ENCRYPTION AND DECRYPTION OF A SIGNAL USING FULLY HOMOMORPHIC ALGORITHM

Mr. Dr. S. Dola Sanjay.S,
Professor & H.O.D, Dept of ECE, NRI Institute of Technology, Visadala, Guntur, A.P,India

B. Ankammarao,
B. Tech Students, NRI Institute of Technology, Visadala, Guntur, A.P, India

G.Laksmi Kanth,
B. Tech Students, NRI Institute of Technology, Visadala, Guntur, A.P, India.

B. Sireesha,
B. Tech Students, NRI Institute of Technology, Visadala, Guntur, A.P, India

D.Bargav
B. Tech Students, NRI Institute of Technology, Visadala, Guntur, A.P, India.

ABSTRACT: *Due to privacy leakage of sensitive data, the conventional encryption systems are not completely secure from an intermediary service like cloud servers. The Homomorphic encryption is a special kind of encryption mechanism that can resolve the security and privacy issues. Unlike the public key encryption, it has three security procedures, i.e., key generation, encryption and decryption. In this project, design and implementation of homomorphic encryption and decryption using hybrid finite field Elliptic Curve (EC) architecture is presented. Initially, original bits and key is assigned to the processor and expanded serially. Next, bits are substituted using S-Box. After that shifting and mixing operation is performed. Now these bits are encrypted. Here, a high-performance hybrid elliptic curve point multiplication is used by the efficient finite-field arithmetic unit in affine coordinates, where elliptic curve point multiplication is the key operation of an Elliptic curve based Cryptographic (ECC) processor. Similarly, decryption process is reverse to this operation. Hence elliptic curve point multiplication based Homomorphic encryption and decryption is implemented and it gives better security compared to exist one. The proposed design is synthesized in field-programmable gate array (FPGA) technology with the VHDL. This system will provide better security, resource efficiency and high performance compared to existing standards. This elliptic curve based Homomorphic encryption technique guarantee both privacy and integrity.*

***KEYWORDS**: Cryptography, Homomorphic Encryption, Field-Programmable Gate Array (FPGA), Elliptic Curve Based Cryptographic) ECC Processor.*

INTRODUCTION

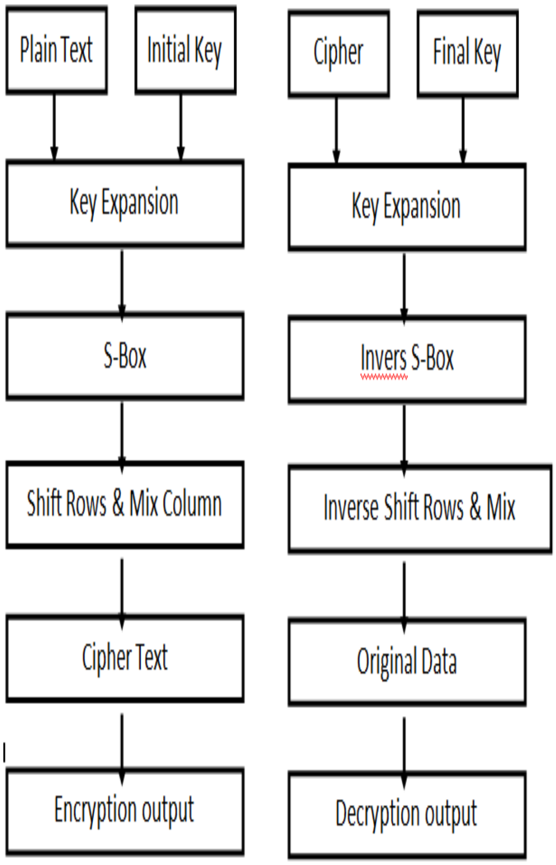
The confidential and private data through an internet or computer networks, there is a chance of getting threats to integrity of data, data confidentiality and availability of data because it provides the worldwide communication. The data integrity, data confidentiality and authentication can be maintained by the data encryption. In everyday of life, information become most important advantage in the growing of demand and it is need for storing the every single event significance. Securing of messages is necessity from unauthorized party's. To protect the information from public accesses an Encipherment is used and it is the one of the security mechanism. The original content of a message can be hiding with the help of encryption, so it cannot be readable for everyone except a person who has special ability to read it. In older days, the meaning of cryptography is, the secret keys are only used by the encryption and decryption, but nowadays cryptography can be defined in various methods such as asymmetric key encipherment it also known as a public key cryptography as well as symmetric key encipherment it also called as a private key cryptography. Therefore computation time is more high in public key algorithm and it is quite complex. Moreover, a single key can be used for both decryption and encryption in the private key algorithms whereas, 2 keys are used in public key algorithm that is one key is used for encryption and another key is used for decryption.

