SEED 알고리즘을 이용한 디지털 보안 전화기의 설계 및 구현

김정태* 류대현, 정창훈, 이상진
목원대학교, 한세대학교, 씨큐어텔레콤(주), 고려대학교

The Design and Implementation of Digital Secure Telephone with SEED Algorithm

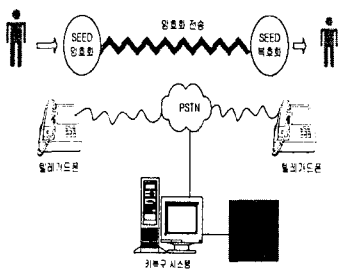
Jung-Tae Kim, Dae-Hyun Ryu, Chang-hoon Jung, Sang-jin Lee
Mokwon University, Hansei University, Securetelecom, Korea University
E-mail : jtkim5068@hanmail.net

요 약

정보화 사회가 됨에 따라 정보의 중요성과 함께 역기능으로 인한 부작용 또한 갈수록 심각해질 수 있으며 이에 따라 정보보호 요구가 크게 늘어나고 있고 관련 정보보호제품의 수요증가가 예상 되고 있다. 한편 선진각국은 OECD, APEC 등 다자간 협의를 통하여 정보 시스템의 안전과 암호정책에 관한 논의를 활발히 진행 중에 있어, 조만간 정보보호제품도 통상문제로 제기될 가능성이 다분하다. 그러나 국내 정보보호산업이 취약한 상태에 있고 정보보호의 특성상 정보보호 제품의 해외시장 의존은 바람직하지 않을 것이며 독자적인 기술력의 제품개발이 필수 불가결할 것으로 생각된다. 본 논문에서는 공중전화망(PSTN)의 전화 정보보호를 위한 디지털 보안전화기(이하 텔레가드폰)를 제안하고 이를 설계 및 구현하였다. 본 연구에서 제안한 디지털 보안전화기는 음성을 저속 압축 디지털 코드로 변환하고, 이에 국내 128 비트 블록 정보보호 알고리즘의 표준으로 정해진 SEED를 적용하여 안전한 통신이 가능하도록 하였다. 뿐만 아니라 키 복구 기능이 구현하여 개발된 시스템이 합법적 암호 접근을 허용하도록 하였다.

Ⅰ. 서 론

정보화 사회가 됨에 따라 정보의 중요성과 함께 역기능으로 인한 부작용 또한 갈수록 심각해질 수 있으며 이에 따라 정보보호 요구가 크게 늘어나고 있고 관련 정보보호제품의 수요증가가 예상 되고 있다. 한편 선진각국은 OECD, APEC 등 다자간 협의를 통하여 정보 시스템의 안전과 암호정책에 관한 논의를 활발히 진행 중에 있어, 조만간 정보보호제품도 통상문제로 제기될 가능성이 다분하다. 그러나 국내 정보보호산업이 취약한 상태에 있고 정보보호의 특성상 정보보호 제품의 해외시장 의존은 바람직하지 않을 것이며 독자적인 기술력의 제품개발이 필수 불가결할 것으로 생각된다. 본 논문에서는 공중전화망(PSTN)의 전화 정보보호를 위한 디지털 보안전화기(이하 텔레가드폰)를 제안하고 이를 설계 및 구현하였다. 본 연구에서 제안한 디지털 보안전화기는 음성을 저속 압축 디지털 코드로 변환하고, 이에 국내 128 비트 블록 정보보호 알고리즘의 표준으로 정해진 SEED를 적용하여 안전한 통신이 가능하도록 하였다. 뿐만 아니라 키 복구 기능이 구현하여 개발된 시스템이 합법적 암호 접근을 허용하도록 하였다.



(그림 1) 텔레가드폰 동작기능의 개념

본 논문에서 개발한 전화 정보 보호 시스템(일명 텔레가드 시스템)은 외산에 비해 월등히 낮은 가격으로 구현이 가능하고, 또한 규격화된 부품을

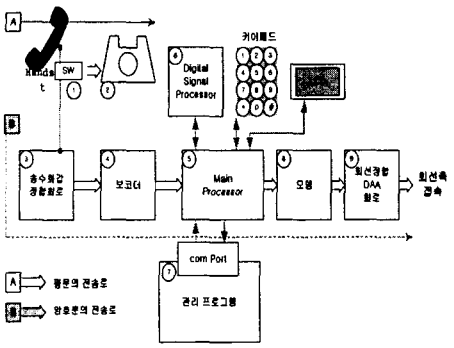
사용함으로써 추후 호환성에 있어서 유리할 것으로 사료된다. 뿐만 아니라, 현재 국내에서 일부 기관에서만 사용되어지던 전화 정보보호 장비에 대하여, 표준으로 공개된 SEED 알고리즘을 적용함으로써 추후 호환성을 비롯한 다양한 문제를 해결하는데 한발 앞서갈 수 있는 기반을 제공할 수 있을 수 있다. 본 논문의 구성은 다음과 같다. 먼저 2장에서는 본 논문에서 제안하는 디지털 전화기의 설계에 관한 내용을 3장에서는 구현에 관한 내용을 기술하고 있으며 4장에서 결론을 맺는다.

