Design of Post Quantum Public Key Cryptography & Reliable Key Generation Unit with Reversible Logic

[1]Rohini H, [2]Nikhita M, [3]Rajashekar B. Shettar
[1] Assistant Professor , [2]PG Scholar , [3]Professor
[1]Electronics & Communication Department ,
[1]B.V.B.C.E.T, Hubli, India

Abstract : In the state of art technology, substantial amount of research on quantum computers is explored. Mathematical problems unsolved by classical computer are well addressed by quantum device. Such future computers are capable of breaking existing public key crypto systems very well. The strength of any cryptographic technique depends on key's size and secure transmission. Need arises to build post quantum security algorithms to counter act the quantum attacks. This paper is intended to present generalized approach in building robust and more secure key generation unit for cryptography. Algorithms are proposed for generating private and public keys. Further paper discusses on design of proposed key generation algorithm using reversible logic to reduce the power dissipation. Paper also presents quantum resistant design approach for asymmetric public key algorithm. Functional verification and performance analysis in terms hardware requirement of reversible design is carried out and discussed.

IndexTerms **- Quantum, PKC, Reversible, Security.**

I. INTRODUCTION

In this era, security is one of the main constraints, as huge amount of data has been transmitted over the networks such as banks, telecoms, insurance companies, credit card issuers, mobile wallets, ecommerce companies, hospitals, and gas agencies etc. Due to digitalization and new emerging technologies, there are advantages as well as disadvantages, the need of data security becomes utmost important. We need to secure our sensitive data from interceptors, cryptography is one such method to secure our data. The cryptography which we use, is referred as classical cryptography, which involves complex mathematical equations for encryption and decryption. Classical crypto systems consists of three types namely symmetric, asymmetric and hashing. Both symmetric and asymmetric types need keys for encryption and decryption. In case of symmetric cryptography the communication between two trusted system may fail if for some reason key is leaked to third person. The reason would be, symmetric algorithms uses same key for both encryption and decryption. Deciding on which key to be used and shared between faithful devices also will be the major problem with such type of cryptography. Taking the case of asymmetric cryptography, both public and private keys are used for communication. Public key is shared by the user and an attacker can easily get hold of it. Private key generated for that public key involves rigorous calculations having many combinations. It is difficult to crack such algorithms by any supercomputer in use today[1,3,4,6,7]. But with pace of changing technology, specially invention of quantum computers may take fraction of time to crack such public key algorithms. Grover's and Shor's algorithm running on quantum device can solve any complex mathematical operation used by asymmetric algorithms. Quantum physics used in such computers gives high communication speed and efficiency. This shows new approach towards generation of key and faithful communication is required to counteract attacks by quantum technology [19,20,21,22].

1.1 Reversible Logic Gates

Research interest in quantum technology has started when Landauer proved that traditional binary irreversible gates lead to power dissipation in a circuit regardless of implementation. That is, each bit of information lost will produce KTln2 Joules of heat energy. From a thermo dynamic point of view, it is also proved that KTln2 energy dissipation would not occur, if a computation is carried out in a reversible way[27,28]. Such reversible logic gates are built using quantum gates, has gained greater attention due to its applications in low power VLSI. Using reversible logic power dissipation can be reduced (ideally zero internal power dissipation) to design low power circuits. The special feature of reversible logic gate is that, it uniquely maps between input and output vectors and called as NXN gate. It means, using outputs, the inputs can be recovered uniquely, also fan out is not allowed in reversible circuits as one to-many idea is not reversible. However Feynman gate can be used to achieve fan-out [12,23,24,25].

With respect to reversible circuit design, there are few parameters need to be considered for determining the complexity and performance of circuits. These are as follows

- The number of reversible gates : The number of reversible gates used in circuit.
- The number of constant inputs : This refers to the number of inputs that are to be maintained constant at either '0' or '1' in order to synthesize the given logical function.
- The number of garbage outputs : This refers to the number of unused outputs present in a reversible logic
- Quantum cost: The quantum cost of a reversible gate is the number of 1x1 and 2x2 reversible gates or quantum logic gates required in designing it.

One example of reversible gate as Feynman gate which is a 2*2 matrix is shown in Figure. 1. Feynman gate's quantum cost is 1. This gate is useful for duplication of the required outputs, as fan-out is not allowed in reversible logic. The inputs are A, B and the outputs are X, Y where Y=A, X=A^B. One of the outputs of Feynman gate is XOR gate operation and the other output is known as garbage which is used to maintain the reversibility.

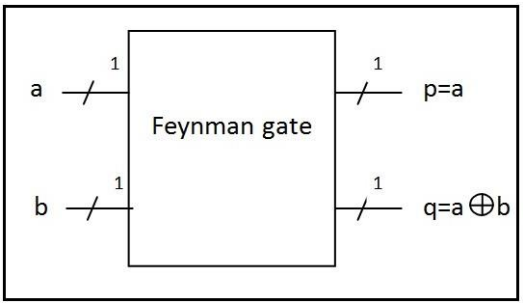

Fig.1 Feynman Reversible Gate

II. BACKGROUND

The concept of a public key distribution system is proposed by Diffie Hellman in 1976. In this two strangers can generate the same key by exchanging their public keys without directly communicating private key[1]. It is seen that, a fixed length key has been cracked by the hackers and predicted the information. Paper[2] discuss about stream cipher techniques which can provide cipher texts with higher security than by single key encryption with stream. It means it is more difficult to hack stream based cipher than the that based on single key. Paper discusses on providing higher level of network security, integrity using point to point encryption method for a wireless communication. Pseudo generator uses seed as a input to trigger and invokes the increasing sequence algorithm to produce random sequence. 98.6% of the numbers produced are undergone 600000 random tests determined by FIPS [3]. It means technique ensures secure transmission of information. OTP cipher is used to generate required key along with Xoring operation with one time key modules to accomplish supplementary services of OTP cipher. Strength of the key used depends on a random key module[4,5,6,7].

