무선 키 갱신 프로토콜 OTAR의 암호 시스템 개선 방안☆

On the Security Enhancement of the OTAR Protocol and Cryptosystems

이 훈 재* 이 상 곤** 박 종 욱*** 윤 장 홍****
HoonJae Lee SangGon Lee JongWook Park JangHong Yoon

요 약

OTAR 시스템은 높은 보증 등급의 키 관리 기능을 구현한 것이며, 접근 통제, 무결성, 기밀성 기능을 확신할 수 있는 무선을 통한 원격 키 갱신 기술을 갖는다. 하지만 TIA/EIA OTAR 기술은 현실적인 측면에서 안전성의 개선이 요구된다. 본 논문에서는 무선 정보보안시스템에 적용 가능한 무선을 통한 키 갱신 기술인 TIA/EIA OTAR에 대한 보안 취약점을 분석한 후, 취약점을 수정 보완한 개선된 OTAR 보안 시스템을 제안한다. 제안 시스템에는 신뢰성이 높은 난수 동기방식을 포함한다.

Abstract

OTAR system is a highly authentic key management system that has functions with access control, data integrity and data confidentiality. In this paper, we analyze the existing TIA/EIA Over-The-Air-Rekeying key managements protocol, focused to symmetric ciphers. It can be used to understand the technical trend on technologies about TIA/EIA OTAR standardization. This results can be used to evaluate security properties of a remote rekeying. The proposed system contains a highly reliable system synchronization.

☞ Keyword : Component Integration, Connection Contract, Variability, Workflow, Component Architecture

Ⅰ. 서 론

암호 알고리즘 설계 시 일반적으로 개발자 및 공격자는 암호 알고리즘이 공개된 상태를 가정하여 알고리즘을 설계하며, 이때 알고리즘의 안전성은 암호 키에 크게 의존한다. 이러한 관점에서 암호 키의 관리는 암호 장비 연구 개발에 있어서 핵심 부분이다. 암호 키는 키 생성, 키 분배, 키 저장, 키 사용, 키 복구, 키 갱신, 키 폐기 및 키 보관 등의 생명 주기(life cycle)를 가진다. 특히, 키 갱신(rekeying)은 위협이나 어떤 동기로부터 사용 중인 키를 새로운 키로 교체하고자 할 때 사용하는 기능이다. 유선에 의한 갱신 및 무선에 의한 갱신이 가능하며, 키 갱신 시에는 반드시 식별 및 인증(identification and authentication) 기능이 필수적이다.

OTAR 시스템은 높은 보증 등급의 키 관리 기능을 구현한 것이며, 접근 통제, 무결성, 기밀성 기능을 확신할 수 있는 무선을 통한 원격 키 갱신 기술을 갖는다. 무선을 이용한 키 갱신 기술은 다음과 같은 적용 사례를 분석할 수 있다. 미국 TIA/EIA에서는 1996년 Project 25 Digital Radio Over- the-Air Rekeying (OTAR) Protocol (TIA/EIA-102 . AACA) [1,2]을 통하여 표준화하였다. 1990대 후반부터, TALK II-SINCGARS 무전기(Army, Marine Corps, Navy, Combat Air Forces)[3], 영국 TETRA 무전기[4], 미국 KY-99A 키 주입/갱신 장비[5] 등 이미 OTAR 기술이 적용된 안전한 무선 키 갱신 기술이 실용화 적용되고 있다.

* 정 회 원 : 동서대학교 인터넷공학부 교수
hjlee@dongseo.ac.kr(제 1저자)
** 정 회 원 : 동서대학교 인터넷공학부 교수
nok60@dongseo.ac.kr(공동저자)
*** 정 회 원 : 국가보안기술연구소 책임연구원
khspjw@etri.re.kr(공동저자)
**** 정 회 원 : 국가보안기술연구소 팀장
jhyoon@etri.re.kr(공동저자)
☆ 이 논문은 ITRC 육성지원사업 및 NSRI 위탁연구과제 지원에 의해 수행되었음.
[2004년/08/11 투고 - 2004/10/19 심사 - 2005/04/08 심사완료]

원격 키 갱신에 대한 주요 요구 기능은 다음과 같이 요약될 수 있다[6]. 첫째, 원격지로부터 통신 보안장비(COMSEC)에 키 갱신 기능이 적용되면 장비를 중앙 집결시킬 필요가 없어질 뿐 아니라, 야전지역에 신규 키를 전송할 필요성이 줄어든다. 둘째, 이동 과정에서 일어날 수 있는 키와 관련된 위협이 줄어들 뿐 아니라, 키 갱신을 위한 시간을 크게 단축시켜 준다. 셋째, 전술상황에서 네트워크 상의 한 노드가 적의 수중에 탈취되었을 때, 그 노드를 네트워크로부터 분리시킨 후 나머지 모든 노드를 원격으로 키 갱신할 수 있다는 점이다. 이렇게 되면 탈취된 키와 장비를 입수한 적으로부터 민감한 통신상황을 도청할 수 없게 만들며, 또한 네트워크상에서 유효한 단말인 척 보임으로써 적을 유인하여 기만 전술공격이 가능하게 된다.

본 연구에서는 최근 미국 통신보안장비를 위하여 표준화된 무선을 통한 키 갱신 기술 OTAR [6,7]에 대한 최신 표준화 연구동향을 분석하며, 본 기술을 적용하여 안전성과 신뢰성이 높은 무선 키 갱신 프로토콜의 설계 기초자료를 제공한다. 또한, TIA/EIA OTAR 시스템에 대한 보안 취약점을 분석한 후, 취약점을 수정 보완한 개선된 OTAR 보안 시스템을 제안한다. 제안될 보안 시스템에는 신뢰성이 높은 난수 동기방식이 적용되어야 한다.

II. OTAR 무선 키 갱신 알고리즘 표준화 분석

2.1 OTAR 요구사항

무선을 통한 키 초기화(OTAZ, over-the-air-zeroize)와 무선을 통한 키 전달(OTAT, over- the-air-transfer) 기술은 OTAR[6-16]와 연관성이 많은 기술이다. 이 과정들은 중앙 키 관리 센터로부터 분산 배치된 통신보안장비에 대하여 통신 링크를 통한 키 갱신, 초기화, 그리고 전달이 가능하게 한다. 이러한 과정에서의 하나의 큰 문제는 어떻게 하면 네트워크 통제국(network control station)과 종단 장비(end-user equipment) 간의 실체를 인증할 것인가 하는 문제이다. 적절한 식별 및 인증 서비스가 제공되지 않는다면, 정교한 적의 장비가 네트워크 통제 국으로 가장한 후 키를 갱신하고, 전술 망의 일부분이 적의 통제 하에 넘어가게 될 수도 있다.

