IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 4, April 2015.
www.ijiset.com
ISSN 2348 – 7968

Study Of Hardware Design Of High Speed Modular Multiplier

Yamini Banjare[1], Vishal Moyal[2]

(Student[1] of M.E (VLSI design), associate professor[2] of Shri Shankaracharya Technical Campus (SSGI), Bhilai, Chhattisgarh)

Abstract

Many public key cryptographic algorithms require modular multiplication of very large operands as their core arithmetic operation. To perform this operation reasonably fast is to use specialized hardware. However large sizes are often required to increase security. This comes at the expense of either reducing the clock rate or dramatically increasing the size and hence the cost of system. In this paper there is a study of the hardware of the modular multiplier which is drawn in different design style. There are a study of two design of modular multiplier. This paper shows the study about design and component used for the fast computation. In this paper there is study of the two different technologies and these designs operating frequency, delays, required area and there consumed power. This paper shows the study about the various parameters of implementing the high speed computing modular multiplier.

Introduction

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 moduli, 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.

In the design (I) there was a scalable Montgomery multiplier used a small processing element with fixed word size multiple times to process very long operands. Their used hardware disable carry propagation in the latter case. Their used circuit implementation reduces the inter outer loop pipeline stall from two cycle resulting in shorter latencies.

Design (II) was proposed by Yang Li et al.they proposed new feature of arithmetic involved in pairing to find more space for refinement. In design II two Fp multipliers based on residue number system (RNS) combined with lazy reduction technique targeting to FPGA platforms are proposed.

ISSN 2348 – 7968

The RNS based approach achieves high performance benefitting from lazy reduction and deep pipelines, but double precision arithmetic, multiple memory and register banks required in designs impose heavy hardware cost. Their proposed modular multiplier had two main parts

1. Efficient pipelined data path
2. Partial products generators

Their efficient pipeline architecture of the proposed multiplier. They chose radix r=53,n=6 and β=2^4 to archive suitable tradeoffs between performance and hardware complexity. They use booth encoding to reduce the no for partials products. Partial products are selected from possible values (0, X, 2X,-X,-2X) by control signals generated from booth controller. This design choice was aiming at booth encoding.

Hardware description

Design (I)

The first design was proposed by Mathew et al [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 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.

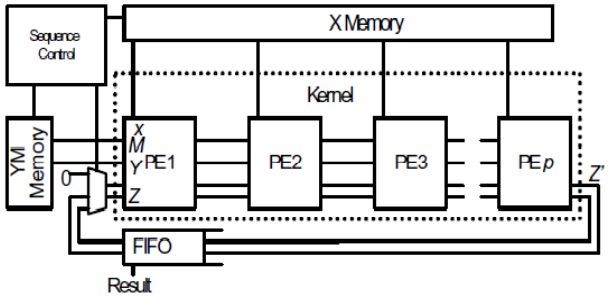

Figure 1: Montgomery multiplier block diagram

Processing element

In each processing element used carry save adder to add the partial product word (xi Y) to the accumulating result Zj. A second CSA was used to conditionally add in the modulus M, after testing the odd bit is computed and stored in first cycle of each outer loop iteration. System throughput is increased by processing the accumulating result Z in carry save redundant from within the loops and converting to non redundant binary form in the last cycle of the inner loop gives priorities to storage in the FIFO. That conversion reduces the FIFO size to prior implementations, without impacting multiplier latency. This design schematic diagram shown in figure (2)[1]. This circuit having two transistors named f_{sel} to the carry gate (fig.2) of CSA. This gate computes the majority function of its inputs (S,P,C) and kills the carry (C_{out},Z_c).

ISSN 2348 – 7968

The processing elements are arranged in a systolic array, called kernel. This kernel handles many bits.

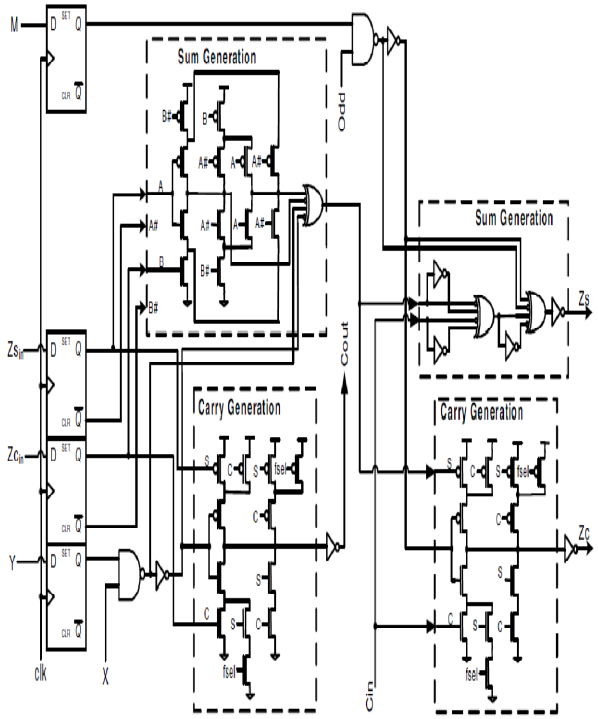

Fig. 2 processing element schematic diagram

Design (II)

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 fp2 multiplication 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 (3)[2].