Paper[8], propose a new Diffie-Hellman-based Public Key Distribution System which uses a stream cipher technique to encode plaintext with a pseudo random number. A technique generate self-invertible matrix is discussed. Addition to this, new technique of generating thin matrices supported a polynomial and how to it will constitutes the general public key matrix is conferred [9].

Introduction to basic theories of RSA cryptosystem and applies to key algorithm for encryption and decryption, such as Euclidean and its extended theorem, prime number testing and square-multiply algorithm. At last, provides a overview of Matlab simulation of key algorithm and RSA encryption and decryption [10]

Paper[11], discusses the method to enhance OTP encryption. It uses AND & XOR logical functions to combine key and message. New text generated using AND operation initially, then generated text is again XORed with key to get complex cipher.

The remaining section of the paper is organized as follows. Section 2 discusses the proposed new algorithms and design using reversible gates to generate private and public keys required for public key crypto systems. Using these keys a new algorithm for quantum resistant asymmetric cryptography[9] is also proposed and discussed implementation using reversible logic in section 2. Section 3 summarizes the functional verification using Xilinx tool and tabulates the hardware requirements in terms gate count for each algorithm implementation. Section 4 concludes the work carried out.

III. PROPOSED WORK

Asymmetric algorithm uses public and private keys for encryption and decryption as previously mentioned. Both private and public keys are independent to each other and is shown in Figure 3.1.

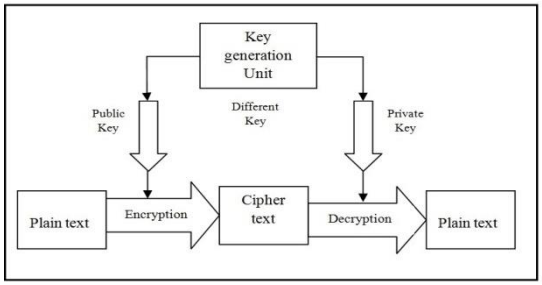

Fig.3.1 Basic Asymmetric Block Diagram

3.1 Proposed Public Key Generator

The basic concept behind this generator is used to produce n-bit of key and use it for encryption. 'n' is defined by user, it may be 128, 256, 512, 1024 and so on bits. That is general method is designed to generate any length key based on requirement as strength of any security algorithm basically depends on length of key chosen. Though using concept of pseudo random generator by LFSR can be used to generate desired key, but no known generalized polynomial exist to generate desired length key. Also rather than using fixed set of keys from generation unit, if varying key is generated depending on message received, security and reliability of the encryption can be improved. Keeping these objectives, an novel algorithm has been proposed to generate any length key for public key cryptography. In this approach, key is made dependent on message and is designed only using addition and multiplication operations, so that both hardware and software implementation is possible. The flow of algorithm, block diagram and example of public key generator are shown in Figure 3.2, Figure 3.3 and Figure 3.4 respectively. The unit is generalized as it can produce any bits of public key. Entire algorithm is realized using reversible logic gates.

