사물인터넷 기기를 위한 통합 보안 코어의 하드웨어 설계

Dennis A. N. Gookyi · 류광기
한밭대학교 정보통신전문대학원

The Hardware Design of Integrated Security Core for IoT Devices

Dennis A. N. Gookyi · Kwangki Ryoo
Graduate School of Information and Communication, Hanbat National University
E-mail : dennisgookyi@gmail.com, kkryoo@hanbat.ac.kr

요 약

본 논문에서는 인터넷 장치의 보안을 위해 경량 대칭 암호화와 경량 인증을 통합 한 하드웨어 아키텍처를 제안한다. 암호화 핵심은 PRESENT 알고리즘과 제안된 새로운 경량 암호화 알고리즘으로 구성된다. 또한 HB 및 HB +, HB-MP, HB-MP + 인증 알고리즘들을 포함한다. 통합 보안 시스템은 Verilog HDL을 사용하여 설계되었으며 Modelsim SE 및 Xilinx Design Suite 14.3 프로그램을 사용하여 검증 및 합성되었다. 제안하는 암호화 코어 하드웨어 구조는 Spartan6 FPGA 장치에서 합성한 결과 189Mhz 주파수와 1130개 슬라이스를 가진다.

ABSTRACT

In this paper we provide a unified crypto core that integrates lightweight symmetric cryptography and authentication. The crypto core implements a unified 128 bit key architecture of PRESENT encryption algorithm and a new lightweight encryption algorithm. The crypto core also consist of an authentication unit which neglects the use of hashing algorithms. Four algorithms are used for authentication which come from the Hopper-Blum (HB) and Hopper-Blum-Munilla-Penado (HB-MP) family of lightweight authentication algorithms: HB, HB+, HB-MP and HB-MP+. A unified architecture of these algorithms is implemented in this paper. The unified cryptosystem is designed using Verilog HDL, simulated with Modelsim SE and synthesized with Xilinx Design Suite 14.3. The crypto core synthesized to 1130 slices at 189Mhz frequency on Spartan6 FPGA device.

키워드
IoT, lightweight encryption, HB Authentication, Cryptosystem, FPGA

Ⅰ. Introduction

The lower abstraction of IoT architecture consists of low power and low cost sensing and identification electronic components like the Radio Frequency Identification (RFID) tags. these devices are constrained in a sense that they comprise of less than 512 bits of memory, consume less than 10mW of power and consist of less than 10k hardware gate count out of which less than 2k gate count is available for security purposes[1]. These constraints have led to the branch of lightweight cryptography where algorithms with simple structures and medium level security are implemented on constrained devices. The focus of this paper is the integration of lightweight encryption and authentication into a single crypto core.

A popular lightweight encryption algorithm that has been accepted as an ISO/IEC standard is the PRESENT algorithm[2]. PRESENT is a 80 or 128 bit key size, 64 bit block size and a 31 round cipher. It requires 310us to encrypt a block of data at 100KHz. A new lightweight encryption algorithm [3] is designed to reduce the encryption time. This algorithm requires 80us to encrypt a block of data at 100KHz.

Lightweight authentication algorithms consists of components such as pseudorandom number generators (PRNG) and cyclic redundancy check (CRC). This paper provides the unified architecture of four Hopper-Blum (HB) and Hopper-Blum-Munilla-Penado (HB-MP) Family of lightweight authentication protocols: HB, HB+, HB-MP and HB-MP+[1]. The unified crypto core is shown in Figure 1.

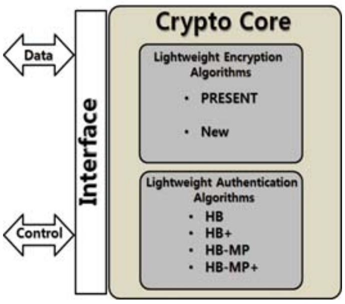
Crypto Core
Lightweight Encryption Algorithms
• PRESENT
• New
Lightweight Authentication Algorithms
• HB
• HB+
• HB-MP
• HB-MP+
Interface
Data
Control

Fig. 1. A Unified Crypto Core

Ⅱ. Crypto Core Algorithms

The unified crypto core is shown in Figure 1. It consist of lightweight encryption algorithms and lightweight authentication algorithms.

```
Inputs: key[127:0], plaintext[63:0]
Outputs: state[63:0], {state131:0], state2[31:0]}
Algorithm 1: PRESENT Algorithm
generateRoundKeys(key)
for i = 1 to 31 do
   state = addRoundKey(state,keyi)
   state = sBoxLayer(state)
   state = pLayer(state)
end for
addRoundKey(state, key32)
Algorithm 2: New Algorithm
generateRoundKeys(key)
for i = 1 to 8 do
   //stage 1
   state1 = addRoundKey(state1, keyi)
   state1 = sBoxLayer(state)
   state1 = pLayer(state, keyi)
   state1 = addRoundKey(state1, keyi)
   //stage 2
   state2 = addRoundKey(state1, keyi)
   state2 = sBoxLayer(state2)
   state2 = pLayer(state2, keyi)
   state2 = addRoundKey(state2, keyi)
end for
```

