RSA ENCRYPTION USING VLSI ARCHITECTURE FOR HIGH SPEED APPLICATIONS

Dr. Salai Thillai Thilagam J,
Department of Electronics and Communication Engineering,
G Pulla Reddy Engineering College,
Kurnool, Andhra Pradesh, India
salaithillai@gmail.com

Abstract: The major concern for the governments and private network communication is the security of systems against eavesdropping and illegal access. To overcome such illegal access the security of modern computer systems uses public-ciphers key namely Rivest, Shamir and Adleman (RSA). The RSA provides both authentication and secrecy of communication. In conventional encryption method the cryptography using RSA provides good secrecy and reduces area but generates more delay due to time taken by the multiplication part. To overcome such a problem, a 32-bit RSA using modulo (2^n+1) multiplication based VLSI architecture is presented in this study. This method offers less delay with high performance which can be used in any communication network field. The proposed method is implemented using Xilinx 12.4 ISE and simulated in MODELSIM 6.3c.

Keywords: Encryption, RSA, modulo 2n+1, Xilinx ISE.

I. INTRODUCTION

The main objective of the cryptographer is to make the crypto process easy and execute fast by advanced implementation techniques. RSA encryption and decryption by vedic mathematics is described in [1]. To enhance the efficiency of RSA architecture, straight division algorithm of vedic mathematics is developed. Three methods of multiplication modulo operations using (n+1)*(n+1)-bit array multiplier, modulo p carry-save addition, and modulo (p-1) carry save addition is described in [2]. They are implemented in pipelined realizations that produce a very high throughput.

A 16 bit RSA cipher for encryption and decryption using greatest common divider algorithm is described in [3]. It improves the security of the transmitted data or information. The realization of the RSA cryptographic algorithm based on the digit method and montgomery multiplier is described in [4]. It increases the speed of RSA encryption and decryption technique. Montgomery multiplication based on the residue number system is described in [5] to avoid timing attack and fault induction attack. The structure of the constituent modules of RSA is described in [6] based on the cellular automata.

An efficient Very Large Scale Integration (VLSI) structure based on the polymorphic cipher is described in [7] by considering unconditionally encipher procedure. VLSI structure for PRESENT block cipher algorithms is described in [8] for the key length of 128-bit and 80-bit. Various stages of the pipelining architecture of 128-bit Advanced Encryption Standard (AES) are described in [9] to increase the throughput.

Different architecture of the mix column is described in [10] to realize the AES encryption algorithm using Altera Quartus tool II. An enhanced mix column using asynchronous AES architecture with less transistor count is described in

[11]. A comparative study of various standard multipliers is discussed in [12]. All multipliers are implemented in VLSI and their performances are also analyzed.

VLSI implementation of combinational and pipelined circuits for addition and multiplication modulo are discussed in [13]. A study of various approaches for hardware implementation of AES is discussed in [14]. It includes pipelining, sub-pipelining and loop unrolling. Also, it discusses the resource sharing issues between the encryption and decryption of AES algorithm. The revocable identity based encryption in cloud to secure the data is discussed in [15].

In this study, VLSI architecture based RSA cipher for high performance secret communication is presented. The paper is organized as follows. Section 2 explains the RSA encryption using modulo 2^n+1 multiplication and section 3 describes the simulation and result analysis. The final section 4 describes the conclusion of the work.

II. METHODS AND MATERIALS

The flowchart of proposed RSA encryption with modulo multiplication is shown in Fig.1. The input data is given to the key distribution, key generation and message modules. The size of message is 32-bit data and the RSA encryption is obtained from modulo multiplication.

