通信情報保護學會誌
第7卷 第4號. 1997. 12

타원 곡선을 이용한 암호 시스템

Cryptosystems Using the Elliptic Curve

양 대 헌*, 송 주 석*

요 약

본 논문에서는 최근 주목받고 있는 타원 곡선을 이용한 암호 시스템에대해 고찰해본다. 타원 곡선을 이용한 암호 시스템의 장점 및 이를 이용하여 구현한 여러가지 시스템에 대해 살펴보고, 또한 타원 곡선으로의 평문 imbedding 방법을 제시해 본다.

1. 서 론

1976년 Diffie와 Hellman에의해 공개키 암호 시스템이 제안된 이래 많은 종류의 공개키 암호 시스템이 개발 되었다[1,12]. 대표적인 공개키 암호 시스템으로 RSA, Rabin, ElGamal, Lattice 에 기반한 암호시스템 등이 있으며, 이들은 각각 소인수 분해 문제, 이산 대수 문제, CVP(Closest Vector Problem)등에 안전성을 기반하고 있다[4, 6, 7]. 이런 공개키 암호 시스템들은 매우 유용한 장점들이 있는데, 기존의 대칭키 암호 시스템이 가지는 키 분배 문제를 없앴다는 점, 그리고 디지탈 서명의 개념을 등장 시켰다는 점이다. 또한 다양한 종류의 프로토콜, 예를 들어 전자 화폐, 사용자 인증 프로토콜 등이 공개키 암호 시스템을 기반으로 설계되었다.

공개키 암호 시스템이 가지는 많은 장점에도 불구하고 현재까지 널리 쓰이지 못하고 있는것은 지나치게 넓은 키 스페이스(key space)와 암호화/복호화에 소요되는 긴 시간 때문이다. 이와 별도로 대부분의 공개키 암호 시스템이 가지는 선택적 평문 공격에 대한 취약성이 있다. 이 부분을 보완하기 위해서 확률적 공개키 암호 시스템(Probabilistic Cryptosystem)이 제안 되었으며, 많은 연구가 이루어지고 있다. 공개키 암호 시스템이 가지는 이러한 단점은 스마트 카드처럼 아주 작은 용량의 컴퓨팅 파워와 제한된 양의 메모리를 갖는 디바이스에 적합하지 않고 이로 인해 공개키 암호 시스템의 사용 분야에 제약을 받게 되었다. 예를 들어 RSA의 경우 소인수 분해 공격에 대해 안전하기 위해서는 적어도 1024비트 정도의 블럭 크기를 요구하고 있으며, 이 경우 McCorquodale사의 MC68HC05SC49 칩에서는 서명의 생성에 약 5,600ms의 시간이 서명의

* 연세대학교 공과대학 컴퓨터과학과

확인에 168ms의 시간이 소요된다. Philips사의 스마트 카드 TRT DX에 사용되는 칩 P83C858의 경우 각각 2,000ms, 500ms의 시간이 소요된다. 또한 이산 대수 문제에 기반하고 있는 ElGamal 공개키 암호 시스템이나, Schnorr의 디지탈 서명 방법등에서도 소인수 분해 문제에 기반한 RSA와 비슷한 크기의 블럭을 필요로하며 많은 시간이 소요된다. 이것은 아직까지는 스마트 카드와 같은 디바이스에서는 현재의 공개키 알고리즘을 사용하기 매우 어렵다는것을 의미한다.

