사용자 신원확인을 위한 타원곡선 암호알고리즘의 적용

정 재 훈, 박 영 만, 박 상 규

한양대학교 전자전기컴퓨터공학부

User Identification Using Elliptic Curve Cryptography

Jae Hoon Jeong, Young Man Park, Sang Kyu Park

Division of Electrical and Computer Engineering Hanyang, Univ.

요 약

본 논문에서는 이동 통신 시스템에서 사용자 신원확인 및 인증을 하기 위해 타원곡선과 지문인식을 적용하는 시스템을 제안하였다. 제안된 시스템은 타원곡선 암호 시스템의 계산량, 키 크기, 대역폭의 측면에서의 효율성이 고려되었다. 또한, 타원곡선 이산대수 문제가 어렵다는 점에 초점을 맞추었다. 수학적인 증명과 안전성을 분석하여 제안된 시스템의 성능을 분석하였다.

I. 서론

정보화시대로 표현되는 현대사회는 컴퓨터, 유·무선 통신기술등의 발달로 다양한 분야에 걸쳐 개인뿐만 아니라 사회에 편리함을 제공하고 있다. 반면, 이러한 기술 발달의 장점에 역행하여 개인정보의 누출, 도청, 신분 위조 및 노출뿐만 아니라 국가적인 중요 기밀사항까지 누출되는 큰 부작용의 발생이 지속적으로 문제시되고 있다. 이러한 문제점을 줄이고자 하는 노력은 이미 오래 전부터 시도 되어왔으며 그 시도중의 하나가 바로 암호를 적용하는 것이다[1].

암호가 사용되던 초창기 시절에는 대칭키 알고리즘이 사용되었지만 암호 사용자가 늘어나고 다양한 암호 서비스에 대한 요구가 제기되면서 키의 관리 문제와 인증문제가 발생하였고, 이러한 문제를 해결하기 위해 공개키 암호시스템이라는 개면이 제안되었으며 1978년에는 소인수분해의 어려움에 기반을 둔 RSA가 소개되어 지금까지 넓게 사용되고 있다[2]. 하지만 최근에는 RSA의 안전성이 위협받고 이동 통신 단말기와 같은 저용량 소형 및 휴대용 장비의 보급 확대로 인해 좀 더 안전하고 효율적인 공개키 알고리즘의 필요성이 요구되었고 타원곡선을 응용한 암호 알고리즘이 소개되어 꾸준히 연구되고 있다[2][3].

정보 자체에 암호를 적용하는 것도 중요하지만 일차적으로 정보 자체의 접근을 통제하는 것도 중요하다. 기존에는 패스워드를 사용하였지만 분실이나 도난 등의 문제를 방지하기 위해 최근에는 생체인식을 통해 사용자 신원확인 및 인증을 하기 위한 연구가 활발하며 이미 상용화된 분야도 있다. 특히 지문인식은 효율성 및 안전성이 우수하여 가장 널리 쓰이고 있다[4]. 하지만 분실이나 도난 당하기 쉬운 이동 통신 단말기와 같은 휴대용 장비에서의 생체인식 시스템 구현은 사용자의 생체에 대한 정보가 유출될 우려가 높다.

본 논문에서는 지문인식 알고리즘에 대해서는 직접적으로 다루지 않지만, 이동 통신 단말기에서의 사용자 신원 확인 및 인증을 동시에 할 수 있으며 지문정보 유출을 방지하기 위한 방안으로 타원곡선 암호 알고리즘과 지문인식을 연계시킨 모델을 제시하였다. 제안된 모델에 대한 분석에서 단말기, 사용자, 그리고 스마트 카드 각각의 관점에서 바라본 안전성을 확인하였고 시스템에 대한 수학적인 증명을 통해 그 진위여부를 판단할 수 있었다. 또한 지문의 랜덤성에 대한 분석에서 동일한 지문들의 해쉬값이 상관성이 낮다는 점을 확인하였다.

II. 제안된 사용자 신원확인 기법

사용자 신원확인을 자동 지문 인식 시스템과 타원곡선 암호 시스템을 연결함으로써 안전성이 높고 빠른 시간 내에 이루어 질 수 있도록 하였고 자동 지문 인식 시스템을 통하여 사용자 인증까지 할 수 있는 모델을 제안하였다. 또한 사용자간의 키 교환에서 지문의 랜덤성을 활용하였고 replay 공격에 대한 방안을 검토하여 이를 적용하였다[5].

