의사난수발생기를 이용한 새로운 유선전화 도청방지장치에 관한 연구

김순석* · 이용희*

Study on New Security Device of Telephony Using the Pseudo Random Number Generator

Soon-seok Kim* · Yong-hee Lee*

요 약

본 논문은 의사난수발생기를 이용한 디지털 음성 암호화 모듈 및 이를 이용한 유선전화 도청방지장치에 관한 것이다. 제안하는 방법은 유선전화의 통화내용을 암호화하여 제 3자로부터 도청을 방지하는 유선전화 도청방지장치의 암호화 수단에 있어서, 통화 당사자 간 공유 비밀키와 통화 당시 시간 값을 이용하여 암호 키를 발생시키는 의사난수발생기 및 의사난수발생기에서 만들어진 암호키를 이용하여 데이터를 암호화하는 암호화기로 구성됨을 특징으로 한다.

ABSTRACT

We suggest the digital voice encryption module using the pseudo random number generator and design the security device of a telephone using the module. The proposed method provides encryption method of the telephone against the third party. This encryption method uses pseudo random number generator which computes the encryption key using the shared secret key and the current time value.

키워드

encryption key, telephone, pseudo random number generator

Ⅰ. 서론

제안하는 음성통화용 암호화기술은 최근 사회적으로 이슈화되고 있는 도청에 대한 일반 회사나 가정에서의 불안과 또 무엇보다 사용자 개인의 프라이버시를 해소할 수 있는 필수적인 요소기술이라 할 수 있다. 또한 본 기술을 이용할 경우 유선전화를 이용한 기업의 CEO, 정치인 간의 통화나 산업스파이의 도청활동 등을 원천적으로 봉쇄할 수 있어 매우 중요한 기술이라 할 수 있다.

현재까지 알려진 바에 의하면 기존에 시판되고 있는 국산 음성 암호화 모듈[1]의 경우, 음성 메시지의 암복호화를 위한 비밀키를 생성하는 데 있어 Diffie-Hellman이라는 암호화 기법[2]을 사용하고 있다. 그러나 이 기법은 공개키 방식을 통한 키분배 방법으로 비밀 통화를 원하는 당사자 간에 암호화 키 외에 별도의 키(앞서 말한 암호화 키를 생성하기위한 또 다른 키 정보라든가 당사자 각각의 개인키와 공개키쌍 등)를 반드시 저장하고 있어야하며, 키를 생성하는 데 있어서도 많은 시간을 필요로

* 한라대학교 컴퓨터공학과

접수일자 2008. 05. 30

한다. 또한 이러한 키 생성 작업은 음성 암호화 모듈을 사용할 때마다 즉, 통화 요청 시 매번 수행되므로 초기에 음성통화를 위한 기초적인 셋업(음성통화 암호화를 위한 키생성 과정을 말하는 것으로 암호 키 생성을 위한 100자리수 이상의 지수승 연산을 수행)을 하는데 많은 시간을 필요로 하는 단점이 있다. 그러나 제안하는 기술의 경우는 앞서 말한 Diffie-Hellman 기법이 아닌 암호학적인 난수발생기(PRNG, Pseudo Random Number Generator)[2,3]를 제안하는 장치에 내장하여, 이용하고자 할 당시의 시간정보와 양측에 미리 내장한 공유 비밀키를 시드(seed) 값으로 하여 암호화를 위한 비밀키를 그 즉시 생성(또는 사전에 정해진 시간 주기마다 계산)하고 동기화함으로써, 앞서 말한 초기 셋업시간을 획기적으로 개선하였다. 제안하는 방법의 경우 단순한 비트 이동이나 자리바꿈 등의 연산이 수행되므로 기존 방식에 비해 그 시간을 약 100배 이상 단축시킬 수 있다.

본 논문의 2장에서 본 연구와 관련한 국내외 기술현황에 대해 살펴보고 3장에서 새로운 도청방지 암호화 모듈을 제안한 후, 4장을 끝으로 결론을 맺고자 한다.

