팩시밀리용 암호 시스템 개발

유병욱* · 한상수**

Development of Encryption System for Facsimile

Byong-wook Yoo* · Sang-soo Han**

요 약

자동으로 암호문과 평문의 수신이 가능한 팩시밀리용 암호통신시스템을 개발하였다. 개발된 암호시스템은 128bit SEED알고리즘을 적용하였으며 1024bit 모듈러, 256bits Exponent의 Diffie-Hellman 키교환방식을 적용하였다. 암호문 고속 전송을 위해 Dual FAX Server를 개발함으로써 실시간 암호통신을 구현하였다. Diffie-Hellman 키교환 시 등록된 시리얼번호를 서로 교환시켜 안전한 키 교환이 가능하게 하였다.

ABSTRACT

We developed the facsimile encryption system that could send/receive the cipher text and plain text automatically. This facsimile encryption system is adopting the 128bits SEED encryption algorithm , 1024bits modular and 256bits exponential Diffie-Hellman key exchange method. We can reduce the cipher text transmitting time by developing the Dual Facsimile Server, it can make the real time encryption communication. Key is safely exchanged by the exchanging the listed serial numbers when the Diffie-Hellman key exchanging.

키워드

암호통신시스템, 팩스 비화기, Secure FAX, Diffie-Hellman Key Exchange

Ⅰ. 서 론

최근 컴퓨터의 향상과 정보통신 기술의 발달로 인하여 통신로의 다양화가 더욱 활발해지고 정보유통은 폭증하고 있으며 통신의 상업화는 한층 가열되고 있는 추세이다.

비례하여 통신정보의 불법도청, 불법용도 변경, 개조 등 악용사례가 증가하고 있으며 많은 사람들이 도청에 대비한 정보보호에 대하여 심각하게 고민하기 시작하고 있다. 도청문제는 국가 경제적 측면에서 문제를 발생시킨다. 테러 또는 불순세력에 대한 폭력 및 차단, 감시를 위하여 극히 부분적으로는 합법적인 감청이 필요하다. 문제는, 산업부분에서의 도청으로 인한 전략 및 개인정보유출이다. 이는 매우 큰 재산권의 손실로 이어진다. 중요문서의 유통에 대해 기업들은 전혀 대책수립이 되어 있지 않고, 도청에 대한 개념조차 없다. 일부 대기업인 경우 보안장비를 가동하고 있는 경우도 있지만 일부 임원들인 경우에만 사용하고 있는 편이다[1].

한편, 문서를 원거리에 전송할 때 가장 많이 사용하는 방법이 팩시밀리를 이용하는 것이다. 팩시밀리는 기존의 전화선을 이용할 수 있고, 전화선이 설치되어 있는 곳이라면 원거리의 사무실이라도 서류 전송이 용이하기 때문

* (주)하이드로소닉

** 경원전문대학 정보통신과

접수일자 : 2005. 11. 22

에 사무실의 기본 필수기기가 되어 있으며 오늘날 전 세계적으로 가장 많이 사용되는 통신기기중 하나이다.

E-mail에 의한 문서유통이 많은 것 같으나 아직도 전 세계에는 PSTN(public switched telephone network)사용자가 가장 많으며 특히 서명과 공문서의 유통은 팩시밀리를 사용하고 있다. 최근에 개인정보보호가 매우 중요한 이슈가 되고 있는 상황에서, 통신의 편리하기 때문에 은행거래 또는 각종 가입신청서 등에 중요정보가 나타난 상태로 팩시밀리에 의해 문서를 전송하는 것은 큰 문제를 일으킬 수 있다. 팩시밀리를 이용하여 중요한 개인정보를 전송하면 번호를 잘못 입력하거나, 도청당하면 고객정보가 유출되어 고객에게 큰 손해를 끼칠 수가 있다. 실제로 보안을 유지해야 하는 민감한 문서를 전송하면서 외부로 문서 유출이 되는 경우가 종종 발생하고 있다[1-9]. 이에 따라 보안 유지를 위해 일반 우편이나 인편을 사용하여 전달해야 한다면 긴급과 보안을 필요로 하는 문서의 신속한 처리는 매우 어렵다.

일반적으로 위와 같은 문제 발생시, 통신보안을 위해 사용하는 것이 비화기이다. 비화기란, 전화에 의해 전송되는 신호를 원래의 메시지에 전혀 영향 없이 조작함으로써 선로중간에서 제3자에 의해 도청되는 것을 방지하는 것을 말한다. 그러나 최근에 다양한 통신수단이 발달되면서 비화기의 적용영역도 매우 넓게 확장되었고 팩시밀리용 비화기, 또는 VPN(Virtual Private Network) 까지도 일종의 비화기로 통칭하고 있다. 따라서 이제 비화기는 암호통신 단말기라는 표현이 정확하다.

통신보안을 위한 비화기의 원리는 다음과 같다. 송신측의 팩시밀리에서 읽은 문서의 정보를 분할하여 송신측에서 수신측과 사전에 약속된 암호를 입력한다. 수신측에서도 동일한 암호를 입력한 후에 다수개의 정보로 분할한다. 랜덤하게 다수개의 정보를 전송하고 수신에서는 동일한 순서로 복원한다. 이러한 비화방법은 전송 규칙이 알려질 수 있으므로 보안성이 매우 떨어진다. 보안성을 향상시키기 위해서는 암호알고리즘을 채택해야 하다. 하지만 암호화 기능을 수행하면 통신 속도의 저하로 인하여 시스템 구성 비용이 추가되는 단점이 있다.

