情 報 保 護 學 會 誌
第21卷 第5號, 2011. 8

타원곡선 암호 구현 WIPO 특허 동향

고 승 철*, 남 길 현**

요 약

타원곡선 암호는 기존의 RSA 암호와 더불어, ANSI와 IEEE 표준 공개키 암호방식을 활용되고 있으며, 특히 WAP 표준으로 채택되어, 스마트폰 등에 의한 이동통신 환경에서 암호 기능을 효율적으로 처리하는 수단으로 각광을 받고 있다. 국내외 보안업체들 역시 최근 스마트폰 등 의 모바일 장치에서 동작되는 타원곡선 암호 장치를 개발 및 출시하고 있으며, 타원곡선 암호 구현과 관련된 국제특허들을 출원하고 있는 추세이다. 본 논문에서는 국내 보안업체들의 타원곡선 암호 상용화 제품 개발을 지원하는 차원에서, WIPO에 최근 출원된 타원곡선 암호 구현기술들을 소개한다.

Ⅰ. 서 론

최근 국내에서는 스마트폰 보급이 1,000만 대를 돌파하며 다양한 분야에서 스마트폰 기반 응용 서비스들이 제공되고 있다. 전자거래 서비스 역시 기존의 PC 기반 인터넷 전자거래와 더불어, 스마트폰 기반 모바일 전자거래 서비스들이 출현하고 있다.

이러한 모바일 전자거래 환경에서, 사용자들의 프라이버시를 보호하고, 전자거래의 안전성을 보장하는 모바일 전자거래 보안기술 역시 그 중요성이 재차 강조되고 있으며, 다양한 형태의 제품 및 서비스들이 개발되고 있는 추세이다.

모바일 전자거래에서 전송되는 데이터를 도청자로부터 보호하고, 송수신자 사이의 상호인증 기능을 지원하는 암호기술은 전자거래의 안전성 및 신뢰성을 보장하는 모바일 전자거래 보안의 핵심기술로 간주된다.

그동안 RSA(Rivest-Shamir-Adlemann) 암호는 전자서명과 상호인증을 지원하는 다양한 보안 프로토콜에서 가장 널리 이용되었다. 그러나 RSA는 암호 처리 과정에서 막대한 연산 처리량과 전력 소모가 필요하기 때문에, 계산 능력과 공간 및 가용 전력이 제한적인 모바일 환경에서의 전자거래 보안 용도로는 적합하지 않다.

ECC(Elliptic Curve Cryotosystem, 타원곡선 암호)는 유한 체 위에서의 타원곡선의 대수적 구조를 기반으로 설계된 공개키 암호 방식으로서, RSA 비해 암호화 과정에 소요되는 연산 처리량이 적고, 키 관리가 용이한 장점이 있다.

ECC는 RSA 암호와 더불어, 미국과 국제 표준 기관인 ANSI(American National Standards Institute)와 IEEE(Institute of Electrical and Electronics Engineers) 등에서 표준 암호로 채택되었으며, 특히 WAP (Wireless Application Protocol) 표준으로 채택되어, 스마트폰 등에 의한 이동통신 환경에서 암호 기능을 효율적으로 처리하는 수단으로 최근 각광을 받고 있다.

이러한 ECC의 새로운 수요에 부응하기 위해, 미국은 2009년 6월 새로운 ECC 표준문서인 FIPS PUB 186-3을 발표하여 [1], ECC 활용을 촉구하고 있다. 국내외 보안업체들 역시 최근 스마트폰 등 의 모바일 장치에서 동작되는 ECC 장치를 개발 및 출시하고 있으며, 효율적인 ECC 구현과 관련된 국제특허들을 출원하고 있는 추세이다.

본 논문에서는 국내 보안업체들의 ECC 제품 개발과 국외 업체들과의 특허분쟁 예방을 지원하기 위해, WIPO (World Intellectual Property Organization, 세계지적소유권기구)에 출원된 ECC 구현 기술들을 소개한다.