이러한 취약점을 보완하기 위하여 IATF에서는 다음과 같은 요구사항을 제시하고 있다[6].

1) 전술 사용자는 EKMS (enhanced key management system), PKI (public key infrastructure) 및 재프로그래밍 가능한 암호설계 기능을 갖는 KMI (key management infrastructure)의 개발을 요구한다. 고신뢰 원격 제어 키관리 기능은 OTAR, OTAT 및 OTAZ 기능을 갖는 전술네트워크상에서 구현되어야 한다. 게다가, 프로세서들은 PKI 및 다중 네트워크상에서 키를 통제할 수 있도록 재프로그래밍 암호 장비에 대한 타협 키 정보를 설정할 수 있어야 한다.
2) 전술 사용자는 야전에 배치된 종단 보안장비에 전달하는 모든 방법상에 있어서 키 타협의 취약성을 극적으로 줄일 수 있도록 블랙 키를 전달하는 절차를 요구한다.
3) 고신뢰 식별 및 인증 서비스가 네트워크 관리국과 OTAR, OTAT 및 OTAZ 기능을 위한 종단 사용자 모두에게 요구된다.
4) 전술 사용자는 어떤 전술 자동화 시스템에서도 작동될 수 있는 OTAR 운용에 대한 자동화된 과정을 가져야 한다.
5) 전술 사용자는 다양한 암호 키 형태와 다양한 종단 시스템에서 작동될 수 있는 공통 키 충진 장치를 가져야 한다.

2.2 APCO 표준문서와 키 관리 유형

본 항에서는 TIA/EIA Telecommunications Systems Bulletin, APCO Project 25, TSB102.AACA [1]

에 대하여 다룬다. APCO (Association of Public Safety Communication Officials International)는 국제 공공 안전통신 사무협회를 말한다.

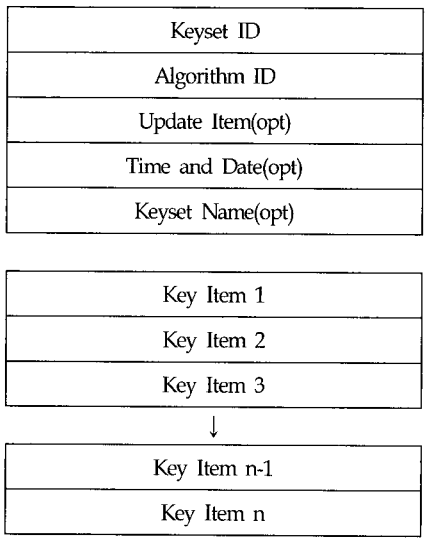
APCO 프로젝트 25 표준은 공공 안전 지상 이동무선통신(public safety land mobile radio communications)을 위한 시스템상의 모든 부분을 다룬다. 이들 시스템은 가입자 유니트, 기지국 및 고정장치들을 포함한다. 가입자 유니트는 휴대형 무전기와 차량용 이동 무전기를 포함하며, 기지국은 지형학적 고정 시스템을 말한다. 고정 장치로는 원거리 작동 및 콘솔 작동기를 들 수 있으며, 컴퓨터 장치는 상기 장치들을 연결해주는 인터페이스로 사용된다. 공통 무선 인터페이스(CAI, Common Air Interface)는 무선 채널을 통하여 디지털 정보를 송.수신토록 하는 인터페이스 장치이다.

TSB-102, APCO 프로젝트 25 시스템 및 표준 정의[8]에는 4가지 보안 유형(Type 1, Type 2, Type 3, Type 4)의 암호화 보안(encryption security)이 정의되어 있다. 유형-1은 비밀로 분류된 국가 정부 통신(classified national government communications), 유형-2는 공개된 국가 보안 관련 통신(unclassified national security related communications), 유형-3은 공개된 민감한 정부 통신(unclassified sensitive government communications), 예를 들면, 공공 보안(public safety), 유형-4는 수출 가능한 암호화(exportable encryption)로 정의된다. 만일 키가 DES와 같은 유형-3 암호 알고리즘이라면, 이 때 키 관리 역시 유형-3이며, OTAR 역시 유형-3을 따른다. 같은 토큰에 의하여, 만일 암호 알고리즘이 유형-1이라면, 키 관리 및 OTAR 역시 유형-1을 따른다. OTAR의 모든 유형은 기능이 유사하다. *OTAR 프로토콜* 문서는 연결된 여러 무선 장비(출처와 관계없이)들 사이에 상호 작용을 조정하도록 설계한 포괄적인 문서이다. OTAR 문서는 유형-3 OTAR에 대한 APCO 프로젝트 25의 OTAR 프로토콜을 정의한다.

2.3 OTAR 무선 키 갱신 알고리즘 및 취약점 분석

2.3.1 키 갱신 알고리즘

키의 암호학적 기간 연장을 위한 키 갱신은 결정론적이지만 비가역적으로 키를 변경하는 암호학적 처리과정이라 정의된다. 키들은 주기적으로 갱신되어 새로운 키 값이 된다. 갱신은 무선기기가 키 관리 장치인 KMF(Key Management Facility)로부터 명령을 받거나 지정된 날짜 및 시간에 따라 자동으로 수행된다. 어떤 키에 대하여 수행된 갱신 횟수를 갱신카운터(update count)라 부른다. 허용 갱신회수(updates allowed)는 키가 대체되어지기 전에 한 개의 키에서 실행될 수 있는 허용된 최대 갱신횟수를 규정한다. 타입 1 키에 대한한 구체적인 키 갱신 알고리즘이 미연방표준 1104(Federal Standard 1104)에 정의되어 있다.



〈그림 1〉 키 세트 사용 예

효율적인 키 관리를 위해서 많은 키들이 함께 그룹화되며, 이러한 키 그룹들을 키 세트라 한다. 키 세트는 같은 알고리즘을 위한 것이나, 같은 형태

의 (TEK or KEK; Traffic-Encryption Key or Key-Encryption Key) 키들을 하나 또는 그 이상 포함한다. 키 세트 내의 모든 키들은 같은 암호학적 기간, 갱신 파라미터 그리고 자동 키 관리를 사용할 때 활성화 시간을 가진다. 키 세트 내에서 이 정보는 공통이기 때문에 각각의 개인 키로 저장될 필요가 없다는 것을 알 수 있다. 키 세트마다 논리적 ID가 할당되고 모든 관리는 키 세트를 통하여 수행된다. 키 세트의 예는 그림 1에서 보여준다. 키 세트는 사용자 선택이나 KMF의 무선 명령, 또는 지정된 날짜와 시간에 따라 자동적용 방법 등에 의하여 활성화 된다. 키 세트가 활성이라면, 키 세트 내의 키들이 트래픽을 암호화하는데 사용되어짐을 의미한다.

