International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 09
August 2017

A Survey on Montgomery Modular Multiplication for High-Performance

Boggarapu Kantha Rao [1], Pola Pavithra [2] & Sk.Mujafar Ahmed [3]
[1]HOD & Assoc Prof, Medha Institute of Science & Technology for Women, Khammam,
[2]M-Tech, Medha Institute of Science& Technology for Women, Khammam,
[3]Associate Professor, Medha Institute of Science& Technology for Women, Khammam,
E-mail:- kantharao.b@gmail.com; Email: - pavithra.pola@gmail.com
Email: - mujju87@gmail.com

Abstract

This paper proposes a basic and efficient Montgomery duplication calculation to such an extent that the ease and elite Montgomery particular multiplier can be actualized in like manner. The proposed multiplier gets and yields the information with paired portrayal and uses just a single level convey save snake (CSA) to sidestep the convey spread at every additament operation. This CSA is moreover used to perform operand pre computation and configuration transformation from the carry save organization to the twofold portrayal, prompting a low equipment cost and short basic way delay to the detriment of additional clock cycles for culminating one secluded augmentation. To surmount the impotency, a configurable CSA (CCSA), which could be one full-viper or two serial half-adders, is proposed to diminish the additional clock cycles for operand precipitation and configuration transformation by a moiety. In coordination, a component that can distinguish and skirt the superfluous convey protect joining operations in the one-level CCSA design while keeping up the short basic way delay is produced. Accordingly, the additional clock cycles for operand precomputation and organize change can be hidden and high throughput can be acquired. Trial comes about demonstrate that the proposed Montgomery measured multiplier can accomplish higher execution and significant area–time item enhancement when contrasted and precursor plans.

Key words: - Carry-Save Addition, Low-Cost Architecture, Montgomery Modular Multiplier, Public-Key Cryptosystem, Computation in finite fields, Computer arithmetic, Montgomery multiplication,

Parallel arithmetic and logic structures.

INTRODUCTION

In MANY public-key cryptosystems, modular multiplication (MM) with immensely colossal integers is the most critical and time-consuming operation. [1] [2]Consequently, numerous algorithms and hardware implementation have been presented to carry out the MM more expeditiously, and Montgomery's algorithm is one of the most well-kenned MM algorithms. [3]Montgomery's algorithm determines the quotient only depending on the least paramount digit of operands and supersedes the intricate division in conventional MM with a series of shifting modular integrations to engender $S = A \times B \times R^{-1} \pmod N$, where N is the k-bit modulus, R^{-1} is the inverse of R modulo N, and $R = 2^k \bmod N$.[4] As a result, it can be facilely implemented into VLSI circuits to expedite the encryption/decryption process. [6]-[7]To solve this quandary, several approaches predicated on carry-preserve integration were proposed to achieve a paramount speedup of Montgomery MM. Predicated on the representation of input and output operands, these approaches can be roughly divided into semi-carry-preserve (SCS) strategy and full carry-preserve (FCS) strategy. In the SCS strategy [5]–[8], the input and output operands (i.e., A, B, N, and S) of the Montgomery MM are represented in binary, but intermediate results of shifting modular integrations are kept in the carry-preserve format to eschew the carry propagation. However, the format conversion from the carry-preserve format of the final modular product into its binary representation is needed at the cessation of each MM. [9]This conversion can be accomplished by an extra carry propagation adder (CPA) or reusing the carry-preserve adder (CSA) architecture iteratively.[10] Nevertheless, this strategy implicatively insinuates that the number of operands will increment . Ergo, the FCS-predicated Montgomery modular multipliers possibly have higher hardware intricacy and longer critical path than the SCS-predicated multipliers.

2. MODULAR MULTIPLICATION ALGORITHMS

2.1 Montgomery Multiplication

As said before, the Montgomery measured item S of An and B can be gotten as $S = A \times B \times R^{-1} \pmod N$, where R^{-1} is the backwards of R modulo N. That is, $R \times R^{-1} = 1 \pmod N$. Note that, the documentation

Xi in Fig. 1 demonstrates the i th bit of X in twofold portrayal. In mix, the documentation Xi : j betokens a portion of X from the i th bit to j th bit.

Since the merging scope of S in MM calculation is $0 \leq S < 2N$, an additional operation $S = S - N$ is required to extract the curiously large deposit if $S \geq N$. To take out the last examination and subtraction in step 6 of Fig. 1, Walter transmuted the quantity of cycles and the estimation of R to k + 2 and 2k+2 mod N, separately. In any case, the long convey spread for the significantly and cosmically huge operand additament still confines the execution of MM calculation.

