© 2018 IJSRST | Volume 4 | Issue 2 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

VLSI Implementation of High Performance Montgomery Modular Multiplication

M. Sravan Kumar, B. Jyothi Priya
Assistant Professor, Tadipatri Engineering College, Tadipatri, Anantapur, India

ABSTRACT

The multiplier gets and yields the information with paired portrayal and uses just a single level Carry Save Adder (CSA) to maintain a strategic distance from the convey proliferation at every expansion operation. This CSA is additionally used to perform operand pre calculation and arrangement transformation from the convey spare organization to the paired portrayal, prompting a low equipment cost and short basic way delay to the detriment of additional clock cycles for finishing one particular duplication. To conquer the shortcoming, a Configurable CSA (CCSA), which could be one full-viper or two serial half-adders, is proposed to decrease the additional clock cycles for operand pre calculation and organization change significantly. The system that can distinguish and avoid the pointless convey spare expansion operations in the one-level CCSA engineering while at the same time keeping up the short basic way delay is created. The additional clock cycles for operand pre calculation and organization change can be covered up and high throughput can be gotten.

Keywords : CCSA, Clock Cycles, Montgomery Modular Multiplication, VLSI, SCS, FCS

I. INTRODUCTION

In Many open key cryptosystems [1]– [3], particular duplication (MM) with substantial numbers is the most basic and tedious operation.Therefore, various calculations and equipment usage have been exhibited to complete the MM all the more rapidly, and Montgomery's calculation is a standout amongst the most surely understood MM calculations. Montgomery's calculation [4] decides the remainder just relying upon the slightest huge digit of operands and replaces the convoluted division in traditional MM with a progression of moving particular increases to create $S = A \times B \times R–1 \pmod N$, where N is the k-bit modulus, R–1 is the opposite of R modulo N, and $R = 2k \bmod N$. Subsequently, it can be effortlessly executed into VLSI circuits to accelerate the encryption/decoding process. In any case, the three-operand expansion in the cycle circle of Montgomery's requires long convey engendering for extensive operands in paired portrayal. To take care of this issue, a few approachesof in view of convey spare expansion were proposed to accomplish a huge speedup of Montgomery MM. In view of the portrayal of information and yield operands, these methodologies can be generally partitioned into semi-convey spare (SCS) technique and full convey spare (FCS) methodology. In the SCS technique [5]– [8], the info and yield operands (i.e., A, B, N, and S) of the Montgomery MM are spoken to in twofold, however middle of the road consequences of moving secluded increases are kept in the convey spare arrangement to maintain a strategic distance from the convey proliferation. Be that as it may, the organization transformation from the convey spare arrangement of the last measured item into its paired portrayal is required toward the finish of every MM. This transformation can be proficient by an additional convey proliferation snake (CPA) [5] or reusing the convey spare viper (CSA) design [8] iteratively. In spite of the SCS system, the FCS procedure [9], [10] keeps up the information and yield operands A, B, and

S in the convey spare arrangement, signified (AS, AC), (BS, BC), and (SS, SC), separately, to stay away from the organization change, prompting less clock cycles for finishing a MM. By and by, this procedure infers that the quantity of operands will increment and that more CSAs and registers for managing these operands are required. Hence, the FCS-based Montgomery measured multipliers conceivably have higher equipment many-sided quality and longer basic way than the SCS-based multipliers.

II. PROPOSED ARCHITUCTURE

2.1. Montgomery Modular Multiplier

In propose another SCS-based Montgomery MM calculation to diminish the basic way postponement of Montgomery multiplier. Moreover, the downside of more clock cycles for finishing one augmentation is likewise enhanced while keeping up the upsides of short basic way postponement and low equipment intricacy [2].

2.2. Basic Path Delay Reduction

The basic way postponement of SCS-based multiplier can be diminished by consolidating the upsides of FCS-MM-2 and SCS-MM-2. That is pre register D = B + N and reuse the one-level CSA design to perform B+N and the configuration change. Figure.1 demonstrates the changed SCS-based Montgomery increase (MSCS-MM) calculation and conceivable equipment engineering, individually [3].