본 연구는 한국과학기술정보연구원 ReSEAT 프로그램의 일환으로 수행되었습니다.

* 한국과학기술정보연구원 전문연구위원실(goh5703@reseat.re.kr)
** 한국과학기술정보연구원 전문연구위원실(khnammk3@reseat.re.kr)

Ⅱ. ECC 구현 기법별 WIPO 주요 특허 개요

타원곡선 암호는 타원곡선 위의 주어진 점 P와 양정수 k에 대해, 점 $Q=kP$를 계산하는 스칼라 곱셈에 의해 암호화를 처리한다.

스칼라 곱셈은 양정수 k의 이진 표현 형태에 따라, 일련의 주어진 점의 2배화인 $2P=P+P$와 서로 다른 점들의 덧셈 P_1+P_2의 반복에 의해 처리된다. 따라서 양정수 k를 작은 수들의 합으로 표현하여, 반복 횟수를 줄이거나, 2배화 또는 덧셈을 효율적으로 계산하면, ECC를 고속으로 처리할 수 있다.

최근에 제안된 WIPO 특허들의 핵심 청구사항들을, 크게 양정수 k에 대해 모듈러 감소 등의 기법을 적용하여, 2배화 및 점들의 덧셈들의 반복 횟수를 감축하는 기법들과 2배화 및 덧셈 자체를 효율적으로 처리하는 기법들을 구분할 수 있다.

Nokia 등은 양정수 k를 충분히 작은 수들의 결합으로 표현하는 기법들을 핵심 특허 청구사항으로 제안 하였으며, Thomson Licensing 등은 점들의 2배화 또는 서로 다른 점들의 덧셈을 효율적으로 처리하는 기법을 청구사항으로 제안하였다.

Nokia는 LLL(Lenstra-Lenstra-Lovasz) 알고리즘을 사용하여, ECC 암호화 과정에 필요한 매개변수를 크기가 원래 매개변수의 제곱근 정도인 2개의 매개변수들의 결합, $k=k1+k2\times\lambda(\bmod n)$을 만족하는 정수 k_1과 k_2를 결정하는 기법과 장치 및 컴퓨터 프로그램 제품을 제안하였으며[2], 또한 Amtel은 모듈러 감소를 고속으로 처리하기 위해, 기존의 Barrett 기법을 변형한 새로운 모듈러 감소기법을 핵심특허 청구사항으로 제안하고 있다[3].

Thomson Licensing은 위수가 d인 점을 포함하는 타원곡선 위에서 d-동형을 사용하여, ECC를 고속으로 처리하는 기법 [4]과 일반화된 Edwards 곡선으로 타원곡선을 사영하여, 타원곡선 위의 점들의 덧셈을 효율적으로 계산하는 기법[5] 및 보조좌표를 사용하여, 타원곡선 위의 점의 2배화를 고속으로 처리하는 기법[6]을 핵심 특허청구 사항으로 제안하였다.

IBM은 복합좌표계를 사용하는 부 채널 원자적 곱셈 알고리즘을 특허 청구 사항으로 제안 하였다[7]. 제안된 방식은 미국 NIST(National Institute of Standards and Technology)의 FIPS PUB 186-2를 효율적으로 구현할 수 있다고 IBM은 주장하였다.

Ⅲ. 양정수 k의 분해에 의한 기법들

3.1 Nokia 제안 특허[2]

본 발명은 정수 k에 대해, 수식 (1)을 만족하는 을 만족하는 정수 k_1과 k_2를 결정하는 기법과 장치 및 컴퓨터 프로그램 제품을 제안한다.

$$k=k1+k2\times\lambda(\bmod n) \tag{1}$$

본 발명은 k_1과 k_2의 크기의 한계가 결정되도록 구현될 수 있다. k_1과 k_2의 크기의 한계가 결정되면, 타원곡선 위의 점 P와 정수 k와의 곱은 정수 k_1과 k_2에 의해 결정될 수 있다.

