SHA3-512 해시 함수의 최적 하드웨어 설계조건 분석

김동성 · 신경욱*

금오공과대학교

Analysis of Optimal Hardware Design Conditions for SHA3-512 Hash Function

Dong-seong Kim · Kyung-wook Shin*

Kumoh National Institute of Technology

E-mail : kdsung322@kumoh.ac.kr

요 약

본 논문에서는 Secure Hash Algorithm3-512 (SHA3-512) 해시 함수의 최적 하드웨어 설계조건을 분석하였다. SHA3-512 해시 코어를 64-비트, 320-비트, 640-비트, 960-비트 그리고 1600-비트의 5가지 데이터 패스로 설계하여 RTL 시뮬레이션을 통해 기능을 검증하였으며, Xilinx Virtex-5 FPGA 디바이스로 합성한 결과를 바탕으로 최대 동작주파수, 처리율 그리고 슬라이스 수를 비교하였다. 분석 결과로부터, SHA3-512 해시 코어를 1600-비트의 데이터 패스로 설계하는 것이 가장 우수한 성능을 갖는 것으로 확인되었다.

ABSTRACT

In this paper, the optimal design conditions for hardware implementation of the Secure Hash Algorithm3-512 (SHA3-512) hash function were analyzed. Five SHA3-512 hash cores with data-path of 64-bit, 320-bit, 640-bit, 960-bit, and 1600-bit were designed, and their functionality were verified by RTL simulation. Based on the results synthesized with Xilinx Virtex-5 FPGA device, we evaluated the performance of the SHA3-512 hash cores, including maximum frequency, throughput, and occupied slices. The analysis results show that the best hardware performance of SHA3-512 hash core can be achieved by designing it with 1600-bit data-path.

키워드

Secure Hash Algorithm3, Hash, KECCAK, Security, Integrity

Ⅰ. 서 론

정보통신 기술의 발전과 함께 다양한 형태의 보안 위협들이 증가하고 있으며, 그에 따라 보안기술도 지속적으로 발전해 오고 있다. 최근에는 IoT (Internet of Things) 기술의 급속한 발전에 따라 유·무선 네트워크에 연결되는 장치가 크게 증가하면서 적절한 보안수준을 제공해야 할 필요성이 증가하고 있다. 보다 효율적인 보안수준을 제공하기 위해서는 적은 자원을 사용하여 높은 보안성능을 제공하는 것이 중요하다. 정보보안 시스템은 대칭키 암호, 공개키 암호, 해시 함수를 기본으로 하며, 해시 함수는 사용자 인증, 디지털 서명, 메시지 인증코드와 같은 다양한 보안 목적으로 사용되고 있다. 2007년 미국 국립표준기술국 (National Institute of Standard and Technology; NIST)은 Secure Hash Algorithm2 (SHA2)의 보안수준을 우려하여 SHA3의 후보 알고리듬을 공개 모집했고, 2012년 10월에 차세대 해시 함수로 KECCAK 알고리듬 [1]이 선정되었다. KECCAK 알고리듬은 SHA2에 비해 높은 보안수준을 제공하며, 소프트웨어나 하드웨어로 구현함에 있어서 적은 자원을 소모하는 것으로 평가되고 있다.

본 논문에서는 SHA3 표준 [2]에 제시된 해시 함수 중, SHA3-512를 다양한 크기의 데이터 패스로 구현하여 최적의 하드웨어 설계조건을 분석한 결과를 기술한다. II장에서는 SHA3 해시 알고리듬에 대해 간략히 기술하고, III장에서는 5가지 데이터

* corresponding author

패스로 구현된 SHA3-512 해시 코어에 대해 설명한다. IV장에서는 최적 설계조건 분석 결과에 대해 기술하고, V장으로 결론을 맺는다.

II. SHA3 해시 알고리듬 [2]

SHA3 해시 알고리듬의 연산은 *Keccak-p*에 의해 이루어진다. *Keccak-p*는 *Keccak-p*[*b*, n_r]의 형태로 스테이트 (state)의 크기 *b*와 라운드에 대한 매개변수 n_r로 정의된다. *b*는 최솟값인 25부터 두 배씩 증가하는 값을 가지며 최댓값은 1600이다. 매개변수 *b*에 관련된 변수 *w*와 *l*은 아래 표 1과 같은 값을 갖는다. $w = b/25$, l은 $\log2(b/25)$이다. 매개변수 $n_r = 12+2l$인 경우에는 *Keccak-f*[*b*] = *Keccak-p*[*b*, $12+2l$]로 정의된다.

Table 1. Parameter values of SHA3 hash function

b	25	50	100	200	400	800	1600
w	1	2	4	8	16	32	64
l	0	1	2	3	4	5	6

*Keccak-p*는 그림 1과 같이 스테이트 단위로 연산되며, Theta(Θ), Rho(ρ), Pi(π), Chi(χ), 그리고 Iota(ι)의 5단계 연산으로 이루어진다.

