논문 2007-44SD-1-2

수동형 RFID 태그에 적합한 암호 회로의 설계

(Design of Cryptic Circuit for Passive RFID Tag)

임 영 일*, 조 경 록**, 유 영 갑**

(Young-IL Lim, Kyoung-Rok Cho, and Younggap You)

요 약

본 논문은 소형·저전력 환경에 적합하게 개발된 HIGHT 블록 암호 알고리즘의 소형·저전력화된 하드웨어 구조를 제안하고 성능을 분석한다. HIGHT 알고리즘은 일반화된 Feistel 구조의 변형된 형태를 취하고 있다. 설계된 HIGHT는 암·복호화 기능을 내장하고 있으며 소형 설계를 위하여 모든 변환 과정이 하나의 블록으로 설계되어 중복된 부분을 최소화 하였다. 성능 향상을 위하여 32비트 서브키를 1 클럭에 출력되게 하였다. 제안된 암호 회로를 Hynix 0.25-μm 표준 CMOS 공정에 적용한 결과, 2,658 EG의 회로 크기를 가진다. 그리고 2.5V 동작 전원과 100kHz의 클럭 주파수로 동작시켰을 경우의 10.88μW의 소비 전력 특성을 나타냈다. 본 논문에서 제안된 HIGHT 암호 회로는 수동형 RFID 태그나 스마트 IC 카드와 같은 소형·저전력의 회로에 적용 가능하다.

Abstract

This paper proposed hardware architecture of the block cryptographic algorithm HIGHT aiming small size and low power application, and analyzed its performance. The HIGHT is a modified algorithm of the Feistel. The encryption and decryption circuit were designed as one iterative block. It reduces the redundant circuit that yields small area. For the performance improvement, the circuit generates 32-bit subkey during 1 clock cycle. we synthesized the HIGHT with Hynix 0.25-μm CMOS technology. The proposed circuit size was 2.658 EG(equivalent gate), and its power consumption was 10.88μW at 2.5 V for 100kHz. It is useful for a passive RFID tag or a smart IC card of a small size and low power.

Keywords: cryptographic, hardware architecture

I. 서 론

최근 유비쿼터스(Ubiquitous)와 같은 무선 네트워크 환경의 정보 기술이 주목을 받고 있다. '언제 어디서나' 무선으로 네트워크에 접속하여 편리하게 정보를 주고받을 수 있도록 휴대성이 강조된다. 그러나 휴대형 모바일 장치를 사용할 경우 소비되는 에너지 문제는 풀어야할 큰 문제로 부각된다. 또한 무선 네트워크 환경에서 개인 정보를 어떻게 보호해야할 것인지가 USN (Ubiquitous Sensor Network) 환경 구성을 위한 가장 큰 과제이다.

국내·외 여러 기업, 연구소, 그리고 학교에서 USN에 관한 연구는 꾸준히 연구되어 왔고, 특히 USN 환경의 기초 연구 과제인 RFID와 관련하여 연구가 진행 중이다. ISO 18000 표준에 따르면 RFID를 사용하기 위해 여러 주파수 대역을 정하고 있다. 많은 연구를 통하여 표준 주파수 대역에서 사용할 태그 칩을 준비 중이거나 이미 출시하였다. 그러나 이러한 RFID 태그 칩들은 보안 기능을 포함하고 있지 않다. RFID 칩의 보안 기능을 담당하고 있는 암호 회로에 대한 연구는 대학의 연구 과제로 주로 연구되어 왔다.

미국의 표준 블록 암호 알고리즘인 AES (Advanced Encryption Standard)의 소형·저전력 설계에 관한 연

* 학생회원, ** 정회원, 충북대학교 정보통신공학과
(Dept. of Information & Communication Engineering, Chungbuk National University)
※ 이 논문은 2006년도 교육인적자원부 지방연구중심대학 육성사업의 지원에 의하여 연구되었음.
접수일자: 2006년3월10일, 수정완료일: 2006년12월27일