Ⅱ. 국내외 관련 기술 현황

현재 유선전화에서 도청방지장치의 일환인 음성 통화를 위한 암호화 모듈의 경우 국내에서 기술을 보유하고 개발 중인 회사가 단 한 곳이 있다. 제안하는 음성 암호화 모듈의 경우 기술적인 면에 있어 가장 핵심이 되는 기술이 바로 음성 통화 내용의 암호화 성능이라고 할 수 있다. 암호화 성능을 비교하는 데 있어 중요한 부분은 크게 두 가지로 첫째, 음성 통화 내용을 암복호화 하는데 소요되는 시간과 둘째, 암복호화를 위해서 필요한 비밀키를 생성하는데 소요되는 시간이다. 그 가운데 첫 번째 요소의 경우는 현재까지 알려져 있고 널리 이용되고 있는 암호 알고리즘들이 극히 제한적이기 때문에 성능 면에서 비교우위에 있거나 큰 차이를 느끼지 못한다. 그러나 두 번째 요소의 경우는 암호 키 생성에 있어 알려진 알고리즘들이 다양하며 또한 암호 알고리즘들에 따라 필요한 키라든가 키 생성에 소요되는 시간들이 다양하게 나타난다. 이러한 점에서 볼 때, 제안하는 방법의 경우, 자체 테스트 결과, 키 생성에 소요되는 시간이 기존 타사 제품에 비해 성능 면에서 약 100배 이상의 비교우위를 보이고 있다.