Theta(Θ) 단계는 열(column) 단위의 회전과 비트별 XOR로 구성되며, Rho(ρ) 단계는 레인(lane)에서 위치에 따른 오프셋에 의한 순환 시프트연산이다. Pi(π) 단계에서는 치환(permutation)이 이루어지고, Chi(χ) 단계는 비트 단위 XOR, NOT, AND 연산으로 구성된다. 마지막 Iota(ι) 단계에서는 라운드 상수와 XOR 연산이 이루어진다.

SHA3 해시 함수는 그림 2의 스폰지(sponge) 함수로 구성되며, 처리되는 블록에 입력 메시지가 길이 *r* 만큼 포함되며, 나머지 길이 *c*의 capacity가 존재하여 스테이트의 크기는 $b=r+c$의 값을 갖는다. 그림 2에서 N은 입력 메시지, Z는 출력 메시지를

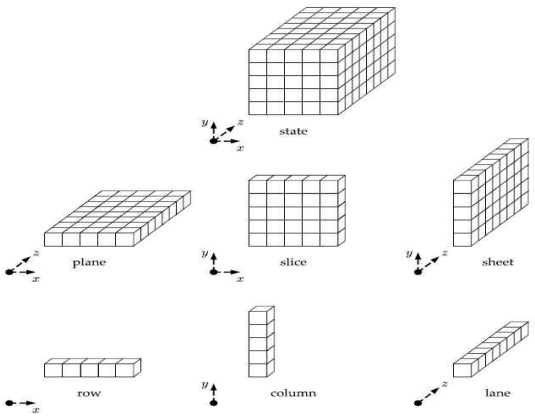

Fig. 1. State array and parts

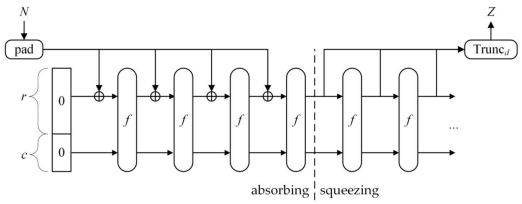

Fig. 2. Sponge construction of SHA3

나타내며 *d*는 출력 해시 값의 길이를 나타낸다. 패딩 알고리듬에 의해 패딩 된 메시지가 블록 단위로 연산되며, 이 과정이 모든 블록에 대해 반복되어 absorbing 단계가 완료된다. squeezing의 경우 출력 확장 함수인 SHAKE128과 SHAKE256에서만 사용된다. SHA3 표준에는 224-비트, 256-비트, 384-비트, 512-비트의 4가지 출력 길이를 제시하고 있으며, 이 경우 absorbing 단계가 완료된 후 squeezing 단계를 거치지 않고 표준에 명시된 길이만큼 출력된다.

III. SHA3-512 해시 코어의 하드웨어 구현

SHA3 표준에 제시된 4가지 출력 길이 중, 512-비트를 선택하였고, 스테이트의 크기는 1600비트로 결정하였다. SHA3-512 해시 코어를 64-비트, 320-비트, 640-비트, 960-비트, 1600-비트의 5가지 데이터 패스 구조를 적용하여 하드웨어로 설계하였다. 전체 구조는 그림 3과 같으며, 패딩 알고리듬을 수행하는 padder 블록, *Keccak-p* 연산을 수행하는 keccak_core 블록, 그리고 연산에 필요한 제어신호들을 생성하는 ctrl 블록으로 구성된다.

keccak_core의 내부 구조는 데이터 패스의 비트 폭에 따라 그림 4와 같은 구조를 갖는다. 64-비트 데이터 패스로 설계되는 코어는 그림 4-(a)의 구조를 가지며, 스테이트를 구성하는 레인 단위로 연산이 수행되며, Theta(Θ), Rho(ρ), Pi(π) 단계와 Chi(χ), Iota(ι) 단계로 나뉜다. 단계별 연산이 수행될 때마다 이전 라운드의 결과 값을 레지스터에 저장하고 있어야 하므로, 1600-비트 레지스터 2개를 갖도록 설계되어야 한다. 각 단계는 64-비트 단위로 25 클록 사이클에 걸쳐 연산되며, 한 라운드 당 50 클록 사이클이 소요된다. 24라운드로 구성되는 한 블록 연산에 1200 클록 사이클이 소요된다. 320-비트, 640-비트 960-비트의 데이터 패스로 설계되는 코어는 그림 4-(b)와 같은 구조를 가지며, 스테이트

