ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A 65 Nm Cryptographic Processor For High Speed Pairing Computation Using Vedic Multiplier

Barmavathu Nagalatha
PG Scholar,
Department of ECE(VLSI),
Sree Vahini Institute of Science & Technology.

Kongala Ramesh, M.Tech
Assistant Professor,
Department of ECE
Sree Vahini Institute of Science & Technology.

Abstract:

Pairings are attractive and competitive cryptographic primitives for establishing various novel and powerful information security schemes. This paper presents a flexible and high-performance processor for cryptographic pairings over pairing-friendly curves at high security levels. In this design, hardware for Fp2 arithmetic is optimized to accelerate the pairing computation, and especially a combined modular multiplier which is based on the 16-bit vedic multiplier, which implements (AB + CD) based on Montgomery method, is proposed. This combined multiplier has the data path delay close to that of a single multiplier implementing (AB) but saves area cost compared with two single multipliers. The Design I of the proposed processor is the first fabricated chip for pairing cryptography. For the comparison of results of our design with previous designs we used Xilinx tool.

I.INTRODUCTION:

For the last decade, pairings have been creatively andwidely deployed to build novel and powerful digitalsecurity schemes in considerable quantity, such as identitybasedencryption [1] and identity-based signatures [2]. Research of cryptographic pairings hasadvanced substantiallyboth in theory and implementation. However, due to theintricate mathematical structure, pairing requires more complicatedcomputation than the previous public key ciphers, suchas Rivest-Shamir-Adleman and elliptic curve cryptography.

Infact, when high security is desired, challenges grow even moreenormously for high computational complexity. Therefore,one of the key factors in realizing a pairing-based securityscheme is to make pairing computation efficient in softwareand hardware, especially for embedded applications. Finite field multiplication is a fundamentaloperation for many cryptographic algorithmsincluding RSA, digital signature algorithmand elliptic curve (ECC).

Modular multiplication can be performed with in anordinary multiplication followed byremainder computation, where the product isdivided by the modulus. Now a day'sMontgomery multiplier are more successful.Modular multipliers are most the importantarithmetic function in public keycryptosystem because they are most used once and require large moduli, thereforecomputational method to accelerate, reducedenergy consumption and simplify the use ofsuch operation especially in hardware arealways of great value for system that require data security. The Montgomery algorithmsavoid expensive division by transforming itinto another multiplication and right shiftoperation.

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.

This design has three mainelements 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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

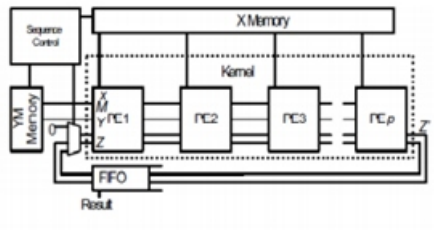

Fig .1.Montgomery multiplier blockdiagram

The second design was proposed by Li et al.they proposed the cryptographic pairingprocessor whose modular multiplier hardware having new combined Montgomery multiplier which implementsthe 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 computes the result in 0.64ms. The architecture of the combined Montgomery multiplier is shown in figure (2)[2].

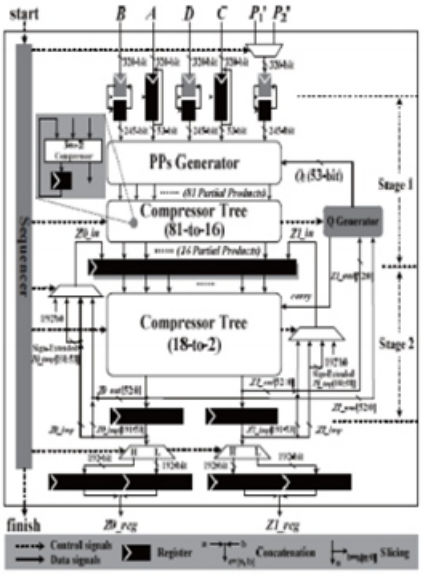

Fig. 2. Architecture of the combinedhigh-radix Montgomery multiplier.

The architecture of pairing processor employs a RISC architecturewith five pipeline stages, such as instruction fetch, instructiondecode, execution, memory, and write back, as well as severalspecial hardware units for high speed pairing computation. The modular multiplier and the modular adder/subtractorimplement the Fp2 arithmetics . TheS-Regfile is the special register files with the volume of16 × 320-bit, and the MAU is responsible for fetching datafrom data memory and preparing the 320-bit-width variables that can be latched in the S-Regfile.