본 발명은 또한 확장된 주어진 점 P의 위수 n과 승수(multiplier) λ에 대해, 확장된 유클리드 알고리즘(extended Euclidean algorithm)을 적용하여 일련의 몫들과 나머지들을 생성한다. 이때 m번째 나머지는 k_1의 한계로 결정된다. 또한 일련의 정수 t들의 수열이 몫들의 수열을 기반으로 결정될 수 있다. 또한 k_2의 한계는 적어도 2개의 정수 t와 n과의 관계를 기반으로 결정될 수 있다.

k_1과 k_2가 결정되며, kP는 수식 (2)에 의해 계산된다.

$$kP=k_1P+(k_2\lambda)P \tag{2}$$

본 발명이 응용되는 통신 환경은 이동 단말기 등의 제1차 통신장치와 네트워크를 통해 통신할 수 있는 제2차 통신장치로 구성된다. 네트워크는 관련된 유선 또는 무선 인터페이스를 통해 통신할 수 있는 다양한 노드(node)들과 장치 또는 설비들을 포함할 수 있다.

3.2 Amtel 제안 특허[3]

이 발명은 Barrett 감소 기법의 변형된 형태에 의해, U/N의 몫 근사치 $\hat{q}$ 를 계산한다.

$$\hat{q} = \lfloor U_1N_1/2^{(\alpha-\beta)} \rfloor \tag{3}$$
$$U_1 = \lfloor U/2^{(\alpha+\beta)} \rfloor$$
$$N_1 = \lfloor 2^{n+\alpha}/N \rfloor$$

$2^{n-t} \le N < 2^n$

t : 기계의 워드를 구성하는 비트 수

n : 모듈러의 비트 수

y 는 $U < 2^{n+y}$를 만족하는 정수

U는 $n+y$ 비트에 의해 구성되는 정수

α, β는 기계 워드의 배수가 되는 정수

이 발명에서 제안하는 기법은 Barrett 수식의 변형을 사용한다. 변형된 수식은 모듈러의 특수 형태에 의해 몫의 근사치 $\hat{q}$ 의 계산을 단순화한다. 따라서 몫의 근사치 $\hat{q}$의 교정 과정이 단순화되며, 이에 따라 나머지의 근사치 $\hat{r}$ 계산 과정을 개선할 수 있다.

주어진 수 U 의 모듈러 N에 대한 추정 감소 값 계산 처리 과정은, 먼저 주어진 입력 U의 값과 특수한 형태의 모듈러 N을 결정한 다음, Barrett 감소의 변형 기법을 사용하여, 모듈러 감소를 처리하고, 추정 감소 값 $\hat{r}$를 출력한 다음 종료한다. 이러한 처리과정은 소수 체 F_p 또는 이진체 F_{2^m} 또는 확장 체 F_{p^m} 에서 정의된 타원곡선을 사용하는 타원곡선 암호 처리에 사용된다.

이 발명은 무의미한 연산이 포함된 공개키 암호 또는 전자서명 연산을 고속으로 처리하기 때문에, 부 채널 공격 차단 기법이 적용된 스마트카드 기반 전자거래 보안에 응용될 수 있다.

Ⅳ. 2배화와 덧셈 고속처리 기법들

4.1 Thomson의 위수 기반 스칼라 곱셈 기법[4]

이 발명은 위수가 d인 타원곡선 위의 점 P의 스칼라 곱 $Q = [kd]P$ 를 계산하는 기법과 장치를 제안한다. 점 P는 $d-$동형 곡선(d-isogenous curve)에 내장(embedded) 되어, $P' = \phi(P)$(ϕ는 $d-$동형 함수)를 구하고, $d-$동형 곡선 위에서 $Q' = [k]P'$을 계산한 다음, Q'을 ϕ의 쌍대 함수 ϕ'에 의해 원래의 곡선 위의 점 Q로 변환한다. 여기서

$$\phi \cdot \phi' = \phi' \cdot \phi = [d] \tag{4}$$

이 발명의 바람직한 실시 사례로서, $d=2$인 2개의 점 $(\theta_1, 0)$와 $(\theta_2, 0)$을 포함하는 Weierstrass 수식 형태의 타원곡선 (5)와 Edward 수식 형태의 2-동형 곡선 (6)을 제안한다.