구를 통하여 수동형 RFID 태그에 암호 기능을 추가하는 연구가 이루어지고 있다. 수동형 태그가 적용될 AES를 이용하여 소형·저전력화하는 연구의 예는 *CHES 2004* 국제 학회에서 발표된 RFID 시스템에서의 인증을 위한 저전력 AES의 구현 기법이 있다[1]. 수동형 RFID 태그 회로에 암호화 기능을 적용하기 위해서는 5,000 EG 이하의 회로 크기와 $15\mu A$ 이하의 적은 소비 전류, 그리고 $18ms$의 암호화 또는 복호화 시간 조건을 만족해야 한다. Feldhofer 등이 제안한 방법은 AES를 구현하기 위해 3,595 EG(Equivalent Gates)의 회로 크기와 $100kHz$에서 $8.15\mu A$의 전류 소비($0.35\mu m$ CMOS 공정) 특성을 가지고 있다[1]. 128비트의 데이터를 암호화를 위해 약 1,000 clock cycle이 요구된다. 소형·저전력을 위해 제안된 다른 암호 알고리즘은 Gaubatz 등에 의해 소개되었다[2]. 공개키 암호 알고리즘을 이용하여 USN 환경에 적용 가능하게 하였다. Robin 암호 알고리즘과 NTRU 암호 알고리즘이 있는데 NTRU 암호 알고리즘은 RFID 태그와 스마트 태그에 적합하게 이용될 수 있는 알고리즘이다. NTRU는 $500kHz$에서 동작시켰을 경우 $19.13\mu W$의 소비 전력을 나타냈고 2,850 EG의 작은 회로 사이즈를 나타냈다. USN 환경과 같이 무선 네트워크를 기반으로 하는 환경에서는 개인의 정보 보호가 중요시 되므로 암호 회로의 소형·저전력 설계는 무엇보다 필요하다.

이러한 흐름에 맞추어 국내에서도 소형·저전력 환경에 맞는 암호 알고리즘이 개발되고 있다. 대표적으로 HIGHT 블록 암호 알고리즘이 있다. 이것은 수동형 RFID 태그에 사용될 만큼 소형·저전력 소비의 회로로 개발된 암호 알고리즘이다. HIGHT은 AES나 ARIA에 비해 암·복호화 할 수 있는 데이터의 크기가 작다. HIGHT은 64비트의 데이터 입·출력을 가지며 128비트의 고정된 키 길이의 입력을 받을 수 있게 되어 있다. 라운드 변환 32회와 초기 및 최종 변환을 포함하여 총 34회의 데이터 변환을 취한 후에 암호화나 복호화된 데이터를 얻을 수 있다. 본 논문에서는 소형·저전력 소비 특성을 갖는 HIGHT 블록 암호 알고리즘에 대하여 하드웨어로 설계하였으며, 수동형 RFID 태그 환경에 적합한 회로 크기와 소비 전력 특성에 대하여 특성을 분석하였다.

본 논문은 다음과 같이 구성되어 있다. Ⅱ장에서는 HIGHT 블록 암호 알고리즘에 대하여 소개하였다. Ⅲ장에서는 HIGHT 블록 암호 알고리즘에 적합한 하드웨어 구조를 제안하고 설계된 HIGHT에 대하여 회로 크기, 소비 전력 및 성능을 분석하였다. 그리고 Ⅳ장에서 결론을 맺는다.

Ⅱ. HIGHT 알고리즘의 소개

본 장에서는 새로운 블록 암호 알고리즘인 HIGHT에 대하여 소개하고, HIGHT 알고리즘에 적합한 하드웨어 구조를 제안한다. HIGHT 블록 암호 알고리즘은 일반화된 Feistel 구조의 변형된 형태를 가진다. 입·출력의 데이터는 64비트 크기를 가지며 키의 크기는 128비트로 고정 된다. 입력되는 데이터는 1워드(8비트) 단위로 법 2^8 덧셈(⊞), 법 2^8 뺄셈(⊟), XOR(⊕), 좌측순환이동(≪)의 단순한 연산만을 사용하여 암·복호화를 수행한다. 그림 1은 HIGHT 알고리즘의 전체 블록 다이어그램을 나타낸다. 32회의 라운드 변환을 통하여 암·복호화가 이루어지지만, 라운드 함수 내부 연산의 입력 정보를 숨기기 위해 화이트닝키(Whitening Key)를 사용하여 초기변환(Initial transform)과 최종변환(Final transform)을 한다. 암·복호화가 같은 데이터 패스를 가지나 암·복호화 연산에는 각 블록의 기능이 조금씩 다르다.

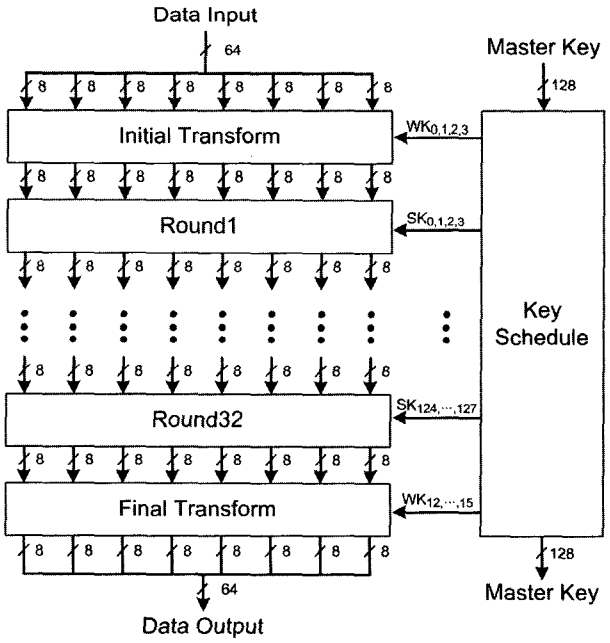


그림 1. HIGHT의 블록 다이어그램
Fig. 1. Block diagram of HIGHT.