이런 공개키 암호시스템의 문제들은 타원 곡선을 이용한 공개키 암호 시스템에서 해결할 수 있다. 즉 타원 곡선위에서 그룹(Group)을 정의하고 이에대한 이산 대수 문제를 정의하므로써 새로운 종류의 일방향 함수를 정의할 수 있게되었다. 타원 곡선위에서의 이산대수 문제는 일반적인 그룹에서 정의되는 이산대수 문제보다는 더욱 어렵고 이에 따라 키 스페이스와 계산량의 문제를 어느정도 해결할 수 있게되었다. 타원 곡선을 이용한 공개키 암호 시스템은 Neal Koblitz와 V. S. Miller에 의해 독립적으로 고안 되었으며 본 논문에서는 타원곡선에 대한 소개와 이를 이용한 암호 시스템들을 살펴본다[9, 10]. 또한 암호 시스템의 설계에 필요한 평문 imbedding 방법을 제시한다. 타원 곡선은 Fermat의 마지막 conjecture를 증명하는데도 사용되었으며, 이산대수 문제나 소인수 문제에 대한 해를 찾는데도 이용되고 있다.

2. 타원 곡선

정의 $p>3$을 소수라 하자. Z_p위의 타원 곡선 $y^2=x^3+ax+b$는 다음의 congruence를 만족하는 $(x, y)\in Z_p*Z_p$의 집합이다.

$$y^2=x^3+ax+b \bmod p$$

여기서 $a, b\in Z_p$는 $4a^3+27b^2\neq 0(\bmod p)$인 상수이며 타원 곡선은 point at infinity라고 하는 원소 O를 포함한다.

타원 곡선 E는 적절한 연산을 적용하므로써 abelian group으로 구성할 수 있다. 일반적인 group을 정의 하는것처럼 타원 곡선위의 점에 대해 덧셈을 다음과 같이 정의 한다. 단 모든 연산은 Z_p 위에서 정의 된다.

$P=(x_1, y_1)$, $Q=(x_2, y_2)$ 을 E위의 점이라 하자.

만약 $x_2=x_1$이고 $y_2=-y_1$이라면 $P+Q=O$이다. 그렇지 않은 경우는 $P+Q=(x_3, y_3)$로 정의 되며 , x_3, y_3는 다음과 같이 정의 된다.

$$x_3=c^2-x_1-x_2$$
$$y_3=c(x_1-x_3)-y_1$$
$$c=(y_2-y_1)/(x_2-x_1), \text{ if } P\neq Q$$
$$c=(3x_1^2+a)/2y_1, \text{ if } P=Q$$

마지막으로, E위의 모든점 P에 대해서 $P+O=O+P=P$로 정의 된다.

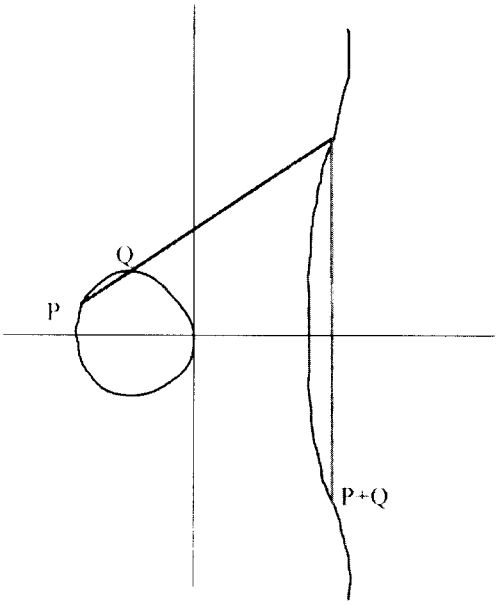


그림 1 타원 곡선

위와 같이 E위의 점에 대한 덧셈을 정의 하면 E는 덧셈에 대한 항등원 O를 갖는 abelian group이 됨을 알 수 있다. 덧셈의 정의에 따라 주어진 타원 곡선위의 점 P에 대해 배수 mP는 a^m을 필드위에서 계산하는것과 같은 복잡도로 구할 수 있다. 예를 들어 $11P=P+2(P+2(2P))$와 같이 평균 $1.5\log_2 m$step에 계산할 수 있다. 다음은 타원 곡선 E가 abelian group이 됨을 보이는 예이다.

