Cortex-M0 기반의 보안 SoC 프로토타입 설계

최준백 · 최준영 · 신경욱

금오공과대학교

A Design of Security SoC Prototype Based on Cortex-M0

Jun-baek Choi · Jun-yeong Choe · Kyung-wook Shin

Kumoh National Institute of Technology

E-mail : chlwnsor@kumoh.ac.kr

요 약

마이크로프로세서에 블록암호 크립토 코어를 인터페이스한 보안 SoC (System-on-Chip) 프로토타입 구현에 대해 기술한다. 마이크로프로세서로 Cortex-M0를 사용하였고, ARIA와 AES를 단일 하드웨어에 통합하여 구현한 크립토 코어가 IP로 사용되었다. 통합 ARIA-AES 크립토 코어는 ECB, CBC, CFB, CTR, OFB의 5가지 운영모드와 128-비트, 256-비트의 두 가지 마스터키 길이를 지원한다. 통합 ARIA-AES 크립토 코어를 Cortex-M0의 AHB-light 버스 프로토콜에 맞게 동작하도록 인터페이스 하였으며, 보안 SoC 프로토타입은 BFM 시뮬레이션 검증 후, FPGA 디바이스에 구현하여 하드웨어-소프트웨어 통합 검증을 하였다.

ABSTRACT

This paper describes an implementation of a security SoC (System-on-Chip) prototype that interfaces a microprocessor with a block cipher crypto-core. The Cortex-M0 was used as a microprocessor, and a crypto-core implemented by integrating ARIA and AES into a single hardware was used as an intellectual property (IP). The integrated ARIA-AES crypto-core supports five modes of operation including ECB, CBC, CFB, CTR and OFB, and two master key sizes of 128-bit and 256-bit. The integrated ARIA-AES crypto-core was interfaced to work with the AHB-light bus protocol of Cortex-M0, and the crypto-core IP was expected to operate at clock frequencies up to 50 MHz. The security SoC prototype was verified by BFM simulation, and then hardware-software co-verification was carried out with FPGA implementation.

키워드

보안 SoC, 암호 프로세서, ARIA, AES, Cortex-M0, AHB 프로토콜

Key word

Security SoC, cryptographic processor, ARIA, AES, Cortex-M0, AHB protocol

Ⅰ. 서 론

반도체 제조공정의 미세화에 의해 단일 칩에 집적되는 소자 수가 크게 증가하고 있으며, CPU와 반도체 설계자산 (intellectual property; IP)을 단일 칩에 집적시킨 시스템-온-칩 (System-on-Chip; SoC) 기술이 보편화되고 있다. 정보보안 응용분야에서도 기존에 소프트웨어 또는 전용 하드웨어로 구현되던 다양한 보안 알고리듬들을 SoC 형태로 구현하는 추세가 가속화되고 있다. 최근에는 사물인터넷 (internet of things; IoT), 무선센서 네트워크, 자율주행 자동차 등 강력한 보안성능과 함께 다양한 보안 프로토콜을 구현해야 하는 응용분야가 확대됨에 따라 보안 SoC의 중요성이 증가하고 있으며, 다양한 보안 SoC들이 개발되고 있다 [1].

본 논문에서는 Cortex-M0 기반의 보안 SoC 프로토타입 설계에 관해 기술한다. 블록암호 국제표준인 AES [2]와 우리나라 표준인 ARIA [3]를 단일 하드웨어로 통합 구현한 UAAP (Unified ARIA-AES Processor) [4]를 슬레이브 IP로 이용하였으며, 설계된 보안 SoC를 FPGA에 구현하고 하드웨어-소프트웨어 통합검증을 통해 정상동작을 확인하였다.

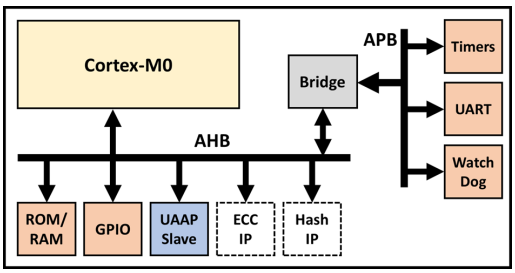


Fig. 1. Architecture of security SoC

II. AES[2], ARIA[3] 알고리듬

AES 알고리듬은 2001년 NIST (National Institute of Standard and Technology)에서 표준으로 제정된 대칭키 블록암호이며, 128 비트의 평문(암호문)을 입력받아 128 비트의 암호문(복호문)을 출력한다. 128, 192, 256 비트의 세 가지 마스터키 길이를 지원하며, 키길이에 따라 10, 12, 14회의 라운드 변환을 수행한다. 라운드 변환은 SubByte, ShiftRows, MixColumn 연산으로 구성되고, 복호화에는 각각의 역변환인 InvSubByte, InvShiftRows, InvMixColumn이 사용된다.

