근접 통신망의 보안성 향상을 위한 자기키 생성 알고리즘에 관한 연구

정우열* · 이선근**

A Study on the Self-Key Generation Algorithm for Security Elevation in Near Field Communications

Woo-Yeol Jeong* · Seon-Keun Lee**

요 약

NFC, 블루투스, WiFi 등과 같은 근접 통신망의 발달과 더불어 보안의 중대성이 강조되고 있지만 아직까지는 괄목할 만한 연구가 진행되고 있지 않다. 본 연구에서 근접 통신망의 보안성 향상을 위하여 SSEN 알고리즘을 제안하였다. 제안된 SSEN 알고리즘은 별도의 암호기능이 필요없이 자기키를 생성하는 알고리즘으로서 인증기능을 부가적으로 수행하여 자체적으로 서비스의 처리속도 및 오류에 대하여 보다 나은 성능을 가질 수 있도록 하였다.

ABSTRACT

Importance of security is emphasized along with development of local area network such as NFC, Bluetooth, WiFi etc., but research that is worth watching eagerly up to now is not gone. This paper proposed SSEN algorithm for security elevation of approximation communication network. Proposed SSEN algorithm is algorithm that special cryptographic function creates own key without necessity. Also, SSEN achieving certification function additionally, did so that can have more than performance about the processing speed and mistake of service voluntarily.

키워드

NFC, bluetooth, WiFi, cryptographic algorithm, authentication
NFC, 블루투스, WiFi, 암호알고리즘, 인증

Ⅰ. 서 론

무선 네트워크 기술은 IT 통신 기술의 발달로 휴대기기의 지능적 통신 인프라 구축[1]을 발전시키며 미래의 정치, 경제, 사회, 문화 등 다양한 분야의 파급효과에 지대한 공헌을 하고 있다.

특히, 근접 통신망의 경우, 스마트폰의 대중화로 인하여 다양한 종류의 서비스 및 서비스 품질을 요구하고 있다.

이와 같은 소비자의 서비스 및 품질 등을 만족시키기 위해서 근접 통신망[2]은 향후 비약적인 발전을 계속하게 될 것으로 생각된다.

* 한려대학교 멀티미디어정보통신공학과(jeongyeol@hanmail.net)
** 전 원광대학교 전기전자 및 정보공학부(caiserisk@googlemail.com)
접수일자 : 2012. 07. 23 심사(수정)일자 : 2012. 09. 05 게재확정일자 : 2012. 10. 05

그러나 이와 동시에 보안 문제가 대두되고 있다. 유/무선, 원/근거리, 단/양방향 등의 네트워크 종류 및 서비스 종류가 다양화 되고 사용자들의 수가 증가[2] 되면서 고정된 플랫폼에서 발생되었던 해킹, 크래킹 등의 보안상의 문제점들이 점차 발생빈도가 증가하고 있는 추세이다.

이러한 현실에 적응하기 위하여 본 연구에서 SSEN(Self-key generation for Security Elevation in Near field communication) 알고리즘을 제안하였다. 제안된 SSEN 알고리즘은 보안 문제를 보다 원활한 통신체계속에서 해결할 수 있도록 하기 위한 것이다.

제안된 SSEN 알고리즘은 베이스 밴드의 시스템 구조를 설계하고 이를 확인한 결과, 기존 시스템의 성능에는 거의 차이가 없으며 별도의 ID 및 키 정보 없이 자기 키를 생성하여 자체 보안기능에 사용함으로서 리소스를 절약할 수 있으며 시스템 전체 성능저하를 효율적으로 억제할 수 있는 장점이 있는 것으로 확인되었다.

II. 근접 통신망 서비스에 적합한 변복조기

본 논문에서 적용한 구조의 처리 속도는 무선 LAN 시스템[2]에 맞게 개선할 목적으로 SSEN 변복조 구조를 이용한 프로세서에 파이프라인 구조의 프로세서를 적용하여 처리속도와 상호간섭 억제를 수행할 수 있도록 하였으며 SSEN 변복조기에 자기 키 생성기능을 추가하였다.