과거의 스크램블(Scamble)팩시밀리는 기존의 팩스에 연결 가능하고 가격이 저렴하였으나 보안성의 문제로 사라지고 있다[1-9].

현재의 팩시밀리용 비화기는 기존의 팩시밀리를 사용하는 것이 아니라 팩시밀리 엔진 내부에 암호화 기능을 탑재한 별도의 전용 암호팩시밀리의 형태이다. 이러한 암호팩시밀리는 일반팩스와 겸용으로 사용하지 못하며 또한 기존의 팩시밀리에 부착하지 못한다. 따라서 구입 및 사용을 위해 비용이 많이 발생하는 문제를 가지고 있으며 기업에서 쉽게 사용하기가 어려웠다.

따라서 본 논문에서는 구입비용을 감소시키고자 기존의 팩시밀리에 별도로 부착하는 형태의 단말기로 개발하고 사용의 편리성을 제공하기 위해, 단말기가 평문에 의한 팩시밀리통신과 암호 통신이 모드 전환되어 송신하고 암호문 또는 평문에 관계없이 자동 모드전환 되어 수신되는 저비용의 팩시밀리용 암호 단말기를 개발하였다.

평문의 송수신시는 FAX모뎀을 채택하여 기능을 수행하도록 하였으며 암호문의 송수신시에는 PSTN모뎀을 채택하여 수행하도록 하였다.

암호처리시 전송속도 감소를 위해서 Dual FAX Server를 제안함으로써 실시간 암호통신이 가능하도록 하였다.

팩시밀리 암호통신에 있어서 Diffie-Hellman 키 교환의 문제는 공격자가 수신 측의 암호팩시밀리를 제거하고 중간에 정상적인 수신자로 위장하여 공개키를 송신자에게 보내는 경우이다. 이를 방어하기 위해 송수신자에 대해 등록된 ID를 Diffie-Hellman 키 교환시에 포함시켰다. 수신자에 대한 정보를 확인하게 하여 안전한 암호통신을 수행하도록 하였다.

Ⅱ. 자동모드 변환의 팩시밀리 암호 시스템 구성

1. 시스템의 개요

기존의 팩시밀리를 활용하고 평문 및 암호통신을 수신하기 위해서는 팩시밀리 엔진이 제공되어야 한다. 암호문과 평문 통신을 자동 인식하여 처리하기 위한 시스템 구성을 그림 1에 나타내었다. 암호통신을 하기 위해서는 송신자가 모드변환기를 암호모드로 설정하면 된다. 암호모드 변경은 스위치를 1로 연결하게 하고, 부착된 송신팩시밀리로부터 받은 수신처의 DTMF(Dual-Tone Multi Frequency)정보와 평문이 버퍼에 저장된다. 암호시스템에 의해 암호화 된 후 PSTN모뎀을 통해 망에 연결되어 있는 수신처로 전송된다. 수신 암호단말기는 수신된 신호가 팩시밀리신호인지 모뎀신호인지를 신호 해석기에서 분석한다. 모뎀신호이면 암호화 모드이므로 스위치를 1로

연결하여 PSTN 모뎀으로 입력되고 평문으로 복호화 한 후 부착된 수신 팩시밀리로 전송된다. 평문 통신시에 모드변환기의 동작모드를 평문모드로 설정하면 스위치는 2로 연결되고 부착된 팩시밀리로부터 전송된 수신처의 DTMF와 평문은 수신처의 팩시밀리로 전송된다. 수신처에 팩시밀리용 암호단말기가 연결되어 있다면 신호해석기에서 팩스신호로 인식한 다음, 수신측 팩시밀리로 평문이 전송된다.

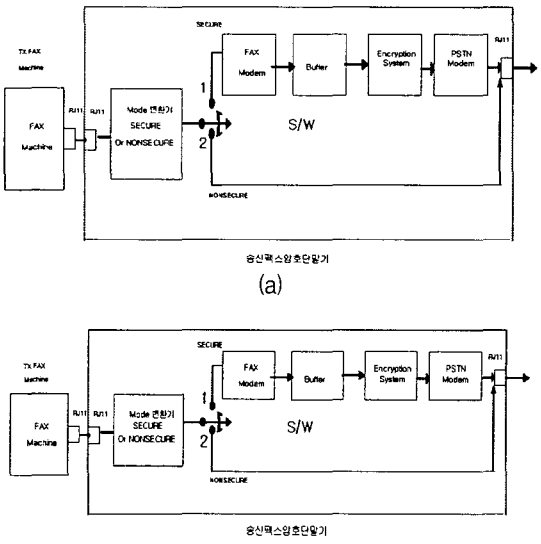


그림 1.(a)FAX 암호단말기의 송신시스템 구성도.
(b)FAX 암호단말기의 수신시스템 구성도.
Fig..1. (a)Diagram for the FAX encryption system.(TX)
(b)Diagram for the FAX encryption system.(RX)

그림 2는 시스템의 운영을 위한 각 장치들의 상태에 따른 동작 순서도이다. 송신 팩시밀리에서 송신을 개시하면 송신암호단말기가 정상인가를 판단한다. 전원이 꺼져 있으면 송신팩스에 에러로 처리하며 정상이면 송신 암호단말기의 모드를 점검한다. 송신암호단말기의 모드가 '암호모드(SEC)'이면 수신암호단말기에 암호통신 수신 준비를 요구하고 수신된 암호문을 복호화 후 수신측 팩시밀리에 전송한다. 송신암호단말기의 모드가 '평문모드(NONSEC)'이면 수신측에 수신암호단말기가 설치되어 켜져 있거나 또는 팩시밀리인 경우에는 평문으로 정상 수신한다.