ARIA 알고리듬은 NSRI 주도로 개발된 블록 암호 알고리듬으로 128 비트의 평문(암호문)을 입력받아 128 비트의 암호문(복호문)을 출력하는 대칭키 블록암호이다. AES와 동일하게 128, 192, 256 비트의 마스터키 길이를 지원하며, 키길이에 따라 12, 14, 16회의 라운드 변환이 진행된다. ISPN (Involution substitution and permutation network) 구조를 기반으로 하므로, 암호화와 복호화 연산이 라운드 키만 다르고, 그 과정은 동일하다. 라운드는 AddRoundKey, Substitution, Diffusion의 함수로 연산이 진행되고, 홀수와 짝수 라운드에는 다른 치환 계층이 사용되며, 최종 라운드는 확산계층이 라운드 키 가산으로 대체된다.

III. 보안 SoC 프로토타입 설계

ARIA와 AES를 단일 하드웨어로 통합하여 설계된 UAAP [4] IP를 그림 1과 같이 Cortex-M0에 슬레이브로 인터페이스하여 보안 SoC 프로토타입을 구현하였다. UAAP_Slave는 AHB 프로토콜을 통해

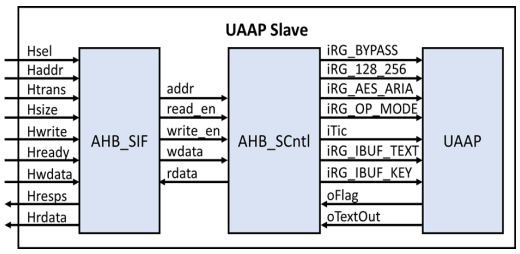


Fig. 2. UAAP_Slave module

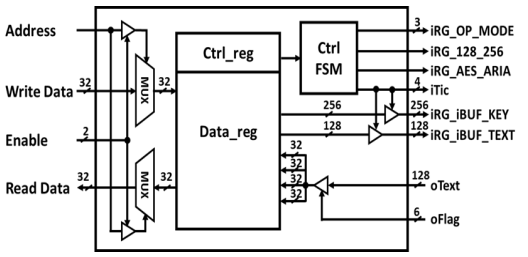


Fig. 3. AHB_Cntl module

Cortex-M0와 데이터를 송수신하며, 그림 2와 같이 AHB_SIF 모듈, AHB_SCntl 모듈, UAAP 코어 IP로 구성된다. AHB_SIF 모듈은 AHB 프로토콜을 통해 들어오는 데이터를 분석해 AHB_SCntl 모듈에 필요한 데이터를 전송하는 역할을 한다. AHB_SCntl 모듈은 전송받은 데이터를 UAAP IP에 맞게 변환시켜 전송하고, IP의 출력데이터를 AHB 프로토콜로 전송, 메모리에 저장하는 기능을 수행한다.

AHB_SCntl 모듈의 내부 구조는 그림 3과 같이 Data_reg와 Ctrl_FSM으로 구성된다. Data_reg는 전송받은 키, 평문/암호문 데이터, 그리고 IP로부터 출력된 암호문/복호문 데이터 임시 저장하며, Ctrl_FSM은 Cortex-M0로부터 들어온 데이터를 분석하여 IP의 동작모드와 데이터 송수신 과정을 제어한다. UAAP IP는 AES와 ARIA의 알고리듬이 공통된 연산과정과 동일한 키길이와 블록길이를 갖는 특성을 이용하여 단일 하드웨어 구조에 통합 구현한 IP이다. UAAP 크립토 코어는 ECB, CBC, OFB, CFB, CTR의 5가지의 운영모드와 128 비트, 256 비트의 키길이를 지원한다.

IV. BFM simulation 및 FPGA 검증

설계된 UAAP_Slave를 Cortex-M0와 연결하였을 때 AHB 프로토콜에서 정상동작 하는지 확인하기 위해 BFM (Bus Function Model) 시뮬레이션을 통해 기능검증을 수행하였으며, BFM 시뮬레이션 결과는 그림 4와 같다. 128 비트의 키 "2b7e_1516_28ae_d2a6_abf7_1588_09cf_4f3c"로 평문 "6bc1_bee2_2e40_9f96_e93d_7e11_7393_172a"을 AES ECB 운영모드로 암호화한 결과로 암호문 "3ad7_7bb4_0d7a_3660_a89e_caf3_2466_ef97"이 출력되었다. 또

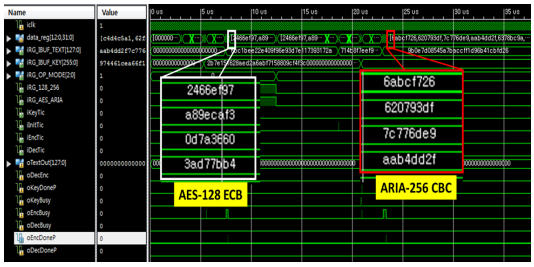
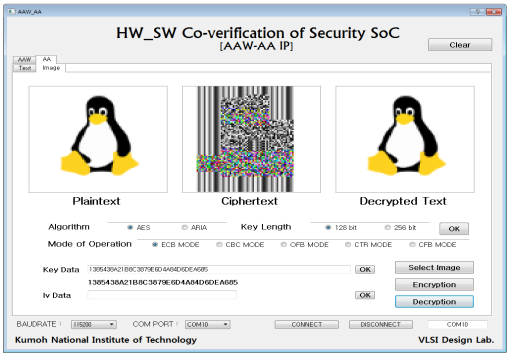
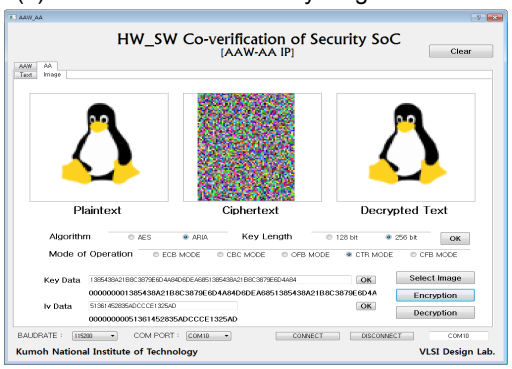