키 세트의 그룹을 암호그룹(crypto group)이라 부르며, 암호그룹들은 키 관리를 편리하게 해준다. 암호그룹은 같은 종류의 키(TEKs or KEKs)로 구성된 하나 또는 그 이상의 키 세트들로 구성된다. 하나의 암호그룹 내에 오직 하나의 키 세트가 어떤 주어진 시간 내에 활성화 될 것이다. 암호그룹 내의 키 세트들의 전형적인 사용은 하나의 활성화된 키 세트와 그 다음에 활성화될 하나 또는 그 이상의 미래 키 세트를 가지는 것이다. 이것은 암호그룹내의 다른 키 세트들이 키 갱신되는 동안, 하나의 활성화된 키 세트를 MR(Mobile Radio)에게 제공한다. 활성화된 키 세트 내의 키들의 암호기간이 만료되면, MR은 암호그룹 내의 다른 키 세트들로 변경하도록 명령을 받게 된다.

MR내에 키 값이 어떻게 저장되는지와 특정한 전송을 암호화하는데 사용될 TEK를 선택하는 한 방법은 다음과 같다. 이 방법은 하나의 MR 채널, 대화 그룹(Talk Group, TGID), 또는 데이터 그룹(Data Group, LLID)을 하나의 TEK로 연결시킨다. 이러한 매핑은 그 MR channel 상에 전송이 있을 경우나 그 TG에 메시지가 전달될 경우 어느 TEK를 사용할 것인지를 규정한다. MR 채널, 대화 그룹, 데이터 그룹 등을 TEK에 연결시키는데 사용되는 매개변수는 SLN(Storage Location Number)로 알려져 있다. 키 세트 ID와 결합되어진 SLN은 ALGID(algorithm identification)나 KID(key identification)를 참조하지 않고도 전송 암호화에 사용될 적당한 TEK를 간접적으로 가리키는데 사용된다. (사용자는 그가 원하고 제조회사에서 허락하는 한 간접 키 매핑을 사용하지 않고도 수동으로 키를 선택할 수 있다.) SLN은 특정 암호그룹에 있는 활성화된 키 세트 내에 있는 암호그룹과 키를 규정한다. SLN은 암호그룹들 사이에 중복될 수 없다. 활성화된 키 세트 그 자체는 KMF로부터 명령에 의하여 선택된다.

기존 OTAR 시스템의 취약점은 안전성이 낮은 DES 암호 알고리즘과 MD5를 사용하고 있으며, 또한 단일 알고리즘을 사용함으로써 적용 통신망에 따라 다양한 적용이 불가능한 단점을 지닌다.

2.3.2 OTAR 취약점

OTAR에 사용된 표준화 암호 알고리즘은 기밀성 서비스를 위하여 DES 암호 알고리즘, 인증서비스를 위하여 MD5 알고리즘이 적용되고 있다. 현 수준에서의 안전성을 고려할 때 DES 알고리즘은 취약한 알고리즘이며, 따라서 이를 대체할 안전한 알고리즘이 요구된다. 또한 다양한 통신망 접속을 위하여 경량·고속화 스트림 알고리즘이나 키 크기가 다양하게 적용되는 블록 암호 알고리즘과 같은 다양한 선택이 필요하다. 인증시스템의 경우에도 다양한 알고리즘이 적용될 필요가 있다.

III. 개선된 OTAR 시스템 제안

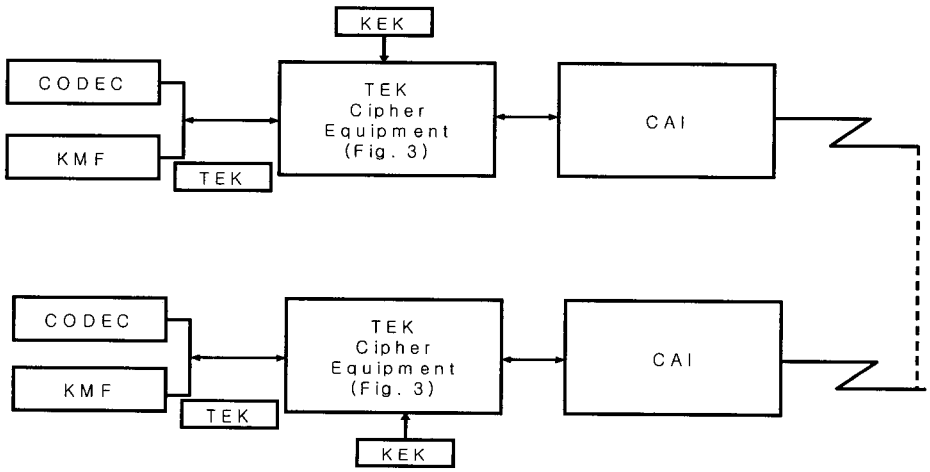
본 논문에서는 OTAR 기능을 갖는 암호시스템을 제안하고, 암호시스템의 비트 스트림통신을 위한 스트림동기방식을 설계 제안한다. 비트 스트림 통신에서는 송·수신 암호문 출력 수열의 동기가 일치되지 않으면 암호문으로부터 평문을 복호할 수 없기 때문에 스트림동기(stream synchroniza-

tion)가 필수적이다. 송·수신단에서 동일한 비트 스트림을 유지하기 위하여 비트 수열의 시작점을 일치시켜야 하며, 실제로 시작점을 맞추기 위해서는 추가적인 동기 신호의 교환이 따라야 한다. 스트림동기 방식은 비트 수열의 동기를 일치시키는 횟수에 따라 초기 동기 방식(initial synchronization)과 연속 동기 방식(continuous synchronization)으로 분류된다. 초기 동기 방식에서는 1대 다수 통신시 나중 가입자에게는 암호 통신이 불가능하게 되지만, 연속 동기 방식에서는 나중 가입자도 암호 통신이 가능하다. 그러므로 연속 동기 방식은 통신 효율은 떨어지더라도 채널 오류가 많은 무선 통신망 또는 반이중(half duplex) 통신에 유리하며, 초기 동기 방식은 채널 상태가 양호한 유선 통신망, 전이중(full duplex) 통신에 많이 쓰인다. 본 연구에서 제안된 방식은 초기동기방식과 연속동기방식의 혼합형이며, 통신 초기에 동기신호의 교환이 이루어지고, OTAR 시스템의 암호 통신도중에 에러가 발생될 경우에만 재동기를 이루게 된다.

