# 표준 암호화 알고리즘을 이용한 RFID 판독 시스템의 구현

# (Implementation of RFID Reader System using the Data Encryption Standard Algorithm)

박 성 욱*
(Sung-Wook Park)

***요 약*** 표준 암호화 알고리즘(DES : Data Encryption Standard)은 20년 이상 국제 암호화 표준으로 사용되고 있다. DES는 64비트의 데이터 블록을 56비트의 키를 이용하여 암호화시키는 블록 암호화 기법중의 하나이다. 이 알고리즘은 64비트의 입력을 연속된 과정에 의해 64 비트의 출력으로 전환하는 방법이며, 이렇게 암호화시킨 문장은 키 없이는 해독이 불가능하다. 본 논문에서는 DES 알고리즘을 이용하여 RFID(Radio Frequency Identification) 판독 시스템을 구현하였다. 구현된 시스템은 CBC(Cipher Block Chining) 모드를 사용하여 암호화 알고리즘의 신뢰성을 높였으며, 기존 상용 제품과의 성능 비교 결과 카드 접근 시간과 동작 시간이 상용 제품보다 우수함을 알 수 있었다.

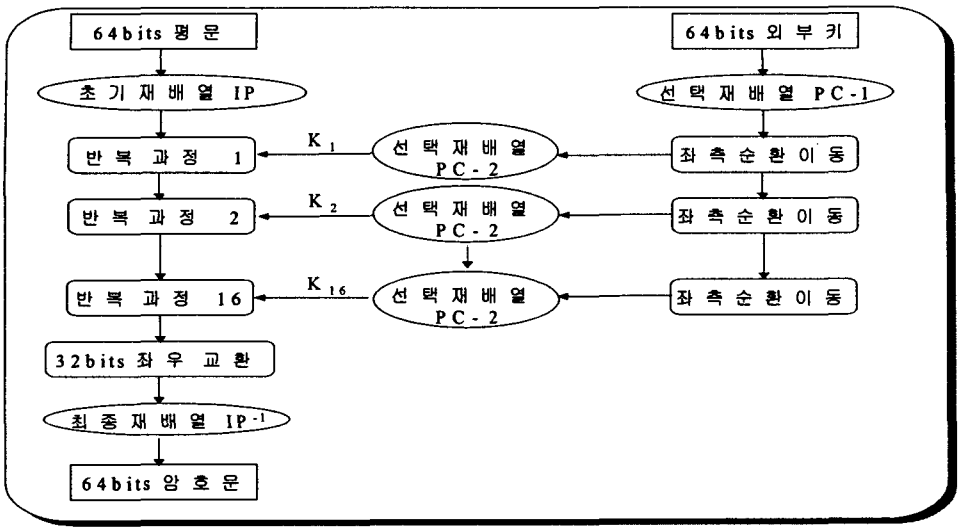
***Abstract*** The Data Encryption Standard(DES) has been a worldwide standard for over 20 years. DES is one of the block encryption techniques which ciphers 64-bit input data blocks using a 56-bit private key. The DES algorithm transforms 64-bit input in a series of steps into a 64-bit output. Thus, it is impossible to deduce the plaintext from the ciphertext which encrypted by this algorithm without the key. This paper presents an implementation of RFID reader system using the DES algorithm. An implemented system enhances the credibility of the encryption algorithm by using the Cipher Block Chining(CBC). Experimental results also show that the implemented system has better performance over the conventional commercial product.

## 1. 서 론

정보화 사회의 도래로 정보의 교환과 공유에서 획기적인 기술이 발전하고 우리의 생활에 절대적인 영향을 미치고 있다. 이에 따라 이들 정보의 안전한 보관과 교환시의 정보 보호문제는 정보화사회의 발전과 더불어 심각하게 고려되어야 할 부분이다. 이러한 정보 보호 및 보안을 위한 암호화 알고리즘 중 DES(Data Encryption Standard)는 NBS(Nation Bureau of Standards)가 암호 알고리즘을 공모하여 IBM이 응모한 방식을 근간으로 미국의 NSA(National Security Agency)가 안정성을 평가, 수정을 가하여 채택한 알고리즘이다. DES는 ANSI(American National Standard Institute)와 ISO(International Organization for Standard)에서 1977년 표준안으로 승인하여 국가 및 국제 표준 알고리즘으로 채택되어 현재까지 사실상 세계 표준암호로써 주로 금융망과 상업용 네트워크를 중심으로 널리 사용하고 있다.

