암호화 알고리즘의 패턴 인식 Feasibility

신승원 박종진 최종욱
상명대학교 첨단정보기술연구소 숭실대학교 컴퓨터공학과 상명대학교 정보통신학부

Feasibility of Pattern Recognition of Encryption Algorithms

Seung-Won Shin
Advanced Information Technology Laboratory, Sangmyung University
swshin@oak.sangmyung.ac.kr

Jong-Jin Park
Department of Computer science, Sangmyung University
spel@chollian.net

Jong-Uk Choi
School of Information and Telecommunications, Sangmyung University
juchoi@pine.sangmyung.ac.kr

요 약

본 연구에서는 암호화 알고리즘의 안전성을 평가하기위해 암호화된 문장의 패턴 인식 가능성에 대해 연구하였다. 암호화 알고리즘의 출력정보를 시스템의 출력 신호로 간주하고 신호처리 기법을 응용하여 암호문의 특성을 분석하였으며 시영역(time domain)의 분석은 카오스 이론을, 주파수 영역(frequency domain)은 이산 푸리에 변환을, 시-주파수 영역 분석을 위해서는 웨이브렛을 각각 활용하였다.

본 연구는 다양한 암호화 알고리즘으로 출력된 암호문은 신호처리 관점에서 모두 무작위하고 불규칙하여 일정한 규칙성을 발견하는 것이 불가능한 것으로 알려져 있으나, 암호화 알고리즘별로 나타나는 불규칙성에 내재된 패턴을 통해서 암호문이 어떤 알고리즘으로 생성되었는가를 식별할 수 있는가에 초점을 두고 실험하였다. 이에 DES, IDEA, MD5등의 암호화 알고리즘으로 생성한 암호문을 분석하여 카오스 분석과 푸리에 분석, 웨이브렛 분석의 결과를 종합적으로 활용하여 각각의 암호문을 출력한 시스템, 즉 암호화 알고리즘을 식별할 수 있다는 가능성을 찾아냈다. 또한, 암호화 알고리즘의 주기성은 본 연구를 통해서는 뚜렷이 관측할 수 없었으나, 보다 고차원 위상공간으로 투영시켜 분석한다면 주기성도 관측할 수 있을 것으로 판단된다.