안전한 무선 인터넷을 위한 타원 곡선 알고리즘을 사용한 신뢰된 파티가 없는 쓰레시홀드 암호시스템

성순화
충남대학교 전자전파정보통신
shsung@cnu.ac.kr

Threshold Cryptosystem without a Trusted Party using Elliptic Curve Algorithm for Secure Wireless Internet

SoonHwa Sung
Dept. of Electronics, Radio, and Communications Engineering, Chungnam National University

요 약

무선 인터넷 통신은 유선 인터넷 통신보다 더욱 정보 노출이 쉬운 상태여서 강도 높은 보안 솔루션이 요구된다. 본 논문에서는 무선 인터넷의 암호 시스템을 위해, 키 길이가 짧아 처리 속도가 빠른 타원 곡선 알고리즘을 사용한 신뢰된 파티가 없는 쓰레시홀드 암호시스템을 제안한다. 따라서 제안한 시스템은 타원 곡선 알고리즘 사용으로 휴대 단말기 용량 한계에 부딪혔던 WPKI(Wireless Public Key Infrastructure) 서비스를 개선할 수 있으며, 신뢰된 파티를 보장할 수 없는 무선 인터넷 통신에서 안전한 그룹 통신을 할 수 있게 된다. 또한 제안한 시스템은 다양한 타원 곡선을 활용할 수 있는 타원 곡선 암호시스템 장점으로 다양한 암호시스템 설계가 가능하다는 것이 증명되었다.

1. 서 론

무선 인터넷 인프라 구축에 힘입어 각종 모바일 기기를 통한 정보교류나 전자상거래가 활발해지게 됐다. 이동통신 단말기를 이용해 인터넷 쇼핑을 하거나 인터넷 뱅킹을 할 수 있는 인프라 구축에도 불구하고 모바일 전자상거래가 대중화되려면 여러 가지 과제를 해결해야 한다.

이동통신 단말기를 통해 보내는 계좌번호나 비밀번호 등 개인 신상명세를 인증되지 않은 누군가에 의해 나쁜 의도로 사용된다면 어떻게 할 것인가(confidentiality). 또 주문을 해 놓고도 주문하지 않았다고 발뺌하는 무선 네티즌에 대해서는 어떻게 할 것(non repudiation)이며 메시지의 내용이 누군가에 의해서 위변조된다면 어떻게 할 것인가(integrity). 이같은 문제들은 모바일 전자상거래 시대를 여는 데 있어 핵심적인 사안들이다. 특히 무선 환경은 유선보다 더욱 정보가 노출되기 쉬운 상황이어서 강도 높은 보안 솔루션이 요구된다. 이같은 보안 솔루션으로 최근 타원곡선 알고리즘을 이용한 암호시스템이 주목을 받고 있다.

타원곡선 알고리즘은 RSA, ElGmal, DSA 등 공개키 암호시스템보다 키의 길이가 짧아 처리 속도가 빠르며 성능 또한 우수하다. 즉 RSA 1024 비트 키와 타원곡선 알고리즘 160 비트 키를 갖는 암호 방식이 대등한 안전도를 가진다. 또한 RSA는 주요 연산이 곱셈인 반면 타원곡선 알고리즘은 덧셈이기 때문에 계산이 훨씬 빠르다[1].

타원곡선 알고리즘은 공개키 암호의 특징인 암호화 연산 방향의 계산이 쉬운 것에 비해 복호화를 위한 역방향 연산이 어려운 것에 착안한 타원곡선 이산대수 문제에 기반을 두고 있다. 또 암호화의 기반이 되는 타원곡선을 무한히 생성할 수 있어 주기적인 암호 변경과 빠른 암호키 생성이 가능한 타원곡선 알고리즘 개발은 그동안 휴대용 단말기의 용량으로 한계에 부딪혔던 WPKI(Wireless Public Key Infrastructure) 상용서비스의 대중화를 앞당길 수 있는 촉진제가 될 것으로 기대된다.