$$Y^2 = X^3 + a_2X^2 + a_4X \tag{5}$$

$$Y^2(1-4\theta_1X^2) = 1 - 4\theta_2X^2 \tag{6}$$

타원곡선 암호의 핵심 연산은 위수가 n인 점 P의 스칼라 곱셈이다. 타원곡선 C 위에서의 연산 $Q=[m]P$는 2-동형 Edwards 곡선 E위에서 $P' = \phi(P)$를 계산하고, $m' = m/2(\mathrm{mod}n)$을 계산한다. 그 다음 E위에서 $Q' = [m']P'$을 계산하고, 원래의 곡선 C 위에서 $Q = \phi'(Q')$을 계산한다.

이 발명에 의해 위수가 d인 점을 포함하는 타원곡선 위에서 d-동형을 사용하여, 적절한 형태로 표현될 수 있는 동시에 매개변수의 크기가 작은 타원곡선들의 집합을 확장할 수 있다. 따라서 이 발명은 타원곡선 암호의 보안 수준을 향상시키며, 암호연산 처리 속도를 개선하는 효과가 있다.

4.2 Thomson의 Edwards 형식 기반 덧셈 처리기법[5]

이 발명은 일반화된 Edwards 수식 (7)에 의한 타원곡선 위에서 계산을 수행하는 장치와 기법 그리고 컴퓨터 프로그램과 관련된다. 장치는 (8)과 (9)를 를 계산하여, 곡선 위의 2 점들인 (x_1, y_1)과 (x_2, y_2)의 합(x_3, y_3)을 계산하는 프로세스를 포함한다.

$$y^2(1-dfx^2) = f^2 - ex^2 \tag{7}$$

$$x_3 = (x_1y_2 + x_2y_1)/(f + dx_1x_2y_1y_2) \tag{8}$$

$$y_3 = (y_1y_2 - ex_1x_2)/(f - dx_1x_2y_1y_2) \tag{9}$$

점 (x_i, y_i)의 아핀(affine) 표현의 동치 좌표는, 일반화된 Edwards 수식 (10)에 의해 표현되는 타원곡선에 대응되는 일반화된 Edwards 수식 (11)로 표현되는 사영 타원곡선 위의 모든 $Z_i \neq 0$에 대해, 사영 점 $(x_iZ_i : y_iZ_i : Z_i)$ 이다.

$$E_{/K} : y^2(1-dfx^2) = f^2 - ex^2 \tag{10}$$

$$E_{/K} : Y^2(Z^2 - dfX^2) = f^2Z^4 - eX^2Z^2 \tag{11}$$

사영 점들의 합은 수식 (12)와 (13) 및 $Z_3 = MN$을 계

산하여 구할 수 있다.

