International Journal of Research in Engineering, Science and Management
Volume-3, Issue-1, February-2020
www.ijresm.com | ISSN (Online): 2581-5792

Efficient Design of Elliptic Curve Cryptography based on Montgomery Modular Multiplication

Mahantagouda S. Patil[1], Nagaraj Balashetti[2], H. S. Navitha[3], S. Prerana[4], V. Shalini[5]
[1,2,3,4]*Student, Department of Electronics and Communication Engineering, Atria Institute of Technology, Bangalore, India*
[5]*Assistant Professor, Department of Electronics and Communication Engineering, Atria Institute of Technology, Bangalore, India*

***Abstract*: ECC (Elliptical Curve Cryptography) is the one of the buzzwords in network security. It is one of the best cryptography technique which provides security to our personal as well as professional data over the network. Finite Field arithmetic is one of the widely used operation for multiplication. In this paper we are using finite field multiplier architecture and VLSI implementations are proposed using the Montgomery Modular Multiplication Algorithm. The architecture is used in order to reduce the area and to minimize the time delay.**

***Keywords*: ECC, Galois Field, Montgomery modular multiplier.**

1. Introduction

ECC (Elliptic Curve Cryptography) is a commonly used technique for the cryptography. ECC is an approach to the public key cryptography based on the algebraic structure of elliptic curves over finite fields.

Galois field which is also called as finite field, this contains a finite number of elements. Compare to other field a Galois field is a set on which the operation of multiplication, addition, subtraction and division are defined.

Montgomery Modular Multiplication is one of the fast modular multiplication as a result it is going to reduce the time for multiplication.

2. Literature survey

[1] In ECC, the same level of security as the RSA can be achieved using much smaller key size. The basis of the ECC systems is the hardness of discrete logarithm problem over elliptic curve (ECDLP). in order to reduce the complexities of the arithmetic operations. The elliptic curves can be defined over GF (2 k), GF(q) and GF (p m), where p and q are positive primes, k and m are positive integers. In this study a scalable VLSI multiplication architecture based on Montgomery multiplication (MM) algorithm for elliptic curve cryptography (ECC) over GF (p m), where p is a positive prime and m is the degree of extension of the base field GF(p), is designed. The coefficients of the polynomials are represented in Montgomery residue format to simplify the multiplications over GF(p).

[2] Electronics advancements in the last decades have made communication systems available to everyone. However, to assure the secure transmission of sensitive information through public channels, cryptographic primitives need to be employed. When creating a new application, system engineers need to choose an appropriate public key primitive. Examples of standardized public key cryptosystems are based on RSA and elliptic curve cryptography (ECC). In this study an area-optimized FPGA architecture of the Montgomery modular multiplication algorithm on a low power reconfigurable FPGA is designed. It uses mapping of the Montgomery algorithm to the specific architecture of the target FPGA.

[3] Cryptography has a lot of algorithms, which are hard to break and are having a great deal of computational effort. To achieve cryptography, encryption is the most effective way. So that to access the encrypted file and to decrypt the file, there must be the secret key. Based on the type of key, Encryption is segregated into symmetric encryption and asymmetric encryption or public-key encryption. The strength of public-key cryptography depends on the degree of difficulty of a private key to be determined from its corresponding public key. Such a

Key can be generated from high radix arithmetic operations like modular exponentiation with very large integer values. To perform this modular exponentiation, different multiplication algorithms like Montgomery algorithm, Karatsuba algorithm, VLM3 algorithm are used. In this study, these algorithms results are analyzed and their performance towards measure of algorithm complexity, critical path delay, area, time period and frequency are compared.

[4] Rapid increase in the amount of information transferred via network communications and networks virtually also becoming main pathways for commercial and money transfers. It is a real challenge keeping information secret during communication, also to ensure who are the real sender and receivers. Cryptography techniques based on keys are broadly utilized to undertake these tasks. For secured transmission of data over internet, mobile, wireless in network communication Elliptic Curve Cryptography (ECC) is gaining more acceptances worldwide. In this study design and implementation of a Montgomery multiplier algorithm is implemented and compares it with RSA.

[5] The security of Elliptic Curve Cryptography relies on the difficulty of solving the Elliptic Curve Discrete Logarithm Problem ECDLP. For ECC, we only consider those points which lie in some finite fields. To develop the fast-elliptic curve multiplication, the less known algorithm of Montgomery ladder is used in the computations and this algorithm has full of generality and applies to all abelian groups. In this study improving an algorithm of public key cryptography, Montgomery Ladder, to make an efficient Elliptic Curve point multiplication in terms of area and throughput. This algorithm computes point multiplication on Elliptic Curves such as generic curves in which it is optimized by using parallel multipliers in Digit size architectures.