1. 암호화 과정

키 스케줄 블록은 입력되는 128비트 키를 사용하여 라운드 변환에 사용될 서브키를 생성한다. 그림 2와 같

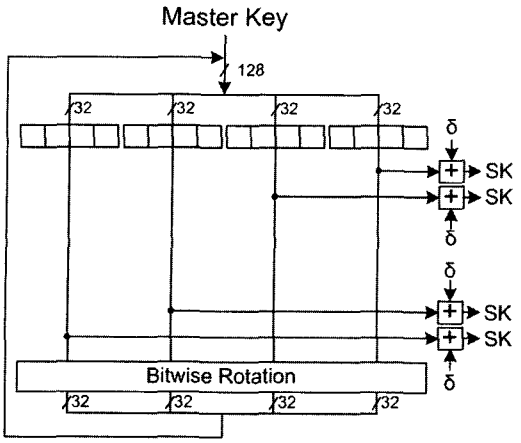


그림 2. 키 스케줄 블록 다이어그램
Fig. 2. Block diagram of key schedule.

이 표현된 이 블록은 초기 변환 및 최종 변환에 사용될 화이트닝키(WK_i)와 32 회 라운드 변환에 사용할 서브키(SK_i)를 다음의 식으로 정의한다.

```
KeySchedule (MK, WK, SK) {
    WhiteningKeyGeneration (MK, WK);
    SubkeyGeneration (MK, SK);
}
```

이 블록은 입력되는 128비트 키가 그림 3과 같이 비트 순환(Bitwise rotation)되어 다음 키의 입력이 되는 순환 구조를 가진다. 비트 순환의 주기는 8회이며, 8회의 비트 치환을 하게 되면 처음에 입력했던 키와 동일한 키 값을 얻을 수 있다. 순환되는 128비트의 키 중에서 32비트의 데이터와 LFSR h의 내부 상태인 δ_i값의 덧셈으로 서브키가 생성된다. 다음은 *WhiteningKey-Generation* 함수와 *SubkeyGeneration* 함수를 나타낸 것이다.

```
WhiteningKeyGeneration (MK, WK) {
    For i = 0 to 7 {
      If 0≤i≤3, then WK_i ← MK_{i+12};
      Else, WK_i ← MK_{i-4};
    }
}
SubkeyGeneration (MK, SK) {
    Run ConstantGeneration
    For i = 0 to 7 {
      For j = 0 to 7 {
        SK_{16·i+j} ← MK_{j-i mod 8} ⊞ δ_{16·i+j};
      }
      For j = 0 to 7 {
        SK_{16·i+j+8} ← MK_{(j-i mod 8)+8} ⊞ δ_{16·i+j+8};
      }
    }
}
```

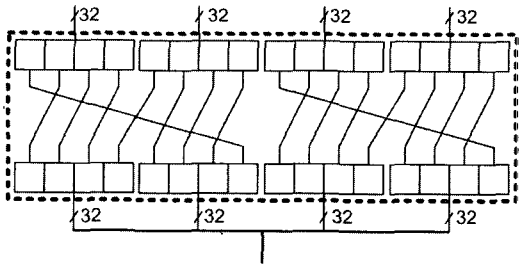


그림 3. 비트 순환
Fig. 3. Bitwise rotation.