Fig. 2. Lightweight Encryption Flow

Lightweight encryption Algorithms: This consist of PRESENT which is a 31 round Substitution-Permutation (S-P) structure cipher and a New algorithm which is a 8 round Feistel structure cipher. Both algorithms consist of 128 bit key and 64 bit block. The encryption algorithm flow for PRESENT and the New cipher is shown in Figure 2.

```
Input: $x = \{0,1\}^k$, $y = \{0,1\}^k$, $ai = \{0,1\}^k$
output: $b_i = \{0,1\}^k$, $z_i$
Algorithm 3: HB Algorithm
for i = 1 to n do
   generate random noise $v_i = \{0,1\}$
   compute $z_i = x.a_i \wedge v_i$
end for
Algorithm 4: HB+ Algorithm
for i = 1 to n do
   generate random number $b_i$
   generate random noise $v_i = \{0,1\}$
   compute $z_i = (x.a_i) \wedge (y.b_i) \wedge v_i$
end for
Algorithm 5: HB-MP Algorithm
for i = 1 to n do
   generate random noise $v_i = \{0,1\}$
   generate round key $x_i = rot(x,y_i)$
   compute $z_i = (x.a_i) \wedge (y.b_i) \wedge v_i$
   generate $b_i$ such that $b_i.x_i = z_i$
end for
Algorithm 6: HB-MP+ Algorithm
for i = 1 to n do
   generate random noise $v_i = \{0,1\}$
   generate round key $x_i = f(a_i,x)$
   compute $z_i = (x.a_i) \wedge (y.b_i) \wedge v_i$
   generate $b_i$ such that $b_i.x_i = z_i$
end for
```

Fig. 3. Lightweight Authentication Flow

Lightweight Authentication: The crypto core consist of HB, HB+, HB-MP and HB-MP+ authentication algorithms. The algorithms flow is shown in Figure 3 where (.) is dot product and (^) is an XOR gate.

Ⅲ. Proposed Hardware Architecture

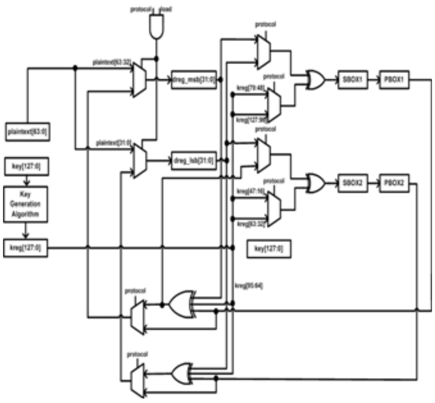

Fig. 4. A Unified Encryption Architecture

Figure 4 shows the proposed hardware architecture datapath for the unified lightweight ciphers. The input consist of the plaintext and key while the output is the ciphertext which concatenates two 32 bit registers dreg_msb and dreg_lsb. Multiplexers are used to route the data based on the selection signal protocol.

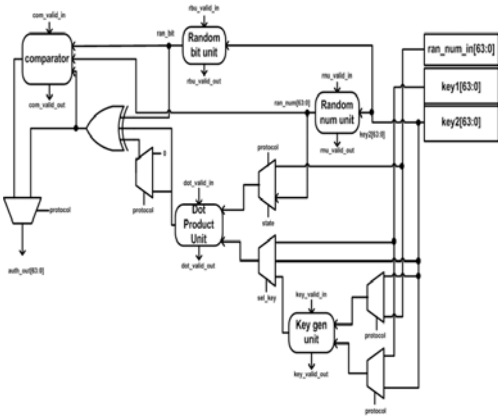

Fig. 5. Unified Authentication Architecture

Figure 5 shows the proposed hardware architecture datapath for the unified lightweight authentication algorithms. The architecture consists of random bit and a random number generation unit which uses linear feedback shift registers (LFSR). The dot product unit computes the dot product of the key and the random number using AND (&) and XOR (^) gates in the equation: ^(key[63:0] & random[63:0]).

Ⅳ. Results and Discussion

The hardware architecture of the proposed crypto core was designed using Verilog HDL and was verified using FPGA. Xilinx Spartan6 was used for the purposes of synthesis and Modelsim SE-64 10.1c was used for the purposes of simulation. The synthesis results are tabulated in Table 1.

Table 1. Synthesis Results

Algorithms	Area	Max Freq.
PRESENT[2]	202 Slices	254 MHz
NEW[3]	196 Slices	337 MHz
HB[4]	77 Slices	311 MHz
HB+[4]	302 Slices	223 MHz
HB-MP[4]	430 Slices	157 MHz
HB-MP+[4]	366 Slices	160 MHz
Proposed Core	1130 Slices	189 MHz
Area Saving	443 Slices	-

Ⅴ. Conclusion

In this paper we propose the hardware architecture of an integrated crypto core that combines two lightweight encryption algorithms and four lightweight authentication algorithms. the core synthesized to 1130 slices at 189 maximum clock frequency on Spartan6 FPGA device. The core saves up to 443 slices as compared to implementing the algorithms individually.

Acknowledgments

This research was supported by the MSI(Ministry of Science, ICT and Future Planning), Korea, under the Global IT Talent support program(IITP-2017-0-01681) and Human Resource Development Project for Brain scouting program(IITP-2016-0-00352) supervised by the IITP(Institute for Information and Communication Technology Promotion)

References

[1] F. Armknect, M. Hamann, and V. Mikhalev, "Lightweight Authentication Protocols on Ultra-constrained RFIDs - Myth and Facts," LNCS, Springer-Heidelberg, Vol. 8651, pp. 1-18, Nov. 2014.

[2] M. Sbeiti, M. Silbermann, A. Poschmann, and C. Paar, "Design Space Exploration of PRESENT Implementation for FPGAs," 5th Southern Conference on Programmable Logic, pp. 141-145, Apr. 2009.

[3] D. A. N. Gookyi, S. Park, and K. Ryoo, "The Efficient Hardware Design of a New Lightweight Block Cipher," IJCA, Vol. 10, No. 1, pp. 431-440, Jan. 2017.

[4] D. A. N. Gookyi, and K. Ryoo, "Hardware Design of HB Type Lightweight Authentication Protocols for IoT Devices," International Conference on Innovation Convergence Technology, pp. 59-60, Jun. 2017.