한편 유무선을 통한 정보 교환은 이제 개인 대 개인을 떠나 개인과 그룹, 그룹과 그룹간의 정보 교환 시대이다. 특히 사용자들이 언제 어디서나 정보를 제공 받고 제공 하기를 원하는 현실에서는 그룹 간의 안전한 정보 교환이 필수가 되고 있다. 이러한 그룹을 기반으로 하는 암호시스템 중 일정한 그룹 구성원들이 모여야만 비밀키를 복구하여 암호문을 복호하는 쓰레시홀드 암호시스템이 사용되고 있다. 그러나 이러한 쓰레시홀드 암호시스템은 신뢰된 파티가 있어 일정한 그룹 구성원들의 비밀 정보를 모아 비밀키를 만들어 원문을 구하여 수신자에게 전달한다. 무선 인터넷 환경에서는 이러한 신뢰된 파티를 보장할 수 없으므로 안전한 정보 교환을 위해 신뢰된 파티가 없는 쓰레시홀드 암호시스템이 필요하다.

따라서 무선 인터넷의 WPKI 서비스를 제공하기 위한 단말기의 제한된 용량과 무선 인터넷 환경에 알맞은 개

인과 그룹, 그룹과 그룹간의 정보를 안전하게 교환할 수 있는 암호 시스템이 절실하다. 본 논문에서는 무선 인터넷의 WPKI 서비스를 위해 타원곡선 알고리즘을 도입하여 신뢰된 파티가 없는 쓰레시홀드 암호시스템을 제안한다. 본 논문 구성은 2장 타원곡선 알고리즘, 3장 쓰레시홀드 암호시스템, 4장 신뢰된 파티가 없는 쓰레시홀드 암호시스템, 5장 타원곡선 알고리즘을 사용한 신뢰된 파티가 없는 쓰레시홀드 암호시스템, 6장 결론으로 이루어진다.

2. 타원곡선 알고리즘

2.1 타원곡선 개요

체 F 상의 타원곡선(elliptic curve)은 $y^2 + a_1*x*y + a_2*y = x^3 + a_3*x^2 + a_4*x + a_5$, 단, $a_1,a_2,a_3,a_4,a_5 \in F$ 형태의 방정식으로 주어진 곡선을 말한다[2].

(I) 체 F의 표수(characteristic)가 2와 3이 아닌 경우

체의 표수(characteristic) p 가 2 와 3 이 아닐 때는, 위 타원곡선을 적당히 이동을 하면 $y^2 = x^3 + a*x + b$ 형태로 나온다. 이 때 암호론에서 사용하는 곡선은 변형된 타원곡선이 smooth 인 경우, 즉 우변의 방정식이 중근($4*a^3+27*b^2 \equiv 0 \pmod p$ 이면 중근존재)을 갖지 않을 경우에, 변형된 타원곡선 상의 점과 무한원점(0)(항등원)으로 구성된 점들 사이에 적당한 덧셈연산을 정의하면 가환군이 된다는 것을 이용한 암호방법이다. 곡선상의 점 $P=(x_1, y_1)$, $Q=(x_2, y_2)$의 덧셈연산은 아래 그림과 같이 두 점 P,Q 를 지나는 직선과 타원곡선과 만나는 제 3 의 교점(x,y)을 x 축에 관해 대칭한 점(x, -y)을 $P+Q=(x_3, y_3)$ 로 정의한다. 계산을 해보면 아래(1)(2)와 같다. 제 3 의 교점이 없으면, 즉 직선이 y 축과 평행하면 (3)과 같이 정의한다.

단, $P + Q = (x_1, y_1) + (x_2, y_2) = (x_3, y_3)$

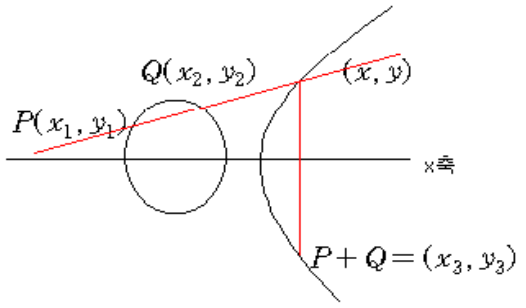

그림 1

(II) 체 F의 표수(characteristic)가 2인 경우

이 경우의 체의 원소수는 2^p (단 p 는 양의 정수)인 유한체가 된다.

