Simulation of SHA-3 Algorithm (KECCAK) With Area Efficient Module

[1]Priya Kotewar, [2]Prof. R.N.Mandavgane,[3]Prof.D.M.Khatri·
[1]Student Mtech (VLSI), [2] Associate Professor, [3]Assistant Professor
[1] Department of Electronics & Telecommunication Engineering
[1] Bapurao Deshmukh College of Engineering, Sevagram, Wardha, India

Abstract: SHA-3 is widely used in security protocols and applications such as message authentication in wireless senor nodes. Efficient implementation of SHA-3 is desired to achieve speed and power performance. In this paper, design, simulation and implementation of SHA-3 Keccak algorithm on Xilinx ISE software is presented. The design was coded in VHDL and implemented on Vertex 6 FPGA.The objective of the work was to achieve minimum gate count or area so as to increase speed and decrease power dissipation. Results clearly indicate that the presented design achieve less area and high speed.

***IndexTerms*—SHA-3, Keccak-512.**

1. INRODUCTION

The Secure Hash Algorithms are a family of cryptographic hash function published by the Institute of Standards and Technology (NIST) as a U.S.Federal Information Processing Standard (FIPS). All of the current SHA algorithms are developed by the NSA. A hashing algorithm is a mathematical function that condenses data to a fixed size. They are convenient for situations where computers may want to identify, compare, or otherwise run calculations against files and strings of data. It is easier for the computer to first compute a hash and then compare them than it would be to compare the original files. The key properties of hashing algorithm are determinism. Hashing algorithm is used for storing passwords they also used in computer and in databases. There are hundreds of hashing algorithms they all have specific purposes some are optimized for certain types of data, others are for speed, security, etc. Cryptographic hash function produces irreversible and unique hashes which is the most important factors. Irreversible means if you only had the hash you couldn't use that to figure out what the original piece of data was, therefore allowing the original data to remain secure and unknown. Unique so that two different pieces of data can't produce the same hash.

Many scientist work on SHA3 algorithm on various factors such as latency ,throughput, power and area with their differ ideas ,and platforms .They uses software ,hardware or combination of both .The area reduction is the main objective of our project for that we uses VHDL language and simulation is done on Xilinx software [1].

SHA3 is subset of the cryptographic primitive family Keccak it is cryptographic hash function designed by scientists Guido Bertoni, Joan Daemen, MichaëlPeeters, and Gilles Van Assche. SHA-3 is a member of the Secure Hash Algorithm family, SHA-3 standard was released by NIST on August 5, 2015.The NIST hash function competition organized in 2006 to create a new hash standard that is SHA-3. SHA-3 is not meant to replace SHA-2, as no significant attack on SHA-2 has been demonstrated. Because of the successful attacks on MD5, SHA-0 and SHA-1 NIST perceived a need for an alternative, dissimilar cryptographic hash, which became SHA-3.The National Institute of Standards and Technology has released the final version of its "Secure Hash Algorithm-3" standard, a next-generation tool for securing the integrity of electronic information.SHA-3 is the first cryptographic hash algorithm NIST has developed using a public competition and vetting process that drew 64 submissions worldwide of proposed hashing algorithms. Hash algorithms are broadly useful in the world of electronic communications. They transform a digital message into a short "message digest" for use in digital signatures and other applications. Even a small change in the original message creates a change in the digest, making it easier to detect accidental or intentional changes to the original message. Hash functions can be used in a variety of security applications such as message authentication. They also are useful during routine software . [2]

2.LETERATURE REVIEW

1.PriyaKotewar, Prof. R.N.Mandavgane,Prof. D.M.Khatri,"Review on simulation of sha-3 algorithm (keccak) with area efficient module".2017

In this paper the review of the various papers on sha-3 is considered for the fair comparison. Area reduction is the main objective of our project, which is done using xillinx software by using VHDL language. Keccak uses sponge construction in which message bit is xor with the subset of the state.SHA-3 engine is the core of our module,in which various calculations takes place.

2.Miroslav Knezevic, Kazuyuki Kobayashi, Jun Ikegami, Shin ichiro Mats, Akashi Satoh,UnalKocabas¸ Junfeng Fan, Toshihiro Katashita, Takeshi Sugawara, Kazuo Sakiyama,IngridVerbauwhede, Kazuo Ohta, Naofumi Homma, and Takafumi Aoki. "Fair and Consistent Hardware Evaluation ofFourteen Round Two SHA-3 Candidates".

In this paper a design strategy and evaluation criteria for a fair candidates is proposed. Aa SASEBO-GII field-programmable gate array (FPGA) board as a common platform is used in combination with well defined hardware and software interfaces. All 256-bit version candidates are compared with respect to area, throughput, latency, power, and energy consumption. The second contribution is that we provide both FPGA and 90-nm CMOS application-specific integrated circuit (ASIC) synthesis results and thereby are able to compare the results. Our third contribution is that they release the source code of all the candidates and by using a common, fixed, publicly available platform, our claimed results become reproducible and open for a public verification. They conclude that the obtained FPGA resultsrepresent rather reliable way of estimating the ASIC performance, especially with respect to speed and area.[3]

3.George S. Athanasiou, George-Paris Makkas, GeorgiosTheodoridis "High Throughput Pipelined FPGA Implementation Of The New Sha-3 Cryptographic Hash Algorithm".