한편, RFID(Radio Frequency Identification)는 바코드, 마그네틱, IC-CARD등과 같은 자동인식의 한 분야로서 초단파(MHz, GHz)나 장파(KHz)를 이용하여 기록된 정보를 무선으로 인식하는 방법이다. RFID는

* (주)로직메카 멀티미디어통신연구소

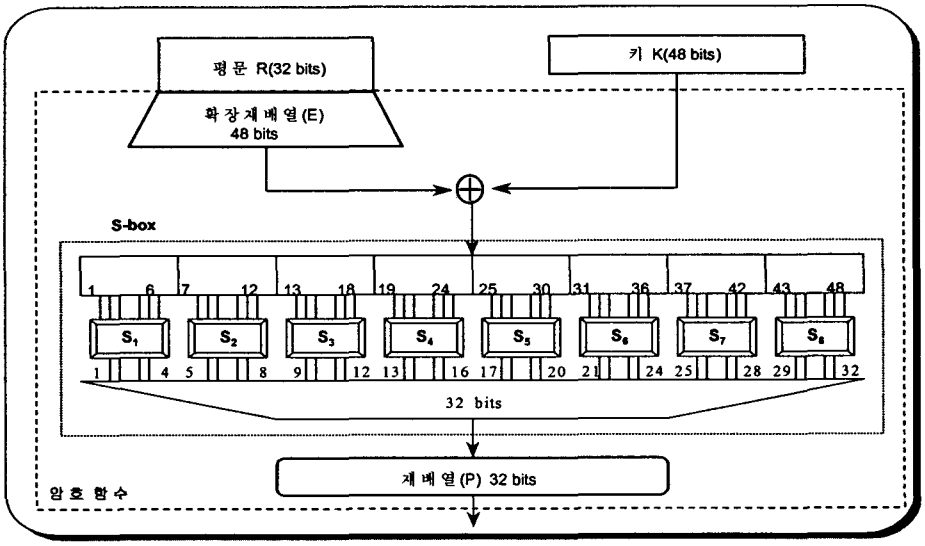



<그림 1> DES의 전체적 구성

주위 환경에 민감하지 않고, 인식 속도가 빨라 이동 중에도 인식이 가능하며 투과력이 우수하다는 장점이 있다. 또한 제조 과정에서 제조 코드(Manufacturing Code)가 부여되므로 위조 자체가 불가능하다.

본 논문에서는 현재 널리 사용되고 있는 비대칭 암호화 키 방식인 DES 알고리즘을 이용하여 RFID 판독 시스템을 구현하였다. 구현된 RFID 판독 시스템은 MDB(Microsoft Data Base)를 이용하여 효율적인 데이터 베이스 관리가 가능하도록 설계되었고, 현재 널리 사용되고 있는 DES 알고리즘을 stand-alone 보드에 이식시켜 구현하였다. 프로그램은 마이크로소프트사에서 제공하는 MFC(Microsoft Fundmental Class)를 사용하였으며, 판독 시스템과 PC는 RS-232방식을 사용하여 통신한다. 판독 시스템의 구성은 PC와의 상호통신을 위한 제어부와 판독 제어부 그리고 안테나부로 각각 구성되어져 있다.

본 논문은 다음과 같이 구성된다. 2장에서 DES 알고리즘에 대한 이론과 원리에 대하여 기술하고, 3장에서 CBC 모드에서의 DES 알고리즘에 관하여 간략히 설명한다. 4장에서는 실제 구현된 판독 시스템의 구성에 대




<그림 2> DES의 암호함수

하여 설명하며, 5장에서는 구현된 시스템에 대한 실험과 성능에 대하여 평가하고 마지막 6장에서 결론을 맺는다.

