암호화기술을 적용한 무선 도어락시스템 디자인에 대한 연구

A Study on the Wireless Door Lock System with Advanced Encryption Standard(AES) in Design

유보현(Yoo, Bohyeon)
경기대학교 디자인공예학부 교수

이 논문은 2002년도 경기대학교 교내연구과제 연구비에 의하여 연구되었음.

記述論文 Review Articles ● Received : Nov. 05. 2003 ; Accepted : Jan. 09. 2004

(要約)

개인생활의 프라이버시와 외부로부터 자신의 안전성(Safety)을 확보하고자하는 노력은 오늘날 기술의 진보와 더불어 보안시스템의 발전을 가져왔다. 특히 아파트형태의 주거생활이 보편화되면서 프라이버시의 확보와 외부침입으로부터 자신과 가족의 보호라는 측면에서 도어락 시스템(Door Lock System)의 역할과 기능의 중요성이 증대되고 있다. 이러한 추세에 발맞추어 기술의 발전뿐만 아니라 사용자중심의 다양한 방법의 인터페이스에 대한 연구가 이뤄지고 있으며 그 일환으로 지문이나 홍체인식과 같은 최첨단의 보안시스템이 등장하고 있다. 본 연구는 암호화기술(Advanced Encryption Standard)을 적용하여 보안과 안전성을 확보함과 동시에 사용자가 쉽게 작동하고 사용할 수 있는 인터페이스를 바탕으로 한 도어락 개발에 초점을 두고 있다. 특히 가격 면에서도 기존제품과 경쟁력을 가질 수 있고, 보다 근본적으로 도어락 뿐만 아니라 전반적인 잠금장치에 대한 새로운 가능성과 방법을 모색해 봄으로써 향후 잠금장치와 보안시스템에 대한 대안을 제시코자 한다.

(Abstract)

The human effort to make personal privacy and safety from outer environment has brought the improvement of security system through the technological development. Especially as a apartment dwelling and lifestyle is general,
the role and function of door lock system is more important than ever. The research for user-centered approach and design on the door lock system should be implemented under the circumstances. This study has focused on the development of making safety as well as easy interface to design door lock system. The price also is competitive as compared with other door lock products. The goal of this study is to propose the alternatives not only to develop door lock design but also to search the innovative way of locking system design.

(Keyword)

AES (Advanced Encryption Standard),
RF (Radio Frequency), Door Lock

1. 서 론

1.1. 연구의 배경과 목적

오늘날의 고도화 정보사회에서 재산이나 정보, 기타 시설물들에 대한 보안문제는 매우 중요하며 아파트형태의 주거생활이 보편화되면서 외부로부터 개인과 가족의 프라이버시와 안전성의 확보라는 측면에서 도어락시스템(Door Lock System)의 역할과 기능의 중요성이 점점 증대되고 있다. 우리사회도 맞벌이가정이 크게 늘고 여가생활의 증대 등의 사정으로 자주 집을 비우는 경우가 많아 보조키만으로는 안심하고 집을 비울 수 없을 뿐만 아니라 절도범들의 손쉬운 범행대상이 되기에 이르렀다. 비단 아파트뿐만 아니라 단독주택 및 빌라를 비롯해서 회사사무실까지 전문절도사건이 크게 증가하고 있는 것이 오늘의 현실이다.

경찰청의 보고에 따르면 한달 동안 서울지역 에서만 평균 100건 이상의 빈집털이가 발생하는 등 전국적으로 전문 절도범들이 기승을 부리고 있다고 한다. 이와 같은 도난사건을 예방하기 위해선 철저한 문단속과 이중 삼중의 잠금장치를 해두는 것이 최선의 방법일 것이다. 이러한 현실에 발맞추어 최근 전문털이범에 의한 절도사건을 확실하게 예방할 수 있는 디지털방식의 잠금장치가 개발되고 있으며 더 나아가 홍채인식이나 지문인식(그림 1)과 같은 생체인식의 최첨단의 보안시스템도 속속 선보이고 있다. 보안과 관련한 개인 인증 방식이 단순한 자물쇠에서 비밀번호, 카드로 발전하여 현재는 사용자의 신체의 일부를 이용하는 지문, 정맥, 홍채 등의 생체인식기술로 발전하고 있으나 아직까지 출입문의 경우 보조키 혹은 비밀번호를 이용한 디지털도어락(그림 2)이 주류를 이루고 있다. 인터페이스방법은 근접 카드식이나 키패드 터치 또는 카드 리더기를 이용한 방법이 대부분이다. 아파트나 단독주택 등 가정집의 경우 대부분 3만-10만원 정도 가격대의 보조키를 사용하고 있지만, 방송 등에서도 여러 번 검증되었듯이 단 1-2초 내에 열고 침입할 수 있을 정도로 안전에 취약하다. 사무실 등에서 주로 사용하는 근접 카드식 도어락의 경우에는 복제의 위험이 있고 분실 시 재발급 과정이 복잡하며 많은 비용이 든다. 최근에 신축되는 아파트에 대부분 적용하고 있는 비밀번호를 이용한 디지털 도어락의 경우, 설치하기가 어렵고 가격이 비쌀 뿐 아니라 파손의 위험이 있고, 노인이나 어린이의 경우 비밀번호를 기억하기 힘들고 비밀번호 외부유출의 위험이 있다. 이런 단점을 해결하기 위하여 지문이나 홍채 등을 이용한 생체인식 도어락이 개발되고 있지만 이는 가정이나 일반 사무실에 설치하기에는 고가의 장비이고, 기술의 정확성에 대한 검증이 미비할 뿐 아니라 쉽게 파손될 수 있는 위험을 안고 있다. (표 1)

