Performance Enhancement of The RSA Algorithm by Optimize Partial Product of Booth Multiplier

[I]Jyoti Kalia, [II]Vikas Mittal

[I,II]Dept. of Electronics and Communication Engineering, MMU University, Mullana, Haryana, India

Abstract

Objective: *To develop and enhanced RSA algorithm by optimize booth multiplier for reducing power consumption. Methods/Statistical Analysis: Security is an important concern in computing in today scenario. RSA is one of the asymmetric encryption algorithms which is used in hardware base application RSA encryption algorithm is very computation efficient algorithm in computation use booth multiplier but booth multiplier is increase the computation time and energy consumption. In this paper proposed the different areas of booth multiplier and analysis it's energy and time consumption during encryption. Finding: The power of the proposed RSA algorithm is very less as compared to the existing one. Application/Improvements: When we optimize the booth multiplier by reducing the partial products, we can reduce the energy and time in cryptography and ALU circuit.*

Keywords

Booth multiplier, RSA algorithm, Booth Multiplier Algorithm.

I. Introduction

With the internet innovation advancement, security has turned out to be increasingly imperative. For create cryptographic frameworks fundamentally for dependable classification and validation. Public key cryptographic algorithm in which broadly utilizing RSA algorithm [1] as a part of digital signature and information integral security. The execution of various modular multiplication in RSA algorithm is needed. Furthermore, to acquire security, extensive scale, e.g. 1024-piece or 2048-piece keys are required. Montgomery algorithm [2] is considered as a standout amongst the most productive approach for modular multiplication. Several algorithms like SOS, FIOS and CIOS which utilize small scale multiplier for implementing Montgomery multiplication in which higher clock frequencies can be achieved [3] moreover, in a single encryption required are many clock periods. With both modified □ and ordinary booth algorithm □, the completion of multiplication operation takes place in lesser clock cycles. Booth 64 multiplier is secondary encoding scheme based which reduces the complexity and large- scale booth multiplier speed is lifted with high radix that makes it more compatible for Montgomery algorithm.

Multiplication is the fundamentally, arithmetic operation in different type of data is multiplication of intensive applications such as image processing, asymmetric encryption, and so on. The classification of the multipliers is done mainly into parallel and serial multipliers. The "shift and add" algorithm is utilized in serial multiplier for realizing limited area multiplication and large delay relatively in power. Firstly, in parallel, the partial products are computed by parallel multiplier, and then together they are added for obtaining the result. In comparison to the serial multiplier, parallel multiplier has power overhead and large area but have shorter delay. Several algorithms exist there for optimizing the multiplication like Toom-Cook algorithm □, Karatsuba's algorithm □, and Booth algorithm □. Among different optimization algorithms type, Booth optimization algorithm for binary digit multiplication is the multiplication algorithms that is most efficient, while more efficient are other optimizing algorithms where binary digits are not operands □. The focus of Booth algorithm is on the partial products generation optimization. In this paper, various bit Booth multipliers are analysed and compared on the bases of two parameters: power and time delay. Additionally, for encryption RSA algorithm is used and for the booth multiplier optimization utilizing a Meta- heuristic algorithm. The paper is arranged in the below given format: section 2 defining the reviewed literature in context of the proposed approach. Section 3 gives the overview of the methodology used and section 4 gives the results. Finally, section 6 gives the conclusion.

II. Literature Survey

The computing units that is one among the most important is large-width multiplier, such that to encrypt the basing of chip on RSA algorithm. In [1]□, putting forward the booth algorithm innovation along with the optimized multiplier in a circuit structure. An innovative algorithm is proposed which generalizes for N-bit multiplier design. Moreover, compared to Booth multiplier originally, from the time complexity speeding up its computation and its computation characteristics parallelly making it compatible for multiplier of larger no. In a FPGA board, the algorithm is implemented that showing its performance is much better in comparison with original booth multiplier and the Xilinx one: 9.3% reduction in the logic delay. Additionally, a design of method is also proposed which makes the multiplier extension to N-bit easy. In [11], various large-scale Booth multiplier area and performance are discussed with the utilized high radices in Montgomery algorithm along with secondary encoded technique. The implementation of the modular implication with technology SMIC 0.13m at 160 MHz frequency and 125 MHz technology respectively which is 128-bit and 256-bit multiplier based with 64, 128 and 256 both encoding. The results of the experiment show the multiplier having 64, 128 and 256 booth which achieves the similar performance timing, while there is rise in radix with the rise in the area owing to its partial generation product and pre-computational complexity.

