이 공개키 암호시스템에서는 RSA 암호가 그 대명사로서 자리를 지켜 왔는데 관련 기술 및 제품은 미국의 RSA 데이터시큐리티가 거의 독점적으로 공급하고 있다. 타원 곡선 암호는 이 RSA의 독점 체제를 무너뜨릴 가능성이 높은 것으로 평가받고 있다. 타원 곡선 암호가 부상하고 있는 것은 RSA보다 우수하다는 것이다. 예를 들면 키의 길이가 1024비트인 RSA암호와 동일한 안전성을 실현하는데 타원 곡선 암호는 키 길이가 160비트면 된다. 키 길이는 필요한 메모리 용량과 직결되는 문제로 IC카드, 휴대전화 등에 탑재하는 데는 짧을수록 유리하다. 또 RSA 암호의 단점으로 지적되는 전자 서명 속도도 대폭 향상된다. 이에 본 논문에서는 타원 곡선을 이용한 공개키 방식의 전자 서명의 알고리즘에 적용하는 방안을 제시하고자 하며, 타원 곡선을 사용함으로 얻을 수 있는 특징에 대해서 알아 보고자 한다.

본 논문의 구성은 2장에서는 타원 곡선에 대한 일반적인 사항에 대하여 논의 하고 3장에서는 타원 곡선을 이용하여 전자 서명 알고리즘을 제안하기 위해서 전자 서명에 대해서 논의 한다. 그리고 4장 에서는 제안하는 알고리즘을 소개하고자하며 마지막으로 5장에서는 문제점과 향후 연구 관련에 대해서 서술한다.

2. 타원 곡선

많은 다른 암호시스템은 대수학 그룹(algebraic group)사용이 필요시 되고 있지만, 타원 곡선 에서는 타원 곡선 그룹(elliptic curve group)을 사용한다. 그룹은 사용자가 정의한 수학 연산(custom-defined arithmetic operation)을 하는 엘리먼트들의 집합이다. 타원 곡선 그룹에서 이러한 특정한 연산은 기하학적으로 정의되어 있다.

필드 F_2^m의 엘리먼트들은 m-비트의 길이를 갖는다. F_2^m에서 연산

규칙은 polynomial representation과 optimal normal basis representation에 의해 정의 되어져 있다. F_{2^m}의 연산은 비트 단위로 수행하기 때문에 컴퓨터가 이러한 필드에서 연산 수행을 하는 것은 매우 효율적이다. 필드 F_{2^m}를 이용한 타원 곡선의 형태는 필드 F_{2^m}내의 엘리먼트 중에서 a,b를 선택함으로써 구할 수 있다(단, b는 0이 아니어야 한다). 그래서 타원 곡선 방정식은 다음과 같이 나타낼수가 있다

$$y^2 + xy = x^3 + ax^2 + b \quad (b \neq 0)$$

타원 곡선은 다음 곡선 방정식을 만족하는 모든 점(x,y)를 포함한다. 단, x, y는 필드 F_{2^m}내의 한 엘리먼트이어야 한다. F_{2^m}에 대한 타원 곡선 그룹은 다음 두가지로 구성되어 있다

1. 타원 곡선을 만족하는 모든 점
2. 무한 수 O

F_{2^m}에서 타원 곡선 그룹에서 점들의 개수는 한정되어 있으며 연산 중 반올림 에러(round off error)가 발생하지 않는다. 다음의 연산은 F_{2^m}에서의 대수학적 규칙에 의한 것이다.

타원 곡선에서의 연산은 서로 다른 두점에 대한 덧셈과 동일한 두 점의 덧셈이 있다. 타원 곡선 상의 점 $P=(x_P, y_P)$의 역수는 $-P=(x_P, x_P+y_P)$이다. 만일 P와 Q가 서로 다른 점이라면 P와 -Q도 서로 다른 점이다. 다음은 서로 다른 두점 P와 Q를 더하여 점 R을 구하는 공식이다

$$\begin{aligned}
&P + Q = R, \ (P=(x_P, y_P),\ Q=(x_Q, y_Q),\ R=(x_R, y_R)) \\
&s = (y_P + y_Q) / (x_P + x_Q) \\
&x_R = s^2 + s + x_P + x_Q + a \\
&y_R = s(x_P + x_R) + x_R + y_P
\end{aligned}$$

만약에 동일한 두점에서의 덧셈 공식은 다음과 같다.

