사물인터넷 보안용 경량 블록암호 알고리듬 HIGHT의 효율적인 하드웨어 구현

배기철* · 신경욱**

*국립금오공과대학교

An Efficient Implementation of Lightweight Block Cipher Algorithm HIGHT for IoT Security

Gi-Chur Bae* · Kyung-Wook Shin**

*Kumoh National Institute of Technology

E-mail : bae921216@kumoh.ac.kr

요 약

한국기술표준원(KATS)과 국제표준화기구(ISO/IEC)에 의해 표준으로 채택된 경량 블록암호 알고리듬 HIGHT용 저면적/저전력 암호/복호 코어를 설계하였다. IoT(Internet of Things) 보안에 적합하도록 개발된 경량 블록암호 알고리듬 HIGHT는 128비트의 마스터 키를 사용하여 64비트의 평문을 64비트의 암호문으로, 또는 그 역으로 변환한다. 저면적과 저전력 구현을 위해 data path를 32 비트로 축소하여 설계하였으며, 암호화 및 복호화를 위한 라운드 변환 블록과 키 스케줄러의 하드웨어 자원이 공유되도록 설계를 최적화하였다.

ABSTRACT

This paper describes a design of area-efficient/low-power cryptographic processor for lightweight block cipher algorithm HIGHT which was approved as a cryptographic standard by KATS and ISO/IEC. The HIGHT algorithm which is suitable for the security of IoT(Internet of Things), encrypts a 64-bit plain text with a 128-bit cipher key to make a 64-bit cipher text, and vice versa. For area-efficient and low-power implementation, we adopt 32-bit data path and optimize round transform block and key scheduler to share hardware resources for encryption and decryption.

키워드

HIGHT, Cryptography, Internet of Thins, Lightweight Block Cipher, Security

Ⅰ. 서 론

오늘날 사물 인터넷 혹은 지능형 전자기기 네트워크라고 불리는 새로운 컴퓨팅 환경에서는 많은 수의 IT 기기들이 인터넷에 연결되어 있다. IT 기기들은 네트워크를 통해 서로 상호작용을 하며 우리에게 새로운 경험을 제공한다. 이런 새로운 경험을 즐기기 위해서는, end 노드의 보안이 중요하다. 만약에 노드들 중 하나가 보안공격에 뚫린다면, 네트워크는 심각하게 피해를 입을 것이다. 하지만 IT 기기들에 충분한 암호화 기능을 구현하는 것은 쉽지가 않다. 왜냐하면 IT 기기들이 가지고 있는 자원의 제약 때문이다.[1]

이와 같은 조건에 맞추어 암호연산에 필요한 하드웨어 자원과 전력소비가 최소화되도록 순수 국내기술로 개발된 초경량 블록암호 알고리듬 HIGHT (HIGh security and light weigHT)가 2006년 12월에 국내 표준으로 제정되었으며, 2010년 6월에 국제표준화기구의 최종 승인을 거쳐 국제표준으로 채택되었다.[2]

본 논문에서는 IoT 환경에 적합하도록 초경량 HIGHT 블록암호 코어를 설계하고 기능을 검증하였다. 저면적과 저전력 구현을 위해 data path를 32비트로 축소하여 설계하였으며, 암호화와 복호화를 위한 라운드 변환 블록과 키 스케줄러의 하드웨어 자원이 공유되도록 최적화하였다.

II. HIGHT 블록암호 알고리듬

HIGHT는 64비트의 평문(암호문) 블록을 128비트의 마스터 키로 암호화(복호화)하여 64 비트의 암호문(평문)을 생성하는 대칭키 방식의 블록암호 알고리듬 이다. 변형된 Feistel 구조를 기반으로 총 34라운드의 연산을 통해 암호화(복호화)가 이루어지며, 128비트의 마스터 키로부터 생성되는 서브키가 라운드 변환에 사용된다. 라운드 변환과 서브키 생성은 바이트 단위의 mod-2^8덧셈과 순환이동(cyclic shift), mod-2 덧셈 등의 단순한 연산만으로 구현되어 IoT 보안용으로 적합한 작은 하드웨어와 저전력 구현이 가능하다는 특징을 갖는다.[3]

HIGHT 알고리듬의 구조는 그림 1과 같으며, 초기변환, 32회의 라운드 변환, 최종변환의 총 34회 라운드 변환으로 구성되며, 초기변환과 최종변환은 순환이동 없이 화이트닝 키 가산만으로 이루어진다. 암호화 과정과 복호화 과정은 역순으로 이루어지며, 암호화 과정의 모듈로 덧셈은 복호화 과정에서 모듈로 뺄셈으로 구현되고, 순환이동 방향도 반대로 이루어진다.[4]

III. HIGHT32 코어의 라운드 변환 블록

라운드 변환 블록은 그림 2와 같이 구성되며, 64비트의 평문(암호문) 입력과 32비트의 라운드 서브키를 받아 초기변환, R1~R32, 그리고 최종변환으로 구성되는 34번의 라운드 변환을 반복적으로 처리하여 암호(복호)연산을 수행한다. 하드웨어 효율적인 코어를 설계하기 위하여 암호화와 복호화 연산의 하드웨어 공유가 최대화되도록 회로를 설계하였다.