2. 암/복호시스템의 구성

그림 3은 본 논문에서 구현한 암호 시스템의 블록도를 나타낸 것이다. 키 생성 및 교환은 1024bit 모듈러, 256bit의 Exponent인 Diffie-Hellman 키 교환을 사용하였으며 암호알고리즘으로는 국내 TTA 표준인 128bit SEED알고리즘을 사용하였다. 암호데이터 전송시 에러를 감소시키기 위한 전송모드는 OFB(Output Feed Back)모드를 적용하였다[12].

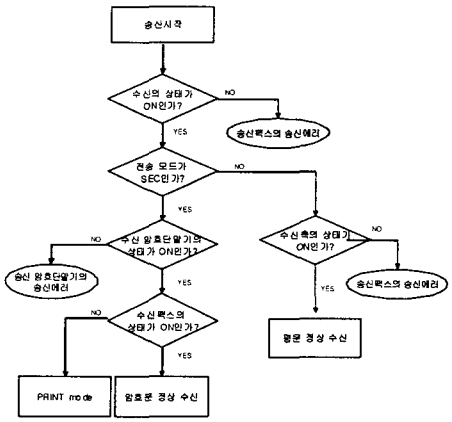


그림 2. 동작 상태에 따른 순서도.
Fig. 2. Flow chart of operation.

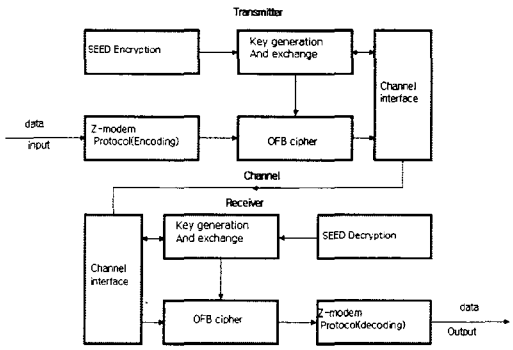


그림 3. 구현된 암호시스템 블록도.
Fig. 3. Block diagram of encryption system.

Ⅲ. 설계 및 구조

1. 고속 전송 처리를 위한 Dual FAX Server의 설계

암호통신시 일반적인 암호단말기는 부착된 로컬 팩시밀리로부터 평문을 받기 위해 양측간 통신로를 구성하며 통신이 종료가 되어야 리모트의 암호단말기와의 통신을 수행할 수가 있다. 이러한 한계로 실시간 통신이 매우 어렵다.

고속전송처리를 위해서 다음과 같이 Dual FAX Server를 구성하였다. 부착된 로컬 팩시밀리와 암호단말기간 평문 통신처리를 위해 FAX모뎀을 구성하였으며 리모트 암호단말기와 단말기 간 통신에는 PSTN모뎀을 구성하였다.

Dual FAX Server는 로컬 팩시밀리와의 데이터 송수신 및 전화선을 통한 리모트 PSTN모뎀과의 데이터 송수신을 담당하는 실질적인 기능을 하는 인터페이스 서버이다. 최상위 레이어에서 두개의 모뎀 디바이스와 PLD 디바이스를 제어하고 보안기능이 필요할 경우 팩스 데이터에 암호화를 한다. 리모트 PSTN모뎀과의 데이터 송수신 프로토콜은 z-modem을 통해 구현되었다.

그림 4는 기능별로 본 Dual FAX Server 구조이다. 프로그램은 표 1과 같이 모두 3개의 Task로 이루어져 동작한다. 처음 구동시에 모뎀과 PLD 디바이스를 초기화하고 이벤트의 발생을 감시하는 메인 Task와 송신측에서 리모트로 팩스 데이터를 내보내는 기능을 담당하는 Task, 그리고 수신측에서 로컬로 팩스로 데이터를 내보내는 기능을 담당하는 Task와 같이 3개의 Task로 이루어져 있다.

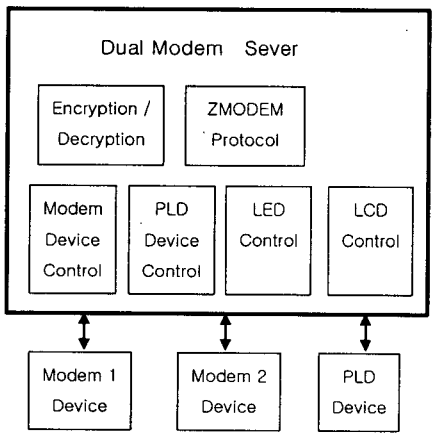


그림 4. Dual FAX Server의 구성.
Fig. 4. A structure of the dual facsimile Server.

