# Galois Field based Montgomery Multiplier for RSA Cryptosystem using Area Efficient Adder

Ritu Gupta
ECE Department
MANIT, Bhopal

Kavita Khare, PhD
ECE Department
MANIT, Bhopal

## ABSTRACT
Data security is the major point of concern in today's internet communication system for which cryptography plays a vital role. Modular multiplier plays a key role in modern cryptography system. Galois field arithmetic is being popularly used in such applications. Montgomery multiplication is the method for boosting up the speed of modular multiplication. Montgomery modular multiplier is implemented for larger operand size to design encryption and decryption algorithm for RSA security system. This paper contributes to the implementation of modular multiplier using Montgomery algorithm for RSA encryption and decryption ,where existing architecture is implemented using carry select adder and modified carry select adder and it is concluded that later uses 23% less area and approximate 4.5% less output delay as compared to former, in VHDL using Xilinx ISE 9.2i and has been simulated on FPGA device spartan3, xc3s200-5ft256.

## Keywords
Carry select adder, Montgomery algorithm, RSA cryptography, modular arithmetic.

## 1. INTRODUCTION
Cryptography systems are mainly based on mathematical theory and computer science and play. In this era of universal connectivity network security is an important issue, so many algorithms, Advanced Encryption system, RSA, Data Encryption System, Digital Signature, Diffie hellman[4] key exchange are developed for data security. Moreover, the rising growth of data communication technique and electronic transactions over the web has made system security to become the most important issue over the network. In this age of RSA is one of the most widely used secure high quality public key cryptography algorithm, which is based on large mathematics. Montgomery modular exponentiation multiplier is the heart of RSA system, where Montgomery multiplication is iteratively performed to obtain $a^b$ mod m. Karatsuba algorithm[7], Blakely's method[5] are also used for modular multiplication but Karatsuba algorithm doesn't perform reduction operation whereas Blakely method needs a comparison of the integers at each step of modular reduction. This drawback is reduced by using Montgomery multiplier without trial division. This was achieved by reducing the operands to a residue class mod M. The algorithm discussed here provides the hardware architecture for the exponential multiplier. Now a days use of mobile phone communication, e-business, e-transactions, transmitting financial information is exponentially increasing. It is of utmost importance to store information securely. This led to a heightened awareness to protect the data from disclosure, to guarantee the authenticity of data and messages, and to protect the systems from network based attacks. So the cryptography algorithms are used to authenticate the document and hence Cryptography architecture has to be designed to work with limited area and low power.

## 2. MONTGOMERY MUTLIPLICATION
Montgomery multiplication is the method of performing fast modular multiplication. It was introduced by P.L. Montgomery in 1985[1]. Montgomery avoided the time consuming approach which is the main drawback of other algorithms. In conventional modular multiplication, when all bits of multiplicand are processed, modulus is repeatedly subtracted from the result until the result is less than modulus. But this method is tedious and complex when the operand size is larger. In Montgomery multiplier the bits are shifted out at each multiplicand bit is processed which results in no need of subtraction at the end. This algorithm is suitable for both hardware and software implementation. Let N(modulus) and R be two integers relatively prime to each other. We redefine the multiplier and multiplicand as A=AR mod M and B=BR mod M such that R>M and GCD (R,N)=1. Hence the new Montgomery product is $C=ABR^{-1}$ mod M. the drawback of this method is redundant term R required for the calculation. The necessary and sufficient conditions for this algorithm is 1.M > multiplier and multiplicand 2.M should be odd multiples of multiplier and multiplicand.
The architecture required to implement this algorithm is shown in figure1. As division operation is costly and is not easy to implement. Hence is replaced by right shift operation. Thus major issue of computational complexity is reduced by this algorithm.

