Indian Journal of Science and Technology, Vol 9(38), DOI: 10.17485/ijst/2016/v9i38/101808, October 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

High Performance Design of Elgamal Cyrptographic Algorithm using Vedic Mathematics

S. Leonard Gibson Moses[1*], S. Ganesan[2], C. Vimala[3], I. RabiyaBegam[4] and M. NivethaPriya[4]

[1]Department of ECE, Periyar Maniammai University, Thanjavur - 613403, Tamil Nadu, India; gibs.ml@gmail.com
[2]Department of ECE, Mailam Engineering College, Mailam – 604304, Tamil Nadu, India; sangs.2007@rediffmail.com
[3]Department of Mathematics, Periyar Maniammai University, Thanjavur – 613403, Tamil Nadu, India; hodmathspmu@gmail.com
[4]Department of ECE, Jei Mathaajee College of Engineering, Siruvakkam - 631552, Tamil Nadu, India; rabiyabegam25@gmail.com, nivethapriya23@gmail.com

Abstract

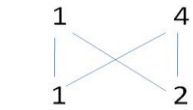
Objectives: Vedic mathematics contains 16 formulae or Sutras. Employing these shortcut formulae in the computations of Elgamal cryptographic algorithm will reduce the logic elements, layout area and power consumption. **Methods/Statistical Analysis**: Simulation programming for the paper has been done through Verilog HDL code in MODELSIM software and performance parameters like speed, power etc., using XILINX software. **Findings**: In this paper, when employing these Vedic formulae, lesser number of logic elements are consumed when compared with conventional method. **Improvements/ Applications**: By investigating the various Sutras in Vedic mathematics, it has been observed that speed is increased and layout area is minimized.

Keywords: Elgamal Algorithm, Multiplier and Accumulate Unit, Urdhva Tiryagbhyam Sutra, Vedic Multiplier

1. Introduction

Cryptography is nothing but studying the techniques of providing communication securely even though third parties are present. Elgamal algorithmis based on the problem of discrete log .No method exists for solving a discrete log problem with a large prime modulus for cryptanalysis. Hence this cryptosystem is suggested to be secure for sufficiently large prime modulus. Primitive root is used to create a key for this algorithm. Construction of an ElGamal encryption key is as follows. First choosing a very large prime number, then a primitive root modulo p, say α, is chosen. An integer α is chosen finally. And then compute β =α(mod p). The encryption key (p, α, β) is made public. However, the integer used to create β is kept secret. In this cryptographic algorithm, Multiplication and modulus operations are performed using high speed Urdhva Tiryagbhyam Sutra in Vedic Mathematics.

Vedic mathematics deals with various fields in mathematics like algebra, arithmetic and geometry etc. It optimizes the conventional mathematical algorithms[1]. Multiplication is the operation which takes too much time in mathematical calculations. We can optimize the crypto processor by optimizing the Multiplier and Accumulate Unit (MAC). By going through the papers[2,3], we can understand the techniques in ancient mathematics thoroughly. Most of the algorithms use multiplication operation. So, there is a need of high efficiency multiplier. Urdhva tiryagbhyam means vertically and crosswise[4]. It uses a formula which can be applicable to all multiplication cases which is shown.



(1*1) (2 + 4) (4*2) = 168

*Author for correspondence

X3X2	X3X2	X1X0	X1X0
Y3Y2	Y1Y0	Y3Y2	Y1Y0
$S_{33}S_{32}S_{31}S_{30}$	$S_{23}S_{22}S_{21}S_{20}$	$S_{13}S_{12}S_{11}S_{10}$	$S_{03}S_{02}S_{01}S_{00}$

Steps:

i. Multiply MSB (1) of first decimal number and MSB (1) of second decimal number. So MSB of answer is 1(1x1=1)
ii. Then multiply MSB(1) of first decimal number and LSB(2) of second decimal number; multiply LSB(4) of first decimal number and MSB(1) of second decimal number. So, middle bit of result is the sum of two multiplication results. ((1x2) + (4x1) =6)
iii. Finally LSB of result is the result of multiplication of two LSB's of two decimal numbers. (4x2=8)

Using this multiplier, partial product generation is done in parallel and summation also. Due to parallel calculation, this multiplier is not dependent on processor clock frequency. We know that processing power is directly proportional to clock frequency. Thereby reduce the power consumption a lot. This multiplier can be designed for all NxN bit binary numbers[5].