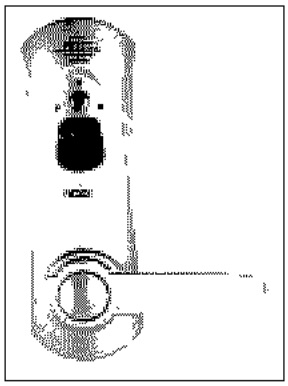

그림 1. 지문인식 도어락

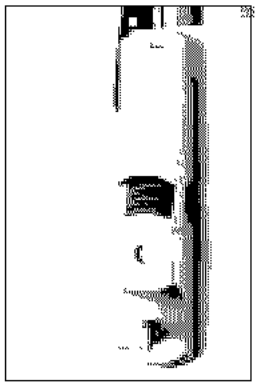

그림 2. 키패드형 디지털도어락

이제 우리사회도 가정이나 사무실의 보안 및 침입방지에 대한 인식이 크게 늘어 일반인들의 관심사항 중의 하나가 되었지만 아직까지 대중화되고 있지는 못한 실정이다. 이는 가격이 비싸고 설치하기가 어렵기 때문에 대부분의 가정에서는 아직까지 10만원대 미만의 보조키를 설치하는 정도이지만, 앞으로 점점 정보유출이나 안전의 위협을 느끼는 요소가 증가할수록 보안기능이 뛰어나고 사용이 편리한 도어락제품에 대한 수요는 폭발적으로 증가할 것으로 예상되며 특히 안전성이 담보된 무선 디지털도어락의 개발이 활발히 진행되고 있으나 개발실적은 아직 미미하다.

구 분	지문인식도어락	디지털도어락	보조키
보안성	우수 / 도구를 이용, 지문복제 가능	비밀번호가 유출될 수 있음	만능키로 손쉽게 열 수 있음
편의성	키를 소지하지 않아도 되어서 편리/인식시간이 다소 소요	키를 소지하지 않아도 되어서 편리/ 노인이나 어린이의 경우 암기에 어려움	무거운 키를 소지해야 하며 사용 시에도 매우 불편함
파손가능성	가능	가능	가능
호환성	고가 / 특수한 곳이 아니면 구입이 어려움	-	-
가 격	100-200백만원	10-35만원	5-10만원

표 1. 기능비교 및 분석

본 연구는 암호화기술 (Advanced Encryption Standard)을 적용하여 무선으로 조작되어 보안과 안전성을 확보함과 동시에 사용자가 쉽게 작동하고 사용할 수 있는 인터페이스에 기초한 도어락 개발에 그 초점을 두고 있다. 이를 위하여 사용자가 쉽게 휴대하

고 작동이 용이한 RF(Radio Frequency)방식의 토큰을 이용, 사용상의 편의성을 증대시켰으며, 특히 가격 면에서도 기존제품과 경쟁력을 가질 수 있고 근본적으로 도어락 뿐만 아니라 전반적인 잠금장치에 대한 새로운 가능성과 방법을 모색해 봄으로써 향후 보안시스템에 대한 대안을 제시코자 한다.

1.2. 연구내용 및 방법

본 논문의 내용은 암호화기술에 대한 적용가능성과 기존의 디지털도어락의 제품분석을 통해 기존제품의 단점을 극복하고 암호화를 통하여 안전성을 확보하여 향후 보안 및 통제시스템에서 요구되는 문제점들을 해결하고자 하는 것이다. 이를 위한 방법으로 제품분석을 통해 그 제품에 사용된 기능 및 기술들을 파악하여 본 제품에 구현할 수 있는지를 타진한다. 이를 통하여 구현하고자하는 제품의 기능을 우선 선정하고 그 기능을 구현하기 위한 기술들을 고려하여 제품기능에 대한 상세 설계를 하며 동시에 설계된 기능을 테스트할 수 있는 방법을 고려한다. 그리고 각종 기능을 위한 구체적인 프로토콜 및 프로그램을 구현하고 병행해서 하드웨어적인 보드 설계 및 기구 설계를 통한 시제품을 제작한다. 이러한 하드웨어와 구현된 각종 소프트웨어를 통합하고 테스트를 통하여 개발을 완료하는 프로세스로 진행하였다.

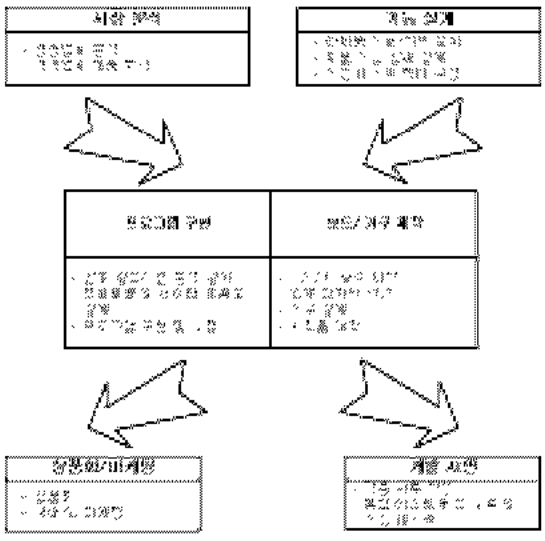

그림 3. 개발추진 절차

2. 기술현황 및 전망

2.1. 암호화기술

정보유통이 급증함에 따라 정보보호에 대한 인식의 확산은 암호화기술의 급속한 발전을 가져오고 있다. 과거에는 DES (Data Encryption Standard)라는 56비트 키를 사용하는 암호 알고리즘과 국내에서는 SEED라는 64비트 키를 사용하는 알고리즘을 많이 사용하였다. 그러나 컴퓨터 기술과 알고리즘 공격(Attack) 기술이 점차 발전하여 이러한 알고리즘의 취약점이 나타남에 따라 보다 강력한 암호 알고리즘이 요구되고 있는 실정이다. 암호화기술에 대한 전망은 공격 기술의 급속한 발달에 대처하기 위해, 2001년 11월에 제정된 표준문서 FIP-197은 128비트 키 크기를 갖는 AES (Advanced Encryption Standard) 암호화 알고리즘이며 취약한 DES의 대체 알고리즘으로 변경되리라 전망된다. 정보보호의 발전과 정보의 유통이 급증됨에 따라 새로이 제정된 알고리즘 표준은 과거 DES가 사용된 빈도보다 월등히 많이 사용되리라 전망된다.