A two-staged pipelined architecture of the new SHA-3 algorithm is presented. The core can operate on both one-block and multi-block messages. In this paper a two-staged pipelined architecture of the new SHA-3 (Keccak) algorithm is presented. The core can operate on both one-block and multi-block messages. Special effort has been paid and different design alternatives have been studied to derive efficient FPGA implementations in terms of throughput and throughput/area metrics. The proposed Xilinx Virtex-5, Virtex-6, and Virtex-7 FPGA technologies and achieves significant improvements compared to existing FPGA implementations. Future work include optimized FPGA implementations of the finalized SHA-3 standard.[4]

4.AishaMalikl, Arshad Aziz, Dur- e-ShahwarKunde ,MoizAkhter "Software Implementation of Standard Hash (SHA-3) Keccak on Intel Core-i5 and Cavium Networks Octeon Plus embedded platform".

In this paper the software implementation of Keccak - 512 on two platforms - Intel core-iS and Cavium Networks Octeon embedded platform. Along with this benchmarking of our code on the former platform and its comparison with benchmarking results of other Keccak implementations. The perfonnance of Keccak-512 is evaluated on a resource-efficient platform and a resource-constrained platform for short input messages. The performance result of Intel core-i5 2450M is magnificent as compare to Octeon CN5860 is an embedded system in terms of speed in MB/S.[5]

5. SiavashBayat-Sarmadi, MehranMozaffari-Kermani, and ArashReyhani-Masoleh "Efficient and Concurrent Reliable Realization of the Secure Cryptographic SHA-3 Algorithm".

Propose an efficient concurrent error detection scheme is used in order to provide reliable architectures for this algorithm. The secure hash algorithm has been selected in 2012 and will be used to provide security to any application which requires hashing, pseudo-random number generation, and integrity checking. This algorithm has been selected based on various benchmarks as security, performance, and complexity.Subpipeliningis to overcome the inherentthroughput degradation of this time-redundancy approach. A time-redundancy scheme is presented for errordetection of the recently-standardized secure cryptographicSHA-3 algorithm, i.e., Keccak.[6]

6. ImadFakhriAlshaikhli, Mohammad A. Alahmad , KhanssaaMunthir"Comparison And Analysis Study Of Sha-3 Finalists".

In this paper all the SHA-3 candidates are compared. The comparative study involves different hash functions criteria such as; security,structure, and performance and cost, to measure the robustness of the algorithms through the Fundamentals Security Measurement Factors of Hash Function (FSMFHF) of Secure Hash Algorithm (SHA). [7]

7.Liang Han, BaiGuoqiang "Hardware implementation analysis of SHA-3 candidates algorithms".

Focus on two of these candidate algorithms, namely BLAKE and Shabal by presenting the common structure for all the SHA3 candidates. After the designing of VLSI circuit the hardware evaluations is done on FPGA and ASIC.SHA-256 algorithms and SHA-3 are compared in the same technology, after comparison found that the SHA3 candidates provide higher throughput but cost more area. Because of raising the complexity of circuit, the efficiency of SHA3 is lower than SHA-256.The common architecture and FSM are presented for all the SHA3 candidates, and design VLSI circuit for two SHA-3 candidates namely BLAKE and shabal and implemented by ASIC and FPGA. SHA-3 algorithm has larger throughput and higher circuit complexity, and is more suitable for high speed and security hardware implementation.[8]

3.**EXPERIMENTAL STUDY**

SHA-512

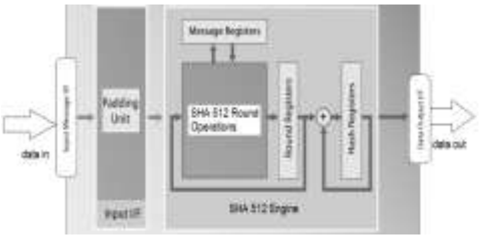

Fig 1: SHA-3 Core

Message padding

In message padding serial data (i.e. either zero or one)is converted into parallel data using flip flops, with the data in ,reset, clock and start signal is given to the flip-flop then parallel data is save in the register having size(0-512).The limit of register and each and every block is of 512 but we can used any value less than the limit. If inputted data is less than the limit then rest bit is set to zero called as “zero padding”, to make it 512bit size, here the data is serial in parallel out to increase the speed of process, then the data is stored in register and we get data out of 512bit.According to the clock frequency the data is input/sec. The clock uses is active low signal, before starting the process we have to reset the system each and every time. Start button is use for start and stop operation.