(III) 체 F의 표수(characteristic)가 3인 경우

2.2 타원곡선 암호알고리즘

타원곡선 암호시스템[3,4,5]은 유한체의 곱셈군에 근거한 시스템으로서 다음의 장점을 가진다. ① 군(Group)을 제공할 수 있는 다양한 타원곡선을 활용할 수 있어 다양한 암호시스템 설계가 용이하다. ② (초특이 타원곡선을 피하면)이 군에서의 subexponential time algorithms 이 존재하지 않는다. 즉, 안전한 암호시스템을 설계하는 것이 용이하다. ③ 타원곡선 암호시스템은 존재하는 다른 공개키 스킴과 같은 안전도를 제공하는 데에 더 작은 키길이를 가지고 가능하다(예, RSA 1024 비트 키와 ECC 160 비트 키를 갖는 암호시스템은 같은 안전도를 갖는다). ④ 타원곡선에서의 더하기 연산은 유한체에서의 연산을 포함하므로, H/W 와 S/W 로 구현하기가 용이하다. 더욱이 이 군에서의 이산대수 문제는 특히, 같은 크기의 유한체에서의 이산대수 문제보다 훨씬 어렵다고 알려져 있다.

다음은 타원곡선을 이용한 ElGamal 암호알고리즘[6]이다.

1. 수신자와 송신자는 타원곡선상 점을 누구나 구할 수 있도록 p, a, b 를 공개한다.
2. 받는 사람은 비밀키 k(정수)와 타원곡선상의 한 점 G 를 선정하여 (비밀키 k)*(공개키 G) = kG 를 계산하여 kG를 공개키로 공개한다.
3. 보내는 사람은 평문 M(타원곡선상의 점)과 암호화시 사용할 임의수 c(정수)를 선정한다. 그리고, c 와 공개키 kG를 이용하여 암호문 (C_1, C_2), 단,

C_1 = (임의수 c)*(공개키 G)= cG

C_2 = [(임의수 c)*(비밀키 k)*(공개키 G)] + (평문 M) = ckG + M 를 수신자에게 보낸다.

4. 복호화는 암호문(C_1,C_2)를 받아 아래와 같이

C_2 - (비밀키 k)*C_1 = [ckG + M] - k(cG) = M(평문)

으로 계산하면 평문을 얻을 수 있다.

이 알고리즘을 이용하여 간단한 예를 보기로 한다.

받는 사람의 비밀키 k (정수)를 "7"로 하고 타원곡선상의 점에서 한 개의 좌표(공개키 G)를 골라 공개키(x_1좌표, y_1좌표)의 값을 "(3,5)"로 한다.

보내는 사람의 암호화시 사용할 임의수 c (정수)를 "11"로 하고, 평문 M (x_1 좌표, y_1 좌표)의 값은 "(2,9)"로 한다.

따라서 받는 사람의 공개키인 kG = (비밀키 k)*(공개키 G)의 결과는 "7(3,5)=(3,5)"이며, 암호문 C_1 = cG = (임의수 c)*(공개키 G)의 좌표는 "11(3,5)=(3,5)"

암호문 C_2 = ckG + M = [(임의수 c)*(비밀키 k)*(공개키 G)] + (평문 M)의 좌표는 "[11*7*(3,5)] + (2,9) = (3,5) + (2,9) = (0,0)"이다.

복호화는 암호문(C_1,C_2)를 받아 C_2 - kC_1 = [ckG + M] - kcG = (평문 M)으로 계산하면 " (0,0) - 7(3,5) = (2,9)"가 된다.