SSEN 변복조 구조는 많은 신호처리 문제들을 해결하는데 있어서 적용할 수 있는 공유 메모리를 사용하며 이 공유 메모리는 각각의 독특한 특성을 가지는 여러 개의 부분적인 메모리로 나뉘고 이 중에서 일부분은 일반적인 형태의 메모리 저장장소로써 이용이 된다. 공유 메모리 안에 존재하는 여러 개의 메모리 셀들은 ALU, 버터플라이, I/O unit, DSP와 같은 연산자와 결합해서 사용하게 된다. 즉, SSEN 변복조 구조는 하나의 메모리 공간을 여러 개의 버터플라이 연산자가 나누어서 사용할 수 있는 형태를 갖게 된다.

SSEN 변복조 구조는 새로운 데이터가 SSEN 변복조 구조에 입력되었을 때 그 데이터가 공유 메모리에 입력되고 버터플라이 연산자는 공유 메모리로부터 저장되어 있는 입력 데이터를 얻게 되며 버터플라이 연산에 의해 생성된 데이터를 공유 메모리에 저장한다. 이와 같은 절차를 통한 연산과정은 SSEN 변복조 신호 흐름에 존재하는 모든 버터플라이 연산자가 모두 계산되어질 때까지 반복해서 행해지게 되고 연산이 모두 끝나게 되면 출력 데이터가 공유 메모리로부터 읽혀져서 출력하게 된다. 기존에는 저장된 데이터 중 하나를 출력으로 보내는 형태를 취했지만, 본 논문은 두 개의 입력된 데이터 값을 조합하여 전혀 다른 값을 출력으로 산출하는 형태를 취하여 많은 간섭요인들과 성능저하 등의 문제점을 억제 할 수 있다. 또한 SSEN 변복조 구조에 요구되는 처리율에 맞추어서 필요로 하는 연산자의 수를 정확하게 사용할 수 있다. 이때 요구되는 연산자의 수(N_{BPE})는 $N_{BPE}= N_{BF}\cdot(T_{BPE}/T_{FFT})$이다.

이때, $N_{BF}(=(N/r)\log_r N)$ 는 변복조 신호 흐름도에서 버터플라이 수이고 T_{BPE}는 버터플라이 연산자가 계산을 수행하기 위해 필요한 시간이며 T_{FFT}는 SSEN 변복조 알고리즘을 계산하기 위해 필요한 시간을 나타낸다.

SSEN 변복조 구조에서 요구하게 되는 메모리는 단지 N 개의 복소 워드만 필요하며, 이는 고정되거나 혼합된 형태의 공통인수를 가지는 radix-r 변복조 알고리즘에서 In-place 특성을 가지고 계산되어진다. 또한 이러한 특성은 자기 키를 생성할 수 있는 근거 자료로 사용된다. 일반적인 암호시스템인 경우, 독립적인 ID 또는 별도의 인식코드가 필요하겠지만, SSEN은 특정 메모리와 변복조기의 입력으로 사용될 데이터의 전처리 과정에서 발생되는 데이터를 가지고 데이터를 처리하는 부가적인 특징을 가지게 된다.

즉, 데이터가 공유 메모리로부터 버터플라이 연산자로 읽혀지게 되면 연산을 수행하는 메모리의 위치가 버터플라이 연산자로부터 계산된 결과를 저장하기 위해서 다시 사용되며 이와 동시에 암호화에 사용될 데이터가 발생되는 것이다.

본 논문은 데이터 성능 향상 및 상호간섭 억제와 처리속도, 보안성 증대 등을 근접 통신망 시스템에 맞게 개선할 목적으로 SSEN 변복조 알고리즘을 이용한 SSEN 변복조 시스템을 설계하였다.

본 논문에서 설계한 SSEN 변복조 알고리즘을 고속 근거리 무선 LAN 시스템과 OFDM 방식에 동시

에 적용하기 위해 54Mbps의 전송률을 갖는 QPSK/BPSK/π/4QPSK SSEN 변복조 구조 알고리즘 설계에 초점을 맞추었다[1][3,4]. 설계에 사용된 설계 사양은 표 1과 같으며,

표 1. SSEN 변복조 프로세서 설계 사양
Table 1. SSEN MODEM processor Spec.

