제18회 한국정보처리학회 추계학술발표대회 논문집 제9권 제2호 (2002.11)

이동 통신 환경에서의 타원곡선 암호 알고리즘을 이용한 효율적이고 안전한 전자지불시스템

강혁*, 이형우, 김태윤*
고려대학교 컴퓨터학과
paranblue@netlab.korea.ac.kr

Effective and Safe Elcetronic Payment System using Elliptic Curve Public Key Algorithm in Mobile system

Hyeok Kang*, Hyung-Woo Lee, Tai-Yun Kim*
Dept of Computer Science, Korea University*
Dept of Information & Communication Engineering, Chonan University

요 약

본 논문은 최소한의 정보량을 가지고 높은 안전성을 제공하는 타원곡선을 이용한 전자 지불 프로토콜을 제안한다. 타원 곡선 공개키 암호 알고리즘의 이용은 지불과정에서 필요한 계산 속도를 빠르게 함으로써 실제로 지불 시스템을 구현하였을 때 사용자들에게 지불시스템의 효율적이고 편리함으로서 실제로 지불 시스템을 구현하였을 때 사용자들에게 지불시스템의 효율적이고 편리한 이용환경을 제공할 수 있고 타원곡선 공개키 암호 알고리즘이 가지는 높은 안전성은 사용자들에게 지불시스템에 대한 신뢰성을 가지게 할 수 있다. 타원곡선 공개키 암호 알고리즘을 통하여 설계된 지불 시스템은 미래의 이동 컴퓨팅 환경에서도 효과적으로 사용될 수 있을 것이다.

1. 서 론

현대에는 컴퓨터의 발달에 따라 은행업무, 전자상거래와 메일 주고받기 등 국가간의 전쟁이 아닌 곳에서도 암호의 사용이 아주 많이 사용하게 되었다. 인수분해의 어려움을 이용한 RSA암호는 사용하는 숫자의 자리수가 너무 많아 계산하는데 사간이 너무 많이 걸리므로 이를 대용할 방법으로 RSA 암호(1024bit)보다 적은 비트(60bit)정도로 더 좋은 보안 효과를 가져올 수 있는 타원곡선 암호는 요즘 각광을 받고 있다. 전자 지불시스템은 1988년 Chaum, Fiat와 Naor에 의해 처음 소개되었으며 이후 많은 암호학적 지불 프로토콜들이 제안되어왔다.[1] 지금까지 전자지불시스템의 연구는 크게 두가지 방향으로 이루어져왔으며 첫 번째로는 지불시스템 자체의 보안성을 증가시키는 것이며 두 번째는 실제적으로 지불시스템을 하드웨어로 구현하고 사용할 때 소요되는 비용을 줄이는 것이다. 그러나 보안성을 증가시키기 위해서는 하드웨어의 구현 및 시스템 유지비용이 증가하게 되고 유지비용을 낮추기 위해서는 보안성이 감쇄되어야 하는 관계를 가지고 있다. 따라서 전자지불시스템에 관련한 많은 프로토콜이 제안되어왔음에도 불구하고 활발하게 이용되지 못하였다.

지불프로토콜은 크게 지불자(Payer), 상인(Merchant)과 은행(Bank)으로 나누어 설계할 수 있으며 지불시스템을 하드웨어 상으로 구현하기 쉽게 하기 위한 지불시스템의 요건은 사용자가 지불에 참여하기 위하여 가지고 있어야 할 정보는 최소로 되어야 하며 지불 과정이 일어날 때 사용자, 상인 은행간에 전송되는 메시지의 크기가 최소가 되어야 한다.

지불프로토콜을 구현하기 위한 보충적인 방법으로는 위의 프로토콜 설계 요건 이외에 스마트 카드의 이용과 타원 곡선 공개키 암호 알고리즘의 적용을 들 수 있다. 스마트 카드를 이용하였을 경우 사용자는 지불시스템을 사용하기 위하여 매번 지불이 일어날 때마다 생성되는 시스템 관련 변수 값을 알지 않아도 되며 단순히 PIN(Personal Identification Number)만을 알고 있으며 swlqnf 시스템의 이용을 가능하게 한다. 타원 곡선 공개키 암호 알고리즘의 사용은 지불 시스템을 사용하는데 필요한 계산 속도의 증가에 따른 키 길이의 증가에도 기존의 공개키 암호 알고리즘에 비하여 짧은 키 길이로 높은 알고

리즘의 안전성을 제공할 수 있다.