실수 타원곡선군에서 원소들을 계산하는 것은 사실 매우 느리고 반올림 오차 때문에 정확하지도 않다. 암호에서는 빠르고 정확한 연산이 필수이므로 실제 암호에서는 이러한 조건을 만족하는 유한체 F_p 나 F_{2^m} 위에서의 타원곡선군을 사용한다.

3. 쓰레시홀드 암호시스템

(t,n) 쓰레시홀드 크립토그래피는 샤미러[7]가 비밀 공유 기법을 제안한 후 발전하기 시작한 결함 허용 방법에서 암호시스템 영향력을 분산시킨 암호이다 [8]. 공개키와 비밀키 쌍을 생성하여 공개키는 한 개, 비밀키는 n 개의 노드로 이루어진 그룹에 의해 비밀 정보가 일부분씩 공유된다. 비밀키는 쓰레시홀드값 t 이하의 노드는 원문을 복구하지 못하고 t+1 이상의 노드가 모여야만 비밀키를 얻을 수 있는 암호시스템이다. 이 시스템에서 송신자가 메시지를 수신자에게 전송하고자 할 경우, n 그룹의 공개키를 가지고 원문을 암호화하여 전송한다. 수신자는 각자가 가지고 있는 비밀 정보를 믿을 수 있는 제 3 노드(trusted party)에게 안전한 채널을 통해 전송한다. 제 3 노드는 t+1 이상의 비밀 정보를 모아서 비밀키를 만들어 원문을 복호화하여 각각의 수신자에게 원문을 전송한다. 여기서 신뢰된 제 3 노드가 있어야만 암호화된 데이터의 원문을 구할 수 있다. 이러한 단점을 보안하기 위해 신뢰된 제 3 노드가 없는 (t,n) 쓰레시홀드 암호시스템 [9]를 제안하였다. 따라서 본 논문에서는 키 길이가 짧고 처리 속도가 빠른 타원곡선

암호알고리즘을 사용하여 무선 인터넷 환경에 적합한 암호시스템인 신뢰된 제 3 노드가 없는 (t,n) 쓰레시홀드 암호시스템을 제안한다.

4. 신뢰된 파티가 없는 쓰레시홀드 암호시스템

신뢰된 파티가 없는 쓰레시홀드 암호시스템은 신뢰된 파티를 피할 수 있는 방법과 그룹의 각 구성원들이 비밀 공유가 정확한지 검증할 수 있는 비밀키를 어떻게 공유할 것인가를 보인다.

키 선택을 위해 다음을 표기한다.

- G_q : the unique subgroup of Z_p^* of order q
- g : a generator of G_q
- p,q: large primes (q divides $p-1$)
- $C(m,r)$:commitment to $m \in \{0,1\}^*$ using the random string r

그룹 $P_1,\ldots,P_n$ 의 구성원 n이 비밀키 $x=\log_g h$ 를 얻기 위해 공개값 (p,q,g,h : $g,h \in G_q$)를 선택하여 소수 p,q 와 g 에 동의한다. 고정 변수 k ($1 \le k \le n$)인 k 구성원은 비밀키를 얻기 위해 서로 협력해야 한다.
키 선택 순서는 다음과 같다.

1. P_i 는 임의로 $x_i \in Z_q$ 를 선택하여 $h_i = g^{x_i}$를 계산한다. 그리고 임의 스트링 r_i를 선택하여 $C_i = C(h_i, r_i)$를 모든 구성원에게 보낸다.
2. 이때, P_i 는 C_i 를 공개한다.
3. 공개키 h 는 $h=\prod_{i=1}^{n} h_i$ 로 계산된다.

모든 구성원들은 공개키를 알지만 그들이 서로 협력하지 않으면 비밀키 $x=\sum_{i=1}^{n} x_i$ 를 얻을 수 없다. 또한 P_i 가 임의로 x_i 를 선택한다면 비밀키의 분산을 구별할 수가 없다.
따라서 k 구성원이 비밀키 x가 어떻게 분배되는지를 [10]에서 검증 가능한 비밀 공유를 확장한 방안을 제안한다.
P_i 는 $h_1,\cdots, h_n$ 가 공개된 상태에서 x_i 를 다음과 같이 분배한다.

