FPGA Based OTP Generation System for Data Security

Fazal Noorbasha, Ch. Rahul Krishna, Shaik. HafijullaIrshad

Abstract: ***The password system is the most conventional method among validation techniques on the internet and is operated more easily and effectively than other methods. However, it is a vulnerable method against attacks such as eavesdropping or replay attack. To prevail over this problem, OTP (One Time Password) technique is used. The most popular OTP is HOTP algorithm, which is based on one-way hash function SHA-1. The recent researches show the weakness of the hash function. So, in this paper we created a module which uses another cryptographic algorithm. Cryptography in the current world serves an important role in data security. Cryptography means writing of secret codes (cipher text) which is in an unintelligible form and cannot be read unless we have a perfect key to decode it. The proposed method is AES algorithm (128 bit) followed by Middle Square method to generate an OTP. As OTP is a 4-6 bit number we will decrease the AES output to a 4-6 bit through Middle Square method and this OTP can be used as a security tool in many cases like online transaction purposes.***

Keywords : Ciphertext, HOTP, Middle Square method, SHA-1

I. INTRODUCTION

One Time Password (OTP) is like an access to the particular transaction or information. It is the most secured way to do so. In order to generate the OTP, we used cipher text of AES and converted it to 4-6 bit number. As an encryption algorithm is used it is more difficult for the third party (like hackers) to access the information. In this paper first we have to create a database consisting a list of phone numbers associated with a particular account [1], [2]. As an input we will give a phone number and the database will verify whether the phone number is in database or not. If it is not in the data base the next module will not be executed i.e., the process will be terminated. If the phone number matches then we it will proceed to next module i.e., AES module.AES is asymmetric cryptographic algorithm and uses phone number as an input key. Then the cipher text is sent to the next module which is middle square method. This is a simple hashing method which will square the input and select middle numbers. This number serves an OTP [3].

Revised Manuscript Received on January 15, 2020

Fazal Noorbasha, Associate Professor, Department of ECE, Koneru Lakshmaiah Education Foundation (K L Deemed to be University), Vaddeswaram- 522502, India. Email: fazalnoorbasha@kluniversity.in

Ch. Rahul Krishna, UG Student, Department of ECE, Koneru Lakshmaiah Education Foundation (K L Deemed to be University), Vaddeswaram- 522502, India. E Mail: *rahulkrishnaiit@gmail.com*

Shaik. HafijullaIrshad, UG Student, Department of ECE, Koneru Lakshmaiah Education Foundation (K L Deemed to be University), Vaddeswaram- 522502, India. E Mail: hafeezshaik814@gmail.com

II. SYSTEM BLOCK DIAGRAM

The software used in this paper is Xilinx Vivado as it is most commonly used tool and the language is Verilog [4]. First, we have to create the modules in the proposed model separately and then we have to make an interface through Verilog programming.

In this paper first we have to create a database consisting a list of phone numbers associated with a particular account. As an input we will give a phone number and the database will verify whether the phone number is in database or not. If it is not in the data base the next module will not be executed i.e., the process will be terminated. If the phone number matches then we it will proceed to next module i.e., AESmodule.AES is a symmetric cryptographic algorithm and uses phone number as an input key [5]. Then the cipher text is sent to the next module which is middle square method. This is a simple hashing method which will square the input and select middle numbers. Here we take middle digits of the square. This number serves an OTP. In the above Fig.1 shows a series of steps to be followed in order to obtain the goal which is generation of OTP.

