International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 1 | ISSN : 2456-3307

Design a Finite Field Multiplier for Novel Cryptography

[1]Yaramala Vyshnavi, [2]Bala Nagi Reddy
[1]M. Tech-Scholar, Department of ECE, Pace Institute of Technology and Sciences, Ongole, Andhra Pradesh, India
[2]Associate Professor, Department of ECE, Pace Institute of Technology and Sciences, Ongole, Andhra Pradesh, India

ABSTRACT

The process to develop a federal information processing standard for the advanced encryption algorithm to replace the data encryption standard. In this paper, we proposed an efficient VLSI architecture for advanced encryption standard design methodology in order to provide a high-speed and effective cryptographic operation. High-performance and fast implementation of proposed multiplication is applied to cryptographic systems. The internal multiplier contains three stages of operations. They are pre-processing stage, carry generation stage, post-processing stage. The pre-processing stage concentrate on propagate and generate, carry generation stage focuses on carry generation and post-processing stage focuses on final result. In this paper, we propose efficient and high speed architectures to implement cryptography using proposed multiplier. Cryptography is the operation in wireless communication between transmissions and receiving of data, the secured data is communicated in an unsecured channel between transmitter and receiver with high security. At the transmitter side the original data is converted in to secured sequence and at the receiver side the secured sequence is converted in to original data sequence. Our proposed multiplier is used in that conversion and by using this converter we are designing a cryptography application.

Keywords : Advanced Encryption Standard, Cryptographic Systems.

I. INTRODUCTION

According to Moore's Law, for every two years the number of transistors on a chip almost doubles. For more power density and more heat on the circuits, complicated designs can be implemented on the chip. In security technologies public Key cryptography is popular and most significant one.

It can provide certain unique security Services, such as key exchange and digital Signature. As mentioned above public's key Cryptography is used for the purpose of Security, they are two types (1) RSA (2) Elliptic curve. EC cryptosystem uses shorter key compared with RSA to provide the same level of Security EC used in an EC crypto system is defined over finite field's low-power Design of finite field arithmetic provides results in an EC cryptosystem. It consumes low power and more suitable for wireless application.

For hardware implementation binary Extension field denoted by GF is very attractive because it offers carry free arithmetic. There are various methods to represent field Elements in GF such as polynomial basis (PB) normal basis, and dual basis. The most popularly used basis is PB because it is adopted as one of the basis choices by organizations that set standards for cryptography applications. For efficient implementation of multipliers over GF generalized PB have been proposed. The choice of the irreducible polynomial P(x) affects the complexity of a finite field multiplier.

Irreducible polynomials have less number of non-zero terms. Irreducible polynomials can provide multipliers with lower capacity. PB finite field multiplier architectures can be categorized into bit – serial bit parallel and digit serial architecture. Bit serial architecture is area efficient, and it is too slow for many applications. Bit –parallel is fast and expensive in term of area. The digit serial architecture is flexible, it has moderate speed and reasonable cost of implementation. Two low-energy digit serial PB multipliers have been proposed binary tree structure of XOR gates are used instead of a linear array of XOR gates far degree reduction, reduce both power consumption and delay. Various digit serial multipliers were proposed Such as most significant digit, least Significant digit with modifications in architecture. A factoring technique is involved in design of a digit serial PB multiplier in GF.

II. EXISTED SYSTEM

A finite Field is defined as set of finite many elements where addition and multiplication are the operations. A binary extension field GF (2m) is generated by a degree m irreducible polynomial,
P(x) = x m +pm-1 x m -1 + ------p2 x2 +p1x+1.
P1 is either O or 1.

Dynamic power consumption in CMOS based design consists of a large number of standard cells and nets. It can be expressed as p dynamic = p switching + p internal

Pswitching is the total switching power which Obtained by souring over all nets [a net is a connection to the cells inputs as outputs]. Switching power is the power dissipated due to the charging and discharging of the output load capacitance of a cell. P internal is the total internal power obtained by summing over all cells. The internal power of each cell is the power consumed within the cell because of the charging and discharging of internal nodes capacitances of a cell and short circuit nearest dynamic power (P dynamic) can be reduced by lowering P switching or p internal. The effective method to reduce power consumption is factoring applicable for both architecture and gate level.

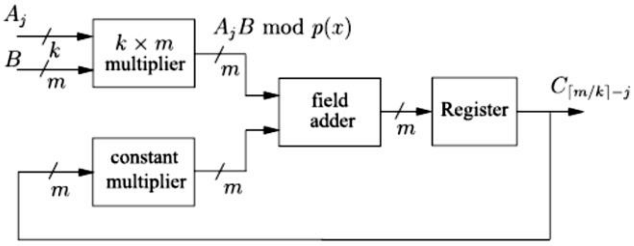


FIG. 1 Finite Field Multiplier

An architecture Diagram for digit serial PB multiplier in GF is shown in fig 1. There are three Modules those are k x m multiplier, and field adder. K x m Multiplier has two Operands one operand B of m-bit and others operand A j of k-bit. A j Changes for different clock cycles j. Therefore it has higher switching activity when compared with operand B.