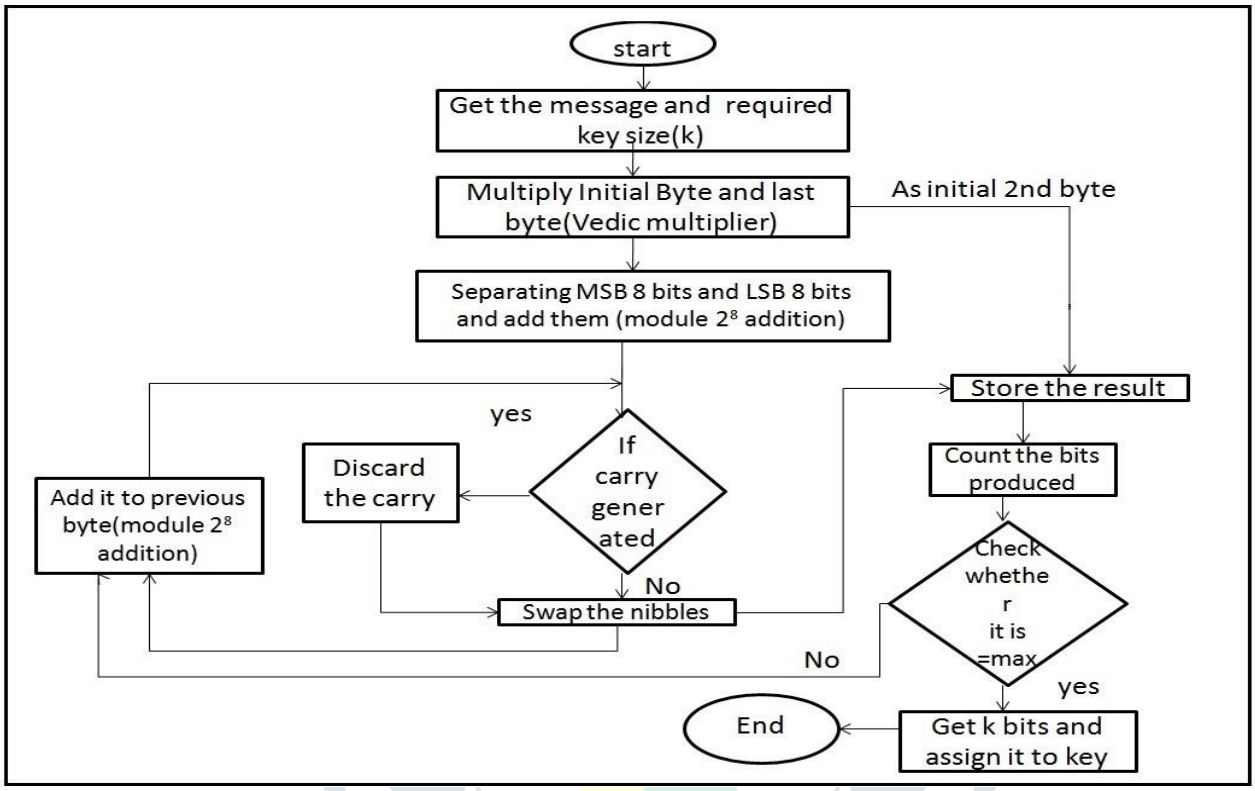

Fig. 3.2 Proposed Flow chart of Public key generator

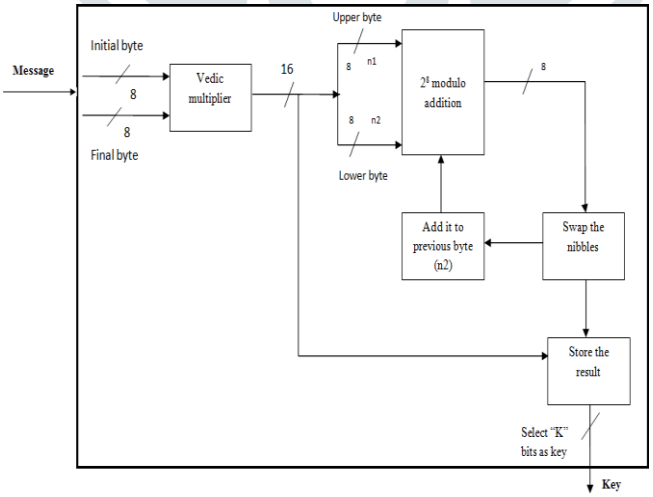

Fig. 3.3 Proposed block diagram of Public key generator

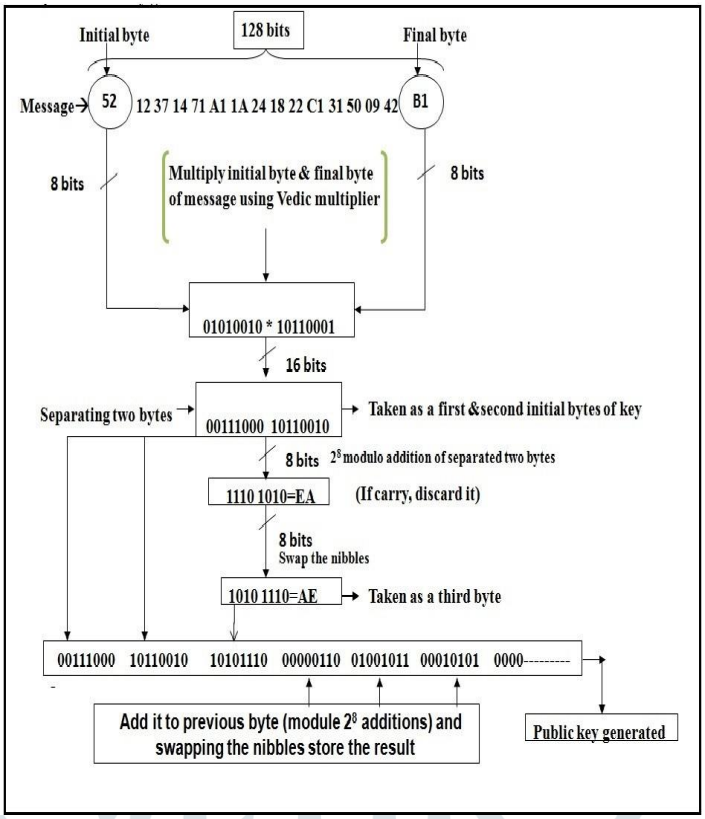

Fig. 3.4 Example of Public key generator

3.2 Reversible implementation of public key generator

The basic components of system are 8X8 bit Vedic multiplier and 2^8 modulo addition. The 2X2 Vedic multipliers are basically built and used for 4X4 multiplier. These 4X4 Vedic multipliers are instantiated in 8X8 multiplier. Basically Feynman gate is used for copying and concatenation, Peres gate for half adder implementation, TR gate for subtraction, Taffoli gate for multiplication and MTS for ripple carry adder. There are 16 sutras in Vedic mathematics. For Vedic multiplier in this work Urdhva Tiryakbhyam sutra is used which is alike array multiplication, but when number of bit increases, compared to other multiplier gate delay and area increases slowly. So the advanced method is called Nikhilam sutra can be used for this[18] and is implemented in our concept. 8X8 Vedic multiplier is shown in Figure 3.5, which takes 1st and last byte of our message, produces 2 byte output.