2. Proposed Work

Multiply – Accumulate unit multiplies the two numbers and sum with accumulator. Figure 1 shows the architecture of MAC unit. Here we have designed MAC unit with Urdhva multiplier. The advantages of Vedic multiplier are increasing the speed of computation, decreasing the delay, reducing the power consumption and decreasing the occupied area. For binary number system, urdhva tiryagbhyam method is given in Figure 2. The proposed 2X2 Urdhva multiplier is designed by using two half-adders & four 2-input AND gates which is shown in Figure 3. The proposed 4x4 Urdhva multiplier module is designed using four 2x2 urdhva multiplier by method of component instantiation which is given in Figure 4. Let us assume each multiplication output as, Figure 4 shows how to multiply the two 4-bit binary numbers, say

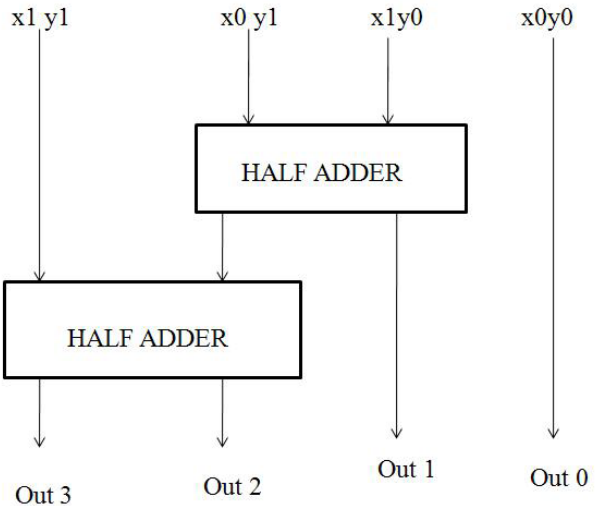


Figure 2. 2x2 binary Urdhva multiplier.

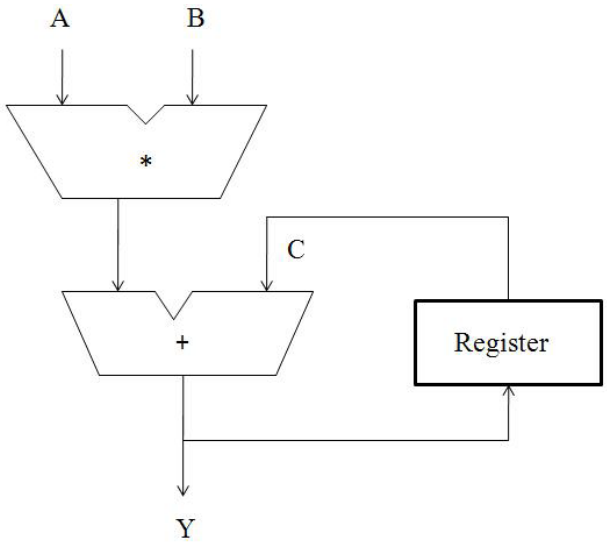


Figure 1. Hardware architecture of general MAC unit.

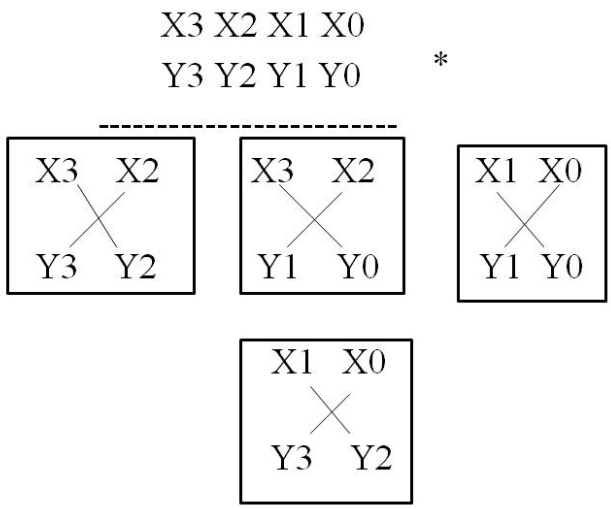


Figure 3. 4x4 binary Urdhva multiplier.

1101(13 in decimal) and 1011(11 in decimal), using the above logic. First full adder performs addition of 1001 and 0010 giving 1011 as result with no carry. The second full adder performs addition of 1000 with the result of first full adder i.e sum of 1011 and 1000 gives result as 0011 and 1 as carry out. Carry out from first and second full adders is provided to half adder. Here carryout is generated from second full adder, there by half adder produces 1 as Sum and 0 as carry out. Half adder's sum and carry is then added with S32 (1) and S33(0) respectively, so Final answer is 10001111 (143 in decimal).Vedic sutra consumes less number of logical elements so power consumption is reduced as well as layout area is reduced. Thereby Computation speed is increased. Figure 5 to Figure 7 show the device utilization summary for key generation, encryption and decryption respectively. Figure 8 shows the simulation result of key generation. Figure 9 depicts the simulation result of encryption. In Figure 10, the decryption simulation result is shown.

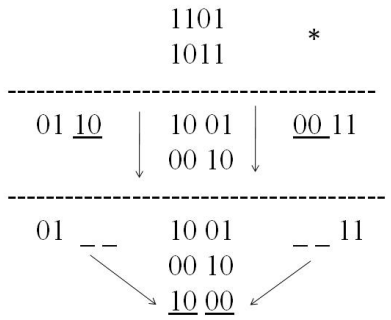


Figure 4. Multiplication logic using Urdhva method.