Nowadays, an important concern is security in cloud computing. The asymmetric algorithms that is gaining popularity is RSA which is widely utilized in internet on application bases for its advantages of strategy of public key over symmetric encryption algorithms. Moreover, Intensive is the very computation in RSA algorithms that affects the encountered applications power and speed efficiency. In future for memory and storage system, a new promising technology is introduced that is Racetrack Memory (RM) which is perfect in scenarios intensive memory utilization owing to its data with high intensity. Moreover, for the RM advantages exploitation applying a novel design while the sequentially access mechanism adverse impacts are avoided. In [12], Racetrack Memory based in-memory Booth multiplier is presented for this problem elevation. As the multiplier building block, proposed an adder which is based on the racetrack memory that is saving power up to 56.3% in comparison to magnetic state of art adder. With the element of storage integration, higher efficiency, scalability and power is shown by the proposed multiplier. In [13], proposed a method for accumulator and multiplier having the combination of carry look-ahead hybrid adder and logic reversible function. Lesser delay is produced by modified booth multiplier while comparing to ordinary multiplication process and partial products are also moderated by it. The MAC overall delay is controlled by utilizing Carry look-ahead adder. Basically, reversible logic designing focuses on reducing the consumption of power, complexity of circuit and information loss. They surveyed the way of making a design of full adder utilizing various reversible logic gates. Hybrid CLA is proposed originated from the existing CLA hierarchically that exhibit higher performance in area, computation and power consumption and reported the design complexities like area, power complexities and delay. The better performance is shown by the proposed MAC in comparison to the conventional techniques and having advantages like critical path delay and decreased area overhead. Xilinx ISE simulator and Synopsys Design complier are utilized for the synthesis and stimulation of high speed carry look ahead hybrid adders. In [1□], a design of RSA algorithm implementation by utilizing VHDL is presented. Spartan-3 device is utilized with Xilinx ISE 14.1. The radix-2 Montgomery multiplier binary left to right is used for the implementation of the RSA encryption method. The RSA algorithm encryption-decryption is done by using modular exponentiation. There is improvement of 14% in the device utilization and 2% improvement in delay. The implementation frequency is 79.546 MHz with the 4.5% improvement.

The project's aim in [1□] is the development of RSA encryption system for higher performance. The architecture of multiplier proposed achieves a significant performance improvement. Adder circuits and shift registers are in encoded multipliers which reduce its cost, delay, complexity and power consumption. Several multipliers are used by RSA encryption algorithm to compare and implementing by using encoder multiplier which is 1.26 times fast as compared to the Vedic multiplier, 6.5 times fast as compared to booth multiplier and 8.2 times fast as compared to array multiplier. The slice LUTs usage is more efficient along with the encoder multiplier that uses 2% less Slice LUTs in comparison to Vedic multiplier, slice LUTs lesser up to 33% as compared with booth multiplier and slice LUTs less up to 42% with respect to array multiplier. In [1□], describing the modified booth multiplier having pipeline high speed architecture. The multiplier circuits that are proposed are modified booth algorithm based and for multiplication speed acceleration using the most widely used technique that is pipeline technique. For the pipelined multipliers optimal implementation, experiments of various type are conducted. The multipliers speed is improved greatly with the proper discussion regarding the pipeline stage number and the pipeline registers position is inserted. The booth multiplier circuits that is modifies is proposed in Verilog HDL and the level gate circuits are synthesized by 0.13 um standard cell library utilization. The better performance of the multiplier resultant circuits is shown in comparison to others. The operation of the proposed multiplier is at the range of GHz, which is utilized in systems that requires high performance.

