네트워크 환경 적용을 위한 혼합형 암호시스템 설계에 관한 연구

강 필 중, 이 선 근, 김 환 용
원광대학교 전자공학과
firsthidden@hanmail.net

Study on the Hybrid Cryptosystem Design for Application of Network Environment

Pil Joong Kang, Seon Keun Lee, Hwan Yong Kim
Wonkwang University

요 약

본 논문에서는 정보화 사회와 더불어 네트워크 환경에서 사용하는 여러 시스템들의 정보보안을 위한 보안 시스템을 연구하였다. 이에 따라 복잡성 및 낮은 처리 속도 등의 문제를 해결하기 위하여 블록 및 스트림 방식을 적용한 대칭형 기반 혼합형 암호 시스템을 설계하였다. 인증 기능을 포함한 대칭형 기반 혼합형 암호 시스템은 처리 속도와 계산량이 비대칭형보다 우수한 성능을 가지고 있다. Synopsys 1999.10과 ALTERA Quartus II ver 3.0으로 시스템을 설계하여 시뮬레이션을 한 결과 제안된 혼합형 암호 시스템은 네트워크 환경에서 정보보안이 필요한 분야에 매우 효율적인 지원과 성능을 제공할 것이다.

I. 서론

현대 사회는 수많은 정보를 필요로 하는 고도의 정보화 시대이다. 이런 정보화 물결과 더불어 산업 및 사회 전반에 걸쳐 정보의 중요성은 점점 심화되고 있다. 특히 인터넷과 같은 네트워크를 기반으로 한 대량의 정보 교환이 급속히 증가하는 추세이다. 그러므로 네트워크에 적용 가능한 보안 시스템을 사용하는 것이 매우 중요하다[1].

1990년대까지 사용되어온 대부분의 스트림 암호알고리즘은 LFSR(Linear Feedback Shift Register)을 기본으로 하여 여러가지 비선형적 결합을 통해 주기가 긴 키 스트림을 발생하는 형태가 일반적이었다. 이런 형태는 하드웨어 구현에 용이하고 안전도를 수식적으로 표현할 수 있는 장점이 있지만 소프트웨어의 구현성이 문제가 되어 최근에는 RC4, SEAL3.0, ISAAC 등의 알고리즘과 혼합형 알고리즘이 제안되고 있다[2][3][9].

본 논문에서는 네트워크 환경에 적합하도록 블록 및 스트림 암호알고리즘에 기반을 둔 혼합형 암호알고리즘을 제안하였다. 제안한 혼합형 암호알고리즘을 이용하여 네트워크 환경에 적합한 암호시스템을 Synopsys ver 1999.10으로 설계하였고 40MHz의 시스템 속도 환경에서 모의실험 및 검증한 결과 단일 라운드로 640Mbps의 데이터 처리율을 확인하였다.[2][8].

II. 기존 대칭형 암호시스템

블록 암호알고리즘은 DES와 같은 형태인 Feistel 구조와 치환(substitution) 및 재배열(permutation)을 반복하여 사용하는 SPN(Substitution and Permutation Network) 구조 등으로 구성된다. Feistel 방식은 한 라운드에 평문의 일부만 처리하여 병렬처리 효율이 낮은 반면 라운드 함수 설계의 융통성과 암·복호화 과정이 동일하다는 장점을 가진다. SPN 방식은 한 라운드에서 전체 평문을 암호화하므로 병렬처리가 가능하여 속도가 빠르지만 복호화를 고려하여 암호화 과정을 설계하므로 설계의 폭이 좁은 단점을 가진다[3][5][7].

Feistel 방식의 암호화는 반복되는 블록 암호화의 특