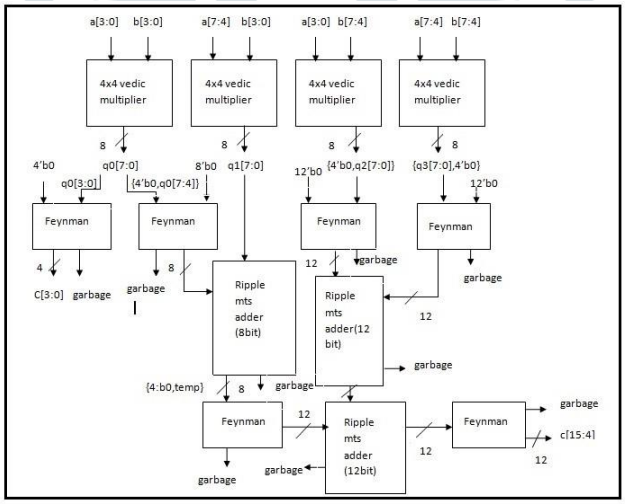

Fig. 3.5 Block diagram of 8X8 Vedic Multiplier

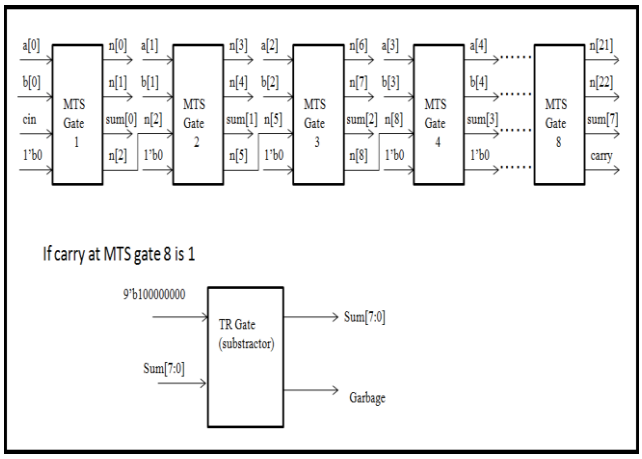

Fig. 3.6 Block diagram of modulo adder

2^8 modulo adder is build using MTS gate, input to this unit are two 8 bit numbers. They are added and if carry generated the sum is subtracted from 9'b100000000 using TR gate else the sum is directly taken for further steps. Reversible implementation of 2^8 modulo adder is as shown in Figure 3.6.

3.3. Proposed Private key generator

The unit uses 9-bit LFSR as shown in Figure 3.7 to produce 511 combinations and reversible block diagram is shown in Figure 3.8 using Feynman reversible gate. The basic concept behind private key generator is on reset LFSR is given with 9 selected bits of message. When reset equal to 0, LFSR produces 511 combinations, each combinations are stored and concatenated to produce the private key. Private key is considered as OTP (one time password) here, as we are using 9 bit LFSR ,4096 bits private key can be generated i.e. 1024 digit OTP can be produced. Proposed flow chart of private key generator is shown in Figure 3.9. The basic unit of private key generator is LFSR, is built using Feynman gate. Example of private key generator is shown in Figure 3.10.