그림 1. 기본 모델
Fig. 1 Basic Model

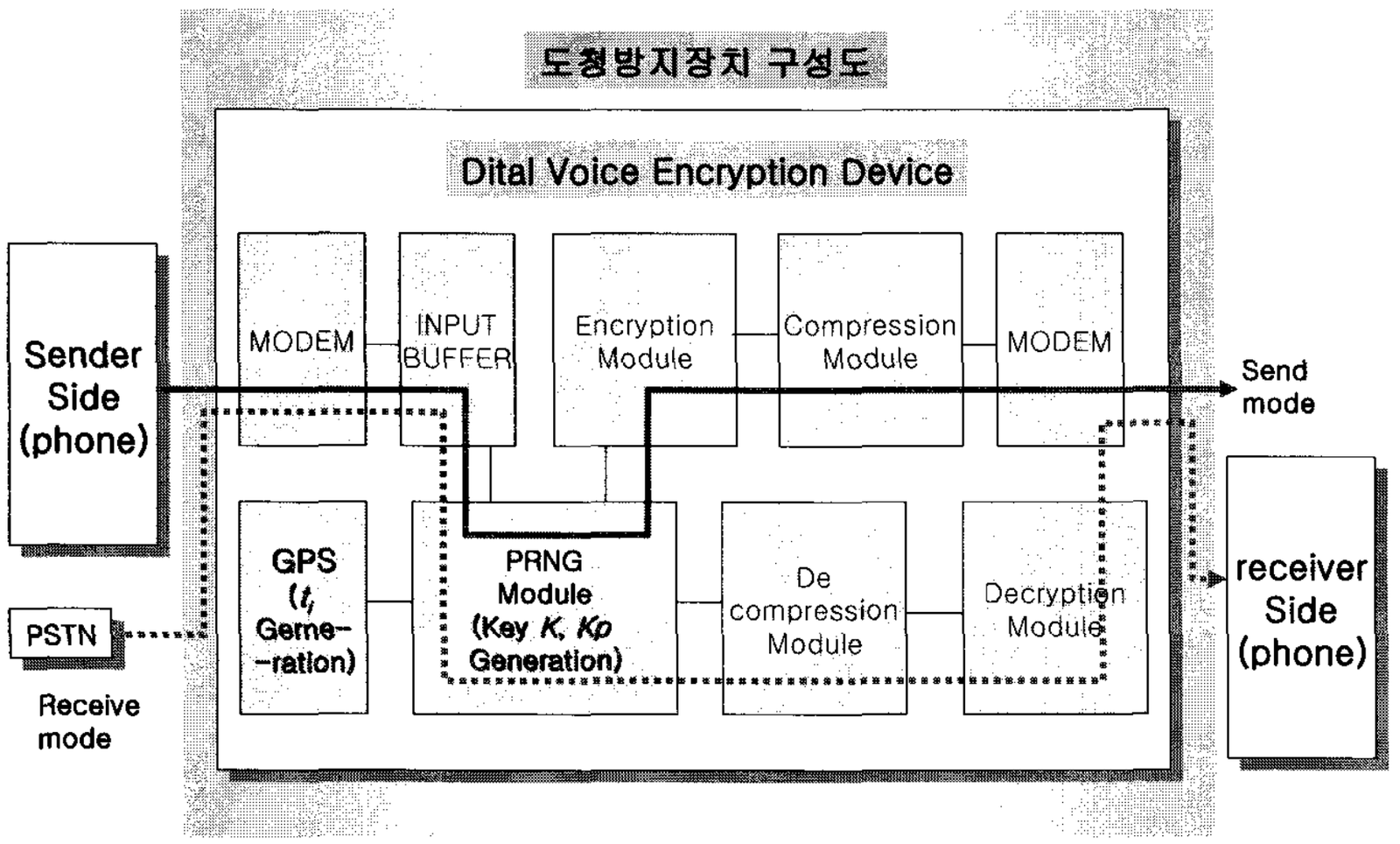


그림 2. 제안하는 도청방지장치 암호화 모듈의 구성도
Fig. 2 Flow diagram of the proposed security module

한편, 국외의 경우는 제안하는 제품과 관련하여 소문만 무성할 뿐 현재까지 알려진 바는 없는 실정이다. 그 이유는 대부분 국외 제품의 경우 그 가격이 매우 고가이며 기술이 비공개적이고 정부의 공식적인 인가를 받지 아니한 비합법적인 제품들이기 때문이다.

Ⅲ. 제안하는 도청방지장치 암호화 모듈

제안하는 방법은 일반 가정에서 사용하는 유선전화에서 전화 가입자들이 이용하는 통화내용을 암호화하여 불법적인 제 삼자로부터 도청을 방지하기위한 장치이다. 제안한 방법을 이용한 도청방지 암호화 모듈은 그림 1에서 보는 바와 같이 기존 유선 전화기와는 별도로 제작되는 것으로, 기존의 전화기 내부에 변형을 가하지 않으면서 사용자들이 손쉽게 이용할 수 있으며 포켓용으로 휴대가 가능하다는 장점이 있다. 또한 기존에 개발된 타사의 도청방지 암호화기와는 달리 보다 향상된 성능, 기능성, 그리고 간편성에 중점을 두어 개발되었다.

제안하는 방법은 내부적으로 그림 2의 흐름을 통해 당사자들 간의 통화내용이 암호화되어 전달되며 그 과정은 다음과 같다. 먼저 사용자로부터 전달된 음성 아날로그 신호가 실시간으로 모뎀을 통해 디지털신호로 변환된 다음 입력버퍼를 통해 임시로 저장된다. 그 후 고유 신기술인 암호학적 의사난수발생기(PRNG)를 이용하여 비밀키 K를 생성[1]하고, 변환된 디지털 신호의 음성 데이터를 기 생성한 K를 이용하여 국내 256비트 대칭키 암호 표준인 SEED 또는 아리아를 통해 암호화한다. 암호화된 음성데이터는 고효율의 압축 알고리즘을 거쳐 모뎀을 통해 아날로그신호로 변환되어 실시간으로 수신자의 음성암호화기의 입력으로 전달된다.

여기서 그림 3의 구성도에서 보는 바와 같이 송수신자 간에 음성통화 메시지 M에 대해 암복호화를 수행하는데 있어 필요한 공유 비밀키를 생성하는 역할을 *PRNG*가 담당하고 있다. 이때 *PRNG*는 암복호화에 사용할 공유 비밀키를 아래와 같이 생성한다.

$$K=PRNG(K_P, t_i)$$

(K_P :통화당사자간 공유비밀키, t_i :통화 당시 시간값, *PRNG* : 암호학적인 의사난수발생기)

이때 *PRNG*에 입력되는 값으로 t_i를 사용하고 있는데, 이 값은 송수신 양측의 암호화 모듈에서 동시에 동기화되며 암호화 모듈 내에 별도의 위성추적장치인 *GPS*