II. 디지털 보안 전화기의 설계

2.1 디지털보안 전화기의 구성

본 논문에서는 제안한 전화 정보보호 시스템을 개발하기 위하여 크게 텔레가드폰 시스템과 이의 관리 및 정보보호 기능 지원을 위한 텔레가드 관리 프로그램 및 키 복구 시스템을 개발하는데 목표를 두고 있다. 이중에서 본 과제의 핵심이라 할 수 있는 텔레가드 시스템의 주요 구성은 아래(그림 2)과 같다.

- DTMF 제어를 통한 전화 호출 및 호 설정 등을 관장하는 프로토콜 제어부
- 음성 신호를 디지털로 변환 후 압축을 수행하는 보코더부
- 입력되는 음성 디지털 데이터들을 보호할 수 있는 암/복호부



(그림 2) 텔레가드폰의 주요 기능 블록

2.2 디지털 보안 전화기의 동작

이와 같은 텔레가드폰 시스템의 동작 시나리오는 다음과 같다.

가. Call Setup

(그림 2)의 (1) 부분의 스위치(SW)를 A 방향에서 B 방향으로 전환한 후 텔레가드폰은 정보보호 통신을 위한디지털 통신을 시작한다. 먼저 전화를걸기 위해 키 패드를 이용하여 상대방 전화번호를 누르면, 이는 (5)의 주프로세서에 의해 해석되어 (4)의 보코더에 내장된 DTMF 송수신 기능을 이용하여, 상대국에 전화를 건다. 상대국에도 동일한 장비가 장착된 경우라면 상대국에서OFF HOOK 이된 후 상대국으로부터 응답 신호가 수신될 것이다.

나. 송수신 처리 서비스 Setup

Call Setup 이후 응답신호가 상대국으로부터 오면, 이후 데이터전송을 위한 모뎀 Line Setup 과정이 진행된다. 모뎀부는 전송되는 모뎀 신호를 디코딩(복조)하여 주 제어부에 입력하여 처리하고, 제어부에서는 이를 다시 회선측모뎀을 제어하여, 변조하고, 회선 인터페이스를 통하여 전송하는 서비스를 수행한다.

다. 암/복호화 처리

상기 나)항의 모뎀 Setup 과 동시에 주제어부 프로세서는 음성을 디지털 송수신 하기 위하여 보코더를 구동한다. 보코더를 구동하여 생성된 디지털 압축 음성을 암호화 또는 복호화 처리를 하기위하여, 제어부는 이를 DSP프로세서에 보내고 받는다. 제어부는 DSP 프로세서에 데이터의 암호화를 위하여 일정한 단위 프레임을 송수신하여 암호화 입출력 서비스를 제어한다.

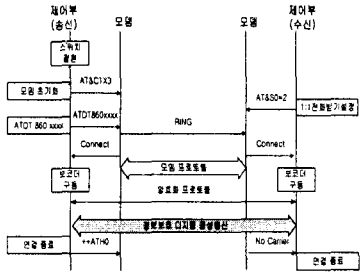
라. 송수신 정보보호 프로토콜의 처리

위와 같은 텔레가드폰 시스템의 키관리, 시스템 검사 등을 위하여본 과제에서는 별도의 관리 프로그램을 개발하였다. 이 관리 프로그램은 PC 상에서 동작하는 프로그램으로 OFF LINE 상에서 사용자 조작에 의하여 운용된다. 텔레가드폰 관리 프로그램의 주요 기능은 다음과 같다.

- SEED 알고리즘을 위한 키 발생 기능
- 발생된 키의 저장 기능
- Serial 인터페이스를 통한 저장된 키의 주입 기능
- 키의 발생 및 저장에 관한 기록 기능
- 텔레가드2000의 진단 기능
- 상기 기능의 친숙한 사용자 인터페이스

2.3 디지털 보안 전화기의 음성압축부 설계

잘 알려진 대로 전화 회선을 이용하여 무한정 디지털 신호를 전송할 수 있는 것은 아니다. 어느 정도의 제한이 있는 상황에서 통상의 64kbps PCM 과 같은 파형 부호화 (waveform coding) 방식을 적용할 경우 일반적인 전화 회선을 이용하여 전송하는 데에는 무리가 있다. 이를 해결하고자 음성의 특징을 나타내는 부분만 전송하고, 복원 시에는 그 특징을 이용하여 합성하는 음원 부호화 (source coding) 방식이 많이 이용되고 있다.