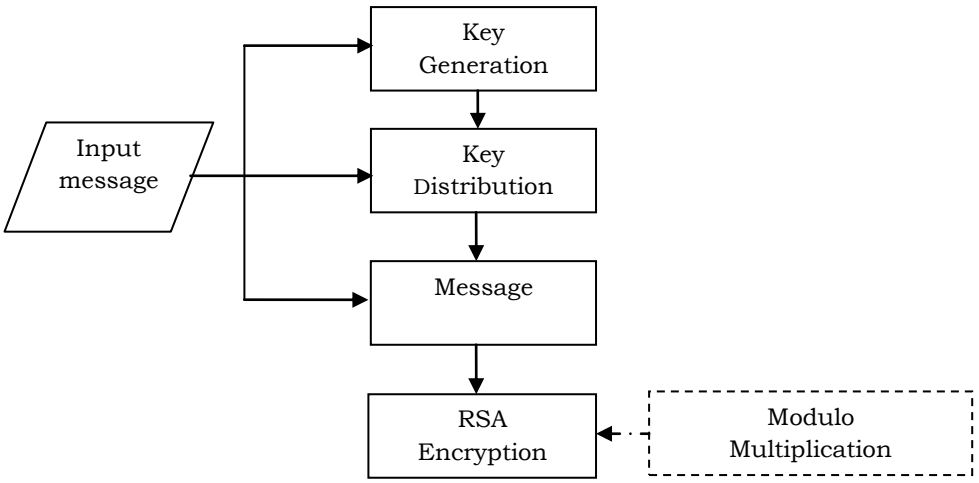

Fig. 1 Flowchart of the proposed RSA encryption

Figure 2 depicts the architecture of RSA cryptosystem. The RSA configuration module consists of two registers to store the key as well as the message text. The intermediate results are stored temporarily in the core unit of RSA architecture and the control unit controls the movement of data between the units of RSA architecture. Also, the modulo operations [13] are performed in core unit. It consists of four main components such as one intermediate register with 512-bit, multiplexer, control unit and arithmetic logic unit with modulo 2^n+1 multiplication which is shown in Fig.3. More information on modulo 2^n+1 multiplication operation can be found in [13].

