IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 12, Issue 4, Ver. II (Jul.-Aug. 2017), PP 74-77
www.iosrjournals.org

Elliptic Curve Scalar Multiplication over GF (2^m) using Karastuba Algorithm

*Smitha A B[1], Sachin C N Shetty[2], Shikha[3]
[1](Electronics & Communication Engineering, Sahyadri College of Engineering& Management, India[2](Assistant Professor Electronics & Communication Engineering, Sahyadri College of Engineering & Management, India)
[2](Assistant Professor Electronics & Communication Engineering, Sahyadri College of Engineering & Management, India)
Corresponding Author: Smitha A B

Abstract: *Cryptography offers high security for communication and networking. Elliptic Curve Cryptography (ECC) provides similar level of security to conventional integer-based publickey algorithms, but with much shorter keys. ECC over binary field is of special interest because the operations in binary field are thought more space and time efficient. It replaces RSA because of its increased security with lesser number of key bits. This paper proposes an efficient pipelined architecture of elliptic curve scalar multiplication (ECSM) over GF(2^m). The architecture uses a bit-parallel finite field (FF) multiplier accumulator (MAC) based on the Karatsuba-Ofman algorithm. The most important operation in Elliptic Curve Cryptosystem is the computation of scalar multiplication using Karatsuba-Ofman multiplier.The implementation of the elliptic curve scalar multiplication is achieved by using a Galois Field arithmetic simulated on Xilinx ISE 10.1.*

Keywords: *Cryptography, Elliptic curve cryptography, Karastuba-Ofman Multiplier, Scalar Multiplication, Galois field*

Date of Submission: 17-07-2017 Date of acceptance: 28-07-2017

I. Introduction

Enormous data such as credit card numbers and social security numbers are transmitted over the Internet during transactions. Thousands of transactions take place over the world-wide web day by day. Securing electronic transaction has become a very important problem. Cryptography can be used to provide and assure confidentiality and integrity of such transactions and it is an efficient way to protect and secure information. Cryptography is science concerned with providing secure communications. The goal of cryptography is to construct schemes which allow only authorized access to information. All malicious attempts to access information are prevented. An authorized access is identified by a cryptographic key. A user having the right key will be able to access the hidden information, while all other users will not have access to the information. There are two types of cryptographic algorithms such as symmetric key and asymmetric key algorithms. Symmetric key cryptographic algorithms have a single key for both encryption and decryption.It can be used only when the two communicating parties have agreed on the secret key. This could be a hurdle when used in practical cases as it is not always easy for users to exchange keys. In asymmetric key cryptographic algorithms two keys are involved-a private key and a public key. The private key is kept secret while the public key is known to everyone. Elliptic Curve Cryptography (ECC), which is an asymmetric algorithm,is gaining attraction as with their high level of security with low cost, small key size and smaller hardware realization. Elliptic curve scalar multiplication (kP), where k is a scalar (integer) and P is a point on the curve, is the most important operation in elliptic curve cryptosystems. Scalar multiplication consists of elliptic curve group operations such as point addition and point doubling. The elliptic curve group operations perform finite field operations like field addition, filed multiplication, field squaring, field division and modular reduction. Asymmetric encryption uses a separate key for encryption and decryption. Anyone can use the encryption key (public key) to encrypt a message. However, decryption keys (private keys) are secret. This way only the intended receiver can decrypt the message. The key exchange algorithm provides a method of publicly sharing a random secret key. Security of these algorithms depends on the hardness of deriving the private key from the public key.

II. Preliminaries

2.1 Finite Field

Elliptic curves are defined over FFs. The most commonly used FFs are prime fields GF(p) and binary fields GF(2^m). Both canprovidethesame levelofsecurity.Because arithmetic in GF(2^m) is carry-free, ECC over GF(2^m) is more efficient for hardware implementation. Elements in GF(2^m) have many basis representations,

among which polynomial basis and normal basis are the most commonly used ones. Normal basis has cheaper FF square but much more complex FF multiplication than polynomial basis. Here, we consider ECC over GF(2^m) with polynomial basis. In polynomial basis, elements in GF(2^m) are represented as binary polynomials with degrees less than m, i.e., $a(x) = \sum_{i-0}^{m-1} a_i x^i$ $a_i \in [0,1]$. Arithmetic operationsinGF(2^m) are computed over an irreducible polynomial f(x) with degree m. Addition a(x) + b(x) in GF(2^m) is bitwise EXCLUSIVE OR (XOR) between coefficients of two polynomials. Multiplication $a(x)\cdot b(x)$ in GF(2^m) is more involved, which is performed in two steps: 1) polynomial multiplication and 2) reduction modulo f(x). Square $a^2(x)$ is cheaper than multiplication, because the polynomial multiplication in square is simply padding zeros to the odd bits. Inversion $a^{-1}(x)$, which is the most complex operation in GF(2^m), is to find a polynomial b(x) that satisfies $a(x)\cdot b(x) = 1$ for a givena(x).