E를 Z_{11}위에서의 타원 곡선 $y^2=x^3+x+6$이라 하자. 우선 타원 곡선의 order를 알아보자. 타원 곡선 E의 order는 타원 곡선을 이루고 있는 점들의 수와 같고, 타원 곡선위의 임의의 점 $m=(2, 7)$에 대해서 덧셈 연산을 적용하면 다음과 같은 결과를 얻는다.

$m=(2, 7)$, $2m=(5, 2)$, $3m=(8, 3)$, $4m=(10, 2)$, $5m=(3, 6)$, $6m=(7, 9)$, $7m=(7, 2)$, $8m=(3, 5)$, $9m=(10, 9)$, $10m=(8, 8)$,$11m=(5, 9)$, $12m=(2, 4)$

위의 12개의 점과 O를 합해서 13개의 점이 타원곡선을 이루고 있으므로 E의 order는 13이된다. 위의 점들은 Z_{11}에서 주어진 x좌표에 대해 $y^2=x^3+x+6 \pmod{11}$을 계산하면 쉽게 얻을 수 있다. 이때 y에 대한 quadratic residue를 구해야 하고 $p=11=3 \bmod 4$ 이므로 다음과 같이 square root를 쉽게 구할 수 있다.

$$c^{1/2}=\pm c^{(11+1)/4} \bmod 11=\pm c^3 \bmod 11$$

일반적으로 Z_p 위의 타원 곡선 E의 order $\#E$는 다음을 만족한다(Hasse의 정리).

$$p+1+2p^{1/2}<=\#E<=p+1+2p^{1/2}$$

정확한 타원곡선의 order는 시간 복잡도가 $O((\log p)^8)$인 Schoof의 알고리즘을 이용해서 구할 수 있다[8].

3. 타원 곡선을 이용한 암호 시스템

잘 알려진 $GF(q)$에서 정의되는 암호 시스템은 타원 곡선의 그룹 E위에서의 암호 시스템으로 변형 할 수 있다. 이 절에서는 타원 곡선에서의 이산대수문제를 정의하고 이를 기반으로 Massey-Omura의 암호시스템과 ElGamal의 암호시스템을 타원 곡선에서 다시 정의해 본다.

타원 곡선에서의 이산대수문제(Elliptic Curve Discrete Logarithm Problem) : $GF(q)$에서 정의된 타원 곡선 E와 두 점 $P, Q \in E$가 주어졌을 때, $Q=xP$를 만족하는 x를 찾는다.

타원 곡선 위의 Massey-Omura system : $q=p^n$이라 하고, E를 $GF(q)$에서 정의 되는 타원 곡선이라 하자. $N=\#E$이고 q, E, N은 공개된 값이다. 또한 m을 타원 곡선위의 한점 P_m으로 매핑하는 imbedding 함수가 있다고 가정한다.

사용자 A가 메시지 m을 사용자 B에게 보낸다고 가정하면, A는 $\gcd(c, N)=1$인 랜덤수 c를 선택하고 cP_m을 계산해서 B에게 전송한다. B는 A와 마찬가지로 d를 선택하고 $d(cP_m)$을 A에 전송한다. A는 $c'c=1 \bmod N$ 인 c'대해서 $c'(dcP_m)=dP_m$을 계산하고 이를 B에 전송한다. 마지막으로 B는 $d'd=1 \bmod N$인 d'를 선택해서 $d'(dP_m)=P_m$을 복원한다.