## 2. DES 알고리즘

DES는 재배열(Permutation)과 치환(Substitution), 키 스케줄로 구성되어 있고, 암호화 과정은 64비트 평문 블록을 32비트로 분할하고 확장재배열을 거친 후 56비트의 키를 사용하여 암호화한다. 내부적으로 16라운드의 암호화 과정을 거치고, 복호화 시에도 동일한 키의 역순을 사용하여 16라운드의 복호화 과정을 수행한다[1,2]. 그림 1은 DES의 전체적 구성을 나타내며, 3단계로 설명된다.

최초 평문 64비트는 초기재배열을 거친 다음 32비트씩의 L과 R의 두 개의 서브블록으로 나뉜다. 이후 S-box를 이용한 치환과 전치가 포함된 암호함수의 16회 반복을 거쳐 마지막으로 최종재배열을 한다. 이때 i번째 라운드의 결과를 $X_i=(L_i, R_i)$이라면, $L_i$와 $R_i$는 다음 식과 같이 나타낼 수 있다.

$$L_i = R_{i-1} \tag{1}$$

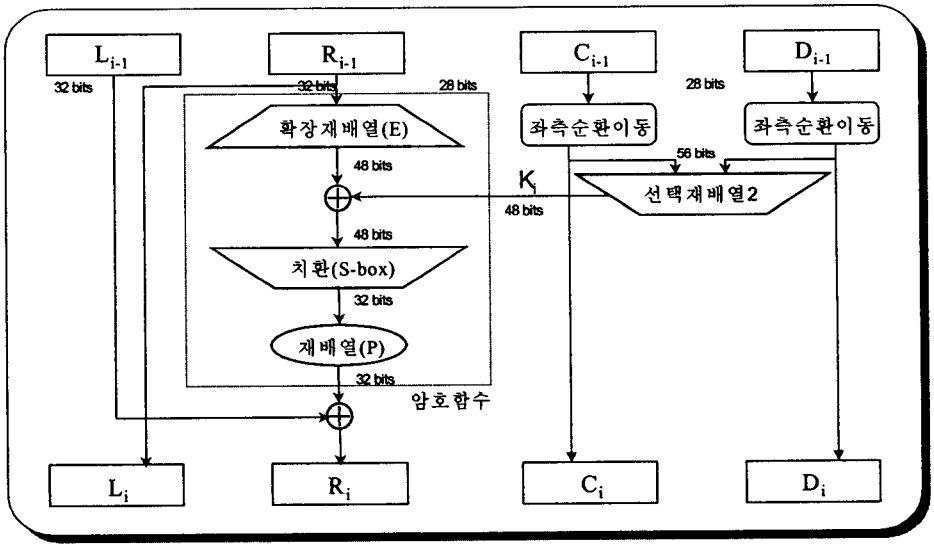
$$R_i = L_{i-1} \otimes f(R_{i-1}, K_i) \tag{2}$$

키 스케줄은 64비트의 외부키 중 8개의 패리티 비트를 제외한 56비트를 선택재배열(PC-2)하고, 28비트씩 두 개로 나누어 키 스케줄에 의해 각각 1혹은 2비트씩 좌로 쉬프트 한다. 이후 56비트 키는 두 번째 선택재배열(PC-2)을 통하여 48비트를 선택하여 각 라운드의 서브키로 사용된다.

치환과 재배열과정으로 구성된 암호함수 내부의 S-box는 암호화 강도를 높이는 기능으로 설계되어 있다. DES에서는 8개의 S-box로 구성하였다. 각 S-box는 6비트의 입력과 4비트의 출력을 갖는다. 그림 2는 DES의 S-box를 중심으로 한 암호함수 구조를 나타낸다[2].

DES의 S-box는 설계 방법이 공개되지 않아 설계자만이 암호를 풀 수 있는 특별한 trap-door가 있는 것이 아닌가 하는 의구심을 제기하고 있다. 이 S-box의 구성은 암호화의 비도를 좌우하는 매우 중요한 요소로서 암호학적으로 DES형 암호알고리즘을 설계하기 위해서는 반드시 심도 있게 연구해야 할 중요한 과제이다. 그림 3은 DES알고리즘의 단일 반복과정으로 그림 2에서 예시한 암호함수와 키 스케줄을 중심으로 나타낼 수 있다[3].