2.2. 인증(Authentication)기술

암호화기술과 더불어 사용자의 정당성을 확인하는 사용자인증 매커니즘(authentication mechanism)과 같은 보호 매커니즘의 개발도 활발히 이루어지고 있다. 특히 사용자인증 매커니즘은 시스템에 대한 접근 제어를 목적으로 하는 기반기술로서, 패스워드(password)매커니즘 같은 것이 이에 해당된다. 이러한 사용자 고유번호와 패스워드 기반의 사용자인증 매커니즘을 수행하는 시스템에서는 고정된 패스워드를 사용하기 때문에 패스워드의 누출이 쉽고, 네트워크 상에서 해커(hacker) 또는 도청에 의하여 패스워드를 가로채는 경우에 방어할 방법이 없다. 실제로 국내외에서 발생한 대부분의 해킹사건은 IP주소 및 패스워드 도용을 통한 방법이었으며 사용자 패스워드는 스니퍼 프로그램(sniffer program) 등을 통하여 불법 도청함으로써 쉽게 알아낼 수 있다. 이러한 패스워드 누출을 방지하는 기술은 사용자 인증기술의 확보로 가능하며, 대표적인 사용자인증 기술은 패스워드, 비암호학적인 방법, 암호학적인 방법으로 분류할 수 있다.

패스워드를 이용한 사용자인증 기술은 대부분의 실제 인증 시스템에서 채택하고 있는 매커니즘이지만, 외부노출, 추측, 도청, 재연 등에 특히 취약하다. 비암호학적인 방법으로는 일회용 패스워드, challenge-response, 개인특성, 주소기반 등의 방식이 있으며, 넓은 의미에서 challenge-response도 일회용 패스워드의 범주에 포함시킬 수도 있다. 그러나

challenge-response방식이 수행하는 인증 프로토콜패스가 2패스로 일회용 패스워드의 1패스와 다르고, 기존의 실제 시스템에 구현 시 고려사항들도 많이 상이함으로 일반적으로 다른 방법으로 분류된다. 암호학적인 방법으로는 Kerberos 등의 대칭키(symmetric key) 방식과 X.509 등의 공개키(public key)방식 등이 있으나 실제 시스템 구현에서는 키관리 등에 많은 노력과 비용이 소요된다.

실제로 구현된 많은 사용자인증 시스템은 패스워드 방식 또는 비암호학적인 방법 중에서 일회용 패스워드, challenge-response 방식들이다. 이 방식들은 국내외적으로 많은 연구가 진행되어 왔으며, 현재 수백 종의 인증제품이 생산되어 다양한 응용분야에 적용되어 사용 중에 있다. 비암호학적인 방법 중에서, 클라이언트가 생성한 인증값을 서버에 전달하여 바로 인증을 수행하는 1패스 인증 프로토콜인 일회용 패스워드시스템은 기존의 사용자 고유번호와 패스워드 기반인증 프로토콜에 아무런 변경 없이 적용이 가능하다. 즉 프로토콜에는 변화 없이 클라이언트 프로그램에 인증값 생성함수와 서버 프로그램에 검증값 계산함수의 추가로 쉽게 구현된다. 그러나 challenge-response방식은 3패스로 인증 프로토콜을 수행하며, 클라이언트 프로그램에 challenge를 받아서 response를 계산하는 함수와 서버프로그램에 challenge 생성, 전송 및 response를 계산하는 함수가 구현되어야 한다.

2.3. 키 관리기술

키 관리기술은 암호화 또는 인증기술과 같이 매우 중요시되고 있으며 보안문제를 보다 철저히 하기 위해 안전한 키 생성과 키 교환방식에 집중되어 있으며, 기본적으로 보안 알고리즘을 위한 negotiation 프로세스를 가지고 있고, 수동적인 키 관리를 필수요소로 자동화된 키 관리가 필요하다. 이러한 키 관리기술로는 썬마이크로 시스템의 SKIP(Simple Management for IP)방식과 아이비엠(IBM)의 Photuris, 시스코의 ISAKMP 방식 등의 키 관리기술이 사용되고 있다.

현재 일반적인 통신환경에서 보편적으로 사용하는 키 관리방식으로는 암호화 키 방식과 복호화 키 방식으로 분류할 수 있다. 암호화 키는 송신하려는 모든 통신 참여자에게 공개하고, 복호화 키는 각자가 비밀리에 관리하는 방법인 공개키 암호화 방식이다. 이 공개키에 대한 인증을 공인기관에서 보장하기 위해 CA(Certificate Authority)를 지원하는데, CA가 갖고 있는 인증서는 공개키를 배포하는데 있어 안전한 방법을 제공하기 위해 사용되는 프로토콜로서 X.509를 사용하는 PKI 기반으로 변화하고 키 생성은 pseudo random number generation 기법보다는 true random number generation 기법을 하드웨어적인 보안칩(모듈) 내부에 두어 더욱 안전하게 하려는 방향으로 진행되고 있다. 또한 키 분배를 위한 알고리즘도 이산대수문제(discrete logarithm problem)의 어려움에 근거한 D-H 프로토콜은 키 사이즈 크기증가에 대한 문제점이 있어 elliptic curve discrete logarithm problem의 어려움에 근거한 타원곡선 기반 D-H 프로토콜로 진화되어 나아가고 있다.

2.4. 키 보호기술

키 보호기술은 암호 및 인증 등에 사용되는 키를 안전하게 보호하는 기술을 말한다. 특히 무선통신 장치에는 장치 내에 키를 저장하고 있기 때문에 키 정보에 대한 물리적인 불법 접근을 차단해야 한다. 이를 위해 무선 통신장치는 메모리 상에서 안전하게 각종 키를 유지, 관리할 수 있는 기능을 제공하여야 한다.