타원 곡선 위의 ElGamal system : Massey-Omura system과 같은 설정을 가지며, 다만 타원 곡선의 order는 계산할 필요가 없다. 타원 곡선의 order를 계산 할 필요가 없다는 사실은 실용적인 측면에서는 매우 중요한 사실이다. 왜냐하면 시간 복잡도가 $O((\log p)^8)$인 Schoof의 알고리즘이 존재 하지만 이것은 그다지 효율적이지 않기 때문이다. 이제 $G \in E$를 정해진 공개값이라 하자. 수신자 B는 랜덤수 a를 선택하고 aG를 공개키로 a는 비밀키로 한다. 이제 메시지를 전송하기 위해서 사용자 A는 랜덤수 k를 선택하고 $(kG, P_m+k(aG))$를 B에 전송한

다. 메시지를 복원하기 위해서 B는 첫번째 점 kG와 자신의 비밀키 a를 이용해서 $a(kG)=k(aG)$를 계산한 후, 두번째 점 $P_m+k(aG)$에서 뺀다.

타원곡선 위에서 Massey-Omura system과 ElGamal system을 공격하려면 앞에서 정의한 타원 곡선에서의 이산대수 문제를 풀어야 하며 이는 일반적인 $GF(p)$에서의 이산대수 문제보다 어렵다.

타원 곡선위에서의 암호 시스템은 대부분 앞에서 정의한 타원 곡선위에서의 이산 대수 문제에 안전성을 기반하고 있지만 RSA나 Rabin 공개키 암호시스템처럼 소인수 분해 문제의 어려움에 기반한 시스템도 제안되었다. [2]에서 Kenji Koyama등은 링 Z/nZ에서의 타원 곡선을 정의하고 RSA와 Rabin 스타일의 암호시스템을 제안하였다. 또한 [3]에서 Koyama는 앞의 암호시스템의 단점인 시간 복잡도를 어느정도 개선한 방안을 제시했다. 하지만 이렇게 타원 곡선위의 이산대수문제에 의존하지 않고 소인수 분해 문제에 의존한 암호 시스템은 원래 타원 곡선을 암호 시스템에 사용하게된 목적인 작은 블럭 크기의 장점을 가지지 않는다. 즉 [2, 3]에서 제안된 암호 시스템은 기존의 RSA보다 좋은 성능을 가지지 못하며, 소인수 분해 공격에 안전하기 위해서는 기존의 RSA와 같은 수준의 키 크기를 가져야 하기 때문이다. 따라서 타원 곡선위에서 암호시스템을 설계하는 경우에는 이산 대수문제에 기반한 시스템을 설계하는 것이 효율적이고, 타원 곡선의 장점을 충분히 살릴 수 있게된다. [2, 3]에서 제안된 시스템은 ring위에서 타원 곡선을 이용해 암호시스템을 설계했다는 의의 외에는 실용적인 가치가 없다.

이제 마지막으로 Menezes와 Vanstone이 설계한 암호 시스템을 살펴본다[11]. 이들이 설계한 암호 시스템은 타원 곡선 위의 한점으로 메시지를 imbedding 할 필요가 없다. 즉 타원 곡선의 임의의 점을 선택한 후 이들은 원래의 메시지를 마스킹(masking)하는데 사용하기 때문이다. 따라서 이 시스템은 메시지의 imbedding의 오버 헤드가 없으며 또한 메시지 확장율이 원래의 ElGamal 시스템 처럼 2가 된다. 이것은 앞에서 제시한 타원 곡선 위의 ElGamal 시스템의 메시지 확장 율이 4인것이 비교해서 매우 좋은 효율을 보인다. 다음은 이들이 설계한 암호시스템의 암호화/복호화 과정이다.

E를 Z_p에서 정의되는 타원 곡선이라 하고 E는 이 위에서 이산대수 문제가 풀기 어려운 (intractable) cyclic subgroup을 포함한다고 하자. $P=Z_p{}^*Z_p$, $C=E^*Z_p{}^*Z_p$라하고 다음을 정의 한다.

$K=\{(E, M, a, N):N=aM\}$, 여기서 $M\in E$이다. M과 N은 공개키가 되고 a가 비밀키가 된다. $K=(K, M, a, N)$에 대해 랜덤수 k를 생성하고 암호함수 eK는 다음과 같이 정의 한다.

$$e_K(x, k)=(y_0, y_1, y_2),$$

여기서

$$y_0=kM,$$
$$(c_1, c_2)=kN$$
$$y_1=c_1x_1 \bmod p$$
$$y_2=c_2x_2 \bmod p$$이다.

