Microprocessors and Microsystems 37 (2013) 246–257

Contents lists available at SciVerse ScienceDirect

Microprocessors and Microsystems

journal homepage: www.elsevier.com/locate/micpro

Design and benchmarking of an ASIC with five SHA-3 finalist candidates

Meeta Srivastav *, Xu Guo, Sinan Huang, Dinesh Ganta, Michael B. Henry, Leyla Nazhandali, Patrick Schaumont

Center for Embedded Systems for Critical Applications (CESCAs), Bradley Department of Electrical and Computer Engineering, Virginia Tech, Blacksburg, VA 24061, United States

ARTICLE INFO

Article history:
Available online 10 September 2012

Keywords:
Application specific integrated circuit (ASIC)
Field programmable gate array (FPGA)
Hash algorithm (HASH)
SHA-3 competition

ABSTRACT

This contribution describes our efforts in the design of a 130 nm CMOS ASIC that implements Skein, BLAKE, JH, Grøstl, and Keccak, the five candidates selected by NIST in the third round SHA-3 competition. The objective of the ASIC is to accurately measure the performance and power dissipation of each candidate when implemented as an ASIC. The design of this ASIC, and its optimization for benchmarking, creates unique problems, related to the integration of five heterogeneous architectures on a single chip. We implemented each algorithm in a separate clock region, and we integrated an on-chip clock generator with flexible testing modes. The chip is further designed to be compatible with SASEBO-R board, a power-analysis and side-channel analysis environment. We report the design flow and test results of the chip, including area, performance and shmoo plot. Furthermore, we compare our ASIC benchmark with an equivalent FPGA benchmark.

1. Introduction

The SHA-3 competition organized by NIST aims to select, in three phases, a successor for the mainstream SHA-2 hash algorithms in use today. By the completion of Phase II in December 2010, five out of the 14 second round candidates were identified for further evaluation as SHA-3 finalists. For each round in this competition NIST wants to evaluate algorithms [19] and find the best performing algorithm across a large set of computers/architectures. So, their benchmarking process studies how a single algorithm behaves across a broad range of architectures (ASIC being one of them). The winner will be announced by NIST in spring 2012.

NIST recommended benchmarking of both software and hardware platforms. Although the underlying goal of doing benchmarking for both software and hardware is the same, the methodology used is very different and unique. Our effort and contribution to this competition, is to develop an environment for doing un-biased and comprehensive evaluation of SHA-3 candidates on hardware platform. Hardware benchmarking is an important aspect as it evaluates the algorithm based on area, performance and power. There are two primary hardware benchmarking targets: FPGA and ASIC implementations. FPGA benchmarking is very similar to software benchmarking. Because an FPGA can be reprogrammed, each SHA-3 algorithm can be tested in isolation from the others. ASIC benchmarking, on the other hand, requires an expensive and labor intensive tape-out process. Therefore, we need to design all SHA-3 candidates in a single chip, and their low-level implementation (place-and-route) is a shared effort for all candidates at the same time. Since ASICs still cover a significant portion of the hardware design market, we cannot ignore ASIC benchmarking. At the same time, ASIC implementation generally has better performance, smaller die area, and lower power consumption than FPGA.

To evaluate each algorithm on ASIC, we have designed, functionally verified and successfully fabricated chip with SHA-3 finalists. The chip is compatible with SASEBO-R board, which is widely used among cryptographic research community. It provides early access to SHA-3 ASIC hardware. We have open-sourced RTL designs and are also providing other teams with copies of this chip. However, to achieve benchmarking in ASIC in a timely manner and to ensure fairness, we have faced several challenges at different phases, which includes design, implementation and testing. In this article, we will discuss this in further details and present our findings as measured on hardware.

To summarize, key contributions of this article are as follows:

- First, we propose a platform, methodology and evaluation criteria for a comprehensive comparison between five finalists in FPGA and ASIC platforms.
- Second, we present design details and challenges faced in ensuring fairness while benchmarking in ASIC.
- Third, we present the measurement, trends and ranking of these candidates across both FPGA and ASIC platforms.

* Corresponding author. Tel.: +1 7327894768.
E-mail addresses: meeta@vt.edu (M. Srivastav), xuguo@vt.edu (X. Guo), shuang86@vt.edu (S. Huang), diganta@vt.edu (D. Ganta), mbh@vt.edu (M.B. Henry), leyla@vt.edu (L. Nazhandali), schaum@vt.edu (P. Schaumont).

0141-9331/$ - see front matter © 2012 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.micpro.2012.09.001

The rest of the article is structured as follows: In Section 2, we will discuss related work towards ASIC benchmarking. Our methodology towards prototyping is described in Section 3. In Section 4, we present evaluation metrics for these candidates. Section 5 describes the implementation details of ASIC chip. In Section 6, we will analyze the ASIC measurement results and conclude our work in Section 7.