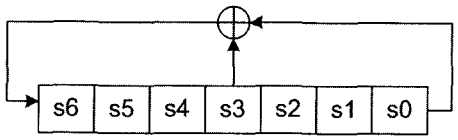


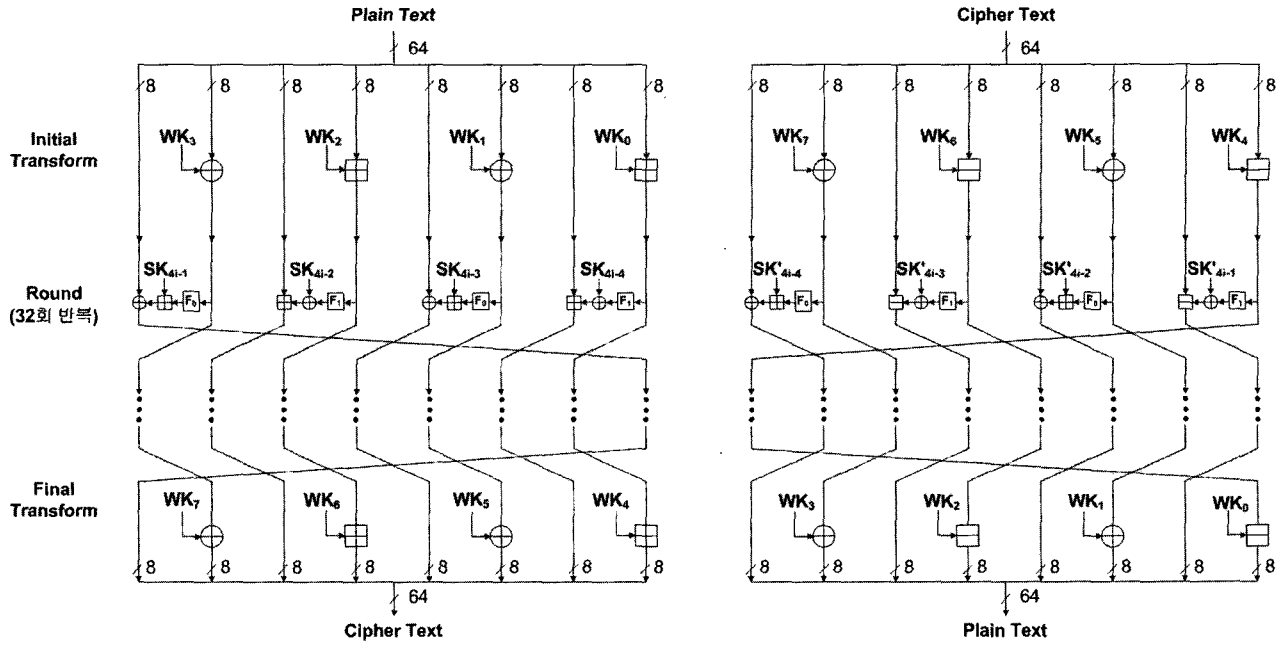
그림 4. LFSR h
Fig. 4. LFSR h.

LFSR(Linear Feedback Shift Register)로 구성된 *ConstantGeneration* 함수는 δ_i를 생성하며 연결 다항식은 x^7+x^3+1로 표현된다. δ_i는 총 7비트의 레지스터로 구성되고 $(1011010)_2$의 초기값을 가진다. LFSR h의 블록도인 그림 4에서 $s6$이 MSB(Most Significant Bit)를 나타내며 $s0$가 LSB(Least Significant Bit)를 나타낸다. 매 클럭마다 오른쪽으로 쉬프트를 하여 내부의 상태값($s6$, $s5$, $s4$, $s3$, $s2$, $s1$, $s0$)이 변하게 된다. 내부 상태값인 δ_i는 127의 주기로 반복($\delta_0=\delta_{127}$)되므로 i는 $0\le i\le 127$의 범위를 가진다.

생성된 δ_i와 비트 순환되는 마스터키의 ⊞연산을 통해 서브키를 생성할 수 있다. 입력되는 128비트의 마스터키를 이용하여 1회의 비트 순환을 하면 4회의 라운드 변환에 사용되는 서브키가 생성된다. 그러므로 32회의 라운드 변환에 사용되는 서브키의 생성은 8회의 비트 순환을 통해 이루어진다.

그림 5a는 HIGHT의 암호화 과정을 보여주며 초기변환, 32회의 라운드 변환, 최종변환을 나타낸다. 초기 및 최종변환은 마스터키를 사용하여 연산을 하게 된다. 키 스케줄에서 8회 주기를 갖는 비트 치환 특성으로 최종변환에 사용되는 서브키는 새로운 마스터키를 입력받지 않고 생성될 수 있다. 라운드 변환에 사용되는 *F0*, *F1* 함수는 좌측순환이동(≪)과 XOR(⊕)의 조합으로 구성되며 다음의 식으로 정의된다.

$$F0(x)=(x\ll 1)\oplus(x\ll 2)\oplus(x\ll 7)$$
$$F1(x)=(x\ll 3)\oplus(x\ll 4)\oplus(x\ll 6)$$



(a) 암호화 과정 (b) 복호화 과정
(a) Encryption (b) Decryption

그림 5. HIGHT의 암호화 및 복호화 과정
Fig. 5. Encryption and decryption process of HIGHT.

2. 복호화 과정

HIGHT의 복호화 과정은 암호화 과정과 유사하다. 복호화에 사용되는 서브키는 암호화에 사용된 서브키의 역순으로 수행된다. 즉, 암호화에 사용된 최종 변환의 서브키는 복호화에서 초기 변환의 서브키로 사용된다. 복호화에 사용되는 서브키(SK'_i)는 다음으로 정의된다.

$$SK'_i = SK_{127-i} \quad , i = 0, \cdots, 127$$

그림 5b는 HIGHT의 복호화 과정을 나타낸다. 암호화 과정과 유사하나 라운드 변환과 최종 변환의 스왑(swap)이 반대로 수행되는 것과 각 변환 단계 중 일부의 ⊞연산이 ⊟연산으로 변경되는 것이 다른 점이다.