2.2SSC-BasedMontgomery Multiplication

To shun the long convey engendering, the middle outcome S of moving particular incorporation can be kept in the convey save portrayal (SS, SC). Note that the quantity of cycles has been transmuted from k to k + 2 to extract the last correlation and subtraction. Be that as it may, the organization transformation from the convey safeguard arrangement of the last particular item into its twofold configuration is required. demonstrates the engineering of SCS-predicated MM calculation proposed in (signified as SCS-MM-1 multiplier) made out of one two-level CSA archi-tecture and one organization converter, where the dashed line signifies a 1-bit flag. In a 32-bit CPA with multiplexers and registers (indicated as CPA_FC), which incorporates two 32-bit sources of info and induces a 32-bit yield at each clock cycle, was embraced for the configuration change. Consequently, the 32-bit CPA_FC will take 32 clock cycles to perfect the arrangement con-form of a 1024-piece SCS-predicated Montgomery augmentation. The additional CPA_FC presumably develops the zone and the basic way of the SCS-MM-1 multiplier.

The works in precomputed D = B + N so that the calculation of Ai × B + qi × N can be rearranged into one separate operation. One of the operands 0, N, B, and D will be separated if (Ai , qi) = (0, 0), (0, 1), (1, 0), and (1, 1), individually. Therefore, just a single level CSA engineering is required in this multiplier to play out the convey protect combination to the detriment of one additional 4-to-1 multiplexer and one supplemental enroll to store the operand D. Be that as it may, they didn't present an effective way to deal with theoretical the CPA_FC for arrange change and along these lines this sort of multiplier still experiences the basic way of CPA_FC.

2.3FCS-BasedMontgomery Multiplication

To dodge the arrangement change, FCS-predicated Montgomery increase keeps up A, B, and S in the convey save portrayals (AS, AC), (BS, BC), and (SS, SC), two (three-level) and one four-to (two-level) CSA design, individually.. The barrel enlist full viper (BRFA) comprises of two move registers for putting away AS and AC, a full viper (FA), and a flip-tumble (FF).On the other hand, the FCS-MM-2 multiplier proposed in [9] incorporates up BS, BC, and N into DS and DC at the beginning of every MM. Therefore, the profundity of the CSA tree can be diminished from three to two levels. In any case, the FCS-MM-2 multiplier needs two additional 4-to-1 multiplexers tended to by Ai and qi and two more registers to store DS and DC to decrease one level of CSA tree. Subsequently, the basic way of the FCS-MM-2 multiplier might be barely diminished with a considerable increment in equipment range when contrasted and the FCS-MM-1 multiplier.

3. EXPERIMENTAL RESULTS

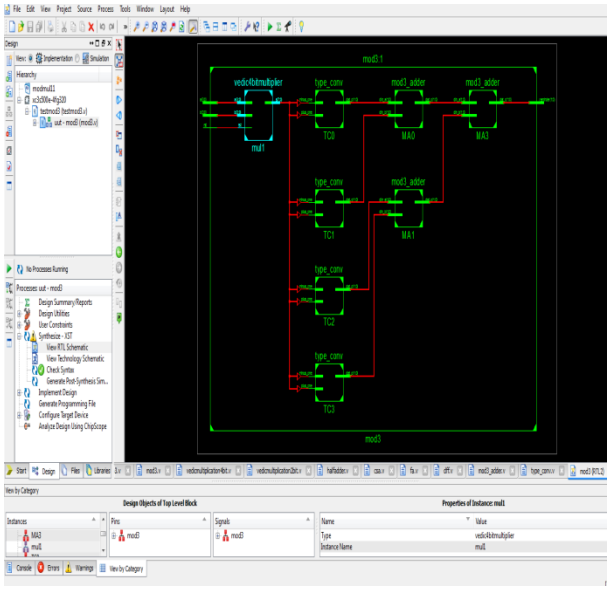

Fig 1 Schematic Output

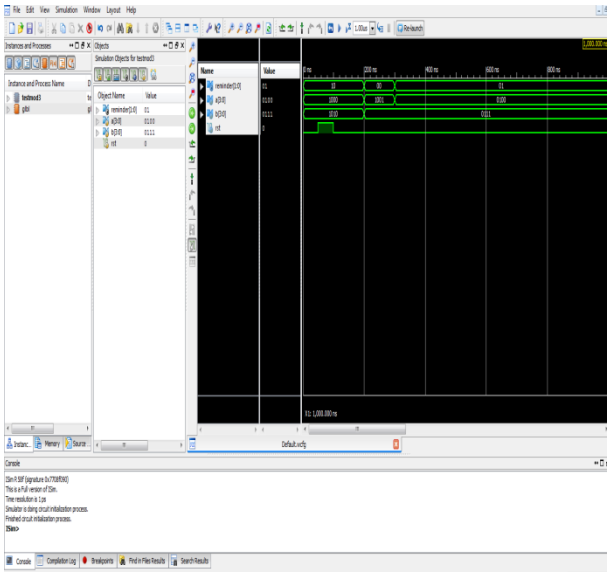

Fig 2 Simulation output.

