ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 6, Special Issue , August 2019

International Conference on Recent Advances in Science, Engineering, Technology and Management at Sree Vahini Institute of Science and Technology-Tiruvuru, Krishna Dist, A.P

Cryptographic Implementation of the Processor Using Vedic Multiplier for Pairing At High Velocity

K.RAMESH, S. LAKSHMI PRASANNA

Asst Prof, Dept of ECE, Sree Vahini Institute of Science and Technology, Tiruvuru, AP, India.
Asst Prof, Dept of ECE, Sree Vahini Institute of Science and Technology, Tiruvuru, AP, India.

ABSTRACT: Pairings are appealing and competitive cryptographic primitives for different new and strong information security systems to be established. This article introduces a versatile and high-performance processor at high safety concentrations for cryptographic pairings over pairing-friendly curves. Hardware for Fp2 arithmetic is optimized in this model to speed up pairing computation, and a mixed modular multiplier based on the 16-bit Vedic multiplier (AB + CD) based on Montgomery technique is suggested. This mixed multiplier has a information route delay similar to that of implementation of a single multiplier (AB), but saves area costs compared to two single multipliers. The suggested processor's Design I is the first manufactured cryptographic pairing chip. We used Xilinx tool to compare our design outcomes with prior models.

KEYWORDS: Cryptographic, Montgomery Multiplier, Vedic Multiplier.

I. INTRODUCTION

For the last decade, pairings have been creatively and widely deployed to build novel and powerful digital security schemes in considerable quantity, such as identity based encryption [1] and identity-based signatures [2]. Research of cryptographic pairings has advanced substantially both in theory and implementation. However, due to the intricate mathematical structure, pairing requires more complicated computation than the previous public key ciphers, such as Rivest-Shamir-Adleman and elliptic curve cryptography. Infact, when high security is desired, challenges grow even more enormously for high computational complexity. Therefore, one of the key factors in realizing a pairing-based security scheme is to make pairing computation efficient in software and hardware, especially for embedded applications. Finite field multiplication is a fundamental operation for many cryptographic algorithms including RSA, digital signature algorithm and elliptic curve(ECC). Modular multiplication can be performed with in an ordinary multiplication followed by remainder computation, where the product is divided by the modulus. Now a day's Montgomery multiplier are more successful. Modular multipliers are most the important arithmetic function in public key cryptosystem because they are most used once and require large module, therefore computational method to accelerate, reduced energy consumption and simplify the use of such operation especially in hardware are always of great value for system that require data security. The Montgomery algorithms avoid expensive division by transforming it into another multiplication and right shift operation.

II. HARDWARE DESCRIPTION

The first design was proposed by Mathew etal [1]. they proposed the scalable 256/1024 bit encryption acceleration Montgomery multiplier. This design was based on 90nm technology. This design's operating frequency was 2.4 GHz with operating voltage as 1.2v and total power consumption of 69mW. in this design the Montgomery multiplier used a small processing element with fixed word size. This processing element was repeated multiple times to process very long operands. This design disabling the carry propagation in the later case. This design circuit implementation reduces the inter-outer-loop pipeline stall from 2 cycle to one cycle and having shorter latency as result.

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 6, Special Issue , August 2019

International Conference on Recent Advances in Science, Engineering, Technology and Management at Sree Vahini Institute of Science and Technology-Tiruvuru, Krishna Dist, A.P

This design has three main elements as processing element, memory element, FIFO and sequence circuit. The block diagram of the Montgomery multiplier is shown in figure (1)[1]. The memory arrays stores the input values. The final result is fed back from the end of the array through a FIFO.

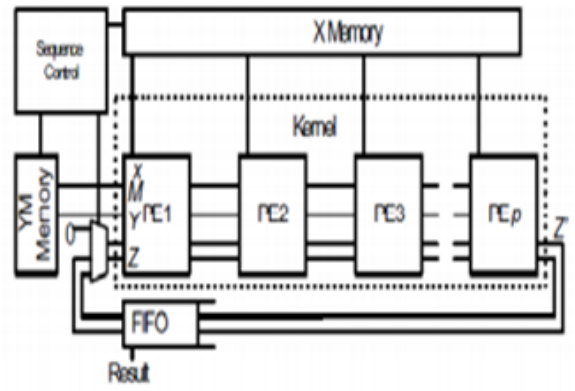

Fig .1.Montgomery Multiplier Block Diagram.

