Implementation of 4-way Superscalar Hash MIPS Processor Using FPGA

Safaa Sahib Omran¹, Laith Fouad Jumma²

¹ College of Electrical and Electronic Techniques, Computer Engineering Techniques
² College of Electrical and Electronic Techniques, Computer Engineering Techniques

¹ Omran_safaa@ymail.com, ²Laith1993@gmail.com

Abstract. Due to the quick advancements in the personal communications systems and wireless communications, giving data security has turned into a more essential subject. This security idea turns into a more confounded subject when next-generation system requirements and constant calculation speed are considered in real-time. Hash functions are among the most essential cryptographic primitives and utilized as a part of the many fields of signature authentication and communication integrity. These functions are utilized to acquire a settled size unique fingerprint or hash value of an arbitrary length of message. In this paper, Secure Hash Algorithms (SHA) of types SHA-1, SHA-2 (SHA-224, SHA-256) and SHA-3 (BLAKE) are implemented on Field-Programmable Gate Array (FPGA) in a processor structure. The design is described and implemented using a hardware description language, namely VHSIC “Very High Speed Integrated Circuit” Hardware Description Language (VHDL). Since the logical operation of the hash types of (SHA-1, SHA-224, SHA-256 and SHA-3) are 32-bits, so a Superscalar Hash Microprocessor without Interlocked Pipelines (MIPS) processor are designed with only few instructions that were required in invoking the desired Hash algorithms, when the four types of hash algorithms executed sequentially using the designed processor, the total time required equal to approximately 342 us, with a throughput of 4.8 Mbps while the required to execute the same four hash algorithms using the designed four-way superscalar is reduced to 237 us with improved the throughput to 5.1 Mbps.

Keywords: MIPS, FPGA, SHA-1, SHA-2, BLAKE.
1. Introduction
Cryptography is an important science of building protocols or plans that qualify users to transmit data over a risky path without victimizing the transmission confidentiality or the authenticity.

Contemporary cryptography is used in many fields of applications to ensure the safety of not only data, but also for commercial applications such as electronic payment schemes and voting. The basic building blocks are classified into block ciphers, stream cipher and hash function. They occupy a substantial role in vast applications. The modern technologies such as online banking, online trading, email, ATMs and mobile applications claim efficient and secure schemes. The most important matter in crypto algorithm design is the harmonization and trade-off between efficiency and security, also the required property from integrity, authentication and confidentiality determine the field of security used. One of the most important concepts of cryptography is protecting the confidentiality and authenticity of data [1]. The hash functions deal with two important codes which are very useful with hash applications, these codes are: Hash Message Authentication Code (HMAC) and Message Integrity Check (MIC). These codes are providing an important property to the hash functions which is the collision resistance.

2. Related Work
In 2003, N. Sklavos et. al. designed a high speed Architecture for SHA-1 and RIPEMD-160. Pipelined technique is applied to achieve operation mode for RIPEMD-160 and SHA-1 [3].
In 2013, Fatma et. al. they implement an efficient hardware of secure hash algorithms (SHA-3) BLAKE-256 and they report the result implantation of BLAKE-256 on FPGA Xilinx Virtex 7, Virtex 6 and Virtex 5. They report the performance of its design [4].
In 2015, Mestiri et. al. suggested a new plan for the SHA-256 and SHA-512 hash algorithms. The proposed scheme has been performed by Xilinx Vertex- 5 FPGA [5].
In 2016, Mohamoud et. al. studied the computation bottlenecks of SHA-3 on a 32-bit MIPS processor and introduced two of ASIP architecture to increase performance of SHA-3 which designed on FPGA Xilinx Virtex 6 [6].

In this paper, SHA-1, SHA-224, SHA-256 and SHA-3 (BLAKE) are implemented in 4-way superscalar Hash MIPS processor using FPGA.

