UHF 대역 RFID 시스템을 위한 블록 암호 회로와 프로토콜

Block Cipher Circuit and Protocol for RFID in UHF Band

이상진, 박경창, 김한벼리, 김승열, 유영갑
충북대학교 정보통신공학과

Sang-Jin Lee(sjlee@hbt.cbnu.ac.kr), Kyung-Chang Park(kcpark@hbt.cbnu.ac.kr),
Hanbyeori Kim(hbkim@hbt.cbnu.ac.kr), Seung-Youl Kim(kimsy@hbt.cbnu.ac.kr),
Younggap You(ygyou@cbnu.ac.kr)

요약

본 논문은 HIGHT 블록 암호 알고리즘의 성능 개선을 위하여 하드웨어 구조와 키 스케줄의 공유를 위한 FSM을 제안하였다. 또한 HIGHT 블록 암호 알고리즘을 RFID 시스템에 적용하였을 때 사용 가능한 효과적인 프로토콜을 도입하였다. 개선된 HIGHT 블록 암호 회로의 하드웨어 크기는 RFID 태그에 적용 가능한 작은 크기를 가지면서 기존의 HIGHT 블록 암호 회로에 비해 암호화 성능을 두 배로 향상시켰다. 제안하는 프로토콜은 무선 주파수 통신으로 인한 보안의 취약성을 극복하여 RFID 태그의 개인정보에 대한 보안을 강화할 수 있다.

■ 중심어 : | RFID | UHF 대역 | 초경량 블록 암호 | HIGHT | 프로토콜 |

Abstract

This paper proposes a hardware structure and associated finite state machine designs sharing key scheduling circuitry to enhance the performance of the block cypher algorithm, HIGHT. It also introduces an efficient protocol applicable to RFID systems comprising the HIGHT block cipher algorithm. The new HIGHT structure occupies an area size small enough to accommodate tag applications. The structure yields twice higher performance them conventional HIGHT algorithms. The proposed protocol overcomes the security vulnerability of RFID tags and thereby strengthens the security of personal information.

■ keyword : | RFID | UHF Bnad | Ultra-weight Block Cipher | HIGHT | Protocol |

I. 서론

최근에 유비쿼터스 컴퓨팅이 중요시 되면서, 암호 어플리케이션을 이러한 환경에 적합하도록 설계하는 연구가 활발하다. 특히 Radio Frequency Identification (RFID) 시스템은 자동 요금 징수 및 물류 유통 관리 등에 많이 활용되고 있다. 하지만 리더(reader)와 태그(tag)간의 무선 주파수 통신은 정보의 기밀성과 보안에 문제를 갖고있다. 이러한 문제는 RFID 기술을 진보시키기 위하여 고려되어 왔다. 그러나 유비쿼터스 컴퓨팅은 low-cost, low-power, light-weight 플랫폼에서 이루어지기 때문에 암호 알고리즘을 적용하는데 제약이 따른다[2].

UHF 대역의 RFID 태그의 사용자 정보를 암호화하

접수번호 : #090909-006
접수일자 : 2009년 09월 09일
심사완료일 : 2009년 11월 24일
교신저자 : 유영갑, e-mail : ygyou@hbt.cbnu.ac.kr

기 위해 경량화된 Advanced Encryption Standard (AES)가 주로 연구되어 왔다[4-6]. 최근에 RFID에 적용 가능한 초경량 암호 알고리즘으로 High Security and Light Weight(HIGHT) 암호 알고리즘이 개발되었다. D. Hong 등은 RFID 보안을 위해서 AES보다 경량화된 HIGHT를 RFID 태그에 적용하였다[2]. 하지만 S-box의 최적화를 통한 32-bit 구조를 갖는 A. Satoh의 AES가 적용된 RFID 시스템[5]에 비하여 낮은 처리량을 갖는다.

본 논문에서는 HIGHT의 처리량을 개선하기 위하여 새로운 구조를 제안하였다. 또한 RFID 시스템에서 무선 주파수 통신에 의해 야기될 수 있는 문제를 해결하기 위해 RFID 시스템의 새로운 프로토콜을 제안한다. 개선된 HIGHT는 128-bit의 데이터 블록과 128-bit의 키 길이를 가진다. 이것은 0.25um 공정에서 합성하였을 때 3882GE(Gate Equivalent)s의 크기를 가진다. 개선된 HIGHT는 기존과 동일한 클럭 cycle을 가지면서 80MHz 시스템 클럭에서 301.2Mbps 의 처리량을 가진다.