항 목	내 용
적용된 알고리즘	SSEN 변복조 알고리즘
수의 표현	고정 소수점
수의 형태	부호를 갖는 2의 보수
데이터 속도	54Mbps
변조방식	QPSK/BPSK/π/4QPSK
부반송파의 수	52
서브캐리어 수	48
파일럿 서브캐리어 수	4
서브캐리어 주파수 간격	0.3125MHz
가상 반송파수	12
전송 대역폭	5/10/20MHz
데이터 포맷 방식	block
암호방식	symmetric
입력/출력	128/128 bits
키 크기	64/128 bits
키 블럭	16 bits
키 생성	Self(in data)

총 52개의 부반송파(서브캐리어 48개 + 파일럿 서브캐리어 4개)를 사용하였고 52개를 제외한 나머지 12개는 인접채널의 간섭을 방지하기 위한 가상 반송파로 사용되었다. 본 논문에 적합한 알고리즘의 경우 규칙성과 대칭성이 좋은 SSEN 변복조 알고리즘을 이용하고 설계 구조에서는 위에서 설명한 여러 문제점 등을 보완해주기 위해서 고속 무선 LAN[5]과 근접 통신시스템 설계에 적합한 SSEN 변복조 알고리즘을 적용한 구조로 설계하였다.

식 (1)은 본 논문에서 사용된 2의 보수 표기를 나타내는 수식이다. 2의 보수 표기는 대부분의 컴퓨터에서 사용되는데 이와 같은 표기 방법의 가장 큰 두 가지 특징은 숫자 '0'을 정확히 표현할 수 있다는 것과 뺄셈의 구현이 쉽다는 것이다. 즉, 단지 피연산(operand) 함수의 보수를 더함으로서 구할 수 있다.

$$X = -x_0 + \sum_{i=1}^{n-1} x_i 2^{-i} \quad (1)$$

$$G(x) = x^7 + x^5 + 1 \quad (2)$$

식 (2)는 SSEN에 사용된 제안된 키 스케줄러의 생성 다항식으로 식 (2)의 탭 계수는 식 (3)을 만족하며 초기값은 모두 0을 제외한 값을 사용하였다.

$$g_1 = g_6 = g_8 = 1 \quad (3)$$

SSEN 64 비트를 처리하기 위한 8단 LFSR의 초기 상태가 모두 '0'일 경우 LFSR 탭 범위는 $1 \le i \le 8$이므로 지연소자의 초기값 s_i는 모두 영의 값을 가지게 된다[6]. 그러므로 LFSR 키 스트림 생성수열은 식 (2), 식(3)의 생성 다항식에 이용하면 키 출력수열 Z는 식 (4)를 얻는다.

식 (4)는 식 (2)의 생성 다항식에 의한 키 수열을 나타내는 것으로써 본 논문은 식 (4)의 MSB와 LSB만을 이용하도록 하였다. 일반적으로 의사난수발생기의 주기는 $2^m - 1$로써 표현되어지며, 이때 m값이 클수록, 주기가 길수록 선형특성에 안전하다. 그러므로 m값이 긴 의사난수발생기를 설계하게 되는데 이는 안전성에는 좋은 특성을 가지지만 주기에 비례하여 처리시간이 길어지며 특히 동기시스템인 경우 오류발생시마다 동기 획득에 걸리는 시간이 길어지는 단점을 가진다. 제안된 SSEM은 난수발생에서 한 주기 안에 절대적으로 하나의 정보가 존재한다는 것을 이용한다. 즉 한 주기 안에 존재하는 모든 의사난수를 이용하는 것이 아니고 초기 난수를 암호화에 이용하여 주기 시스템에 대한 주기시간의 단축을 꾀한다. 즉 LFSR의 초기값에 대하여 m만큼의 시간이 지날 때 출력되는 의사난수출력 Z_m을 LFSR의 출력으로 사용한다.

그림 1은 식 (2), (4)를 이용하여 SSEN에서 자기키를 생성하는 과정이다. 이 과정을 수행하게 되면 별도의 키 정보 없이, 입력되는 정보만을 이용하여 안전성이 보장되는 키 값을 생성하게 된다.

$$
\begin{aligned}
z_0 + k_0 &= g_1 s_1 + g_6 s_6 + g_8 s_8 \\
z_1 + k_1 &= g_1 k_0 + g_6 s_5 + g_8 s_7 \\
z_2 + k_2 &= g_1 k_1 + g_6 s_4 + g_8 s_6 \\
z_3 + k_3 &= g_1 k_2 + g_6 s_3 + g_8 s_5 \\
z_4 + z_4 &= g_1 k_3 + g_6 s_2 + g_8 s_4 \\
z_5 + k_5 &= g_1 k_4 + g_6 s_1 + g_8 s_3 \\
z_6 + k_6 &= g_1 k_5 + g_6 k_0 + g_8 s_2 \\
z_7 + k_7 &= g_1 k_6 + g_6 k_1 + g_8 s_1 \\
z_8 + z_8 &= g_1 k_7 + g_6 k_2 + g_8 k_0 \\
z_9 + k_9 &= g_1 k_8 + g_6 k_3 + g_8 k_1 \\
z_{10} + k_{10} &= g_1 k_9 + g_6 k_4 + g_8 k_2 \\
z_{11} + k_{11} &= g_1 k_{10}
\end{aligned}
\tag{4}
$$