2.2 Elliptic Curve Scalar Multiplication

A nonsupersingular elliptic curve over GF(2^m) is represented as follows

$$E : y^2+xy= x^3+ax^2+b.$$

Points on elliptic curve E, along with the point at infinity, form a commutative finite group under point addition and doubling. Given a base point P on the curve, and a positive integer k, computing

$$Q = kP = P + P\ldots\ldots\ldots\ldots..+P$$

(K times)

is called scalar multiplic… result Q is another point on the elliptic curve. Scalar multiplication is performed by repeated point addition and doubling, which essentially rely on a series of FF arithmetic, such as multiplication, square, addition, and inversion. Point addition and doubling in affine coordinate involve inversion each time. As inversion is the most complex and time-consuming operation in FF, it is more practical to represent curve points using a projective coordinate.

III. Proposed Architecture Of Elliptic Curve Scalar Multiplication

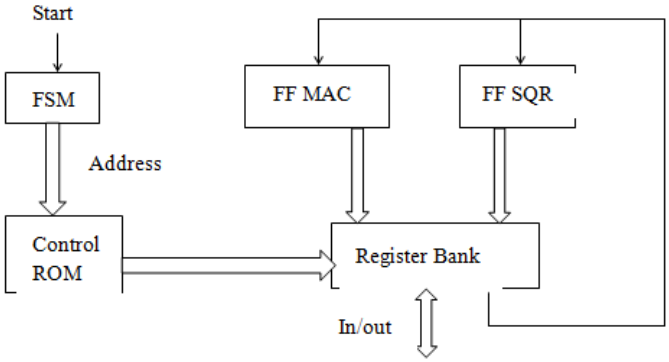

Fig 1 Proposed block diagram of ECSM

The proposedECSM architectureconsists of one bit-parallel FF MAC, one FF squarer, a register bank, a finite-state machine, and a 6 × 18 control ROM. The FF MAC is implemented using the Karatsuba–Ofman algorithm, and is well pipelined. The n-stage pipelined FF MAC takes n clock cycles to finish one multiplication. The FF squarer is not pipelined, and one clock cycle is required to finish one square.

The scalar multiplication is done using Lopez-Dahab (LD) Projective co-ordinate system. The LD coordinate form of elliptic curve over finite field is,

$$Y^2 + xyz = x^3 + ax^2y^2 + bz^4$$

The curve constant b and base point P are stored in ROM. a is taken as 1. Initially the curve constant and base points are loaded from ROM into registers. There are two phases of computation. During first phase scalar multiplication takes place. The scalar k is multiplied to base point. During second phase projective point result from first phase is converted to affine co-ordinate kP. Second phase involves inversion which is done using Itoh-Tsujii inverse algorithm. The register bank consists of eight registers of size 233 bits each. The registers are used to store results of computations. Multiplexers associated with register bank determines which of the inputs are to be stored in the register banks. It also determines which output of a register bank gets driven on the output buses.

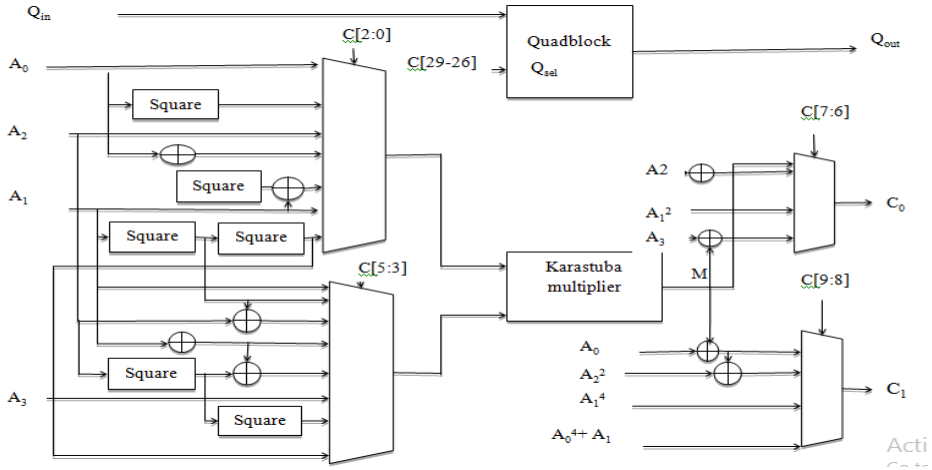

Fig 2 ECSM using Finite Field Arithmetic Unit (FF MAC)