1. P_i 는 $f_i(0) = x$ 를 만족하는 최대 차수 $k-1$의 임의의 다항식 $f_i(z) \in Z_q(z)$를 선택한다.

   $f_i(z) = f_{i0} + f_{i1} z + \cdots + f_{i,k-1} z^{k-1}$ (where $f_{i0} = x_i$)

2. P_i 는 $j=0,\cdots,k-1$에 대하여 $F_{ij} = g^{f_{ij}}$를 계산하여 모든 구성원들에게 $(F_{ij})_{j=1,\cdots,k-1}$ ($F_{i0}=h_i$) 를 보낸다.
3. 모든 구성원들이 $k-1$ 값을 보낼 때, P_i 는 $j=1,\cdots,n$ 에 대하여 비밀스럽게 $s_{ij} = f_i(j)$와 s_{ij} 에 대한 서명을 P_j 에게 보낸다.
4. P_i 는 P_j (s_{ji})가 다음을 검증함으로써 미리 공표된 값과 일치한다는 것을 검증한다.

$$g^{s_{ji}} = \prod_{l=0}^{k-1} F_{jl}^{i^l}$$

   만약 이것이 실패이면, P_i 는 모든 구성원에게 에러가 발생했다고 전달하고 s_{ij} 와 서명을 공표하고 중단한다.

5. P_i 는 3 번에서 $s_i = \sum_{j=1}^{n} s_{ji}$ 로 받은 모든 공유의 합으로 x 의 공유를 계산한 후, P_i 는 h를 서명한다.

모든 구성원들이 h 를 서명할 때, 키 인증 센터는 서명을 검증하여 그 서명이 정확하면 키 인증 센터는 h가 그 그룹의 공개키라는 인증서를 만든다.
f 가 Z_q 의 다항식 $f(z) = f_1(z) + \cdots + f_n(z)$ 이라고 하면, $s_i = f(i)$ ($i=1,\cdots,n$)를 구성한 s_i 는 $f(0)=x$ 의 공유이다[7]. 따라서 x 의 각 공유 s_i에 대하여 σ_i를 g^{s_i} 로 표시하면 P_i 가 정확한 공유를 받는다면 각 P_j ($j \neq i$)는 다음과 같이 σ_i 를 계산할 수 있다.

$$\sigma_i = \prod_{j=1}^{n} g^{s_{ji}} = \prod_{j=1}^{n} \left(h_j \prod_{l=1}^{k-1} F_{jl}^{i^l} \right)$$

5. 타원곡선 알고리즘을 사용한 신뢰된 파티가 없는 쓰레시홀드 암호시스템

본 논문에서 제안한 신뢰된 파티가 없는 쓰레시홀드 암호시스템은 타원곡선 알고리즘을 사용한다.

5.1 타원곡선 알고리즘에서의 키 생성 및 암복호화 단계

키 생성 단계

1) 공통 변수 (q, a, b, Q, ℓ, t)를 미리 정해 공개
2) GF(q)상에서 정의 되어진 타원 곡선 선정
   Eq(a,b) : $y^2 = x^3 + ax + b$
3) 타원곡석상의 점 Q의 위수 ℓ가 커다란 소인수 t를 가지는 것으로 함
4) 이용자는 x $\in_U Z_\ell$ 를 정하고 Eq(a,b)상에서 키 Y=xQ를 계산

암호화 및 복호화

- 공개키 : Y
- 비밀키 : X
- 암호화 : m : 평문, r$\in_U Z_\ell$: 난수
  $c_1 = rQ$, $c_2 = rY + m$
- 복호화 : $m = c_2 - xc_1$

이를 바탕으로 신뢰된 파티가 없는 쓰레시홀드 암호 시스템에서의 키 생성과 암호화 및 복호화를 제안한다.

5.2 타원곡선 알고리즘을 사용한 신뢰된 파티가 없는 쓰레시홀드 암호시스템

키 선택을 위해 다음을 표기한다.