본 논문의 2장에서 HIGHT 암호 알고리즘에 대해 설명하고, 3장에서 개선된 HIGHT 회로를 제안한다. 4장에서는 RFID 시스템에 HIGHT를 적용한 프로토콜을 제시하고, 5장에서 제안된 회로의 성능 평가 및 분석을 한다. 6장에서 결론을 맺는다.

II. HIGHT

본 장에서는 RFID 시스템에서 사용되는 초경량 블록 암호에 대하여 소개하고 구조에 대해 기술한다. HIGHT는 태그 부에 탑재된다. HIGHT는 초경량 블록 암호로서 태그 데이터의 보호와 면적의 한계를 해결 할 수 있다.

1. 초경량 블록 암호 HIGHT

본 절은 초경량 블록암호인 HIGHT 블록암호 알고리즘에 대해서 소개한다. HIGHT는 소형 · 저전력 환경에 적용하기 위하여 설계되었다. HIGHT 블록 암호 알고리즘은 64비트의 데이터 입 · 출력과 128비트의 키를 사용할 수 있다. 또한 HIGHT구조는 일반화된 Feistel 구조의 변형된 형태를 가진다. 입력데이터는 1워드 (8 비트) 단위로 법2^8 덧셈($\boxplus$), 법 2^8 뺄셈($\boxminus$), exclusive-OR($\oplus$), 좌측 순환이동(<<<)의 간단한 연산만으로 암호화와 복호화를 수행한다. 그림 1은 HIGHT 블록 암호 알고리즘의 전체 블록 다이어그램을 나타낸다. 화이트닝 키(whiteing key)는 라운드 함수 내부 연산의 입력 정보를 숨기는데 사용된다. 이를 이용해 초기변환(intial transform)과 최종변환(final transform)을 수행하게 된다. 또한 32 라운드 변환을 통해 암호화와 복호화가 이루어진다[1].

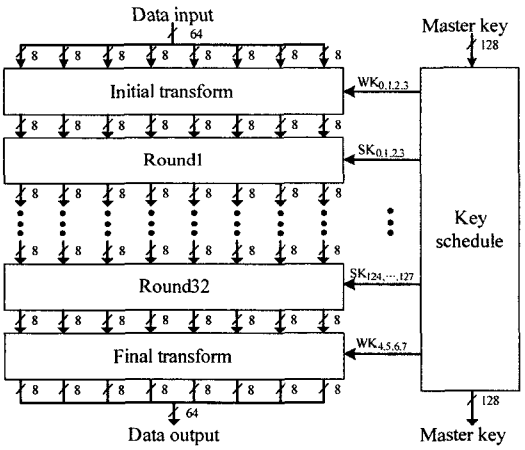


그림 1. HIGHT 블록 다이어그램[1]

2. HIGHT 암호화 과정

키 스케쥴 블록은 128비트의 마스터 키(MK)를 이용하여 각 라운드 변환에 사용될 128 바이트 서브 키(SK)를 생성한다. 또한 초기 변환 및 최종변환에 사용되는 화이트닝 키(WK)를 생성하는 과정은 다음과 같다[2].

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

화이트닝 키는 총 8 바이트($WK_0, \ldots, WK_7$)가 생성된다. 화이트닝 키 생성알고리즘은 아래와 같다.

```
WhiteningKeyGeneration {
 For i = 0 to 7 {
    If 0 ≤ i ≤ 3, then WKi ← MKi+12
 Else, WKi ← MKi−4
   }
}
```

서브 키는 총 128개가 생성되며 32라운드 변환에 사용된다. 또한 각 라운드 변환마다 4개의 서브 키가 사용된다. 서브 키 생성을 위한 과정은 다음과 같다[2].

```
SubkeyGeneration(MK, SK) {
  Run ConstantGeneration
   For i = 0 to 7 {
    For j = 0 to 7 {
      SK16·i+j ← MKj−8i mod 8 ⊞16·i+j
    }
    For j = 0 to 7 {
      SK16·i+j+8 ← MK(j−8i mod 8)+8 ⊞16·i+j+8
    }
   }
}
```

SubkeyGeneration 함수에는 LFSR (Linear Feedback Shift Register)로 구성된 constant generation 함수가 있다. 이는 δ_i를 생성하며 연결 다항식은 $x^7 + x^3 + 1$ 이다. δ_i는 7비트의 레지스터이며 초기값은 1011010_2로 초기값을 갖는다. LFSR h는 내부 상태 값 δ_i을 생성한다. LFSR h 매 클럭마다 7비트 값이 우측 쉬프트를 하여 내부 상태 값 δ_i이 변한다. δ_i는 주기가 127 로 반복되고 i 의 범위는 $0 \le i \le 127$이다.