3.1Karatsuba-Ofman (KOM) algorithm for Finite Field Multiplier Accumulator

Karatsuba algorithm is considered to be the one of the fastest way to multiply long integers. It is based on divide and conquer strategy. Let a and b are the two long integers to be multiplied. In Karatsuba algorithm, these polynomial operands are split into two as higher order bits and lower order bits. That is a is divided to a_h and $a_l$and b as $b_h$and b_l

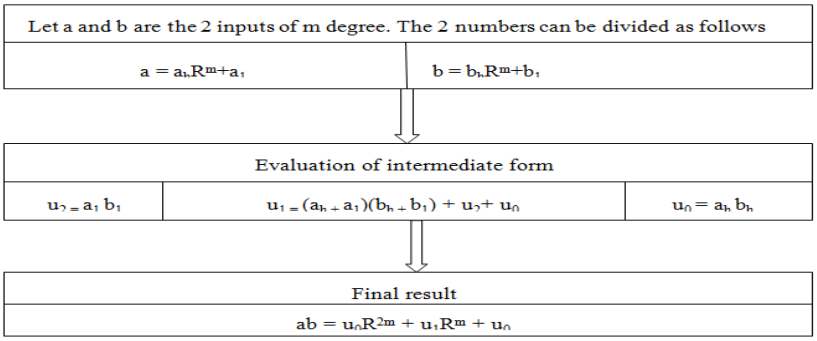

Fig 3 Karatsuba Multiplication Flow Chart

The Karatsuba algorithm is applied recursively for the three m/2 bit multiplications $a_1\, b_1$, $(a_h + a_1)(b_h + b_1)$ and $a_h b_h$.Each recursion reduces the size of the input by half, while it triples the number of multiplications. After several recursions, the number of small multipliers becomes significant. Initially the Karatsuba multiplier splits the input operands to produce threshold operands.It consists of threshold level multipliers and recursively combines the outputs from threshold level multipliers and does the modular reduction

