여 웹상에서 알고리듬 솔루션을 구현하였다. 기존의 알고리듬은 개인 컴퓨터 에서만 그 결과를 알아낼 수 있었으나 본 논문에서 개발한 C API는 웹상에서 편리하게 솔루션을 제공하였다. 또한 서로 다른 운영체제에 존재하는 웹 서버와 데이터베이스 서버를 C API를 이용하여 서버간의 데이터를 상호 교환하게 하여 기존의 기능을 제공하게 되었다. CGI나 PHP의 문제점인 데이터의 전송방식Post방식으로 인한 해커들로부터의 해킹위험을 본 논문에서 개발한 C API가 제공하는 인터페이스에 의해 해커들로부터의 위험부담이 줄어들었다.

앞으로의 연구 과제는 C API를 WIN API처럼 사용자가 손쉽게 사용할 수 있도록 사용자 인터페이스를 개발하는 것이며, 웹상에서 입력되는 무한한 데이터를 데이터베이스에 입력할 수 있도록 MYSQL 데이터베이스에 삽입시키는 하는 인터페이스의 개발이다.

2. 타원곡선 암호시스템의 핵심 연산에 대한 효율성의 비교와 분석

응용수학과 김 건 호
지도교수 김 재 환

무선단말기 보급의 증가와 더불어 무선인터넷 사용자가 급속하게 증가하고 있는 추세와 비교해서 현재의 무선인터넷의 보안 수준은 초기 단계에 불과 하다고 할 수 있다. 이는 무선단말기와 무선인터넷의 특수한 환경과 밀접한 연관이 있다. 즉, 기존의 유선의 장비와 비교해 볼 때 낮은 통신의 대역폭을 가지며, CPU와 메모리의 리소스가 작고, 배터리의 수명이 짧으며, 사용자의 인터페이스가 부족하다는 것 등이다. 그러나 이러한 제약에도 불구하고 무선단말기를 이용한 무선인터넷의 사용이 증가하는 이유는 이와 같은 제약이 계속해서 보완되고 있으며, 또한 기존의 On-Line 시스템에서 제공하지 못하는 이동성과 편의성을 동시에 제공한다는 것이 주요한 요인으로 작용하고 있다. 이러한 무선인터넷의 효용성에 기초한 무선인터넷의 발전과 발맞추어 무선 환경의 보안 문제는 아주 중요한 분야이다. 이와 함께 무선시스템의 IWF 망 개방 정책에 따라, 기존의 On-Line 시스템과의 연계가 이루어지고 있다. 망 개방이 완전히 이루어지게 되면 유선과 무선의 호환성이 보장되는 보안 대책이 강구되어야 한다. 현재 이러한 보안 대책에 대해 여러 학자들과 관련 기업, 연구 기관 등을 통해 계속해서 연구가 이루어지고 있다.

무선인터넷과 망 개방에 따른 유·무선 통합 보안에 대해 현재 여러 가지 방안들이 제시되고 있으나 그중 가장 효율적인 방안으로 주목받고 있는 보안 대책이 바로 ECC(Elliptic Curve

Cryptosystem)이다. ECC는 기존의 On-Line 시스템의 보안을 책임지고 있던 RSA/DSA에 비해 수행속도 면에서나 메모리의 효율적인 측면 그리고 보안성 등에서 이미 RSA/DSA를 상당히 능가하는 것으로 여러 논문들이나 관련자료 등은 말하고 있다. 이러한 ECC를 무선 환경에서 실제 상용화에 적용하기 위해서는 아직까지 여러 가지 문제들이 남아있다. 그 중 가장 핵심이 되는 요인이 바로 ECC의 기반이 되는 타원곡선군의 원소들의 효율적인 연산에 대한 것이다.

ECC는 유한체 위에 정의된 타원곡선(elliptic curve) 위의 점들이 덧셈에 대해 군(group)을 이루며, 이러한 타원곡선군의 원소에 대한 덧셈 연산을 기초로 시스템이 수행된다. 이러한 연산은 타원곡선이 정의되는 정의체에 따라서 달라질 수 있으며, 또한 타원곡선의 형태에 따라서도 달라질 수 있다. 본 논문에서는 이러한 여러 가지 정의체와 타원곡선의 형태에 따른 연산에 대해 현재까지 연구된 다양한 연산방법의 효율성에 대해 비교, 분석을 하였다.

유한체에서 정의된 타원곡선군에서의 상수배는 암호시스템의 효율성에 직접적인 영향을 미친다. 이러한 타원곡선군에서의 상수배를 보다 효율적으로 구현하기 위해서는 많은 연구가 필요하다. 상수배에 관한 연구는 현재에도 아주 활발하게 진행되고 있는 부분이다. 본 논문에서는 구현에서의 효율성을 고려하여 제시된 여러 알고리듬 중 Binary Method와 Binary NAF Method, Sliding Window Method를 중심으로 연구하였다. 효율성은 주로 상수배에 소요되는 수행시간과 연관되며, 또한 메모리의 효율적인 사용과도 관계된다. 이와 같은 효율성에 근거하여 각각의 알고리듬에 대해 수행시간을 비교, 분석하였다. 그 결과 Binary NAF Method가 연구한 알고리듬 중 가장 효율적임을 알 수 있었으며, 그 외 Binary Method와 Sliding Window Method도 암호 시스템에 적용하기에 무리가 없음이 판명되었다. 그러나 이러한 각 알고리듬이 근소한 차이의 수행시간을 나타내었다는 것을 볼 때, 실제적인 사용에서의 차이는 거의 느낄 수 없을 것으로 기대 되었다. 장기적인 시각으로 본다면, 이러한 상수배 알고리듬은 앞으로도 많은 연구에 의해 더욱 향상된 성능을 갖는 알고리듬이 개발 되어야 할 것이다.

앞으로 무선 단말기나 유선과 무선이 통합된 환경에서의 암호시스템에 적용하기 위해서는 향후의 보안 수준을 고려한다면 더욱 많은 계산량이 요구되므로 상수배 알고리듬의 개선이 불가피해 질 것이다. 전혀 새로운 암호시스템이 나오지 않는 한은 현재의 RSA/DSA에서 ECC로의 전환은 일반적인 생각으로 인식되고 있으며, 또한 표준화 등도 그 동향을 뒷받침하고 있다. 차후 새로운 암호시스템이 나오더라도 다시 암호시스템의 전환이 일어나기 전까지는 상당시간이 소요될 것이므로 ECC의 상수배 연산 알고리듬의 개선은 중요한 문제이다.