2. Related work

The hardware evaluation of SHA-3 candidates has started shortly after the specifications of 51 algorithms submitted to the contest became available. More comprehensive efforts became feasible only after NIST's announcement of 14 candidates qualified for the second round of the competition in July 2009. Since then, several comprehensive studies for FPGA [6,13,16] and ASIC implementations [18,17,12,7,8,11,14] have been reported. Guo et al. [7] used a consistent and systematic approach to move the SHA-3 hardware benchmark process from the FPGA prototyping by [15] to ASIC implementations using 130 nm CMOS standard cell technology. Tillich et al. [17] presented the first ASIC post-synthesis results using 180 nm CMOS standard cell technology with high throughput as the optimization goal and further provided post-layout results [18]. Henzen et al. [12] implemented several architectures in a 90 nm CMOS standard cell technology, targeting high- and moderate-speed constraints separately, and presenting a complete benchmark of post-layout results. Knezevic et al. [14] provided ASIC synthesis results in a 90 nm CMOS standard cell technology as a comparison with their primary FPGA prototyping results.

In December 2010, five candidates were selected for the last round of SHA-3 competition. These candidates then submitted the final specification of their algorithms in January 2011. The only comparison of the five candidates in ASIC implementations at this stage was provided by [10] based on post-layout simulation. Although Henzen et al. [11] reported the performance results of a compact BLAKE implementation based on ASIC measurements. However, as the BLAKE hash designers they only focused on the BLAKE ASIC characterization. In this article we present implementation details and results that are measured on hardware chip. This is likely the first SHA-3 test chip with five finalists, and as such stands out among all the previous work summarized in Table 1.

3. Methodology

In this section we describe the overall design environment that we have built for both FPGA and ASIC prototyping.

The Side-channel Attack Standard Evaluation Board (SASEBO) [2] is a board specifically designed to develop standard evaluation schemes to secure the cryptographic module against physical attacks. The experimental environment for FPGA prototyping was done using SASEBO-GII board as shown in Fig. 1. A SASEBO-GII board contains two FPGAs: a control FPGA, which provides the interfacing activities with a PC, and a cryptographic FPGA, which contains the hashing candidate. We use the same environment for ASIC benchmarking. ASIC implementation is tested using SASEBO-R board. SASEBO-R board contains a socket, which is used to mount our SHA-3 chip and a control FPGA, which is used to provide interface logic. We test the functionality of each candidate by sending message blocks from the host PC to the SASEBO board and reading the digest generated by the SHA-3 ASIC once it is ready. The digest is then compared with a pre-computed digest by a software testbench running on PC. Power and performance analysis is also performed for both FPGA and ASIC platforms.

FPGA prototyping was done in an earlier phase of our project [7], and in this article we will not cover any details on FPGA prototyping. However, we want to emphasize the advantages of using this setup. First, we now have unique capability of analyzing the design and implementation characteristics for all candidates in both FPGA and ASIC platforms. Second, by using the same test interface we accelerate the process of building and testing of ASIC chip.

4. Evaluation metrics

In this section, we discuss the various metrics based on which we evaluate the five candidates. Common metrics include area, maximum frequency, maximum throughput and power/energy consumption.

4.1. Area

We use the circuit area of each SHA-3 candidate including both, the interface and hash core after layout. The area is reported in kilo-gate-equivalents (kGEs), where a gate equivalent corresponds to the area of a standard NAND2 gate in the standard-cell library. We divide the reported layout area with unit in mm^2 by the area of an NAND2 gate for conversion from the absolute circuit area to kGE.

4.2. Throughput (Tp)

The time required to hash a message consists of four parts: the latency for loading one block of message, L_{in}, the hash core latency, L_{core}, the latency for finalization step, L_{final}, and the latency for outputting the message digest, L_{out}. For short message hashing, all these four latencies are important performance factors. The total latency is frequently used to characterize the short message hashing speed instead of throughput. In the case of hashing a long message, L_{final} and L_{out} can be neglected. Since L_{in} is dependent on the system I/O throughput which may vary in different contexts, here we report the throughput *Tp* of the hash core function as follows:

Table 1
The related SHA-3 hardware benchmarking work in ASICs.

	14 Second round candidates				5 Third round candidates
	Tilinch [18,17]	Guo [7]	Henzen [12]	Knezevic [14]	Guo [10]
Technology node	180 nm CMOS	130 nm CMOS	90 nm CMOS	90 nm CMOS	130 nm CMOS
Hardware interface	Assume infinite bandwidth interface	Defined standard 'handshake' interface	Assume infinite bandwidth interface	Defined standard 'handshake' interface	Defined standard 'handshake' interface
Chosen metrics	Area, throughput	Area, throughput, power, energy	Area, throughput, energy	Power, energy	Area, throughput, power, energy
Design result	Post-layout	Post-layout	Post-layout	Post-synthesis	Post-layout
Hardware testing	No	No	No	No	No