National Conference on 'Innovative Research on Robotics, Circuits and Technology' (IRCT 2018)
Organized By : CIrcuit Branches of SCSVMV, (EEE, ECE, EIE & Mechatronics) , Kanchipuram, Tamil Nadu, India
In Assotiation with International Journal of Scientific Research in Science, Engineering and Technology
© 2018 IJSRSET | Volume 5 | Issue 1 | | Print ISSN: 2395-1990 | Online ISSN : 2394-4099

A Survey on low power and memory efficient VLSI architecture for million bit multiplier Design

ShakthiMurugan. K. H[1], K. Bhuvaneshwari[2]
[1]Assistant Professor, Department Of ECE, Jeppiaar Maamallan Engineering College, Vadamangalam, Tamil Nadu, India
[2]U.G.Scholar, Department Of ECE, Jeppiaar Maamallan Engineering College, Vadamangalam, Tamil Nadu, India

ABSTRACT

The motto of this proposal is to design an area and memory efficient VLSI architecture for million bit multiplier design. The proposal work split the multiplier bit into 3FIFO architecture through NTT Ram technology. The final architecture include the Synchronizer, state control module as well as 3 state FIFO buffer module .The synchronizer module is used to synchronize the NTT RAM and state controller arbiter. The state controller module gives the control signal and priority of the multiplier design. The FIFO module is used for split the million bit multiplier into 8 bit multiplier i.e 256value.here we are going to design 3fifo module ,so we can achieve 256*256*256 bits of value aprx million bit, Based on this technology we have to achieve high speed as well as low power dissipation finally memory efficient vlsi architectures.

Keywords: VLSI, FIFO, NTT, Synchronizer, Statecontroller.

I. INTRODUCTION

This brief proposes a double modulus number theoretical transform (NTT) method for million-bit integer multiplication in fully homomorphism encryption[1]. The employment of double modulus enlarges the permitted NTT sample size from 24 to 32 bits and thus improves the transform efficiency. Based on the proposed double modulus method, we accomplish a VLSI design of million-bit integer multiplier. Implementation results on SPARTON-6 FPGA

Most of the earlier works focus on reducing the multiplication time but give small concern to area efficiency. Area efficiency is also moderately significant, because high area cost implementations normally require a high-end field-programmable gate array (FPGA) platform or a high gate count ASIC platform, both of which are too costly for practical applications. The purpose of this brief is to design a fast million-bit integer multiplier without compromising its area efficiency in hardware NTT[1].

In previous works, First implemented technologies on million-bit integer multiplier using FHE processing and then consider hardware employing fast Fourier transform using recursive multiplication Algorithm[2]. Third existing an architecture design of 768k-bit multiplier on Stratix-V FPGA.In these paper consider high speed and low power dissipation memory efficient architectures[3].

FPGA Implementation of a large number multiplier for FHE explains about 1st plausible scheme for FHE and it also advance development in the field of

information security[6]. They have long latency FPGA Implementation is twice as fast as the same FFT algorithm.

Accelerating Integer Based fully Homomorphic encryption using combo multiplication explains about allows computation on encrypted data[5]. But it is not used for real time applications.

VLSI design of a large number multiplier for FHE explains discuss about power efficient based on FHE and FFT operations[7]. Optimized multiplication architectures for accelerating FHE[2] shows that speed improvement by factor of 130 is possible

II. EXISTING SYSTEM

In these design, two 1024k bits integers A and B are divided into 64k pieces of 32-bit words (the first 32k pieces are padding zeros). A and B modulo $p2 = 216 + 1$ is computed and the 17-bit result together with the unique word (modulo $p1$) are input into two 81 × 216 bits RAMs: NTT_RAM_A and NTT_RAM_B, correspondingly.

Then, two pipeline double modulus NTT units are employed to designed NTT *(A)* and NTT *(B)*.

The NTT results are put back into NTT_RAM_A and NTT_RAM_B. In the 2nd stage, the digit wise multiplication results of $C[i] = NTT(A)[i] * NTT(B)[i]$ are designed and the results are stored in a 81 × 216 bits

RAM (INTT_RAM_C). One pipeline double modulus INTT unit is employed to designed INTT*(C)* and the results are put back into INTT_RAM_C. Lastly, the INTT results are input to a pipeline CRT-accumulation unit to obtain the final multiplication result.