(그림 3) 텔레가드폰 송수신 정보보호 프로토콜의 처리

전화 회선을 이용한 디지털 음성 통신을 위하여 압축 및 합성 소자로 AMBE-1000 이라는 소자를 선택하였다. 전송 기술이 발전하기 전에는 Vocoder (voice coder)의 유용성은 적은 양의 데이터로 디지털 통신이 가능하다는데 있었다. 특히, 아날로그 방식의 스크램블러는 감청이 가능하다는 취약성을 갖기 때문에 보다 강력한 전화 보안 기능이 필요로 하게 되었다. 이는 Vocoder 의 응용이 일반용보다는 군용이나 보안용으로 활용된 사례가 더 많다는 면에서도 쉽게 알 수 있다. 결국, 미국의 국방성에서는 이들 방식에 대한 표준으로 제정하게 되었고, 최근에는 이동통신에 적용하기 위하여 많은 방식의 Vocoder가 소개되고 있다. 다음은 여러 가지 표준의 Vocoder 와 전송 능력을 나타낸 것이다.

- 미국 국방성 (DoD) 표준 FS-1015 (LPC-10e), 2.4 kbps
- 미국 국방성 표준 FS-1016 (CELP), 4.8 kbps
- IS 표준 IS-54 (VSELP), 7.95 kbps
- IS-96 (QCELP), 9.6 kbps
- ITU-T 권고 G.729 (CS-ACELP), 8 kbps
- ITU-T 권고 G.729A (CS-ACELP), 8 kbps
- APCO Project 25 (AMBE+), 2.4 ~ 9.6 kbps

이들 음성 부호화 방식의 성능 비교는 여러 논문에서 제시되고 있으며, 그 중 필요한 자료만 발췌하면 다음 <표 1>과 같다.

<표 1> 대표적인 디지털 압축 기법의 특징

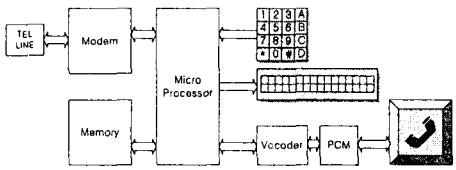
방식	속도 (Kbps)	품질	강인성	특징	구현 형태
LPC 10e	2.4	안좋음	안좋음	FS-1015, 화자 인식이 안됨	소프트웨어
CELP	4.8	보통	좋음	FS-1016	소프트웨어
CS-ACELP	8	좋음	좋음	ITU-T G.729.A	소프트웨어
VSELP	7.95	좋음	좋음	IS-54	소프트웨어
QCELP	9.6, 13.3	좋음	좋음	가변 부호화, IS-96	소프트웨어, 칩($70)
IMBE/AMBE	2.4, 4.8, 9.6	좋음	좋음	가변 부호화, DVSI 사	소프트웨어, 칩($48)

2.4 정보보호 기술

암호알고리즘은 암·복호화에 사용되는 키의 특성에 따라 암 복호화 키가 같은 대칭키 암호알고리즘과 암 복호화 키가 서로 다른 공개키 암호 알고리즘으로 크게 구분할 수 있으며, 대칭키 암호알고리즘은 데이터 처리 형식에 따라 스트림 암호알고리즘과 블록 암호 알고리즘으로 나눌 수 있다. 본 과제에서 음성 데이터 보호에 적용하고자 하는 SEED는 대칭키 암호 알고리즘으로, 블록 단위로 메시지를 처리하는 블록 암호알고리즘이다. 대칭키 블록 암호알고리즘은 비밀성을 제공하는 암호시스템의 중요 요소이다. n비트 블록 암호알고리즘이란 고정된 n비트 평문을 같은 길이의 n비트 암호문으로 바꾸는 함수를 말한다(n비트 : 블록 크기). 이러한 변형 과정에 암·복호키가 작용하여 암호화와 복호화를 수행한다. 블록 암호알고리즘은 대부분 Feistel 구조로 설계된다(예 : DES, FEAL, LOKI, MISTY, Blowfish, CAST, Twofish 등). Feistel 구조란 각각 t비트인 블록으로 이루어진 2t 비트 평문 블록이 r라운드를 거쳐 암호문으로 변환되는 반복 구조를 말한다. 반복 구조란 평문 블록이 여러 라운드를 거쳐 암호화되는 과정을 말한다(라운드 함수란 암호키로부터 유도된 각 서브키(또는 라운드 키라 불림)를 중요 입력으로 하여 바꾸어 주는 함수를 말한다). 또한, 전체 알고리즘의 라운드 수는 요구되는 비도와 수행 효율성의 상호 절충적 관계에 의해 결정된다. 보통 Feistel 구조는 3 라운드 이상이며, 짝수 라운드로 구성된다. 이러한 Feistel 구조는 라운드 함수에 관계없이 역변환이 가능하며(즉, 암·복호화 과정이 같음), 두 번의 수행으로 블록간의 완전한 diffusion이 이루어지며, 알고리즘의 수행속도가 빠르고, H/W 및 S/W로 구현이 용이하고, 아직 구조상의 문제점이 발견되고 있지 않다는 장점을 지니고 있다.