SSEN 변복조 구조의 연산에서 회전 인자 값으로써 사용되는 계수의 구성방식은 ROM 테이블에 cosine과 sine값을 구성하여 radix engine에서 출력되는 신호 값과 연산될 수 있도록 구성하였고 radix engine은 radix-2 버터플라이 구조를 이용하였으며 입력과 출력에 각각 2개씩의 RAM 버퍼를 두어서 연속된 데이터의 입력을 저장함과 동시에 입력되는 데이터를 실시간으로 처리할 수 있도록 구성하였다.

이와 같은 설계 방식을 적용해서 구성한 SSEN 변복조 구조의 전체 블록 다이어그램은 그림 2와 같으며 64-point 및 64/128 키 생성 변복조 프로세서의 구조를 가진다.

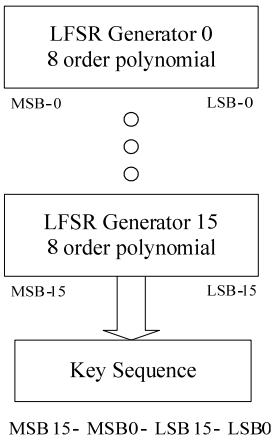

그림 1. SSEN 자기 키 생성
Fig. 1 SSEN self-key generation

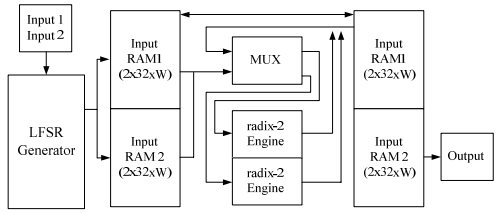

그림 2. 설계된 64-point SSEN 변복조기 블록 다이어그램
Fig. 2 Block diagram of designed 64-point SSEN Modem

본 논문에서 설계된 입력 RAM 버퍼는 SSEN 변복조 구조에서 사용하는 공유 메모리 구조를 이용하였다. 입력되는 신호값은 샘플링률(sampling rate)에 따라서 저장하게 된다. 그림 3은 입력 버스에 따른 타이밍 도를 나타낸다.

설계된 출력 RAM 버퍼는 입력 RAM 버퍼에서와 마찬가지로 Startp 신호의 영향을 받게 된다. 따라서 출력 RAM 버퍼는 Startp 신호의 하강에지(falling edge)에서 Swap을 일으킨다. 출력 RAM 버퍼의 뱅크 Swapping은 출력 데이터의 흐름에 영향을 미치지 않고 radix-2 버터플라이 연산자에 의해서 처리된 데이터를 계속해서 처리해줌과 동시에 다른 뱅크에서는 radix-2 버터플라이에서 처리되는 데이터들을 저장하기 위해서 사용된다.

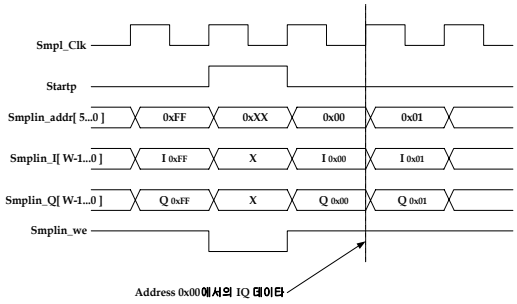

그림 3. 입력신호에 따른 타이밍 도
Fig. 3 Timming charts of inputs

SSEN 변복조 구조는 내부연산에 의해 발생되는 오버플로워 방지 및 키 생성시 발생될 수 있는 LC, DC[7,8]를 방지하기 위하여 데이터 포맷 스케일링을 수행하여야 한다. 안전한 스케일링 방법을 사용하면 계산시에 오버플로워 및 LC, DC가 발생하지 않는 것

을 보장할 수 있기 때문에 스케일링은 반드시 필요하게 된다.