They use schonhage-strassen large integer multiplication algorithm with a maximum word length of a few million bits. Number theoretical transform: It is generated by fast Fourier transform by replacing with a primitive root of unity[1].

Schönhage–Strassen algorithm is a special kind of discrete Fourier transform (DFT) defined over a finite field $Zp = Z/pZ$.Let ω be a primitive nth root of unity in Zp.$\boldsymbol{a} = (a0, a1, \ldots, an-1)$ be a vector of degree n, where coefficient$ai \in Zp$, $i = 0, 1, \ldots, n-1$. The n-point NTT of vector $\boldsymbol{a}$ (denotedby $NTTn\omega(\boldsymbol{a})$) is defined as$Ai = NTTn\omega(\boldsymbol{a})i = n-1_j=0 a j\omega i j \bmod p$.

(1)The n-point inverse number theoretical transform (INTT) of vector A (denoted by $INTTn\omega(\boldsymbol{A})$) is defined as$INTTn\omega(\boldsymbol{A})\, i = n-1 * NTTn\omega-1(\boldsymbol{A})\, i=n-1 * n-1_j=A j\omega-i j \bmod p$.

Each NTT point is generated by two modules and the result can be generated by chines remainder theorem. They can design and implement 12 bit in a NTT module. In this Existing they have high end field programmable gate array. Its is very much costly for practical applications. High area cost implementation

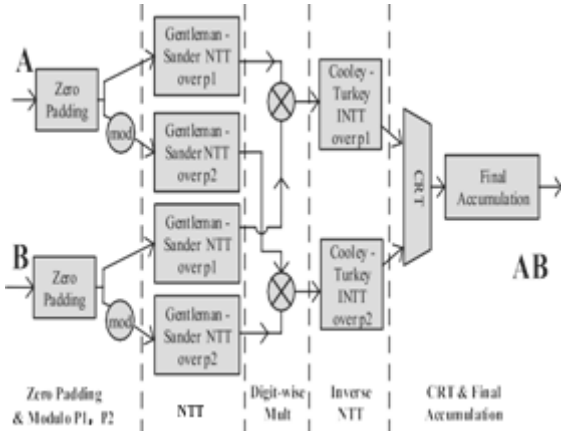

Figure 1. multiplication architecture based on double modules NTT.

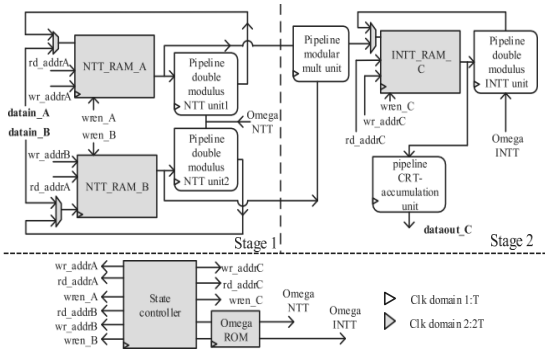

Figure 2.VLSI architecture of integer multiplier

It shows that multiplication architecture based on double modules NTT and VLSI architecture of integer multiplier.

III. PROPOSED SYSTEM

In this proposed system to design a area and memory efficient VLSI architecture for million bit multiplier design. In this to split the multiplier bit into 3FIFO architecture through NTT RAM technology. It includes Synchronizer, State control module and 3FIFO buffer module. The synchronizer module is used to Synchronizer the NTT RAM and state controller arbiter. The state controller module gives the control signal and priority of the multiplier design.

