타원곡선 키 교환 프로토콜 응용을 위한 마이크로소프트 COM 소프트웨어 모듈 구현

*김태호 *김창훈 **권순학 *홍춘표
*대구대학교 **성균관대학교

{thkim, chkim}@dsp.daegu.ac.kr shkwon@math.skku.ac.kr cphong@daegu.ac.kr

Implement of Microsoft COM Software Modules for Elliptic Curve Key Exchange Protocol Applications

*Tae Ho Kim, *Chang Hoon Kim, **Soonhak Kwon, *Chun Pyo Hong
*Daegu Univ. **Sungkyunkwan Univ.

요 약

본 논문에서는 타원곡선 키 교환 프로토콜 응용을 위한 마이크로소프트 COM 소프트웨어 모듈을 구현하고 그 성능을 평가한다. 개발된 COM 소프트웨어 모듈은 IEEE 1363의 모든 유한체 $GF(p)$와 $GF(2^m)$상의 ECDH(Elliptic Curve Diffie-Hellman)을 지원한다. 본 논문에서 개발된 소프트웨어 모듈은 마이크로소프트 COM 인터페이스를 따르기 때문에 타원곡선 암호 시스템에 대한 깊은 지식 없이 타원곡선 키 교환 응용 소프트웨어를 쉽게 개발할 수 있다. ECDH를 위한 타원곡선 정수 곱셈 알고리즘으로 $GF(p)$상에서 Right-to-Left 바이너리, $GF(2^m)$상에서 Lopez-Dahab Montgomery를 사용하였으며, 다항식 기저를 사용할 경우 가장 좋은 성능을 보였다.

1. 서론

타원곡선 암호 시스템(Elliptic Curve Cryptosystem: ECC) 기반 보안 소프트웨어를 개발하기 위해서는 유한체 연산 및 타원곡선에 대한 깊은 지식을 필요로 하기 때문에 RSA나 Elgamal과 같은 다른 암호 시스템에 비해 구현이 상당히 어렵다. 따라서 ECC기반 보안 소프트웨어를 개발하기 위해서는 상당히 많은 시간과 노력이 필요하다. 이러한 문제점 때문에 개발자들은 미리 만들어진 ECC 소프트웨어 보안 모듈을 요구할 수도 있다. 더욱이 최근 윈도우기반 소프트웨어 개발 과정에 있어 대부분의 소프트웨어 모듈은 COM 인터페이스를 지원한다. 이는 소스코드 라이브러리 형태에 비해 훨씬 빠르고 쉬운 소프트웨어 개발 환경을 제공할 뿐만 아니라 윈도우 기반 소프트웨어 개발 언어와 툴에 독립적이다. 따라서 각 암호 알고리즘의 COM 소프트웨어 모듈의 개발은 바람직하다[6].

본 논문에서는 ECC에 대한 깊은 지식 없이 ECDH 응용 소프트웨어를 쉽게 개발할 수 있는 COM 모듈을 설계 및 구현한다. 이를 위해 우리는 IEEE 1363[2]의 모든 유한체 $GF(p)$, $GF(2^m)$상의 연산 알고리즘과 타원곡선 정수 곱셈 알고리즘의 자료구조를 정의하고, COM 인터페이스를 설계 및 구현한다. 또한 ECDH 응용을 위해 부가적으로 의사난수발생기(Psuedo Random Number Generator: PRNG)의 인터페이스를 설계 및 구현한다. 그리고 ECDH 소프트웨어 모듈의 성능평가를 하였으며, $GF(2^m)$상의 다항식 기저를 사용할 경우 가장 좋은 성능을 보였다.

2. ECDH

ECDH는 임의의 두 사용자가 안전한 랜덤 키를 사용할 수 있도록 한다. 이 프로토콜은 타원곡선상의 이산대수 문제에 기반한다. 타원곡선 알고리즘을 이용한 키 교환은 다음과 같이 이루어진다. 선택된 타원곡선 E상의 임의의 점 B를 선택한다. 그리고 사용자 A, B는 자신의 개인키로 점 B와 계산하여 각각의 공개키를 생성한다.

$$P_A = k_A B, \quad P_B = k_B B \tag{1}$$

생성된 공개키를 A, B가 서로 교환하고, 전달 받은 상대방의 공개키와 자신의 개인키를 계산하면,