Device Utilization Summary				
Logic Utilization	**Used**	**Available**	**Utilization**	**Note(s)**
Logic Distribution				
Number of Slices containing only related logic	0	0	0%	
Number of Slices containing unrelated logic	0	0	0%	
Number of bonded IOBs	4	158	2%	
Total equivalent gate count for design	0			
Additional JTAG gate count for IOBs	192			

Figure 5. Device Utilization Summary for Key Generation.

Device Utilization Summary				
Logic Utilization	**Used**	**Available**	**Utilization**	**Note(s)**
Logic Distribution				
Number of Slices containing only related logic	0	0	0%	
Number of Slices containing unrelated logic	0	0	0%	
Number of bonded IOBs	8	158	5%	
Total equivalent gate count for design	0			
Additional JTAG gate count for IOBs	384			

Figure 6. Device Utilization Summary for Encryption.

Device Utilization Summary				
Logic Utilization	**Used**	**Available**	**Utilization**	**Note(s)**
Logic Distribution				
Number of Slices containing only related logic	0	0	0%	
Number of Slices containing unrelated logic	0	0	0%	
Number of bonded IOBs	4	158	2%	
Total equivalent gate count for design	0			
Additional JTAG gate count for IOBs	192			

Figure 7. Device Utilization Summary for Decryption.

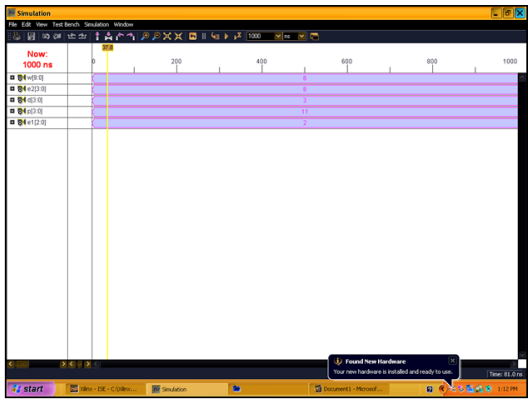


Figure 8. Simulation result of Key Generation.

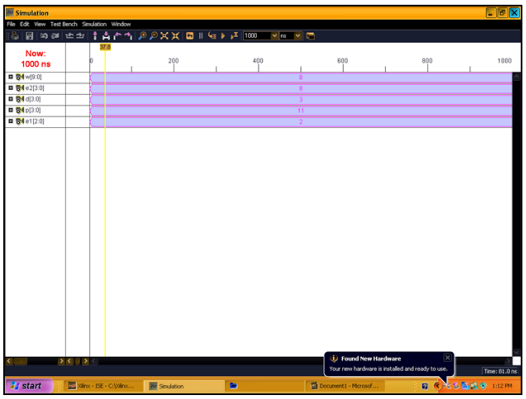


Figure 9. Simulation result of Encryption.

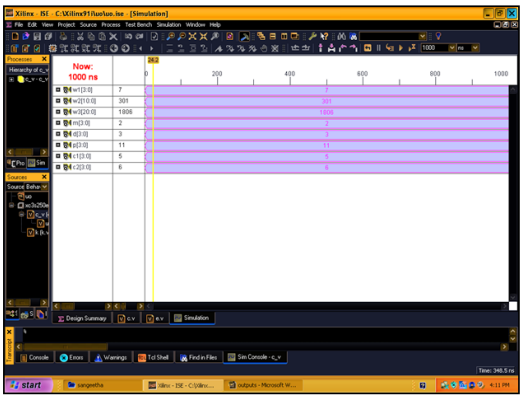


Figure 10. Simulation result of Decryption.

3. Conclusion

Thus an efficient Vedic multiplier is designed which consume less power and calculate the computations rapidly. High performance Elgamal cryptographic algorithm is designed using this Vedic algorithm.

4. References

1. Swami J, Tirthji Maharaj SBK. Vedic Mathematics. MotilalBanarsidas, Varanasi, India, 1986.
2. Dani SG. Vedic Maths, Facts and myths. One India One people. 2001 Jan; 4/6:20–1.
3. Vedic Mathematics for Faster mental Calculations and High Speed VLSI Arithmetic. Available from: http://hthapliyal.engineering.uky.edu/vedic-maths/. Date Accessed: 14/11/2008.
4. MeenaakshiSundari RP, Subathra. Enhancing multiplier speed in fast Fourier transform based on vedic mathematics. International Journal of VLSI design and Communication Systems. 2013 Jun; 4(3):135–44.
5. Poornima M, Shivaraj Kumar P, Shivu K. Shridhar KP, Sanjay H. Implementation of Multiplier algorithm using Vedic Mathematics. International Journal of Innovative Technology and Exploring Engineering. 2013 May; 2(6):219–23.