III. 제안된 HIGHT의 하드웨어 구조 및 성능 분석

본 장에서는 II장에서 소개된 HIGHT 블록 암호 알고리즘에 적합한 하드웨어 구조를 제안한다. 소형화와 저전력을 위하여 불필요하게 중복되는 로직을 공유하여 사용하였다.

1. 제안된 HIGHT의 하드웨어 구조

소형·저전력 구조로 개발된 HIGHT 암호 알고리즘은 회로의 크기를 최소화시켜 수동형 RFID 태그의 소형 환경에도 적용 가능하도록 설계되어야 한다. 그림 6은 본 논문에서 제안하는 HIGHT 블록 암호 회로의 블록 다이어그램을 나타낸다. 키 생성을 하는 키 스케줄 블록과 암·복호화를 수행하는 라운드 블록으로 나눌 수 있다. 라운드 블록은 입력되는 64비트의 데이터를 암호화나 복호화할 때 사용된다. 라운드 블록은 알고리즘에서 나타낸 초기·라운드·최종 변환을 모두 수행할 수 있게 설계되었다. 입력되는 데이터의 반복을 위해서 64비트의 레지스터를 포함하고 있다. 키 스케줄 블록은 on-the-fly 방식으로 매 클럭마다 라운드 변환에 필요한 32비트의 키를 생성할 수 있도록 설계 되어 하드웨어 구조의 효율성을 높였다. 또한 암·복호화 선택신호(en_de)에 의해서 암호화나 복호화를 선택할 수 있다.

제안된 HIGHT의 키 스케줄 구조는 그림 7과 같이 암호화의 비트 순환과 복호화의 비트 순환을 병행하여 수행하도록 설계되었다. 초기 변환과 최종 변환에 사용되는 서브키는 δ_i와의 연산을 수행하지 않고, 마스터키를 그대로 출력하기 위해 '0'의 ⊞연산을 수행한다. 이

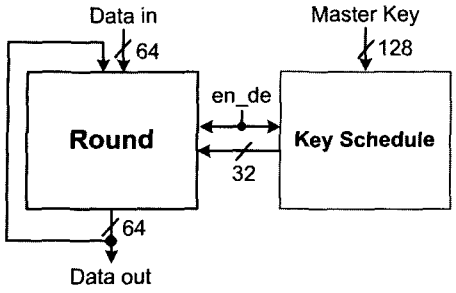


그림 6. 제안된 HIGHT의 데이터 패스
Fig. 6. Proposed data paths of HIGHT.

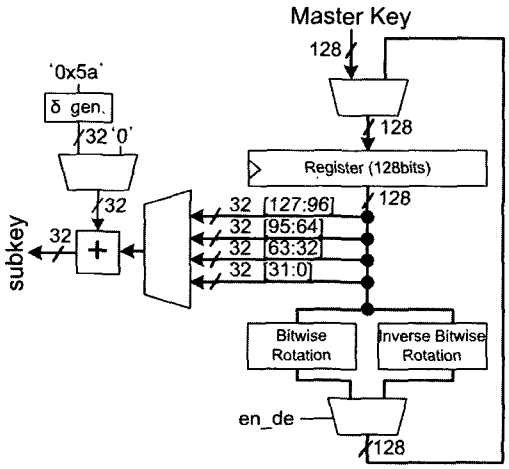


그림 7. 제안된 키 스케줄 블록
Fig. 7. Proposed key schedule block.

것은 추가적인 MUX 로직을 사용하지 않기 위한 방법이다. 즉, 마스터키의 일부를 서브키로 그대로 사용가능하게 만들었다.

LFSR h를 통해 나온 δ_i와 마스터키의 비트 순환된 데이터 중 32비트만을 사용하여 라운드 변환에 사용되는 서브키를 생성할 수 있다. 32비트의 δ_i와 비트 순환된 마스터키는 각 8비트씩 ⊞연산을 통해 32비트의 서브키를 생성한다. 32회의 라운드 변환에 사용될 서브키는 8회의 비트 순환을 통해 구할 수 있다. 이 때 반복되는 마스터키의 입력을 위해서 레지스터에 클럭 게이트 방법을 사용하였다. 이 방법은 회로를 저전력 및 소형화할 수 있다. 비트 순환을 위해 사용된 블록은 그림 3과 같이 단순한 선연결(wiring)로 구성이 가능하며 사용된 로직은 없다. 암호화와 복호화 기능을 모두 포함하기 위해 병렬로 처리되며 암·복호화 선택신호에 의해 각각의 동작이 이루어진다.

