Elliptic Curve Cryptographic System Over Binary Galois Field

[1.] Jasmin Salim, [2.] Ajeesh A. V
[1.] PG student, [2.] Assistant professor
TKM Institute of Technology,
Karuvelil P.O, Kollam, Kerala-691505, India

***Abstract*— Cryptography is the most standard and efficient way to protect the security of web transactions. An efficient cryptosystem must be one that is strong enough to ensure a high level of security for reliable transmission of information. Elliptic Curve Cryptography is one such type of public key cryptosystem based on small key size. Elliptic Curve Cryptography is an alternative to traditional techniques for public key cryptography. It can be called the future generation of public key systems since it involves less number of bits suitable for resource constrained and wireless applications without compromising on the security level. The proposed architecture for elliptic curve scalar point multiplication is based on Lopez–Dahab Elliptic Curve Scalar Point Multiplication algorithm.. The design can be coded using VHDL and simulated using ModelSim 6.2C.**

Keywords— ***Elliptic Curve Cryptosystem,FPGA, public key, galois field, scalar point multiplication.***

I. INTRODUCTION

Cryptography is the science of providing security for information. It is the process of encrypting the plain text into an incomprehensible cipher text by the process of Encryption and the conversion back to plain text by process of Decryption. Many information and communication security systems are based on the public key cryptography. Elliptic Curve Cryptography(ECC) is one type of public key cryptography that has become popular due to its superior strength per bit compared to existing public key algorithms such as RSA. As far as cryptographic systems having larger key lengths are concerned, the processing load on applications using such cryptographic systems will be greater. However some devices have limited processing capacity, storage, power supply, and bandwidth like the newer wireless devices and cellular telephones. When using these devices, efficiency of the resource management is very important in these devices. ECC provides encryption functionality requiring a smaller percentage of the resources required by other algorithms. Hence ECC is the best choice of cryptography in these types of devices.

Elliptic Curve Cryptography(ECC) is a crypto-system, suggested independently, by Neals Koblitz and Victor Miller. At present, Elliptic Curve Cryptography has been commercially accepted, and has also been adopted by many standardizing bodies such as ANSI, ISO and NIST. Since then, it has been the focus of a lot of attention and gained great popularity due to the same level of security they provide with much smaller key sizes than the level of security provided by conventional public key crypto-systems. Intuitively, there are numerous advantages of using Field Programmable Gate Array (FPGA) technology to implement in hardware the computationally intensive operations needed for ECC. In particular, performance, cost, efficiency, and the ability to easily update the cryptographic algorithm in fielded devices are very attractive for hardware implementations of ECC.

Elliptic curves are rich mathematical structures that have shown usefulness in many different types of applications[10]. ECC plays an important role in digital Signatures, secure key distribution, and encryption and decryption. In most cases, the longer the key length, the more protection that is provided, but ECC can provide the same level of protection with a smaller key size. ECC makes use of the properties of elliptic curves in their public key systems. The elliptic curves provide ways of constructing groups of elements and specific rules of how the elements within these groups should combine. Elliptic Curve Cryptography is emerging as an attractive public-key cryptosystem for mobile/wireless environments. It results in faster Computations, reduced power consumption, as well as savings in memory space and bandwidth.

II. ELLIPTIC CURVE SCALAR POINT MULTIPLICATION(ECSM)

Scalar point multiplication is by the most important operation in Elliptic Curve Cryptosystems. ECSM is an operation in which, on input an integer *k* and a point *P* on the elliptic curve *C*, computes another point *Q* such *Q=Kp.* In the ECSM architecture proposed, a variant of the algorithm due to Lopez and Dahab algorithm, which is an improvement of the traditional Montgomery ECSM algorithm. The algorithm consists of three stages: 1) conversion of point *P* from affine coordinates to projective coordinates; 2) computation of *Q=Kp* in projective coordinate; and 3) conversion of Q from projective coordinates back to affine coordinates.

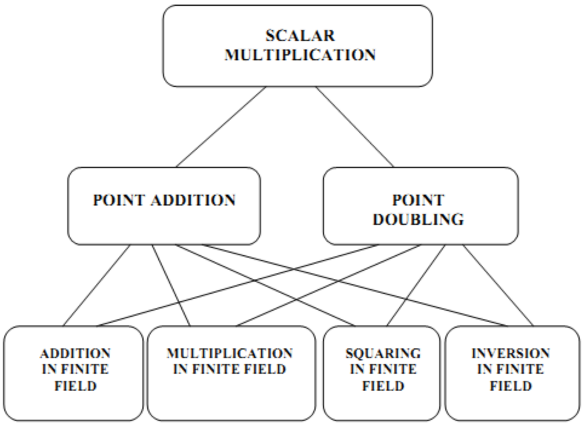

Figure 1: Hierarchy of Elliptic Curve Cryptosystem

The design hierarchy of a typical elliptic curve cryptosystem is shown in the figure 1. Point multiplication is composed of point addition and point doubling. Point multiplication, point doubling and point addition are operations involving with the points on the elliptic curve. Point addition is the process in which two points on an elliptic curve is added to give a third point on the elliptic curve. A line drawn through both these points intersects the elliptic curve in another point. The point where this line intersects with the curve is noted. The negative of this intersection point is used as the result of point addition. Point doubling is achieved by adding a point on the elliptic curve to itself. The bottom level of the ECC system is the galois field arithmetic [6]. The galois field arithmetic involves addition, multiplication, squaring and inversion in galois field. The trapdoor function is achieved by the scalar point multiplication.The strength of ECC security comes from the difficulty of Elliptic Curve Discrete Logarithm Problem. Suppose the points P and Q on an elliptic curve are given, then according to ECDLP, it is difficult to find a number k such that Pk=Q [6].