The second design was proposed by Li et al.they proposed the cryptographic pairing processor whose modular multiplier hardware having new combined Montgomery multiplier which implements the fundamental operations of fp2multiplication efficiently. This architecture was based on 65nm technology. This design used 800 MHz as the operating frequency with 1.2 v operating voltage. Its power consumption was 266.5mW. This design

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 6, Special Issue , August 2019
International Conference on Recent Advances in Science, Engineering, Technology and Management at Sree Vahini Institute of Science and Technology-Tiruvuru, Krishna Dist, A.P

computes the result in 0.64ms. The architecture of the combined Montgomery multiplier is shown in figure (2)[2].

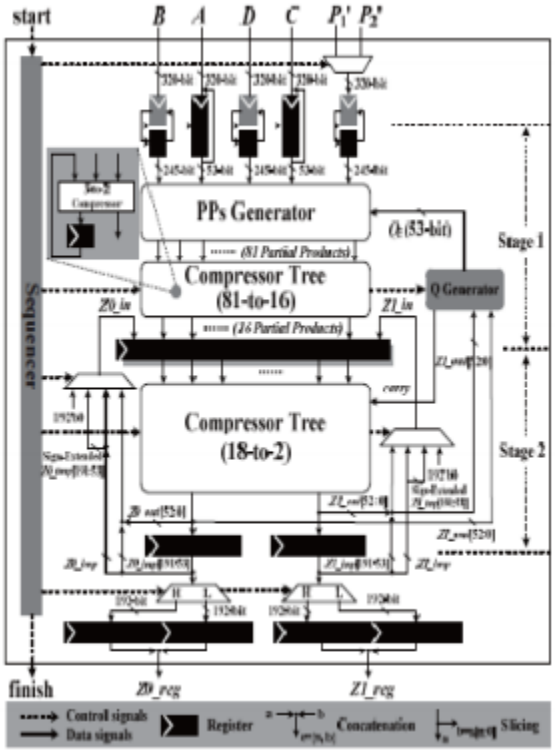

Fig.2. Architecture of the combined high-radix Montgomery multiplier.

The architecture of pairing processor employs a RISC architecture with five pipeline stages, such as instruction fetch, instruction decode, execution, memory, and write back, as well as several special hardware units for high speed pairing computation. The modular multiplier and the modular adder/subtractor implement theFp2 arithmetic's. The S-Regfile is the special register files with the volume of16 × 320-bit, and the MAU is responsible for fetching data from data memory and preparing the 320-bit-width variables that can be latched in the S-Regfile. The main RISC pipeline decodes instructions and then multiplier, adder/subtractor, and MAU execute the corresponding instructions in multiple cycles.

III. INTRODUCTION TO VEDIC MULTIPLIERS

Furthermore to speed up the multiplier performance, here we are proposing technique called Vedic Multiplier. Generally, the microprocessor operations are operating at increase in high clock frequency which leads sin increasing the power. Whereas in Vedic multiplier, the microprocessor designer can easily detects these problems for avoiding device failure. Vedic multiplier is faster than above mentioned multipliers. As number of bits increases from 8-bits to 16-bits, there is greater reduction in timing delay for Vedic multiplier when compared to other multipliers. In terms of gate delays, regularity of structure there is greater advantage for Vedic multiplier compared with other multipliers. In Vedic multiplier ―Urdhva-Tiryagbhyam‖ (Vertically and Crosswise) sutra is used for the multiplication of two binary (or) decimal numbers shown in Fig 3 The importance of Vedic multiplier here is partial product generation and additions are done parallely. Therefore, it is well suited for parallel processing. Therefore the delay is reduced, which is the primary motivation behind this work. The below Fig4 illustrates the 8-bit Vedic multiplier.

