LeMeniz Infotech

36, 100 Feet Road, Natesan Nagar, Near Indira Gandhi Statue, Pondicherry-605 005.

Call: 0413-4205444, +91 9566355386, 99625 88976.

Web : www.lemenizinfotech.com / www.ieeemaster.com

Mail : projects@lemenizinfotech.com

Low-Cost High-Performance VLSI Architecture for Montgomery Modular Multiplication

Abstract:

This paper proposes a simple and efficientMontgomery multiplication algorithm such that the low-costand high-performance Montgomery modular multiplier can beimplemented accordingly. The proposed multiplier receives andoutputs the data with binary representation and uses onlyone-level carry-save adder (CSA) to avoid the carry propagationat each addition operation. This CSA is also used to performoperand pre-computation and format conversion from the carrysave format to the binary representation, leading to a lowhardware cost and short critical path delay at the expense of extra clock cycles for completing one modular multiplication.To overcome the weakness, a configurable CSA (CCSA), whichcould be one full-adder or two serial half-adders, is proposed toreduce the extra clock cycles for operand pre-computation andformat conversion by half. In addition, a mechanism that candetect and skip the unnecessary carry-save addition operationsin the one-level CCSA architecture while maintaining the shortcritical path delay is developed. As a result, the extra clock cyclesfor operand pre-computation and format conversion can be hiddenand high throughput can be obtained. Experimental resultsshow that the proposed Montgomery modular multiplier can achieve higher performance and significant area–time productimprovement when compared with previous designs.Using VHDL to design the RTL, and the result to be shown in Xilinx 14.2 with Power consumption and area reduction.

Enhancement of the project:

Increase the size of the data values or use different adder for the addition operation

Existing System:

In existing system the SCS based Montgomery multiplier design having more hardware complexity and short critical path will be lessened. To overcome the weakness,we then modify the one-level CSA architecture to be ableto perform one three-input carry-save addition or two serialtwo-input carry-save additions, so that the extra clock cyclesfor format conversion can be reduced byhalf. Finally, the condition and detection circuit, which aredifferent with that of FCS-MMM42 multiplier, and also developed to pre-compute quotients and skip the unnecessarycarry-save addition operations in the one-level configurableCSA (CCSA) architecture whilekeeping a short critical pathdelay.Therefore, the required clock cycles for completing oneMM operation can be significantly reduced. As a result, theproposed Montgomery multiplier can obtain higher throughputand much smaller area-time product (ATP) than previousMontgomery multipliers.

LeMeniz Infotech

36, 100 Feet Road, Natesan Nagar, Near Indira Gandhi Statue, Pondicherry-605 005.

Call: 0413-4205444, +91 9566355386, 99625 88976.

Web : www.lemenizinfotech.com / www.ieeemaster.com

Mail : projects@lemenizinfotech.com

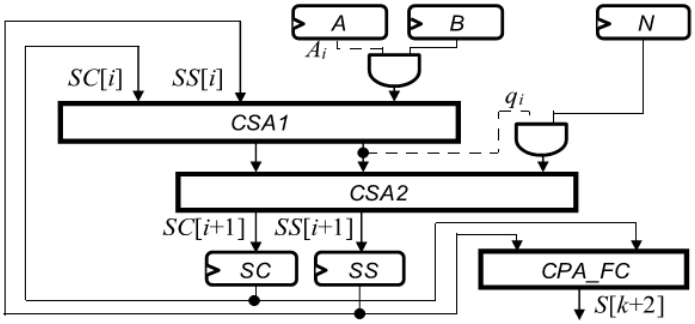

Fig a. SCS based Montgomery multiplier 1

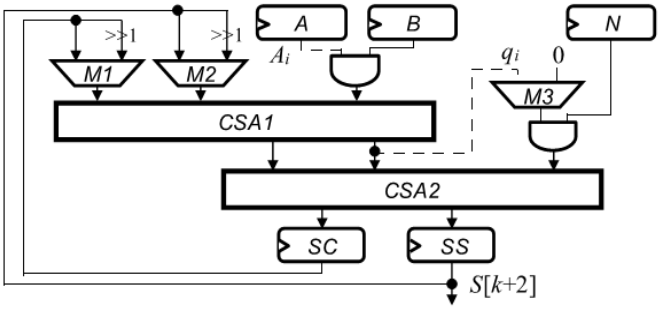

Fig b. SCS based Montgomery multiplier 2

Disadvantages:

