An Efficient Way to Implement Scalar Multiplication In Elliptic-Curve Cryptography

Sachin K Sunny
Dept. Electronics and communication
Rajagiri School of Engineering and Technology
Cochin, Kerala, India

Dhanesh M S
Dept. Electronics and communication
Rajagiri School of Engineering and Technology
Cochin, Kerala, India

***Abstract*— Privacy is most required in modern society. Encryption and decryption of data can be done in different ways. Public key cryptography is most widely used in real life applications such as e-banking, military applications, bit coin, IoT application (internet of things). Two major ways to implement public key cryptography is are RSA and Elliptic curve cryptography. An important operation in elliptic curve cryptography is scalar multiplication. There are several ways to implement scalar multiplication. In this paper we use Montgomery algorithm. Some design modification is made such that the system latency is reduced for scalar multiplication is reduced. This system is simulated in Xilinx ISE 14.7 and implemented in Sparten 6 FPGA.**

***Keywords*— IoT, FPGA, ECC, RSA**

I. INTRODUCTION

Cryptography is the combination of encryption and decryption of data. A key is a piece of information that decrypts the cipher. Without the key message cannot be decrypted back. There are so many cryptographic algorithms. They are mainly divided into two categories. Asymmetric cryptography and symmetric cryptography. When different keys are used for both encryption and decryption it is known as asymmetric key cryptography (Public key cryptography). When same key is used for both encryption and decryption it is known as symmetric key cryptography (private key cryptography). Different types of symmetric key cryptographic algorithms are AES (Advanced encryption standard), DES (Data encryption standard). Similarly asymmetric key encryption algorithms are RSA (Rivest, Shamir, and Adleman), ECC (Elliptic curve cryptography).The concept of public key cryptography is mainly discussed here. A comparison between RSA and ECC shows that ECC uses les number of bits and provide same level of security with RSA encryption [2]. ECC consist of several operations, they are mainly field operations and curve operations. Field operations are modular addition and modular division or inversion. Curve operations are point addition and point doubling. Both operations are used in scalar multiplication. There are different algorithms used for scalar multiplication LSB first algorithm [3], MSB first algorithm [3], and Montgomery algorithm [1]. Montgomery algorithm uses two registers and does point addition and point doubling together.

II. BASICS OF CRYPTOGRAPHY

A. *Public key cryptography*

This system uses a pair of keys, public key, which is known to everyone in the communication circle, private key, which are known only to the owner. In public key encryption any person can encrypt message using public key of the receiver. And such message can only be decrypted using receiver's private key. The strength of a public key cryptography system relies on the degree of difficulty (computational impracticality) for a properly generated private key to be determined from its corresponding public key. Only risk is in keeping the private key safe. Public key can be published to everyone. Public key cryptography systems often rely on cryptographic algorithms based on mathematical problems that currently admit no efficient solution particularly those inherent in certain integer factorization, discrete logarithm, and elliptic curve relationships.

Basically two types of public key encryption

- RSA(Rivest, Shamir, Adleman)
- ECC(Elliptic curve cryptography)[5]

A comparison between RSA and ECC is given below

Table 1.Comparison between RSA and ECC

Time to break(years)	RSA/DSA key size	ECC key size	RSA/ECC key size
104	512	106	4.8:1
109	768	132	5.8:1
1011	1024	160	6.4:1
1020	2048	210	9.8:1
1079	21000	600	35:30:1

B. *Elliptic curves*

An elliptic curve E is a graph of an equation of the form [5]

$$Y^2 = X^3 + AX + B \quad (1)$$

Where A and B are constants. This equation is referred to as weierstrass equation for an elliptic curve. This curve is defined over a finite field Fp for a prime p. Example for elliptic curve is drawn in figure 1.

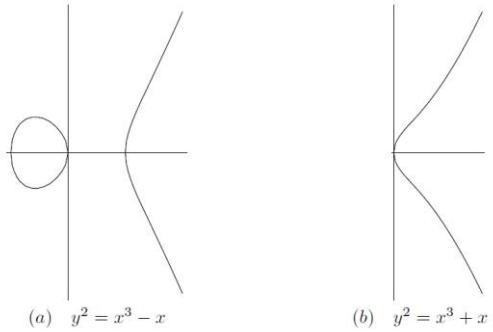

Figure 1 Different types of Elliptic curves

Assume that

$$4\,A^3 + 27\,B^2 \qquad (2)$$

This is used for avoiding multiple roots.

III. CURVE OPERATIONS

There are mainly two curve operations point addition and point doubling start with two points, or even one point, on an elliptic curve, and produce another point [5].

A. Point addition

Whenever two points on the curve are added to find the third point, first draw a straight line passing through that curve. That line meets a third point. From there draw a line perpendicular to x axis. That line meets a point which is the sum of two points. Here P and Q are two points on the curve added to get new point R, shown in figure 2.