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 6, Special Issue , August 2019

International Conference on Recent Advances in Science, Engineering, Technology and Management at Sree Vahini Institute of Science and Technology-Tiruvuru, Krishna Dist, A.P

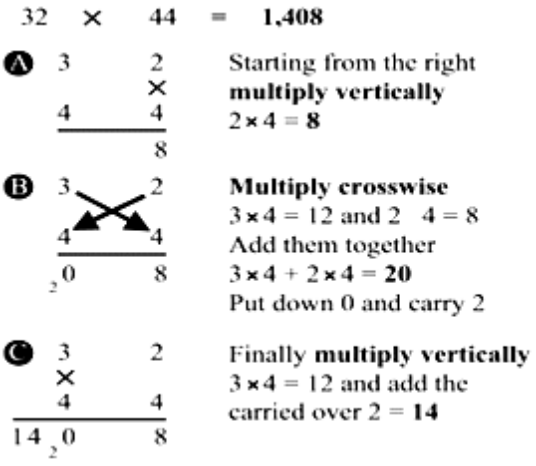

Fig. 3 Vedic multiplication.

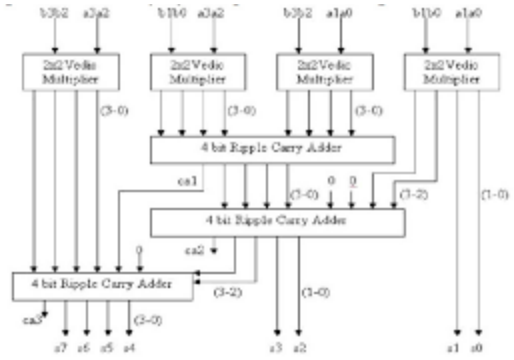

Fig4. 4-bit Vedic Multiplier.

The 4x4 bit Vedic multiplier is implemented by using four 2x2 Vedic multiplier. To illustrate, 4x4 Vedic multiplication, it have A=A3A2A1A0, B=B3B2B1B0 and the output is S7S6S5 S4S3 S2S1S0. Let's A & B is divided into 2 parts A3A2& A1A0 for A and B3B2 & B1B0 for B by using the basic of Vedic multiplication, taking the 2 bit simultaneously in the circuit by using two bit multiplier block.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 6, Special Issue , August 2019
International Conference on Recent Advances in Science, Engineering, Technology and Management at Sree Vahini Institute of Science and Technology-Tiruvuru, Krishna Dist, A.P

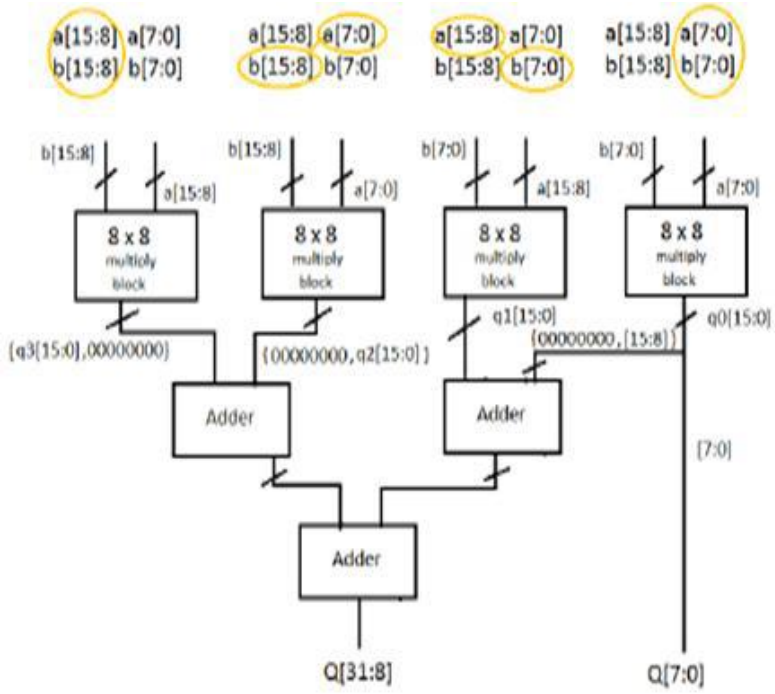

Fig 5.16-bitVedic multiplier.