양자화 잡음이 일어나는 부분은 버터플라이내부에서 곱셈연산을 하기 전에 발생하므로 곱셈연산을 해주기 전에 안전한 스케일링을 해주어야만 한다. 본 논문에서 이용하게 되는 radix-2 버터플라이의 연산과정은 식 (5)와 같다.

$$|X_0| = |x_0 + x_1| \leq |x_0| + |x_1| < 1$$

$$|X_1| = |(x_0 - x_1) \cdot W^p| = |x_0 - x_1| \leq |x_0| + |x_1| < 1 \quad (5)$$

III. 모의실험 및 비교분석

본 논문에서는 OFDM 방식 고속 무선 LAN 시스템과 근거리 무선 LAN에 적용할 SSEN 변복조 시스템을 설계하였다. 또한 simulation 검증을 위해 먼저 Matlab을 이용하였다.

OFDM 방식 고속 무선 LAN 시스템과 근거리 무선 통신시스템에서는 PLCP 프리엠블 구조를 갖는 데이터 프레임을 이용해서 송신을 하게 된다. 송신되는 데이터 프레임에서 PLCP 프리엠블은 수신기에서 동기 추적을 위해 사용되며 SSEN 변복조 알고리즘에 가장 먼저 입력되는 데이터이다. 따라서 본 논문에서는 송신기에서 PLCP 프리엠블의 Short sequence와 Long sequence의 데이터 값을 이용해서 SSEN 변복조 알고리즘의 연산을 Matlab을 통해 검증하였으며 또한 random 벡터를 통해서 얻은 입력값을 텍스트 파일로 저장해서 Synopsys tool을 이용해 시뮬레이션을 통해 검증하였다. 표 2는 SSEN 변복조 알고리즘의 연산을 검증하기 위해서 사용된 Short sequence와 Long sequence 값을 나타내고 있다.

이 랜덤 벡터는 설계 규격에서 설정하였던 QPSK/BPSK/π/4QPSK 심볼에 맞도록 4개의 복소 성상도(complex constellation)를 갖는 QPSK/BPSK/π/4QPSK 심볼로 결정하였다. 이는 벡터파일로 변환하여 Synopsys에 의해 불려진다.

표 2. Short sequence와 Long sequence 데이터
Table 2. Short/Long sequence data

	Data coefficient(64)
Short sequence	0, 0, 0, 0, -1-i, 0, 0, 0, -1-i, 0, 0, 0, 1+i, 0, 0, 0, 1+i, 0, 0, 0, 1+i,0, 0, 0, 1+i, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1+i, 0, 0, 0,-1-i, 0, 0, 0, 1+i, 0, 0, 0, -1-i, 0, 0, 0, -1-i, 0, 0, 0, 1+i, 0, 0, 0
Long sequence	1, 1, -1, -1, 1, 1, -1, 1, -1, 1, 1, 1, 1, 1, 1, -1, -1, 1, 1, -1, 1, -1, 1, 1, 1, 1, 0, 1, -1, -1, 1, 1, -1, 1, -1, 1, -1, -1,-1, -1, -1, 1, 1, -1, -1, 1, -1, 1, -1, 1, 1, 1, 1, 1, 1, 1, 1, -1, -1, -1, -1, -1, 1, 1

그림 2와 같이 설계된 SSEN 변복조 구조에 대한 시뮬레이션은 그림 4에 나타내었다. 그림 4에서 2.8㎲에서 데이터가 처리되어 출력됨으로서 파이프라인 구조의 고속 무선 LAN 시스템의 처리속도인 3.6 ㎲ 보다도 0.8 ㎲ 성능이 향상됨을 알 수 있었고, LFSR[9]을 이용한 자기 키 생성기능을 수행하고 있다는 것을 모의실험 결과를 통하여 확인하였다.

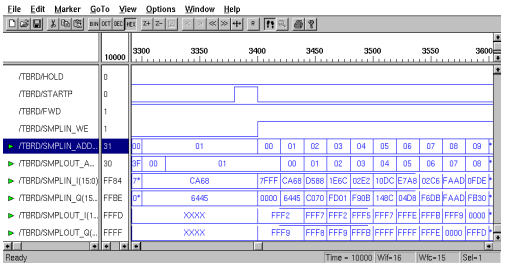

그림 4. 입력 신호에 의해 생성된 출력 신호
Fig. 4 Generated output following input

또한 이러한 점으로 보아 상호간섭 억제를 향상시키는 것을 확인하였다. 그리고 표준안에서 제시하고 있는 FFT 프로세서의 연산처리 시간인 3.2 ㎲를 만족함을 확인하였다.