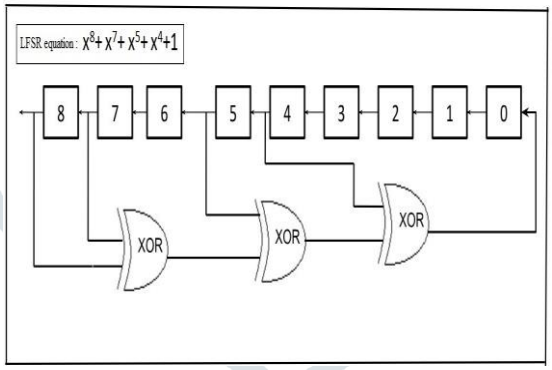

Fig. 3.7 Basic 9 bit LFSR

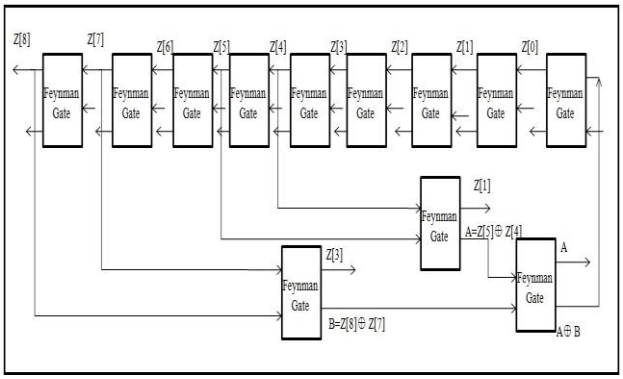

Fig. 3.8 Proposed block diagram of 9 bit reversible LFSR

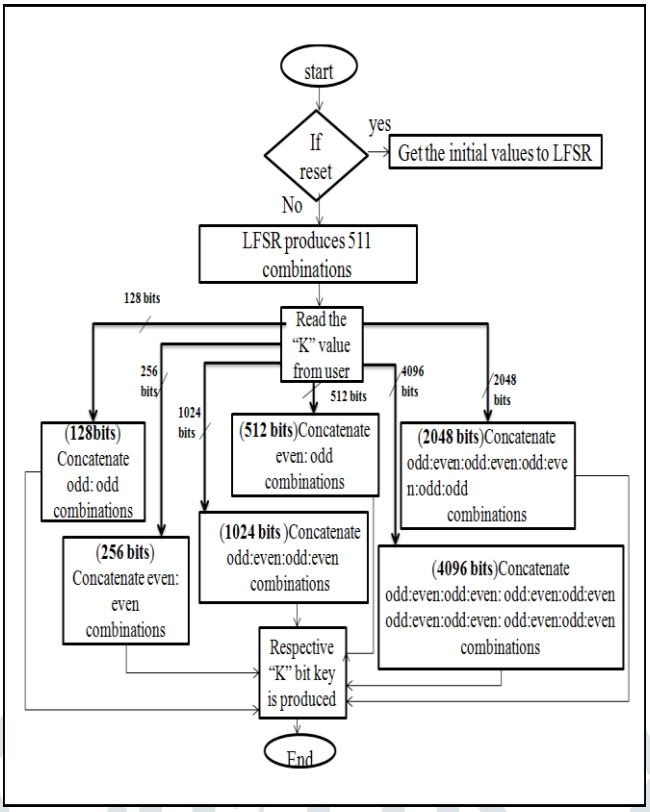

Fig. 3.9 Proposed flow chart of Private key generator

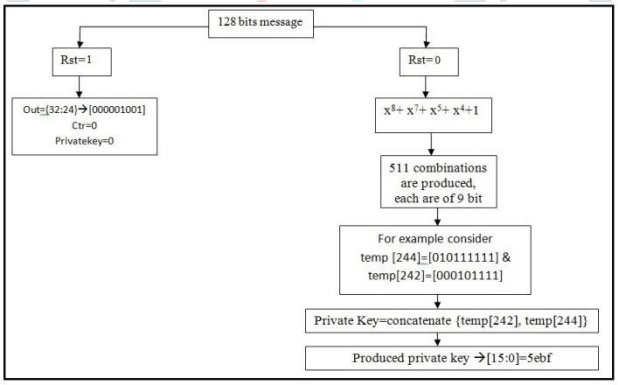

Fig. 3.10 Example of Private key generator

3.4 Proposed Asymmetric encryption module

Asymmetric algorithm uses both above generated keys, public key for encryption and private key for decryption. The logarithmic and exponential steps of basic asymmetric encryption are not considered in proposed algorithm as to reduce Shores and Groves attacks.

Message and public key are considered, set of operation are carried out as shown in proposed algorithm flow Figure 3.12 and fed to 8 bit LFSR as a initial value on reset. Basic LFSR is as shown in Figure 3.11. When reset is 0, 255 combinations are produced each are of 8 bit. These values are stored in a memory of size 16X16. This is one part of encryption module and memory.txt file is generated, refer Figure 3.12. The second part of module is, take each byte of message as address to the memory, fetch vale at that location as encrypted message to that respective byte as shown in Figure 3.13. and hide.txt le is generated, which is our encrypted data. The basic component of encryption module is 8 bit LFSR and is converted to reversible by using Feynman gate.

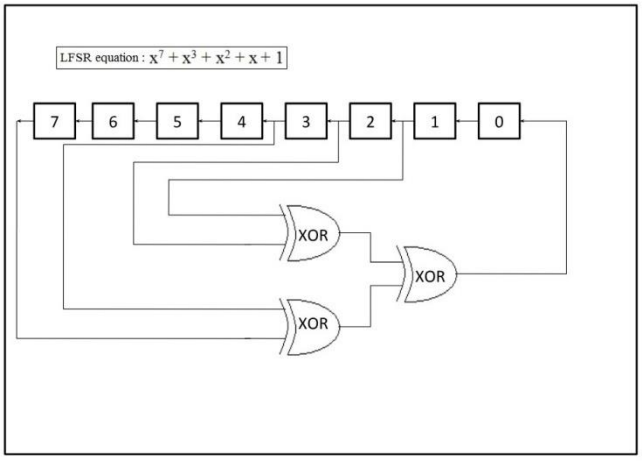

Fig. 3.11 Basic LFSR 8 bit

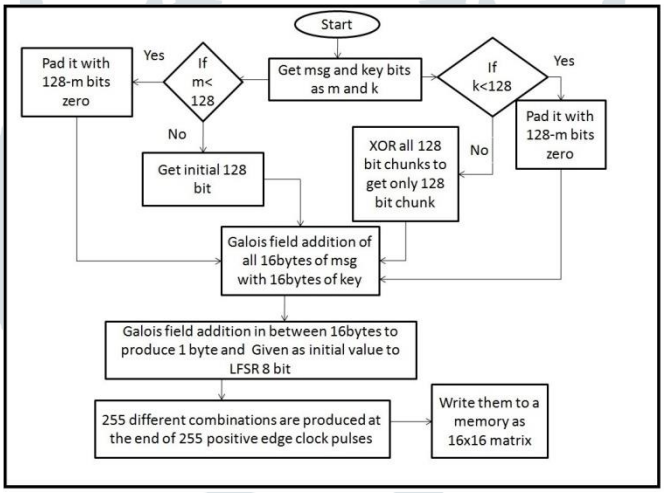

Fig. 3.12 Proposed Flow chart of Encryption module part 1

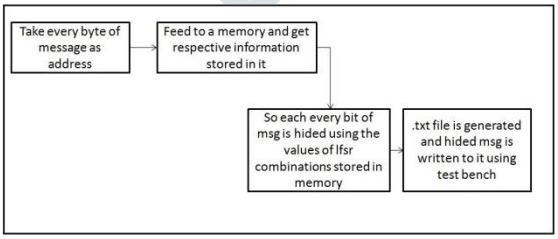

Fig. 3.13 Proposed Flow chart of Encryption module part 2

3.5 Proposed Asymmetric decryption module

Private key which is generated is considered and the OTP given by user are compared. If they are equal, decryption process is carried out or else "OTP is not valid" message is displayed. Encrypted message is taken from hide.txt, byte by byte it is checked for which row and column that value is present. The value of row and column indirectly gives the message back. Flow chart of proposed decryption are as shown in Figure 3.14.

