IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 9, Issue 10, October 2020

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.512

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 10, October 2020||

Implementation of Modified Secure hash Algorithm-3 for High speed and Throughput

Jyoti Hirve, Uma Shankar Kurmi

M.Tech Scholar, Dept. of ECE., Lakshmi Narain College of Technology, Bhopal, India

Assistant Professor, Dept. of ECE., Lakshmi Narain College of Technology, Bhopal, India

ABSTRACT: Secure Hash Algorithms belongs to cryptographic functions which are designed to keep data secured. It works by transforming the data using a hash function: an algorithm that consists of bitwise operations, modular additions, and compression functions. This paper presents implementation of secure hash algorithm-3 for password protection. Simulation is done using Xilinx ISE 14.7 software with verilog code. Result show that proposed SHA-3 gives better area and delay than previous.

KEYWORDS: Secure, Hash-3. Password, Storage, Xilinx, ISE.

I. INTRODUCTION

Cryptographic hash function is a special class of hash function that has certain properties which make it suitable for use in cryptography. It is a mathematical algorithm that maps data of arbitrary size to a bit string of a fixed size (a hash) and is designed to be a one-way function, that is, a function which is infeasible to invert. The best way to reproduce the information from an ideal cryptographic hash capacity's yield is to endeavor a savage power search of potential contributions to check whether they produce a match, or utilize a rainbow table of coordinated hashes [1]. In digital CMOS circuits, parametric yield improvement may be achieved by reducing the variability of performance and power consumption of individual cell instances. In recent years, increasing demand of portable digital systems has led to rapid and innovative development in the field of low power design. Such improvement of variation robustness can be attained by evaluating parameter variation impact at gate level. Statistical characterization of logic gates are usually obtained by computationally expensive electrical simulations [2].

The ideal cryptographic hash work has five primary properties:

•It is deterministic so a similar message consistently brings about a similar hash

•It rushes to process the hash an incentive for some random message

•It is infeasible to create a message from its hash an incentive with the exception of by attempting every conceivable message

•A little change to a message should change the hash esteem so widely that the new hash esteem seems uncorrelated with the old hash esteem.

•It is infeasible to discover two unique messages with similar hash esteem.

Hashing techniques are sorted into two gatherings:

Data-situated hashing versus security-arranged hashing-

(i) Information Situated Hashing Information arranged hashing alludes to techniques that expect to utilize hashing to accelerate information recovery or correlation, where a hash table is frequently kept up for a question.

(ii)Security-Arranged Hashing Security-situated hashing eludes to techniques that utilization hashing for check or approval. For instance, a client may download programming from a public web worker however is concerned whether the product hosts been altered by a third get-together.

A. Message-Digest Algorithm (MD5)

MD5 algorithm uses four rounds, each applying one of four non-linear functions to each sixteen 32-bit segments of a 512-bit block source text. The result is a 128-bit digest. Figure 1 is a graph representation that illustrates the structure of the MD5 algorithm.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 10, October 2020||

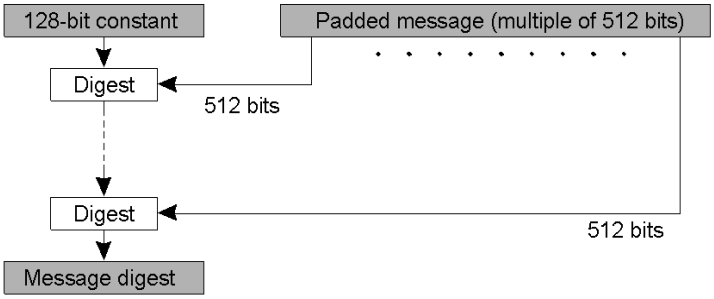

Figure 1: The structure of MD5 algorithm

MD5 algorithm takes a b-bit message as input, where b is an arbitrary nonnegative integer. The following five steps are performed in C programming language to compute the message digest of the input message.

B. SHA-3

SHA-3 (Secure Hash Algorithm 3) was released by NIST. SHA-3 is a subset of the broader cryptographic primitive family Keccak. The Keccak algorithm is the work of Guido Bertoni, Joan Daemen, Michael Peeters, and Gilles Van Assche. Keccak is based on a sponge construction which can also be used to build other cryptographic primitives such as a stream cipher. SHA-3 provides the same output sizes as SHA-2: 224, 256, 384 and 512 bits.