As shown in fig 5.we are using the 16-bit Vedic multiplier for our proposed system to get the better results compare to the previous reports. Here we are concatenating the 8-bit based designs to get the 16-bit multiplier. Here the multiplication process is done as shown in above figure.

IV. EXPERIMENTAL RESULTS

In our extension of Vedic multiplier the area of system reduced compared with the previous systems. The simulation results of our proposed system are as shown in fig 6.

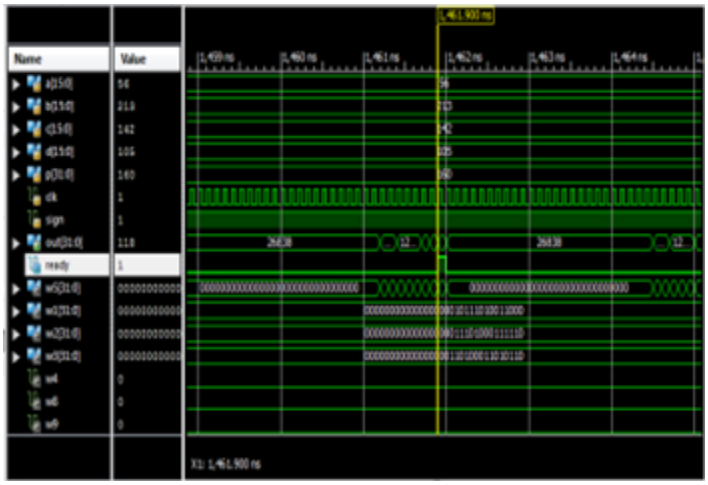

Fig6. Simulation Result.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 6, Special Issue , August 2019
International Conference on Recent Advances in Science, Engineering, Technology and Management at Sree Vahini Institute of Science and Technology-Tiruvuru, Krishna Dist, A.P

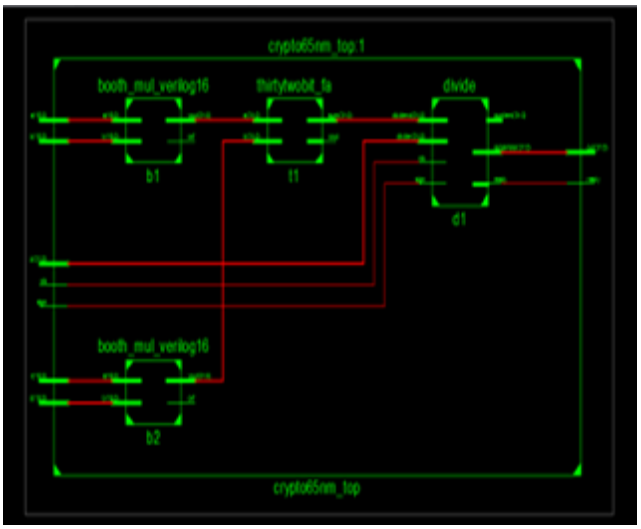

Fig 7. RTL Schematic.

The synthesis results of our proposed design based on Vedic multiplier are shown in fig9.The RTL schematic is shown in fig 7.