여러 개의 Task를 만들어 처리한 이유는 2개의 모뎀을 동시에 구동하여 내부의 데이터를 빠르게 처리하기 위함이다. Dual FAX Server는 로컬의 팩스 데이터를 수신함과 동시에 리모트로 데이터를 송신할 수 있으며 반대로 리모트의 데이터를 수신함과 동시에 로컬로 데이터를 송신할 수 있다. 제어는 모두 메인 Task가 담당한다. 그림 5는 Task별로 본 Dual FAX Server의 구조를 나타낸다.

표 1. Task.
Table 1. Task.

Task	Task의 주요 기능
main_task	• 모뎀 및 PLD 디바이스 초기화 • 팩스나 전화선, 스위치들로부터 들어오는 이벤트 처리 • 로컬 팩스의 데이터 수신 • 리모트 팩스 서버의 데이터 수신 • 다른 Task의 제어
tx_pstn_task	• 리모트 팩스 서버로 데이터 송신
tx_fax_task	• 로컬 팩스로 데이터 송신

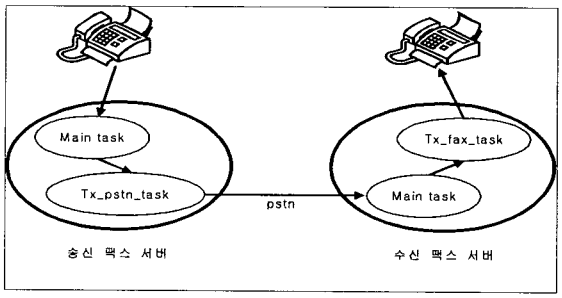


그림 5. Task별 Dual Fax Server 구조.
Fig. 5. Dual facsimile Server with task.

Dual FAX Server는 두 가지 동작 모드를 갖고 있는데 하나는 평문모드(Non-Secure Mode)이고 다른 하나는 암호모드(Secure Mode)이다. 초기화된 Dual FAX Server는 평문모드로 동작하며 보안이 필요할 경우 암호모드로 동작시킬 수 있다. 동작의 전환은 단말기에서 스위치를 누름으로써 가능하다. 평문모드로 동작될 때 Dual FAX Server는 단지 로컬 팩시밀리로부터 수신되는 데이터를 그대로 리모트로 전송하며 수신측 역시 전송된 데이터를 그대로 로컬 팩시밀리로 내보낸다.

이 과정에서 팩스 데이터에 대한 지연은 없다. 암호모드로 동작될 때 Dual FAX Server는 팩스 데이터에 대해 암호화를 처리한다. 암호화된 팩스의 데이터 송수신 과정은

다음과 같다. 수신측 Dual FAX Server는 걸려온 전화의 신호를 통해 일반 팩시밀리에서 걸려온 전화인지 Dual FAX Server로부터 걸려온 전화인지를 판단한다. Dual FAX Server로 걸려온 전화일 경우 송수신간에 암호 모드로 동작하게 된다. 양측은 먼저 시리얼 번호를 교환한 후에 서로 생성해낸 공개키 키를 교환한다. 송신측 Dual FAX Server는 자신의 암호화 키와 수신측 FAX Server로부터 받은 암호화 키를 이용해 팩스 데이터를 암호화하고 암호화된 팩스 데이터를 수신측 FAX Server로 전송한다. 수신측 팩스는 수신된 팩스 데이터를 이전에 주고 받은 두개의 암호화 키를 이용해 복호화 하여 본래의 팩스 데이터를 얻어낸다. 모든 데이터의 송수신을 마친 후에는 양측 모두 평문모드로 되돌아 간다. 그림 6은 평문모드일 때와 암호모드일 때의 FAX Server의 동작을 나타낸다.

그림 7은 위에서 설명한 암호모드일 때의 팩스 서버의 동작 과정을 나타낸 것이다.

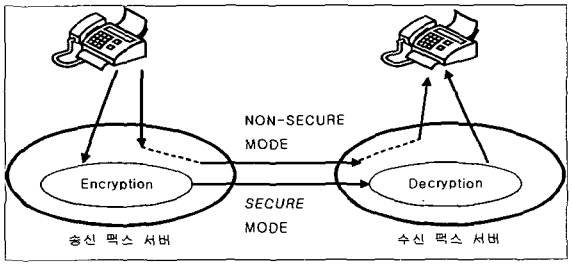


그림 6. MODE별 FAX Server 동작.
Fig. 6. Dual facsimile Server with secure/nonsecure mode.

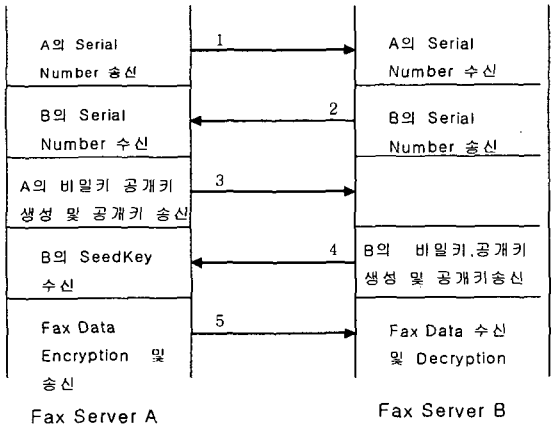


그림 7. 암호모드시 Dual FAX Server 동작.
Fig. 7. Dual facsimile Server operation of secure mode.