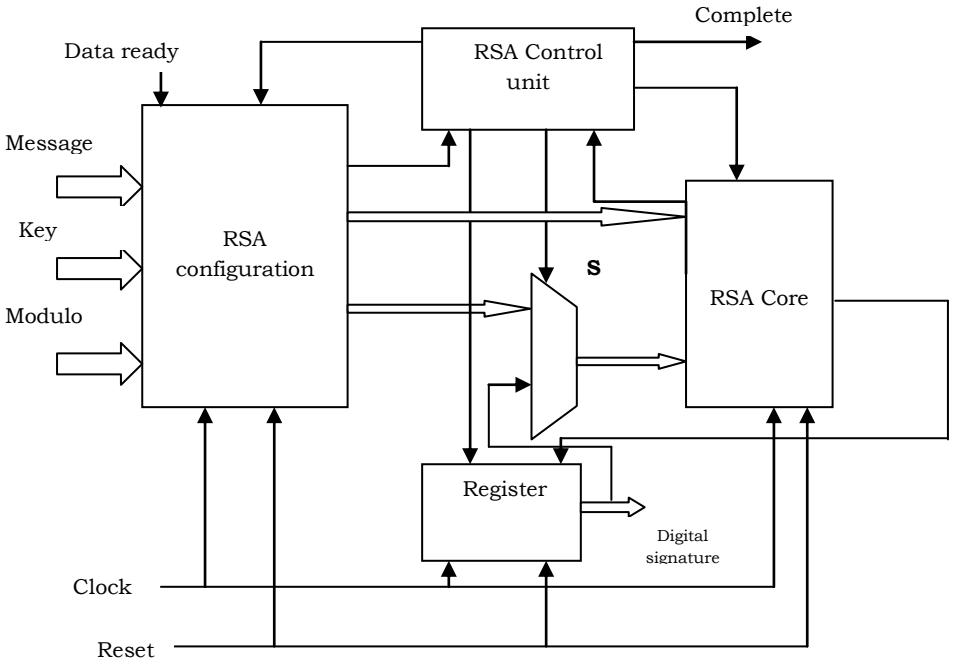

Fig. 2 Architecture of RSA in cryptosystem

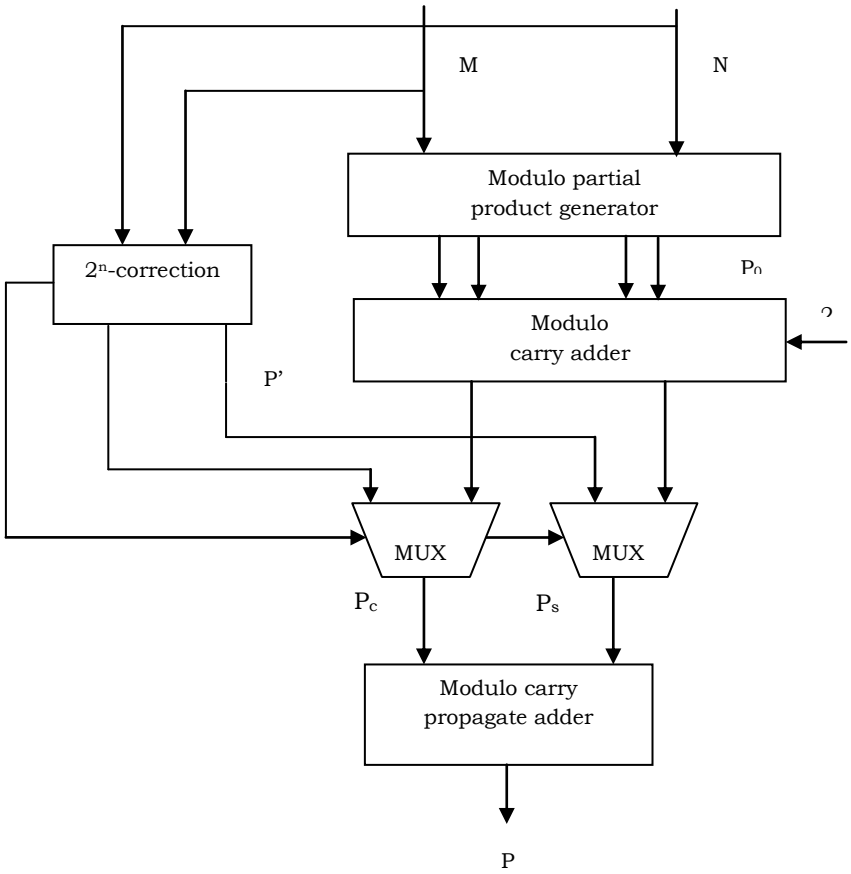

Fig. 3 Architecture of Modulo 2^n+1 multiplication

III. RESULTS AND DISCUSSION

The 32-bit RSA encryption using modulo (2^n+1) multiplication based VLSI architecture is simulated using Xilinx 12.3 ISE (Family-Virtex 4, Package-FF668, Speed:-12 and Devices-XC4VLX15/XCVLX25) design tool. The simulation waveform for the proposed 2^n+1 multiplication for RSA encryption is depicted in Fig. 4. Also, the simulation wave form for the RSA encryption is shown in Fig. 5.