- GF(q): 정의 되어진 타원 곡선
- g : a generator of GF(q)
- p,q: large primes (q divides $p-1$)
- $C(m,r)$:commitment to $m \in \{0,1\}^*$ using the random string r

그룹 $P_1,\ldots,P_n$ 의 구성원 n이 비밀키 $x=\log_g Y$ 를 얻기 위해 공개값 (q, a, b, Q, ℓ, t)를 선택하여 소수 p,q 와 g 에 동의한다. 고정 변수 k ($1 \le k \le n$)인 k 구성원은 비밀키를 얻기 위해 서로 협력해야 한다.
키 선택 순서는 다음과 같다.

1. P_i 는 임의로 $x_i \in$ GF(q)를 선택하여 $Y_i = g^{x_i}$를 계산한다. 그리고 임의 스트링 r_i를 선택하여 $C_i = C(Y_i, r_i)$를 모든 구성원에게 보낸다.
2. 이때, P_i 는 C_i 를 공개한다.
3. 공개키 Y 는 $Y = \prod_{i=1}^{n} Y_i$ 로 계산된다.

모든 구성원들은 공개키를 알지만 그들이 서로 협력하지 않으면 비밀키 $x = \sum_{i=1}^{n} x_i$ 를 얻을 수 없다. 또한 P_i 가 임의로 x_i 를 선택한다면 비밀키의 분산을 구별할 수가 없으므로 다음과 같은 방법을 제안하여 k 구성원이 비밀키 x가 어떻게 분배되는지 알 수 있다.
P_i 는 $Y_1,\cdots, Y_n$ 가 공개된 상태에서 x_i 를 다음과 같이 분배한다.

1. P_i 는 $f_i(0) = x$ 를 만족하는 최대 차수 $k-1$의 임의의 다항식 $f_i(z) \in Z_q(z)$를 선택한다.
   $f_i(z) = f_{i0} + f_{i1} z + \cdots + f_{i,k-1} z^{k-1}$ (where $f_{i0} = x_i$)
2. P_i 는 $j=0,\cdots,k-1$에 대하여 $F_{ij} = g^{f_{ij}}$를 계산하여 모든 구성원들에게 $(F_{ij})_{j=1,\cdots,k-1}$ ($F_{i0} = h_i$) 를 보낸다.
3. 모든 구성원들이 $k-1$ 값을 보낼 때, P_i 는 $j=1,\cdots,n$ 에 대하여 비밀스럽게 $s_{ij} = f_i(j)$와 s_{ij} 에 대한 서명을 P_j 에게 보낸다.
4. P_i 는 P_j (s_{ji})가 다음을 검증함으로써 미리 공표된 값과 일치한다는 것을 검증한다.

$$g^{s_{ji}} = \prod_{l=0}^{k-1} F_{jl}^{il}$$

만약 이것이 실패이면, P_i 는 모든 구성원에게 에러가 발생했다고 전달하고 s_{ij} 와 서명을 공표하고 중단한다.

5. P_i 는 3 번에서 $s_i = \sum_{j=1}^{n} s_{ji}$ 로 받은 모든 공유의 합으로 x 의 공유를 계산한 후, P_i 는 Y를 서명한다.

모든 구성원들이 Y 를 서명할 때, 키 인증 센터는 서명을 검증하여 그 서명이 정확하면 키 인증 센터는 Y가 그 그룹의 공개키라는 인증서를 만든다.

f 가 Z_q 의 다항식 $f(z) = f_1(z) + \cdots + f_n(z)$ 이라고 하면, $s_i = f(i)$ ($i=1,\cdots,n$)를 구성한 s_i 는 $f(0) = x$ 의 공유이다. 따라서 x 의 각 공유 s_i 에 대하여 σ_i 를 g^{s_i} 로 표시하면 P_i 가 정확한 공유를 받는다면 각 P_j ($j \neq i$)는 다음과 같이 σ_i를 계산할 수 있다.