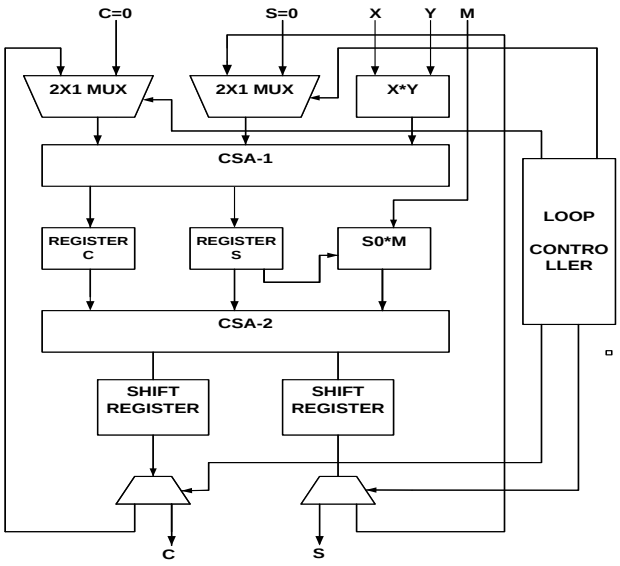


**Fig 1: Block diagram of Montgomery Multiplier.**

## 3. RSA CRYPTOSYSTEM

The RSA cryptosystem was proposed by Rivest, Shamir, and Adleman in 1978[2]. This was one of the first practical public key cryptosystem that is most widely used for secure data transmission. The encryption and decryption both are modular exponential and encryption key and decryption key differs from each other. The modular exponentiation is basically a square and multiply algorithm. The modular multiplications are iteratively performed to finish exponentiation. RSA cryptosystem are described as

1. Choose two prime numbers randomly. Let P and Q.
2. Compute N=P*Q, N is the modulus.
3. Compute φ=(P-1)*(Q-1).
4. Choose an integer 'e' such that gcd(φ,e)=1 and 1<e< φ.
5. Compute D such that De= 1 mod φ.

Thus, Encryption Key is (e,N) and Decryption key is (D,N). Let M be the plain then the ciphered code will be **$C=M^e \bmod N$** and after decryption the plaintext will be obtained as **$M=C^d \bmod N$.**.

## 4. PROPOSED WORK

In proposed work, the existing architecture is implemented using carry select adder and modified carry select adder in place of carry save adder. Carry select adder is composed of two n bit Ripple Carry Adders, where n is the number of bits. The logic operation of n bit RCA is performed using n full adder stages. Suppose two n bit numbers are to be added in Carry select adder then RCA1 and RCA2 generate n bit sum S0 and S1 and an output carry C0 and C1 corresponding to input carry Cin=0 and Cin=1 respectively.

In modified carry select adder RCA-2 is replaced by an add 1 circuit i.e binary to excess-1 converter circuit which results in further improvement in area.

The sum and carry selection unit is composed of 2x1 multiplexer, which select the output depending on the value of Cin. The architecture of Carry Select Adder and modified carry select adder is shown in Fig 2 and Fig 3 respectively. The tabular comparison of the 8- bit adders is shown in Table1.