본 논문에서는 Markus Jakobsson이 제안하였던 전자지불 프로토콜에 타원 곡선 공개키 암호 알고리즘을 적용하여 효율적이고 안정성이 높은 지불 시스템을 설계한다.[2]

2. 타원 곡선 공개키 암호 알고리즘

암호프로토콜에서의 안전도는 프로토콜이 기반한 수학적 문제의 복잡도에 따라서 결정된다. 기존의 암호학적 시스템은 수학적 문제의 복잡도를 DLP(Discrete Logarithm Problem)에 기반하고 있으며 이러한 시스템의 비도를 증가시키는 방법은 패스워드의 길이를 증가시키는 것이다. 이 경우 컴퓨터의 계산 능력에 따라서 어느정도까지는 비도를 증가시킬 수 있지만 그 이상이 될 경우 같은 정도의 비도를 증가시키기 위해서 패스워드의 길이를 기하급수적으로 증가시켜야만 한다. 이러한 배경 하에 등장하게 된 것이 타원 곡선 공개키 암호 알고리즘이다.

2.1 공개키 암호알고리즘의 분류

공개키 암호 알고리즘 표준화 그룹인 IEEE P1363은 공개키 암호 알고리즘을 기반하고 있는 수학적으로 어려운 문제에 따라 분류하고 있다 수학적으로 어려운 무제란 그 문제를 polynomial-time내에 해결할 수 있는 효율적인 알고리즘이 존재하지 않는 문제를 의미한다. IEEE P1363은 이러한 문제를 IFP(Integer Factorization Problem), DPL(Discrete Logarithm Problem) 및 ECDLP(Elliptic Curve Discrete logarithm)의 세가지로 구분된다.[3]

2.2 ECDLP(Elliptic Curve Discrete Logarithm Problem)

$$Q = x_P$$

여기서 P는 타원곡선상의 한 점이며 Q는 P를 x번 더한값이다. 알려진 공격알고리즘으로는 Pollard rho-method가 있으며 fully exponential time의 복잡도를 갖는다.[4,5]

2.3 타원곡선 공개키 암호 알고리즘의 장점

타원곡선 공개키 암호 알고리즘은 ECDLP를 기반으로 하며 이것이 DLP기반의 공개키 암호알고리즘에 비해 가지는 장점은 키크기 이외에도 보안적 측면과 효율적 측면으로 나누어 볼 수 있다.[6]

첫 번째 보안적 측면에서 DLP가 Sub-exponential time complexity에 기반을 하고 있는 반면 ECDLP는 Fully-exponential time complexity에 기반하고 있다. 이것은 같은 키 크기 증가에 대해서 타원곡선 암호 시스템의 보안성이 훨씬 증가한다는 것을 의미한다.

두 번째 효율적 측면에서 Computational overhead, 키 크기, Bandwidth로 나누어 생각했을 때 암호 알고리즘은 RSA와 DSA에 비해 대략 10배의 수행속도를 가지며, 16bit의 타원 곡선 키 크기는 1024bit의 RSA와 DSA와 같은 안전도를 가진다.

마지막으로 RSA가 전송하는 bit수의 1/3정도의 크기로 전송하므로 Bandwidth를 적게 할 수 있다.

이와 같은 장점으로 인해 타원곡선 공개키 암호 알고리즘은 스마트 카드와 같은 용량이 제한 된 하드웨어의 구현이 용이하고 앞으로 컴퓨터 계산속도가 증가하더라도 암호학적 비도를 유지하기 위해 키 크기의 선형증가율을 가지게 된다. 이외에도 RSA에 비해 특허문제를 피할 수 있는 장점이 있다.