III. Methodology

In this section, figure 1 shows the work methodology and figure 2 shows the input output (I/O) pins in RSA.
The steps of the methodology are described below:
Step 1: Input the files.
Step 2: Encryption start with RSA.
Step 3: Apply the Booth Multiplier.
Step 4: Optimized the Booth multiplier by Meta- heuristic.
Step 5: Reduce the partial products.
Step 6: If Booth multiplier is optimized then it Analysis the energy and time.
Step 7: If Booth multiplier is not optimized then it retransmit step 3

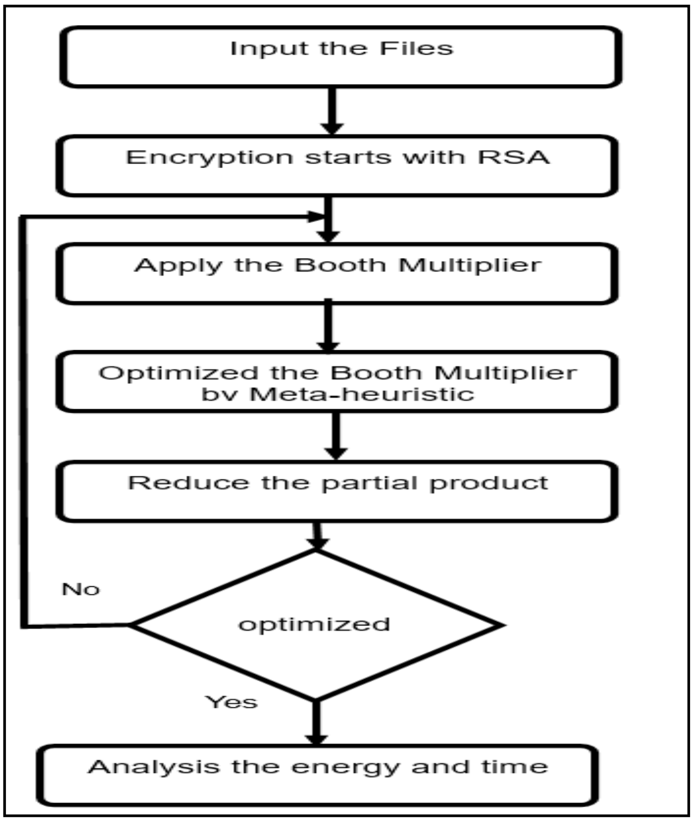

Input the Files
Encryption starts with RSA
Apply the Booth Multiplier
Optimized the Booth Multiplier bv Meta-heuristic
Reduce the partial product
No
optimized
Yes
Analysis the energy and time

Fig. 1: Work Methodology

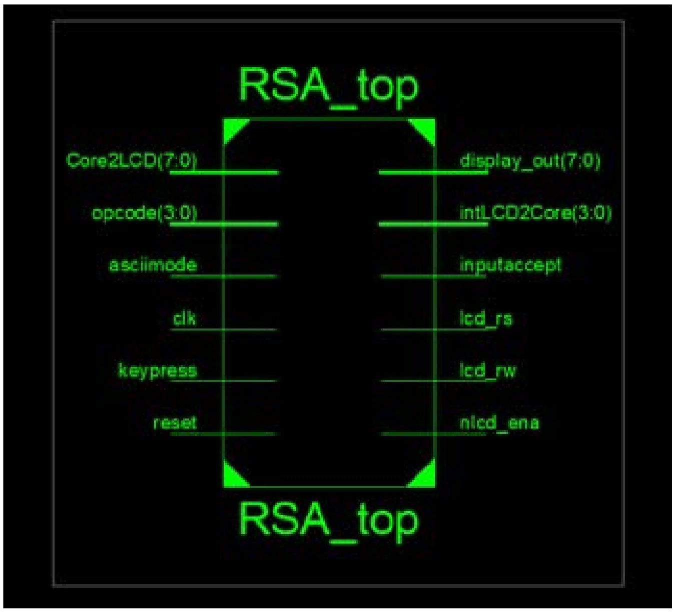
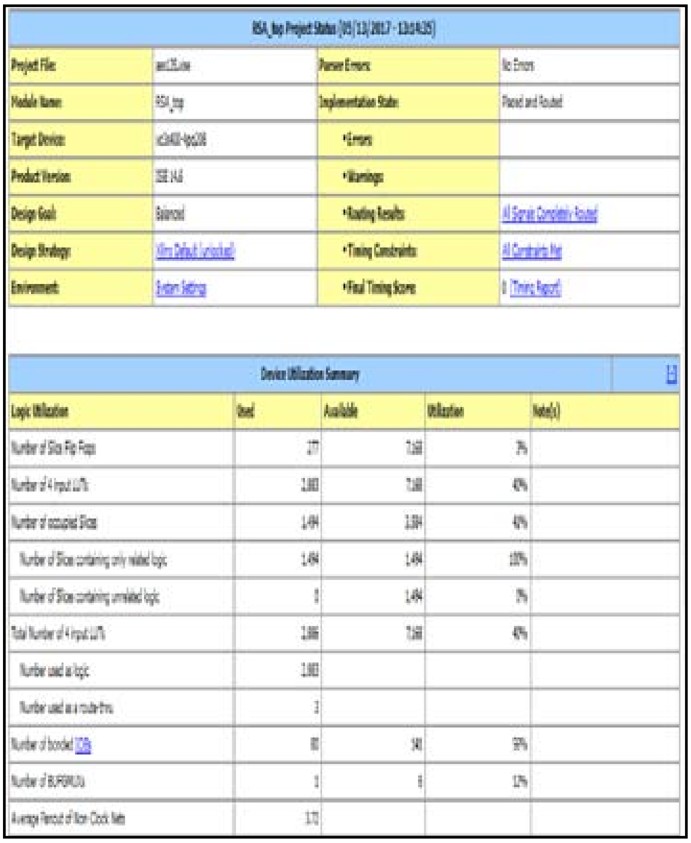


