International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

DESIGN A LOW-COMPLEXITY VLSI ARCHITECTURE OF AHL MULTIPLIERS FOR FULLY HOMOMORPHIC ENCRYPTION

[1]NANDAM SANKEERTHANA, [2]K. RAJKAMAL, [3]M.APPARAO

[1]M.Tech Scholar, Dept of ECE, Guntur Engineering College, Yanamadala, Guntur, Andhra Pradesh, India
[2]Associate Professor, Dept of ECE, Guntur Engineering College, Yanamadala, Guntur, Andhra Pradesh, India
[3]Professor and HOD, Dept. of ECE, Guntur Engineering College, Yanamadala, Guntur, Andhra Pradesh, India

ABSTRACT: Large integer multiplication has been widely used in fully homomorphic encryption (FHE). Implementing feasible large integer multiplication hardware is thus critical for accelerating the FHE evaluation process. Hence in this paper, design low complexity VLSI architecture of AHL Multiplier for Fully Homomorphic encryption is implemented. An operand reduction scheme is proposed to reduce the area requirement of radix-r butterfly units. This is extended to the single port, merged-bank memory structure to the design for further area minimization. In addition, an efficient memory addressing scheme is developed to support resolving carries computations. Experimental results shows that the proposed system gives effective results. The low-complexity feature of the proposed AHL multiplier designs is thus obtained without sacrificing the time performance.

KEY WORDS: Fully Homomorphic Encryption, Large Integer **Multiplication, VLSI Architecture, AHL (Adaptive Hold Logic) Multiplier**

.

I. INTRODUCTION

Fully Homomorphic Encryption is for the most part utilized in the Database Memory Based System (DMBS). One of the present issues related with the utilization of databases is the test of verifying and securely putting away the legitimate treatment of classified information in the remote database. Privacy of touchy data can be guaranteed using cryptography. It may, be the utilization of industrious encryption calculations to store the data in remote databases can fundamentally decrease the presentation of the framework without interpreting.

To take care of the Issue, in MIT examines exhibited Crypto system. Utilizing additively homomorphic crypto framework enables the server to execute Sum, Average, and Count Questions over encoded information; the other SQL inquiries utilize the distinctive encryption calculations with the vital usefulness. The adjustment of completely homomorphic cryptosystem will keep the capacity to perform run of the mill database tasks on encoded information without decoding the information in a confided condition. In any case, such a cryptosystem must fulfill certain prerequisites for practical qualities and computational unpredictability, which is significant.

Fully Homomorphic Encryption (FHE) is a huge achievement in cryptographic research in recent years. A FHE plan can be utilized

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

to elective perform calculations on figure content without trading off the substance of relating the plain text [1]. Therefore, a practical FHE plan will open the way to various new security advances and protection related to the applications, for example, security safeguarding pursuit and cloud-based processing. For the most part, FHE can be ordered into three classifications: cross section based, number based, and learning with mistakes.

One of the fundamental difficulties in the improvement of FHE applications is to moderate the amazingly high-computational intricacy and asset necessities [2-4]. For instance, programming usage of FHE in superior PCs still expend the critical calculation time, especially to achieve the vast whole number duplication which more often than not includes more than countless bits. For cross section based FHE, bit increase the required for the little setting with a grid measurement. To quicken the FHE tasks, different effective plans have been proposed to handle the extensive whole number duplication.

The objective of this paper is to revive the encryption natives in entire number based FHE using FPGA advancement. This particular FHE count is picked because of the less unpredictable theory, humbler key size and equivalent execution. Also, the introduction of a grouped FHE plots over the entire numbers ensures further capability upgrades. Augmentation is a key segment in these FHE plans the features in the encryption, unscrambling and evaluation steps. Broad entire number FFT duplication has furthermore been used in the late of referenced gear and GPU use of other FHE plans. Future work will look into the impact of the gear multiplier on substitute walks inside the FHE plot. Specifically, presenting the primary gear execution of encryption rough required for FHE over the numbers.

II. TYPES OF MULTIPLIERS

Array multiplier is circuit which uses array of AND gates and full adders to perform multiplication of binary operands is called as Array multiplier. It is one of the widely used fundamental algorithms for multiplication. The array of AND gates present in the multiplier performs AND operation of multiplicand with each bit of the multiplier. These partial products produced by AND gates are shifted to left according to the position of multiplier bit. The shifted partial products are summed up with a N-1 adders in parallel. However, addition performed in parallel there is large delay is introduced by CRAs. This is due to carry propagation in sequence of adders. The CRAs are replaced with Carry save adders (CSA) to reduce the delay in array multiplication process. The CSAs compress the three number addition to number addition so, that three operands are added at a time.