1. 사용자 신원확인

본 논문에서 제안한 사용자 신원확인 모델은 그림 1과 같다.

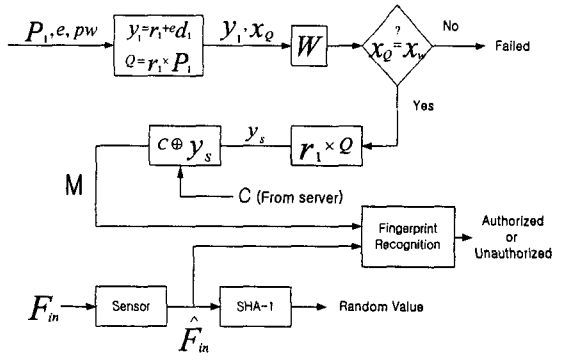

그림 1 제안된 사용자 신원확인 시스템

그림 1에 제안된 시스템은 사용자, 단말기, 서버로부터 받은 정보를 통해 암호 연산을 위한 스마트 카드에서 수행되는 과정을 나타낸 것이다.

1) 사용자와 단말기의 역할

첫째, 사용자의 역할은 다음과 같다.

step 1-1. 패스워드(pw)를 입력한다. 이것은 사용자가 단말기와 스마트 카드를 모두 분실한 경우, 사용자 지문 정보의 유출에 대비한 최소한의 대안이다.

step 1-2. 사용자 신원확인이 성공되었을 경우 지문을 센서를 통해 입력시킨다.

사실, 패스워드의 입력은 사용자에게 불편함을 주고 전통적인 방식에 대해서도 완전히 벗어나지 못한다는 것을 의미할 수 있지만 탬퍼(tamper)와 같은 스마트 카드에 대한 불법적인 공격에 대한 완벽한 방어 체계를 갖추지 못한다고 가정했을 경우에는 최소한의 패스워드는 필요하다고 볼 수 있다.

둘째, 단말기의 역할은 다음과 같다.

step 2-1. e값을 스마트 카드에 전송한다. 여기서 $e(\in F_q)$는 PIN(Personal Identification Number)의 역할을 한다.

step 2-2. P_1값을 스마트 카드에 전송한다. 여기서 P_1은 $Q=(r_0+pw)P_1 = r_1P_1=(x_Q, y_Q)$, $r_1 \in F_q$ 을 만족하는 값이다.

단말기는 스마트 카드의 메모리 효율을 높이고 시스템 전체의 보안을 위해 스마트 카드의 연산에 필요한 정보들을 가지고 있다고 볼 수 있다.

2) 스마트 카드에서의 연산

이 절에서는 제안된 시스템의 핵심 내용인 스마트 카드의 연산 과정에 대해서 살펴본다. 우선, 스마트 카드는 사용자와 단말기로부터 pw, e 그리고 타원곡선상의 한 점 P_1값을 받았다고 가정한다. 그리고 스마트 카드 내부적으로는 상수인 d_1, r_0을 가지고 있고 신원확인이 성공적으로 된 경우에만 암호화된 지문의 특징점 정보 $C=y_S \oplus M$ 을 서버로부터 실시간 전송 받는다고 가정한다. 여기서 M이 지문의 특징점 정보이다. 그림 1의 각 과정은 다음과 같다.

step 3-1. 단말기로부터 받은 e과 P_1을 사용하

여 y_1과 Q를 구한다.

$$y_1 = r_1 + ed_1 \quad (1)$$
$$Q = r_1 \times P_1 \quad (2)$$

step 3-2. 식 (1)에서 구한 y_1을 이용하여 W를 구한다.

$$W = y_1 P_1 - e(d_1 P_1) = (x_W, y_W) \quad (3)$$

step 3-3. W와 Q가 동일한지 판단한다.

$$x_Q \stackrel{?}{=} x_W \quad (4)$$

만약 x_Q와 x_W가 동일하다면 다음 단계로 넘어가고 그렇지 않다면 중지한다.

step 3-4. pw, r_1 그리고 Q를 사용하여 S를 구한다.

