경량 블록암호 TWINE의 하드웨어 구현

최준영 · 엄홍준 · 장현수 · 신경욱

금오공과대학교

A Hardware Implementation of lightweight block cipher TWINE

Jun-Yeong Choe · Hong-Jun Eom · Hyun-Soo Jang · Kyung-Wook Shin

Kumoh National Institute of Technology

E-mail: wnsdud6679@kumoh.ac.kr

요 약

본 논문에서는 경량 블록암호 알고리듬 TWINE의 하드웨어 설계에 대해 기술한다. TWINE은 80-비트 또는 128-비트의 마스터키를 사용하여 64-비트의 평문(암호문)을 암호(복호)하여 64-비트의 암호문(평문)을 만드는 대칭키 블록암호이며, s-box와 XOR만 사용하므로 경량 하드웨어 구현에 적합하다는 특징을 갖는다. 암호화 연산과 복호화 연산의 하드웨어 공유를 통해 게이트 수가 최소화 되도록 구현하였으며, 설계된 TWINE 크립토 코어는 RTL 시뮬레이션을 통해 기능을 검증하였다.

키워드

TWINE, Symmetric-key cryptosystem, Lightweight block cipher, Information security

I. 서 론

최근 IoT (Internet of Things) 기술의 응용분야가 급속히 확대됨에 따라 정보보안의 중요성이 강조되고 있으며, 제한된 자원을 갖는 IoT 분야의 특성상 경량/저전력 암호 프로세서가 IoT 보안의 핵심 기술로 인식되고 있다. 정보보안 기술은 대칭키 암호, 공개키 암호, 해시 함수 등을 기반으로 정보의 기밀성, 인증, 무결성 검증 등의 보안 서비스를 포함하며, IoT 환경에서의 보안 위협에 대응하기 위한 경량 정보보안 기술들이 지속적으로 개발되고 있다.[1] 대칭키 암호는 암호화와 복호화에 동일한 키를 사용하는 방식이며, 정보를 정해진 길이로 분할하여 블록단위로 암호화하는 블록암호 방식이 가장 널리 사용된다. 대표적인 경량 블록암호 알고리듬으로는 PRINCE, SIMON, SPECK, TWINE 등이 있다. TWINE [2] 블록암호는 IoT, 무선센서 네트워크 (WSN) 등의 보안에 적합하도록 경량화에 초점을 맞추어 개발되었으며, 기존의 블록암호 알고리듬과 유사한 보안강도를 가지며, 로우엔드 하드웨어부터 하이엔드 하드웨어까지 다양한 하드웨어를 구현할 수 있도록 만들어졌다.

TWINE 블록암호를 하드웨어로 설계하고 RTL 시뮬레이션을 통해 기능검증을 하였다. 설계된 TWINE 코어는 80-비트와 128-비트의 마스터키를 지원하며, on-the-fly 방식의 키 스케쥴러를 포함하여 연속적인 암호/복호화 동작이 가능하다.

II. 경량 블록암호 TWINE 알고리듬 [2]

2012년 일본 NEC사에서 개발된 대칭키 암호 TWINE은 80-비트와 128-비트의 키 길이를 지원하며 블록 크기가 64-비트인 경량 블록암호 알고리듬이다. S-box와 XOR만을 사용하므로 다른 암호 알고리듬 보다 경량 하드웨어 구현에 적합하다는 특징을 갖는다. 암호화 과정에서 키 스케줄은 80-비트 또는 128-비트의 마스터 키를 입력받아 연산한 후, 행 치환 과정을 거친 최종 화이트 키로부터 라운드 키를 만들어낸다. 이때 최초 라운드 키는 연산과정과 행 치환 과정을 거치지 않은 마스터 키로부터 생성하게 되며, 나머지 라운드 키는 앞서 설명한 과정을 거쳐 생성된다.

데이터 프로세싱에서는 평문을 최대 64-비트까지 입력받아 36번의 라운드 변환을 거쳐 암호화를 진행하게 된다. 먼저 S-box와 라운드 키를 이용하여 행의 홀수 번째 자리들을 연산한 후, 36번째 라운드를 제외한 모든 라운드에서 Π-치환 테이블을 이용하여 행 연산을 실행한다. 복호화 과정은 키 스케줄에서의 키 연산과정과 행 치환과정을 역으로 진행하여 생성된 라운드 키를 이용하고, 데이터 프로세싱에서는 역 Π-치환 테이블을 이용하는 것 외에는 암호화 과정과 동일한 과정을 거친다. 마지막 라운드에서 나온 암호화된 데이터를 암호문으로 출력하며, 이 일련의 과정에서의 모든 연산은 4-비트를 한 단위로 진행된다.