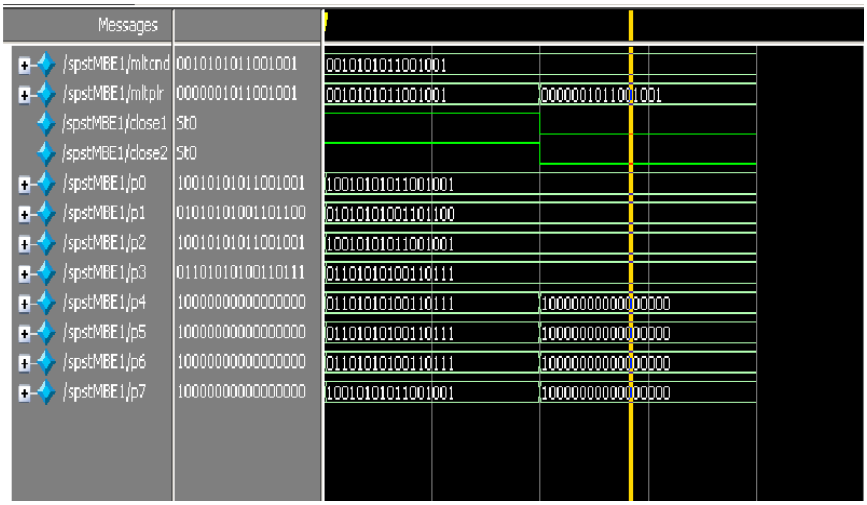

Fig. 4 simulation waveform of modulo 2^n+1 multiplication

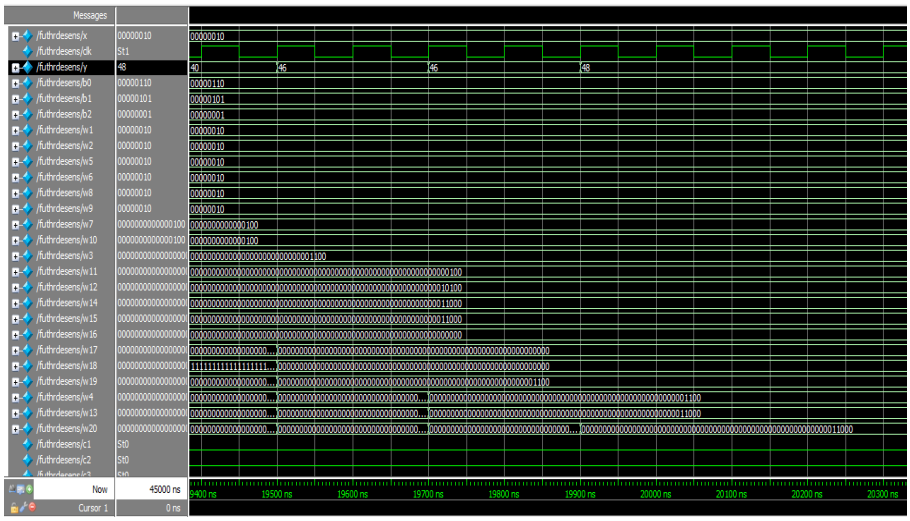

Fig. 5 Simulation waveform of the RSA Encryption

Let us consider, the public keys are 7663 and 2347 and the private keys are 7663 and 67. Based on these keys, the original message 3452 is sent as 2978 which is the encrypted value of 3452. Thus, RSA guarantees the safe transmission of original message. After simulating the code, the delay is computed and given in the design summary of the tool. Figure 6 shows the performance analysis of the RSA encryption in terms of delay.

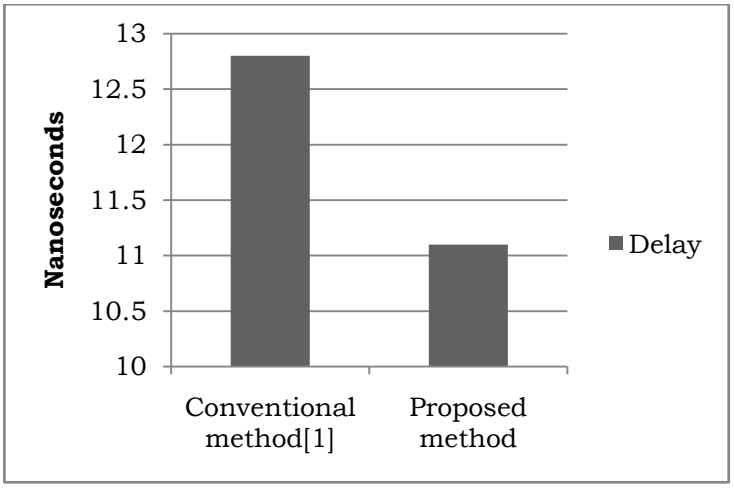

Fig. 6 Performance analysis of the RSA encryption

From the chart analysis, it is observed that the delay taken for the conventional method is 12.888ns whereas it is 11.388ns for the proposed system. Thus, the proposed RSA encryption method offers less delay with high performance than the conventional method.