3. 기존제품분석

제품의 기능	내 용
복제 불가	플로팅 기술을 이용한 반도체칩 방식으로 키 복제가 불가능 키 타입: 주키
열쇠 추가/삭제	키를 추가 등록/삭제가 가능하여 분실한 키를 사용중지 시킬 수 있는 기능. 등록가능 키 수: 9개 프론트키 개폐방식: 원터치방식 비밀번호 입력
비밀번호기능	비밀번호 입력방식: LED 판 버튼방식 키와 함께 사용자가 설정해 놓은 비밀번호를 사용하여 문을 열 수 있는 기능 (입력수:4-8자리) 메인바디 개폐방식: 버튼타입 재질: 아연다이캐스팅, 알루미늄
강제잠금장치	내부강제잠금: 외부에서 키나 비밀번호를 입력해도 문을 열 수 없도록 하는 기능 외부강제잠금: 내부에서 문을 열 수 없도록 하는 기능. 장시간 외출시 사용. 우유투입구에 의한 침입 방지
파손경고음	80db의 경보음 발생
자동잠김	자동으로 문을 잠궈주는 기능 동작전원: DC 6V (AA Size 건전지 4개)
리모콘	무선으로 열고 닫을 수 있는 기능(선택사양) 전원 사용기간: 2년 (1일 10회 사용기준)
사용자 조회기능	키를 이용한 사용자들의 출입내역을 최대 16명까지 확인할 수 있는 기능(Trace Key사용) 동작온도: -20℃-70℃
하나로 키	키 하나로 Floating ID 시스템이 설치되어 있는 4곳 까지 사용가능

표 2. S사 G 제품의 기능 및 특징

제품의 기능	내 용
비밀번호 기능	열쇠를 휴대할 필요 없이 입력된 비밀번호로 문을 열며 비밀번호를 자유롭게 변경 (4자리에서 12자리까지 가능)
10키 버튼	견고한 재질(아크릴수지)로 외부파손 없이 사용할 수 있으며, 지문표시가 나지 않아 안전
키패드 조명	낮에 축적한 햇빛이나 불빛으로 야간에도 빛을 발생해 번호판 식별 용이
비밀번호통제	많은 사람들이 사용하는 사무실이나 장기외출 시 보안이 필요할 때 기존의 비밀번호를 통제하는 통제비밀번호(4자리에서 12자리) 추가설정으로 출입을 통제
방범방어기능 I (키 실린더)	장난이나 범죄목적으로 틀린 번호를 5회 이상 실수로 입력하면 자동으로 경고부저음이 울린 뒤 약 1분 동안 모든 동작이 정지되어 도난을 방지
방범방어기능 II	키 실린더에 본 키가 아닌 이물질 삽입 시 도어락 내부의 감지센서와 제어회로에 의해 키 실린더 회전체에 빗장이 쳐 져 문을 열 수가 없음
방범퇴지 경보	본 키가 아니면 110db의 경보음 발생
외부핸들 잠금	외부에서 #버튼을 누른 후 핸들을 돌리면 문이 잠김
원격 문열림(유선)	실내에 설치된 인터폰이나 비디오폰 등 홈 오토메이션과의 연결로 떨어진 위치에서도 연격 문열림 기능
무선 문열림	무선 리모콘은 유선시공이 어려운 장소에 적합하며 특수암호방식을 채택하여 신뢰성 보장
자동 되잠김	장난이나 실수로 원격문열림 기능을 사용하여 문을 열었을 때나 밖에서 비밀번호로 문을 열고 들어오지 않았을 경우 일정시간이(7초) 경과되면 자동으로 되잠김
견고한 키실린더	특수 실린더를 채택하여 극히 우수한 보안성과 신뢰성을 보장 (방범방어기능 내장)
실내 2중 잠금장치	실내측 몸체에 슬라이드식 이중잠금장치를 채택하여 안정성확보
건전지 교환	내장된 건전지가 소모되면 교환시기를 알려주는 경고음과 알림램프가 적색으로 점멸
롬 메모리기능	건전지 방전 시 입력 비밀번호는 지워지지 않음
방범시스템과의 호환(선택사양)	방범방어, 퇴자신호, 문의 개폐상태, 파괴감지 등의 원격제어 가능

표 3. N사 N 제품의 기능 및 특징

표 2와 3은 국내의 디지털 도어락시장에서 점유율이 높은 두 업체를 선정하여 그 주력상품에 대한 제품기능과 그 내용을 분석한 자료이다. 회사에 따라 제품의 기능과 방식에 약간의 차이는 있었지만 사용자 환경에서 요구되는 디지털도어락의 역할과 기능을 기술하였다. 사용자환경 중심의 다양한 인터페이스 방법이 개발되어 제품에 실용화되고 있으나 역시 가장 큰 관건은 안정성의 확보를 위한 기술개발이라 할 수 있다. 인터페이스방법에 있어서도 보조키를 소지하거나 비밀번호 방식의 경우 비밀번호를 암기하고 있어야 된다는 점은 기존 디지털도어락 제품이 가진 공통적인 인터페이스 방법이며 가격대는 사용자의 기대수준을 충족시킬 수 있는 제품의 경우 30만원대에 이르고 있다.

4. 기술 및 제품개발

4.1. 기술개발의 개요

사용자 인증을 하는 방법으로서 고유번호, 패스워드 등이 실제적으로는 많이 사용되지만 이러한 매커니즘은 패스워드 누출 또는 도청에 의하여 패스워드를 가로채는 경우에 방어할 방법이 없다. 인증시스템에서 안전하다고 알려져 있는 원타임 패스워드의 일종인 challenge-response 방식은 1패스가 아닌 2패스 또는 3패스로 이루어져 있다. 이러한 challenge-response 방식은 그 인증 방식뿐만 아니라 키의 생성 및 보관 기술이 매우 중요하기 때문에 그와 관련된 기술이 함께 개발되어야 한다.

인증시스템이 가장 활발히 이루어지는 곳은 컴퓨터 억세스제어, 인터넷 뱅킹, 출입시스템 등 여러 환경이 존재한다. 그러나 인증시스템은 그 적용환경에 적합하여야 함으로 인증시스템 단독으로 개발되기란 어렵다. 그래서 이러한 인증시스템을 적용하기 위하여 인증환경을 우선 출입시스템에 한정하여 그와 관련된 모든 기능 및 기술을 동시에 개발하고자 하는 것이다.