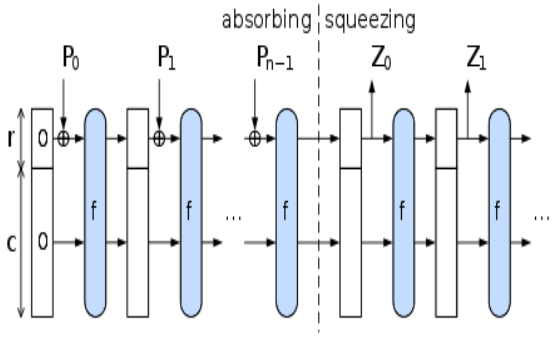

Figure 2: HASH-3

Configurable output sizes can also be obtained using the SHAKE-128 and SHAKE-256 functions. Here the -128 and -256 extensions to the name imply the security strength of the function rather than the output size in bits.

SHA-3 uses the sponge construction, in which data is "absorbed" into the sponge, then the result is "squeezed" out. In the absorbing phase, message blocks are XORed into a subset of the state, which is then transformed as a whole using a permutation function f. In the "squeeze" phase, output blocks are read from the same subset of the state, alternated with the state transformation function f.

A 160 bit buffer is used to hold intermediate value and final results of the hash function.

The buffer can be represented as five 32 bit registers (A, B, C, D, E)

A= 67452301, B = EFCDAB89

C= 98BADCFE, D= 10324576

E =C3D2E1F0

The values are stored in little-endian format, which is the most significant byte of a word in the low address byte position.

Word A= 01 23 45 67, Word B= 89 AB CD EF

Word C= FE DC BA 98, Word D= 76 45 32 10, Word E= F0 E1 D2 C3

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 10, October 2020||

II. PROPOSED WORK

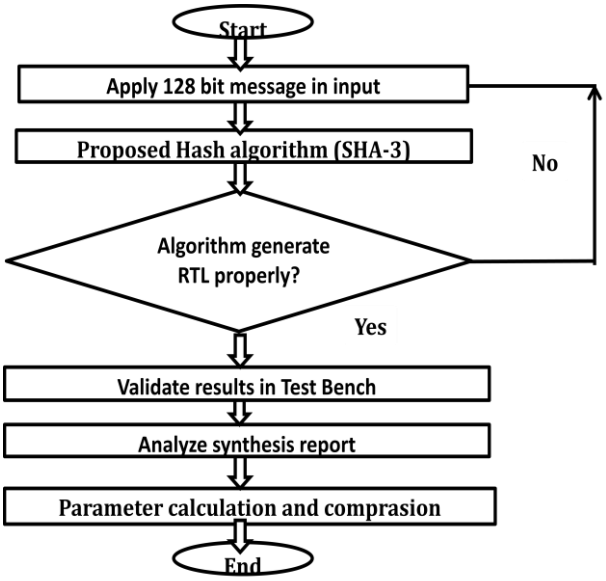

Figure 3: Flow Chart

Algorithm-

- Apply input bits upto 128 bit that may be password or any secure data.
- Now apply proposed hash-3 algorithm, it can generate hash function through hash table.
- Now it will be check from data base, if entered data match from database than user can be access.
- Now view RTL results.
- Now check all result in test bench using Isim simulator.

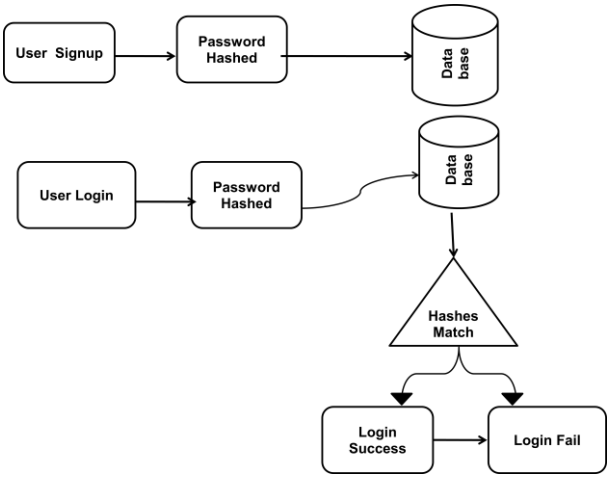

Figure 4: Working

A cryptographic hash function is an algorithm that can be run on data such as an individual file or a password to produce a value called a checksum. The main use of a cryptographic hash function is to verify the authenticity of a piece of data. Hashing is a mathematical operation that is easy to perform, but extremely difficult to reverse. (The difference between hashing and encryption is that encryption can be reversed, or decrypted, using a specific key.)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 10, October 2020||