δ_i 생성 회로는 그림 8에 나타나 있다. δ_i의 값은 복호화시 반대로 연산 되므로 암호화를 위한 δ_i생성 회로와 복호화를 위한 δ_i생성 회로를 다르게 만들어 MUX

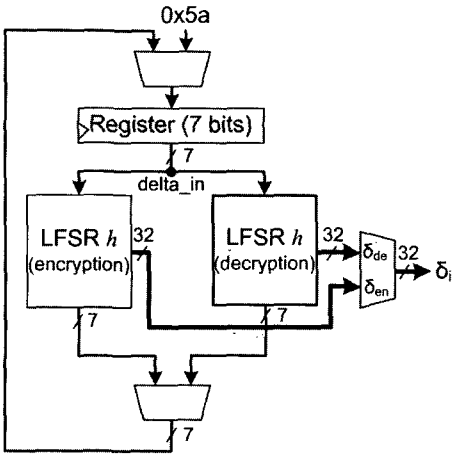
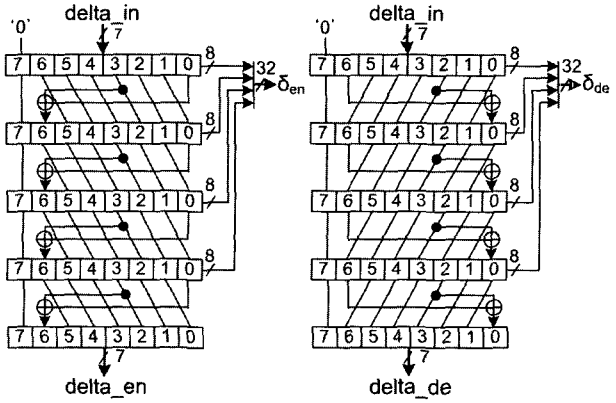


그림 8. δ_i 생성 회로
Fig. 8. δ_i generation. circuit



(a) LFSR h - encrypt (b) LFSR h - decrypt

그림 9. LFSR h 내부 회로
Fig. 9. Inner circuit of LFSR h.

로 선택할 수 있게 하였다. 그림 9은 LFSR h의 내부 회로를 자세히 나타낸 것이다. 각 숫자는 데이터의 각 비트를 나타내며 단순히 선연결(wiring)로 구성된다. ⊞연산을 위해 8비트의 δ_i 출력을 32비트로 묶어서 출력하게 설계하였다. 복호화시에는 LFSR h 회로가 역으로 수행 할 수 있도록 그림 9b와 같이 설계되었다. LFSR h의 회로는 4개의 XOR만을 사용하여 회로의 크기를 최소화 시켰다.

그림 10은 제안된 라운드 변환 회로이다. 그림 5에서 설명된 암·복호화 알고리즘 중 수행 횟수가 많은 라운드 변환에 초점을 맞추어 설계되었다. 제안된 라운드 회로는 초기 변환과 최종 변환 연산에도 적용 가능하다. 입력되는 64비트의 데이터를 8비트의 워드 단위로 다음과 같이 표현 가능하다.

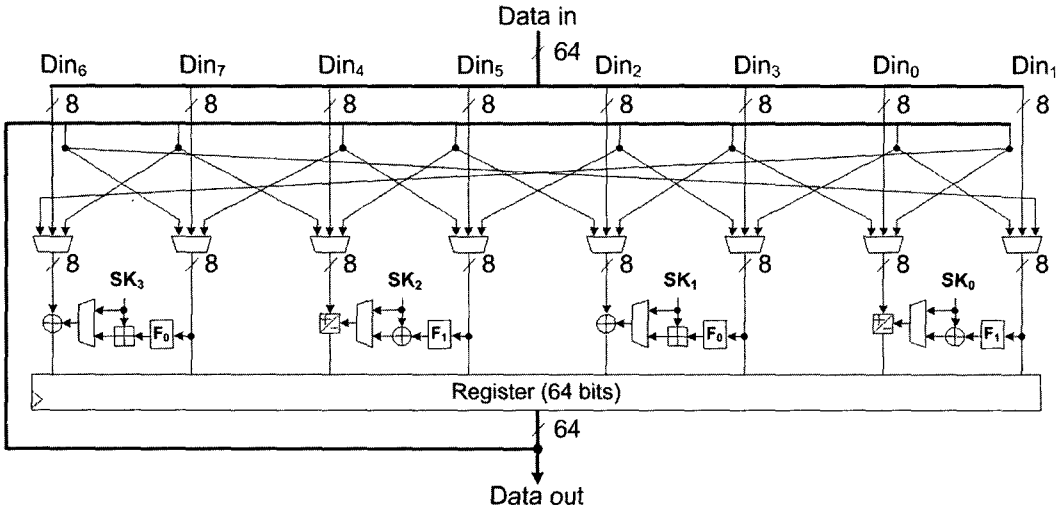


그림 10. 제안된 라운드 변환 회로
Fig. 10. Proposed round circuit.

$$Data\ in = Din7||Din6|| \ldots ||Din1||Din0$$

*Din7*과 *Din0*을 각각 MSB와 LSB로 정의한다. 암호화를 위해 초기 변환을 하려면 데이터 입력을 그림 10과 같이 홀수 번째와 짝수 번째 데이터로 교차 입력시킨다. 이 후에는 레지스터에 입력된 데이터가 순환되면서 32회의 라운드 변환을 한다. 데이터 입력 부분에 있는 3-to-1 MUX를 이용하여 라운드 변환의 출력의 스왑을 해결할 수 있다. 최종 변환 과정은 입력되는 데이터의 MUX를 교차 입력시켜 원하는 암호화된 데이터를 얻을 수 있다.