암호화 과정은 초기변환, 32번의 라운드 변환, 최종변환으로 구성된다. 초기 변환은 마스터 키를 이용해 연산된다. 최종 변환에 사용되는 서브 키는 새로운 마스터 키를 입력 받지 않고 생성 가능하다. 그것은 키 스케줄에서 주기 8을 갖는 비트 치환 특성이 있기 때문이다.

각 라운드 변환에서 사용된 F_0, F_1함수는 좌측순환이동(<<<)과 Exclusive-OR(⊕)의 조합으로 구성된다. 함수에 대한 정의는 아래와 같다.

$$F_0(x) = (x \lll 1) \oplus (x \lll 2) \oplus (x \lll 7)$$
$$F_1(x) = (x \lll 3) \oplus (x \lll 4) \oplus (x \lll 6)$$

3. HIGHT 복호화 과정

HIGHT의 복호화 과정은 암호화 과정과 유사한 형태를 가진다. HIGHT 복호화 과정은 라운드 변환과 최종변환의 스왑(swap)이 반대로 되는 것, 각 변환단계의 SK'_{4i-3}, SK'_{4i-1}이 적용되는 부분에서 ⊟연산을 수행한다는 점이 다르다. 키는 암호화에서 사용되는 키의 역순으로 적용된다. 복호화에 사용되는 서브 키(SK'_i)는 다음과 같이 정의 된다.

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

III. 제안하는 암호 회로

본 절에서는 태그 정보의 암호화를 위한 블록 암호 회로를 제안한다. [그림 2]는 제안된 암호 회로 구조이다.

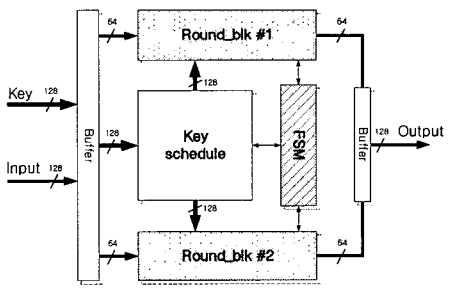


그림 2. 제안하는 암호 회로의 블록도

제안된 암호 회로는 FSM, key schedule block, 그리고 2개의 라운드 블록(Round_blk1, Round_blk2)으로 구

성된다. 제안된 암호 회로 구조는 HIGHT의 기본 구조를 따르며 라운드 블록을 2개로 확장하였으며, FSM과 키 스케쥴 블록을 동시에 공유하는 방식을 사용했다.

[표 1]은 0.25um 공정에서 HIGHT의 게이트 수를 나타낸 것이다. 라운드 블록은 총 면적의 27.5%를 차지한다. 제안된 암호 회로는 HIGHT회로 총 면적의 약 70% 이상을 공유하고 128bit블록 암호가 가능한 구조이다.

표 1. HIGHT의 게이트수

Component	Gate Counts	%
Control Logic	562	14.5
Key Schedule	1648	42.5
Round Block	1668	43.0
Total	3882	100

IV. 제안하는 프로토콜

제안하는 프로토콜은 리더와 태그의 무선 주파수 통신에서 야기될 수 있는 위험으로부터 USER 영역의 데이터를 보호할 수 있다. 제안하는 프로토콜은 UHF 대역의 RFID 프로토콜을 크게 변경하지 않고 RFID 리더와 태그의 보안성을 높이는데 중점을 두었다. [그림 3]은 UHF 대역의 RFID 태그의 메모리 뱅크를 나타낸다[7]. 보안이 필요한 정보는 USER 영역에 위치한다. HIGHT 암호 회로는 USER 영역의 데이터를 암호화한다.

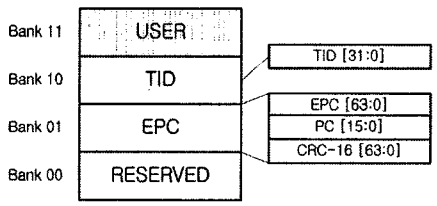


그림 3. RFID Tag의 logical memory map[7]

[그림 4]는 RFID 리더가 access 상태일 때, 태그가 리더를 통해 호스트로 USER 데이터를 송신하는 과정을 보여준다. RFID 시스템의 리더와 태그 간의 통신은 무선으로 이루어지기 때문에 태그의 개인 정보와 제어 신호가 무선으로 전송하기 때문에 불법적으로 태그의 정보가 해킹당할 소지가 있다.

