고속 데이터 처리용 ARIA 암호시스템 및 디바이스 드라이버 설계

*김무섭, *최용제, 전성익
*한국전자통신연구원
*{gomskim, choiyj, sijun}@etri.re.kr

Design of ARIA Cryptographic System and Its Device Driver for High Speed Data Processing

*Moo-seop Kim, *Yong-je Choi, and Sung-ik Jun
*Electronics and Telecommunications Research Institute (ETRI)

요 약

본 논문은 고속 네트워크 시스템에 적용 가능한 고속 ARIA 암호 시스템의 설계에 관한 것으로써, 고속 데이터 처리를 위한 ARIA 암호회로의 설계 및 설계된 고속 ARIA 암호회로를 윈도우 XP 환경에서 효율적으로 사용하기 위해 필요한 디바이스 드라이버의 설계에 관한 것이다. 설계된 고속 ARIA 암호회로의 효율적인 적용을 위해 고속 PCI 인터페이스를 사용하였으며, 데이터 입·출력에서 발생하는 데이터의 지연을 방지하기 위하여 DMA 방식을 사용하는 PCI 인터페이스용 마스트 모드의 디바이스 드라이버를 설계하였다. 본 논문에서 설계된 ARIA 암호회로는 750 Mbps 의 성능을 가지며, 윈도우 환경에서 활용 가능하도록 설계된 디바이스 드라이버는 데이터 전송과 수신에 각각 450 Mbps 의 전송률을 가지므로 기존 암호 시스템에서 발생하던 암호 데이터 전송에서 발생하던 지연문제를 해결하여 고속 전송이 가능하며, 고속 PCI 인터페이스를 사용하는 시스템에 쉽게 적용하여 활용할 수 있으므로 시스템의 보안성을 향상 할 수 있다.

. 서론

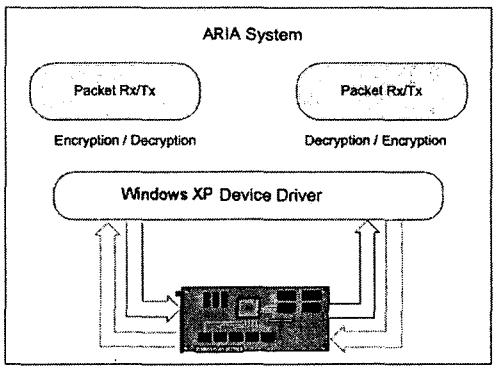
오늘날 정보화 사회에서 음성, 화상, 데이터 등과 같이 다양한 종류의 정보를 교환하고 저장하는 시스템에서 데이터 및 시스템의 신뢰성과 안전성은 필수적이며, 이러한 신뢰성을 제공하기 위해 다양한 암호 알고리즘이 적용되어 사용되어지고 있다. 특히 데이터의 안전한 전송을 위해 사용하는 암호 알고리즘의 경우, 최근 미국 국가 표준 알고리즘으로 채택된 AES 나 한국의 ARIA 암호 알고리즘과 같이 국가기간망에서 보안 확보차원에서 각 국가별로 고유의 알고리즘을 채택하여 사용하고 있다. 최근 이러한 암호 알고리즘들을 활용하여 고속의 데이터를 처리를 목적으로하는 다양한 하드웨어 구현 연구와 결과들이 발표되어져 왔다.

그러나 고속 암호회로들을 실제 시스템에 적용하여 사용하는 경우, 암호 회로와는 별개로 암호 연산에 필요한 데이터의 전송과 결과값을 읽어오는데 걸리는 시간이 암호 연산처리 시간보다 더 길어서 시스템의 전반적인 성능을 감소시키는 원인으로 지적되어 왔다. 이러한 문제는 암호회로를 적용하는 시스템의 인터페이스를 고려하지 않은 상황에서 암호회로를 설계하였으므로 발생하는 문제이다.

본 논문에서는 이러한 문제를 해결하는 방안으로 고속 데이터 처리를 위해 최근 국가 표준 암호로 선정된 ARIA 암호알고리즘을 위한 하드웨어를 설계하였으며, ARIA 암호 회로의 고속 데이터 전송과 효율적인 활용을 위해 상용 PCI 인터페이스 회로를 적용하여 인터페이스 회로에서 발생하는 데이터 지연 현상을 해소하였다. 또한 고속 PCI 인터페이스의 구동을 위해 응용 프로그램에서 ARIA 암호회로로 데이터를 전송하고 읽어오는데 필요한 전반적인 제어를 위한 디바이스 드라이버 프로그램을 설계하였다. 특히 데이터의 전송에 걸리는 시간을 줄이기 위해 마스터 모드의 디바이스 드라이버를 설계하였으며, PCB 형태로 제작된 ARIA 암호 회로와의 연동을 고려하여 설계하였다.

II. 본론

본 논문에서 설계하는 고속 데이터 처리용 ARIA 암호 시스템은 데이터 패킷의 고속 암호화 또는 복호화 기능을 수행하기 위한 시스템이다. 설계된 암호 시스템을 상용 컴퓨터에 장착하여 검증하기 위하여 고속 PCI 인터페이스를 사용하고, PCI 카드 형태의 시험 시스템을 제작하여 윈도우 운영환경에서 구동되도록 설계하였다.



[그림 1] 고속 데이터 처리용 암호 시스템