International Journal of Research
Available at https://edupediapublications.org/journals

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 16
June 2018

Design a Novel FFT for Fault Tolerant Razor Flip Flop

[1]P.LAKSHMI , [2]DR.K.GOUTHAMI

[1]M.Tech student, , Dept of ECE, Malineni Women's Engineering College, Guntur, Andhra Pradesh

[2]Professor &Dean, Dept of ECE, Malineni Women's Engineering College, Guntur, Andhra Pradesh.

ABSTRACT: In this paper, a cryptographic algorithm is used to perform the time consuming operations like modular multiplication operation. The time required to implement the modular multiplication is more than 75% of RSA. To minimize the delay and increase the throughput fast multiplier architectures are used. But this architectures occupy large area and gives less efficiency. So, to get high efficiency improved FFT-based Montgomery modular multiplication (MMM) algorithm is used. In existed system zero padding operation is performed to compute the modular multiplication steps.In this proposed architecture single and double butterfly structures are designed to get low area-latency solutions and these are implemented on Xilinx SPARTAN3E FPGAs.

KEY WORDS: Fast Fourier Transform (FFT), Montgomery modular multiplication (MMM),

I.INTRODUCTION

The complexity of communications and signal processing circuits increases every year. This is made possible by the CMOS technology scaling that enables the integration of more and more transistors on a single device. This increased complexity makes the circuits more vulnerable to errors. At the same time, the scalingmeans that transistors operate with lower voltages and are more susceptible to errors caused by noise and manufacturing variations. The importance of radiation-induced soft errors also increases as technology scales. Soft errors can change the logical value of a circuit node creating a temporary error that can affect the system Operation. To ensure that soft errors do not affect the operation of a given circuit, a wide variety of techniques can be used. These include the use of special manufacturing processes for the integrated circuits like, for example, the silicon on insulator. Another option is to design basic circuit blocks or complete design libraries to minimize the probability of soft errors.

In this paper it mainly focuses on hardware implementation of RSA algorithm with more than modulus length 1024-bit. The main intent in this is to create the implementations that achieve high area time efficiency. RSA algorithm is the first public key encryption and digital signature Algorithm. RSA algorithm is mainly used from smart cards to cell phones and SSL boxes. The security in RSA algorithm depends upon the difficulty of factoring a modulus n to find its two prime factors p and q. By selecting higher modulus the security in RSA algorithm is increased. In 1980s the first implementation of RSA algorithm is introduced with 512-bit modulus. Later the bit modulus is extended to 1024-bit. Various implementations are introduced but the national institute of standard and technology recommends 3072-bit or 4096-bit modulus to maintain RSA secure.

Now to compute hardware resources, RSA computation requires modular exponentiation (x^mmodN) which is computed by repeated modular multiplications. There will be direct impact on efficiency of RSA computation. So high performance modular multiplier supports 3072-bit size. To compute the modular multiplications one of the effective method is Montgomery modular multiplication (MMM). In this algorithm, the time consuming trail division is replaced by multiplication and reductions modulo R. to improve the Montgomery modular multiplication integer multiplications are multiplied. Here the existed system divides the multiplication methods into two groups mainly they are first group and second group. The first group is performed in time domain and second group is performed in both time domain and spectral domain. But here for Fast Fourier Transform (FFT) algorithm second group is applied because it produces lower asymptotic complexity. To implement hardware multiplication there are various methods of multiplicationthey are the schoolbook method, Karatsuba method and SSA.

To improve the FFT-based Montgomery product reduction (FMPR) algorithm, state of art architecture is proposed. In this the multiplication and addition steps are of MMM are performed in spectral domain and the time-spectral domain transforms are supported by FFT. Here in existed system Zero padding operation produces less efficiency. So it can be avoided by using modified version of MMM. At last we propose an FFT-based MMM algorithm under McLaughlin’s framework. Depending upon the different parameter sets the cost and cycle of FMLM has high area time efficiency.

II. EXISTED SYSTEM

The below figure (1) shows the architecture of existed system.The starting point for our work is the protection scheme basedon the use of ECCs that was presented for digital filters.This scheme is shown in Fig. 1. In this example, a simple singleerror correction Hamming code is used. The inputs to the three redundant modulesare linear combinations of the inputs and they are used to checklinear combinations of the outputs.This will be denoted asc1 check. The same reasoning applies tothe other two redundant modules that will provide checks c2andc3.Based on the differences observed on each of the checks, the moduleon which the error has occurred can be determined.

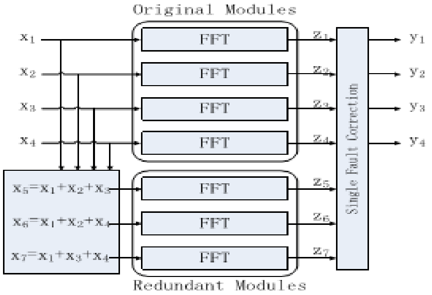

Fig. 1. Existed system

Once the module in error is known, the error can be corrected byreconstructing its output using the remaining modules. Similar correction equations can be used to correct errors on theother modules. More advanced ECCs can be used to correct errorson multiple modules if that is needed in a given application. This shows how the overhead decreaseswith the number of FFTs. So to overcome this a new system is proposed which is discussed in below section.

