65nm CMOS 공정을 이용한 HMAC-PHOTON80 기반 경량 개체 인증 SoC

오치충, 백승범, 홍종필

충북대학교 전기공학부

trung@cbnu.ac.kr, sbbaek@cbnu.ac.kr, jphong@cbnu.ac.kr

A compact entity authentication SoC based on HMAC-PHOTON80 using 65nm CMOS process

Chi Trung Ngo, Seungbum Baek, Jong-Phil Hong

School of Electrical Engineering, Chungbuk National University

요 약

This paper introduces a compact system on chip (SoC) for entity authentication based on HMAC-PHOTON80 as a lightweight security solution for resource constrained internet of things (IoT) devices. The proposed SoC is fabricated using 65nm CMOS process, occupies 0.1575mm^2 with power consumption of 2.46mW and throughput of 1.4Mbps with maximum measured frequency of 125MHz.

Ⅰ. 서 론

Blooming of IoT era has been improving and optimizing our daily life based on a large number of IoT devices and their rich functions. In IoT systems, heterogeneous devices are connected to a network to collect a huge amount of information. However, data transmission over the air comes with heightened security and authenticity issues. To protect security critical data from unauthorized access, entity authentication among various security services is crucial to prove the identity of the user or the IoT device.

In real-world applications, various cryptography algorithms are researched to solve the authenticity issues such as AES. However, the conventional algorithms suffer from high computational complexity which increases the area occupation and power consumption. Therefore, the conventional entity authentication scheme shown in Fig. 1(a) is inefficient to be embedded in lightweight devices such as IoT devices.

This paper introduces a compact SoC implementation of the entity authentication based on HMAC-PHOTON80 which replaces the conventional heavyweight algorithms. The proposed SoC is simulated by MATLAB Simulink for behaviour-level verification, designed in a proprietary 65nm CMOS process, and finally proven by real chip measurement.

Ⅱ. 본론

Figure 1b shows the proposed entity authentication scheme with a direction of authentication from IoT device to server, for the sake of simplicity. First of all, the proposed scheme employs hash-based message authentication code (HMAC) for an authentication algorithm to replace the conventional cipher algorithm. The National Institute of Standards and Technology (NIST) standard defines HMAC as a MAC based on a cryptographic hash function with a secret key. The HMAC is implemented based on a standardized lightweight hash function (i.e., PHOTON-80) to improve area occupation and power consumption while maintaining security strength. The PHOTON is approved as a lightweight cryptography hash function by NISTIR 8114 report [1].

The proposed SoC adopts the conventional cryptographic key management. The private keys are stored in the memory and extracted when it receives the selection signal which is generated the random number generator (RNG). For a specific random number bit, an identical key is extracted. Thus, to prevent the key's duplication, the random number generator needs to satisfy the essential properties of an RNG such as repeatability and randomness. The PRNG generates a random sequence based on a mathematical algorithm with an initialization vector (IV). The random number which is generated from PRNG has an excellent statistical property [2].

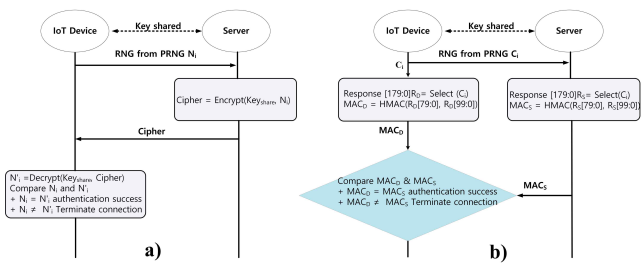

Fig. 1. Entity authentication a) conventional scheme b) proposed scheme.

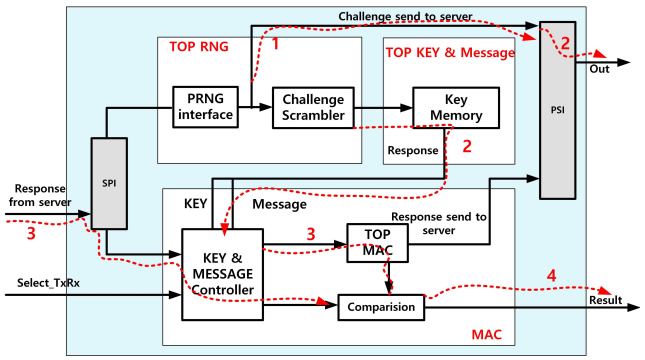

Fig. 2. Implementation of IoT device verifying server in SoC.