Preprocessing

Preprocessing is the process of adding 512bit to datain .The preprocessing is the standard protocol of the hash function with LSB bit is equal to 1 and rest bit is zero, then the total bit is equal to1024.

Message parsing

In message parsing 1024 bit of data which is nothing but the output of preprocessing is divided into 16 subsets having (0-63) i.e. 64 bit of each from m0 to m15.

4.OUTPUT WAVEFORMS

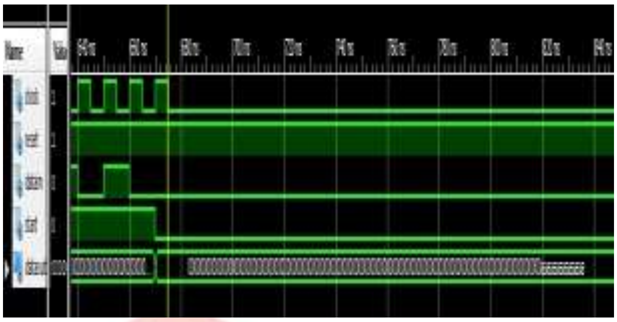

Fig 2: Message padding

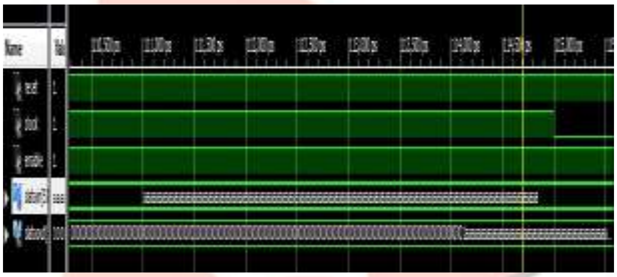

Fig 3: Preprocessing

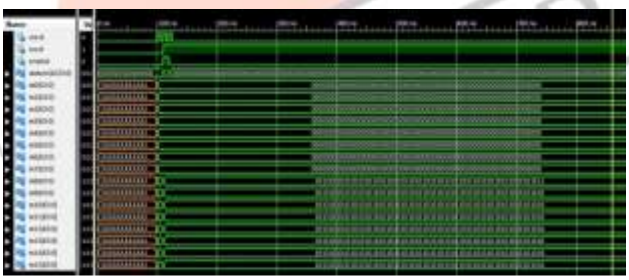

Fig 4: Message Parsing

5.FUTURE WORK AND CONCLUSION

In this propose work we are using the Xilinx software and keccak-512 algorithm .We are improving the performance of SHA-3 by reducing the area as compare with previously design SHA-3.

In future work, we will try to develop SHA-4 to improve security.

6.REFRENCES:

[1]PriyaKotewar, Prof. R.N.Mandavgane,Prof. D.M.Khatri,“review on simulation of sha-3 algorithm (keccak) with area efficient module”.2017

[2]Keccak Hash Function, NIST (National Institute of Standards and Technology),(2014, Mar.)[Online].Available:http://csrc.nist.gov/groups/ST/hash/sha-3

[3]MiroslavKnezevic, Kazuyuki Kobayashi, Jun Ikegami, Shin ichiro Matsuo, Akashi Satoh,UnalKocabas¸ Junfeng Fan, “Fair and Consistent Hardware Evaluation of Fourteen Round Two SHA-3 Candidates”.IEEE-2012

[4] George S. Athanasiou, George-Paris Makkas, GeorgiosTheodoridis “High Throughput Pipelined FPGA Implementation of the New Sha-3 Cryptographic Hash Algorithm”. IEEE-2014

[5] Aisha Malikl, Arshad Aziz, Dur- e-ShahwarKunde ‚MoizAkhter,”Software Implementation of Standard Hash (SHA-3) Keccak on Intel Core-i5 and Cavium Networks Octeon Plus embedded platform”.IEEE-2013

[6] SiavashBayat-Sarmadi, MehranMozaffari-Kermani, and ArashReyhani-Masoleh.”Efficient and Concurrent Reliable Realization of the Secure Cryptographic SHA-3 Algorithm”.IEEE-201

[7]ImadFakhriAlshaikhli, Mohammad A. Alahmad, KhanssaaMunthir”.Comparison And Analysis Study of Sha-3 Finalists”.IEEE-2013

[8] Liang Han, BaiGuoqiang. “Hardware implementation analysis of SHA-3 candidates algorithms”IEEE-2010.

[9] K. Latif, M. Rao, A. Aziz, and A. Mahboob, “Efficient hardware implementations and hardware performance evaluation of SHA-3”IEEE-.2014

[10]S. Tillich, M. Feldhofer, M. Kirschbaum, T. Plos, J. Schmidt, and A.Szekely,“Uniform evaluation of hardware implementations of the round-two SHA-3 candidates,” presented at the 2nd SHA-3 Candidate “.Conf., Santa Barbara, CA, 2010