복호화는 초기 변환과 최종 변환의 ⊞연산이 ⊟연산으로 바뀌는 것과 라운드 변환 중 일부의 ⊞연산이 ⊟연산으로 바뀌는 것, 그리고 스왑이 반대로 수행 된다는 점이 암호화와 다르다. 암호화할 때와 동일하게 복호화할 때도 32회째 라운드는 최종 변환과 연결하면 스왑이 일어나지 않게 할 수 있다. 암호화에서 설명한 방법과 유사하게 32회의 라운드를 동일하게 수행하고 최종 변환에서 역방향으로 스왑을 수행하면 원하는 결과를 얻을 수 있다.

2. 성능 분석

본 논문에서 제안하는 HIGHT 블록 암호 회로는 Verilog-HDL을 이용하여 구현하였다. 구현된 암호 회로는 IDEC에서 지원된 Hynix 0.25-μm 표준 CMOS 공정에서 Synopsys사의 Design Compiler로 합성하였다. 그리고 소비 전력 분석은 공정의 Spice 모델 파라미터와 Synopsys사의 NanoSim을 이용해 측정한 결과이다. 표 1은 제안된 HIGHT 블록 암호 회로의 크기 및

표 1. HIGHT 암호 회로의 크기 및 소비 전력
Table 1. Circuit size and power consumption of HIGHT.

HIGHT	Size		Power Consumption	
	EG	(%)	μW	(%)
Key schedule	1,633	61.4	4.56	41.8
Round	842	31.7	5.90	54.3
Control	183	6.9	0.42	3.9
Total	2,658	100	10.88	100

표 2. 제안된 HIGHT의 하드웨어 특성
Table 2. Hardware property of HIGHT.

HIGHT block cipher	Property
Equivalent Gates	2,658 EG
μA@{$100kHz$, $2.5V$}	4.352 μA
Energy	3.69 nJ
Latency(max freq.)	8 ns(125 MHz)
Power consumption	10.88 μW
Clock cycles	34 clock
Throughput(max)	235 $Mbps$

소비 전력을 보여준다. HIGHT 블록 암호 회로의 크기는 블록 암호 회로로서는 매우 작은 2,658 EG를 나타내었다. 내부 블록 중 키 스케줄 블록이 1,633 EG로 61.4%를 차지하였고 라운드 블록은 31.7%를 차지한 842 EG를 나타냈다. HIGHT 블록 암호 회로가 64비트의 데이터를 암호화 하는데 소비된 전력은 $10.88\mu W$이다. 그 중 54.3%를 라운드 변환 블록이 소비하였고 키 스케줄 블록은 41.8%를 소비하였다. 참고문헌 [2]와 비교하여 에너지 소비를 계산할 경우, 64비트의 데이터를 암호문으로 만드는데 걸린 시간이 $340us$ 이므로 에너지는 $3.69nJ$ 임을 알 수 있다. 표 2는 설계된 HIGHT의 특징을 정리한 것이다.

제안된 HIGHT 암호 회로는 소형·저전력 환경에 적용하기 위하여 설계되었다. 소형·저전력 응용 환경인 수동형 RFID 태그의 적용 가능한 기준은 5,000 EG 이하의 회로 크기, $15\mu A$의 소비 전류, 그리고 $15ms$ 이내의 암호화나 복호화 시간으로 제한을 할 수 있다[1]. 제안된 구조로 설계된 HIGHT 블록 암호 회로는 2,658 EG의 회로 크기, $4.352\mu A$의 소비 전류, 그리고 $340us$의 암호화나 복호화 시간을 가지므로 수동형 RFID 태그 회로에 적용 가능하다. 설계된 HIGHT은 수동형 RFID 태그에 사용하기 위해 낮은 동작 주파수인 100 kHz로 동작시켰을 경우 $1.882Mbps$의 성능을 나타내었으며, 최대 $125MHz$에서 $235Mbps$의 성능을 보였다.