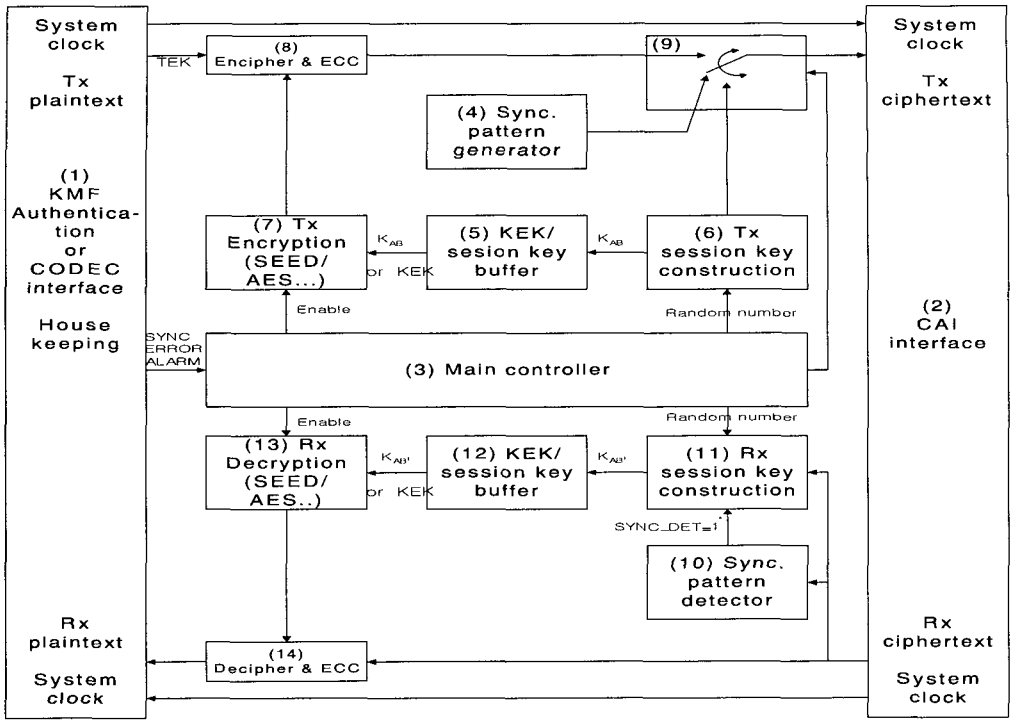
3.1 OTAR 기능을 갖는 암호시스템 제안

무선 MR을 통하여 TEK를 전송하기 위한 제안 암호 시스템은 그림 2와 같이 CODEC을 통하여 아날로그 신호를 디지털 데이터로 전환한 다음 암호 시스템에 적용되며, 암호화 이후에는 MODEM 또는 CAI로 연결된다.

무선 단말 데이터 보호를 위한 OTAR 기능을 내장한 제안 암호 시스템의 블록 구성도는 그림 2와 같다. 그림에서 암호 장치는 KMF/CODEC 후단에 위치하며, 그 시스템 내부 구성은 그림 3과 같다. 블록 (1)은 코덱 인터페이스 또는 KMF 인증부 인터페이스 회로이다. 블록 (2)는 CAI 기능을 갖는 회로이다. 블록 (3)은 본 시스템 전체를 제어하는 주 제어 장치(main controller), 블록 (4)는 암호 동기 패턴을 발생하는 동기 패턴 발생기(synchronization pattern generator), 블록 (5)와 (12)는 TEK 또는 송·수신 세션 키 버퍼(session key buffer), 블록 (6)과 (11)은 공개 전송로 상에서 안전하게 세션 키를 분배하기 위한 송·수신 세션 키 구성(session key construction), 블록 (7)과 (13)은 고비도 특성의 송·수신 암호 알고리즘(예, SEED, AES 등), 블록 (8)과 (14)는 송·수신 암호화/복호화 연산(XOR) 및 ECC(error control code), 블록(9)는 동기 패턴/세션 키/암호문의 구분 선택을 위한 선택 스위치(data selector), 블록 (10)은 송신단에서 발생한 암호 동기 패턴을



〈 그림 2〉 KMF/CODEC 및 암호시스템 제안



〈그림 3〉 OTAR 기능을 갖는 암호 시스템 블록 제안

검출하기 위한 동기 패턴 검출기이다.

3.2 암호 알고리즘 선택 및 적용 제안

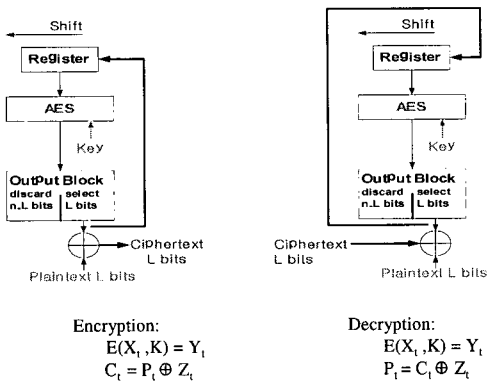
암호 방법은 스트림 암호, 블록 암호 그리고 공개키 암호로 분류될 수 있으며, 블록 암호의 적용 방법은 ECB (electronic codebook) 모드, CFB (cipher feedback) 모드, CBC (cipher block chaining) 모드 및 OFB (output feedback) 모드가 있다. 본 절에서는 MR에 적용된 암호 알고리즘을 신규 설계 및 선택하는 문제를 고려한다. 선택 가능한 알고리즘은 블록 암호를 무선 환경에 맞게 OFB 모드 적용방법과 스트림 암호를 적용하는 두 가지 방법으로 접근한다.

3.2.1 블록 암호의 OFB 모드 적용 방법 제안

블록 암호의 OFB 모드는 잡음이 많은 무선 선로 등에서 적용이 가능하다. 블록 암호를 암호화에 그대로 적용(ECB 모드)할 경우 채널 특성이 나빠질 수 있기 때문에 OFB 모드로 전환하여 적용할 수 있다.

OFB 모드를 적용할 수 있는 알고리즘은 대부분의 블록 암호에 해당한다. 본 연구에서는 기존의 OTAR 프로토콜에 사용된 DES 알고리즘의 암호 취약점을 보완할 수 있는 국제적으로 검증된 알고리즘을 고려하였다. 그 결과, 표 5와 같이 미국 FIPS-197 표준 암호 AES 알고리즘[18], Triple-DES 알고리즘, 국내 표준 암호 SEED 알고리즘[19], 그리고 IDEA 암호 알고리즘 등이 적용 가능하다.