Fig 2: Input and Output pins in RSA

IV. Results

In this section, the results of the 64-bit RSA algorithm is displayed using spartan3 family, XC3S400-PQ208 device, PQ208 package, -4 speed. Design summary of 64-bit RSA algorithm is displayed in figure 3, it contains the number and percentage of slices, LUT's, IOB's and CLK's used by the RSA algorithm. RTL view of 64-bit RSA algorithm is shown in figure 4.



RSA_top Project Status (05/13/2017 - 13:04:25)			
Project File:	aes128.xise	Parser Errors:	No Errors
Module Name:	RSA_top	Implementation State:	Placed and Routed
Target Device:	xc3s400-4pq208	•Errors:	
Product Version:	ISE 14.6	•Warnings:	
Design Goal:	Balanced	•Routing Results:	All Signals Completely Routed
Design Strategy:	Xilinx Default (unlocked)	•Timing Constraints:	All Constraints Met
Environment:	System Settings	•Final Timing Score:	0 (Timing Report)

Device Utilization Summary				
Logic Utilization	Used	Available	Utilization	Note(s)
Number of Slice Flip Flops	277	7,168	3%	
Number of 4 input LUTs	2,183	7,168	4%	
Number of occupied Slices	1,494	3,584	4%	
Number of Slices containing only related logic	1,494	1,494	100%	
Number of Slices containing unrelated logic	0	1,494	0%	
Total Number of 4 input LUTs	2,186	7,168	4%	
Number used as logic	2,183			
Number used as a route-thru	3			
Number of bonded IOBs	83	141	59%	
Number of BUFGMUXs	1	8	12%	
Average Fanout of Non-Clock Nets	3.72			