소유하기 쉽고 분실의 위험이 적은 토큰을 사용하여 버튼을 원터치화 함으로써 출입시스템의 각종 잠금장치를 개폐할 수 있도록 한다. 이와 같은 시스템을 구축하기 위하여 토큰, 통제장치, 통신 프로토콜, 암호 프로토콜 등을 개발한다. 또한 한 사용자가 여러 통제장치에 억세스 할 수 있는 권한을 위해서 여러 개의 토큰을 필요로 하지 않고 단 하나의 토큰으로 이를 해결할 수 있는 시스템의 개발을 목표로 한다.

4.2. 개발내용

4.2.1. 통제장치

통제장치는 사용자가 정당한 사용자인지 아닌지를 인증할 수 있는 장치를 말한다. 본 시스템에서는 사용자가 소유하고 있는 토큰을 이용하여 인증하는 시스템이다. 초기에 토큰의 ID를 통제장치에 등록하고 등록된 토큰만 인증될 수 있으며 인증절차는 난수를 이용한 challenge-response 방식을 이용한다. 통제장치 내에 개발되어 장착될 기능은 다음과 같다.

■ 토큰 ID 등록
■ 토큰 ID 삭제 (전체 혹은 일부)
■ 등록리스트 읽기
■ 트레이스기능
■ 키 생성기능
■ 토큰 인증기능
■ 자동 잠금기능
■ 건전지 교체시기 알림기능
■ 내부 완전 잠금기능

4.2.2. 토큰

토큰은 사용자가 열쇠처럼 항상 가지고 다니며 이것을 이용하여 ID를 통제장치에 등록할 때와 통제장치가 토큰을 인증할 때 사용된다. 토큰에는 사전에 메모리에 고유한 ID가 기록되어 있어서, 토큰을 등록장치에 등록할 때 사용된다. 토큰에는 버튼이 존재하여 사용자가 버튼을 누를 경우 송수신이 시작되며 토큰과 통제장치 간에 미리 정해진 순서대로 송수신한 후에 그것이 사전에 등록된 경우에만 통제장치가 토큰을 인증하여 사용자의 정당성을 입증한다. 사용자가 토큰을 분실하였을 경우에는 통제장치에서 분실된 토큰을 삭제함으로써 안전성을 확보할 수 있으며, 새로운 토큰을 구입하여 다시 등록함으로써 새로운 것을 사용할 수 있다.

■ 전자열쇠 기능
■ 멀티 키 기능 (여러 키를 동시 관리)
■ 키 보관기능
■ 암호기능

4.3. 기술연구 및 기능설계

4.3.1. 기능분석

현재 많이 사용하는 출입시스템의 기계적인 장치는 열쇠의 특수한 모양이 잠금 장치에 미리 기억(형상)되어 있어서 기억된 형태와 일치된 열쇠가 삽입될 경우에만 열림 혹은 잠김이 수행된다. 전자열쇠는 이와 달리 모양이 아닌 특수한 코드를 유무선으로 잠금장치에 전달하고 잠금장치는 이 코드를 분석하여 잠금을 해지 혹은 잠금을 수행할 것인지를 판단한다. 이러한 전자열쇠는 기계적인 열쇠에는 지원할 수 없는 다양한 기능을 제공할 수 있다.

-원터치 개폐기능
토큰을 원터치로 함으로써 송수신이 시작되어 출입시스템이 개폐된다.

-토큰 기능(Radio Frequency 사용)
분실염려가 적고 소유가 편리하여 노약자, 어린이 및 시각장애인의 사용이 편리하며 토큰이 주머니 혹은 핸드백 속에 있을 지라도 꺼내지 않고 버튼을 누름으로써 출입시스템의 열림 혹은 잠금기능을 수행함으로 편리하게 사용할 수 있다.

-멀티키 기능
열쇠가 모양 혹은 형태가 아닌 코드이기 때문에 토큰의 메모리를 이용하여 여러 출입시스템(집, 사무실, 자동차 등)의 키 코드를 한 리모콘에서 관리할 수 있어서 사용자가 단 하나의 토큰을 소지하면서 여러 곳 다수의 출입시스템을 개폐할 수 있다.

-고유번호기능
통제장치 및 토큰에 고유번호가 존재하여 등록 및 삭제를 용이하게 하고 멀티키 기능을 지원할 수 있도록 한다.

-토큰등록
전자열쇠 시스템에서는 새로운 토큰을 새로 구입한 후 통제장치에 등록함으로써 출입시스템을 잠금 혹은 열 수 있도록 한다.

-토큰삭제
기계적인 출입시스템은 열쇠가 분실되었을 때 잠금장치 및 열쇠를 새로 구입하여 새로 설치해야 안전하다. 그러나 경제적인 문제와 불편함으로 일반적으로는 잠금장치를 교체하지 않고 그대로 사용하는 경우가 대부분이다. 이런 경우 분실된 열쇠를 습득한 사람은 언제든지 잠금 장치를 풀 수 있다. 그러나 전자적인 잠금 장치시스템에서는 키에 해당되는 토큰을 잃어 버렸을 때는 통제장치에서 해당되는 토큰의 등록을 삭제함으로 잃어버린 토큰을 이용하여 잠금장치를 열지 못하게 할 수 있다.

-통제장치 등록기능
통제장치 ID를 토큰에 등록함으로써 다수개의 통제장치를 한 토큰으로 조정할 수 있게 한다.

-통제장치 삭제기능
토큰에 기록된 통제장치를 삭제할 수 있게 한다.

-등록리스트 읽기
등록된 토큰의 리스트를 읽을 수 있다.

위와 같은 기능 이외에 가족이 모두 귀가하였거나 필요 시 내부에서 잠금장치를 강제적으로 잠금으로써 외부에서는 정상적인 토큰일지라도 잠금장치를 풀지 못하게 하는 내부 완전 잠금기능이 있다. 통제장치에 내장되어 있는 건전지의 전압을 파악하여 적절한 주기가 되면 사용자가 인지할 수 있도록 알림 기능을 하고(음성, 소리, LED 등을 이용) 통보주기는 건전지의 소모량이 일정 양 이상이고 통제장치와 토큰의 인증이 이루어질 때마다 이다. 최근에 누가 출입하였는지를 기록하여 사용자가 알고자할 때 사용자에게 보고하는 기능과 건전지를 교체하여도 통제장치, 토큰의 등록 혹은 최근 인증기록 등이 지워지지 않아야 한다. 또한 멀티키 기능을 가지고 있기 때문에 아파트 같은 공동 출입구 경우 주 출입구에 한 대를 설치함으로써 출입구에 관계된 다수의 입주자가 혜택을 받을 수 있다.