데이터의 안전한 송수신을 위해 팩스 서버는 z-modem 프로토콜을 사용하여 팩스 데이터를 교환한다. z-modem은 많은 통신 프로그램에서 널리 사용되고 있으며 대량의 파일 전송이 가능하다. 수신측의 응답을 매번 기다리지 않고 송신측의 주도로 통신을 하여 데이터 처리 속도도 빠르며 CRC-32 에러 검출 방식을 채택해 통신의 정확성과 안정성이 높으므로 채택하였으며 받은 파일에 대하여 이어받기가 가능하다는 장점이 있다.

2. Dual FAX Server의 하드웨어 구조

(1) 내부 블록 다이아그램

본 논문에서 구성한 하드웨어 내부 블록다이아그램을 그림 8에 나타내었다. 그림과 같이Analog Mux로 부터 수신되는 신호를 신호 해석기에 의해 평문인지 암호문인지를 분석하였다. 평문인 경우는 SLIC에 의해 부착된 로컬 팩시밀리로 송신시켰다.

암호문인 경우는 PSTN모뎀에 의해 처리되고 암호기/복호기에 입력시킨다. Diffie-Hellman에 의해 암호 키를 생성한 다음, 암호화 또는 복호화를 수행한다. 프로세서는 암호기 및 모뎀과 팩스엔진의 수행과 시스템의 제어를 수행한다. 내부하드웨어의 구성은 그림 8에서 보는 것처럼 3개의 기능 블록으로 구성되어 있으며, 프로세서 부분과 개발 호스트 사이에는 이더넷과 시리얼을 통하여 연결된다. Flash Write및 시스템 동작 검증을 위해 BDM Port를 사용하도록 구성하였다.

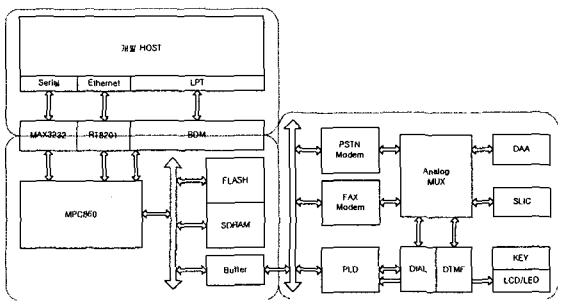


그림 8. H/W의 블록 다이아그램.
Fig. 8. Block diagram of H/W.

프로세서 블록에는 OS 및 응용구동을 위한 FLASH 및 SDRAM으로 구성되고, 모뎀 및 PLD인터페이스를 위한 버퍼로 구성된다.

모뎀 인터페이스부분은 버퍼를 통하여 어드레스 및 데

이터 신호를 전송하게 되며, 2개의 모뎀과 PLD, Analog Mux, SLIC, DAA등으로 구성된다.

(2) 프로세서

CPU는 50MHz로 동작하는 MPC860 프로세서를 사용하였다. 이것은 내부에 Instruction Cache / Data Cache를 각각 4-Kbyte 씩 내장하고 있으며 serial/Ethernet 등의 기능을 포함하고 있다.

전체 시스템을 구동하기 위한 OS로는 임베디드 리눅스를 사용하였고, OS 구동을 위하여 8M Byte의 FLASH와 32M Byte의 SDRAM을 사용하였다.

시스템의 메모리맵은 그림 9과 같다. 전체 8M byte의 FLASH영역을 4개의 영역으로 분할하여 사용하였다. 보드의 초기화 및 OS의 동작을 위한 tftp download, FLASH Fusing을 위한bootloader와 Linux kernel 부팅시 parameter를 위한 저장 공간, 압축된 Linux kernel 및 RAMDISK 저장을 위한 영역등 으로 분할되어 있다.

Bootloader는 ppcboot-1.2를 변경하여 사용하였으며, udp방식을 사용하여 tftp server로부터 압축된 kernel(약 340Kbyte)/RAMDISK(2.7MByte)을 SDRAM에 저장하거나 FLASH에 저장하는 기능을 가지고 있다.

"bootm" 명령을 사용하여 SDRAM에 저장된 kernel image로 부팅하거나 자동부팅 기능을 사용하여 FLASH 의 kernel 코드를 실행할 수 있다

Boot parameter 영역은 임베디드 리눅스 부팅을 위해 kernel에 전달할 값들을 가지고 있으며, 이 영역에 IP와 Ethernet mac address와 부팅을 위한 옵션들을 저장 한다

Linux Kernel과 Ramdisk는 압축된 형태로 저장되어 있으며, 약 340Kbyte와 2.7Mbyte의 공간을 차지한다. driver나 application 개발 기간 동안 이더넷을 통하여 SDRAM에 저장하여 사용하였으며, 개발 완료 후 FLASH에 압축된 형태로 저장하도록 하였다

Dual Fax Server는 FAX의 입출력을 위한 FAX Modem 1개와 PSTN Line 접속을 위한 PSTN Modem 1개로 구성된다. 각각의 모뎀을 위한 메모리 공간을 0x06000000과 0x07000000으로 할당하였으며 각각 8 byte 의 메모리공간을 사용한다.