IV. 결 론

본 논문은 수동형 RFID 태그와 같은 소형·저전력 환경에서 정보 보호 기능을 위해 개발된 HIGHT 블록 암호 알고리즘에 적합한 하드웨어 구조를 제안한다. HIGHT 블록 암호 알고리즘은 64비트의 데이터 입·출력과 128비트의 키를 사용할 수 있으며, 그 구조는 일반화된 Feistel 구조의 변형된 형태를 취하고 있다. 설계된 HIGHT은 암호화 및 복호화 기능을 내장하고 있으며 소형·저전력 설계를 위하여 초기 및 최종 변환 과정과 라운드 변환이 하나의 블록으로 설계되어 중복된 부분을 최소화 하였다. 또한 키 스케줄 블록은 32비트 서브키를 1클럭에 출력되게 하여 암호화 또는 복호화 기능을 수행 할 수 있게 하였다.

HIGHT 암호 회로는 Verilog-HDL로 설계 되었으며 IDEC에서 지원된 Hynix 0.25-μm CMOS 공정에 적용한 결과로 2,658 EG의 회로 크기를 가졌다. $2.5V$ 동작 전원, 그리고 수동형 RFID 태그에서 사용할 $100kHz$의 클럭 주파수로 동작시켰을 경우의 $10.88\mu W$의 소비 전력과 $4.352\mu A$의 소비 전류를 보였다. 적은 소비 전류로 인해 IC 카드나 수동형 RFID 태그와 같이 개인의 정보 보호를 필요로 하는 소형·저전력 환경의 응용 회로에 적용 가능하다.

참 고 문 헌

[1] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, "Strong authentication for RFID systems using the AES algorithm," *In Proc. Workshop on Cryptographic Hardware and Embedded Systems(CHES2004)*, pp. 357-370, Aug. 2004.

[2] G. Gaubatz, J.-P. Kaps, and B. Sunnar, "Public key cryptography in sensor networks-revisited," *In Proc. Workshop on Security in Ad-Hoc and Sensor Networks (ESAS 2004)*, vol. 3313, Aug. 2004.

[3] G. Gaubatz, J.-P. Kaps, E. Ozturk, and B. Sunar, "State of the art in ultra-low power public key cryptography for wireless sensor networks," *In Proc. on Pervasive Computing and Communications Workshops*, pp. 146-150, March 2005.

[4] M. Feldhofer, J. Wolkerstorfer, and V. Rijmen, "AES implementation on a grain of sand," *In Proc. Information Security*, vol. 152, issue 1, pp. 13-20, Oct. 2005.

[5] NIST FIPS PUB 46 : Data Encryption Standard, January, 1977.

[6] K. Finkenzeller, *RFID-Handbook*, 2nd Edition, April 2003.

[7] G. Rouvroy, F.-X. Standaert, J.-J. Quisquater, and J.-D. Legat, "Compact and efficient encryption/decryption module for FPGA implementation of the AES Rijndael very well suited for small embedded applications," *In Proc. International Conference on Information Technology : Coding and Computing (ITCC'04)*, pp. 583-587, April 2004.

[8] Deukjo Hong, Jaechul Sung, Seokhie Hong, Jongin Lim, Sangjin Lee, Bon-Seok Koo, Changhoon Lee, Donghoon Chang, Jesang Lee, Kitae Jeong, Hyun Kim, Jongsung Kim, and Seongtaek Chee, "HIGHT: A New Block Cipher Suitable for Low-Resource Device," *In Proc. Workshop on Cryptographic Hardware and Embedded Systems(CHES2006)*, pp. 46-59, Oct. 2006.

저 자 소 개

임 영 일(학생회원)

2005년 충북대학교 정보통신공학과 공학사.
2005년 3월~현재 충북대학교 정보통신공학과 석사과정.
<주관심분야 : 저전력 디지털 회로 설계, 비동기 회로 설계>

유 영 갑(정회원)

1975년 서강대학교 전자공학과 공학사
1975년~1979년 국방과학연구소 연구원
1981년 Univ. of Michigan, Ann Arbor 전기전산학과 공학석사
1986년 Univ. of Michigan, Ann Arbor 전기전산학과 공학박사
1986년~1988년 금성반도체(주) 책임 연구원
1993년~1994년 아리조나 대학교 객원교수
1998년~2000년 오레곤 주립대학교 교환교수
1988년~현재 충북대학교 정보통신공학과 교수
<주관심분야 : VLSI 설계 및 테스트, 고속인쇄회로 설계, 암호학>

조 경 록(정회원)

1977년 경북대학교 전자공학과 공학사
1989년 일본 동경대학교 전자공학과 공학석사
1992년 일본 동경대학교 전자공학과 공학박사
1979년~1986년 (주)금 성 사 TV연구소 선임연구원
1999년~2000년 Oregon State University 객원교수
1992년~현재 충북대학교 전기전자공학부 교수
<주관심분야 : 통신시스템 LSI 설계, 저전력 고속 회로 설계, Platform기반의 SoC설계>