3. Four-way Superscalar Hash MIPS Processor Design
Firstly a MIPS processor was implemented for executing the hash algorithms sequentially. The design consist of two interacting parts: 32-bits datapath and control unit. The datapath consist of an ALU, a register file, a message computation block and constant port. Then superscalar processor is an advanced technique that enables the processor to execute more than one instruction per clock cycle [7]. This approach is achieved by replicating the internal components of the processor, so that it can launch multiple instructions in each clock cycle. The general name of this technique is multiple issues. Hence, in this section a four-way unit’s 32-bit superscalar MIPS processor is designed. This processor is capable for executing the algorithms for SHA-1, SHA-224, SHA-256 and BLAKE[8][9][10], since the variables for these hash algorithms are 32-bits. Figure 1 shows a general block diagram for this 4-way superscalar processor. As shown in the figure, four units were duplicated to enable the processor for executing 4 instructions per each clock.
The complete design of a 32-bit 4-way superscalar Hash MIPS processor consists of two interacting parts:
1. Four datapath.
2. Four Control unit.

The design has the ability to execute fourth instructions in clock cycle with some limitation. 

'Figure 2' shows the complete design of the single-cycle Hash MIPS processor with its datapath and control unit.

3.1 Four Datapath
A four-way Superscalar has four copies of hardware to execute four instructions simultaneously. All elements in datapath are duplicated except program counter and memories, to allow four instructions pass through it at the same time. Register file's ports and memories' ports are duplicated in turns to be capable to execute four instructions simultaneously. The following sections present the differential units that required in this 4-way superscalar MIPS processor.

3.2 Four Control Units
Four datapaths were needed four control units to guarantee execute four instructions correctly. Each control unit consists of main control as single-cycle MIPS processor. It has the same signal with same meaning.
3.3 Register File
It consists of 32 registers each of 32-bit in size. The register file's ports are duplicated. It has eight read ports (RD1, RD2, RD3, ..., RD8) and four write port (WD, WD1, WD2, WD3). Register file used ports (RD1, RD2, WD, A1, A2, and A3) to communicate with 32-bit datapath 1, and signal WE1 is provided from control unit 1 to register file, this considers entire execution path 0. Also it is used ports (RD3, RD4, WD1, A4, A5, and A6) to communicate with 32-bit datapath 2, and signal WE2 is provided from control unit 2 to register file, this considers execution path 1. and so on in path 2 and path 3.

Figure 2: Block Diagram of 32-bit Superscalar Hash MIPS Processor

The SHA-1, SHA-224, SHA-256 and BLAKE each use varies instructions, table 1 shows all the designed instructions and the requirement from these instruction for each hash algorithm.

Table 1: Instruction need for SHA-1, SHA-224, SHA-256 and BLAKE.

| Instruction | SHA-1 | SHA-224 | SHA-256 | BLAKE |
|-------------|-------|---------|---------|-------|
| XOR         | Y     | Y       | Y       | Y     |
| JMP         | Y     | Y       |         | Y     |
| BEQ         | Y     | Y       | Y       | Y     |
| ADDI        | Y     | Y       |         | Y     |
| LOAD        | Y     | Y       | Y       |       |
| STORE       | Y     | Y       | Y       |       |
| AND         | Y     | Y       | Y       |       |
| NOT         | Y     | Y       | Y       |       |
| OR          | Y     | N       | N       | Y     |
| ADD         | Y     | Y       | Y       |       |
Simulation results and Discussions

Superscalar MIPS processor of 32-bit is tested with a plaintext “abc” to produce fixed 160, 256, 224 and 256 bit for SHA-1, SHA-256, SHA-224 and BLAKE-256. This 4-wat superscalar processor is simulated using the Virtex 7 because the required component for this processor is greater than the available component exists in Spartan-3an. The testing figures of hash function are shown in ‘figure 3’.

|   |   |   |   |   |
|---|---|---|---|---|
| <<< 1 | Y | N | N | N |
| <<< 5 | Y | N | N | N |
| <<< 10 | Y | N | N | N |
| <<< 30 | Y | N | N | N |
| >>> 2 | N | Y | Y | N |
| >>> 6 | N | Y | Y | N |
| >>> 7 | N | Y | Y | Y |
| >>> 8 | N | N | N | Y |
| >>> 11 | N | Y | Y | N |
| >>> 12 | N | N | N | Y |
| >>> 13 | N | Y | Y | N |
| >>> 16 | N | N | N | Y |
| >>> 17 | N | Y | Y | N |
| >>> 18 | N | Y | Y | N |
| >>> 19 | N | Y | Y | N |
| >>> 22 | N | Y | Y | N |
| >>> 25 | N | Y | Y | N |
| >> 3 | N | Y | Y | N |
| >> 10 | N | Y | Y | N |
SHA-224 is first complete at t=86030 ns