4.3.2. 암호, 인증 및 키 관리 분석

무선통신은 통신로가 노출되어 있기 때문에 도청에 매우 취약하다. 이러한 점을 보완하기 위하여 암호기능을 사용하는데 암호기능을 사용하기 위해서는 토큰과 통제장치에 키가 있어야 한다. 본 제품에 사용할 알고리즘은 대칭키 알고리즘으로 토큰과 통제장치에는 서로 공유하는 키가 존재한다. 이를 위하여 키 생성 알고리즘이 필요하며 또한 이렇게 발생된 키를 관리하고 이러한 키를 이용하여 통제장치는 정당한 토큰을 인증 할 수 있다.

-암호기능

토큰이 보관하고 있는 코드를 통제장치에 직접 전송하지 않고 암호기능을 이용하여 매번 전송하는 코드를 다르게 할 수 있어서, 토큰 및 통제장치의 통신을 계속 감시 혹은 도청할 지라도 키로 사용되는 코드는 외부에 유출되지 않기 때문에 이러한 공격으로부터 안전하다.

-키생성 기능

차후의 인증을 위한 암호화에 사용될 키가 등록과 동시에 생성되기 때문에 시스템 설계자, 생산자, 판매자 모두 사용되는 키를 사전에 알아내거나 미리 복사할 수 없다.

-인증기능

정상적으로 등록된 토큰은 통제장치와 키를 공유하기 때문에 통제장치는 공유된 키를 이용하여 토큰이 사전에 잠금장치에 등록이 된 것임을 인증할 수 있다.

-키 보관 및 삭제

키는 통제장치에 생성되어 토큰의 플래쉬 메모리에 안전하게 저장된다. 토큰을 분실하였을 때는 정당한 사용자가 통제장치에서 해당되는 키의 등록을 삭제할 수 있으므로 분실에 대한 위험을 최소화한다.

5. 프로그램구현

5.1. 암호알고리즘 분석 및 설계

5.1.1. 암호알고리즘

DES 알고리즘의 안전성이 점차 문제 시 되자 대체하기 위한 알고리즘을 공모를 통하여 2001년 11월에 FIPS-197로 표준화가 된 AES(Advanced Encryption Standard)알고리즘을 본 개발제품에 사용한다. 이 알고리즘은 현재 PC상에서 32비트 프로세서를 사용하는 프로그램으로 많이 구현되고 있으며 이를 이용하기에는 비교적 값이 비싼 프로세서를 사용하여야 한다. 이러한 경우에 양산제품가격이 상승하여 시장확보에 문제가 생긴다. 그러므로 8751계열의 CPU를 사용하고 AES알고리즘을 이 프로세서에 구동될 수 있도록 다시 프로그램 하여야 한다. 그러기 위하여 AES알고리즘을 분석하여 프로그램을 구현하고 테스트벡터의 결과를 비교함으로써 정확한 프로그램을 구현할 수 있다.

5.1.2. 난수발생기

키 생성을 생산단계에서 하지 않고 등록단계에서 하기 때문에 키를 생성할 수 있는 모듈을 통제장치에 삽입하였다. 또한 서로 다른 통제장치, 리모콘에 대해서는 키가 같을 확률을 극소화하였으며, 이러한 난수발생기는 리모콘과 인증시점에 일회용 nonce로 사용되기도 한다. 그러므로 외부에서 통신로를 장기간 도청할 지라도 이후에 인증되는 코드를 알아내지 못한다. 난수생성 과정은 다음과 같다

Step 0: Seed 128비트(s127, s126, ..., s2, s1, s0)를 read

Step 1: LFSR 1의 LSB(Right Signification Bit) w0를 "1"로 세팅

Step 2: LFSR 1의 32비트 w34, w33, ...,w3을 s31, s30, ..., s1, s0로 세팅

Step 3: LFSR 2의 LSB(Right Signification Bit) x0를 "1"로 세팅

Step 4: LFSR 2의 32비트 x32, w31, ...,x1을 s63, s62, ..., s33, s32로 세팅

Step 5: LFSR 3의 LSB(Right Signification Bit) y0를 "1"로 세팅

Step 6: LFSR 3의 24비트 y30, w29, ...,y7을 s87, s86, ..., s65, s64로 세팅

Step 7: LFSR 4의 LSB(Right Signification Bit) z0를 "1"로 세팅

Step 8: LFSR 4의 24비트 z28, z27, ...,z5을 s31, s111, ..., s5, s88로 세팅

Step 9: LFSR 1, 2, 3, 4를 각각 64회씩 수행한다.

Step10: LFSR 1에서 w34 - w27 8비트를 추출한다.

LFSR 2에서 x32 - x25 8비트를 추출한다.

LFSR 3에서 y30 - y23 8비트를 추출한다.

LFSR 4에서 z28 - z21 8비트를 추출한다.

Step11: Step 9, Step 10을 순차적으로 15번 더 수행하여 레지스터 E를 모두 세팅한다.

레지스터 E의 128비트 난수가 생성된다.

-SEED 128비트 갱신과정

Step 0: Seed 128비트(s127, s126, ..., s2, s1, s0)를 read한다

Step 1: 난수생성과정에서 발생된 128비트 레지스터 E의 128비트와 s127, s126, ..., s0을 각각 XOR를 취하여 E 레지스터를 갱신한다.

Step 2: Step 1에서 생성된 E를 right shift 8회 수행 후 본래 Seed값에 overwrite한다.