Fig. 4. BFM simulation results



(a) AES-ECB mode with key length of 128-bit



(b) ARIA-CTR mode with key length of 256-bit

Fig. 5. FPGA verification results

한, 256 비트 키 길이를 갖는 ARIA의 CBC 운영모드로 암호화 동작한 것으로 키 “9744_61ce_a66f_1554_723a_6977_ed5c_8bbc_5b9b_734c_1088_c649_7b6a_fb5e_6378_bc9a”와 초기화 벡터 “714b_8f7e_ef92_b554_cf08_52c3_efa3_cfa1”로 평문 “9b0e_7d08_545a_7bac_cff1_d96b_41cb_fd26”를 암호화한 결과로 암호문 “aab4_dd2f_7c77_6de9_6207_93df_6abc_f726”이 출력되어 올바로 동작함을 확인하였다.

설계된 보안 SoC 프로토타입을 FPGA에 구현하고 하드웨어-소프트웨어 통합 검증을 수행하였다. Cyclone-V 소자가 탑재된 V2M-MPS2 보드를 이용하였으며, PC와 UART 통신을 통해 동작을 확인하였다. UAAP_Slave를 Cortex-M0 시스템과 합성하기 위해 Quartus Prime을 이용하였고, Keil uVision을 사용하여 Cortex-M0의 동작 제어를 위한 소프트웨어를 크로스컴파일 하였다. 그림 5는 FPGA에 구현된 보안 SoC의 동작 결과를 보인 GUI 화면 캡처이다. 그림 5-(a)는 128비트 키길이의 AES ECB 운영모드 동작에 대한 검증 결과이며, 화면의 좌측 이미지를 암호화한 결과로 화면 중앙의 암호화된 이미지가 출력되며, 이를 다시 복호화한 결과로 화면 우측의 이미지가 출력되었다. 그림 5-(b)는 256 비트 키길이의 ARIA CTR 운영모드 동작에 대한 검증 결과이다. 원본 이미지와 복호화된 이미지가 일치함을 통해 FPGA에 구현된 보안 SoC가 정상 동작함을 확인하였다.

V. 결 론

대표적인 블록암호 중 AES, ARIA를 단일 하드웨어 구조로 설계한 UAAP를 Cortex-M0에 슬레이브 인터페이스시켜 AHB 프로토콜과 결합하여 보안 SoC 프로토타입를 설계하였다. BFM 시뮬레이션과 FPGA 구현을 통해 설계된 SoC 프로토타입이 정상 동작함을 확인하였다. 50 MHz 동작주파수에서 AHB 인터페이스의 데이터 전송에 소요되는 사이클을 포함한 암호화/복호화 연산 처리율은 AES-128, AES-256의 경우 각각 101Mbps, 85.3Mbps이고, ARIA-128, ARIA- 256의 경우 각각 110Mbps, 97Mbps로 예측되었다. 본 논문에서 설계된 보안 SoC 프로토타입에 해시 함수, 공개키 암호 ECC, 난수발생기 (TRGN) IP 등을 추가하면 다양한 분야에 응용될 수 있는 보안 SoC를 구현할 수 있다.

Acknowledgement

This work was supported by KIAT(Korea Institute for Advancement of Technology) grant funded by the Korea Government(MOTIE : Ministry of Trade, Industry and Energy) (No.N0001883, HRD Program for Intelligent semiconductor Industry). 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).

References

[1] A. P. Deb Nath, S. Ray, A. Basak and S. Bhunia, "System-on-chip security architecture and CAD framework for hardware patch," *2018 23rd Asia and South Pacific Design Automation Conference (ASP-DAC)*, Jeju, pp. 733-738, 2018.

[2] FIPS-197, Advanced Encryption Standard, National Institute of Standard and Technology(NIST), Nov., 2001.

[3] KS X 1213:2004, 128 bit Block Encryption Algorithm ARIA, Korean Agency for Technology and Standards (KATS), 2004.

[4] K.B. Ki and K.W Shin, “A Unified ARIA-AES Cryptofraphic Processor Supporting Four Mode of Operation and 129/256-bit Key Lengths”, *Journal of the Korea Institute of Information and Communication Engineering*, vol. 21, no. 4, pp. 795-803, Apr. 2017