$$S = (r_0 + pw)Q = r_1 Q = (x_S, y_S) \quad (5)$$

step 3-5. 식 (5)에서 구한 y_S를 사용하여 지문의 특징점 정보를 암호화한 값 C를 복호화한다.

$$M = C \oplus y_S \quad (6)$$

step 3-6. 센서로부터 입력받은 지문 $\hat{F}_{in}$과 지문의 특징점 정보 M을 이용하여 지문인식 알고리즘을 통한 사용자 인증을 최종적으로 한다.

step 3-3까지가 사용자 신원확인을 하는 과정이다. 식 (4)에서 x_Q와 x_W가 동일해야 하는 이유는 식 (1)을 식 (3)에 대입한 결과 식을 통해 알 수 있다. 즉, 다음과 같다.

$$\begin{aligned} W &= y_1 P_1 - e(d_1 P_1) \\ &= (r_0 + pw + ed_1)P_1 - ed_1 P_1 \\ &= r_1 P_1 + ed_1 P_1 - ed_1 P_1 \\ &= r_1 P_1 \\ &= Q \end{aligned} \quad (7)$$

사용자 인증은 실질적으로 모든 과정을 거치는 것이 된다. 마지막으로 지문인식 알고리즘을 거치지만 이전 과정들을 거치지 않고서는 불가능하기 때문이다. 또한 센서를 통과한 지문 정보를 $\hat{F}_{in}$ 표기한 것은 지문의 물리적 상태, 누르는 압력이나 위치 등에 따라 그 값이 항상 일정하지 않기 때문이다.

III. 제안된 시스템 분석

1. 사용자 신원확인

1) 수학적인 증명

제안된 시스템에서 사용자 신원확인을 하는 부분에 대한 수학적인 증명을 간단한 예를 통하여 확인하였다. 이를 위해 먼저 유한체 F_{11}상에서 정의된 타원곡선 $y^2 = x^3 + x + 6$ 를 정의하였다. 이 타원곡선상의 점들을 정리하면 표 1과 같다.

표 1 유한체 F_{11}위에서 정의된 타원곡선 $y^2 = x^3 + x + 6$ 상에서의 점들

x	$x^3 + x + 6 \mod 11$	정의된 타원곡선상의 점인가?	y
0	6	×	
1	8	×	
2	5	○	4,7
3	3	○	5,6
4	8	×	
5	4	○	2,9
6	8	×	
7	4	○	2,9
8	9	○	3,8
9	7	×	
10	4	○	2,9

표 1에서 점들 중 임의의 한 점 (2, 7)을 선택하여 step 2-2에서 정의된 P_1에 할당하였다. step

1-1에서 정의된 사용자 패스워드 pw는 3, step 2-1에서 정의된 e는 3이라고 가정하였다. 그리고 스마트 카드 내부적으로 가지는 상수 d_1, r_0는 각각 2로 정의하였다. 이와 같이 가정한 변수들을 실질적으로 스마트 카드에서의 연산에 적용시켜 보면 step 3-1에서 다음과 같은 결과를 얻는다.

$$\begin{aligned} y_1 &= r_1 + ed_1 \\ &= (r_0 + pw) + ed_1 \\ &= (2+3)+3 \cdot 2 = 11 \end{aligned}$$

$$\begin{aligned} Q &= r_1 \times P_1 \\ &= (r_0 + pw) \cdot P_1 \\ &= 5 \cdot (2, 7) \\ &= 2 \cdot (2, 7) + 2(2, 7) + (2, 7) \\ &= (5, 2) + (5, 2) + (2, 7) \\ &= 2(5, 2) + (2, 7) \\ &= (10, 2) + (2, 7) \\ &= (2, 4) \end{aligned}$$

step 3-2에서 위에서 얻은 결과를 이용하면

$$\begin{aligned} W &= y_1 P_1 - e(d_1 P_1) \\ &= 11 \cdot (2, 7) - 3(2 \cdot (2, 7)) \\ &= 11 \cdot (2, 7) - 6 \cdot (2, 7) \\ &= 5 \cdot (2,7) \\ &= (2, 4) \end{aligned}$$

이고 이 결과는 step 3-3에서 요구하는 $Q = W$의 조건을 만족시킨다. 또한 Q와 W는 정의된 타원곡선상의 한 점인 (2, 4)를 가진다. 그러므로 제안된 시스템은 수학적으로 올바르게 정의된 것이다.