IV. 결 론

근접 통신시스템 사이에 발생하는 상호 전파 및

주파수 간섭과 성능저하, 사용자들간의 데이터 간섭, 해킹 및 크래킹 등 다양하게 발생되고 있는 기기간의 간섭들을 해결하기 위하여 본 논문에서는 동일하게 사용되는 OFDM(5.8GHz), 2.4GHz(ISM) 대역의 변·복조 스템을 구현함에 있어 요구되는 Bluetooth, OFDM, Wireless, NFC, WiFI 변복조 알고리즘에 대해서 기존에 주로 이용되던 파이프라인 구조를 대신해서 새로운 SSEN 변복조 알고리즘을 이용한 변복조 구조를 설계하였다. 적용된 SSEN 변복조 구조의 응용분야는 IEEE 802.11a,b,x 표준안에 의한 고속 무선 LAN 시스템과 근접 통신시스템의 변복조 프로세서이며, 연산속도는 3.2μs안에 처리되도록 규정되어 있다.

기존 시스템의 경우, ISM 대역에서 사용되는 시스템간 상호간섭이나 성능저하 등 억제 방안이 없어 RF단에서 대책들을 찾았으나, 본 논문은 변복조부의 베이스밴드 알고리즘을 구조적으로 개선하여 간섭현상을 억제하였으며, 안전한 서비스를 받을 수 있도록 하였다.

그러므로 ISM 대역에 사용되는 BPSK/ QPSK/ π/4QPSK 변복조 방식을 통합사용이 가능하며 표준안에 적합한 SSEN 변복조 제어 프로세서를 근접 통신망에 적용하면 상호간섭 현상과 성능저하 억제에 효과적이고, 안전한 서비스를 제공 받을 수 있다.

참고 문헌

[1] Bluetooth, “Update on the Wireless Link for Mobile Computer”, May 8, 2000.

[2] Wireless Portable Devices, “World Market for 2G, 2.5G, and 3G Devices and Connectivity to the Wireless Internet”, Allied Business Intelligence. 1Q 2001.

[3] IDC, “Burgeoning Bluetooth”, April 2000.

[4] Test Mode, “Specification of the Bluetooth System part I”, 2002.

[5] Draft Standard, “Wireless LAN Medium Access Control(MAC) and Physical Layer (PHY) Specifications”, IEEE 802.11, July 1995.

[6] M. Gude, "Concept for a High Performance Random Number Generator Based on Physical Random Phenomena", Frequenz, Vol. 39, pp. 187-190, 1985.

[7] E. Biham, A. Shamir, "Differential Cryptanalysis of the Data Encryption Standard", Springer-verlag, 1993.

[8] E. Biham, A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems", Advances in Cryptology-CRYPTO'90 Proceeding, Springer-verlag, pp. 2-21, 1991.

[9] R. Gottfert, H. Neiderreiter, "On the Linear Complexity of Products of Shift Register Sequences", Advances in Cryptology-CRYPTO'93 Proceeding, Springer-verlag, pp. 151-158, 1994.

[10] 조경연, 송홍복, “비트슬라이스 대합 S-박스에 의한 대칭 SPN 블록암호”, 한국전자통신학회논문지, 6권, 2호, pp. 171-179, 2011.

[11] 나성훈, 신현식, “VoIP 보안 관련 주요기술에 대한 분석”, 한국전자통신학회논문지, 5권, 4호, pp. 385-390, 2010.

저자 소개

정우열(Woo-Yeol Jeong)

1982년 원광대학교 전자공학과(공학사)

1984년 경희대학교 대학원 전자공학과(공학석사)

1999년 원광대학교 대학원 전자공학과(공학박사)

1995년~현재 한려대학교 멀티미디어정보통신공학과 교수

※ 관심분야 : 이동통신시스템, 암호시스템, VLSI 설계

이선근(Seon-Keun Lee)

1995년 원광대학교 전자공학과(공학사)

1997년 원광대학교 대학원 전자공학과 (공학석사)

2003년 원광대학교 대학원 전자공학과 (공학박사)

2006년~2008년 원광대학교 전기전자 및 정보공학부 전임강사

※ 관심분야 : 이동통신시스템, 암호시스템, VLSI 설계