Fig. 3 : Design summary of 64-bit RSA algorithm

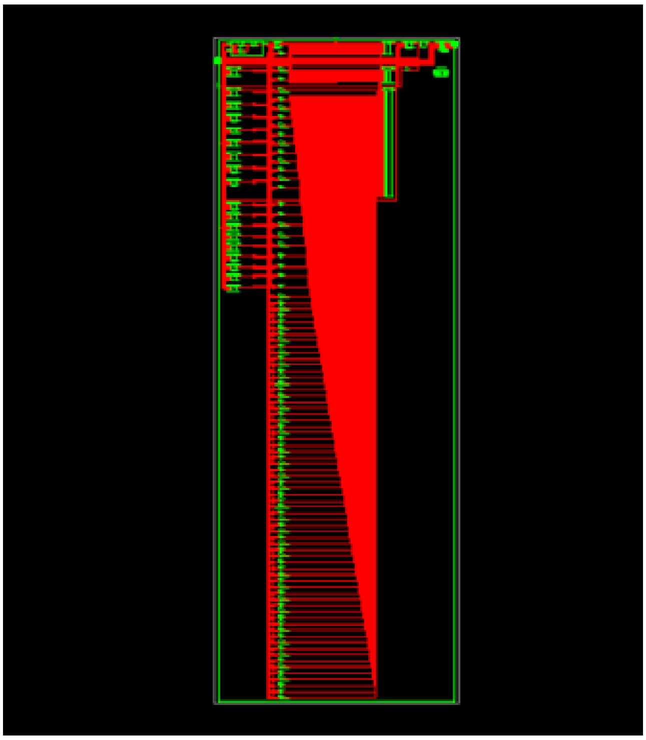


Fig. 4: RTL view of 64-bit RSA algorithm

The output of 8-bit,16-bit,32-bit and 64-bit RSA algorithm is shown in Table 1 and figure 5.

Table 1 : Result of RSA Algorithm

S. No	SPARTAN3 (XC3S400-PQ208)	Proposed RSA Power (W)	Proposed RSA Delay(ns)
1.	8-bit	0.06	8.630
2.	16-bit	0.063	5.439
3.	32-bit	0.066	5.439
4.	64-bit	0.092	86.3

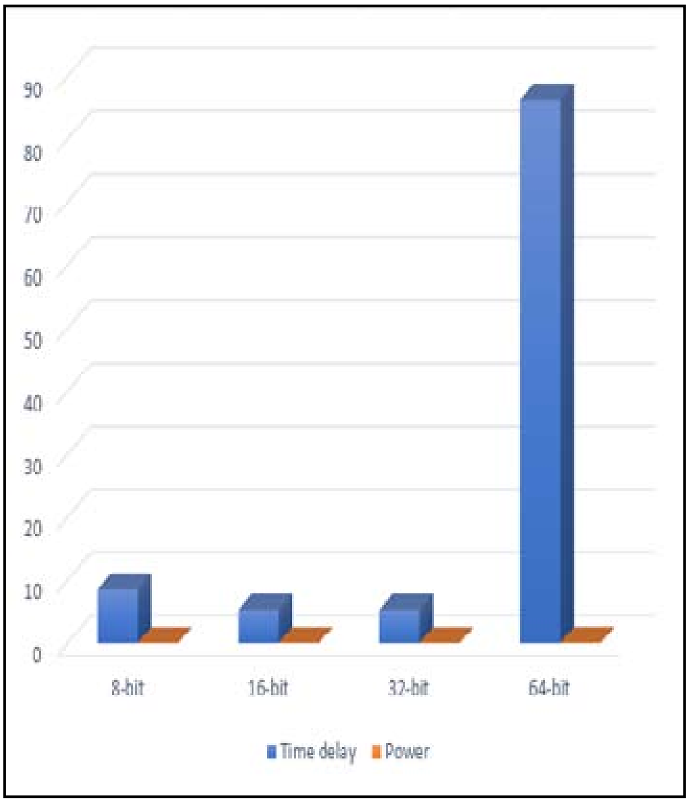


Fig 5: Results of RSA algorithm

V. Comparison

In this section, the results of proposed 64-bit RSA algorithm is compared with the existing RSA algorithm. The power of the proposed RSA algorithm is very less as compared to the existing. Comparison is shown in Table 2 and figure 6.