평문 64비트 중 오른쪽 32비트($R_{i-1}$)가 확장재배열을 통하여 48비트로 변환되고 56비트의 키가 28비트씩 분리된 후 좌측 순환 이동한다. 좌측 순환 이동 후 다시 56비트로 환원된 후 선택 재배열한 $K_i$ 48비트가 확장 재배열된 평문 48비트와 XOR연산 후 치환과 재배열과정을 거치고 다시 평문($L_{i-1}$) 32비트와




<그림 3> DES의 단일 반복 과정

XOR연산 후 암호문이 생성되며 DES는 이러한 과정이 16회 반복된다[4,5]. 이때 16번째 마지막 단계의 출력은 예비 출력을 생성하기 위해 좌우 블록을 교환하여 배치한다.

## 3. CBC 모드의 DES 알고리즘

DES와 같은 대부분의 블록 암호화 기법들은 64 비트 블록으로 데이터를 암호화하고 복호화 한다. 대부분의 암호화 작업들이 이보다 많은 데이터를 수반하므로 결과적으로 모든 블록들을 처리하기 위해 암호 작업을 반복해서 여러 번 수행해야 한다. 블록 암호화를 반복해서 수행하는 방식을 BCM(Block Cipher Mode)라고 한다. 본 논문에서는 BCM 중 가장 보편적이면서 가장 안전하다고 평가된 CBC(Cipher Block Chining) 방식을 채택하였다[1,6].

CBC는 간단한 연산들과 피드백으로 블록을 증가시켜서 상대방이 자료의 암호화 부분을 분석하지 못하도록 한다. 피드백은 각 암호문 블록이 이전 수행에 의존하도록 만들어졌다. CBC에서 이전의 암호문 블록은 같은 평문 블록이라도 나타날 때마다 다른 암호문 블록으로 암호화 되도록 피드백의 역할을 할 수 있다. 이전 암호문 블록이 피드백의 역할을 하기 위해서는 평문 블록을 암호화하기 전에 그 블록을 앞에서 생성된 암호문 블록과 XOR 연산을 수행한다. 그리고 암호문을 해독할 때는 각 암호화된 블록을 다음의 암호문 블록과 다시 XOR 연산을 수행한다. 다음은 CBC 모드의 블록 암호화 연산 식을 나타낸다.

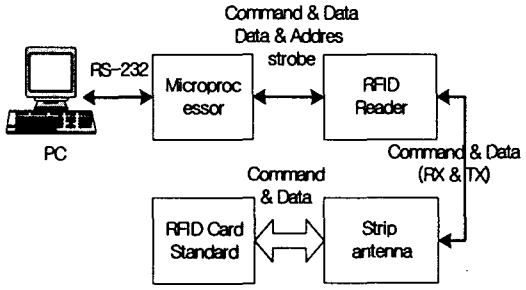
$$C_i = E_k(P_i \otimes C_{i-1}) \quad (3)$$

$$P_i = C_{i-1} \otimes D_k(C_i) \quad (4)$$

위에서 $C_i$와 $P_i$는 암호문과 평문 버퍼 C와 P의 i 번째 블록이고, $E_k$와 $D_k$는 키 K를 사용하는 암호화와 해독 연산이다. 일반적으로 평문의 앞에 임의의 데이터 블록을 추가한다. 이것은 평문의 첫 블록에 무엇이 들어 있는지를 상대방이 짐작할 수 있더라도 그 블록이 암호를 푸는 데 사용될 수 없기 때문이다. 이 블록을 초기화 벡터라고 한다. 이 블록을 피드백 없이 암호화하고 실제 첫 평문 블록을 암호화하거나 복호화 할 때 피드백으로 사용한다.

## 4. RFID 판독 시스템의 구현

본 논문에서 구현된 판독 시스템은 필립스사의 MFRC 500 디바이스를 기본으로 구성되었으며 그림 4와 같이 크게 4가지 부분으로 나누어진다.




<그림 4> 시스템 블록도

### 4.1 PC 제어부

PC 제어부는 마이크로 프로세서와 시리얼 통신하여 명령과 데이터를 주고받는다. 시리얼 통신 속도는 9,600bps부터 55,600bps까지 선택하여 통신할 수 있도록 설계하였다. 시리얼 통신에서 오류 검사 및 복원은 CRC 8 표준을 따랐다. 모든 데이터 및 명령은 1바이트로 구성되어져 있으며 키 값 및 데이터 값은 최대 16바이트까지 확장할 수 있도록 설계하였다. PC 명령의 표준은 MIFARE Classic Command Set을 기반으로 하여 프로그램 하였다.