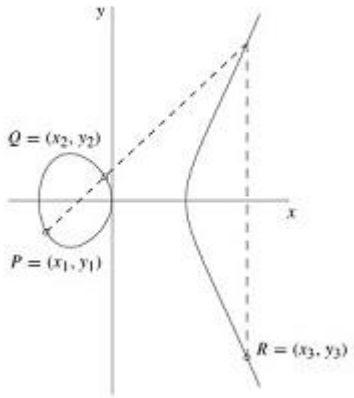

Figure 2. Point addition

B. Point doubling

To find point doubling of a point. First draw a tangent to that point, tangent intersect on a point project it towards x-axis and it meets another point, which is the doubling point. Point doubling of a point P is shown in figure 3

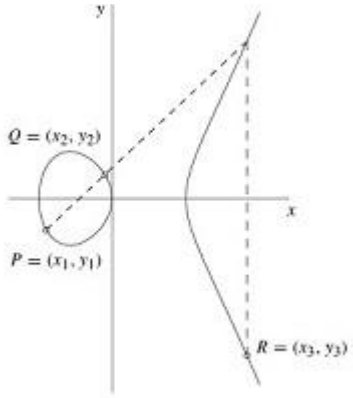

Figure 3. Point doubling

IV. SCALAR MULTIPLICATION

Each and every point of elliptic curve cryptography requires scalar multiplication of a point on the curve. It is the most basic and important unit while implementing ECC. Reducing the time required for doing scalar multiplication is one of the important job. There are many algorithm for implementing scalar multiplication. One of the best algorithm is Montgomery algorithm, which is explained

A. Montgomery Algorithm

This algorithm is the fastest algorithm that find scalar multiplication. In which we can use pipelining which makes the algorithm faster. This algorithm requires more hardware utilization. The algorithm is given as follows [1]

1: Input: K > 0 and P
2: Output Q=K P
3: Set K =$(K_a....K_1,K_o)_2$
4: Set $P_1 = P_1$, $P_2 = 2P$
5: For i from a-2 to 0
6: If Ki=1
7: Set $P_1 = P_1 + P_2$, $P_2 = 2P_2$
8: Else
9: Set $P_2 = P_1 + P_2$, $P_1 = 2P_1$
10: Return Q= P_1

Montgomery algorithm allows pipelining the point addition and point doubling process. That's how montogomery algorithm reduces the computation speed.

V. PROPOSED WORK

This system is designed to reduce the latency of scalar multiplication. For that a single module called scalar multiplication module (SMM) is cascaded to get faster outputs. SMM consist of point addition and point doubling units, which calculates the result which are stored in to registers and then the controller gives corresponding outputs to the next module. The usual scalar multiplication module uses loops which adds more delay. Since here each modules

are cascaded such additional delay can be avoided, which makes the system faster.

The working of scalar multiplication module is shown in figure 4, whole scalar multiplication module with n stage is given in figure 5. Each addition and doubling process require one inversion. Which is the most time consuming process. So number of inversion can be reduced by using projective co-ordinate system instead of affine co-ordinate system.

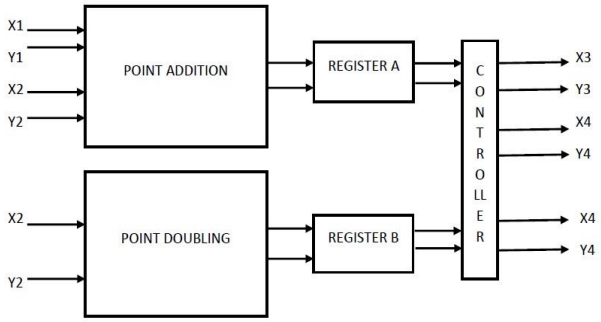

Figure 4. Scalar multiplication module

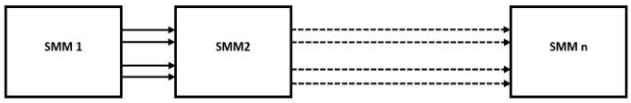

Figure 5. n - Stage Scalar multiplication

VI. RESULTS

The hardware architectures were designed using Verilog HDL. The designs were synthesized and implemented using Xilinx ISE 14.7 for the Xilinx Sparten – 6 target platform, and simulated using Xilinx Isim.

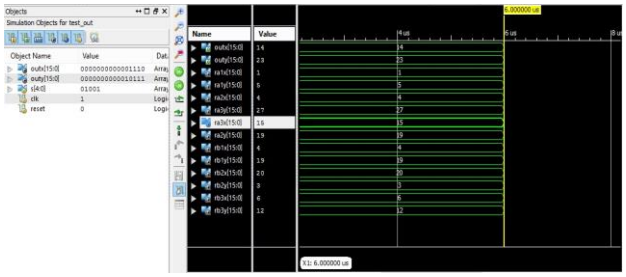

Figure 6. Scalar multiplication simulation

VII. CONCLUSION

Scalar multiplication designs have trade-off between area and speed. Scalar multiplication using Montgomery algorithm is a very powerful technique that reduces the time required to compute the output, which is the main process in Elliptic curve cryptography. Here scalar multiplication unit was designed and synthesized successfully, a 4 stage scalar multiplication is implemented. The latency of the system is decreased since there are no loops. Each stage of scalar multiplication is directly connected to other. 1284 slices are used for implementation. The proposed and demonstrated architecture is very well suited for cryptography.

REFERENCES

[1] Zia-Uddin-Ahamed Khan and Mohammed Benaissa,, "Throughput/Area Efficient ECC Processor using Montgomery Point Multiplication on FPGA," IEEE transactions on circuits and systems, vol. 4(12), pp 1629-1640.2015..

[2] Maryam Savari and Mohammad Montazerolzohour "All about Encryption in Smart Card", Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)}, Pages: 54 - 59(2012)

[3] Douglas R Stinson, Cryptography Theory and Practice, 3.ed canada(2006)

[4] Lawrence C Washington ,Elliptic Curve Number theory and cryptography,3.ed U.S.A(2008).

[5] Neal Koblitz, "Elliptic Curve Cryptosystems",\tMathematics of computation ,48,V-203-209,(1987).