4. CONCLUSION

FCS-predicated multipliers keep up the info and yield operands of the Montgomery MM in the convey safeguard organization to evade from the arrangement transformation, prompting less clock cycles however more enormously giant zone than SCS-predicated

multiplier. To improve the execution of Montgomery MM while keeping up the low equipment multifaceted nature, this paper has modified the SCS-predicated Montgomery duplication calculation and proposed an ease and superior Montgomery measured multiplier. The proposed multiplier utilized one-level CCSA engineering and skirted the superfluous convey protect additament operations to a great extent diminish the basic way delay and required clock cycles for culminating one MM operation. Trial comes about demonstrated that the proposed approaches are for sure fit for upgrading the execution of radix-2 CSA-predicated Montgomery multiplier while keeping up low equipment multifaceted nature.

5. REFERENCE

[1] R. L. Rivest, A. Shamir, and L.Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[2] V. S. Miller, "Use of elliptic curves in cryptography," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 1986, pp. 417–426.

[3] N. Koblitz, "Elliptic curve cryptosystems," Math. Comput., vol. 48, no. 177, pp. 203–209, 1987.

[4] P. L. Montgomery, "Modular multiplication without trial division," Math. Comput., vol. 44, no. 170, pp. 519–521, Apr. 1985.

[5] Y. S. Kim, W. S. Kang, and J. R. Choi, "Asynchronous implementation of 1024-bit modular processor for RSA cryptosystem," in Proc. 2nd IEEE Asia-Pacific Conf. ASIC, Aug. 2000, pp. 187–190.

[6] V. Bunimov, M. Schimmler, and B. Tolg, "A complexity-effective version of Montgomery's algorihm," in Proc. Workshop Complex. Effective Designs, May 2002.

[7] H. Zhengbing, R. M. Al Shboul, and V. P. Shirochin, "An efficient architecture of 1024-bits cryptoprocessor for RSA cryptosystem based on modified Montgomery's algorithm," in Proc. 4th IEEE Int. Workshop Intell. Data Acquisition Adv. Comput. Syst., Sep. 2007, pp. 643–646. [8] Y.-Y. Zhang, Z. Li, L. Yang, and S.-W. Zhang, "An efficient CSA architecture for Montgomery modular multiplication," Microprocessors Microsyst., vol. 31, no. 7, pp. 456–459, Nov. 2007.

[9] C. McIvor, M. McLoone, and J. V. McCanny, "Modified Montgomery modular multiplication and RSA exponentiation techniques," IEE Proc.Comput. Digit. Techn., vol. 151, no. 6, pp. 402–408, Nov. 2004.

[10] S.-R. Kuang, J.-P. Wang, K.-C. Chang, and H.-W. Hsu, "Energy-efficient high-throughput Montgomery modular multipliers for RSA cryptosystems," IEEE Trans. Very Large Scale Integr. (VLSI)Syst.,vol.21,no.11,pp.1999–2009,Nov.2013

AUTHOR-1

Boggarapu Kantha Rao, HOD & Assoc Prof, Medha Institute Of Science & Technology For Women,Khammam, B.KANTHA RAO received his B.Tech degree in Electronics And Communication Engineering from Adams Engineering College,Paloncha,JNTUH in 2006 and M.Tech in EMBEDDED SYSTEMS from Anurag Engineering College,kodad, JNTUH in 2011,is a faculty member in the Department of Electronics And Communication Engineering, Medha Institute Of Science& Technology For Women, Khammam and presently working as Associate Professor. His research interests include Embedded Systems, VLSI Design.E-mail:kantharao.b@gmail.com.

AUTHOR-2

Pola Pavithra bearing Roll no. : 156C1D6814 pursuing M.Tech in VLSI & Embedded Systems branch in Medha Institute of Science & Technology for Women. My area of intrest are vlsi ,embeddedsystems and network on chip

Mail I'D: pavithra.pola@gmail.com

AUTHOR 3:

SK.MUJAFAR AHMED Associate Professor received his B.Tech degree in Electronics And Communication Engineering from Sree Kavitha

Engineering College,Karepally, JNTUH in 2005 and M.Tech in Systems And Signal Processing from Adams Engineering College,Palwancha in 2011,is a faculty member in the department of Electronics And Communication Engineering, Medha Institute Of Science& Technology For Women, Khammam and presently working as Associate Professor. His research interests include Embedded systems, Signal Processing.E-mail:mujju87@gmail.com.