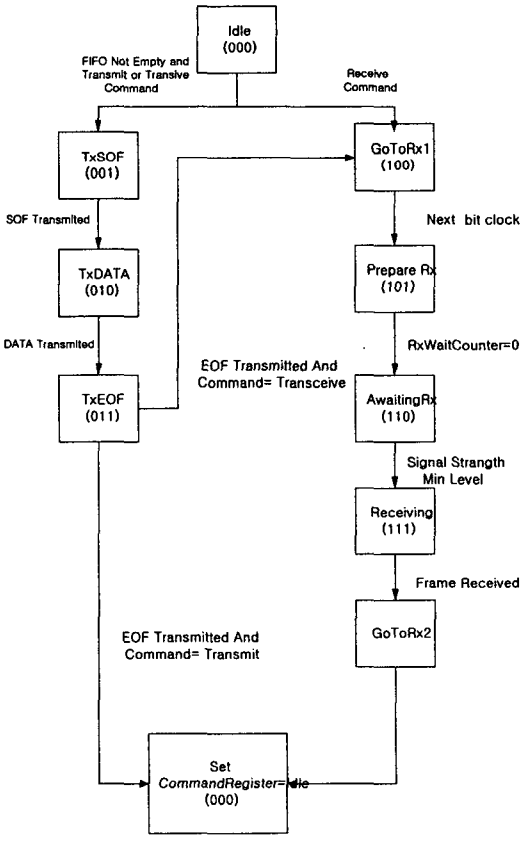
### 4.2 마이크로 프로세서부

마이크로 프로세서부는 PC 블록과 RFID 판독 장치간의 명령 제어 또는 데이터를 전송하는 블록이다. 마이크로 프로세서는 Atmel사의 ATmega 103을 사용하였다. ATmega 103은 RISC 구조의 프로세서로써 명령어 처리가 1 사이클로 처리되므로, 본 논문과 비교되는 P사의 판독 시스템이 사용하는 CISC 구조의 프로세서 보다 빠른 명령어 처리를 할 수 있었다. 본 시스템에서 적용한 메인 클럭은 4MHz이며 최고 20MHz까지 적용이 가능하도록 설계되었다. 마이크로 프로세서와 판독 장치간의 데이터 및 명령의 처리는 외부 메모리의 접근 방식과 동일한 Separated Read/Write strobe 방식 중 Multiplexed Address Bus 방식을 채

택하여 빠른 데이터 이동이 용이하도록 설계하였다.

### 4.3 RFID 판독 장치

RFID 판독 장치는 실질적으로 마이크로 프로세서에서 보내어지는 명령 또는 데이터를 아날로그 부분인 안테나로 전송하는 부분이다. MFRC 500은 RFID 통신 방식인 ISO 14443A를 지원해주는 디바이스로서 크게 명령 또는 데이터를 처리하는 디지털 부분과 데이터를 전송하는 아날로그 부분으로 나눌 수 있다. 송수신 단계는 모뎀 상태에 따라 진행되며 내부 레지스터의 변화 값에 따라서 에러 플래그를 검사하여 자체 오류를 감지할 수 있도록 설계되었으며, 송수신 방식을 ASK 방식을 사용하고 있다. 그림 5는 IC 카드와 통신하기 위한 MFRC 500의 상태 다이어그램을 나타낸다.



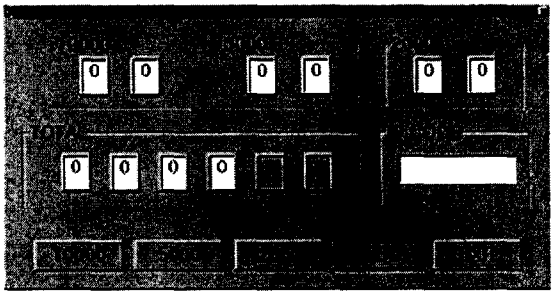

<그림 5> 카드와의 통신을 위한 상태 다이어그램

### 4.4 안테나부의 구성

안테나 부의 안테나는 임피던스 정합이 50Ω으로 고정되어 있다. 본 논문에서 사용한 안테나는 스트립 안테나로써 근거리 통신에 적합하도록 설계되어 있으며 50Ω의 정합 회로를 가지고 있다. 사용된 정합 회로는 Philips 사의 MFRD 700의 개발 도구의 안테나를 사용하였으며, 정합 회로는 Philips의 MFRC 500을 이용한 응용 회로를 참조하였다.