5.2. 프로토콜 설계 및 프로그램구현

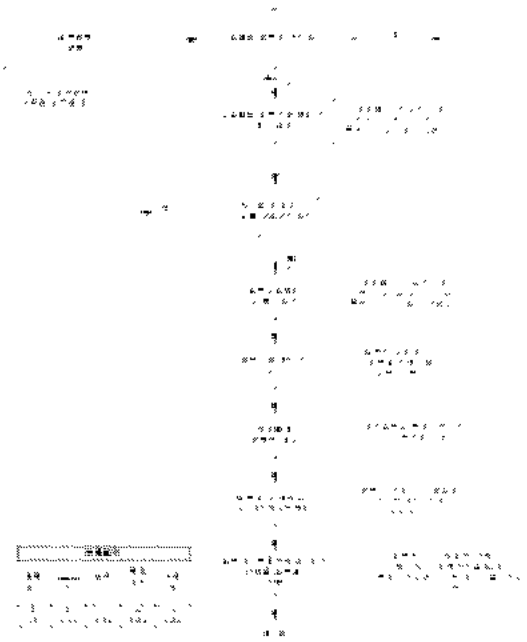

그림 4. 통제장치 측면에서의 토큰 ID등록

정확하고 안전한 인증을 위해서는 단지 인증프로토콜만 안전해서는 불가능하다. 안전한 인증을 위해서는 키가 필요하며, 그에 대한 관리까지 안전하여야만 인증을 할 수 있다. 그러므로 인증과 관련된 여러 기능(토큰등록, 인증, 토큰 등록삭제, 토큰ID 리스트보기)이 안전하게 설계 구현되어야한다.

-토큰 등록절차

통제장치에 등록된 현황을 사용자가 수시로 확인한다는 것은 매우 불편함으로 최초 토큰등록은 인증없이 등록이 가능하지만 최초 이후에는 등록된 사람이 허락할 때만 등록이 가능하도록 하여 등록에 대한 보안조처를 취한다. 토큰으로부터 ID를 수신한 후에 난수발생기를 이용하여 인증키를 생성하여 생성된 인증키를 토큰과 통제장치가 공유하여 이후 해당 토큰을 인증할 때 사용한다. 이렇게 하여 토큰 및 사용자가 본 인증장치를 구매하기 전에 키의 노출을 방지할 수 있다.

그림 5. 인증 절차

통제장치에서 토큰의 인증은 challenge response방식을 사용한다. 토큰으로부터 통신이 있을 경우 통제장치는 난수를 발생하여 그 난수 값을 토큰에 전송한다. 토큰은 전송된 통신문을 자신이 가지고 있는 공유키를 이용하여 암호화시킨 다음 암호문을 통제장치에 재 전송한다. 이때 통제장치는 자신이 생성한 암호문과 토큰 측에서 제시한 암호문이 일치하는가를 판단하여 토큰이 정당한 토큰인가 아닌가를 판단한다.

6. 결 론

RF모듈이 장착된 보드를 1, 2, 3차에 걸쳐서 충분한 테스트와 성능분석을 통하여 안전하게 설계 제작하며, 실제적인 인증시스템이 되기 위하여 출입 통제장치, 토큰 등을 실제 working mock-up으로 구현한다. 이러한 환경 위에서 개발된 프로그램을 토큰 및 토큰 및 통제장치에 다운로드하여 실제적으로 편리하고 안전한 인증시스템을 구축했다.

암호알고리즘을 이용한 무선도어락시스템은 토큰을 사용할 때마다 새로운 사용자인증수열(10의 38승)이 발생하여 안전성을 확보할 수 있다. 10의 38승 이라는 수는 우주의 수많은 행성의 수 보다도 많은 경우의 수로 그 중에서 암호나 비밀 번호가 일치 할 수 있는 경우는 불가능하다 해도 과언이 아니다. 향후 도어락을 포함한 대부분의 사용자인증이 필요한 대다수 어플리케이션은 이러한 암호화기술을 바탕으로 구축되리라 예측된다. 향후에는 PC억세스제어, 금고, 중요서류가 보관되어있는 캐비넷 또는 서랍, 자동차 등에 단 하나만의 토큰으로 사용자인증을 받음으로써 여러 장소에 필요한 종류의 여러 키를 토큰 하나로 작동함으로써 여러 키를 소지하는 불편함을 해소할 수 있으며 보편화되리라 기대한다.

6.1. 디자인개요

본 무선도어락디자인은 출입문에 부착되는 손잡이와 잠금장치(자물쇠) 및 그 제어장치(통제장치), 그리고 열쇠역할을 하는 휴대장치(RF용 토큰)로 구성된다. 출입문 외부 본체(그림 10, 그림 11)와 출입문 내부에 설치되는 통제장치(그림 8, 그림 9)는 인테리어의 요소 중의 하나로서 인식되어, 전체적으로 사용자의 편의성, 인체 공학적인 설계 및 외형적인 아름다움이 조화를 이룬 디자인이 되어야 한다.

6.2. 디자인특징(Characteristics)

본 도어락디자인은 이러한 암호화기술과 기존제품 및 사용자 인터페이스의 분석을 바탕으로 진행되었으며 본 제품에 장착된 기능은 그 결과로 본문 4에서 기술된 내용을 수용하였다. 통제장치라는 도어락이 가지는 무겁고 육중한(heavy duty) 이미지를 탈피하기 위하여 부드러운 곡선을 전체적 형태의 모티브로 취하였으며 문의 내부와 외부 형태의 통일감을 주었다. 이러한 형태의 연속성(sequence)은 토큰의 형태와 디자인에도 적용되었다.