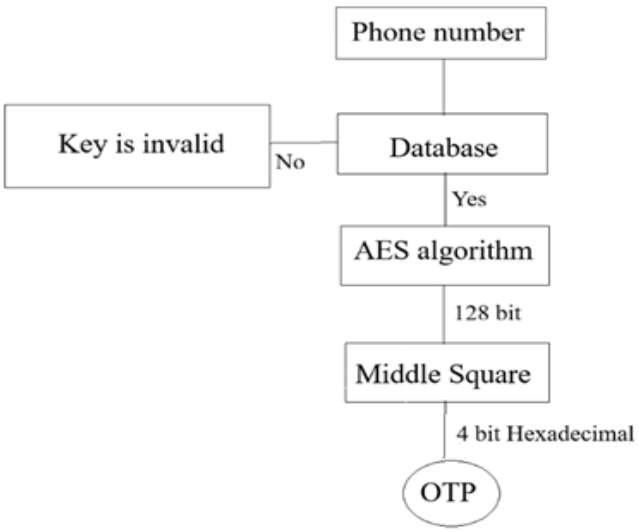

Fig.1 Proposed Model

Module 1

It is a database and consists of phone numbers.As we are using Xilinx Vivado v.2019.1 tool, the database is taken as a notepad consisting of phone numbers. These phone numbers are the root of the module. They should match the database in order to proceed to the next module. If the phone number does not match then there will be no key for the next module i.e., AES algorithm [6]. Then the key will be taken as zeroes which would ultimately result in the failure of the module.

Module 2

It consists of encryption part of 128 bit AES. The key for AES is the phone number in the above module. Generally, phone number is 40 bits. But the key for AES is 128-bit. So, the remaining 80 bits are zeroes. Generally, AES performs 10 rounds and performs four sub operations such as AddRoundKey, SubBytes, ShiftRows, and MixColumns. After all these rounds the cipher text which is of 128 bits is given as input key to the next module.

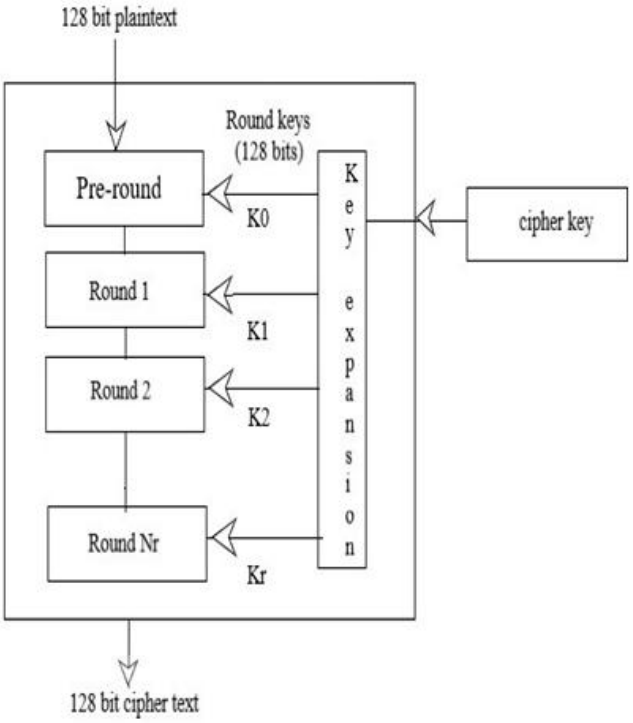

Fig.2 AES algorithm Block Diagram

In the above Fig.2, the 128-bit plaintext is predefined and cipher key is the input phone number. As the cipher key size is 128-bit, number of rounds (r) performed are 10. The cipher key is given to Key expansion block which provides keys for each round. Every round has 4 sub operations that has to be performed [7].

Table 1 Relation between number of rounds(r) and Cipher key size

r	Cipher key size
10	128
12	192
14	256

III. IMPLEMENTATION

The overview of a standard round of AES encryption is restricted in fig. 3. There are four sub-processes in each round. The first-round process is shown fig.3.