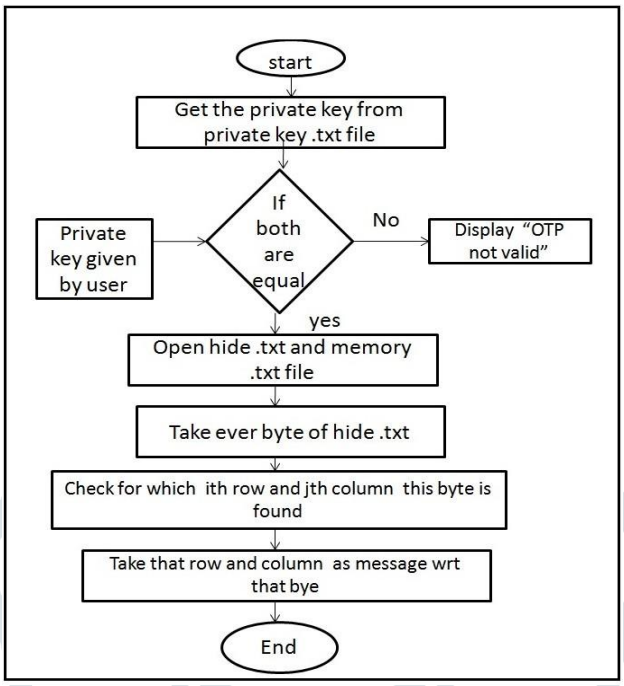

Fig. 3.14: Proposed Flow chart of Decryption module

IV. RESULTS

Proposed Public key, private key, encryption and decryption algorithms are converted to reversible design. The whole is coded using Verilog and verified using Xilinx 14.2 ISE suit. Prototyping is modeled on Virtex 5 FPGA board. Message of 128 bit 2b7e151628aed2a6abf7158809cf4f3c is given, public key is generated of 128 bit 0a14e15f0436a39d041ae1bf0a9c6a60 as shown in Figure 4.1. Private key with 16 bit i;e 5ebf is generated as shown in Figure 4.2. The same message is encrypted to produce encrypted data 71324c988e5a17a24bb64cf73b22f2c7 as shown in Figure 4.3 and decrypted back to 2b7e151628aed2a6abf7158809cf4f3c as shown in Figure 4.4. If the OTP generated by encrypter is 5ecf and OTP given by user is 9122 , then the message cannot be decyrpted back as the OTPs of encrypter and user does not match. Example of OTP not matched is shown in Figure 4.5. Coding is also extended to verify 1024bit encryption and decryption operation and depicted in Figures 4.6 & 4.7 respectively.