$$X_3 = Z_1 Z_2 (X_1 Y_2 + X_2 Y_1) M \quad (12)$$

$$Y_3 = Z_1 Z_2 (Y_1 Y_2 - e X_1 X_2) N \quad (13)$$

$$M = f Z_1^2 Z_2^2 - d X_1 X_2 Y_1 Y_2 \quad (14)$$

$$N = Z_1^2 Z_2^2 + d X_1 X_2 Y_1 Y_2 \quad (15)$$

대표적인 구현 사례에서, 프로세스는 점 (x_i, y_i)를 모든 $Z_i \neq 0$에 대해 사영 표현 $(x_i Z_i : y_i Z_i : Z_i)$로 변환과 $(X_3 : Y_3 : Z_3)$로부터 $x_3 = X_3/Z_3$와 $y_3 = Y_3/Z_3$를 계산하여 제3의 점 (x_3, y_3)를 복원할 수 있다. 매개변수 d, e, f 들은 총 계산량 1d+1e+1f 를 최소화하도록 선택된다. 이때 d와 e 및 f는 각각 매개변수 d, e, f에 의한 곱셈을 나타낸다. 매개변수 d, e, f는 각각 -2, -2, +1, +2 로부터 선택되는 것이 바람직하다.

4.3 Thomson의 RTL 스칼라 곱셈 처리 기법[6]

이 발명은 우측에서 좌측방향으로 점의 덧셈과 2배화를 연속적으로 반복하는 RTL(right-to-left, 우측에서 좌측 방향으로) 방식을 기반으로 타원곡선 위의 점들의 스칼라 곱셈을 계산하는 기법 제안한다.

점 $P = (T_1, T_2, T_3)$의 2배화 $2P$를 계산하기 위해, 먼저 보조좌표 $T_4 = aT^8$(이때 a는 타원곡선의 제1 매개변수)를 계산하고, 중간값 U, V, M, W, S를 계산한 다음, 새로운 값 T_3, T_4, T_1, T_2를 계산한다.

$$U = T_1^2, \quad V = T_2^2, \quad M = 3U + T_4, \quad W = V^2,$$

$$S = 2((T_1 + V)^2 - U - W)$$

$$T_3 = 2T_2 T_3, \quad T_4 = 16 W T_4, \quad T_1 = M^2 - 2S,$$

$$T_2 = M(S - T_1) - 8W$$

이 발명의 핵심 제안사항은 우측에서 좌측 방향으로 스칼라 곱셈을 계산하는 기법에서 점들의 2배화 연산을 고속으로 처리하기 위해 부가적인 좌표 T_4를 사용하는 것이다. T_4는 메모리에 저장된다.

이 발명은 서로 다른 좌표계에 의해 점들의 덧셈과 2배화 연산을 처리하여, 기존 기법에 비해 스칼라 곱셈에 소요되는 시간을 13.3 % 단축할 수 있다. 이 발명은 또한 타원곡선의 매개변수와 상관없이 암호를 처리할 수 있기 때문에, 하드웨어 구현이 용이하며, 특히 저장 및 계산 능력이 제한되는 임베디드 장치에 응용될 수 있다.

4.4 IBM의 원자성 보장 기법[7]

이 발명은 유한 체 위에서 정의된 타원곡선에 근거한 암호 시스템의 원자성(atomicity)과 관련된다. 이 발명은 타원곡선 기반 암호 시스템의 원자성을 제공하는 기법과 수단 및 컴퓨터 프로그램 제품을 제안한다.

제안된 기법은 복합 좌표계를 사용하는 부 채널 원자 스칼라 곱셈 알고리즘으로 구성되며, 원자 블록을 제공하는 타원곡선 위의 점들의 덧셈인 ECADD과 이배화인 ECDBL로 구성되는 일련의 연산들의 반복과정을 포함한다. 부 채널 원자 스칼라 곱셈 알고리즘은 방정식 $y^2 = x^3 + ax + b (a, b \in F_p,\ a = 3)$에 의해 정의되는 타원곡선에서 최적화될 수 있다.

제안된 기법은 I/M 비율을 근거로 좌표계를 선택한다. 이때 I와 M은 각각 체의 원소들의 역원 연산과 곱셈 처리에 필요한 계산 시간을 의미한다. 미국 연방표준이 권고한 타원곡선 암호를 구현하기 위해, 이 발명은 I/M 비율이 60 미만이면, 아핀(affine)과 Jacobian 좌표계가 복합된 좌표계를 사용하며, 60 이상인 경우에는, Chudnovsky-Jacobian 좌표계와 Jacobian 좌표계의 복합 좌표계를 선택한다.