## 4. 시험 및 성능 평가

본 논문에서는 구현된 RFID 판독 시스템의 성능을 평가하기 위해 A사의 MFRD 700 RFID 판독 시스템과의 RFID Access Speed를 비교하였다. 본 실험은 Philips사에서 제공하는 RFID 판독 시스템의 동작 시간을 Windows에서 제공하는 타이머 함수를 사용하여 1/100초의 오차를 가지고 총 동작 시간을 비교하였으며, PC에서 IC Card 사이에 걸리는 시간과 CBC 모드와 일반 DES 모드와의 동작 시간을 각각 비교하였다. PC와의 통신 방식 중 RS232의 속도는 9,600bps, 14,400bps, 33,600bps로 실험하였다. 본 실험의 결과는 판독기 시간을 기준으로 하였으며, 읽어야 할 데이터는 0 블록의 00번지 데이터를 기준으로 하였다.

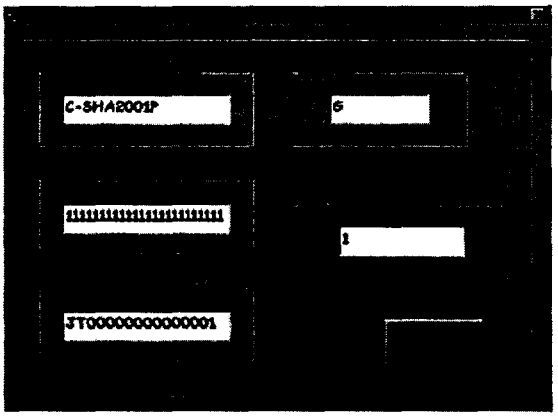


<그림 6> CBC 모드를 이용한 판독 프로그램

그림 6은 실제 CBC 모드를 이용하여 응용 프로그램을 구성한 그림이다. 각각의 다이얼로그들은 RFID Card에서 받은 데이터를 변환하여 각각의 화면에 표현하였으며 ID Code는 Card 제조시 부여되는 생산번호를 표현하였다.

본 논문에서 구현한 RFID 시스템은 그림 7과 같이 Card 내부의 Block60, Block61, Block62를 사용하며

자동 갱신 기능을 사용하여 Card를 일일이 입력하지 않고 자동으로 데이터를 입력하도록 구성하였다.




<그림 7> CBC 모드를 이용한 입력 프로그램

그림 8은 실제 구현된 RFID 판독 시스템을 나타내었다. 안테나부는 Strip 안테나를 장착하였다. 구현된 시스템은 stand alone 상태와 PC 연결 상태를 자동으로 설정할 수 있도록 설계되었다.

<그림 8> 구현된 RFID 판독 시스템

표 1에 수정되지 않은 DES 모드에서 얻은 실험 결과값을 나타내었다. PC에서 전송된 명령이 마이크로프로세서를 통해서 IC Card로 데이터를 보내는데 걸리는 총 시간이며, 다음 상태의 초기화의 시간은 포함되어 있지 않다. 표에서 A는 현재 판매되고 있는 A사의 판독 시스템을 의미하며, B는 본 논문에서 구현된 시스템을 나타낸다. 결과에서와 같이 본 논문에서 구현된 시스템이 인식 속도가 약간 빠르다는 것을 알 수 있다.