Table 2 : Comparison of power of 64-bit RSA Algorithm

S. No	RSA algorithm	RSA Power	Proposed RSA Power
1.	64-bit	185j	7.9396j

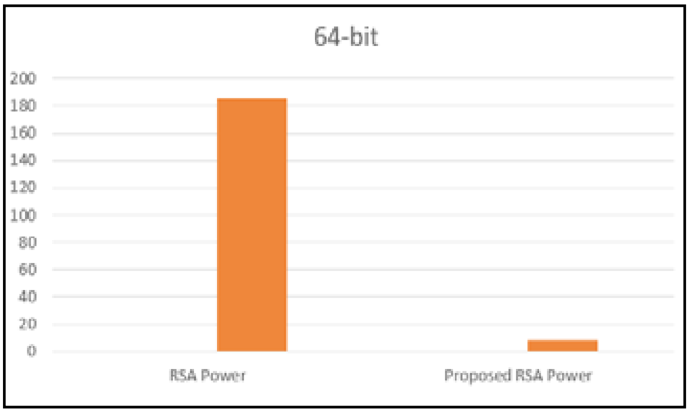


Fig. 6: Comparison of Power of 64-bit RSA Algorithm

VI. Conclusion

The proposed 64-bit RSA algorithm is better than the existing RSA algorithm. In our experiment analysis done work on 8,16,32 and 64 bits. In our analysis Energy and time delay increase when increase the area of booth multiplier. But it has not increase the time delay as much up to 32-bit because of approximation of s-boxes. But it has not shown its effect on after 32-bit because approximation not depend on hardware but RSA depend on hardware.

References

[1]. Rivest, Ronald L., Adi Shamir, and Leonard Adleman. "A method for obtaining digital signatures and public-key cryptosystems." Communications of the ACM 21.2 (1978): 120-126.

[2]. Montgomery, Peter L. "Modular multiplication without trial division." Mathematics of computation 44.170 (1985): 519-521.

[3]. Koc, C. Kaya, Tolga Acar, and Burton S. Kaliski. "Analyzing and comparing Montgomery multiplication algorithms." IEEE micro 16.3 (1996): 26-33.

[4]. Yan, Xiaodong, and Shuguo Li. "Montgomery multiplier based on secondary booth encoded algorithm." ASIC, 2007. ASICON'07. 7th International Conference on. IEEE, 2007.

[5]. MacSorley, Olin L. "High-speed arithmetic in binary computers." Proceedings of the IRE 49.1 (1961): 67-91.

[6]. Lee, Chiou-Yng, et al. "Low-complexity digit-serial and scalable SPB/GPB multipliers over large binary extension fields using (b, 2)-way Karatsuba decomposition." IEEE Transactions on Circuits and Systems I: Regular Papers 61.11 (2014): 3115-3124.

[7]. Mandal, Amar, and Rupali Syal. "Tripartite Modular Multiplication using Toom-Cook Multiplication." International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE) 1.2 (2012): pp-100.

[8]. Chen, Shin-Kai, et al. "Design and implementation of high-speed and energy-efficient variable-latency speculating booth multiplier (vlsbm)." IEEE Transactions on Circuits and Systems I: Regular Papers 60.10 (2013): 2631-2643.

[9]. Zheng, Menghui, and Alexander Albicki. "Low power and high-speed multiplication design through mixed number representations." Computer Design: VLSI in Computers and Processors, 1995. ICCD'95. Proceedings., 1995 IEEE International Conference on. IEEE, 1995.

[10]. Liang, Chengdong, et al. "An innovative Booth algorithm." Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), 2016 IEEE. IEEE, 2016.

[11]. Yan, Xiaodong, and Shuguo Li. "Montgomery multiplier based on secondary booth encoded algorithm." ASIC, 2007. ASICON'07. 7th International Conference on. IEEE, 2007.

[12]. Yan, Xiaodong, and Shuguo Li. "Montgomery multiplier based on secondary booth encoded algorithm." ASIC, 2007. ASICON'07. 7th International Conference on. IEEE, 2007.

[13]. Balakumaran, R., and E. Prabhu. "Design of high speed multiplier using Modified Booth Algorithm with hybrid carry look-ahead adder." Circuit, Power and Computing Technologies (ICCPCT), 2016 International Conference on. IEEE, 2016.

[14]. Singh, Sandeep, and Parminder Singh Jassal. "Synthesis and Analysis of 32-Bit RSA Algorithm Using VHDL." (2016).

[15]. George, Dani, and P. L. Bonifus. "RSA encryption system using encoded multiplier and vedic mathematics." Advanced Computing and Communication Systems (ICACCS), 2013 International Conference on. IEEE, 2013.

[16]. Kim, Soojin, and Kyeongsoon Cho. "Design of high-speed modified booth multipliers operating at GHz ranges." World academy of science, Engineering and Technology 61 (2010): 1-4.