복호함수 d_K는 암호문 $y=(y_0, y_1, y_2)$에 대해 다음과 같이 정의 한다.

$$dK(y) = (y_1c_1^{-1} \bmod p, y_2c_2^{-1} \bmod p),$$
여기서 $ay_0=(c_1, c_2)$

4. 타원곡선으로의 평문 imbedding 방법

이 절에서는 평문을 타원 곡선위의 한점으로 imbedding 하는 간단한 알고리즘을 제시해

본다. 타원 곡선을 이용하여 암호 시스템을 구성하기 위해서는 평문을 타원 곡선 위의 한 점으로 imbedding하는데 derterministic하고 효율적인 방법이 필요하다. Neal Koblitz의 초기 타원 곡선을 이용한 암호 시스템에서는 단순히 랜덤 스트링을 패딩하여 imbedding하므로 효율적으로 평문과 타원 곡선 위의 점을 매핑할 수 없었다[9]. 이를 해결하기 위해 임의의 메시지에 대한 적절한 변형을 통해 imbedding하는 방법을 제안한다.

기본적인 아이디어는 타원 곡선의 x 좌표를 매핑했을때 y의 quadratic residiosity에 따라 메시지와 같게 매핑하거나 또는 $-x(\mathrm{mod}\ p)$로 매핑하는 것이다. 즉 $4n+3$ 형태의 p에 대해서 x가 quadratic non-residue라면 $-x$는 quadratic residue임을 이용한다. 이는 다음의 lemma에서 증명된다.

Lemma 1: p를 홀수인 소수, $a\in Zp$, $L(a/p)$을 Legendre symbol이라 하자.만약 $p=3 \bmod 4$라면, a, $-a$ 중의 하나는 quadratic residue이고 다른 하나는 quadratic non-residue가된다.

증명) $L(-a/p)=L(-1/p)L(a/p)$이고 $L(-1/p)=-1$므로, $L(-a/p)L(a/p)=-1$ 이다. Q.E.D

평문을 타원 곡선위의 한점으로 매핑하는 것은 x좌표는 메시지로, y좌표는 식 (1)을 만족하는 y값을 구하는것으로 생각할 수 있다. 하지만 이 경우에 메시지의 값에 따라 y가 quadratic non-residue 일 수 있으므로 imbedding이 불가능해진다. 다음은 적절한 메시지의 변형을 통해 imbedding하는 방법을 보여준다.

메시지 $m\in Z_n$ 이라 하자.

타원 곡선 E는 $y^2=x^3+ax$로 Z_p의 p는 $4k+3$ 형태의 소수로 $p>2n$인 최소값을 선택한다.

- Embedding

  $x=m$

  if m^3+am is quadratic residue then

  $y=(m^3+am)^{(p+1)/4} \bmod p$

  else

  $x=-m \bmod p$

  $y=((-m)^3+a(-m))^{(p+1)/4} \bmod p$

- Extracting

  if $x<p/2$ then

  $m=x$

  else

  $m=-x \bmod p$

위의 imbedding 방법에의해 항상 x^3+am이 quadratic residue임은 다음과 같이 증명할 수 있다.

1) 만약 m^3+am이 quadratic residue 라면

$y=(m^3+am)^{1/2}=(m^3+am)^{(p+1)/4} \bmod p$

을 만족하는 y가 존재한다.

2) m^3+am이 quadratic non-residue라면

Lemma 1에 의해 $-(m^3+am) \bmod p=(-m)^3+a(-m) \bmod p$는 quadratic residue가 된다. 따라서

$y=((-m)^3+a(-m))^{1/2}=((-\mathrm{m})^3+a(-m))^{(p+1)/4} \bmod p$

을 만족하는 y가 존재한다.