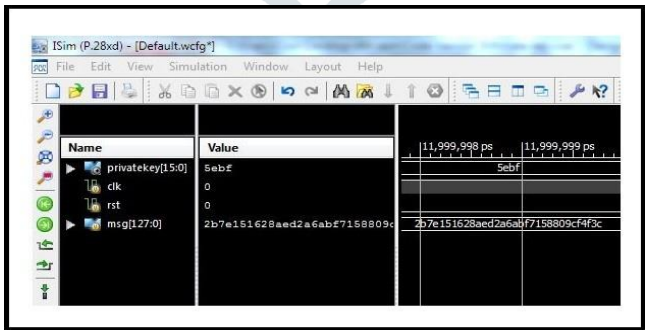

Fig. 4.1 128bit Public key

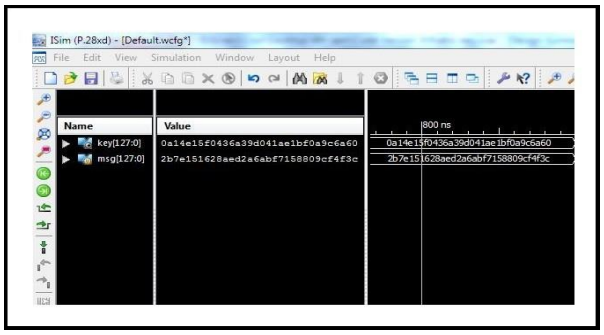

Fig. 4.2 Example of Private key 16 bit

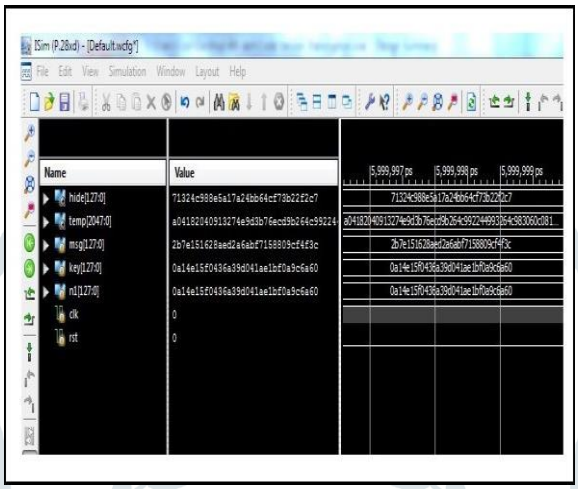

Fig. 4.3 Example of Encryption

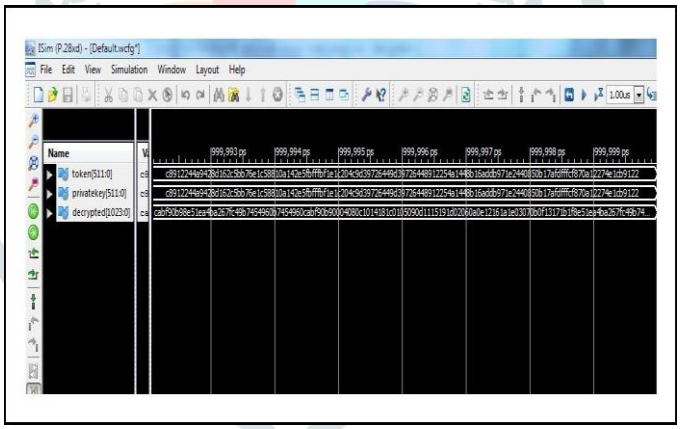

Fig. 4.4 Example of Decryption

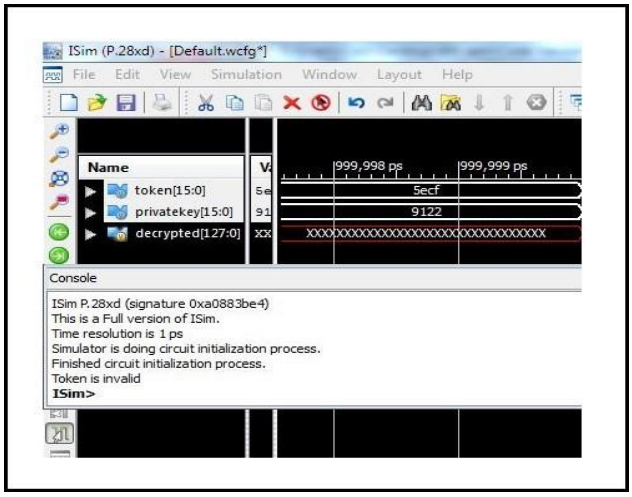

Fig. 4.5 Example of Decryption when OTPs do not match

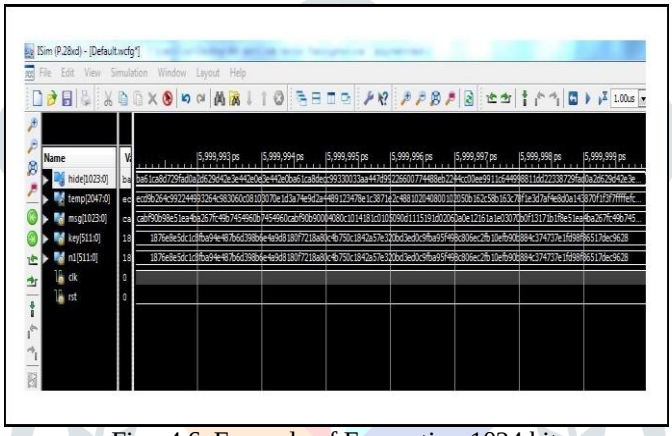

Fig. 4.6 Example of Encryption 1024 bit

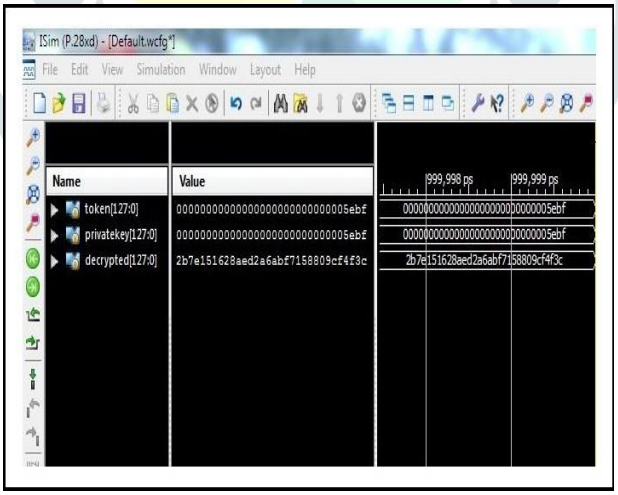

Fig. 4.7 Example of Decryption 1024 bit

Performance parameter like, reversible gate used, numbers of reversible gates used, number of ancilla inputs, number of garbage outputs and quantum cost of reversible circuit with respect to 128 bits message, 128 bits public key and 16 bits private key. Public key generator analysis is shown in Table 1 with respect to 128 bits. Private key generator analysis is shown in Table 2. Table 3 and IV shows analysis of hardware required for both encryption and decryption module respectively.

Table 1
Analysis of Public key generator

Gates used	No of gates	Garbage	Ancilla	Quantum cost
Taffoli	1	2	1	5
Peres	1	2	1	4
Feynman	12	12	12	12
MTS	12	36	12	72
TR	1	2	1	5

Table 2
Analysis of Private key generator

Gates used	No of gates	Garbage	Ancilla	Quantum cost
Feynman	2048	2048	2048	2048
MTS	8	24	8	48
FRG1	3	6	3	12
NOT	1	0	0	1

Table 3
Analysis of Encryption Module

Gates used	No of gates	Garbage	Ancilla	Quantum cost
Feynman	2048	2048	2048	2048

Table 4
Analysis of Decryption Module

Gates used	No of gates	Garbage	Ancilla	Quantum cost
Feynman	16	16	16	16

V. CONCLUSION

To overcome the security issues and counter act the attacks by future computers, this work proposes a new idea, where random keys, both public as well as private keys are generated using two different algorithms and are implemented using reversible logic. Message dependent key generation unit is made dynamic to make it robust, Next, an attempt is made to propose method to post quantum asymmetric algorithm to overcome Shore's attacks. Performance parameter like, numbers of reversible gates used, number of ancilla inputs, number of garbage outputs and quantum cost of reversible circuit are summarized and discussed. Further work can be extended to explore for reliability and security tests.