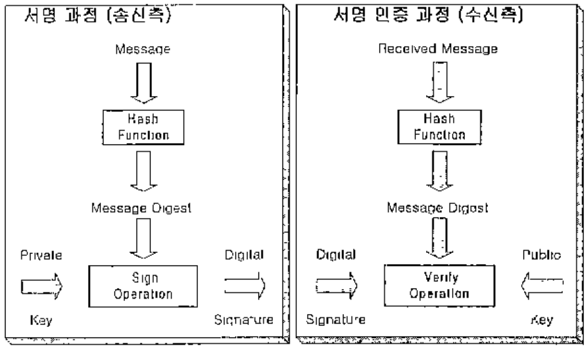
$$\begin{aligned}
&2P = R \ (P=(x_P, y_P),\ R=(x_R, y_R)) \\
&s = x_P + y_P / x_P \\
&x_R = s^2 + s + a \\
&y_R = x_P^2 + (s + 1)x_R
\end{aligned}$$

타원 곡선을 암호 시스템에 사용하는 것은 타원 곡선의 특징인 타원 곡선 이산 로그 문제(ECDLP)의 난이도를 적용함으로써 가능해진다. ECDLP는 다음과 같다. xP는 점 P를 x번 더하기 연산을 수행한 것이다. xP를 Q라 놓으면 Q=xP라 할 수 있는데, ECDLP는 P와 Q를 알고 있을 때 x의 값을 알아내기가 어렵다는 것이다. 타원 곡선 암호 시스템에서는 ECDLP의 난이도에 기본을 둔다. ECDLP는 IFP나 DLP보다 해결하기가 더욱 어렵다. 타원 곡선 암호 시스템에서는 이러한 장점을 이용하고 공개키 암호 시스템에 적용하고 있다. 타원 곡선 암호 시스템에서는 Q=xP에서 x를 개인키로 Q를 공개키로 사용하고 있다.

3. 전자 서명

문서의 전자적인 교환이 일반화 되면서 문서의 인위적인 변조나 여러 가지 결함에 의한 손실에 의한 문제점들이 발생한다. 그래서 전자 문서의 송신자와 수신자간에 문서 내용에 서명을 하는 방식이 필요하게 되었다. 그 해결 방안으로 암호 시스템을 이용하여 만든 전자 서명을 돌출 시켰다. 전자 서명이 갖추어야 할 조건은 첫째로, 공격자에 의해서 서명자의 서명이 변조되어 질수 없어야 하며 수신자는 서명된 메시지가 송신자가 서명한 것인지를 확인 할 수 있어야 한다. 그리고 서명자는 자신의 서명에 대해서 서명한 사실을 부인할 수 없어야 하고 수신자는 서명을 한후 그 서명에 대해서 변경이 불가능하여야 한다.

전자서명의 메카니즘을 살펴볼 때 적용하는 암호기법에 따라서 비밀키 암호기법을 이용하는 것과 공개키 암호기법을 이용하는 두가지 방법이 있다. 공개키 암호 기법을 사용한 전자 서명의 기본적인 메카니즘은 다음 그림과 같다



송신자측에서는 메시지를 해쉬함수에 넣어 일정 길이의 출력을 얻어내어 이것을 개인키를 사용하여 서명을 한후 메시지와 전자서명과 메시지를 수신자측에 보내게 된다. 수신자측에서는 송신자측으로부터 받은 메시지를 송신자가 서명 할 때 사용하였던 해쉬 함수를 적용하고 송신자에 대한 공개키를 사용하여 인증 처리를 하여 얻어낸 값이 송신자로부터 받은 전자 서명과 일치하게 되면 서명 인증을 한것이고 일치하지 않게 되면 송신자에 대한 서명 인증이 이루지지 않게 되는 것이다.