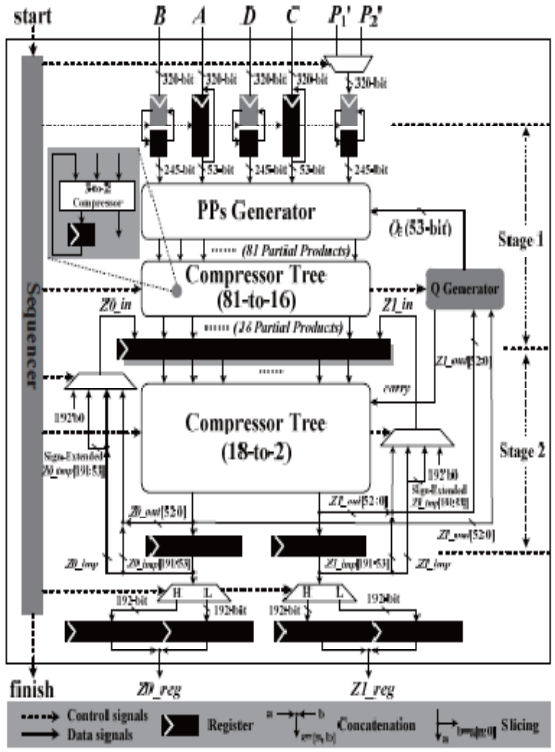

Fig. 3 architecture of combined Montgomery multiplier

Design two having two main blocks there descriptions are as follows:

1. **Efficient pipelined data path**: the efficient pipeline architecture of the proposed multiplier. They chose radix r=53, n=6 and β=2^4 to achieve the suitable tradeoff between performance and hardware complexity. They designed using four booth encoder to reduce the number of partial products. In this design CSA tree was used to accumulate 81 PPs. The compressor tree was implemented in pipelined fashion because it is easy to carry propagation problem. This compression process was split in two

ISSN 2348 – 7968

smaller limbs that are executed sequentially

2. **Partial products generator**: the partial products are selected from possible values (0, X, 2X, -X, 2X) by control signals generated from booth controller. Selection signals are pre evaluated by one cycle earlier. This design choice was aiming at reducing the latency of booth encoding.

Conclusion

Design (I) was implemented in 90nm technology, its operating frequency was quit high as 2.4 GHz. Pipelined structure performed faster and it consumes 69mW power. This can be easily scaled to handle wider modular multiplications.

Design (II) was implemented in 65nm technology. Its operating frequency was 800 MHz and its computation time was 0.64ms. Its area was 2.51mm^2.

BIBLIOGRAPHY

[1] David Harris,Mark Anders, Steven Hsu and Ram krishnmurthy Sanu Mathew, "A 2.4GHz 256/1024-bit Encryption Accelerator Reconfigurable Montgomery," in *IEEE Int. SOC Conf.*, 2007, pp. 25-28.

[2] Jun Han, Shuai Wang, Dabin Fang and Xiaoyang Zeng Yang Li, "A 800Mhz Cryptograhic pairing processor in 65nm CMOS," in *IEEE Asian Solid State circuits Conference*, Kobe ,JAPAN, 2012.

[3] Yang Li, Zhiyi Yu, and Xiaoyang Zeng Jun Han, "A 65 nm Cryptographic Processor for high speed pairing computation," in *IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS*, Shanghai, 2014.

[4] A. Bouridane and M. Nibouche O. Nibouche, "Architectures for Montgomery's multiplication," in *IEEE Proc. Comput. Digit. Tech*, 2003, pp. 361-368.

[5] R.Jacob Baker, *CMOS CIRCUIT DESIGN, LAYOUT AND SIMULATION*, 2nd ed., IEEE Press series on microelectornics, Ed. India: Wilet India Pvt Ltd, 2005.

[6] Yusuf Leblebici Sung Mo Kang, *CMOS Digital Integrated circuits*, 3rd ed. India: Mcgrew hills.