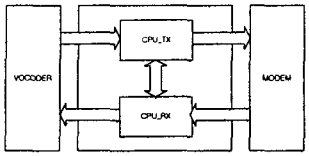
2.5 디지털 전화기의 구현

텔레가드폰 시스템은 키 복구 기능을 갖는 시스템으로써 전화 정보, 즉 음성 데이터를 암/복호화를 수행하여, 통신하는 정보를 보호하는 목적으로 개발하였다. 텔레가드폰 시스템은 전체 시스템의 제어를 담당하는 제어부, 음성을 D/A, A/D를 처리하는 음성 변환부, 외부입력 장치와 표시 장치를 제어하는 입출력부와 음성데이타를 송/수신할 수 있는 통신 제어부로 나눌 수 있다.



(그림 4) 전체 구성도

2.6 시스템의 상세 구현



(그림 5) Micro Processor 구성도

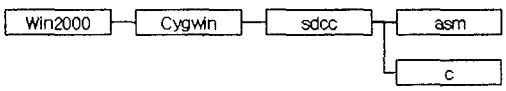
Micro Processor부는 전체 시스템의 모든 제어를 처리하는 부분으로써 VOCODER에서 PCM을 통해 들어오는 음성신호를 A/D 변환하여 추출한 음성 데이터를 송신을 담당하는 CPU_TX는 음성 패킷을 Modem을 통해 전송하게 된다. CPU_RX는 수신을 담당하는 Processor로써 Modem을 통해 들어오는 음성 패킷을 수신하여 패킷을 분석한 후 VOCODER에 보내 진다. Micro Processor부는 위에서 살펴보았듯이 두개의 Processor,즉 Multi Processor로 구성되어 있다. TX를 담당하는 CPU_TX와 RX를 담당하는 CPU_RX가 바로 그것이다. 이 두개의 CPU는 서로 동기를 맞추어 주어야 하며, 동기 설정 방식은 시리얼통신을 하여 서로에 상태를 전송하여 현재 시스템이 어떤 상태인지를 인지하도록 하였다. 전화시스템은 언제나 끊이지 않는 음성을 상대방에게 전달하는 것이 주 목적이다. 이 텔레가드폰 시스템은 전화정보를 보호하는 것이 목적으로써 방대한 음성데이터를 암/복호화하는 처리를 실시간으로 처리하여야 하므로 Multi Processor를 사용한 것이다.

III. 펌웨어 환경

3. 1. 개발환경

개발환경은Windows 2000를 운영체제로 하여 assembler와 C-compiler를 동시에 사용할 수 있는 SDCC cross compiler 사용하였다.

운영체제	Win2000
컴파일러 환경	GNU Cygwin v1.3.0
컴파일러	SDCC cross compiler v1.3.3
개발언어	Assemblier, C language 혼합



(그림 8-6) 개발환경 구성

3.2. 펌웨어 구성

펌웨어는 startup을 중심으로 하여 app, lib, util로 나눌 수 있다.

가. STARTUP
나. APP
다. TEL
라. KIB
마. UTIL

IV. 결론

본 논문에서 개발한 전화 정보 보호 시스템(일명 텔레가드 시스템)은 외산에 비해 월등히 낮은 가격으로 구현이 가능하고, 또한 규격화된 부품을 사용함으로써 추후 호환성에 있어서 유리할 것으로 사료된다. 뿐만 아니라, 현재 국내에서 일부 기관에서만 사용되어지던 전화 정보보호 장비에 대하여, 표준으로 공개된 SEED 알고리즘을 적용함으로써 추후 호환성을 비롯한 다양한 문제를 해결하는데 한발 앞서갈 수 있는 기반을 제공할 수 있을 수 있다.

참고 문헌

[1] 은종관, 음성부호화, 전자과학, pp. 178 ~184, 89. 1.
[2] R. V. Cox, Three new speech coders from the ITU cover a range of applications, IEEE Communication Magazine, pp. 40. ~ 47, 97. 9.
[3] 이상이, 정교일, 정창훈, STE 의 조사, 한국전자통신연구원, '98. 9.