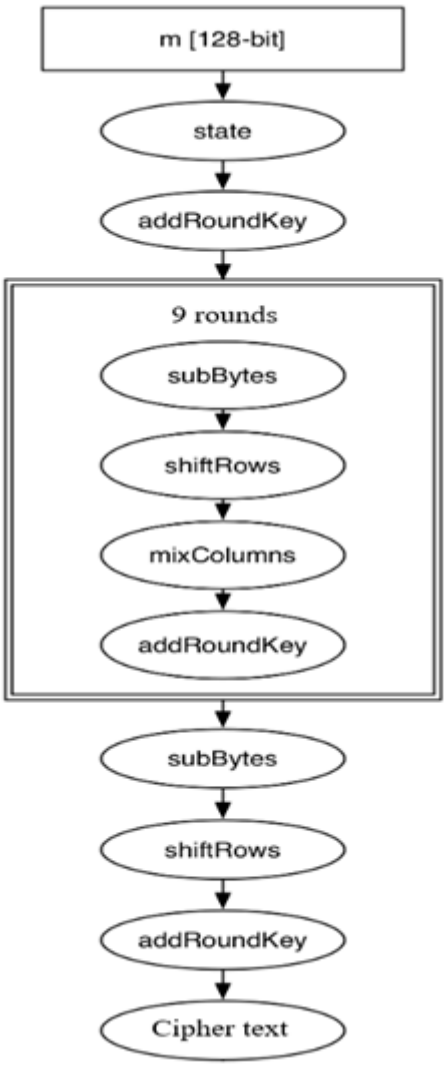

Fig.3 Sub operations of AES

In the above Fig.3, It s showed that all the operations are performed in every round except in last round which exclude MixColumns operation.

Byte Substitution (Sub Bytes): The 16 input bytes are replaced by a fixed table (S-box) in format. The product is a four-row matrix and four-column matrix [8].

Shift Rows: Each of the matrix's four rows is moved to the left. Any entries on the right side of the row that fall off are re-inserted. Shift is performed as follows –

1) There is no shift in the first line.
2) The second row is moving one (byte) to the left.
3) Two places are moved to the left in the third row.
4) Three places were moved to the left in the fourth row.

The effect is a new matrix of the same 16 bits but moved from each other.

Mix Columns: With a special mathematical function, each column of four bytes is now transformed. This method takes the four bytes of a row as input and outputs four entirely new bytes that replace the original column. The result is a new matrix of 16 new bytes. It should be noted that in the last round this step is not taken [9].

Add Round Key: The matrix's 16 bytes are now considered to be 128 bits and XORed to the round key's 128 bits. If this is the last round, the ciphertext is the output.
These four operations are performed in every round i.e., 10 times. The last output is considered as cipher text and is served as an input to the next module.

Module 3:
The 128-bit cipher text is applied to Middle Square method which will square the number and selects middle 4-6 bits by implementing the suitable Verilog code. These 4 bits are in Hexadecimal format and serves an OTP. The Verilog code is written is such a manner that it interfaces all the three modules. In any case if module 1 fails then the process will be failed.

IV. RESULT AND DISCUSSION

It will generate OPT for three times only, after third time t it will not generate OPT because of three time wrong phone **muber or username or password entry.**