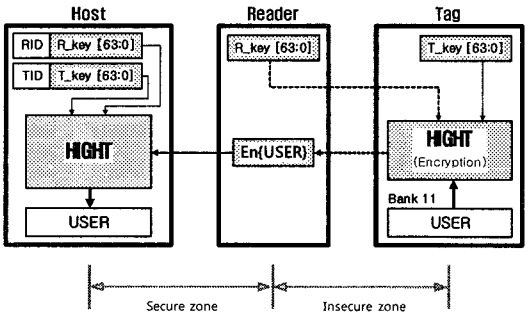


그림 4. Access 시의 USER 데이터 전송

제안하는 프로토콜이 기존의 UHF 대역의 RFID 시스템과 다른 점은 리더와 태그에 각각 리더 키(R_key)와 태그 키(T_key)가 추가 되었다는 것이다. 태그 키와 리더 키는 HIGHT의 암호키로 사용된다. 또한 호스트는 각 리더와 태그의 아이디(RID, TID)에 해당하는 키를 미리 공유하고 있다고 가정한다. 접근된 RFID 리더의 키와 태그의 키를 HIGHT의 암호 키로 사용하므로 호스트에서 태그와 리더를 동시에 인증할 수 있다.

제안하는 프로토콜은 RFID 태그의 정보를 암호화하는데 필요한 정보를 무선으로 노출시키지 않고, 인식하는 리더마다 다른 암호 키 값을 가지기 때문에 해킹이 더욱 어렵다.

V. 성능 분석

본 절은 제안된 암호회로의 성능 평가하고 기존 경량 블록 암호 회로와 비교한다. [표 2]는 제안된 암호 회로의 면적을 기존의 HIGHT와 비교한 것이다.

표 2. Proposed HIGHT의 게이트 수

	This work		HIGHT[3]	
Component	GE	%	GE	%
Control Logic	562	14.5	562	27.5
Key Schedule	1648	42.5	1648	54.1
Round Block	1668	43.0	838	18.4
Total	3882	100	3048	100

회로의 전체 크기는 0.25um 공정에서 3882GEs를 가진다. 제안된 암호 회로는 기존의 key schedule, control logic을 사용하여 라운드 블록의 2배 면적 증가만 있다. 제안된 회로는 HIGHT와 비교해서 면적은 27% 증가한데 비해 처리량은 57% 향상되었다.

Feldholder 등에 의하면 RFID 태그에서 사용할 수 있는 전력은 20uA 정도 이다[6]. 태그의 제어를 위해 5uA의 전력을 소비하기 때문에 암호화를 위해 쓸 수 있는 전력은 나머지 15uA 정도이다. 즉, 하드웨어의 크기가 5000GE 이하가 되어야 한다. 따라서 제안하는 회로의 크기는 3882GEs로 RFID 태그의 보안을 위한 암호 회로로 적합하다.

표 3은 제안된 HIGHT와 기존 암호회로의 성능 을 비교 및 평가한 것이다. 기존 암호 회로는 HIGHT, AES-8, AES-32을 기준으로 하였다. 제안하는 구조는 경량화된 AES[4][5]들과 기존의 HIGHT[3]와 비교하여 가장 높은 처리량을 가진다. 제안된 HIGHT는 기존의 UHF 대역의 RFID 시스템의 보안을 위한 암호 회로들보다 성능적 측면에서 우수하다.

표 3. 암호 회로 성능 비교

	Size(GE)	Cycle	Throughput
This work	3882	34	301.2Mbps(@80MHz)
HIGHT[3]	3048	34	150.6Mbps(@80MHz)
AES-8[4]	3400	1032	9.9Mbps(@80MHz)
AES-32[5]	5400	54	189.6Mbps(@80MHz)

경량화된 AES 하드웨어[4][5]는 암호화를 위해 HIGHT에 비하여 많은 클럭 cycle이 요구된다. HIGHT는 비교적 적은 클럭 cycle로 암호화를 수행할 수 있어 저전력을 요구하는 RFID 태그의 보안에 보다 효율적이다.

VI. 결론

본 논문에서는 기존의 HIGHT 블록 암호 알고리즘을 개선하여 데이터 처리량을 향상시켰다. HIGHT의 암호화 라운드 블록을 두 배로 하면서, 키 스케쥴을 공유할 수 있도록 FSM을 재설계 하였다. 또한 RFID 태그에 HIGHT 블록 암호 알고리즘을 탑재하였을 경우에 효과적인 RFID 시스템의 프로토콜을 제안하였다.