이 발명은 또한 ECC에 대한 단순 전력분석 공격을 차단하기 위해, 복합 좌표계와 부 채널 원자성 개념을 사용하여, w NAF(w non-adjacent form, w 비 이웃 형식) 스칼라 곱셈 알고리즘을 구성한다.

이 발명은 미국 연방 표준인 FIPS PUB 186-2에서 권고한 타원곡선을 사용할 수 있으며, 타원곡선 암호에 대한 부 채널 공격을 차단하는 동시에 타원곡선 암호를 고속으로 처리하는 효과가 있다.

V. 결 론

본 논문은 CPU 처리능력과 설치 공간 및 가용 전력이 제한적인 모바일 환경에서의 사용될 ECC 제품을 개발하는 국내 보안업체들을 지원하는 차원에서, 국제 특허 관리기관인 WIPO 최근 출원된 ECC 구현 기술들을 소개하였다.

참고문헌

[1] http://csrc.nist.gov/publications/fips/fips 186-3/fips_186-3.pdf, "Digital Signature Standard (DSS)," National Institute of Standards and Technology, 2009.

[2] NOKIA CORPORATION, "METHOD. APPARATUS AND COMPUTER PROGRAM PRODUCT FOR EFFICIENT ELLIPTIC CURVE CRYPTOGRAPHY," PCT, WO 2010/0034886, 2010.

[3] ATMEL CORPORATION, "MODULAR REDUCTION USING A SPECIAL FORM OF THE MODULUS," PCT, WO 2009/091748, 2009.

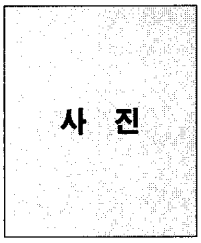
[4] THOMSON LICENSING, "AN APPARATUS AND A METHOD FOR CALCULATING A MULTIPLE OF A POINT ON ELLIPTIC CURVE," PCT, WO 2009/095492, 2009.

[5] THOMSON LICENSING, "A DEVICE, METHOD AND A COMPUTER PROGRAM PRODUCT FOR CALCULATING ADDITIONS OF POINTS ON ELLIPTIC CURVES IN EDWARDS FORM," PCT, WO 2009/095491, 2009

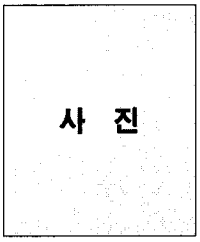
[6] THOMSON LICENSING, "AN APPARATUS AND A METHOD FOR CALCULATING A MULTIPLE OF A POINT ON AN ELLIPTIC CURVE," PCT, WO 2009/101147, 2009.

[7] INTERNATIONAL BUSINESS MACHINES CORPORATION, "METHOD AND SYSTEM FOR ATOMICITY FOR ELLIPTIC CURVE CRYPTOSYSTEMS," PCT, WO 2009/024520, 2009.

〈著者紹介〉



고 승 철 (Sung Cheol Goh)
정회원
1981년 2월 : 연세대학교 수학과 졸업
1983년 2월 : 연세대학교 수학과 석사
1992년 2월 : 포항공대 수학과 박사
2004년 6월~2008년 2월 : 한국지식보안산업협회 상근부회장
2009년 2월~현재 : 한국과학기술정보연구원 전문연구위원
<관심분야> 정보보호



남 길 현 (Kil Hyun Nam)
정회원
1973년 2월 : 서울대학교 토목공학과 졸업
1979년 8월 : 미국 해군대학교 전산학과 석사
1985년 8월 : 루이지아나 대학교 전산학과 박사
1985년 3월~2008년 2월 : 국방대학원 교수
2010년 2월~현재 : 한국과학기술정보연구원 전문연구위원
<관심분야> 정보보호