III. SYSTEM ARCHITECTURE

Elliptic curve cryptographic systems are based on point multiplication which involves time consuming operations like finite field inversion. A scalar point multiplication architecture is proposed in which the number of finite field inversions are reduced. The most important operations for designing an efficient ECC processor are finite field multiplication, finite field inversion and finite field squaring. Field addition and subtraction in GF(2^m) are defined as polynomial addition and can be implemented simply as the XOR addition of the two *m*-bit operands. For the design of the architecture for ECSM, two different parts are considered: the first part involves calculations in the projective coordinate system, and the other part involves the calculations for converting projective coordinates to affine coordinates.

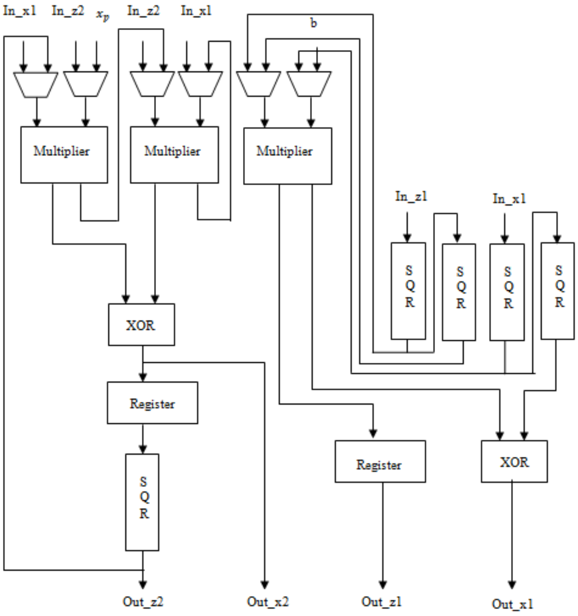

Figure 2. Block diagram of Lopez Dahab Scalar Point Multiplication

The basic block diagram of Lopez Dahab Scalar Point Multiplication is shown in the Figure 2. The architecture of scalar point multiplication proposed here consists of three important blocks. They are namely finite field multiplier, finite field squarer and finite field inverter. These are the most important operations required for performing elliptic curve cryptography. Field addition and subtraction in GF(2^m) are defined as polynomial addition and can be implemented simply as the XOR addition of the two m-bit operands. The galois field chosen here is GF(2^4), where m=4 and there are 16 distinct symbols in this field.

A. *Finite field multiplier*

Several type of multiplier architectures can be used for finite field multiplication. The finite field multiplier used in this system is based on the Shift and Add algorithm. Finite field calculations must be such that any operation that takes place between elements that belongs to the finite field results in an element within the same field. Thus arithmetic in finite field is different from standard integer arithmetic. Finite field multiplication can be achieved if a reduction step is also incorporated in the conventional Shift and Add algorithm [5]. This can be achieved by interleaving the Shift and Add steps with the reduction step.

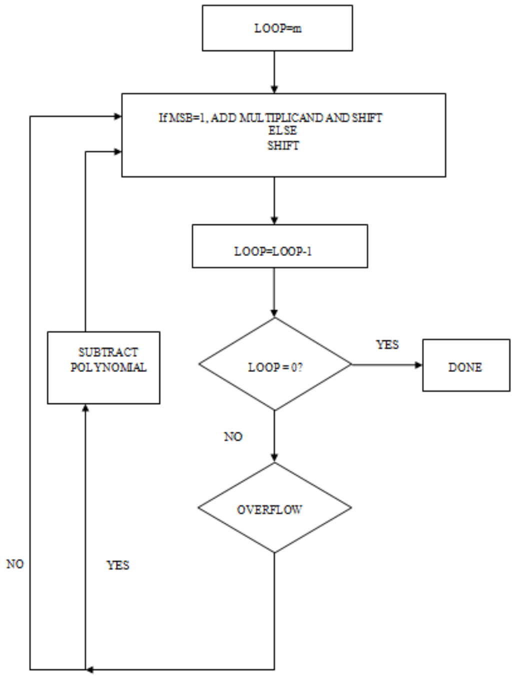

Figure 3. Flowchart of finite field multiplication

An irreducible polynomial is used to perform the reduction step. The irreducible polynomial is unique for each kind of galois field chosen. An irreducible polynomial is a polynomial which cannot be factored into the product of two or more polynomials whose coefficients are of a specified type. Addition in binary galois field is performed by XOR operation. In order to ensure finite field operation, an overflow condition needs to be checked in each iteration along with performing the Shift and Add algorithm.