[6] One of the buzzwords in network security nowadays is the ECC-Elliptical Curve Cryptography. It is one of the best cryptography techniques that provide security to our personal as well as professional data over the network. In our day to day life the need of data sharing has increased exponentially. We like to stay updated with every event occurring around. The need for securing that data has also increased, in order to prevent attacks that may cause unauthorized access to our data, misuse of our data or modification of our data and also to maintain privacy over the network. Thus, sharing the data has to be done in such a way such that only the sender and the receiver understands it and no one else on the network does. In this study two such techniques that encompass not only server and desktop systems, but also large numbers of small devices ranging from PDAs and cell phones to appliances and our data in a way that it becomes senseless to everyone, until it is changed back to its original form in order to make sense.

[7] Montgomery architectures of modular multipliers with one or two bits scanning are described in this paper, Multipliers have been described using hardware description language – VHDL, and implemented on FPGA integrated circuit EP4CE115F29C7. Comparative analysis of multiplier regarding minimum calculation time, maximum operating frequency and number of used logic elements of integrated circuit is given. Based on implemented modules, analysis of RSA module for data encryption is performed.

3. Objectives

1) To design an algorithm for Montgomery multiplication which is highly efficient.
2) Efficiency in terms of power and area consumption is the main objective.
3) The algorithm written deals with the Montgomery multiplication technique which is highly preferred for cryptographic purposes.

4. Block Diagram

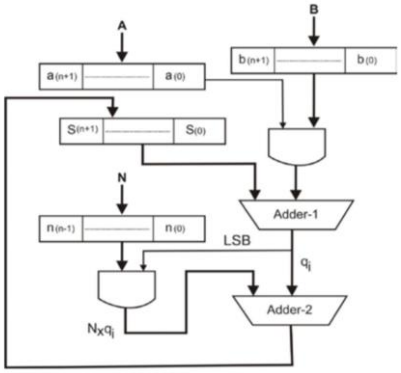

Fig. 1. Architecture

Where, n(x)=f(x) and s(x)=c(x)

5. Algorithm for Montgomery multiplication

Input: a(x),b(x),n(x)
Output: c(x)= a(x) b(x) x^{-k} mod n(x)
Step 1. c(x) = 0
Step 2. for i = 0 to k−1 do
Step 3. c(x) =c(x)+a_ib(x)
Step 4. c(x) =c(x)+c_0n(x)
Step 5. c(x) =c(x)/x

The computation of c(x) involves a regular multiplication in Step 1, a modulo r(x) multiplication in Step 2, and finally a regular multiplication and a division by r(x) operation in Step 3. The modular multiplication and division operations in Steps 2 and 3 are intrinsically fast operations since r(x)=xk. The remainder operation in modular multiplication using the modulus xk is accomplished by simply ignoring the terms which have powers of x larger than or equal to k. Similarly, division of an arbitrary polynomial by xk is accomplished by shifting the polynomial to the right by k places.

The pre-computation of n(x) required in Step 2 constitutes an overhead for computing c(x). However, it turns out the computation of n(x) can be completely avoided if the coefficients of a(x) are scanned one bit at a time.

6. Conclusion

This paper presented an overview on the design of elliptic curve cryptography based on Montgomery modular multiplication.

References

[1] Somsubhra Talapatra and Hafizur Rahaman, “Low Complexity Montgomery Multiplication Architecture for Elliptic Curve Cryptography over GF (p m).”
[2] Pedro Maat C. Massolino, Lejla Batina, Ricardo Chaves and Nele Mentens, Low Power Montgomery Modular Multiplication on Reconfigurable Systems,” ICIS 2016.
[3] Poomagal C. T. and Sathish Kumar G. A., “Modular Multiplication Algorithm in Cryptographic Processor: A Review and Future Directions,” IJACE, Feb. 2017.

[4] Rajesh Bhadada and Aditi Sharma, "Montgomery implantation of ECC over RSA on FPGA for Public Key Cryptography application," 2014.
[5] Anita Aghaie, "Efficient Elliptic Curve Point Multiplication with Montgomery Ladder Algorithm."
[6] Ansah Jeelani Zargar and Mehreen Manzoor, "Encryption/Decryption using Elliptic Curve Cryptography," IJARCS, August 2011.
[7] Velibor Skobic, Branko Dokic, and Zelijko Ivanovc, "FPGA Implementation of Montgomery Modular Multiplication, 2014.