Q.E.D

이 imbedding 방법은 random string의 padding에 의한 algorithm의 non-determinism을 없애며, 짧은 시간에 imbedding 할 수 있다는 장점을 갖는다. 즉 y를 구하기 위한 square root 연산을 위해서 $(p+1)/4$ 의 지수 연산을 수행하면 된다. 간단하게 Square and multiply 알고리즘을 이용하면 평균 $1.5\log p$번의 곱셈으로 y를 구할 수 있다.

이 절에서 제시한 평문 imbedding 방법은

주로 타원 곡선위에서의 이산 대수 문제에 기반한 암호 시스템에 적용할 수 있지만, 이 외에도 3절에서 언급한 ring에서의 암호 시스템에도 간단하게 적용할 수 있다.

7. 결 론

본 논문에서는 다음 세대의 공개키 암호 시스템으로 좋은 성질을 가지고 있는 타원 곡선과 타원 곡선을 이용한 암호 시스템에 대해서 살펴보았다. 또한 간단한 타원 곡선으로의 평문 imbedding 방법을 제시해 보았다.타원 곡선에서의 이산 대수 문제는 $GF(p)$ 위에서의 이산 대수 문제보다 어려운 것으로 알려져있다. 특히 타원 곡선은 $GF(2^n)$에서의 이산 대수 문제를 암호 시스템에 이용할 수 있다[13]. $GF(2^n)$에서의 연산은 일반적인 필드에서보다 소프트웨어 및 하드웨어 구현의 측면에서 그 단순성으로 인해 많은 장점을 갖는다. 예를 들어 $GF(2^{155})$에서의 타원 곡선의 연산은 2,000개의 게이트만으로 설계할 수 있고 이는 일반적인 스마트 카드를 위한 프로세서가 차지하는 면적의 5%정도만을 차지한다. 또한 타원 곡선에서의 이산대수문제의 어려움으로 인해 n의 크기가 매우 작은 경우(160bit)에도 아직까지 알려진 공격방법이 없으므로 서론에서 지적한 공개키 암호 시스템의 단점인 큰 블럭 크기와 많은 계산량을 해결할 수 있는 좋은 해결 방법이라 할 수 있다. 1993년 Menezes, Okamoto, Vanstone은 타원 곡선위에서의 이산대수 문제를 유한 필드 위에서의 이산대수 문제로 변환하는 알고리즘을 제시했지만, 이는 특별한 성질을 갖는 타원 곡선 즉 supersingular 타원 곡선인 경우에만 유한체에서의 이산대수 문제로 변환이 가능했다[11]. 따라서 아직까지 일반적으로는 타원 곡선위에서의 이산대수 문제는 유한체에서의 이산대수문제보다 어렵다고 알려져 있다.

RSA DSI사에서는 타원 곡선에 대해서 회의적인 입장을 표명한 바 있다. RSA에 비해 아직까지 타원 곡선에 대한 연구가 많이 이루어지지 않았고 이에 대한 cryptanalysis가 충분하지 않으므로 이를 사용하는데 아직까지는 안전성의 문제가 있다는것이 이유이다. 하지만 본 논문에서 살펴본 바와 같이 공개키 암호 시스템으로서는 가장 작은 블럭 크기를 가지고 있고 $GF(2^n)$에서의 구현도 가능하므로 RSA DSI사의 이런 부정적인 입장은 RSA를 앞으로도 De Facto standard로 사용하겠다는 것으로 보인다. 최근에는 타원 곡선을 이용한 암호 시스템 외에도 Lattice에서 CVP를 이용한 공개키 암호 시스템등 다양한 방법들이 제안되고 있다. 따라서 새로운 공개키 암호 시스템의 설계를 위한 연구가 이산대수문제나 소인수 분해 문제등을 제외한 영역에서도 활발히 이루어져야 한다.