B. Finite field squarer

Squaring is a particular case of multiplication in finite binary field. Classic squarer is one in which the multiplicand and the multiplier is the same value. Its procedure can be optimized to save the time spent on multiplication.

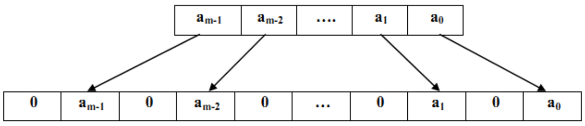

Figure 4. Zeros inserted in am element

However, a squarer can be designed using a more simple method compared to the finite field multiplication. Since squaring a binary polynomial is a linear operation, it is much faster than multiplying two arbitrary polynomials [2]. Similar to the finite field multiplication, a reduction step is also incorporated to achieve finite field square. An element in the chosen galois field can be represented in the following manner.

$$A(x) = a_3x^3 + a_2x^2 + a_1x^1 + a_0x^0 \qquad (1)$$

Zeros are inserted in between the bits of A in order to obtain square of the element A∈GF(2^m).The reduction step must be performed using an irreducible polynomial.

C. Finite Field Inverter

Finite field inversion is much more time-consuming than finite field addition and finite field multiplication and several attempts have been made to carry out this operation fast. In Elliptic Curve Scalar point Multiplication algorithm finite field inversions ae required to perform the calculations to convert projective coordinates back to affine coordinates. The algorithm proposed for multiplicative inversion in GF(2^m) is based on the Fermat's theorem. Fermat’s theorem implies that, since the multiplicative group of the galois field GF(2^m) is cyclic of order $2^m - 1$, then for any non-zero element $a\epsilon$GF(2^m), the finite field inversion of the element denoted as a^{-1} is given by $a^{-1} = a^{2^m-2}$ [9]. The square and multiply algorithm is used here to compute the inverse of an element in finite field.

The three important building blocks needed for scalar point multiplication namely the finite field multiplier, the finite field squarer and the finite field inverter are designed. These blocks are combined to perform the Lopez Dahab algorithm for scalar point multiplication. Elliptic Curve Cryptosystems can make use of this algorithm for public key generation.

IV. CONCLUSIONS

The scalar multiplication operation which is the underlying mathematical operation of elliptic curve cryptography is performed based on the Lopez Dahab algorithm. It is performed in the projective coordinate system; in order to reduce the number of finite field inversions. The x and y coordinates in the affine coordinate system is given as input. These affine coordinates are converted to projective coordinate initially and then the computation of scalar multiplication in projective coordinate is performed. The resulting projective coordinate values are converted back to the affine coordinates.
This gives the public key generation in cryptosystems based on elliptic curves.

REFERENCES

[1] Renuka H.Korti and Vijayalaxmi A.Hiremath, “Implementation of Finite field arithmetic unit for cryptographic applications”, *Proceedings of International conference,* July 2013.

[2] Amar said and Moncef Amara, “Hardware implementation of arithmetic for Elliptic Curve Cryptosystems over GF(2^m)” , *World conf. Internet security*, 2011.

[3] Syed Wasi Alam, Nauman Qureshi, Muhammad Hammad Ahmed and Irum Baig, “Security for Wireless Sensor Network based on Elliptic Curve Cryptography”, *International conference on Computer Networks and Information Technology (ICCNIT)*,2011.

[4] Hero Modares, Yasser Salem, Rosli Salleh and Majid Talebi Shahgoli, “A bit-serial multiplier architecture for finite field over galois field”, *Journal of Computer Science*, 2010.

[5] Rahila Bilal and Dr.M.Rajaram, “High speed point arithmetic architecture for Eliiptic Curve Cryptography on FPGA”, *International journal on Computer science and Engineering (IJCSE)*, Vol.02, No. 06, 2010.

[6] 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.

[7] S. Kummar, T. Wollinger, and C. Paar, “Optimum digit serial GF(2^m) multipliers for curve based cryptography,” *IEEE Trans. Comput.*, vol. 55,no. 10, pp. 1306–1311, Oct. 2006.

[8] K. Jarvinen, M. Tommiska, and J. Skytta, “A scalable architecture for elliptic curve point multiplication,” *in Proc. IEEE Int. Conf. Field-Program,* Dec. 2004,pp. 303–306.

[9] Naufumi Takagi and Kazuyoshi Takagi, “A fast algorithm for multiplicative Inversion in GF(2^m) using normal basis”, *IEEE transactions on computers, Vol.50, No.5,* May 2001.

[10] Julio Lopez and Ricardo Dahab, “ Fast multiplication on elliptic curves over GF(2^m) without precomputation ”, in *Proc. 1st Int. Workshop Crypto-graph. Hardw. Embedded Syst.,* 1999, pp. 316–327.

[11] T. Itoh and S. Tsujii, “A fast algorithm for computing multiplicative inverses in GF(2^m) using normal basis,” *J. Inf. Comput*., vol. 78, no. 3, pp. 171–177, 1998.