Constant multiplier module realizes multiplication between a field element and the constant xk field adder modules implements finite field addition using in m two –input XOR gates formed as a one layer network. Among these three k x m multiplier is the most complex module. By using this multiplier we proposed cryptography for security applications in communications.

III. PROPOSED SYSTEM

The operation of cryptographic protocol is point multiplication. The implementation of point multiplication is done by separating into three distinct layers (1) finite filed arithmetic (2) elliptic curve point addition (3) point multiplication technique. Finite field arithmetic can be designed into any hardware implementation accelerator for finite field arithmetic which is performed in the higher level functions of elliptic curve point arithmetic. Along with program and data memory, the three components are arithmetic logic unit (AU), an arithmetic unit controller (AUC) and a main controller.

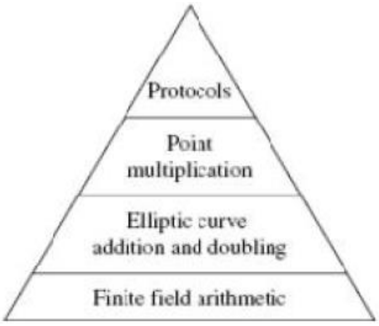


FIG. 2 Hierarchy Of Operations In Cryptography

The Arithmetic logical Unit (AU) functioning is to perform the basic field operation of addition, squaring, multiplication, and inversion, and it is controlled by the AUC. The functioning of AUC is to execute the elliptic curve operation of point addition and doubling. The micro controller coordinates and executes the method chosen for point multiplication and interacts with the lost system.

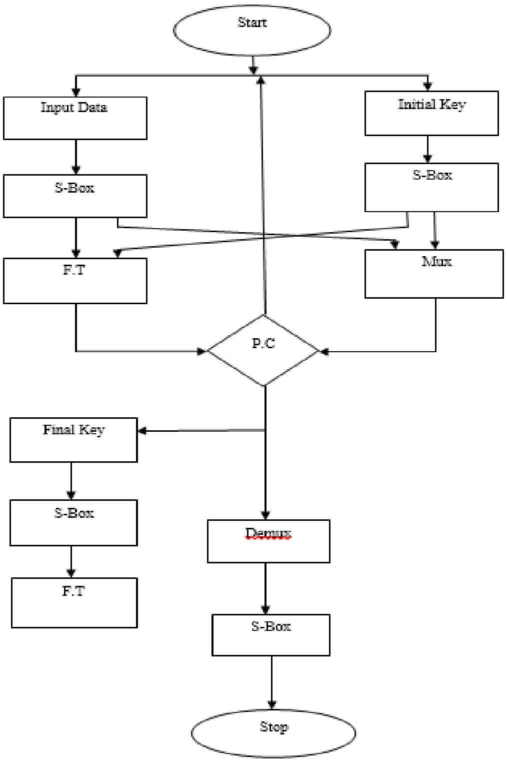


FIG. 3 Algorithm

In the proposed system the total input bits are converted into s-box and initial key is converted into s-box. The two s-boxes are created at a time and then the data from two s-boxes are given to F.T and mux. The mux consisting of finite filed arithmetic, elliptic curve point addition and point multiplication technique. The F.T and mux outputs are mapped to parseval's checks, the checking operation of errors is over come in this parseval's check block and finalized output encryption data is send to decryption block.

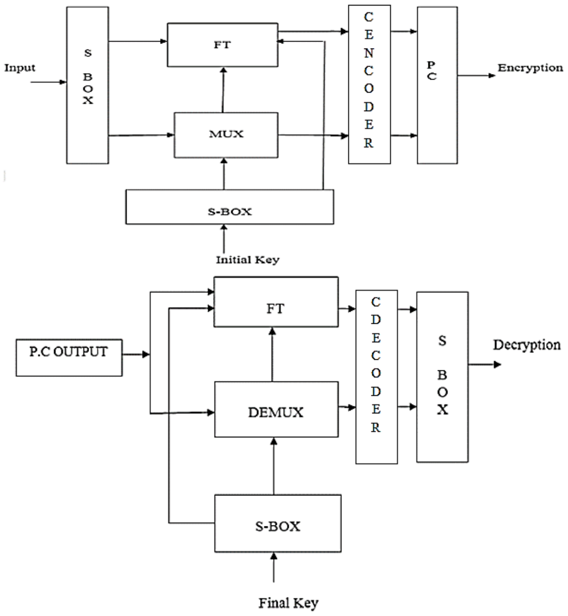


FIG. 4 Proposed Cryptography

The decryption block takes P.C outputs and they are given to I.F.T and de-mux. The total data is done the inverse operations of mux and encrypted F.T block. The total data from de-mux and I.F.T is given to sbox to store the decrypted data.