The privacy and security are the significant concepts for creating the basis of various democracies throughout the world. An ensuring privacy model and securing personal information are the major issues to be concern primarily in the digital age. At first sight, an online websites are receive the information of a person by their first name and send the emails to them, when they recommends goods services or adding their desired goods based on their previous visits and demographic profile and so on. A person can surfing in internet and find the privacy drawbacks of various services. They are "Is there a way to ensure the security of this information? Who else is being provided this information? Where does all that 'private information' go? What happens with the information if the company meets financial difficulties and has to liquidate its assets?"

PROPOSED SYSTEM

The 512-bit plaintext is Exclusive-ORed with initial key in initial round. In each cipher round, key expansion, S-Box, ShiftRows() and MixColumns() transformations are performed on a two dimensional 4×4 array of bytes known as states. Each XORed byte is substituted by in the S-box (Substitution box). S-box is one of the basic components of any symmetric key algorithm that exhibits the property of confusion. This property is provided to increase the difficulty in finding the key from the known cipher text. S-box takes m inputs and transforms them to give n bits at the output. Then ShiftRow (Shift) is used to shift the rows of the State over different offsets. After shifting the rows state is applied to the MixColumn (MixCol) which involves addition and multiplication over G (2n) and can be expressed as a matrix multiplication for each column of the state.

The MixColumn component does not operate in the last round of the encryption algorithm. The transformations in the decryption process perform the inverse of the corresponding transformations in the encryption process. The inverse S-box is applied to each byte of the state which obtained by applying the inverse of the affine transformation and is followed by taking the multiplicative inverse in GF(2n). InvShiftRows transformation is performed in the last three rows of the state are cyclically shifted over a different number of bytes.



KEY EXPANSION

Based on 512– bit initial key the key expansion module generates 512 - bit keys for algorithm each round. The module of key expansion contains SubBytes, ShiftRows and RoundConst functions. Bitwise XOR operation is performed by Roundconst function utilizing round constant array. The Roundconst array consists values, that are given as [X^{i-1}, {00}, {00}, {00}]with X^{i-1} being powers of x (x denoted as {02}) in the field GF(2^8). Hence each round key is column wise generated using Eq.(1).

$$N(r,c) = \{ \begin{matrix} N(r-1,c) + sbox[Rword(N(r \\ -1, c+3)] + Rcon(r-1) \\ N(r, c-1 + N(r-1,c) \end{matrix}$$

(1)

In Eq.(1), N(r, c) denotes cth 32-bit column of rth round key, where 1 c 4 and r > 1. The initialkey (r = 1) is XORed with input plaintext of 128-bit before the first round.

RESULTS

The Xilinx design environment was used to implement and examine the developed algorithm. The FPGA architecture of proposed algorithm is shown in Fig. 5.1 and Fig. 5.2. The below Fig. 5.1 and Fig. 5.2 show the RTL schematic and technology schematic of Proposed Homomorphic cryptography algorithm. RTL schematic is the combination of inputs and outputs. Register-transfer logic deliberation is utilized in equipment portrayal dialects (HDLs) like Verilog and VHDL to make elevated level portrayals of a circuit, from which lower-level portrayals and at last genuine wiring can be determined. Structure at the RTL level is run of the mill practice in present day advanced plan.