기존의 공개키 방식을 사용한 전자 서명인 ElGamal Signature Scheme은 이산 대수 문제(Discrete Logarithm Problem)에 기반으로한 전자 서명과 암호를 모두 사용하는 스킴이다. ElGamal의 전자 서명 방식을 살펴 보면 다음과 같다.

ElGamal에서 공개키와 개인키를 구하기 위해서 먼저 소수 p와 2개의 난수 g, x를 선택한다. g와 x는 소수 p보다는 작은 수이어야 한다. $a = g^x \pmod p$를 계산한다.

공개키는 y,g,p이고 개인키는 x이다. 메시지 M을 서명하기 위해서는 먼저 p-1과 서로 소인 난수 k를 선택하여 a=gk(mod p)를 계산한다. 확장 유클리드 알고리즘을 사용하여 b를 다음의 방정식에서 구한다

M = xa + kb(mod p-1)

전자 서명의 쌍은 a와 b가 된다. 난수 k는 보안을 유지하여야 한다. 전자 서명을 인증은 다음 공식을 사용하여 인증하게 된다

$y^a a^b \pmod p = g^M \pmod p$

두식이 만족을 하게되면 서명 인증이 되고 그렇지 않으면 인증이

되지 않는 방식을 제시하고 있다

4. 타원 곡선 전자 서명 알고리즘

본 논문에서는 이산 로그 문제에 기반한 전자 서명 알고리즘인 ElGamal 스킴을 타원 곡선에 적용하여 타원 곡선 전자 서명 구현 방안을 제시하고자 한다 ElGamal스킴에 대해서는 3절에서 간단하게 살펴 보았다 ElGamal 스킴은 DLP에 기반한 공개키 암호 방식이다 그래서 이를 타원 곡선에 적용하기가 용이하다 다음은 본 논문에서 제안한 ElGamal 전자 서명 알고리즘을 타원 곡선에 적용한 전자 서명 알고리즘이다

알고리즘은 서명을 생성하는 송신자의 측과 서명 인증을 하는 수신자 측으로 나눈다 송신자는 메시지 M을 일정한 키의 길이를 갖게 하기 위해 해쉬함수에 대입하여 m을 구한다 구간 [1 ,n−1]에서 난수 r을 선택하여 rP를 계산한다 난수 r을 선택할 때, r의 값은 통계적으로 유일하고 예측할 수 없게 정의 되어 있어야 한다 P는 타원 곡선 위의 한 점이다 그 결과의 x좌표 값을 a에 대입한다 그리고 a와 해쉬 함수에 의해 얻어진 m과 개인키 d를 사용하여 b = m − ad를 구한다 이렇게 구하여진 (a,b)가 서명이다 송신자는 메시지 M과 (a,b)를 수신자에게 보낸다 이에 수신자는 송신자로부터 받은 값을 가지고 서명에 대한 인증을 하게 된다. 수신자는 메시지 M을 해쉬 함수에 대입하여 m을 구한다 송신자로부터 넘겨 받은 (a, b)로 aQ + bP를 계산한다(Q는 송신자에 대한 공개키). 해쉬 함수에 의해 얻어진 m을 사용하여 mP를 계산하여 두 값을 비교하여 일치 하면 송신자에 대한 서명을 인증하게 되는 것이고 일치 하지 않으면 수신자는 송신자로부터 받은 메시지에 대한 서명 미 정상적인 것으로 간주하게 된다 모든 사람에게 공개 되어 있는 것은 타원 곡선 위의 P, Q의 점과 서명 (a,b), 메시지 M이나 제안한 알고리즘으로는 공격자는 이것만으로 서명의 변조가 불가능하게 된다