2) 보안 측면에서의 분석

보안 측면에서 봤을 때, 발생할 수 있는 모든 경우에 대해서 고려해 보면 크게 다음 세 가지로 구분된다. 최악의 상황을 고려하기 위해 각각의 경우 하드웨어를 분실했을 때 저장되어 있는 데이터가 유출된다고 가정한다. 또한 내부의 전체 알고리즘은 공개적인 것이라고 가정한다.

① 단말기를 분실한 경우
e, P_1가 제 3자에게 알려진 것이다. 이 때, 제 3자는 식 (7)를 만족시키는 r_1과 d_1을 찾아야 한다. step 3-1과 3-2를 무시한다고 해도 식 (7)에서 보다시피 Q를 알지 못하면 r_1을 유한체 F_q상에서의 모든 원소로 대입하는 시도를 해야 한다.

② 스마트 카드를 분실한 경우
d_1 그리고 r_0가 유출된 경우이다. 제 3자는 식(7)를 만족시키기 위한 P_1과 e를 찾아야 한다. 이 경우에도 step 3-1과 3-2를 무시한다고 해도 Q를 알지 못하면 타원곡선상의 모든 점들에 대해 임의의 $(r_0 + pw)$ 값을 곱하는 시도를 해야한다.

③ 단말기와 스마트 카드 모두 분실한 경우
e, P_1, d_1, r_0이 유출된 경우이다. 이 경우에도 step 3-1과 3-2를 무시한다고 했을 때, pw를 모르는 이상 Q를 알지 못한다. 만약 pw를 사용하지 않는 시스템을 고려했을 때, 이 경우에 보안은 사실상 지문인식에 의존하게 되며, 사용자 지문정보 M의 안전을 확신할 수 없게 된다.

2. 지문의 랜덤성에 대한 분석

지문의 랜덤성을 이용한 비밀키 생성에 대해 검토하기 위해서 256×256 크기의 동일한 지문 5개의 해쉬값을 구하였다. 이 실험에서는 SHA-1을 사용하였다. 그 결과는 표 2에 나타나 있으며 서로 간의 상관성을 찾아 보기 어렵다. 지문 화상간의 작은 차이라도 해쉬의 특성으로 인해 전혀 다른 결과를 내는 것이다.

표 2 동일한 지문에 대한 해쉬값

지문1	1488eb70 68648469 e8766b37 42b63dff 2eb5530c
지문2	ee26eb09 c0529f51 358fee84 5f18708d b0664a54
지문3	0a87e549 e3792b0d cebe254b 5af4cea1 229609da
지문4	f6c2f42d 96d65b2b f8ffb50d 2cc205ee 19ae2313
지문5	abb6d5d5 7c14bb69 a8d9acaa 3c5b3dca 441ba66b

IV. 결론

본 논문은 타원곡선 암호 알고리즘의 이산대수 문제에 기초하여 간단한 방식을 사용하고도 보안성이 높은 시스템을 구현하였다. 즉, 사용자 신원 확인을 통하여 일차적으로 제 3자에 의한 단말기의 불법적인 사용을 어렵게 하는 방안을 제안하였다. 또한 수학적인 증명을 통하여 올바른 작동여부를 확인하였다. 지문의 랜덤성을 이용한 난수 생성은 결과에서 보듯이 동일한 지문임에도 불구하고 서로간의 상관성이 낮은 점으로 미루어 볼 때 충분히 고려할 만한 대상이다.

참 고 문 헌

[1] 이민섭, *현대암호학*, 2000

[2] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, *HANDBOOK of APPLIED CRYPTOGRAPHY*, 1997.

[3] Douglas R. Stinson, *CRYPTOGRAPHY Theory and Practice*, 1995

[4] L. C. Jain, U. Halici, I. Hayashi, S. B. Lee, and S. Tsutsui, *INTELLIGENT BIOMETRIC TECHNIQUES in FINGERPRINT and FACE RECOGNITION*, 1999

[5] M. Aydos, B. Sunar, and Ç. K. Koç, *"An Elliptic Curve Cryptography based Authentication and Key Agreement Protocol for Wireless Communication,"* 2nd International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications, Dallas, Texas, October 30, 1998.