IV. CONCLUSION

In this study, 32-bit RSA encryption using modulo 2^n+1 multiplication is presented using Xilinx 12.4 ISE tool. This RSA encryption offers high security and trusted one throughout the cryptography method. When compare to the conventional method the proposed method offers 11.58% reduction in delay with high performance as well as good secrecy in the communication without any degradation in the system performance. This method is used in net-banking systems for secure data transform. In future, the proposed system should be tested to overcome the mobility problem over group communication which enhances the overall parameters like less complexity design and good storage capacity.

REFERENCES

[1]. H. Thapliyal, and M.B. Srinivas, "VLSI implementation of RSA encryption system using ancient Indian Vedic mathematics", International Society for Optics and Photonics, Vol. 5837, 2005, pp. 888-892.

[2]. A.V. Curiger, H. Bonnenberg, and H. Kaeslin, "Regular VLSI architectures for multiplication modulo (2/sup n/+ 1)", IEEE Journal of Solid-State Circuits, Vol. 26, No.7, 1991, pp.990-994.

[3]. E. Chiranth, H.V.A. Chakravarthy, P. Nagamohanareddy, T.H. Umesh, and M. Chethan Kumar, "Implementation of RSA Cryptosystem Using Verilog" International Journal of Scientific & Engineering Research, Vol. 2, No.5, 2011, pp.1-7.

[4]. O. Nibouche, M. Nibouche, A. Bouridane, and A. Belatreche, "Fast architectures for FPGA-based implementation of RSA encryption

algorithm", International Conference on Field-Programmable Technology, 2004, pp. 271-278.

[5]. M. Ciet, M. Neve, E. Peeters, and J.J. Quisquater, "Parallel FPGA implementation of RSA with residue number systems-can side-channel threats be avoided?", Symposium on Circuits and Systems Vol. 2, 2003, pp. 806-810.

[6]. G.V. Iana, P. Anghelescu, and G. Serban, "RSA encryption algorithm implemented on FPGA", International Conference on Applied Electronics 2011, pp. 1-4.

[7]. N. Sklavos, P. Kitsos, and O. Koufopavlou, "VLSI Design and Implementation of Homophonic Security System", August, IEEE Computer Society Annual Symposium on VLSI, 2012, pp. 69-72.

[8]. J.G. Pandey, T. Goel, and A. Karmakar," An efficient VLSI architecture for PRESENT block cipher and its FPGA implementation", International Symposium on VLSI Design and Test Springer, 2017, pp. 270-278.

[9]. M. KN and R.K. Karunavathi, "Secured High throughput implementation of AES Algorithm", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, No.5, 2013, pp1193-1198.

[10]. S. Arrag, A. Hamdoun, and A. Tragha, "Design and Implementation A different Architectures of mixcolumn in FPGA", 2012, arXiv preprint arXiv: 1209.3061.

[11]. K. Sandyarani and P.N. Kumar," Vlsi Architecture For Nano Wire Based Advanced Encryption Standard (AES) With the Efficient Multiplicative Inverse Unit", International Journal of VLSI design & Communication Systems Vol.8, No.6, 2017,pp-15-22.

[12]. R. Rajeswari, "Design and Analysis of Various Standard Multipliers Using Low Power Very Large Scale Integration ", International Journal of MC Square Scientific Research Vol.4, No.1, 2012, pp-48-57.

[13]. R. Zimmermann, "Efficient VLSI implementation of modulo (2/sup n//spl plusmn/1) addition and multiplication", IEEE Symposium on Computer Arithmetic, 1999, pp. 158-167.

[14]. X. Zhang, and K.K. Parhi, "Implementation approaches for the advanced encryption standard algorithm", IEEE Circuits and systems Magazine, Vol. 2, No.4, 2002, pp. 24-46.

[15]. S.J. Rayen, P. Bharathi, V. Renuka, and R. Saranya, "Revocable-Storage Identity-Based Encryption: Secure Data Sharing In Cloud", International Journal Of Engineering And Computer Science, Vol.6, No.3, 2017, pp. 20558-20563.