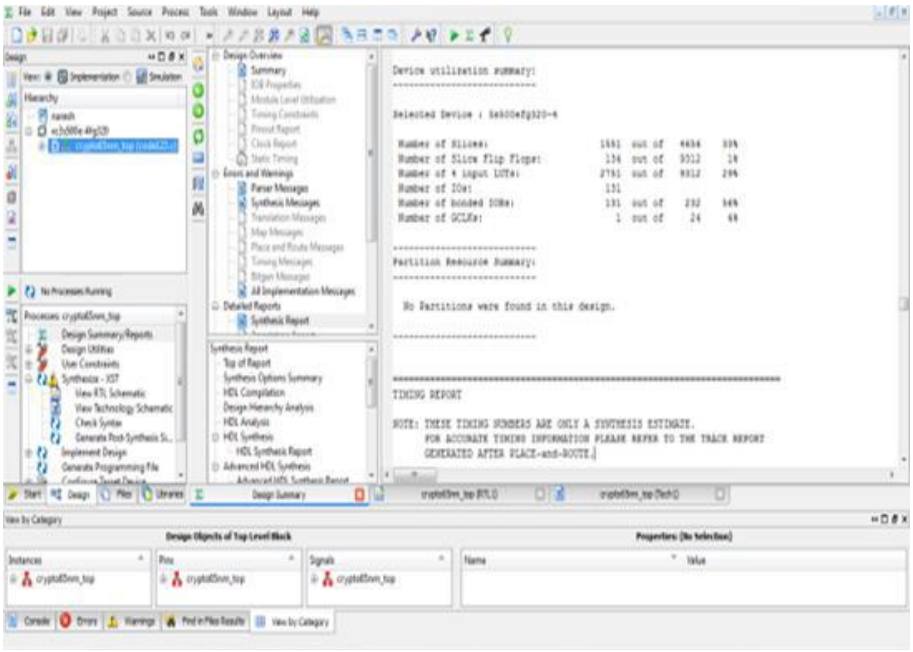

Fig8. Synthesis report of existing system.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 6, Special Issue , August 2019
International Conference on Recent Advances in Science, Engineering, Technology and Management at Sree Vahini Institute of Science and Technology-Tiruvuru, Krishna Dist, A.P

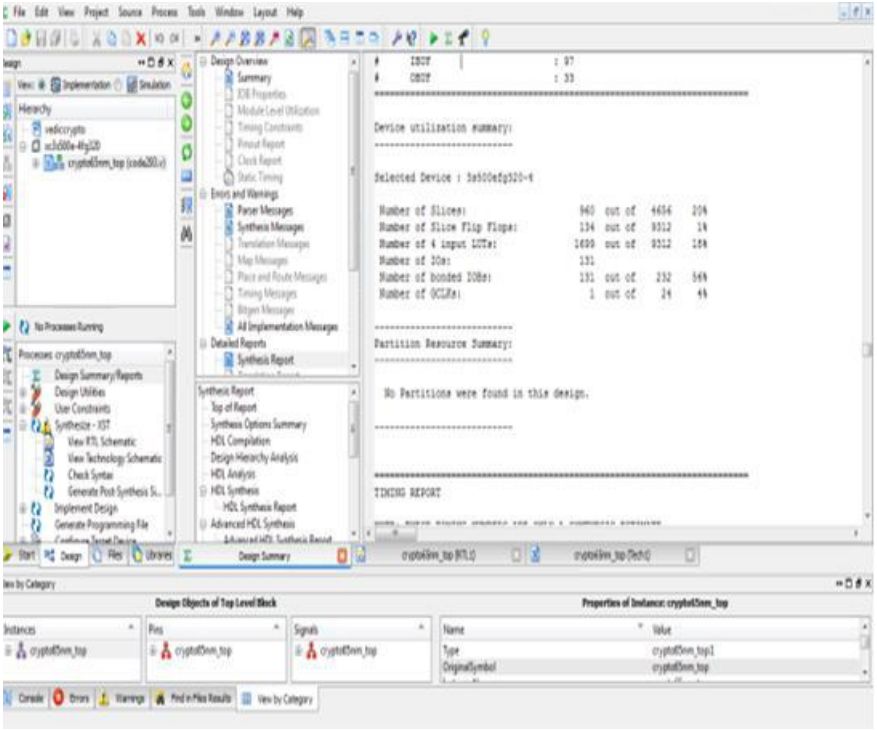

Fig9. Synthesis report of proposed system.

When compared with the results of previous system the slices are reduced 13% in our proposed system and there is 14% improvement in IOs.

V. CONCLUSION

This article suggested a cryptographic processor performing ideal ate pairing high-speed computing. Hardware units for quick calculation of the processor's Fp2 arithmetic speed. In addition, exploiting the parallelism in combining algorithms and using an effective system for accessing memory also contributes to accelerating efficiency. Finally, by using Vedic multiplier in place booth multiplier, we accomplished area effectiveness.