III. SIMULATION RESULT

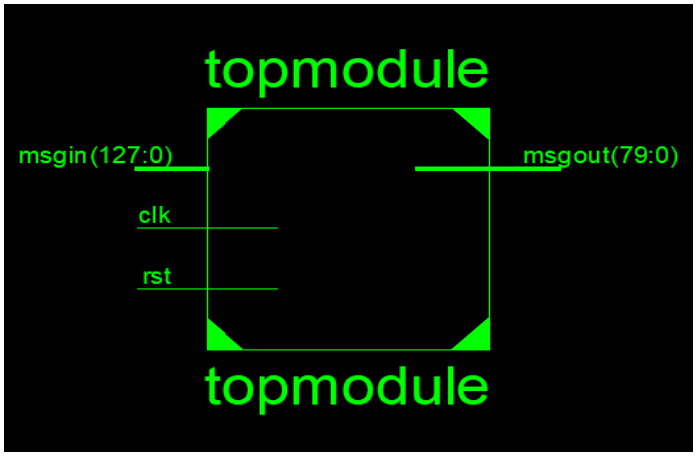

Figure 5: Top view of proposed model

This figure 5 is showing top level module of proposed secure hash algorithm-3. In which apply 128 bit data and it generate 80 bit hash output.

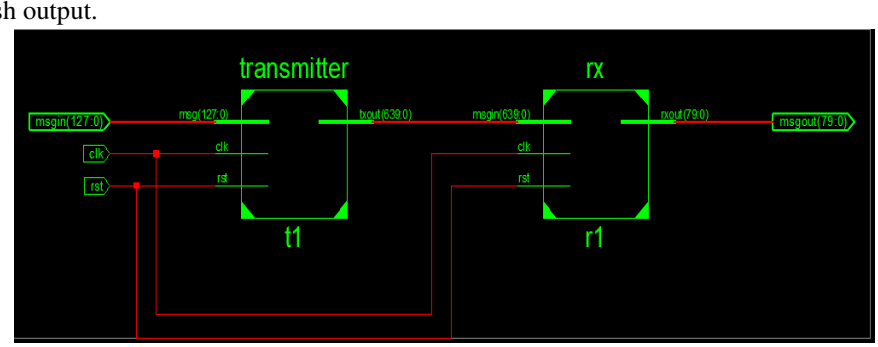

Figure 6: RTL view of proposed Block diagram

Figure 6 is presenting block RTL of sha-3 function. Here firstly apply 128 bit input then at transmitter stage it convert 640 bit. At the receiver end finally it generates 80 bit output.

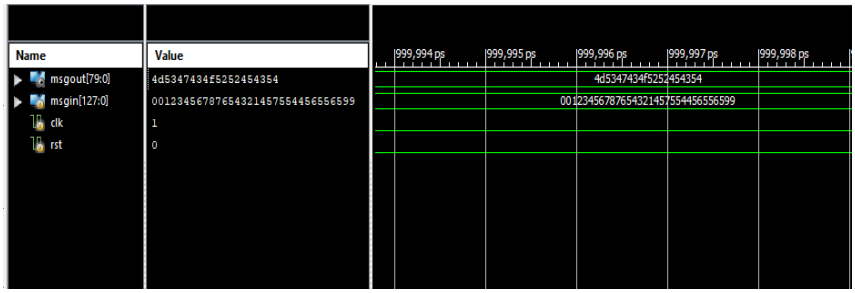

Figure 7: Result validation in test bench

Figure 7 showing 128 bit message in input and it generate 80 bit at output after reduction of bits in modified secure hash algorithm-3 function.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 10, October 2020||

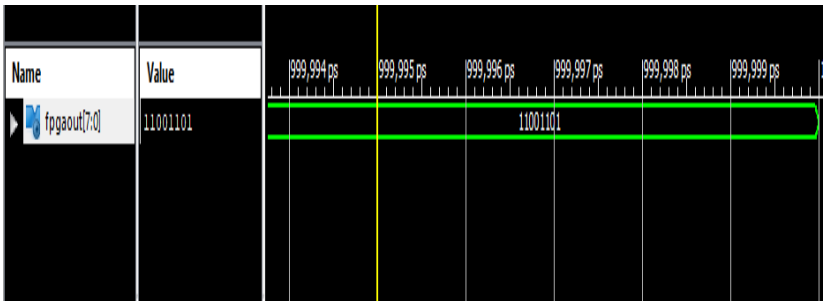

Figure 8: Test bench result for FPGA output

Table 1: Simulation Parameter and Comparison with previous work

Sr No.	Parameter	Previous Work	Proposed Work
1	Method	SHA-3	Modified SHA-3
2	Area (mm)	57.6	7.5
3	Delay (ns)	24	3.259
4	Power(mW)	80	41
5	Time(Secs)	87.31	42.48
6	PDP	1920	133.61

Table 1 showing comparison of proposed work with previous work, so it can be seen that proposed work gives better result than existing work.