$$\sigma_i = \prod_{j=1}^{n} g^{s_{ji}} = \prod_{j=1}^{n} \left(h_j \prod_{l=1}^{k-1} F_{jl}^{il} \right)$$

제안한 쓰레시홀드 암호시스템은 신뢰된 파티가 없이 비밀키가 분배된 그룹 구성원들의 비밀 정보를 모아 비밀키 X 를 생성할 수 있다. 그러므로 타원곡선 암호 알고리즘을 사용하여 암호화 $c_1 = rP$, $c_2 = rY + m$ (m : 평문, r$\in_U Z_\ell$: 난수)에서 원문 $m = c_2 - xc_1$ 를 구할 수 있다.

6. 결론

본 논문에서 제안한 암호시스템은 무선 인터넷 환경에서의 그룹 대 그룹의 안전한 통신을 위해 필요한 문제 해결을 제안하였다. 현재 그룹을 위한 암호시스템으로 많이 사용되고 있는 쓰레시홀드 암호시스템의 단점을 해결하고, 무선 환경에서의 휴대용 단말기 용량의 한계를 해결하기 위한 WPKI 서비스의 대중화를 위해 타원곡선 알고리즘을 사용하여 RSA 보다 짧은 키를 가지고도 대등한 안전도와 처리 속도를 향상시킬 수 있도록 하였다. 쓰레시홀드 암호시스템의 단점은 각 그룹 구성원들의 키를 분배하여 일정 구성원들의 분배 키가 모이면 비밀키를 구성할 수 있는데 이때 신뢰된 파티가 있어야만 일정 구성원들의 분배 키를 모을 수 있다. 따라서 무선 인터넷 특성상 신뢰된 파티가 없는 쓰레시홀드 암호시스템이 필요함으로 이를 해결하였고, 빠르게 발전하고 있는 무선 환경의 이동통신을 위해 보다 신속하고 보다 안전한 성능의 암호시스템을 위해 타원곡선 알고리즘을 사용하였다.

신뢰된 파티가 없는 쓰레시홀드 암호시스템에서 타원곡선 알고리즘 사용은 안전한 무선 인터넷을 위한 필요한 이슈로 자리잡을 것이다. 그러나 제안한 암호시스템은 의도된 공격자에 대하여 얼마만큼 안전도가 있는지 연구되어야 한다.

참고문헌

[1]C.G.Pollman, "XML Pool Encryption", XMLSEC02, USA, pp.1-9,22, Nov.2002.

[2]J.H. Cheon and S.T.Chee, "Elliptic Curves and Resilient Functions", ICISC 2000, LNCS 2015, pp.64-72, Springer-Verlag,2001.

[3]R. L. Rivest, A. Shamir, and L.M.Adleman, "A Method for Obtaining Digital Signatures and Public-key Cryptosystems", Communications of the ACM,vol.12, no.2, pp.120-126.

[4]"IEEE pp.1393: Standard Specification for Public Key Cryptography", http://standards.ieee.org/reading/ieee/std/busarch/1363-2000.pdf, 2001.

[5]J. Guajardo and C. Paar, "Efficient Algorithms for Elliptic Curve Cryptosystems", Advances in Cryptology-CRYPTO' 97, B.S Kaliski, ed., pp.342-356, 1997.

[6]T. ElGamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithm", IEEE Transaction on Information Theory, 31, pp. 469-472, 1985.

[7]A. Shamir, "How to share a secret", Commun. ACM, 22, pp.612-613, November 1979.

[8]Y. Desmedt, Threshold Cryptography. European Trans. on Telecommunications, 5(4):449-457, 1994.

[9]Torben Pryds Pedersen, "A Threshold Cryptosystem without a Trusted Party", pp.522-526, Springer-Verlag, 1998.

[10]I. Ingemarsson and G. J. Simmons., "A protocol to set up shared secret schemes without the assistance of a mutually trusted party", In Advances in Cryptology-proceedings of EUROCRYPT 90, Lecture Notes in Computer Science, pp.266-282, Springer-Verlag, 1991