3. 지불 시스템의 설계

지불시스템을 설계할 때는 하드웨어로 구현되었을 때 효율성과 안정성을 반드시 고려하여야 한다. 본 문에서는 제안하고자하는 지불 시스템을 설정하고 타원곡선 공개키 암호 알고리즘을 이용하여 지불 시스템을 재 설계한다.

3.1 지불 시스템의 모델

지불 시스템 모델의 구성요소는 다음과 같다.

지불자(Payer)	지불을 하는 객체(entity)
상인(Merchant)	지불을 받는 객체
은행(Bank)	지불자와 상인들의 계좌에 관한 정보와 자금 이체등의 정보를 가지고 있음
지불장치 발행기관(Issuer)	지불장치를 생산하고 사용자들에게 보급

[그림2] 지불 시스템 모델의 구성요소

3.2 지불 시스템의 매개변수

본 논문에서 사용하게 될 매개변수는 다음과 같다.

σ	사용자가 가지고 있는 비밀 랜덤 값
max	지불 받기 과정에 필요한 카운터(Counter) 변수 값
next	지불하기 과정에 필요한 카운터 변수 값
g	DLP의 생성자(generator)
G	ECDLP의 생성자
H(),f()	일방향 해쉬 함수(one way hash funtion)
x	지불과정마다 생성되는 비밀키 값
y	x로부터 생성되는 공개키 값

[그림1] 지불 시스템 모델의 구성요소

3.3 지불과정의 원리

지불과정은 max와 next 변수를 가지고 이루어지는데 즉 지불시스템의 사용자는 지불을 위해 max와 next 변수를 기지고 있으며, 이때 자신이 현재 가지고 있는 금액은 next-max 값이 된다. 지불을 받게 되는 상인의 경우 max변수를 증가시키게 되고 지불을 하는 지불자의 경우 next 변수를 증가시키게 된다.

4. ECDLP를 이용한 지불 시스템

DLP상에서의 지불시스템을 ECDLP상에서 설계한다.[7,8]

4.1 지불장치의 초기화

지불장치의 초기화를 위해서는 초기에 은행과 사용자는 비밀 랜덤 초기값 σ 를 분배 받아야 하므로 Diffie-Hellman 키 분배 방식을 이용한다. ECDLP상에서의 키 분배 방식은 [그림 3]와 같으며 이때 공유된 좌표값 $abP = E_p(x_{AB}, y_{AB})$ 중에서 x 좌표값인 x_{AB} 값을 비밀 랜덤 초기값 σ 로 사용한다.

사용자1		사용자2
비밀키 a를 선택		비밀키 b를 선택
A=aP		B=bP
aB=a(aP)=abP		bA=b(aP)=abP

[그림3] ECDLP상의 Diffie-Hellman 키분배 프로토콜

4.2 제안한 타원곡선상의 지불시스템

ECDLP상에서 지불시스템을 설계하면 다음과 같다.

① 지불을 받게 되는 상인은 자신의 비밀 랜덤 초기화값 σ_M과 자신의 $\max_M$ 변수로 f 함수를 이용하여 비밀키 x_M을 생성해 낸다. 생성된 x_M를 이용하여 공개키 값을 생성해 낸다.

비밀키 값 : $x_M = f(\sigma_M, \max_{M+1}, 1)$

공개키 값 : $(y_{M_x}, y_{M_y}) = x_M \cdot G$

이 공개키 값은 x_M으로부터 생성해낸 좌표값의 x 좌표값인 y_{M_x}값을 취하여 지불자에게 전송한다.

② 지불을 할 지불자는 자신의 비밀 랜덤 초기화값 σ_P와 $next_P$를 이용하여 두 개의 비밀키 x_P 와 k 를 생성해 낸다. 생성한 x_P와 k를 가지고 공개키 값을 생성한다.