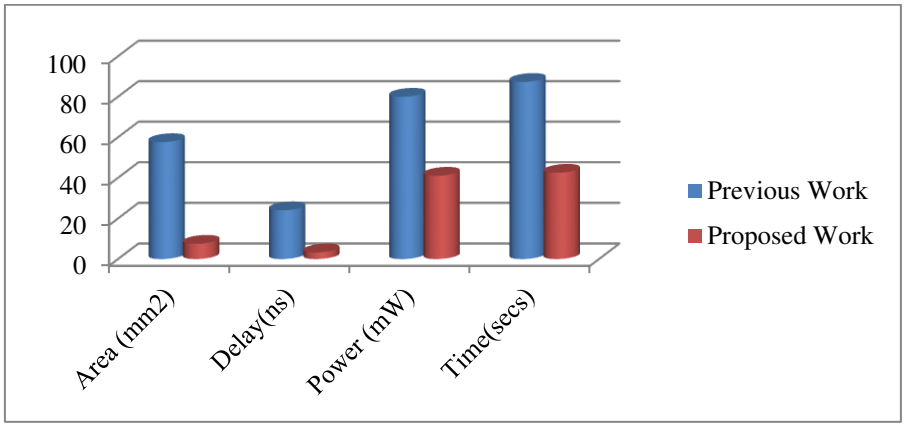

Figure 9: Parameter comparison of previous and proposed work

Figure 9 presents comparison graph of area, delay, power and time of previous and proposed work. It is clear that proposed work achieves better performance than previous work.

IV. CONCLUSION

This paper presents secure cryptographic algorithm, find SHA-3 is latest designed algorithm which is more suitable and useful for secure message in internet applications. Numerous scientists have proposed their own algorithms however none of them are time productive as SHA-3 and furthermore there are odds of enhancing the inward quality of these algorithms. Proposed sha-3 simulation result shows the significant achievement than previous work.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 10, October 2020||

REFERENCES

[1] A. Alzahrani and F. Gebali, "Multi-Core Dataflow Design and Implementation of Secure Hash Algorithm-3," in *IEEE Access*, vol. 6, pp. 6092-6102, 2018.

[2] A. Tanveer, "Estimation of Delay to Consider Leakage in CMOS VLSI Circuit", IJOSCIENCE, vol. 4, no. 11, pp. 13-18, Nov. 2018. https://doi.org/10.24113/ijoscience.v4i11.205.

[3] X. Qiuyun, H. Ligang, L. Qiming, G. Shuqin and W. Jinhui, "The Verification of SHA-256 IP using a semi-automatic UVM platform," *2017 13th IEEE International Conference on Electronic Measurement & Instruments (ICEMI)*, Yangzhou, 2017, pp. 111-115.

[4] I. A. Landge and B. K. Mishra, "Hardware based MD5 implementation using VHDL for secured embedded and VLSI based designs," *2016 International Conference on Communication and Electronics Systems (ICCES)*, Coimbatore, 2016, pp. 1-6.

[5] S. Koranne, "DÉJÀ VU: An Entropy Reduced Hash Function for VLSI Layout Databases," in *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 34, no. 11, pp. 1798-1807, Nov. 2015.

[6] B. Alomair and R. Poovendran, "E-MACs: Toward More Secure and More Efficient Constructions of Secure Channels," in *IEEE Transactions on Computers*, vol. 63, no. 1, pp. 204-217, Jan. 2014.

[7] M. Zhang, M. M. Kermani, A. Raghunathan and N. K. Jha, "Energy-efficient and Secure Sensor Data Transmission Using Encompression," *2013 26th International Conference on VLSI Design and 2013 12th International Conference on Embedded Systems*, Pune, 2013, pp. 31-36.

[8] I. Algredo-Badillo, M. Morales-Sandoval, C. Feregrino-Uribe and R. Cumplido, "Throughput and Efficiency Analysis of Unrolled Hardware Architectures for the SHA-512 Hash Algorithm," *2012 IEEE Computer Society Annual Symposium on VLSI*, Amherst, MA, 2012, pp. 63-68.

[9] N. Sklavos, "Multi-module Hashing System for SHA-3 & FPGA Integration," *2011 21st International Conference on Field Programmable Logic and Applications*, Chania, 2011, pp. 162-166.

[10] A. Shahmoradi and M. Masoumi, "A new nanoelectronic based approach for efficient VLSI realization of SHA-512 algorithm," *IEEE EUROCON 2009*, St.-Petersburg, 2009, pp. 1206-1213.

[11] R. Chaves, G. Kuzmanov, L. Sousa and S. Vassiliadis, "Cost-Efficient SHA Hardware Accelerators," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 16, no. 8, pp. 999-1008, Aug. 2008.

[12] Dan Cao, Jun Han and Xiao-yang Zeng, "A reconfigurable and ultra low-cost VLSI implementation of SHA-1 and MD5 functions," *2007 7th International Conference on ASIC*, Guilin, 2007, pp. 862-865.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.512

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details