그림 10에 모뎀과 PLD에 대한 시스템 메모리 맵을 나타내었다. 보드에 장치된 LED와 LCD 및 DAA/SLIC/Analog Mux/DTMF/DIAL과 관련된 신호의 입력과 제어를 위해 PLD를 0x05000000 영역에 할당하여 사용하였다.

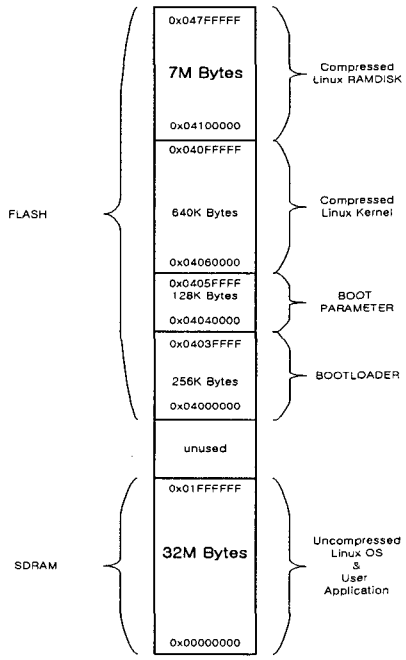


그림 9. 시스템 메모리 맵.
Fig. 9. Memory map for system.

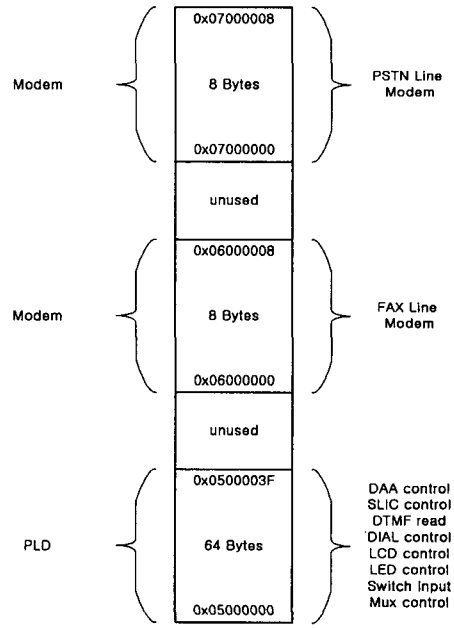


그림 10. 모뎀과 PLD에 대한 시스템 메모리 맵.
Fig. 10. System memory map for the modem and PLD

(3) Modem의 구성

암호화 하여 전송할 FAX Image의 입력이나 복호화된 FAX Image의 출력을 위한 FAX Modem은 14400bps까지 작동 가능하도록 구성하였다. SLIC을 통하여 FAX와 직접 연결되고, 내부의 Dial Tone 생성기와 DTMF detect회로를 사용하여 전화망에 연결된 것과 같은 동작을 수행한다.

그림 11은 사용된 모뎀 디바이스의 구조이다. 암호화된 FAX Image의 송신/수신을 위해서는 PSTN Modem이 사용되며, 외부 PSTN망과 DAA를 통하여 연결된다. 최대 57600bps 수신이 가능하고, 38400bps의 송신이 가능하다. 사용한 모드는 Async 모드에서 19200bps로 고정하여 사용하였다. 이러한 모뎀 구성을 위해 RC56D modem device set는 MCU를 Parallel mode로 설정하여 사용하였으며, 256K의 ROM와 128K의 RAM을 사용하였다. MDP 이외에 음성지원 등의 기능을 갖는 회로는 사용하지 않았으며, MPC860과는 8 Bit Data Bus를 통하여 직접 연결된다.

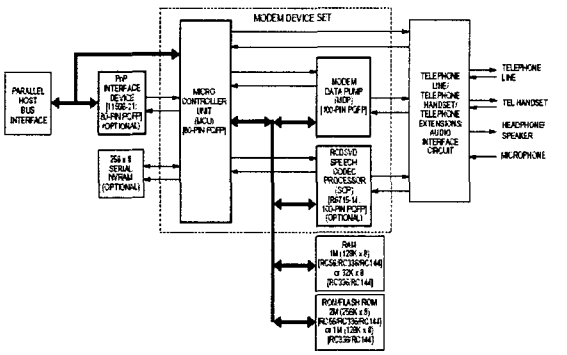


그림 11. Modem Device Set.
Fig. 11. Modem Device Set.

(4) PLD의 기능 설계

PLD에서 DAA/SLIC/Analog MUX 제어신호 생성시켰으며 DTMF Detect 기능을 수행하도록 하였다. 또한 프로그램에 의해 Dial Tone을 생성시켜 사용하였으며 유저인터페이스에 필요한 각종 LCD/LED 제어 및 KEY 입력기능을 설계하였다. 그 외 PSTN Modem/FAX Modem 제어를 수행시켰다. 그림 12는 PLD 내부의 메모리 맵이다.