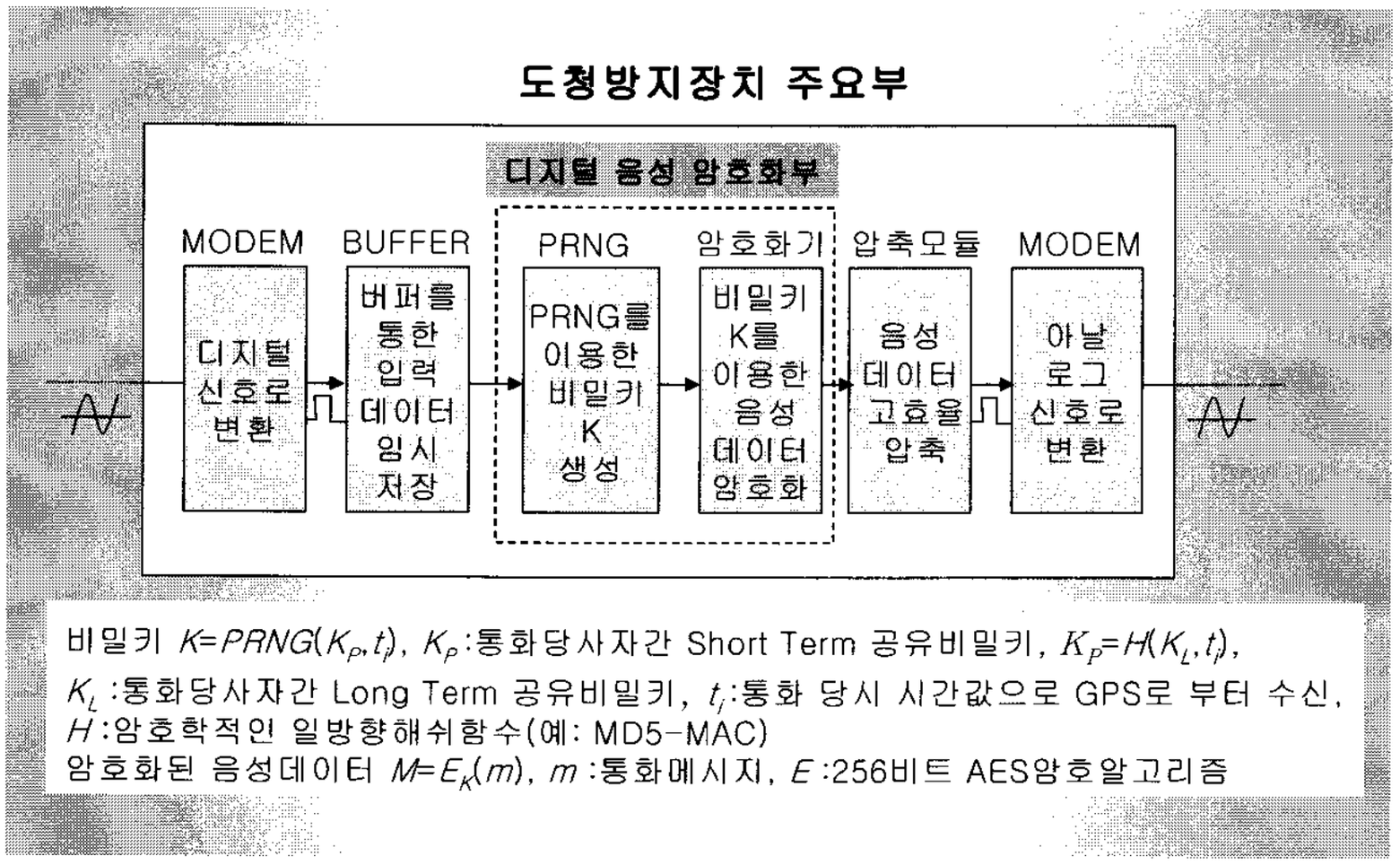


그림 3. 제안하는 도청방지 암호화 모듈
Fig. 3 The proposed security Module

1) 이 과정은 사용자가 본 음성암호화 모듈을 이용하기위해 사용 시 미리 정해진 시간에 따라 당사자들 간에 사전에 계산될 수 있다.