1. Short Critical path
2. More hardware complexity
3. More Power consumption
4. More Cost

Proposed System:

We are propose a new SCS-based MontgomeryMM algorithm to reduce the critical path delay of Montgomerymultiplier. In addition, the drawback of more clock cyclesfor completing one multiplication is also improved whilemaintaining the advantages of short critical path delay andlow hardware complexity.

LeMeniz Infotech

36, 100 Feet Road, Natesan Nagar, Near Indira Gandhi Statue, Pondicherry-605 005.

Call: 0413-4205444, +91 9566355386, 99625 88976.

Web : www.lemenizinfotech.com / www.ieeemaster.com

Mail : projects@lemenizinfotech.com

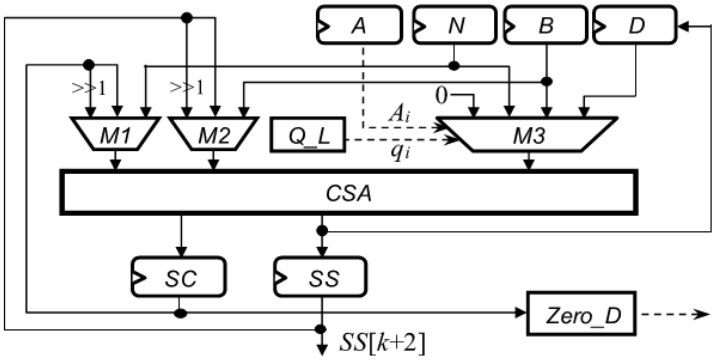

Fig c. Modified SCS based Montgomery multiplication

On the bases of critical path delay reduction, clock cyclenumber reduction, and quotientpre-computation reduction. A new SCS-based Montgomery MM algorithmusingone-level CCSA architecture is proposed to significantlyreduce the required clock cycles for completing one MM.As shown in SCS-MM-New algorithm will be shown below,

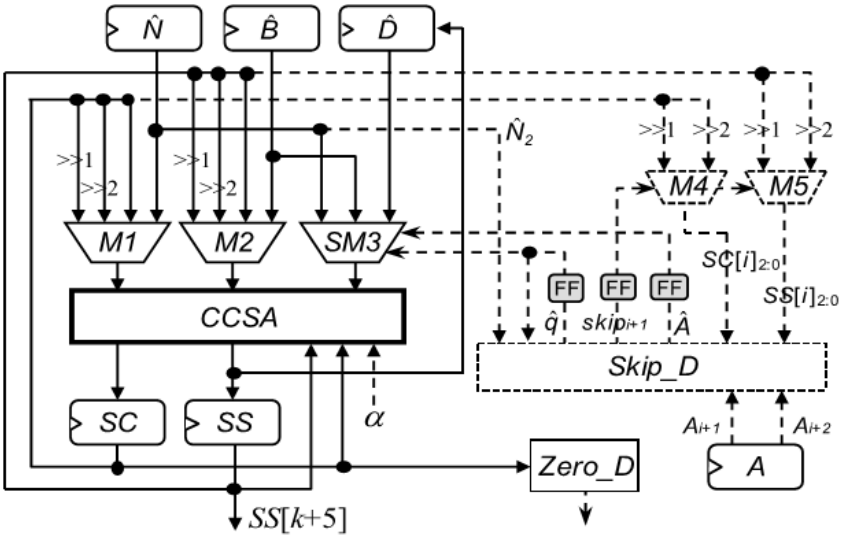

Fig d. Proposed SCS based Montgomery multiplier

Advantages:

1. Reduced Critical path
2. Less Hardware Complexity
3. Less Power Consumption
4. High Performance

Software Implementation:

1. Modelsim

2. Xilinx 14.2