Figure 2 illustrates the overall architecture of the proposed entity authentication SoC with the authentication direction highlighted from the device to the server. Signal flow directions are described in detail by the simulation graph which is shown in Fig. 3. The device starts the process by generating a 128-bit input signal through the PRNG and sending it to the server. In the server side, a key is extracted for the corresponding device and random number from the database. The extracted key is used as a message and a key input for the HMAC, to avoid usage of the received random number as an input which is public information. Meanwhile, the device generates MAC using the key memory in the same manner. When the server finishes generating MAC, it is sent to the IoT device and the device verifies it by comparing it with the self-generated MAC. The comparison results determine the authentication success in terms of that the same MACs indirectly indicate the secret keys between the two parties are identical.

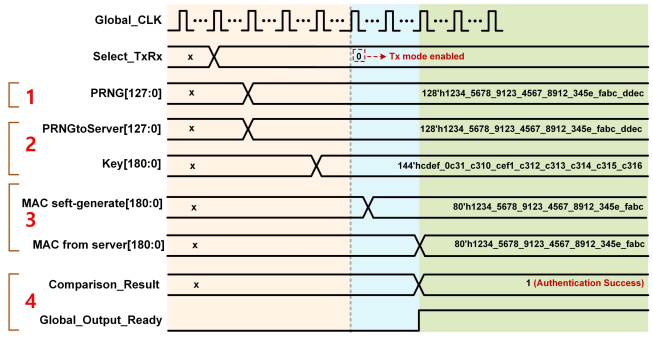

Fig. 3. Simulation graph in the case of IoT device authenticates the server.

Figure 4 shows a layout of the proposed SoC. The proposed SoC is fabricated in 65nm CMOS process and occupies $0.1575mm^2$. Table I shows the performance summary of the proposed SoC in terms of hardware perspective and security perspective. The HMAC-PHOTON in the authentication block costs only 6,233 GE (gate equivalent to basic 2-input NAND gate) and is more compact than AES [3] which costs around 23,000 GE. The throughput which is calculated by the work in [3] indicates 1.4 Mbps, which may be thought of as not high speed however, the HMAC-PHOTON is implemented in a serial way to effectively reduce the area occupation.

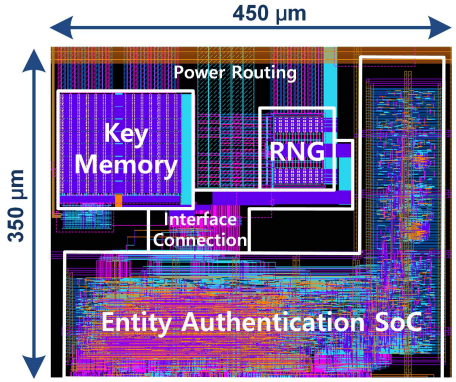

Fig. 4 Layout of the proposed entity authentication SoC.

Table I Performance summary of proposed entity authentication SoC system.

		This work
Parameter	Technology (nm)	65
	Challenge (number of bits)	128
	Response (number of bits)	80
Hardware perspective	Latency (clock cycle)	11334
	Frequency (MHz)	125
	Throughput (Mbps)	1.4
	Power(mW)	2.46
	Area MAC part (GE)	6,233
Security perspective	Entropy (bits per byte)	3.296
	Avalanche effect (%)	50.27

Ⅲ. 결론

Area occupation is one of the hardest challenges for implementing traditional entity authentication algorithms on the resource-constrained devices. The proposed system solves this problem by replacing conventional primitives with state-of-the-art lightweight hash function.

ACKNOWLEDGMENT

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. NRF-2021R1A2C2005258). This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (No. 2020R1A6A1A12047945).

참 고 문 헌

[1] K. A. McKay et al., National Institute of Standards and Technology, "Report on Lightweight Cryptography", NISTIR 8114, March 2017.

[2] NIST. Recommendation for the Entropy Sources Used for Random Bit Generation. [Online]. Available: https://csrc.nist.gov/csrc/media/publications/sp/800-90b/draft/documents/sp800-90b_second_draft.pdf

[3] Adam J. Elbirt, W. Yip, B. Chetwynd, and Christof Paar, "An FPGA Implementation and Performance Evaluation of the AES Block Cipher Candidate Algorithm Finalists", In Third AES Candidate Conference, pp. 13-7, 2000.