(Global Positioning System) 수신기를 양측에 내장하여 생성되는 시간 값이다. 또한 이 값은 효율성을 높이기 위해 사전에 양측이 미리 정한 시간에 따라 일정 주기로 생성될 수 있다.

한편 양측에 생성되는 비밀키 값의 비도를 높이기 위해 통화당사자간의 공유 비밀키인 Kp값을 정기적(예: 월단위)으로 재설정하는 방식을 추가로 적용할 수 있다. 이것은 별도의 모듈로 장기공유 비밀키 K_L(암호화기의 양측에 최초 구입시 동일한 값으로 내장함)을 두고 이 값을 암호학적인 일방향 해쉬함수 H(예, MD5-MAC 등)를 이용하여 정기적으로 GPS가 수신하는 시간이 될 때마다[2] 다음 식

$$Kp=H(K_L, t_i)$$

에 의해 새로운 단기 공유 비밀키인 Kp값을 생성하는 방식을 사용할 수 있다.

한편 비밀키 K값의 경우, 기본적으로 외부의 제 삼자가 GPS로부터 생성되는 시간 값을 알고 있다하더라도 비밀키인 K를 계산하기 위해서는 $K=PRNG(Kp, t_i)$에서 통화당사자간 공유비밀키인 Kp 값을 알아야 하는데 이를 알 수 없기 때문에 안전하다고 할 수 있다. 또한 Kp값은 장기공유 비밀키인 K_L을 이용, 안전하다고 알려진 암호학적인 해쉬함수에 의해 생성($Kp=H(K_L, t_i)$)되기 때문에 외부 제삼자가 Kp값을 알고있다 하더라도 이 값으로부터 K_L의 값을 알 수 없다.

Ⅳ. 결 론

본 연구를 통해 개발된 도청방지장치는 현재 이 분야 시장에서 약 95%가 내수에 의존하고 있을 정도로 독자적인 국내 기술 확보에 어려움이 있었던 게 사실이다. 비록 국내에 1개 업체가 이 분야에 독자 기술을 확보, 상용화가 이루어지고 있지만 금번에 개발된 도청방지장치의 경우 기존 보다 공유 비밀키 생성을 위한 암호화 속도 면에서는 기존의 Diffie-Hellman 방식이 아닌 의사난수발생기인 PRNG를 이용함으로써 100배 이상의 성능 향상을 보여, 기술개발 성과 면에서는 탁월하다 할 수 있다.

2) 이 값은 보다 성능을 높이기 위해 정해진 시간이 되기 이전에 미리 계산될 수 있다.

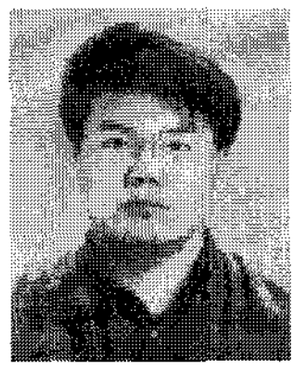
참고문헌

[1] (주)컴섹, http://www.commsec.co.kr.

[2] B. Schneier, Applied cryptography, 2nd Ed., John Wiley & Sons, Inc. 1996.

[3] A. J. Menezes, P. C. Oorschot, and S. A. Vanstone, Handbook of applied cryptography, CRC Press, 1997.

저자소개



김 순 석(Soon-Seok Kim)

1997년 2월 진주산업대학교 컴퓨터공학과(공학사)
1999년 2월 중앙대학교 컴퓨터공학과(공학석사)
2003년 2월 중앙대학교 컴퓨터공학과(공학박사)
2003년 3월～현재 한라대학교 컴퓨터공학과 조교수
※ 관심분야 : 정보보호, 암호응용, 생체보안

이 용 희(Yong-Hee Lee)

1991년 2월 한양대학교 전자공학과(공학사)
1993년 2월 한양대학교 전자공학과(공학석사)
1998년 2월 한양대학교 전자공학과(공학박사)
1999년 3월～현재 한라대학교 컴퓨터공학과 조교수
※ 관심분야 : 의용전자, 임베디드시스템, U-헬스