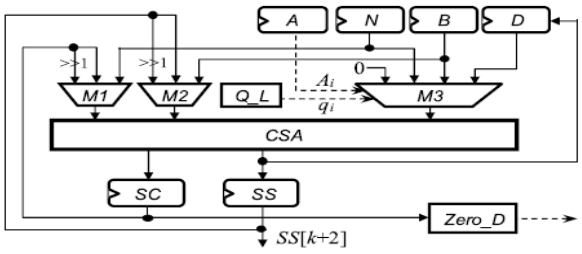


Figure 1. Diagram of Montgomery Modular Multiplier

The Zero_D circuit is utilized to identify whether SC is equivalent to zero, which can be refined utilizing one NOR operation. The Q_L circuit chooses the qi esteem. The convey proliferation expansion operations of B + N and the arrangement transformation are performed by the one-level CSA engineering of the MSCS-MM multiplier through more than once executing the convey spare expansion (SS, SC) = SS + SC + 0 until SC = 0.In expansion, we additionally pre register Ai and qi in cycle i–1 (this will be clarified all the more unmistakably in Section III-C) with the goal that they can be utilized to promptly choose the coveted info operand from 0, N, B, and D through the multiplexer M3 in emphasis I [5] . Along these lines, the basic way postponement of the MSCS-MM multiplier can be decreased into TMUX4 + TFA. In any case, notwithstanding playing out the three-input convey spare augmentations k + 2 times, numerous additional clock cycles are required to perform B + N and the arrangement change by means of the one-level CSA engineering since they should be performed once in each MM. Moreover, the additional clock cycles for performing B+N and the organization change through over and over executing the convey spare option (SS, SC) = SS+SC+0 are subject to the longest convey engendering chain in SS + SC. On the off chance that SS = 111… 1112 and SC = 000… 0012, the one-level CSA engineering needs k clock cycles to finish SS + SC. That is, 3k check cycles in the most pessimistic scenario are required for finishing one MM. In this manner, it is basic to lessen the required clock cycles of the MSCS-MM multiplier [1].

To dodge the basic and tedious operation in secluded duplication when expansive operands are included a few strategies have been proposed. Montgomery's calculation is a standout amongst the most surely understood secluded duplication calculations [18] performed with less basic components and less tedious time when substantial operand utilized like exponentiation. The calculation utilizes manages the minimum noteworthy digit of operands and replaces the division operation with a progression of moving particular increases. Strategies are required to limit

the defer included when long convey spread for expansive operands in paired portrayal. Convey spare expansion accomplishes a decrease in defer an arranged into semi convey spare (SCS) and full convey spare (FCS) strategy. In the SCS technique, the information and yield operands (i.e., A B N and S) of the Montgomery MM are spoken to in twofold, however middle of the road consequences of moving secluded increases are kept in the convey - spare organization to maintain a strategic distance from the convey engendering. The FCS procedure keeps up the info and yield operands A B, and S in the convey spare organization, signified as (AS AC), (BS, BC), and (SS SC) separately, to evade the organization transformation, prompting less clock cycles for finishing a MM. All things considered, this methodology suggests that the quantity of operands will increment and that more CSAs and registers for managing these operands are required. Thusly, the FCS - based Montgomery secluded multipliers conceivably have higher equipment many-sided quality and longer basic way than the SCS-based multipliers. A SCS-Based Montgomery Multiplication is appeared in figure 1 which lessens the postponement because of long convey spread

2.3. Clock Cycle Number Reduction

To diminish the clock cycle number, a CCSA design which can perform one three-input convey spare expansion or two serial two-input convey spare augmentations is proposed to substitute for the one-level CSA engineering [4]. Two cells of the one-level CSA engineering in Figure.2each cell is one ordinary FA which can play out the three-input convey spare expansion. Two cells of the proposed configurable FA (CFA) circuit. In the event that α = 1, CFA is one FA and can perform one three-input convey spare expansion (indicated as 1F_CSA).

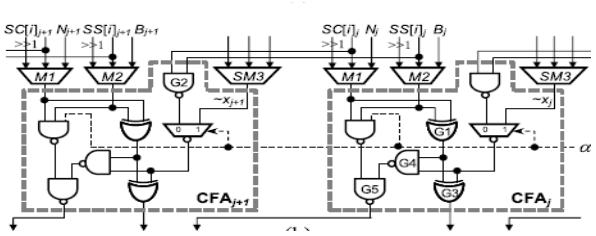
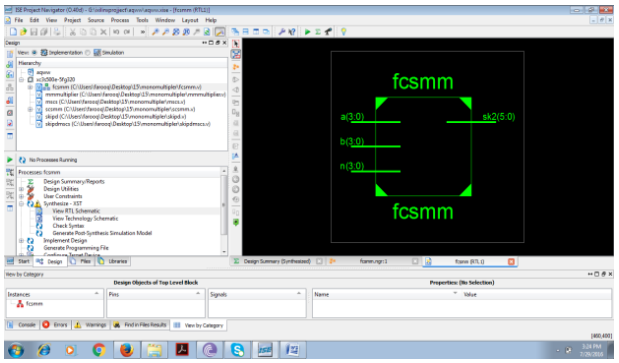
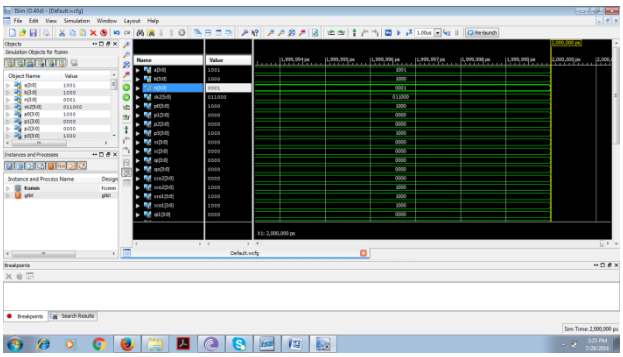