CS5			7	6	5	4	3	2	1	0
W	0x5000000	Interrupt Mask		FM_OH	FM_OH	SW2	SW1	STD	RING	DET
R/W	0x5000001	Interrupt Pend		FM_OH	FM_OH	SW2	SW1	STD	RING	DET
W	0x5000008	DIAL Control				CE	DIAL3	DIAL2	DIAL1	DIAL0
R	0x5000009	DTMF Detect	STD				DTMF3	DTMF2	DTMF1	DTMF0
R/W	0x500000A	SLIC Control	DET	RING			EZEN	C3	C2	C1
W	0x500000B	Analog Mux				SEL4	SEL3	SEL2	SEL1	SEL0
W	0x500000C	DAA_OH Control								OH
R	0x5000010	Switch Input							PRINT	SEC
W	0x5000011	LED Disp						ERROR	PRINT	SEC
R/W	0x5000020	FM Control								OH
R/W	0x5000021	PM Control								OH
W	0x5000030	LCD Write	D7	D6	D5	D4	D3	D2	D1	D0
W	0x5000031	LCD Control						EN	RS	RW
W	0x5000032	LCD Back Light							EN1	EN0

그림 12. PLD 내부 메모리 맵.
Fig. 12. Intrnal memory map for PLD.

(5)DAA/SLIC/ANALOG MUX(Analog signal)

PSTN라인의 Ring Tip 신호로부터 analog 신호를 분리하여 Analog Mux로 전달시키기 위해 DAA를 구성하였고 DAA는 CPCLARE사의 CPC5604를 사용하였다. 그림13에 사용된 CPC5604의 내부 Block를 나타내었다.

입/출력을 위한 RX/TX 신호와 Off-Hook을 위한 OH#, Ring입력을 위한 RING# 그리고 Caller ID인식을 위한 CID# port를 가지고 있으며 analog와 PSTN라인의 절연은 내부의 Optical Isolation Barrier를 통하여 구현된다. 1500V까지 절연이 가능하도록 설계되었다.

한편, 각종 Ringing에 관련된 기능을 수행하기 위해 SLIC을 구성하였다. 사용된 SLIC은 AMD사의 AM79R79-1JC를 이용하였다. 그림 14에 사용된 AM79R79의 내부 구성을 나타내었으며 이를 사용하기 위해서 -24V 와 -70V 를 생성하는 회로를 구성하여 사용하였다. 또한 Ringing을 위한 20Hz를 PLD에서 생성하여 전달시켰다.

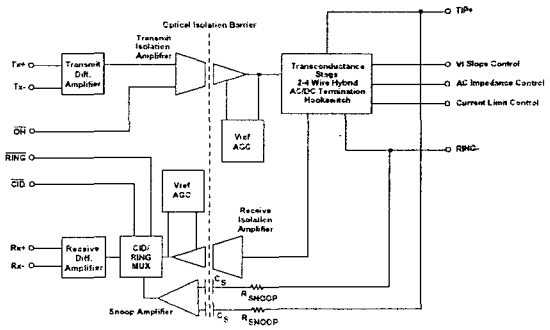


그림 13. CPC5604 Internal Block.
Fig. 13. CPC5604 Internal Block.

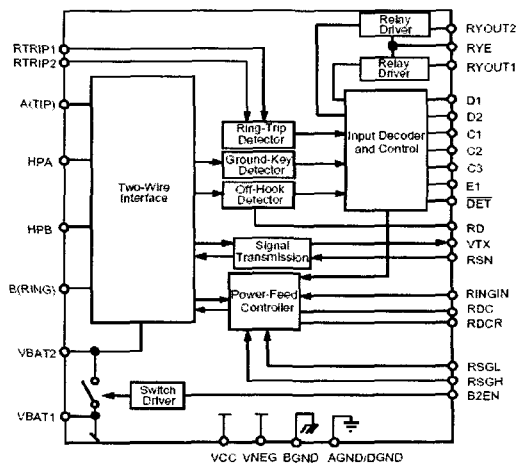


그림 14. AM79R79 Internal Block.
Fig. 14. AM79R79 Internal Block

Analog Mux는 DAA/SLIC/DTMF/DIAL/MODEM들 간의 신호 전달을 위해 사용하였다. 하나의 IC당 3개의 MUX를 갖는 4053을 사용하였다. 각각의 입/출력은 약 2.4V를 기준으로 변화하며, DIAL TONE 발생기의 경우 bypass capacitor와 resister를 사용하여 전압 level을 변경하였다.

암호모드에서의 전송할 데스티네이션에 대한 수신측 번호 처리를 위해 DTMF Detector 및 Dial Tone Generator가 필요하다. DTMF Detector 는 그림 15에 나타낸 CPCLARE 사의 MT88L70을 사용하였으며, 0~9, #, *의 입력의 감지가 가능하다. PLD와의 전달은 STD Pin의 logic '0' state에서 이루어지도록 하였다. STD pin의 falling edge에서 DTMF 입력을 저장한다.

Dial Tone Generator는 CLCPARE사의 M-991을 사용하였다. 그림 16에 사용된 M-991의 내부구조를 나타내었다. 이것으로 Dial Tone을 생성하였고, FAX Modem 과 SLIC이 필요로 하는 off-hook 상태에서의 ring back 과 dial ready tone을 생성시켰다.

V. 결 론

PSTN에서의 팩시밀리용 암호통신 시스템을 개발하였다. 개발된 암호통신 시스템은 기존의 팩시밀리에 부착하는 단말기 형태로 개발함으로써 사용 및 구입비용을 감소시켰다.

신호분석기를 구성함으로써 특별한 조작 없이 자동으로 암호문 및 평문이 송수신 되도록 개발하였다. 또한 암호처리시의 전송속도감소의 문제를 해결하기 위해 Dual FAX Server를 개발하여 실시간 암호문전송이 가능하도록 하였다.