The combination of Look up tables, K-Map, Truth Tables & equations is the Technology schematic. The Fig. 6.2 represents the proposed system Technology schematic. After optimization & technology targeting phase of synthesis process the Technology schematic was generated. Schematic showing the design in terms of optimized logic elements for the Xilinx target device or example, the logic elements are carry logic, I/O buffers, LUTs & other specigied technology components.

CONCLUSION

In this project, VLSI implementation of highly secured homomorphic cryptography algorithm was proposed. First, the S-box values are generated by the PN Sequence Generator. Based on PN Sequence Generator the required initial key for encryption/decryption is generated. Then private key & public key can shifts the bits in one clock cycle. Depending on the hybrid finite field Elliptic Curve Cryptography (ECC) Homomorphic

$c = 1$

$2 \le c \le 4$

encryption and decryption was performed. For performing ECPD & ECPA operations an efficient polynomial – basis inversion and multiplication was developed & hence ECC processor. Within the estimated core area the EC proposed system was synthesized. The homomorphic cryptography was synthesized in FPGA technology with the VHDL experimental results, and this system provides security in efficient way & it is faster than CPU. The ECC proposed processor taken small amount of FPGA resources. Based on the overall performance analysis it can be concluded that this design provides better performance than others in terms of the area and the timing.

FUTURE SCOPE

The main aim of this project to enhance the security measures of the social and confidential information of the user, By upgrading this project we can implement for quantum computing and machine learning and major computing of data, And we can also upgrade the project and give all the security required to the user ,And we can implement in cloud computing and medical fields also.

REFERENCES

[1] *J. M. Pollard, "The fast Fourier transform in a finite field" Math. Comput., vol. 25, no. 114, pp. 365–374, 1971.*

[2] *J. A. Solinas, "Generalized mersenne numbers," Blekinge College Technol., Karlskrona, Sweden, Tech. Rep. 06/MI/006, 1999.*

[3] *W. Wang, Y. Hu, L. Chen, X. Huang, and B. Sunar, "Exploring the feasibility of fully homomorphic encryption," IEEE Trans. Comput., vol. 64, no. 3, pp. 698–706, Mar. 2015.*

[4] *X. Cao, C. Moore, M. O'Neill, E. O'Sullivan, and N. Hanley, "Optimised multiplication architectures for accelerating fully homomorphic encryption," IEEE Trans. Comput., vol. 65, no. 9, pp. 2794–2806, Sep. 2016.*

[5] *Y. Doröz, E. Öztürk, and B. Sunar, "Accelerating fully homomorphic encryption in hardware," IEEE Trans. Comput., vol. 64, no. 6, pp. 1509–1521, Jun. 2015.*

[6] *Y. Doröz, E. Öztürk, and B. Sunar, "A million-bit multiplier architecture for fully homomorphic encryption," J. Microprocessors Microsyst., vol. 38, no. 8, pp. 766–775, Nov. 2014.*

[7] *W. Wang, X. Huang, N. Emmart, and C. Weems, "VLSI design of a large-number multiplier for fully homomorphic encryption," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 22, no. 9, pp. 1879– 1887, Sep. 2014.*

[8] *X. Feng and S. Li, "Design of an area-effcient million-bit integer multiplier using double modulus NTT," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 25, no. 9, pp. 2658–2662, Sep. 2017.*

[9] *H.-F. Luo, Y.-J. Liu, and M.-D. Shieh, "Efficient memory-addressing algorithms for FFT processor design," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 23, no. 10, pp. 2162–2172, Oct. 2015.*

[11] *C. Moore, N. Hanley, J. McAllister, M. O'Neill, E. O'Sullivan, and X. Cao, "Targeting FPGA DSP slices for a large integer multiplier for integer based FHE," in Proc. Int. Conf. Financial Cryptography Data Secur., 2013, pp. 226–237.*