Figure 2. Carry Full Adder Circuit Otherwise,

it is two half-adders (HAs) and can perform two serial two-input carry-save additions (denoted as 2H_CSA). In this case, G1 of CF Aj and G2 of CFAj+1 will act as HA1 j and G3, G4, and G5 of CF Aj will behave as HA2j. Moreover, we modify the 4-to-1 multiplexer M3 into a simplified multiplier SM3 because one of itsinputs is zero, where the INVERT operation. Note that M3 has been replaced by SM3 in the proposed one-level CCSA architecture.

III. RESULTS





IV. CONCLUSION

To enhance the performance of Montgomery MM while maintaining the low hardware complexity, this paper has modified the SCS-based Montgomery multiplication algorithm a low-cost and high-

performance Montgomery modular multiplier. The multiplier used one-level CCSA architecture and skipped the unnecessary carry-save addition operations to largely reduce the critical path delay and required clock cycles for completing one MM operation. FCS-based multipliers maintain the input and output operands of the Montgomery MM in the carry-save format to escape from the format conversion, leading to fewer clock cycles but larger area than SCS-based multiplier

V. REFERENCES

[1]. Amber.P, Pinckney.N, and Harris, DM"Parallel high-radix Montgomery multipliers,"(2008) in Proc42nd Asilomar ConfSignals, Syst., Comput., pp772-776

[2]. Bunimov.V, Schimmler.M, and Tolg.B, "A complexity-effective version of Montgomery's algorihm," (2002) in ProcWorkshop Complex.Effective Designs

[3]. Gang.F, "Design of modular multiplier based on improved Montgomery algorithm and systolic array," (2006) in Proc1st IntMulti-SympComputCo mputSci., vol2Jun2006, pp356-359

[4]. Han, JWang S., Huang W., Yu Z., and Zeng X, "Parallelization of radix-2 Montgomery multiplication on multicore platform,"(2013) IEEE TransVery Large Scale Integr(VLSI) Syst., vol21, no12, pp2325-2330,

[5]. Kuang S.-R., Wang J.-P., Chan K.-C., and HsuH.-W., "Energy-efficient high-throughput Montgomery modular multipliers for RSA cryptosystems," (2013) IEEE TransVery Large Scale Integr(VLSI) Syst., vol21, no11,pp1999-2009,

[6]. McIvor.C, McLoone.M, and McCanny, JV"Modified Montgomery modular multiplication and RSA exponentiation techniques,"(2004) IEE Proc.-ComputDigitTechn., vol151, no6, pp402-408,

[7]. Miyamoto A., Homma N., Aoki, Tand Satoh.A, "Systematic design of RSA processors based on high-radix Montgomery multipliers,"(2011) IEEE TransVery Large Scale Integr(VLSI) Syst., vol19, no7, pp1136-1146

[8]. Neto, JCTenca AF., and Ruggiero WV., "A parallel k-partition method to perform Montgomery multiplication,"(2011) in ProcIEEE IntConfAppl.-Specific Syst., Archit., Processors, , pp251-254

[9]. Sassaw.G,Jimenez.C.J, and Valencia.M, "High radix implementation of Montgomery multipliers with CSA," (2010) in ProcIntConfMicro electron., Dec2010, pp315-318

[10]. Saemen.J and Rijmen.V, The block cipher Rijndael, Smart Card research and Applications, (2010)LNCS 1820, Springer-Verlag, pp288-296

[11]. Wang S.-H., Lin W.-C "Fast scalable radix-4 Montgomery modular multiplier," (2012) in ProcIEEE IntSympCircuits Syst., , pp3049-3052

[12]. Yee.A, Guideline for Implementing Cryptography in the Federal Government, National Institute of Standards and Technology, (1999),NIST Special Publication 800-21