서명 생성

1. 메시지 M을 해쉬 함수에 넣어 m을 구한다
   $m = H(M)$,
2. 구간 [1, n−1]사이에서 난수 r을 구한다.
3. $(x_1, y_1) = rP$를 계산한다
4. $a = x_1$이라 한다
5. $b = m - ad \pmod n$을 계산한다
6. (a,b)가 서명이 된다
7. M과 서명(a,b)를 수신자에게 보낸다

서명 인증

1. 송신자로부터 M과 서명 (a,b)를 받는다
2. 메시지 M을 해쉬 함수에 넣어 m을 구한다
   $m = H(M)$
3. $R = aQ + bP$를 계산한다
4. $R' = mP$를 계산한다
5. R과 R'을 비교하여 서명 인증을 한다.

타원 곡선 알고리즘을 사용하여 전자 서명을 구현함으로써 획득할 수 있는 장점으로는 기존의 공개키 암호 방식에 비해 단위 비트당 안전도가 높으며 그 만큼 키 크기가 작아짐으로써 구현시 서명의 속도가 빠르다 단위 비트가 짧고 속도가 빠름으로 해서 기존의 공개키 방식에서는 적용하기가 힘든 스마트 카드나 휴대 통신기 처럼 작은 하드웨어에 적용하기가 쉬워지며 계산량이 작고 저장에 유리하다는 장점들을 가지고 있다.

5. 결론

본 논문에서는 타원 곡선을 이용하여 기존의 공개키 암호 방식을 타원 곡선에 적용하여 새로운 공개키 방식의 전자 서명 알고리즘을 구현하는 방안을 제시하였다. 타원 곡선 알고리즘을 사용하여 공개키 암호 시스템을 개발함에 있어서 얻을 수 있는 장점들은 타원 곡선 암호 방식은 기존의 공개키 방식보다 더욱 어려운 ECDLP방식을 사용한다는데 있으며 RSA에서 사용하는 연산은 주로 곱하기 연산이다 그럼으로 곱하기가 연속으로 사용되는 만큼 수행 시간이 길어지나, 타원 곡선 알고리즘에서의 주요 연산은 덧셈이기 때문에 수행 시간에 있어서도 많은 절약을 할 수 있다. 타원 곡선 알고리즘이 위에서 언급한 장점이 있지만 타원 곡선 알고리즘은 RSA 암호 시스템 보다 이론적으로나 기술적으로 완벽한 검증을 받지 못하고 있다 그러므로 타원 곡선 암호 시스템의 공격에 대한 안정성 검증에 대한 연구가 앞으로 진행되어야 할것이다

참고 문헌

[1] T. ElGamal, "A public key cryptosystem and a signature scheme based on the discrete logarithm", IEEE Trans. on Information Theory, Vol. 31, No 4,

[2] V Miller, "Uses of elliptic curves in cryptography", Advances in Cryptology CRYPTO '85, Lecture Notes in Computer Science, volume 218. Springer Verlog, pages 417-429, 1986

[3] Bruce Schneier, "Applied Cryptography", Wiley Publishers

[4] K.Nyberg and R.Rueppel, "Message recovery for signature schemes based on the discrete logarithm problem", Designs, Codes and Cryptography, volume 7, pages 61-81, 1996

[5] N Smart, Announcement of an attack on the ECDLP for anomalouse elliptic curve, 1997.

[6] Alfred Menezes, Minghua Qu and Scott Vanstone, "Elliptic Cruve Systems", IEEE P1363, Part 4, 1995

[7] N Koblitz, "Ellipic curve cryptosystems", Mathematics of Computation, 1987

[8] A Menezes, "Elliptic Curve Public Key Cryptosystems", Kluwer Academic Publishers, 1993

[9] C.P Schnorr, "Efficient signature generation by smart cards", Journal of Cryptology, volume 4 pages 161-174, 1991

[10] G Agnew, R Mullin, I. Onyszchuk and S Vanstone "An implementation for a fast public-key cryptosystem", Journal of Cryptology, pages 63-79, 1991