무선 통신 방식의 OTAR 적용을 위하여 OFB 모드 적용이 필요하며, 그림 4는 AES-OFB 모드 적용기법을 나타내었다. OFB 모드는 암호 알고리즘을 의사 랜덤 수열 발생기(PN-generator)로 변



〈그림 4〉 AES-OFB 모드 적용

〈표 1〉 OTAR 개선에 적용될 암호 알고리즘 제안

기존 OTAR 알고리즘		개선된 OTAR 알고리즘	
기밀성 알고리즘	인증 알고리즘	기밀성 알고리즘	인증 알고리즘
DES	MD5	1) Block cipher: AES[18], SEED[19], T-DES, IDEA 2) Stream cipher: LILI-II[22] Parallel LM[23]	SHA-160[20], SHA-1[21], MD5, SEED-CBC, AES-CBC, T-DES-CBC, IDEA-CBC

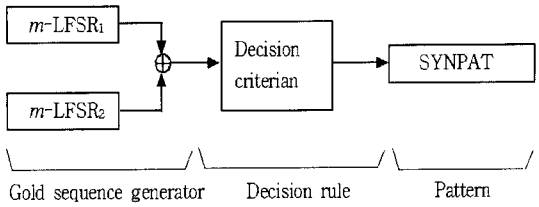
환시켜 활용하며, 출력 블록(output block)을 입력 레지스터로 귀환시켜 PN-수열을 발생한 다음 입력 평문과 bit-by-bit XOR (exclusive-OR) 연산을 수행하여 암호문을 생성한다.

3.2.2 스트림 암호 적용 방법 제안

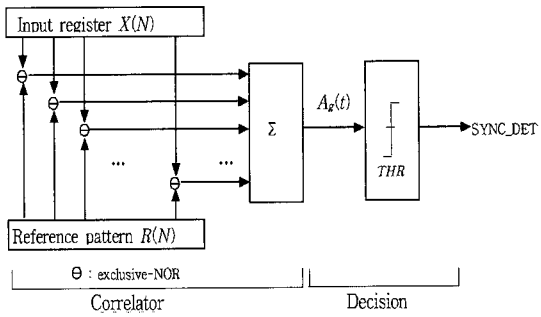
무선통신에 적합한 스트림 암호 알고리즘으로는 LILI-II[22]와 Parallel LM[23]을 들 수 있다. LILI-II의 경우 안전성이 높고, 고속화가 가능하며, parallel LM은 기존 LM 발생기를 고속화하기 위하여 병렬 스트림 암호(parallel stream cipher) 기법을 적용하였다.

3.3 신뢰성이 높은 암호동기방식 설계

본 논문에서는 N의 증가에 대하여 하드웨어 복잡



a) Synchronization pattern generator.



b) Synchronization pattern detector.

〈그림 5〉 암호 동기 패턴 발생기와 검출기

도가 거의 선형적으로 증가되는 자기 상관기(Autocorrelator)를 설계한다.

3.3.1 자기 상관기와 암호 동기

암호 동기부는 블록암호의 OFB 모드나 동기식 스트림 암호에서 송·수신 암호 동기화 역할을 하는데, 일반화된 모델은 그림 5와 같다. 동기 패턴에 대한 자기 상관값 $A(t)$, 문턱 값(Threshold) THR, N_T는 다음과 같다[17].

$$\begin{cases} A(t) = \dfrac{A_g(t) - D_g(t)}{N} \\ THR = N - N_T \end{cases} \quad (4\text{-}1)$$

여기서, $A_g(t) = \sum_{i=1}^{N} X(i) \ominus R(i)$는 일치 비트수, $D_g(t) = \sum_{i=1}^{N} X(i) \oplus R(i)$는 불일치 비트수, $A_g(t) + D_g(t) = N$ 이다.

그림 5 b)의 동기 패턴 검출기(Sync pattern

detector)는 합산 부분을 시스템 클럭에 맞추어 1 클럭만에 옳고 그름을 계산해야 내어야 하므로 이를 하드웨어로 구현하기에는 너무 복잡해진다.

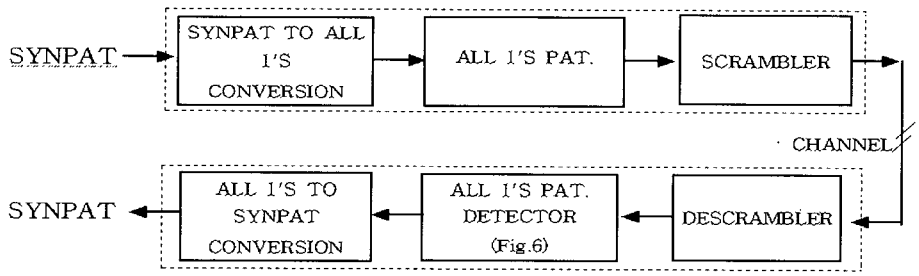
3.3.2 자기상관기 개선 시스템

일반적인 동기 패턴은 랜덤한 값으로 구성되어 있기 때문에 동기 패턴 검출기는 N이 커질수록 구현이 더 복잡해진다. 그러므로 랜덤한 동기 패턴을 단순 패턴으로 변환시켰다가 다시 역변환시키면 하드웨어 복잡도를 줄일 수 있음을 알 수 있다. 즉, 임의의 동기 패턴에 대하여 모든 비트가 "1"(all 1's pattern)이나 "0"(all 0's pattern), "10" 반복 또는 "1100" 반복 등과 같은 단순 패턴으로 변환한 후 일치 비트 수(number of agreement bits)를 구하면 의외로 하드웨어가 간단해진다. 다만 단순 패턴 그 자체는 자기 상관성이 낮아서 동기 패턴으로 적합치 않으므로 자기 상관성이 우수한 동기 패턴을 생성한 후 단순 패턴으로 변환시키는 과정이 별도로 필요하다. 또한 단순 패턴은 송신시 선로 부호화상에서 문제(연속 "0" 또는 연속 "1"로 인한 모뎀 클럭 복구 문제등)가 될 수 있기 때문에 이를 방지하기 위하여 간단한 스크램블러와 디스크램블러를 추가하여야 한다. 이를 도시한 것이 그림 6이다.

그림에서 송신단의 스크램블러는 전 비트 "1" 패턴을 랜덤한 패턴으로 변경시켜 주고 수신단의 디스크램블러는 그 역 과정에 해당하며, 이들은 선로 특성에 맞게 간단히 구현될 수 있다. 또한 수신단에서의 전 비트 "1" 패턴 검출기(all 1's pattern detector)를 자세히 나타낸 것이 그림 7이다. 그림에서 전 비트 "1" 패턴 또는 랜덤 패턴이 N단 레지스터에 입력되면 업-다운 카운터는 레지스터가 보유한 "1"의 갯수를 카운트한다. 즉, 이동 레지스터의 첫째 단에 "1"이 입력되면 카운터는 증가되고, 최종단에서 "1"이 출력되면 카운터는 감소되기 때문에 이 카운터는 이동 레지스터에 포함되어 있는 "1"의 갯수를 항상 보유하게 된다. 출력단에서는 카운터 값을 문턱 값(N_T)과 비교하여 그 보다 크면 동기 검출 사실(SYNC_DET=1)을 알려준다.