IV.RESULTS

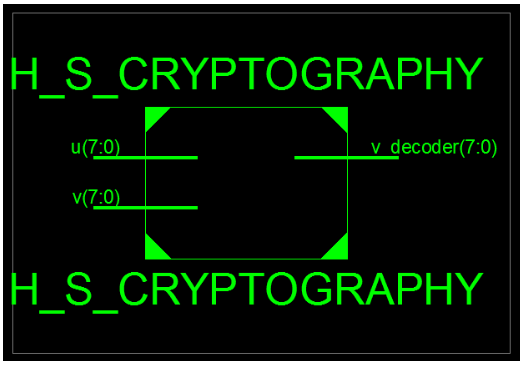
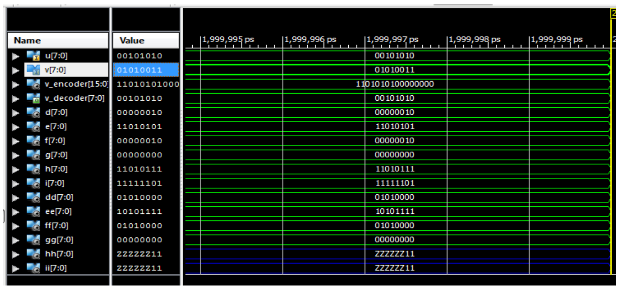


FIG 5. RTL Schematic



Name	Value	
u[7:0]	00101010	00101010
v[7:0]	01010011	01010011
v_encoder[15:0]	11010101000	1101010100000000
v_decoder[7:0]	00101010	00101010
d[7:0]	00000010	00000010
e[7:0]	11010101	11010101
f[7:0]	00000010	00000010
g[7:0]	00000000	00000000
h[7:0]	11010111	11010111
i[7:0]	11111101	11111101
dd[7:0]	01010000	01010000
ee[7:0]	10101111	10101111
ff[7:0]	01010000	01010000
gg[7:0]	00000000	00000000
hh[7:0]	ZZZZZZ11	ZZZZZZ11
ii[7:0]	ZZZZZZ11	ZZZZZZ11

FIG 6. Output Waveform

IV. V.CONCLUSION

In this paper, we propose an efficient VLSI architecture for advanced encryption standard design methodology in order to provide a high-speed and effective cryptographic operation. High-performance and fast implementation of proposed multiplication is applied to cryptographic systems. The internal multiplier consists of three stages of operations to focuses on final result. We proposed efficient and high speed architectures for implementing cryptography using proposed multiplier. Cryptography is the operation in wireless communication between transmissions and receiving of data, the secured data is communicated in an unsecured channel between transmitter and receiver with high security. The total proposal is done in XILINX 14.7 with Spartan 3E family.

V. REFERENCES

[1]. Shoaleh Hashemi Namin, Huapeng Wu, Senior Member, IEEE, and Majid Ahmadi, Fellow, IEEE "Low-Power Design for a Digit-Serial Polynomial Basis Finite Field Multiplier Using Factoring Technique" IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS,1063-8210 © 2016 IEEE

[2]. T. Kean, "Cryptographically Enforced Pay-Per-Use Licensing of FPGA Design Intellectual Property", Proceedings International Workshop on IP Based Design 2002.

[3]. B., Soudan, W. Adi, and A. Hanoun, "Novel SecretKey IPR Protection in FPGA Environment," Proceedings System-on- Chip Conference, September 2005.

[4]. Kahng , A. B., Kirovski , D., Mantik, ., Potkonjak, M., and Wong, J. L., "Copy Detection for Intellectual Property Protection of VLSI Design." Proc. IEEE/ACM Intl. Conference on Computer-Aided Design, November 1999, pp. 600-604.

[5]. Newbould, R. D., Carothers, J. D., Rodriguez, J. J., and HolmanW. T., "A Hierarchy Of Physical Design Watermarking Schemes For Intellectual Property Protection Of IC Designs," Proceedings of the International Symposium on Circuits and Systems, 2002, Vol. IV, pp. 862 - 865

[6]. Technical discussions with Rich Goldman, Vice President, Strategic Alliances, Synopsys. November 2005.

[7]. Actel, "ProASIC3/E Security," Application Note available at http://www.actel.com, cited on 14/4/2005.

[8]. T. Kean, "Cryptographically Enforced Pay-Per-Use Licensing of FPGA Design Intellectual Property", Proceedings International Workshop on IP Based Design 2002.

[9]. W. Adi , Fuzzy Modular Arithmetic for Cryptographic Schemes with Applications to Mobile Security EUROCOM 2000.

Authors

YARAMALA VYSHNAVI completed her B.Tech at RISE Prakasam Group of Institutions and pursuing M.Tech at Pace institute of technology and sciences, Ongole. Her area of interest is VLSI.

YARAMALA VYSHNAVI completed her B.Tech at RISE Prakasam Group of Institutions and pursuing M.Tech at Pace institute of technology and sciences, Ongole. Her area of interest is VLSI.