RFID 태그 칩 내부에 암호회로를 탑재하기 위하여 하드웨어의 크기가 작아야하므로, 기존에 RFID 태그의 암호회로로 제안된 HIGHT 블록 암호 알고리즘을 개선하여 전체 하드웨어 사이즈의 증가는 작으면서 데이터 처리량은 두 배 향상 시키는 결과를 얻었다. 제안하는 회로를 0.25um 공정에서 합성하여 기존의 논문들에서 제시한 하드웨어의 크기 및 성능과 비교분석 하였다. 무선 주파수 통신에서 비롯되는 RFID 시스템의 취약점으로부터, HIGHT 블록 암호 알고리즘에 사용되는 암호 키를 외부에서 알 수 없도록 하기 위하여 새로운 프로토콜을 제안하였다.

제안하는 HIGHT 블록 암호 알고리즘 및 프로토콜을 RFID 시스템에 적용하면 기존의 프로토콜을 크게 변화시키지 않으면서 효과적으로 RFID 태그에 저장된 개인정보에 대한 보안을 제공할 수 있다.

참 고 문 헌

[1] 임영일, 유영갑, 조경록, "수동형 RFID 태그에 적합한 암호회로 설계," 전자공학회논문지, 제41권 제1호, 2004.

[2] D. Hong et al. "HIGHT : A new block cipher suitable for low-resource device," CHES 2006, LNCS 4249, pp.46-59, 2006.

[3] D. Hong et al., "HIGHT: A new block cipher suitable for low-resource device," Lecture Notes in Computer Science, Vol.4249, pp.46-59, Oct. 2006.

[4] M. Feldhofer, J. Wolkerstorfer, and V. Rijmen, "AES implementation on grain of sand," IEE Proceedings on Information Security, Vol.152, No.1, pp.13-20, June 2005.

[5] A. Satoh, "A compact rijndael hardware architecture with S-Box optimization," Lecture Notes in Computer Science, Vol. 2248, No.1,

pp.46-59, Jan. 2001.

[6] 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, 2004.

[7] EPCglobal IncTM, "EPCTM Radio -Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860MHz-960MHz," Version 1.0.9 , Jan. 2005.

저 자 소 개

이 상 진(Sang-Jin Lee) 준회원

- 2008년 2월 : 충북대학교 화학공학과 (공학사)
- 2008년 3월 ~ 현재 : 충북대학교 정보통신공학과 석사과정

<관심분야> : 암호, 디지털 시스템 설계

박 경 창(Kyung-Chang Park) 준회원

- 2008년 2월 : 충북대학교 전자 공학과 (공학사)
- 2008년 3월 ~ 현재 : 충북대학교 정보통신 공학과 석사 과정

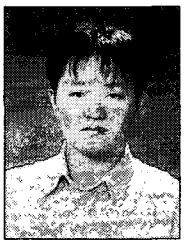
<관심분야> : 암호, 디지털 시스템 설계

김 한 벼 리(Hanbyeori Kim) 준회원

- 2008년 2월 : 충북대학교 전자 공학과 (공학사)
- 2008년 3월 ~ 현재 : 충북대학교 정보통신 공학과 석사 과정

<관심분야> : 암호, 디지털 시스템 설계

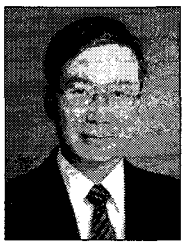
김 승 열(Seung-Youl Kim) 정회원



- 2002년 2월 : 충북대학교 정보통신공학과 (공학사)
- 2004년 8월 : 충북대학교 정보통신 공학과 (공학석사)
- 2005년 3월 ~ 현재 : 충북대학교 정보통신 공학과 박사과정

<관심분야> : 암호, 디지털 시스템 설계, ASIC 설계

유 영 갑(Younggap You) 정회원



- 1975년 8월 : 서강대학교 전자공학과 (공학사)
- 1975년 ~ 1979년 : 국방과학연구소 연구원
- 1981년 8월 : Univ. of Michigan, Ann Arbor 전기전산학과(공학석사)
- 1986년 4월 : Univ. of Michigan, Ann Arbor 전기전산학과(공학 박사)
- 1986년 ~ 1988년 : 금성반도체(주) 책임 연구원
- 1993년 ~ 1994년 : 아리조나 대학교 객원 교수
- 2000년 ~ 2001년 : 오레곤 주립대학교 교환교수
- 2007년 ~ 2008년 : 일리노이 주립대 객원 역구원
- 1988년 ~ 현재 : 충북대학교 정보통신공학과 교수

<관심분야> : VLSI 설계 및 Test, 고속 인쇄회로 설계, Cryptography