참 고 문 헌

[1] Alfred J. Menezes, Tatsuaki Okamoto, Scott A. Vanstone, "Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field," IEEE Trans. on Information Theory, Vol. 39, No. 5, pp. 1639-1646, 1993

[2] Keji Koyama, Ueli M. Maurer, Tatsuaki Okamoto, Scott A. Vanstone, "New Public-Key Schemes Nased on Elliptic Curves over the Ring Zn," Advances in Cryptology-Crypto'91, pp. 252-266, 1991

[3] Keji Koyama, "Fast RSA-type Schemes Based on Singular Cubic Curves," Advances in Cryptology-Eurocrypt'95, pp. 329-340

[4] T. ElGamal, "A public key cryptosystem and a signature scheme based on the

discrete logarithm," IEEE Trans. on Information Theory, Vol. 31, No. 4, pp. 469-472, 1985

[5] N. Koblitz, A Course in Number Tehory and Cryptography, Berlin: Springer-Verlag, 1987

[6] M. O. Rabin, "Digitalized Signatures and Public Key Functions as Intractable as Factorization," Technical Report, MIT/LCS/TR212, MIT Lab., Computer Science, Cambridge, Mass. 1979

[7] R.L. Rivest, A. Shamir, L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, Vol. 21, No. 2, pp. 120-126, 1978

[8] R. Schoof, "Ellipctic curves over finite fields and the computation of square roots mod p," Mathematics of Computation, Vol. 44, No. 170, pp. 483-494, 1985

[9] N. Koblitz, "Elliptic Curve cryptosystems," Mathematics of Computation, Vol. 48, No. 177, pp.203-209, 1987

[10] V. Miller, "Uses of elliptic curves in cryptography," in Advances in Cryptology-Crypto'85, Vol. 218, pp. 417-426, 1986

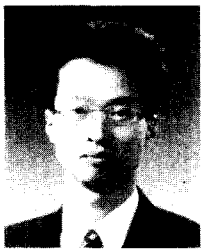
[11] A. Menezes and S. Vanstone, "The implementation of elliptic curve cryptosystems," in Advances in Cryptology-Auscrypt'90, Vol. 453, pp. 2-13, 1990

[12] W. Diffie, M.E. Hellman, "New directions in cryptography," IEEE Trans. on Information Theory, Vol. 22, No. 6, pp. 644-654, 1976

[13] G. B. Agnew, R. C. Mullin, S. A. Vanstone, "An Implementation of Elliptic Curve Cryptosystems Over F2155," IEEE JSAC, Vol. 11, No. 5, pp. 804-813, 1993

[14] S. A. Vanstone, R. J. Zuccherato, "Elliptic Curve Cryptosystems Using Curves of Smooth Order Over the Ring Zn," IEEE Trans. on Information Theory, Vol. 43, No. 4, pp. 1231-1237, 1997

□ 著者紹介



양 대 헌

1994년 2월 한국과학기술대학 전기 및 전자공학과 졸업(공학사)
1996년 2월 연세대학교 컴퓨터과학과 졸업(이학석사)
1996년 ~ 현재 연세대학교 컴퓨터공학과 박사과정 재학중

※ 주관심 분야 : 정보 보안, ATM Congestion control, Protocol engineering

송 주 석

1976년 2월 서울대학교 전기공학과 학사
1979년 2월 한국과학원 전기 및 전자공학과 졸업 석사
1988년 8월 Univ. of California at Berkeley 전산과학과 박사
1979년 2월 ~ 1982년 2월 한국전자통신연구소 전임연구원
1988년 9월 ~ 1989년 2월 Naval Postgraduate School Information System Department 조교수
1989년 3월 ~ 현재 연세대학교 컴퓨터과학과 교수

※ 주관심 분야 : 프로토콜 공학, ATM 통신망, 통신망 보안 등