The main RISC pipelinedecodes instructions and then multiplier, adder/subtractor,and MAU execute the corresponding instructions in multiplecycles.

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 leadsin 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 Vedicmultipliercompared with other multipliers. In Vedic multiplier "Urdhva-Tiryagbhyam" (Vertically and Crosswise) sutrais 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 Fig 4 illustrates the 8-bit Vedic multiplier.

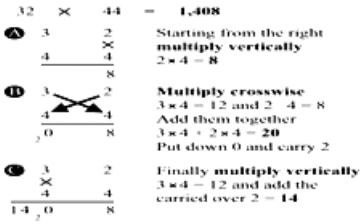

Figure 3.Vedic multiplication

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 S7S6S5S4S3S2S1S0. 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 No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

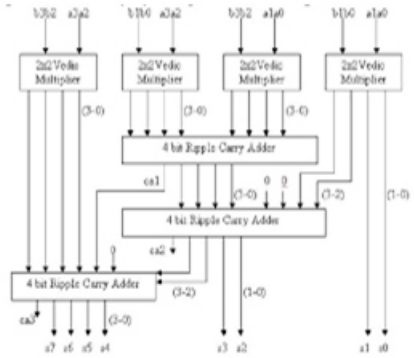

Fig 4. 4-bit Vedic Multiplier

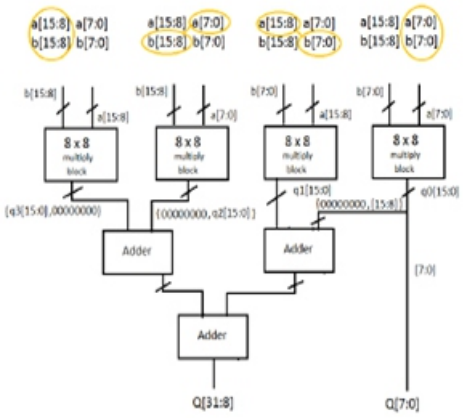

Fig 5.16 bit vedic multiplier

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 systsm are as shown in fig 6.

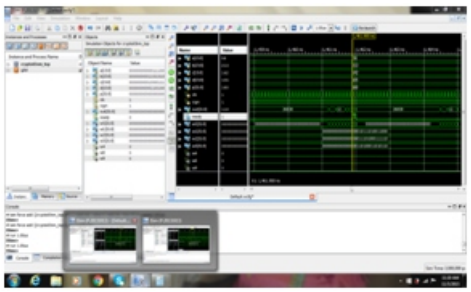

Fig6.simulation result

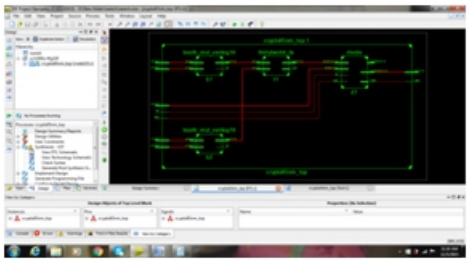

Fig 7.RTL schematic.

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

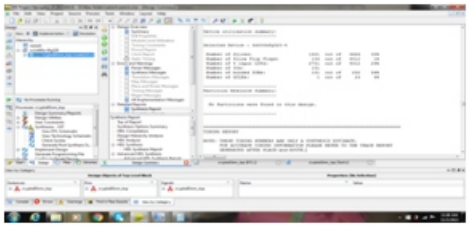

Fig 8.synthesis report of existing system

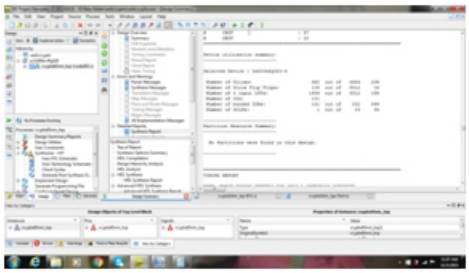

Fig 9.synthesis report of proposed system

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

V. CONCLUSION:

This paper proposed a cryptographic processor that performshigh speed computation of optimal ate pairing. Hardwareunits dedicated to fast calculation of Fp2 arithmeticsspeedup the processor. Moreover, exploiting the parallelism in pairing algorithm and employing efficient memory accessmechanism also contribute to performance acceleration.Finally we achieved area efficiency by using vedic multiplier in place booth multiplier.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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 PublicKey—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 implementationof 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 forMontgomery'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.

[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 modular multiplication," in Proc. 12th