3.4 키 암호화(키 랩핑)

키 암호화 키(KEK, Key Encryption Key) 또는 트래픽 암호화 키(TEK, Traffic Encryption Key)



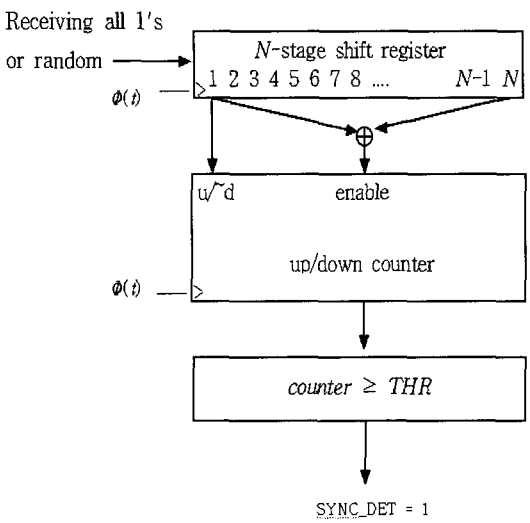
SYNPAT = 6DDA 5191 7C90 726C 7941 AD04 6ABC 8F5D (hexa)

or

SYNPAT2 = 1394 DA8D 7272 C579 B3A8 B379 4BA0 087E (hexa)

= 0001 0011 1001 0100 1101 1010 1000 1101
0111 0010 0111 0010 1100 0101 0111 1001
1011 0011 1010 1000 1011 0011 0111 1001
0100 1011 1010 0000 0000 1000 0111 1110

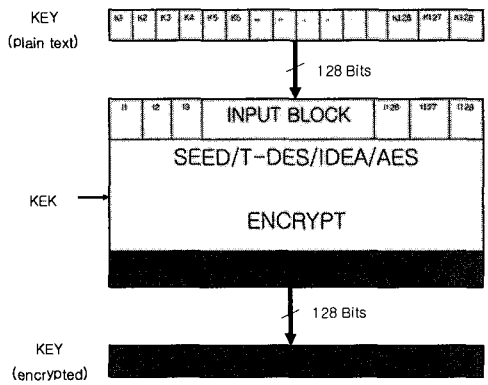
〈그림 6〉 단순 패턴을 이용한 키수열 동기 방식 설계제안



shift register 1 N	counter
0 0	disable down(enable)
0 1	up(enable)
1 0	disable
1 1	

〈그림 7〉 모든 비트 "1" 패턴 검출기 제안

가 유형-3 KMM(Key Management Messages)을 포함하는 모든 SEED/T-DES/IDEA/AES 유형-3 키는 128-비트 길이를 갖게 될 것이다. KMM에 포함된 모든 키는 ECB(Electrinic CodeBook) 모드로 암호화되어야 한다. 이 암호화 과정에 사용된 키는 KEK가 된다. KEK는 다른 키를 암호화시키는데 유일하게 사용된다.



〈그림 8〉 개선된 키 암호화 과정

평문 키를 암호화시키는 개선된 과정은 그림 8에 나타내었다. 128-비트 입력 키는 EED/T-DES/ IDEA /AES를 갖는 ENCRYPT 입력 블록으로 입력되고, 단일 ENCRYPT 암호화가 수행되어 128-비트 출력 블록을 생성한다. 개선 과정에서는 기존의 64-비트 DES 키 암호화 과정 대신 128-비트 SEED/T-DES/IDEA/AES 등과 같은 안전성이 강화된 키 암호화 과정이 적용된다. 이 때 블록 크기의 확장에 따른 동기 블록의 크기 역시 64비트에서 128 비트로 확장되어야 할 필요가 있다.

SEED의 경우에는 입력 블록이 128 비트이며, 키 크기도 128 비트이기 때문에 1회 암호화를 수행하여 128 비트 암호화된 키 출력을 얻을 수 있다. T-DES의 경우에는 입력 블록이 128 비트이며, 키 크기도 128 비트(패리티 비트 포함)이기 때문에 1회 암호화를 수행하여 128 비트 암호화된 키 출력을 얻을 수 있다. AES의 경우에는 128/192/256 비트로 다양한 입력이 가능하며, 이 프로토콜에서는 128 비트의 경우로 한정한다. 이 때 AES 입력 블록이 128 비트이며, 키 크기도 128 비트이기 때문에 1회 암호화를 수행하여 128 비트 암호화된 키 출력을 얻을 수 있다. IDEA의 경우에는 입력/출력 블록이 64 비트이며, 키 크기는 128 비트이기 때문에, 출력 블록을 128에 맞추기 위하여 64 비트 단위로 암호화 과정을 2회 수행하여 128 비트 암호화된 키 출력을 얻을 수 있다.

3.5 메시지 인증(Message Authentication)

메시지는 FIPS PUB 81에 정의된 DES를 개선하여 SEED/AES를 사용한 128-비트 SEED-CBC/AES-CBC 모드 또는 128-비트 SEED-CFB/AES-CFB 모드로 인증되어야 한다. 두 가지 운용 모드는 제공된 알고리즘이 아래와 같이 초기화되는 같은 MAC을 생성하게 될 것이다.: 1) CBC에서는, 초기 벡터 (IV, Initialization Vector)가 전체 "0"로 채워지고, 2) CFB에서는, 초기 벡터

는 첫 128 비트 믿을 수 있는 데이터로 채워진다.