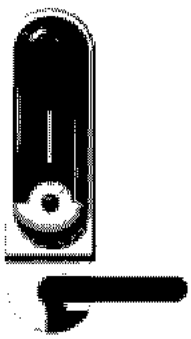

그림 6. 문 내부 정면이미지

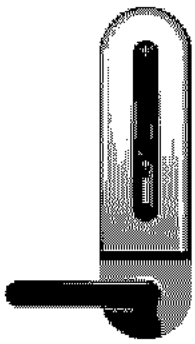

그림 7. 문 외부 정면이미지

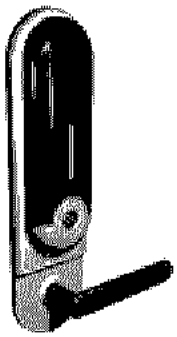

그림 8. 캡이 닫혀 있을 때

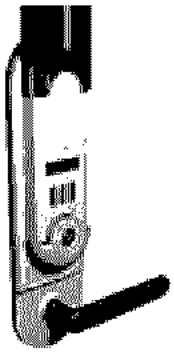

그림 9. 캡이 열려있을 때

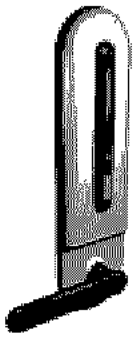

그림 10. 캡이 닫혀 있을 때

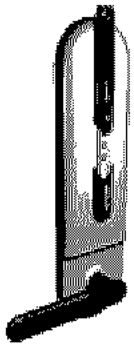

그림 11. 캡이 열려있을 때

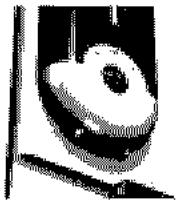

그림12. 강제 잠금장치

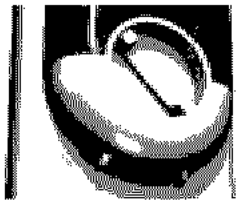

그림13. 캡을 열었을 때

재질은 외부로부터의 충격이나 파손으로부터 견딜 수 있게 외부와 내부 본체는 알루미늄 다이케스팅으로 제작되었으며 문 내부 본체의 재질은 부분적으로

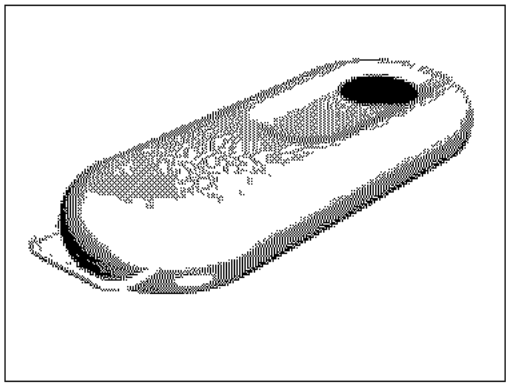

그림 14. 토큰(콘드롤러)

플라스틱을 사용하였다. 장착 후 초기 및 사용 중 프로그래밍은 캡을 올린 후 (그림 9) 내부에 장착된 3개의 버튼을 이용하며 그 내용은 LED 판에 디스플레이 된다. 초기 세팅 후 대부분의 작동과 내, 외부 본체의 제어는 대부분 토큰에 의해 이루어짐으로써 인터페이스의 과정과 내용을 최소화하였다. 다만 본체에 대한 강제적 제어가 필요할 경우 (예를 들어 그림 11. 은 장기간의 외출 등으로 건전지가 완전히 소모되어 외부에서 문을 열지 못할 경우 외부 캡을 올린 후 건전지를 접속하여 토큰을 동작시켜 문을 해 정하는 경우를 보여주고 있다.) 본체에 부착된 장치 등을 통해 이를 통제 할 수 있다. (그림 12, 그림 13)

휴대장치인 토큰은 사용자가 휴대하는 장비이기 때문에 휴대(예를 들어 목걸이와 같이 목에 걸 수 있거나 키 홀더와 같이 주머니에 넣을 수 있는)와 작동(원터치 방식)의 편리성을 고려하였으며 인체에 접촉해야 하기 때문에 인체에 무해한 플라스틱재질을 사용하였다. 이러한 원터치방식의 토큰을 이용하여 사용자는 키를 이용하여 번거롭게 본체를 조작(열쇠나 마그네틱 카드 혹은 다이얼패드 등의 조작)하지 않고 쉽게 문을 개폐할 수 있다.

6.3. 향후과제

이상으로 암호화기술을 무선도어락시스템이라는 잠금 장치에 적용함으로써 그 혁신기술의 활성화를 위한 구체적인 대안을 제시해 보았다. 그러나 본 연구는 암호화기술에 기반한 제품개발의 한 사례연구이며, 암호화기술은 향후 보안이 요구되어지는 여러 분야에 응용되어 그 활용범위가 확대되리라 예상된다.

국내의 경우 사무실의 보안 및 침입방지에 대한 인식이 최근 들어 일반인들에게까지 관심사항이 되고있지만 아직까지 대중화되고 있지는 않다. 그러나 정보유출이나 안전의 위협요소가 증가할수록 안전을 담보할 수 있는 시스템과 제품의 개발에 대한 욕구와 수요는 폭발적으로 증가할 것이다. 이러한 상황에 발맞추어 본 연구와 같은 기반기술을 이용한 연구가 여러 분야에서 활발히 이루어져 기술의 발전과 제품개발이 활성화되기를 기대한다.

참고문헌

- 원격해정식 도어락장치: 강만종, 실용신안공보, 등록번호 실 1996-0005229, (1996)
- 문개폐기의 무선결합장치: 강만종, 실용신안공보, 등록번호 실 1995-0005614, (1995)
- 전자식도어락의 전원공급장치 및 방법: 이성권, 공개특허공보, 공개번호 10-2001-0027072, (1996)
- 무선방범 관제시스템: 이성권, 공개특허공보, 공개번호 특2001-0028404, (2001)
- 디지털도어락 개폐장치: 이성권, 공개특허공보, 공개번호 특2001-0050059, (2001)
- 레버핸들식 도어락: 강만종, 등록실용신안공보, 등록번호 20-0152658, (1999)
- 원격해정식 도어락장치: 강만종, 공개실용신안공보, 공개번호 실 1999-006204, (1999)
- 디지털보조 도어락: 이성권, 공개특허공보, 공개번호 특10-2001-0019650, (2001)

참고사이트

- http://www.newell.co.kr
- http://www.kidp.or.kr
- http://www.gateman2000.com
- http://www.secugene.com
- http://www.dongdaemuncs.co.kr
- http://www.joins.com
- http://www.handpia.com