BLAKE-256 is fourth complete at t=237070 ns

Table 2 shows the throughput, power and time required to complete a 64-bit Hash MIPS processor.
Table 2: 4-way Superscalar Hash MIPS processor with its throughput, power and time to completed

| Hash      | Time    | Throughput | Power     |
|-----------|---------|------------|-----------|
| SHA-1     | 136870 ns | 3.7 Mbps   | 0.039(Watt) |
| SHA-224   | 86030 ns  | 5.6 Mbps   |           |
| SHA-256   | 86050 ns  | 5.6 Mbps   |           |
| BLAKE-256 | 237070 ns | 5.1 Mbps   |           |

The execution time for our design can be enhanced by using a pipeline processor in which will increase the value of throughput. The designed processor in single cycle MIPS processor which easy to design but the drawback of this processor that all instructions must be executed in fixed time (same no.of clk cycle) which is limited by the slowest instruction, from this table SHA-224 is first completed with t=86030 ns and with only one clock SHA-256 is second completed, third SHA-1 is complete with t=136870 ns and last BLAKE is completed with t= 237070 ns. Table 3 summarizes the FPGA resources used in a 32-bit Hash MIPS processor.

Table 3: FPGA resource utilization.

| Device Utilization Summary | 4-way Superscalar |
|----------------------------|-------------------|
| Logic Utilization          | 32777             |
| Number of Slice Flip Flops |                   |
| Number of 4 input LUTs     | 118691            |
| Number of occupied Slices  | 32777             |
| Number of bonded IOBs      | 262               |

4. Conclusions
A hash SHA-1, SHA-224, SHA-256, and BLAKE-256 was implemented using FPGA Virtex-7. A superscalar MIPS processor was designed using VHDL Xilinx ISE software language with only instructions that Hash need. The time required is executing each algorithm along in sequential orders takes about 342 usec with throughput of 4.8 Mbps, while the required time is executing the four algorithms simultaneously by using the 4-way superscalar processor is reduced to 237 us with throughput of 5.1 Mbps. This study is a starting point for future studies and can be extended to invoke the algorithm for SHA-1, SHA-224, SHA-256, and BLAKE-256 by using a Multicore MIPS processor.
Reference

[1] Ö. KÜÇÜK, "Design and Analysis of Cryptographic Hash Functions", Heverlee (Belgium): © Katholieke Universiteit Leuven – Faculty of Engineering, 2012.

[2] L. C. Washington, "Introduction to Cryptography, Wade Trappe": Wireless Information Network Laboratory, 2006.

[3] N. Sklavos, G. Dimitroulakos and O. Koufopavlou, “An Ultra High Speed Architecture for VLSI Implementation of Hash Functions”, Proceedings of the 10th IEEE International Conference on Electronics, Circuits and Systems (ICECS 2003) pp. 990-993 Vol.3, 2003.

[4] F. Kahri, B. Bouallegue, M. Machhout and R. Tourki, "An FPGA implementation of the SHA-3: The BLAKE Hash Function," 10th International Multi-Conference on Systems, Signals & Devices (SSD), Tunisia, 18-21, March, 2013.

[5] H. Mestiri, F. Kahri, B. Bouallegue and M. Machhout, "Efficient FPGA Hardware Implementation of Secure Hash Function SHA-2," I.J. Computer Network and Information Security, pp. 9-15, 2015.

[6] In 2015, Yi wang et. al. proposed a novel SHA-3 implemented using set execution based on a 32-bit LEON3 processor with reducing execution cycles and code size.

[7] M. A. Elmohr, M. A. Saleh, A. S. Eissa, K. E. Ahmed, M. M. Farag, "Hardware Implementation of A SHA-3 Application-Specific Instruction Set Processor,"28th International Conference on Microelectronics (ICM), 17 20,December,2016.

[8] In 2017, S. S. Omran at. al. designed a hash processor for SHA-1 and SHA-2 algorithms by using Multithreading MIPS processor using the Xilinx Spartan-3AN

[9] J. L. Hennessy, D. A. Patterson, “Computer Organization and Design: The Hardware/Software Interface”, 4th ed., Waltham, USA: Morgan Kaufmann, 2012.

[10] J.P Aumasson, L. Henzen, W. Meier, R. C.W. Phan, "SHA-3 proposal BLAKE", version 1.3, December, 16, 2010.