비밀키값 : $x_P = f(\sigma_P, next_P, 1)$,

$k = f(\sigma_P, next_P, 2)$

공개키값 : $(y_{P_x}, y_{P_y}) = x_P \cdot G$, $(r_x, r_y) = k \cdot G$

이때의 공개키값은 x좌표값인 y_{P_x}와 r_x만을 취하며, y_P 와 r_x값을 가지고 상인으로부터 전송 받은 y_{M_x}에 대한 전자서명값을 생성한다.

$$s = k - x_P H(y_{M_x}, r_x)$$

③ 생성된 것들 $(y_{P_x}, y_{M_x}, r_x, s)$을 은행으로 보낸다. 이때 은행에서는 다음과 같이 계산하여서 r_x 값만을 취하여 지불자로부터 전송 받았던 r_x값과 맞는지를 확인하여 정당한 지불을 확인한다.

$$\begin{aligned}(r_x, r_y) &= s \cdot G + H(y_{M_x}, r_x) \cdot y_{P_x} \\ &= s \cdot G + H(y_M, r_x) \cdot y_P \cdot G \\ &= (k - x_P H(y_{M_x}, r_x)) \cdot G + H(y_{M_x}, r_x) \cdot x_P \cdot G \\ &= k \cdot G\end{aligned}$$

④ 위와 같은 확인과정이 끝난 후 은행은 해당 지불자와 상인에게 지불이 성공적으로 이루어졌음을

알려주고 사용자는 $next_P$ 변수 값을 하나 증가시키고 상인의 경우 mex_M 값을 하나 증가시킨다. 또한 은행의 데이터베이스에 있는 해당 상인과 사용자의 변수 값을 증가된 값으로 변경한다.

5.제안한 지불시스템의 효용성

① 사용자의 저장장치에 가지고 있어야 하는 경우보다 적다 사용자는 저장장치에 σ, $next$, max의 세 가지의 변수 값만을 저장하고 있으면 된다. 이것은 또한 은행의 데이터베이스에 저장해야 할 정보량을 적게 한다.

② 프로토콜의 간단한 구조와 적은 데이터양은 하드웨어의 구현에 적합하며 안전성의 증명을 용이하게 하고 지불프로토콜을 운용한 복잡한 프로토콜로의 확장이 용이하다.

③ 타원곡선 공개키 암호 알고리즘의 적용은 지불시스템이 타원곡선이 가지는 장점을 상속받게되므로 지불시스템의 사용자들에게 안전하고 효율적인 자불 환경을 제공할 수 있다.

6. 결 론

전자지불시스템은 현재 널리 쓰이고 있는 현금, 신용카드와 같이 사용자들에게 편리하고 안전한 지불환경을 제고해야 한다. 사용자의 지불장치는 기억용량과 계산 속도에 제한이 있으며 지불시스템을 설계할 때는 간단한 프로토콜의 사용, 효율적인 부가장비의 사용 등이 요구된다. 본 논문에서는 간단한 구조를 가지는 지불프로토콜에 타원곡선 공개키 암호 알고리즘을 적용함으로서 하드웨어 구현시의 비용을 줄일 수 있고 보다 높은 안전성을 가지는 지불시스템을 설계하였다. 현재 보편화되어진 이동 컴퓨팅 환경에서도 적은 정보량과 타원 곡선을 이용한 지불 프로토콜이 보다 효과적으로 구현되어 이용될 수 있을 것이다.

7. 참고 문헌

[1] D . Chaum, A Fiat and M Naor " Untraceable Electronic Cash", Advances in Cryptology - Proceeding of Crypto'88 pp.319-327

[2] Markus Jakobsson " Mini-Cash: A Minimalistic Approach to E-Commerce" PKC'99, 1999

[3] IEEE P1363/D1a Standard Specifications For Public Key Cryptography, Feb.13, 1998

[4] ANSI X9.62 Elliptic Curve Digital Signaure Alforithn(ECDSA), working draft, Oct 1997

[5] ANSI X9.63 Elliptic Curve KeyAgreement and Key Transport Protocols, working draft, Oct 1997

[6] Scott A. Vanstone. Advanced Seminar on the Elliptic Curve Cyptosystem (ECC), Toronto, Apr 1998

[7] Neal Koblitz, A Course in Number Theory and Cryptography, SpringerVerlag, New York, 1987

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