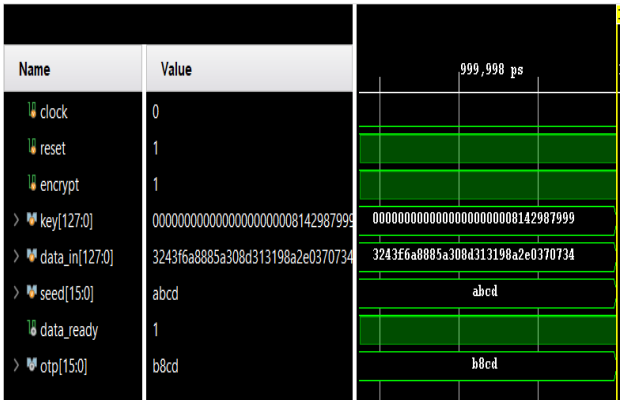

Fig.4 Case 1- Generation of OTP first request

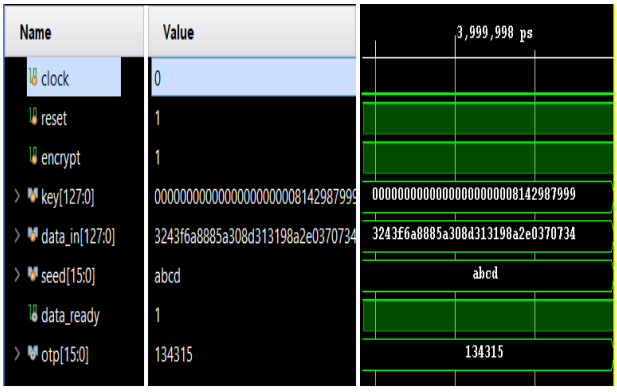

Fig.5 Case 2- Generation of OTP second request

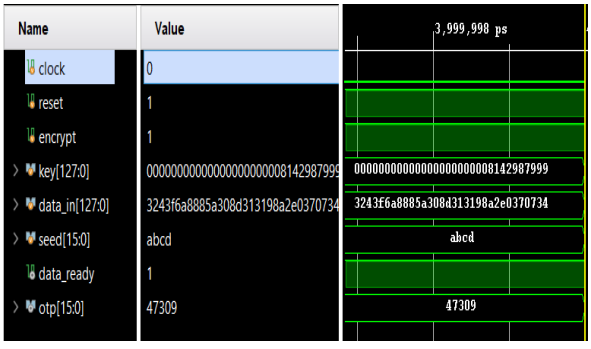

Fig.6 Case 3- Generation of OTP third request

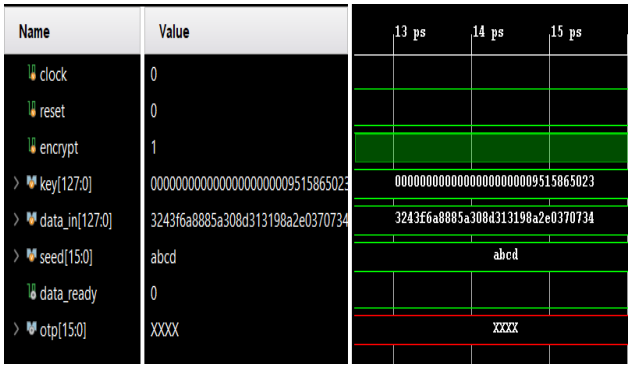

Fig.5 Case 4- Generation of OTP fourth request

Table 2. Containing availability and utilization of resources

Resource	Utilization	Available	Utilization %
LUT	7149	41000	17.44
FF	5892	82000	7.19
DSP	1	240	0.42
IO	292	300	97.33

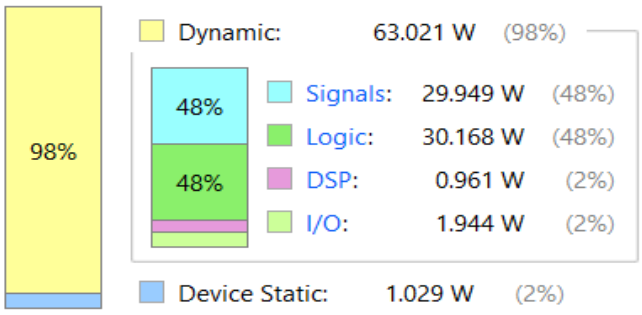

Fig.6 Analysis of power supply

V. CONCLUSION

Totally through this paper, we implemented the Verilog code suitable for the proposed model and generated OTP using AES algorithm and Middle Square method in Xilinx Vivado software. This is proposed OTP give high secured and gives good protection to our data accessing system.

REFERENCES

1. Narendra Babu T., Noorbasha F., Krishna S., Sai Charan K., Sai Kalyan R.S.V.S., FPGA implementation of cryptographic system using BODMAS sequence of operations ,2016, ARPN Journal of Engineering and Applied Sciences, Vol: 11, Issue: 19, pp: 11475 - 11479, ISSN 18196608
2. Narendra Babu T., Noorbasha F., Gunnam L.C., Implementation of high security cryptographic system with improved error correction and detection rate using FPGA ,2016, International Journal of Electrical and Computer Engineering, Vol: 6, Issue: 2, pp: 602 - 610, ISSN 20888708
3. Neelima U., Noorbasha F., Data encryption and decryption using reed-muller techniques ,2016, International Journal of Engineering and Technology, Vol: 8, Issue: 1, pp: 83 - 91, ISSN 23198613
4. Jaya Kumar E., Noorbasha F., Design of static flip-flops for low-power digital sequential circuits ,2016, International Journal of Engineering and Technology, Vol: 7, Issue: 6, pp: 2223 - 2230, ISSN 23198613