III. PROPOSED SYSTEM

The below figure (2) shows the architecture of proposed system. This shows the top level architecture of FMLM. The operations involved in FMLM are computed sequentially. In this the pipelined architecture is designed for each unit. The components used in architecture are multiply adder, FFT, ripple carry adder,subtractor, shift module, RAM sets. Let us discuss each of them in detail.The first and main important component in the architecture is multiply and adder unit. This unit implements the component wise multiplication and addition of FMLM.The multiplier and adder units works with pipeline of 3 bit inputs and one bit output. At last to enhance the performance of multiplication, karatsuba method is applied recursively. This is about multiply and adder unit and let us discuss about FFT unit.

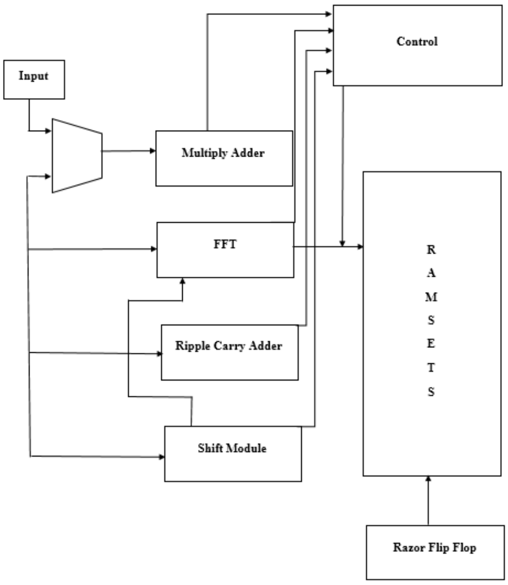

Fig. 2. Proposed system

Forward and reverse networks are formed in FFT/FFT^{-1} unit. Basically, this unit is targeted on high clock frequency and small resource cost. Here constant geometry FFT is applied to FFT computation. The FFT/FFT^{-1} is designed with six inputs. In this the four inputs forward the digits into BFSs for FFT computation and the other two inputs forward the pre-computed upper bound constraints into FSO.

Next one is RAM unit. RAM unit consists of several RAM sets which stores the pre-computed data, the intermediate results, and the final modular product. In RAM the data storage requirement during FMLM computation is not trivial. Now to well manage the input and output of data and to reduce the wiring workload, RAM unit is built. The remaining are the Ripple Carry Adder (RCA), the Subtractor and the Shift Module units are responsible for the time domain operations, such as modulo R and Q0 reductions, conditional selections. Now to generate all control signals of entire system, control unit is designed. At last it can observe that the proposed system gives better results compared to existed system.

IV. RESULTS

NOVEL_FFT
NOVEL_FFT

Fig. 3. RTL schematic

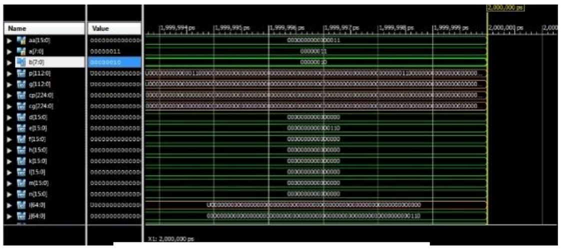

Fig. 4. Input waveform

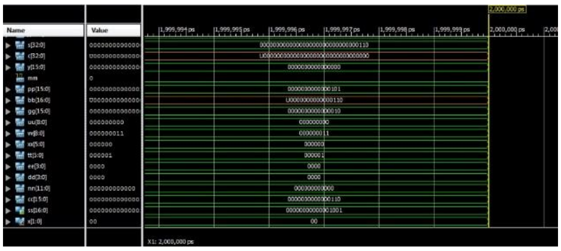

Fig. 5. Output waveform

V. CONCLUSION

A modified version of FFT depending upon the Montgomery modular multiplication algorithm is presented in this paper. Cyclic and nega cyclic convolutions are applied to algorithmto compute the modular multiplication and avoid the zero padding operations. Pipelined architectures aredesigned with one and two butterfly structures to get high efficiency. At last the proposed system gives betterefficiency compared to exist one.

VI. REFERENCES

[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, 1978.

[2] R. L. Rivest, “A description of a single-chip implementation of the RSA cipher,” Lambda, vol. 1, no. Oct.–Dec., pp. 14–18, 1980.

[3] “Recommendation for key management,” NIST, Tech. Rep. Special Publication 800-57, Part-1, Rev.-3, 2012.

[4] P. L. Montgomery, “Modular multiplication without trial division,”MathematicsComput., vol. 44, no. 170, pp. 519–521, 1985.

[5] A. Karatsuba and Y. Ofman, “Multiplication of multidigit numbers on automata,” Soviet Physics Doklady, vol. 7, 1963, Art. no. 595.

[6] S. A. Cook and S. O. Aanderaa, “On the minimum computation time of functions,” Trans.Amer.Math. Soc., vol. 142, pp. 291–314, 1969.

[7] A. Sch€onhageand V. Strassen, “SchnellemultiplikationGroßerZahlen,” Computing, vol. 7, no. 3/4, pp. 281–292, 1971.

[8] M. F€urer, “Faster integer multiplication,” SIAM J. Comput., vol. 39, no. 3, pp. 979–1005, 2009.

[9] D. Harvey, J. van der Hoeven, and G. Lecerf, “Even faster integer multiplication,” CoRR, vol. abs/1407.3360, 2014. [Online].

P.LAKSHMI completed her B.Tech in Malineni Perumallu Educational Society and M.Tech in Malineni Women’s Engineering College. Her M.Tech specialization is VLSI.

DR.K.GOUTHAMI present working as professor in Malineni Women's Engineering College Guntur, Andhra Pradesh.