기존에 라운드 변환 블록과 키 스케줄러의 하드웨어가 공유된 코어에서 data path를 32비트로 줄임으로써 라운드 변환 블록의 하드웨어와 중간 값을 저장하는 레지스터의 비트 수를 절반으로

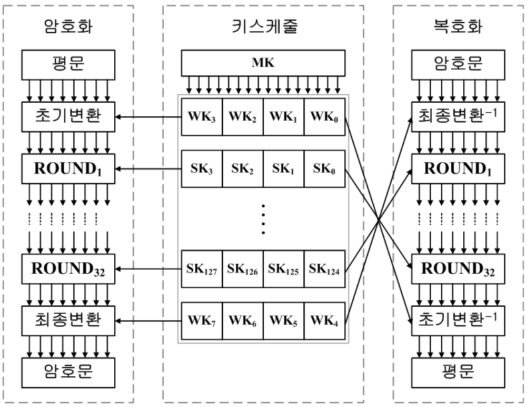

그림 1. Hight 블록암호 알고리듬
Fig. 1. Hight block cipher algorithm

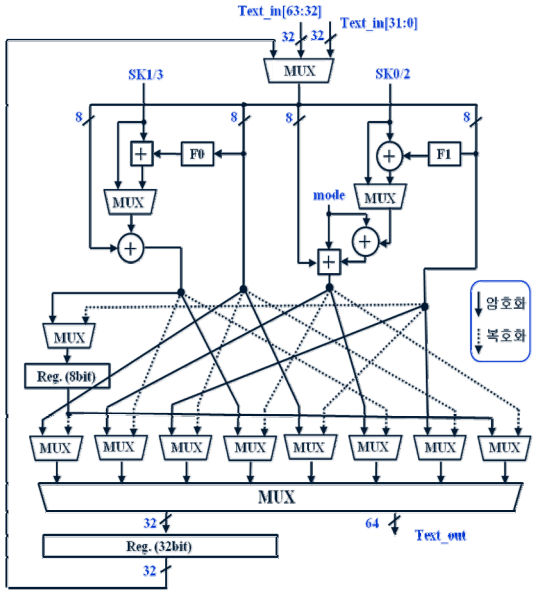

그림 2. Hight32 블록암 코어의 라운드 블록
Fig. 2. Round block of Hight32 block ciphre core

줄였다. 그러나 알고리듬의 특성상 순환 이동으로 인하여 32비트 단위로 변환된 값 중 일부(8비트)가 다른 32비트가 변환되기 이전에 저장이 된다면 이로 인하여 값이 변하게 되어 뒤에 변환되는 32비트가 잘못된 값을 가지게 된다. 본 논문의 설계에서는 8비트 레지스터를 추가함으로써 이와 같은 문제가 발생되지 않도록 하였다.

IV. 기능검증 및 FPGA 검증

Verilog HDL로 설계된 HIGHT32 코어의 기능검증 결과는 그림 3과 같으며, 64비트의 평문 "0011223344556677"와 128비트의 암호키 "ffeeddccbbaa99887766554433221100"을 입력으로 사용하였다. 그림 3에서 암호화의 결과로 64비트의 암호문 "23ce9f72e543e6d8"이 출력되고, 이를 다시 복호한 결과는 암호화 과정에서 입력으로 사용된 평문 "0011223344556677"이 출력됨을 확인함으로써 논리기능이 정상적으로 동작함을 확인하였다.

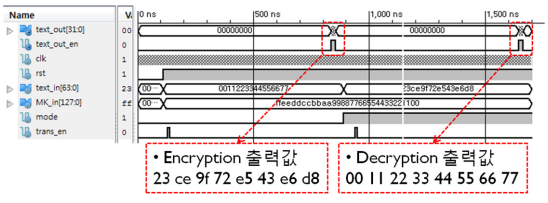

그림 3. Hight32 블록암호 코어의 기능검증 결과
Fig. 3. Simulation result of Hight32 block cipher core

Ⅴ. 결 론

국제표준화기구에 의해 국제표준으로 승인된 64비트 블록암호 알고리듬 HIGHT를 32비트의 하드웨어로 구현하여 동작을 확인하였다. 저면적과 저전력 구현을 위해 data path를 32비트로 축소하여 설계하였으며, 암호화 및 복호화를 위한 라운드 변환 블록과 키 스케줄러의 하드웨어 자원이 공유되도록 설계를 최적화하였다. 그 결과 초경량으로 구현되었으며, IoT, 무선인식 전자태그(RFID), 스마트카드 등과 같이 저전력, 경량화가 요구되는 응용분야의 정보보호 코어로 활용이 가능하다.

감사의 글

※ 반도체설계교육센터(IDEC)의 CAD Tool 지원에 감사드립니다.

참고문헌

[1] M. Katagi and S. Moriai, "Lightweight Cryptography for the Internet of Things", sony corporation, 2011. 3
[2] hight 블록암호 알고리즘 사양 및 세부명세, 한국인터넷진흥원, 2009. 7
[3] Woo Kwon Koo and Hwaseong Lee and Yong Ho Kim and Dong hoon Lee , "Implementation and Analysis of New Lightweight Crypptographic Algorithm Suitable for Wireless Sensor Networks"
[4] 박해원과 신경욱 , “64비트 블록암호 알고리듬 hight의 효율적인 하드웨어 구현”