1. C API를 이용한 웹 기반의 Solver에 관한 연구

응용수학과 김 성 화
지도교수 김 재 환

현재 인터넷의 사용량 증가에 따라 많은 웹 사이트가 만들어지고 있다. 하루에도 몇 만개의 사이트가 만들어져서 사용자에게 정보를 제공하고 있다. 그러나 현재 사용자에게 제공되는 거의 대부분의 사이트는 단순히 정보를 보여주는 것에 그치고 있다. 이제는 단순히 정보만을 제공하는 사이트보다는 정보의 가공에 의한 새로운 솔루션을 제공하는 사이트를 사용자들은 요구하고 있다. 서버의 형태도 지금까지는 한대의 컴퓨터에서 모든 과정을 처리하는 형태이나 지금은 여러 컴퓨터에 서버들의 기능을 분산시켜 처리하는 형태로 바뀌고 있다. 이러한 변화에 따라 사용자의 요구를 해결할 수 있는 사이트의 개발이 활발히 이루어지고 있으며 여러 컴퓨터의 사용에 따른 상호간의 자료의 이동을 적절하게 이용할 수 있는 방법에 대한 연구가 활발히 이루어지고 있다.

본 논문에서는 사용자에게 가공의 정보를 웹상에서 편리하게 제공할 수 있는 C API를 개발하였고 여러 대의 컴퓨터에 서버를 두어 사용하는 변화에 맞추고 나아가 여러 컴퓨터가 서로 다른 운영체제라 하더라도 같은 운영체제에서 사용하는 것과 같은 효과를 주는 방법도 개발하였다.

현재 사이트는 대부분이 정보의 가공 없이 자료를 있는 그대로 사용자에게 제공하는 반면 본 논문에서 개발한 알고리듬은 사용자로부터 정보를 입력 받고 그 자료를 C를 이용하여 새로운 솔루션을 구하여 사용자에게 제공하는 형태이다. 또한 여러 컴퓨터를 사용하더라도 현재 웹 사이트에서 제공되는 서비스와 같은 효과를 주고 아무런 불편 없이 사용할 수 있도록 만들었으며 방대해진 자료의 이동으로 인한 자료의 손실이나 자료 손실로 인해 발생하는 웹 사이트의 오류 등을 줄이고자 한다. 그 방법을 본 논문에서는 다른 운영체제라도 자료의 이동이 가능하도록 개발하였다.

본 논문에서는 현재 개인의 컴퓨터에서만 가능한 알고리듬(본 논문에서는 C알고리듬을 사용함)솔루션을 구하는 것을 웹 사이트를 통하여 편리하게 하게 제공할 수 있도록 그 환경을 개발한다. 서로 다른 환경(WINDOWS2000, LINUX)으로 구성된 서버환경에서 C API를 이용하여 자료의 입·출력이 가능하게 한다. 그리고 서로 다른 운영체제의 컴퓨터에 각각의 서버를 설치하여 운영하더라도 같은 운영체제의 컴퓨터에서 서버를 운영하는 것과 같은 효과를 줄 수 있는 환경을 개발한다. 현재의 웹 사이트에서 제공하는 서비스와 아무런 차이 없이 사용자에게 정보를 계속적으로 제공할 수 있도록 하며 사용자에게 가공의 정보를 웹상에서 편리하게 제공할 수 있는 환경을 개발한다.

본 논문에서는 다른 운영체제간의 데이터의 흐름을 C API를 이용하였고 C API를 이용하

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