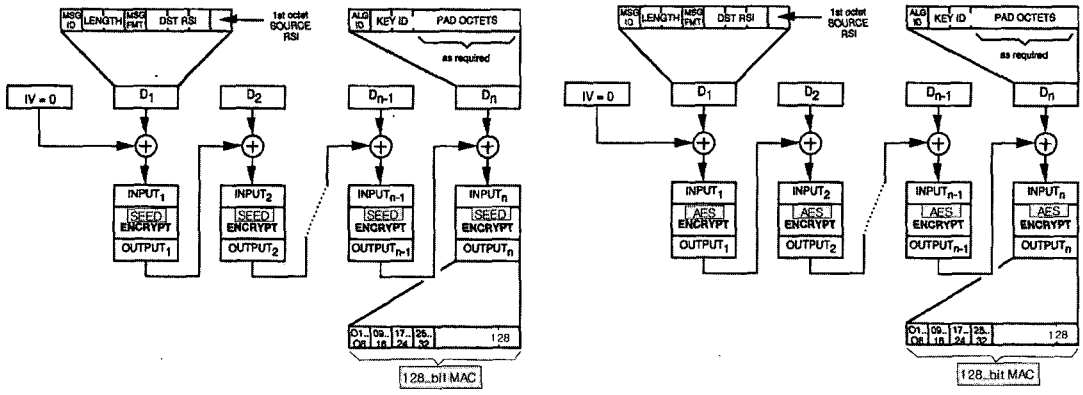
그림 9는 CBC 모드 운용에 대한 인증 과정을 보여준다. SEED/AES 입력 레지스터는 첫 128-비트 블록 데이터(D1)으로 초기화된다. (KMM에 대하여 이 첫 입력 블록은 메시지 ID(Message ID), 메시지 길이(Message Length), 메시지 형식(Message Format), 그리고 SEED/AES 입력 레지스터에 좌로 정렬될 메시지 ID를 갖는 목적지 RSI 필드 및 소스 RSI 필드의 첫 옥텟으로 구성된다.) 이 입력 블록은 128-비트 출력 블록(O1)을 발생시키는 인증을 위하여 선택된 키를 사용하여 암호화된다. 이 암호문 출력 블록은 인증될 두 번째 128-비트 데이터와 비트-단위의 배타적 논리합(XOR, bit-wise exclusive-ored)으로 계산된다. 이 연산의 실행 결과는 SEED/AES 입력 레지스터에 채워진다. 이 블록은 암호화된 다음, 결과 출력 블록이 인증될 세 번째 128-비트 데이터와 XOR 연산된다.

만일 메시지가 128-비트 데이터 블록의 합성 수(integral number)로 구성되지 않는다면, 최종 부분 데이터 블록(D_n)은 좌로 정렬되고, 전체 데이터 블록의 나머지는 "0"으로 채워진다. 이 부가 데이터 블록(padded data block)은 현재 출력 암호문 블록(O_{n-1})과 XOR 연산된다. 결과 블록은 SEED/AES로 입력되며, 최종 출력 블록을 생성하기 위하여 암호화된다. 최종 블록 128-비트는 MAC으로 정의된다. (이 절차에 의하여 생성된 모든 암호문은 버려진다.) 인증될 메시지 데이터는 메시지 ID로 시작되며, MAC 필드의 처음 세 개의 옥텟, 즉, (인증) 알고리즘 ID와 (인증) 키 ID, 를 통하여 계속된다. 이 동일한 과정이 수신 메시지 상에서 MAC를 계산하고, 메시지 목적지에서 수신된 MAC을 검증하기 위하여 적용된다.

SEED-CBC/AES-CBC/MD-5를 사용할 경우에는 MAC 코드 값이 128 비트이므로, 이때 모든 비트가 출력된다. 하지만 HAS-160 [20]/ SHA- 1 [21]을 사용할 경우에는 MAC 코드 값이 160 비트이므로, 이때 처음 128 비트를 적용하고, 나머지 32 비트는 버리게 된다.

3.6 비교 분석

비교 분석 결과를 (표 2)에 나타내었으며, OTAR 적용시 대칭키 방식에서는 암호장비의 키를, 인증서(공개키) 방식에서는 신규 인증서와 신규 키를 무선-원격으로 갱신한다. OTAZ 기술은 대칭 키 방식에서는 암호 주기가 종료되는 시점에서, 인증서(공개키) 방식에서는 사용 종료 시점에서 비밀



a) 128-bit SEED-CBC MAC 적용 방안

b) 128-bit AES-CBC MAC 적용 방안

〈그림 9〉 개선된 인증 알고리즘(SEED/AES)

〈표 2〉 OTAR 방법에 대한 분석 결과

항목		OTAR 시스템		비고
		기존	제안	
Rekey(OTAR) 암호화기능		암호장비의 무선 원격 갱신용 키 암호화 - DES/ECB 모드(56-비트)	- AES(128-비트) - SEED(128-비트) - IDEA(128-비트) - TDES(112-비트)	보안 기능 개선
Rekey(OTAR) 인증기능		암호장비의 무선 원격 갱신용 키 인증 - DES/CBC 모드(56-비트)	- AES(128-비트) - SEED(128-비트) - IDEA(128-비트) - TDES(112-비트)	인증 기능 개선
암호동기 신뢰성		중	상	
인증 파라미터		ALGID(알고리즘 ID), KEYID(키 ID), TOD(Time of Date), KEK 등	ALGID(알고리즘 ID), KEYID (키 ID), TOD(Time of Date), KEK 등	
Security Services	Authentication	△	○	
	Nonrepudiation	△	○	
	Transmission Confidentiality	△	○	
	File Encryption	○	○	
	Integrity	△	○	
	Availability (e.g. Spread Spectrum)	○	○	
	Key Management	○	○	
비트 스트림동기방식		"없음"(표준화 문서)	- 신규 제안 - 하드웨어구현 용이	고신뢰도 통신 기능 포함
OTAR 기능을 갖는 암호시스템		"없음"(표준화 문서)	- 신규 제안 - 하드웨어 및 소프트웨어 구현 용이	

○ : 보안서비스-상위, △ : 보안서비스-중급

키를 무선-원격으로 갱신한다. 적용될 암호화 유형은 각각 키 관리 유형-III, 유형-I로 구분되어짐을 알 수 있었다. 인증 파라미터로는 대칭키 방식에서는 ALGID, KEYID, TOD(Time of Date), KEK 등이 적용됨을 알 수 있었다. 보안 서비스의 경우 기존의 시스템은 인증기능, 부인 봉쇄 기능, 전송 기밀성, 무결성 기능에 대한 안전성이 DES 수준에 의존하기 때문에 안전성이 중급으로 평가되며, 제안 시스템의 경우 AES/IDEA/SEED /TDES/LILI-II/등과 같은 최신암호 알고리즘으로 구성된다. 또한 제안 시스템은 비트 스트림 동기방식을 구체화 설계하였으며, OTAR 기능을 갖는 암호시스템을 구체화하여 설계 제안하였다.

IV. 결 론

OTAR 시스템은 높은 보증 등급의 키 관리 기능을 구현한 것이며, 접근 통제, 무결성, 기밀성 기능을 확신할 수 있는 무선을 통한 원격 키 갱신 기술을 갖는다. 본 논문에서는 대칭키와 공개키 방식에서의 OTAR 기술 적용에 대한 최신 표준화 연구동향을 표준 문서와 문헌 등을 통하여 분석하였다. OTAR 적용시 대칭키 방식에서는 암호장비의 키를, 인증서(공개키) 방식에서는 신규 인증서와 신규 키를 무선-원격으로 갱신한다. OTAZ 기술은 대칭 키 방식에서는 암호 주기가 종료되는 시점에서, 인증서(공개키) 방식에서는 사용 종료 시

점에서 비밀 키를 무선-원격으로 갱신한다. 적용될 암호화 유형은 각각 키 관리 유형-III, 유형-I로 구분되어짐을 알 수 있었다. 인증 파라미터 파라미터로는 대칭키 방식에서는 ALGID, KEYID, TOD, KEK 등이 적용됨을 알 수 있었다.