5. Noorbasha F., Manasa M., Gouthami R.T., Sruthi S., Priya D.H., Prashanth N., Rahman M.Z.U., FPGA implementation of cryptographic systems for symmetric encryption,2017 Journal of Theoretical and Applied Information Technology, Vol:95, issue:9, pp: 2038-2045, ISSN: 19928645
6. Noorbasha F., Hari Kishore K., Naveen T., Sai Anusha A., Manisha Y., Revathi K., Manasa M. .," Implementation of modified Feistel block cipher for OTP generation using Verilog HDL ", 2018, Progress In Electromagnetic Research M ,Vol: 63 ,Issue: ,pp: 163 to:: 173 ,DOI: ,ISSN: 19378726
7. Praveen Blessington T., Bhaskara B., Noor Basha F. .," Efficient analysis for power modeling on routing topologies in three-dimensional network on chip architectures ", 2018, Progress In Electromagnetics Research C ,Vol: 85 ,Issue: ,pp: 191 to:: 208 ,DOI: 10.2528/PIERC18041906 ,ISSN: 19378718
8. PraveenBlessington T., Bhaskara B., Basha F.N. .," Estimation of latency and throughput for three-dimensional network-on-chip architecture ", 2018, Journal of Advanced Research in Dynamical and Control Systems ,Vol: 10 ,Issue: 9 Special Issue ,pp: 323 to:: 332 ,DOI: ,ISSN: 1943023X
9. S. Radha, D. S. Shylu, P. Nagabushanam, J. Sunitha Kumari, "Design of RF LNA with Resistive Feedback and Gain Peaking for ulti-Standard Application" IJRTE, Vol 7, 2018, pp.100-108.

AUTHORS PROFILE

Fazal Noorbasha was born on 29th April 1982, Vedullapalli, Bapatla, Guntur, Andhra Pradesh, India. He received his, B.Sc. (Electronics) Degree in Physical Sciences from BCAS College, Bapatla, Affiliated to the Acharya Nagarjuna University, Guntur, Andhra Pradesh, India, in 2003, M.Sc. Degree in Electronics Sciences from the Dr. HariSingh Gour Central University, Sagar, Madhya Pradesh, India, in 2006, M.Tech. Degree in VLSI Technology, from the North Maharashtra University, Jalgaon, Maharashtra, INDIA in 2008, and Ph.D. Degree in VLSI Technology from Department of Physics and Electronics, Dr. HariSingh Gour Central University, Sagar, Madhya Pradesh, India, in 2011. Science 2011 he is working as an Associate Professor, Department of Electronics and Communication Engineering, and Associate Dean-Academics, Koneru Lakshmaiah Education Foundation (K L Deemed to be University), Guntur, Andhra Pradesh, India, where he has been engaged in teaching, Administration and research. His interest of research and development is Low-power, High-speed CMOS VLSI SoC, Memory Processors LSI"s, Digital Image Processing, Embedded Systems and cryptography systems.

Dr. Fazal is a Scientific and Technical Committee & Editorial Review Board Member in Engineering and Applied Sciences of World Academy of Science Engineering and Technology (WASET), he served as a session chair and co-chair of IEEE conferences, Life Member of Indian Society for Technical Education (ISTE-India), Member of International Association of Engineers (IAENG-China) and Senior Member of International Association of Computer Science and Information Technology (IACSIT-Singapore). He has published and presented over 100 plus Science and Technical papers in various International and National reputed journals and conferences.

Ch. Rahul Krishna was born on 10th September 1998 in Ampapuram village which is located in Krishna district, Andhra Pradesh, India. He is an UG Student in B.Tech degree under the Department of Electronics and Communication Engineering in Koneru Lakshmaiah Education Foundation (K L Deemed to be University), Vaddeswaram, Guntur, Andhra Pradesh, India.

Shaik. HafijullaIrshad, was born on 15th September 1998 in Guntur district, Andhra Pradesh, India. He is an UG Student in B.Tech degree under the Department of Electronics and Communication Engineering in Koneru Lakshmaiah Education Foundation (K L Deemed to be University), Vaddeswaram, Guntur, Andhra Pradesh, India.