타원곡선 암호알고리즘을 이용한 Digital Contents 암호화 시스템 구현

Implementation of Digital Contents Cryptosystem using Elliptic Curve Cipher Algorithm

이승혁*, 황선태** (대전대학교 정보통신공학과)
Seung-hyuk Lee, Suntae Hwang

대전시 동구 용운동 96-3 대전대학교 정보통신공학과
Tel +82-42-280-2550, Fax +82-42-280-2559
E-mail : xlove@ice.taejon.ac.kr* Hwang@dragon.taejon.ac.kr**

키워드 : Digital Contents, Smart card, 타원곡선 암호알고리즘, 부분 암·복호화

요 약

최근, 네트워크의 발달로 인해 인터넷을 기반으로 하는 전자상거래가 급속도로 확대되고 있는 추세이다. 이러한 전자상거래는 여러 가지 장점에도 불구하고 개방형 네트워크의 특성상 거래 전반에 걸친 정보들이 자칫 노출될 수 있다는 문제점을 지니고 있다. 따라서, 이와 관련하여 정보보호 문제를 해결할 수 있는 안전한 장치가 필요한데, 이러한 장치들 중의 하나로 제시되고 있는 것이 암호 알고리즘을 이용한 암호시스템이다.

본 논문에서는 최근 유료화 추세에 따른 디지털 컨텐츠들의 정보보호를 위해 공개키 기반구조에서 스마트카드를 이용하여 디지털 정보의 권한을 효율적으로 관리함으로서 정보를 보호하고자 한다. 이와 같은 목적을 달성하기 위해서, 타원곡선 암호 알고리즘을 이용하여 키의 생성 및 분배 문제를 해결하고, 정보의 암복호화 시간을 단축하며 서버의 부하를 감소시키는 부분 암호화 기법을 제시하였다.