REFERENCES

[1] D. Boneh and M. Franklin, ―Identity-based encryption from the weilpairing,‖ in Proc. 21st Annu. Int. Cryptol. Conf. Adv. Cryptol.—CRYPTO,LNCS 2139. Santa Barbara, CA, USA, 2001, pp. 213–229.
[2] C. J. Choon and C. J. Cheon, ―An identity-based signature from gapDiffie-Hellman groups,‖ in Proc. 6th Int. Workshop Pract. Theory Public Key—PKC, LNCS 2567. Miami, FL, USA, 2003, pp. 18–30.
[3] S. Ghosh, D. Mukhopadhyay, and D. Roychowdhury, ―High speedflexible pairing cryptoprocessor on FPGA platform,‖ in Proc. 4th Int.Conf., Pairing-Based Cryptography Pairing, LNCS 6487. Palo Alto, CA, USA, 2010, pp. 450–466.
[4] R. C. Cheung, S. Duquesne, J. Fan, N. Guillermin, I. Verbauwhede,and G. X. Yao, ―FPGA implementation of pairings using residuenumber system and lazy reduction,‖ in Proc. 13th Int. Workshop CHES, LNCS 6917. Nara, Japan, 2011, pp. 421–441.
[5] J. Fan, F. Vercauteren, and I. Verbauwhede, ―Faster Fp-arithmeticfor cryptographic pairings on Barreto–Naehrig curves,‖ in Proc. 11thInt. Workshop CHES, LNCS 5747. Lausanne, Switzerland, 2009,pp. 240–253.
[6] D. Kammler et al., ―Designing an ASIP for cryptographic pairings over Barreto–Naehrig curves,‖ in Proc. CHES, LNCS 5747. Lausanne, Switzerland, 2011, pp. 254–271.
[7] J. Fan, F. Vercauteren, and I. Verbauwhede, ―Efficient hardware implementation of Fp-arithmetic for pairing-friendly curves,‖ IEEE Trans.Comput., vol. 61, no. 5, pp. 676–685, May 2012.
[8] O. Nibouche, A. Bouridane, and M. Nibouche, ―Architectures for Montgomery's multiplication,‖ IEE Proc. Comput. Digit. Tech., vol. 150,no. 6, pp. 361–368, Nov. 2003.
[9] Y. Li, J. Han, S. Wang, D. Fang, and X. Zeng, ―An 800 MHz cryptographicpairing processor in 65 nm CMOS,‖ in Proc. IEEE A-SSCC,Kobe, Japan, Nov. 2012, pp. 217–220.

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 6, Special Issue , August 2019

International Conference on Recent Advances in Science, Engineering, Technology and Management at Sree Vahini Institute of Science and Technology-Tiruvuru, Krishna Dist, A.P

[10] F. Vercauteren, ―Optimal pairings,‖ IEEE Trans. Inf. Theory, vol. 56,no. 1, pp. 455–461, Jan. 2010.
[11] J.-L. Beuchat, J. E. González-Díaz, S. Mitsunari, E. Okamoto,F. Rodríguez-Henríquez, and T. Teruya, ―High-speed software implementationof the optimal ate pairing over Barreto―Naehrig curves,‖ inProc. 4th Int. Conf. Pairing-Based Cryptography, LNCS 6487. Palo Alto, CA, USA, 2010, pp. 21–39.
[12] D. F. Aranha, K. Karabina, P. Longa, C. H. Gebotys, and J. López,―Faster explicit formulas for computing pairings over ordinary curves, in Proc. 30th Annu. Int. Conf. Theory Appl. Cryptographic Eurocrypt,LNCS 6632. Tallinn, Estonia, 2011, pp. 48–68.
[13] S. Mathew, D. Harris, M. Anders, S. Hsu, and R. Krishnamurthy,― A 2.4 GHz 256/1024-bit encryption accelerator reconfigurable Montgomery multiplier in 90 nm CMOS,‖ in Proc. 20th IEEE Int. SOCConf., Hsinchu, Taiwan, Sep. 2007, pp. 25–28.
[14] H. Orup, ―Simplifying quotient determination in high-radix