Figure 3. NTT RAM through FIFO

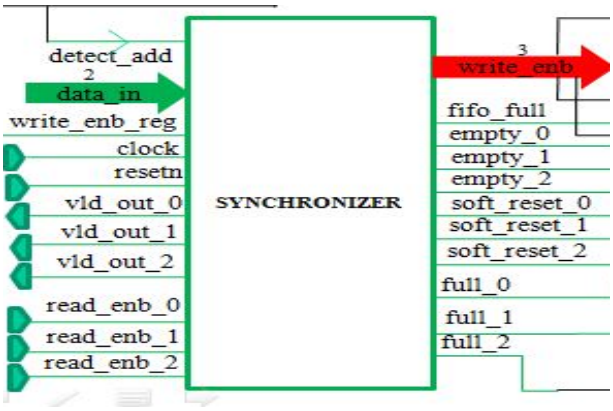

Figure 4. Synchronizer

Figure 5. State controller arbiter

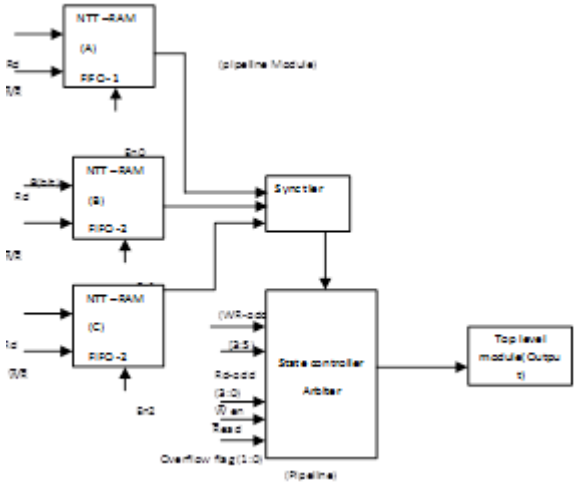

Figure 6. Proposed Block diagram

The FIFO module is used for split the million bit multiplier into 8-bit multiplier i.e. 256 value. Here we are going to design three FIFO module, so we can achieve 256*256*256 bits of value approximately million bits, based on this Technology. We have to achieve high speed as well as low power dissipation. At last, efficient VLSI architecture.

FIFO module means buffer module commonly used in Digital communication, Digital signal processing, VLSI. This FIFO modules are verified using in test benches by writing and reading values to and from the FIFO while observing the RAM data and the condition of output flags.

The synchronizer module is to synchronizer the NTT RAM and state controller arbiter. The state controller arbiter gives the control signal and priority multiplier of the design.

IV. CONCLUSION

Based on these technology, they have more area efficient, significant reduction on computing time,Less costly than the cache architecture. We can achieve 256*256*256 bits of approximately million bit integer multiplier design.

V. REFERENCES

[1]. A.Mkhinini,P.Maistri,R.leveugle,R.Tourki,M.Machhout , "A flexible RNS-based large

polynomial multiplier for fully Homomorphic encryption",IEEE conference 2016

[2]. Cao,Xiolin and Moore,Ciara and Oneil,Maire and osullivan,elizabath and hanleyneil "optimized multiplication architecture for accelerating fully homomorphic encryption" published on IEEE transactions on computers 65.1-1.0.1109/TC.2015.2498606

[3]. Ciara Rafferty-Maire o'neill-neil Hanley I "Evaluation of large integer multiplication methods on hardware",IEEE T COMPUTE 2017

[4]. Ghada ahmed Ei-mahdy "Design space Exploration for a co-designed accelerator supporting homomorphic encryption",IEEE 2015

[5]. Wang ,Wei and hu,vin and Chenlianmuang and huang,IEEE "Accelerating fully homomorphic encryption using GPU" IACR Cryptol,2013

[6]. Wei Wang,Xinming huang,IEEE international conference symposium on circuits and systems. "FPGA implementation of a fully homomorphic encryption",May 2013

[7]. Wei Wang,xinming Huang,naill Emmart,charles weems,"VLSI design of a large number multiplier for fully homomorphic encryption IEEE T VLSI SYST,sep 2014

[8]. Wei Wang,xinming huang,IEEE conference : circuits and systems(iscas),2013

[9]. Yarkan Doroz,Erdinc ozturkberk sunar,IEEE 16th euro micro conference on Digital system design DSD 2013.955-962.10.1109/DSD 2013.108

[10]. Yarkandoroz, Erdinc ozturksunar,,IEEE "Evaluating the hardware performance of a million bit multiplier Euro micro Conf. DigitaSyst. Design (DSD), Sep. 2013

[11]. J. M. Pollard, "The fast Fourier transform in a finite field" Math.Comput., vol. 25, no. 114, pp. 365–374, 1971.