IV. Result

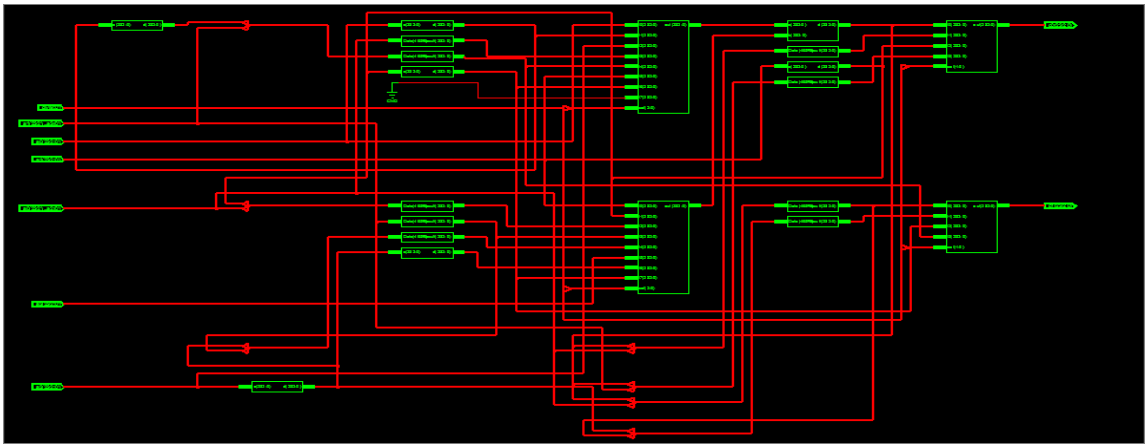

Fig 4 RTL view of Arithmetic Unit

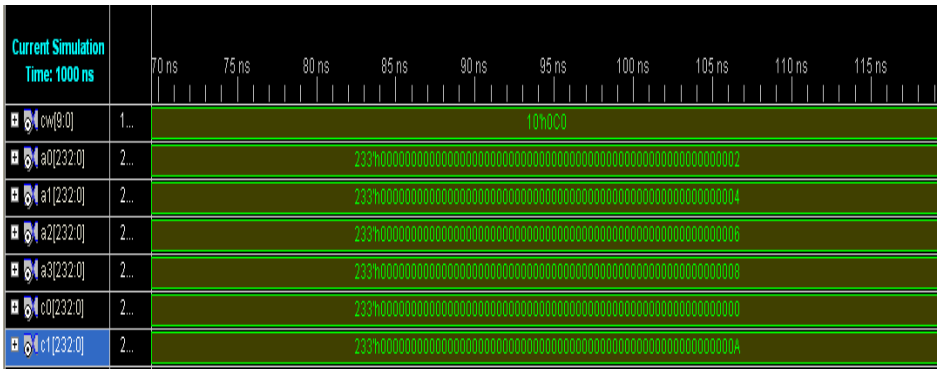

Fig 5 Output of ALU

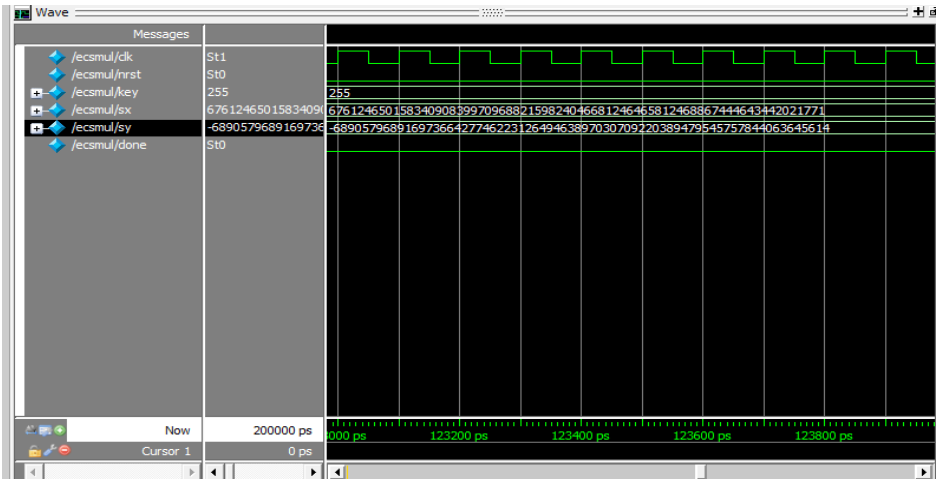

Fig 6 Output of ECSM

V. Conclusion

The arithmetic unit is used in a Elliptic Curve Crypto Processor to compute the scalar product kP. This design has more efficient FPGA utilization .High speed is obtained by implementation of quad and squarer circuits. The Quad ITA algorithm is used to reduce computation time. We use carry look ahead adder in ALU because it is faster than any other adder. It will generate and propagate the carry so that computation time requirement is less. Also the area and power requirements are less in this design. The most important factor contributing the performance is the finite field multiplication and finite field inversion.

References

[1] Lijuan Li and Shuguo Li, Member, IEEE "High-Performance Pipelined Architecture of Elliptic Curve Scalar Multiplication Over GF(2^m)" IEEE Transactions On Very Large Scale Integration (VLSI) Systems, Vol. 24, No. 4, April 2016

[2] F. Rodríguez-Henríquez, N. A. Saqib, A. D. Pérez, and Ç. K. Koç, "Cryptographic Algorithms on Reconfigurable Hardware". New York, NY, USA: Springer-Verlag, 2006

[3] E. Wenger and M. Hutter, "Exploring the design space of prime field vs. binary field ECC-hardware implementations," in Proc. 16th Nordic Conf. Secure IT Syst. Inf. Security Technol. Appl. (NordSec), Tallinn, Estonia, Oct. 2011, pp. 256–271

[4] P. H. W. Leong and I. K. H. Leung, "A microcoded elliptic curve processor using FPGA technology," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 10, no. 5, pp. 550–559, Oct. 2002

[5] W. N. Chelton and M. Benaissa, "Fast elliptic curve cryptography on FPGA," IEEE Trans, Very Large Scale Integr. (VLSI) Syst., vol. 16, no. 2, pp. 198–205, Feb. 2008

[6] Ajitha.S.S, Retheesh.D "Efficient Implementation Of Bit Parallel Finite Field Multipliers "IJRET: International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN: 2321-7308

IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) is UGC approved Journal with Sl. No. 5016, Journal no. 49082.

Smitha A B. "Elliptic Curve Scalar Multiplication over GF (2m) using Karastuba Algorithm." IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) 12.4 (2017): 74-77.