결론적으로, 본 연구에서는 최근 미국 통신보안 장비를 위하여 표준화된 무선을 통한 키 갱신 기술 OTAR에 대한 최신 연구동향을 분석하였으며, 본 기술을 적용하여 안전성과 신뢰성이 높은 무선 방식의 키 갱신 프로토콜의 설계 기초자료를 분석하였다. 또한, TIA/EIA OTAR 시스템에 대한 보안 취약점을 분석한 후, 취약점을 수정 보완한 개선된 OTAR 보안 시스템을 제안하였다. 제안 시스템은 비트 스트림 동기방식을 구체화 설계하였으며, OTAR 기능을 갖는 암호시스템을 구체화하여 설계하였다.

참 고 문 헌

[1] TIA/EIA Telecommunications Systems Bulletin, APCO Project 25, TSB102. AACA, "Over-The-Air-Rekeying(OTAR) Protocol New Technology Standards Project Digital Radio Technical Standards," Jan. 1996.

[2] TIA/EIA Telecommunications Systems Bulletin, TSB 102.AACB, "Over-The-Air -Rekeying (OTAR) Operational Description," Jan. 1997.

[3] TALK II-SINCGARS (ARMY, MARINE CORPS, NAVY, COMBAT AIR FORCES), http://www.armymard.net/ArmyMARS/Mil-Equip-Manuals/Resources/sincgars.pdf

[4] ETS 300 396-1: "Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); Direct Mode; Part 1: General network design"

[5] Minterm KY-99A, http://www.acd.itt.com/pdf/minterm.pdf, 1999.

[6] NSA, "Information Assurance Technical Framework," *IATF Release 3.1(unclassified)*, Sep. 2002. Web site, http://www.iatf.net/framework_docs/version-3_1/docfile.cfm?chapter=ch09.

[7] TIA COMMITTEE TR-45, "Compendium of Emergency Telecommunications and Telecommunications Network Security-related Work Activities within the Telecommunications Industry Association (TIA)," *MOBILE & PERSONAL COMMUNICATIONS STANDARDS(TR-45)*, Sep. 4-5, 2002.

[8] Project 25 *System and Standards Definition*, TIA, TSB-102.

[9] TSB-102.BAAA, *Recommanded Common Air Interface*, TIA.

[10] FIPS Publication 46-2, *Data Encryption Standard*, NIST.

[11] FIPS Publication 81, *DES Modes of Operation*, NIST, , December 2, 1980.

[12] ANSI X3.92, *Data Encryption Algorithm*, ANSI, 1981

[13] ANSI X3.106, *Data Encryption Algorithm -Modes of Operation*, ANSI, 1983

[14] IS-102.AAAA, *DES Encryption Protocol*, TIA.

[15] TSB-102.BAAD, *Common Air Interface Operational Description for Conventional Channels*, TIA.

[16] TSB-102.BAAC, *Common Air Interface Reserved Values*, TIA.

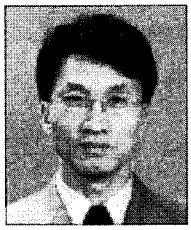
[17] H. J. Beker and F. C. Piper, *Secure Speech Communications*, Academic Press, London, 1985.

[18] NIST, "Announcing the Advanced Encryption Standard (AES)", FIPS-197, Nov. 2001

[19] KISA, "128비트 블록 암호알고리즘(SEED)," 1998년 10월. (http://www.kisa.or.kr)
[20] 한국정보통신기술협회, "해쉬함수 표준 - 제2부 해쉬함수 알고리즘(HAS-160), 1998. 11
[21] NIST, "Secure Hash standard - FIPS PUB 180-1, Department of Commerce, Washington D.C., Apr. 1995.
[22] A. Clark, E. Dawson, J. Fuller, J. Golic, Hoon-Jae Lee, W. Millan, Sang-Jae Moon, L. Simpson, "The LILI-II Keystream Generator," LNCS 2384, pp.25-39, Jul. 2002 (ACISP'2002)
[23] Hoonjae Lee, Sangjae Moon, "Parallel Stream Cipher for Secure High-Speed Communications," Signal Processing, Vol. 82, No.2, pp.259-265, Feb. 2002.

◐ 저 자 소 개 ◑

이 훈 재 (HoonJae Lee)
1985년 경북대학교 전자공학과 졸업(학사)
1987년 경북대학교 대학원 전자공학과 졸업(석사)
1998년 경북대학교 대학원 전자공학과 졸업(박사)
1987년2월~1998년1월 국방과학연구소 선임연구원
1998년3월~2002년2월 경운대학교 컴퓨터공학과 조교수
2002년3월~현재 동서대학교 인터넷공학부 조교수
관심분야 : 정보보안, 네트워크 보안, 스마트카드 보안, etc.
E-mail : hjlee@dongseo.ac.kr



이 상 곤 (SangGon Lee)
1986년 2월 경북대학교교 전자공학과 졸업(학사)
1988년 2월 경북대학교 대학원 전자공학과 졸업(석사)
1993년 2월 경북대학교 대학원 전자공학과 졸업(박사)
1991년 3월~1997년2월 창신대학교 정보통신과 조교수
1997년 3월~현재 동서대학교 인터넷공학부 조교수
관심분야 : 암호 프로토콜, 네트워크 보안, 자바기술
E-mail : nok60@dongseo.ac.kr

박 종 욱 (JongWook Park)
1986년 경북대학교 전자공학과 졸업(학사)
1988년 경북대학교 대학원 전자공학과 졸업(석사)
2002년 경북대학교 대학원 전자공학과 졸업(박사)
2000.2~현재 국가보안기술연구소 책임연구원
관심분야 : 정보통신보안 etc.
E-mail : khspjw@etri.re.kr

윤 장 홍 (JangHong Yoon)
1982년 경북대학교 전자공학과 졸업(학사)
1984년 경북대학교 대학원 전자공학과 졸업(석사)
1997년 경북대학교 대학원 전자공학과 졸업(박사)
1987년~2000년1월31일 국방과학연구소 팀장
2000년2월1일~현재 국가보안기술연구소 팀장
관심분야 : 정보보호시스템, 센서네트워크
E-mail : jhyoon@etri.re.kr