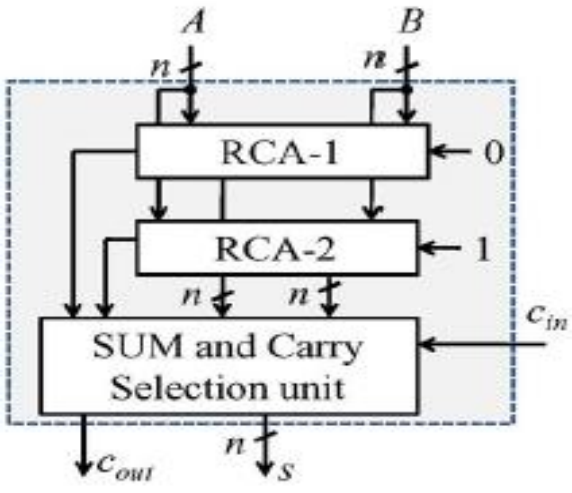


**Fig 2: Block Diagram Of Carry Select Adder.**

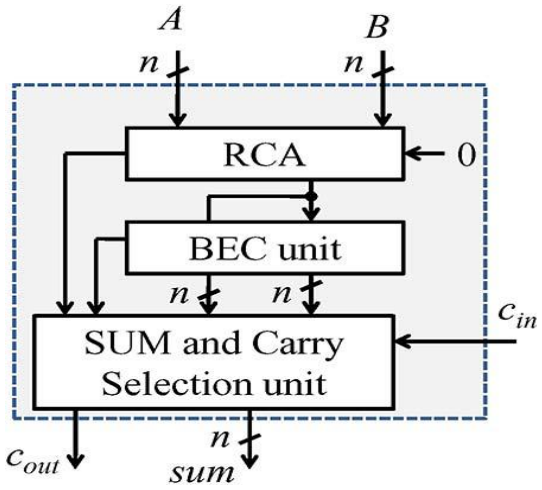


**Fig 3: Block diagram of Carry Select Adder Using Add 1 Circuit.**

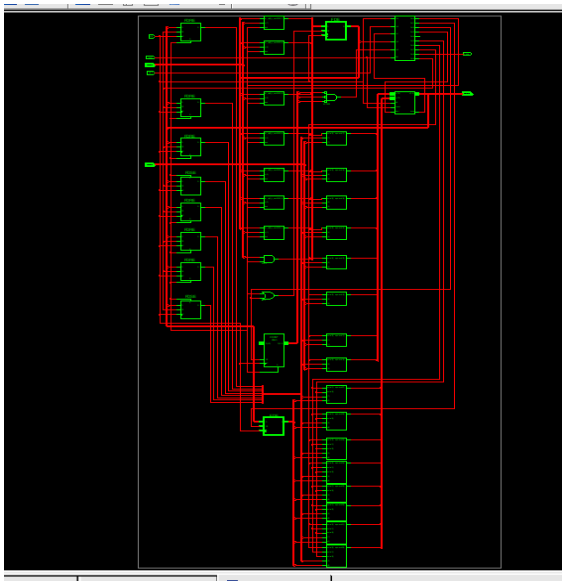

**Fig 3: RTL schematic of 16 bit montgomery multiplier.**

**Table 1. Comparison of Adders used.**

| Selected device | Carry Save Adder | Carry Select Adder | Modified Carry Select Adder |
|---|---|---|---|
| Number of slices | 17 | 15 | 11 |
| Number of 4 input LUTs | 30 | 26 | 21 |
| Number of bonded IOBs | 34 | 26 | 26 |
| Maximum combinational path delay (in ns) | 18.361 | 17.480 | 13.365 |
| Operating frequency(in Mhz) | 54.46 | 57.20 | 74.82 |

**Table 2. Design and Timing Summary of 16 bit Montgomery Multiplier**.

| Selected device(3S200-5FT256) | Using Carry Save Adder(existing)[3] | Using Modified Carry Select Adder |
|---|---|---|
| Number of slices | 104/1920 | 85/1920 |
| Number of 4 input LUTs | 182/3840 (3%) | 162/3840 |
| Number of bonded IOBs | 67/173 (76%) | 52/173 |
| Maximum Combinational path delay((ns) | 13.656 | 7.578 |
| Frequency of operation(Mhz) | 73.22 | 131 |

## 5. CONCLUSION

In this work Montgomery modular multiplier algorithm is studied and existing carry save adders are replaced by carry select adders and modified carry select adders and shift registers that results in reduction in area and delays as compared to conventional adder and division operation because the later are complex and time consuming. Table 2 shows the performance analysis of 16- bit multiplier. The waveform is synthesized for an 8-bit multiplier. The architecture is implemented in VHDL using Xilinx simulator and it was synthesized for xc3s200-5ft256 device.

## 6. REFERENCES

[1] Peter L. Montgomery, "Modular Multiplication without trial division", Mathematics of computation,44(170):519-521,1985.

[2] R.L. Rivest , A.Shamir and L.Adleman, "A Method for obtaining digital signature and public key cryptosystem", Communication of ACM, vol.21, pp.120-126,February 1978.

[3] E. F. Brickel, "A fast modular multiplication algorithm with application to two key cryptography" in Advances in Cryptography – CRYPTO '82, Plenum, New York, pages 51–60, 1983.

[4] S.kakde,S.Baswaik,Y.Deodhe, "Power analysis of Montgomery Modular multiplier for Cryptosystem",ICMIRA,2013,IEEE.

[5] W.Diffie and M.Hellmen, "new directions in cryptography",IEEE transaction on information technology,vol.22 pp.644-654, November 1976.

[6] G.R.Blakley, " A computer algorithm for the product of AB modulo M", IEEE transaction on computers, vol.32,no.5 pp.497-500, may 1983.

[7] Basant kumar Mohanty, senior member IEEE, and Sujit kumar patel, "Area-delay-power effi-cient Carry select adder", IEEE transaction on circuit and system-II, vol.61,no.6, june 2014.

**[8]** Huapeng wu, "Efficient bit-serial finite field montgomery multiplier in GF($2^m$)", $4^{th}$ IEEE International Conference on Information and technology (ICIST), pp. 527-530, april 2014.

[9] Aswathy B.G, Resmi R, "Modified RSA Public key Algorithm", Internatonal conference on computational systems and communications(ICCSC), pp.252-255, December-2014.

[10] I.-C. Wey, C.-C. Ho, Y.-S. Lin, and C. C. Peng, "An area-efficient carry select adder design by sharing the common Boolean logic term," in *Proc. IMECS*, pages 1–4, 2012.

[11] Jayanthi,A.N; Ravichandran, C.S, "Comparison of performance of high speed VLSI adders", International Conference on Current Trends in Engineering and Technology (ICCTET), pages 99-104, 2013.

[12] Mahalakshmi.R, Sasilatha.T, "A power efficient carry save adder and modified carry saver adder using CMOS technology", IEEE International conference on computational intelligence and computing research (ICCIC), pages 1-5, 2013.