<표 1> DES 모드의 동작 시간의 비교(단위 : 10msec)

| 속도 / 횟수 | 9600bps | | 14,400bps | | 33,600bps | |
|---|---|---|---|---|---|---|
| | A | B | A | B | A | B |
| 1 | 12.8 | 12.6 | 12.2 | 12.1 | 11.6 | 11.5 |
| 2 | 13.1 | 12.6 | 12.2 | 12.1 | 11.6 | 11.5 |
| 3 | 13.2 | 12.6 | 12.3 | 12.1 | 11.5 | 11.4 |
| 4 | 12.9 | 12.6 | 12.5 | 12.0 | 11.3 | 11.4 |
| 5 | 12.9 | 12.5 | 12.4 | 12.0 | 11.3 | 11.5 |
| 6 | 12.9 | 12.5 | 12.4 | 12.1 | 11.3 | 11.4 |
| 7 | 13.1 | 12.6 | 12.5 | 12.0 | 11.6 | 11.4 |
| 8 | 13.2 | 12.6 | 12.4 | 12.0 | 11.5 | 11.5 |
| 9 | 12.7 | 12.5 | 12.4 | 12.1 | 11.6 | 11.4 |
| 10 | 12.8 | 12.5 | 12.4 | 12.1 | 11.4 | 11.4 |

표 2는 CBC 모드에서 얻은 실험 결과값을 나타내었다. A사의 제품이 CBC 모드를 지원하지 않기 때문에, 본 논문에서 구현된 시스템의 측정 데이터만을 가지고 비교하였다. 결과에서와 같이 CBC 모드를 적용할 경우, 일반 DES 모드와 인식 속도에서 그다지 큰 차이를 나타내지 않음을 알 수 있다.

<표 2> CBC 모드의 동작 시간(단위 : 10msec)

| 속도 / 횟수 | 9600bps | 14,400bps | 33,600bps |
|---|---|---|---|
| 1 | 16.2 | 16.1 | 15.8 |
| 2 | 16.2 | 16.1 | 15.8 |
| 3 | 16.2 | 16.1 | 15.8 |
| 4 | 16.3 | 16.1 | 15.8 |
| 5 | 16.4 | 16.1 | 15.9 |
| 6 | 16.3 | 16.2 | 15.8 |
| 7 | 16.4 | 16.2 | 15.8 |
| 8 | 16.3 | 16.1 | 15.9 |
| 9 | 16.4 | 16.2 | 15.9 |
| 10 | 16.4 | 16.1 | 16.1 |

## 5. 결 론

실험 결과에서와 같이 본 논문에서 구현된 RFID 판독 시스템은 일반 상용 제품의 Card 엑세스 시간에 있어 보다 우수함을 알 수 있다. 또한 CBC 모드를 사용할 경우 일반 DES모드를 채택한 판독 시스템과의 Card 검출 시간은 큰 차이를 나타내 않았다. 따라서 약간의 시간적 손실을 감수하더라도 개인 보안성에 역점을 둔다면, 본 논문에서 구현된 시스템이 충분한 역할을 할 수 있음을 알 수 있다.

향후 연구 과제로는 쓰기 기능의 추가와 다양한 응용 프로그램을 구현하여, 본 시스템의 응용성을 확장시킴과 동시에 PC와의 고속통신을 위한 추가적인 연구가 수행되어야 한다.

## 참 고 문 헌


[1] Bruce Schneier, Applied Crypto-graphy, John Wiley & Sons Inc., 1994

[2] Man Yung Rhee, Cryptography and Secure Communications, McGraw-Hill, 1994

[3] William Stallings, Network and Internetwork Security, IEEE press, 1995

[4] L. Brown and J. Seberry, Key Scheduling in DES type Crypto-systems, Abstract of AUSCRYPT90, 1990

[5] E. F. Brickell, J. H. Moore and M. R. Purtill, Structure in the S-boxes of the DES, Proc. of CRYPTO86, 1986

[6] E. Biham and A. Shamir, Differential Cryptanalysis of The Full 16-round DES, Proc. of CRYPTO92, 1992



**박 성 욱** (Sung-Wook Park)

1999년 인천대학교 전자공학과 공학석사

2003년 인천대학교 전자공학과 공학박사

1999년 ~ 2000년 한국철도기술연구원 철도신호통신 연구팀 연구원

2001년 ~ 2002년 (주)경인기계 부설 기술연구소 연구원

2002년~ 현재 (주)로직메카 멀티미디어 통신연구소 선임연구원

관심분야 : 멀티미디어,영상 압축,마이크로 컨트롤러