REFERENCES

[1] W. Diffie and M.E. Hellman, "New Directions in Cryptography," IEEE Transactions on Information Theory, vol. 22, Jun. 1976, pp.638-654.
[2] X. Yang, H.H. Chen, X. Du and M. Guizani, "Stream-based Cipher Feedback Mode in Wireless Error Channel," IEEE Transactions on Wireless Communications, vol. 8, issue 2, Feb. 2009, pp. 622 – 626
[3] Security Requirements for Cryptographic Modules: FIPS PUB 140-2, Information Technology Laboratory National Institute of Standards and Technology, http://csrc.nist.gov, May 2001
[4] D. Bishop,"Introduction to Cryptography with java™ Applets, Jones and Bartlett Publishers Inc., USA, 2003
[5] R. Oppliger, "Contemporary Cryptography", Artech House Inc., 2005
[6] W. Stallings, Cryptography and Network Security, Fourth Edition, Principles and Practices, 2005.
[7] C.A. Henk and V. Tilborg, Encyclopedia of Cryptography and Security, Springer, 2005

[8] Yi-Fung Huang, Fang-Yie Leu, Ko-chung Wei, " Constructing a Secure Point-to Point wireless environments by Integrating Diffie-Hellman PKDS and stream ciphering" International conference on complex, intelligent and software intensive systems, 2010

[9] Ray A Perlner and David A Cooper, "Quantum resistant public key cryptography: a survey," In Proceedings of the 8th Symposium on Identity and Trust on the Internet, pages 85 93. ACM, 2009

[10] H. Wang, Z. Song, X. Niu, and Q. Ding. "Key generation research of RSA public cryptosystem and matlab implement," In PROCEEDINGS OF 2013 International Conference on Sensor Network Security Technology and Privacy Communication System, pages 125 129, May 2013

[11] Yaqeen S.MezaaP, Dalal A. Hammood2, Mohammed H, "OTP encryption Enhancement based on logical operations" *2016 I(ICDIPC)*, Beirut, 2016, pp. 109-112.

[12] Rohini H, Rajashekar and P. Kumar, "Design of basic sequential circuits using reversible logic," 2016 International conference on Electrical, Electronics and Optimization techniques(ICEEOT), Chennai, 2016, pp. 2110-2115

[13] Hans-Joachim Muschenborn, "Symmetric and asymmetric encryption method with arbitrarily selectable one-time keys," December 19, 2002. US Patent App. 10/161,723

[14] Tannu Bala and Yogesh Kumar," Asymmetric algorithms and symmetric algorithms," A.Artur K Ekert. Quantum cryptography based on bell's theorem. Physical review letters, 67(6):661, 1991

[15] R. Landauer, "Irreversibility and Heat Generation in the Computational Process," IBM Journal of Research and Development, 5, pp. 183-191, 1961.

[16] Omer K Jasim Mohammad, Sa a Abbas, El-Sayed M El-Horbaty, and Abdel-Badeeh M Salem. Innovative method for enhancing key generation and management in the AES- algorithm. arXiv preprint arXiv:1504.03406, 2015

[17] H. Wang, Z. Song, X. Niu, and Q. Ding. Key generation research of RSA public cryptosystem and matlab implement. In PROCEEDINGS OF 2013 International Conference on Sensor Network Security Technology and Privacy Communication System, pages 125 129, May 2013

[18] BS Premananda, Samarth S Pai, B Shashank, and Shashank S Bhat. Design and implementation of 8-bit vedic multiplier. International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, 2(12):5877 5882, 2013

[19] L. O. Mailloux, C. D. Lewis II, C. Riggs and M. R. Grimaila, "Post-Quantum Cryptography: What Advancements in Quantum Computing Mean for IT Professionals," in *IT Professional*, vol. 18, no. 5, pp. 42-47, Sept.-Oct. 2016

[20] S. Gajbhiye, S. Karmakar, M. Sharma and S. Sharma, "Paradigm shift from classical cryptography to quantum cryptography," *2017* International Conference on Intelligent Sustainable Systems (ICISS), Palladam, 2017, pp. 548-555

[21] M. Farik and S. Ali, "The Need for Quantum-Resistant Cryptography in Classical Computers," 2016 3rd Asia-Pacific World Congress on Computer Science and Engineering (APWC on CSE), Nadi, 2016, pp. 98-105

[22] J. Li *et al*., "A Survey on Quantum Cryptography," in Chinese Journal of Electronics, vol. 27, no. 2, pp. 223-228, 3 2018

[23] Rohini H, Rajashekar S: Design of Reversible logic based combinational circuits. Communications on Applied Electronics (CAE),Sept 2016, Vol 5, pp. 38-43.

[24] Rohini S H, Jyoti R H, Rajashekar B. S: Reversible Logic Based Modified Design of AES-CBC Mode. Seventh International conference on Advanced electrica Measurement & instrumentation Engineering (EMIE), 13,14 July 2018, pp.171-176.

[25] Rohini S. H, Nikhita M, Pooja A, Rajashekar B. S: Performance Analysis of AES-128bits,192bits & 256bits using reversible logic. Seventh International conference on Advanced electrica Measurement & instrumentation Engineering (EMIE), 13,14 July 2018, pp.165-170.

[26] Rohini H,Jyoti H, Rajashekar S: An Approach towards Design of N-bit AES to enhance Security using Reversible logic. Communications on Applied Electronics (CAE),Sept 2016, Vol 7, pp. 7-13.

[27] R. Landauer, , "Irreversibility and Heat Generation in the Computational Process," IBM Journal of Research and Development, 5, pp. 183-191, 1961.

[28] C.H. Bennett, "Logical Reversibility of Computation," IBM J.Research and Development, pp. 525-532, November 1973.