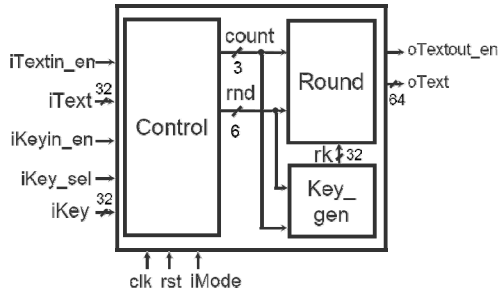
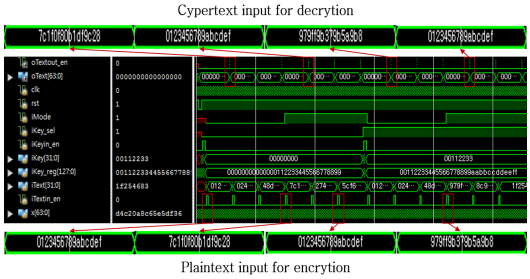


Fig. 1. Block diagram of TWINE.

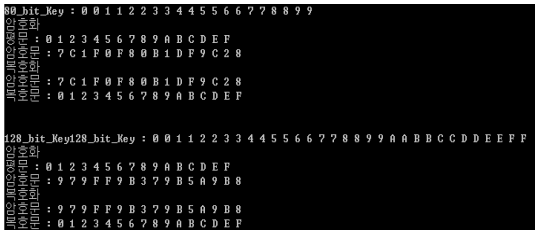
III. TWINE 경량 블록암호 프로세서 설계

TWINE 대칭키 암호 프로세서의 내부 구조는 그림 1과 같으며, Round 블록, Key_gen 블록, Control 블록으로 구성된다. key_gen 블록에서는 Round 블록에서 사용될 라운드 키를 생성하며 iKey_sel 신호와 iMode 신호에 따라 키 길이, 암·복호화 모드가 결정된다. TWINE 알고리듬에서의 라운드 키 생성과정은 연산과정을 거친 후 행 치환 과정을 거치지만, 본 논문에서는 이 두 과정을 통합하여 라운드키가 생성되도록 하였다. Round 블록은 Key_gen 블록에서 입력된 라운드 키를 사용하여 암·복호화 과정을 수행하며, Key_gen 블록과 동일하게 iMode 신호로 암·복호화 모드가 결정된다. 라운드 변환은 데이터 입력, 홀수 자리 연산, 행 연산 순서로 진행되며 암·복호화 과정에 있어서 행 연산 과정만을 별도로 실행할 뿐 두 모드의 홀수 자리 연산과정을 통합하여 저면적을 추구하였다. Control 블록에서는 32-비트의 데이터를 각 블록에 필요한 데이터의 길이에 맞추어 사용될 수 있도록 해주는 제어신호와 암·복호화 연산을 위해 라운드를 생성해주는 제어신호를 만들어낸다.

설계된 TWINE 크립토 프로세서를 Xilinx ISim을 이용한 RTL 시뮬레이션과 C언어로 구현한 소프트웨어 결과를 비교하여 논리기능을 검증하였다. 그림 2는 TWINE 크립토 프로세서의 RTL 시뮬레이션 결과값과 C언어 소프트웨어 암·복호화 결과값의 비교를 보인 것이다. 64-비트의 평문 “0123 4567 89ab cdef”를 80-비트 마스터 키 “0011 2233 4455 6677 8899”로 암호화한 결과로 “7c1f 0f80 b1df 9c28”의 암호문이 출력되었으며, 동일한 평문을 128-비트의 마스터 키 “0011 2233 4455 6677 8899 aabb ccdd eeff”로 암호화한 결과로 “979f f9b3 79b5 a9b8”의 암호문으로 출력되는 것을 확인할 수 있다. 복호화 과정의 경우, 암호화를 통해 얻어진 암호문 “7c1f 0f80 b1df 9c28”와 “979f f9b3 79b5 a9b8”를 복호화한 결과로, 암호화 과정에 사용된 평문과 동일한 “0123 4567 89ab cdef”가 출력되는 것을 확인할 수 있으며, 따라서 설계된 TWINE 크립토 프로세서의 논리기능이 올바로 동작함을 확인하였다.



(a)



(b)

Fig. 2. Simulation results of TWINE processor (a) simulation result (b) software result.

IV. 결 론

경량 블록암호 TWINE 알고리듬을 하드웨어로 구현하고 기능을 검증하였다. Xilinx Spartan6 XC6SLX45 FPGA 디바이스로 합성결과, 164 슬라이스로 구현되었다. 본 논문의 TWINE 대칭키 암호 프로세서는 경량화 구현을 우선시 하였으므로, IoT와 같이 저전력 및 경량화가 필요한 분야의 보안에 활용될 수 있다.

ACKNOWLEDGMENT

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education (No. 2017R1D1A3B03031677)

참고문헌

[1] Cryptographic Technology Guideline (Lightweight Cryptography), CRYPTREC Lightweight Cryptography Working Group, National Institute of Information and Communication Technology, Jun. 2017.

[2] S. Tomoyasu, M. Kazuhiko, M. Sumio, and K. Eita, “TWINE: A Lightweight Block Cipher for Multiple Platforms,” Selected Areas in Cryptography: 19th International Conference, SAC 2012, Windsor, Aug. 2012.