암호통신 시 Diffie-Hellman 키 교환을 구현할 때 안전성에 대한 문제점을 해결하고자 제작 시 시리얼 번호를 입력시켰다. 키 교환 시에 입력된 시리얼번호를 서로 확인시킴으로써 안전한 Diffie-Hellman키 교환 시스템을 구현하였다.

정치 사회적 불안요소가 증가하고 산업스파이에 의한 국내 정보유출이 극심해 지고 있는 현재, 통신보안에 관한 요구가 절실해 지고 있으나 국내 통신보안 시스템의 사용은 미비하다. 따라서 국내기술에 의한 저가의 통신보안 제품의 필요성이 매우 중요하다. 본 논문에서 구현한 국내 표준의 암호알고리즘의 팩스용 암호단말기가 국내 산업보안에 큰 활용이 있기를 기대한다.

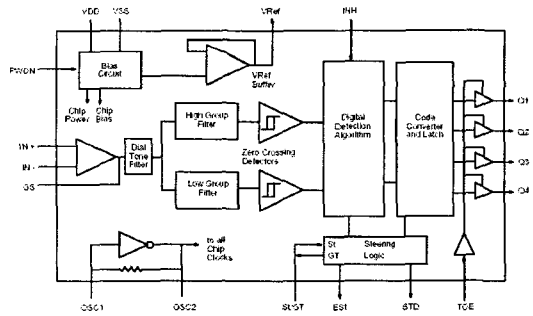


그림 15. MT88L70 Internal Block.
Fig. 15. MT88L70 Internal Block.

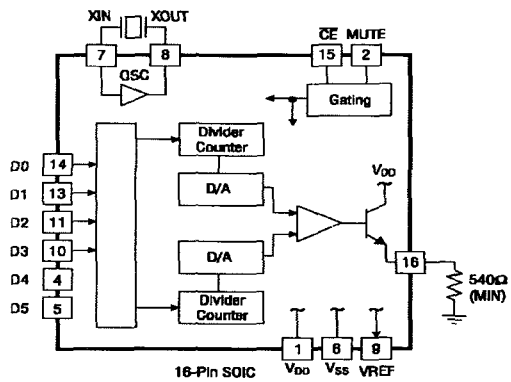


그림 16. M-991 Internal Block.
Fig. 16. M-991 Internal Block.

참고문헌

[1] 한국정보보호진흥원, "국외암호산업전망보고서", 2000.

[2] R. Ishii and M. Kkishita, "A desing method for a periodically time-varying digital filter for spectrum scrambling," IEEE Trans. Acoust., Speech, Signal Processing, vol. 38, 1990, pp.1219-1222.

[3] K. Sakurai, K. Koga, and T. Muratani, "A speech scrambler using the fast fourier technique," IEEE J. Select. Areas Comm., vol. SAC-2, 1984, pp.434-442.

[4] S. C. Kak and N. S. Jayant, "On speech encryption using waveform scrambling", Bell Syst. Tech. J., vol. 56, 1997, pp.781-808.

[5] N. S. Jayant et al., "A comparison of four methods for analog speech privacy", IEEE Comm., vol. COM-29, 1981, pp.18-23.

[6] Louis M. Pecora and Thomas L. Carroll, "Synchronization in Chaotic Systems", Review Letters, vol. 64, no. 8, 1990, pp.821-824.

[7] Thomas S. Parker, Leon O. Chua, "Chaos : A tutorial for engineers", IEEE, vol. 75, no. 8, 1987, pp.982-1008.

[8] 한국전자통신연구소, "현대암호학", 1991.

[9] C. W. King, C. A. Lin "A Unified Approach to scrambler Filter Design", IEEE Trans, Signal Processing, vol. 43, No. 8, 1995, pp. 1753-1765.

[10] N. S. Jayant et al., "A comparison of four methods for analog privacy", IEEE Trans. Comm., vol. COM-29, 1981, pp.18-23.

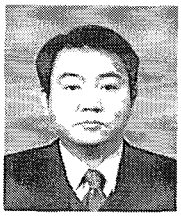
[11] L. S. Lee, G. C. Chou, and C. S. Chang, "A new frequency speech scrambling system which does not require frame synchronization", IEEE Trans. Comm., vol. COM-32, 1984. pp.444-456

[12] Man Yonng Rhee, "Cryptography and secure communications", 1994.

저자소개

유병욱(Byong-wook Yoo)

1986년 명지대학교 전자공학과 공학사
1988년 명지대학교 대학원 전자공학과 공학석사
1999년 명지대학교 대학원 전자공학과 공학박사
1997년~2000년 Datasecure 연구소장
2000년~2001년 Telesecure 이 사
2001년~2005년 COMMSEC 대표이사
2005년~현 재 (주)하이드로소닉 이 사
※ 관심분야 : 통신보안, 정보보호, 생체인식, 수처리 시스템



한 상 수(Sang-soo Han)

1983년 명지대학교 전자공학과 공학사
1985년 명지대학교 대학원 전자공학과 공학석사
1999년 홍익대학교 대학원 전자공학과 공학박사
1988년~1989년 (주)LG산전 선임연구원
1989년~현 재 경원전문대학 정보통신과 교수
※ 관심분야 : 지능제어, 불규칙 신호처리, 유량시스템 설계