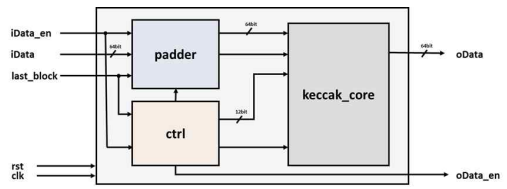

Fig. 3. Architecture of SHA3-512 hash core

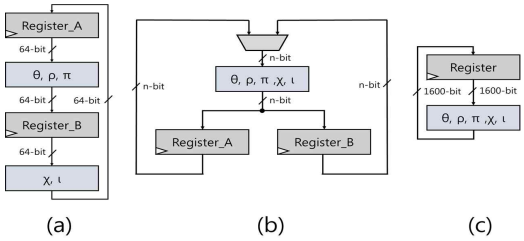

Fig. 4. Structures of keccak_core (a) 64-bit data- path, (b) 320-/640-/960-bit data-path, (c) 1600-bit data-path

를 구성하는 plane 단위로 연산이 수행된다. 64-비트 데이터 패스의 경우와 마찬가지로 1600-비트 레지스터 2개를 갖도록 설계되어야 한다. 블록 당 각각 120, 78, 48 사이클이 소요된다. 1600-비트의 데이터 패스로 설계되는 코어는 그림 4-(c)의 구조를 가지며, 하나의 라운드 연산에 1 클록 사이클이 소요되므로, 1600-비트 레지스터 하나만 필요하며, 블록 당 24 클록 사이클이 소요된다.

Ⅳ. SHA3-512 해시 코어의 검증 및 분석

III장에서 설명된 5가지 데이터 패스의 해시 코어를 Verilog HDL로 모델링하였으며, ModelSim을 이용한 RTL 시뮬레이션으로 기능검증을 수행했다. 그림 5는 설계된 SHA3-512 해시 코어의 시뮬레이션 결과 중 일부를 보인 것이며, 0-비트 평문 메시지 “”에 대한 해시 값 “a69f73cca23a9ac5c8b567dc185a756e97c982164fe25859e0d1dcc1475c80a615b2123af1f5f94c11e3e9402c3ac558f500199d95b6d3e301758586281dcd26”이 출력되었다. 이 결과는 NIST에서 제공하는 테스트 벡터와 동일한 결과이며, 소프트웨어로 구해진 값과도 일치하여 SHA3-512 해시 코어가 올바로 동작함을 확인하였다.

5가지 데이터 패스로 설계된 SHA3-512 해시 코어를 Xilinx Virtex-5 FPGA 디바이스로 합성하여 최대 동작주파수, 슬라이스 수, 처리율의 성능을 비교, 분석한 결과는 그림 6과 같다. 1600-비트의 데이터 패스로 설계된 코어의 최대 동작주파수는 약 289.022 MHz로 가장 컸으며, 약 5.04 Gbps의 처리율을 갖는 것으로 평가되었다. 또한 소요된 슬라이스 수는 1,554로 하드웨어 면적이 가장 적은 것으로 나타났다. 이와 같은 최적 설계조건에 대한 분석을 통해, SHA3-512 해시 코어를 1600-비트의 데이터 패스로 설계하는 것이 가장 바람직한 것으로 판단된다.

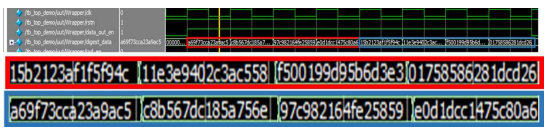

Fig. 5. Simulation result of SHA3-512 hash core

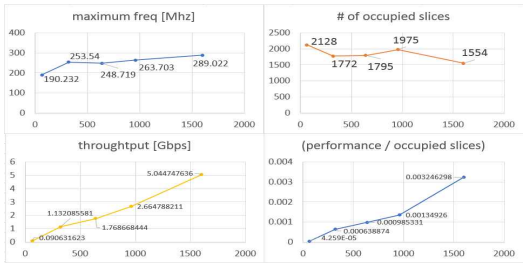

Fig. 6. Performance analysis results

Ⅴ. 결 론

본 논문에서는 SHA3-512 해시 함수를 5가지의 데이터 패스로 설계하여 최적 하드웨어 설계조건을 분석하였다. 64-비트, 320-비트, 640-비트, 960-비트, 1600-비트의 데이터 패스로 구현된 코어 중, 1600-비트의 데이터 패스가 면적 대비 성능이 가장 우수한 것으로 확인되었다. 향후 1600-비트 데이터 패스로 SHA3 표준에 제시된 해시 함수를 구현할 예정이다.

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] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche, The KECCAK SHA-3 submission, Version 3, Jan. 2011, http://keccak.noekeon.org/Keccak-submission-3.pdf.

[2] National Institute of Standards and Technology. FIPS PUB 202 - SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, Aug. 2015.