The multiplier delay in addition of partial products like in array multiplier are reduced by some multiplication techniques based on shift and add techniques. The multiplier bit decides whether to shift the partial product or add the multiplicand to the product. Here we explained how conventional addition is performed. In order to fasten the multiplication procedure custom multiplication process divided into two sections. The first section focuses on producing partial products and the second section focuses on accumulation and addition of the partial products. Before adding of PPs they need to be aligned in their corresponding positions by shifting.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

Booth technique is the most dominating method of multiplication for signed numbers. In this technique multiplication of both positive and negitive operands are similarly performed. This technique is based on add-shift algorithm. In conventional multiplication procedures the number of partial products depends upon the operand size of the multiplier. If the size of the multiplier increases number of partial products also increases resulting in large delay when they get added to produce the end result. Since the delay of the multiplier is dominated by addition operation he focused to reduce the number of additions occur in a multiplication task

The multiplication of signed numbers must be observed through the operation to produce the appropriate sign of the result. Whereas in case of unsigned numbers there is no need to think about sign of the operands. If the multiplication of signed 2's complement numbers is performed in the way of positive number multiplication would results in incorrect output. Therefore, booth's algorithm introduced a technique to perform multiplication of signed numbers with the sign protection. In this technique the LSB bits of the multiplier are bi and bi-1 are tested at every clock cycle. If the two bits are zeros results shifting one bit position of the multiplier to the right. In case of sequence of 1's arithmetic operations like addition and subtraction are need to be performed at the edges of block of one's while changing from 1 to 0 and 0 to 1.

Booth's algorithm performs addition if last bits of multiplier encounters '0 1' and subtraction of multiplicand is needed if the LSB bits encounter '1 0'. This method efficiently works for signed numbers also. When multiplier consists of long blocks 1's this algorithm works well and effectively reduces number of additions performed.

III. EXISTED SYSTEM

The below figure (1) shows the architecture of existed system. In this system mainly, two NTT units, a controller unit, an AGU, and several memory units are used. ROM main intent is to store the twiddle factors. There are mainly two single ports of SRAM in NTT block. Here firstly two inputs are computed at same time by using the two NTT data there are NTT1 and NTT2. For the purpose of multiplication the NTT is used as inverse NTT and because of R input data is processed.

Addition and subtraction operations are performed in the Mul Mod unit. The result of this unit is processed to the buffer unit. Now the values are saved in ROM. Here point wise multiplication process is performed in the NTT block and bits are computed depends on the current status of operation.

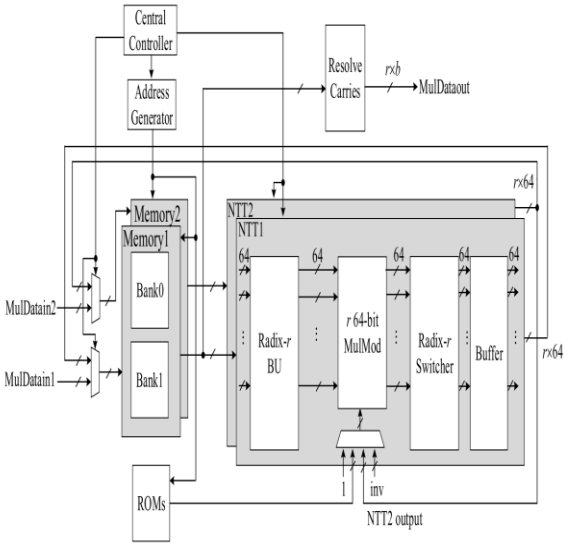

Fig. 1: EXISTED SYSTEM

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

To relocate the data radix r is used and this will saves the memory temporarily. Basically there are four pipelined stages in the MulMod unit. To get conflict free address in the system buffer is used. But this system does not give effective results in terms of delay and time. Hence to overcome this, a new system is introduced which is discussed in below section.

IV. PROPOSED SYSTEM

The below figure (2) shows the proposed system. In this AHL multiplier plays very important role to increase the speed of operation. Address generator block will generate the address according to given inputs. Memory banks will save the both inputs and address. Controller will control the entire operation.

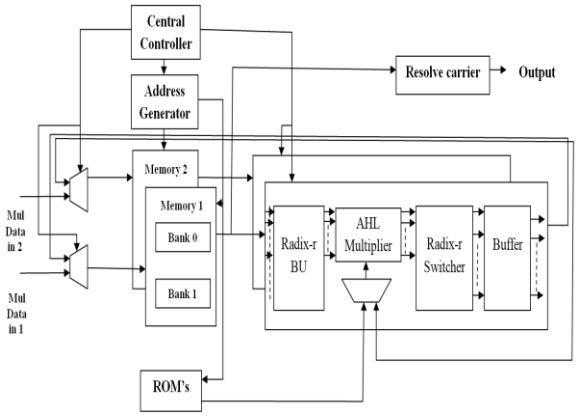

Fig. 2: PROPOSED SYSTEM

Multiplication is one of the most important functions in various VLSI applications. Multiplier plays an important role in computation and other advanced mechanism. The basic idea is to divide the merged-bank memory into two banks, which are read or written according to certain rules during operations. These rules ensure that when one of the banks is being read, the other is being written in every cycle.

Given a radix-r BU (Buffer Unit), this paper explores the inherent features in the set of operands for each Xk and proposes an efficient operand reduction algorithm to minimize the number of effective operands. Moreover, to increase the chance of merging operands, we extended the concept of compatible operands to consider the segmented data point xn. Generally, the single-port memory structure is preferred over the multiport memory for its area efficiency.

V. RESULTS

The below figure (3) & (4) shows the RTL schematic and technology schematic of identity based fully homomorphic encryption and decryption system.

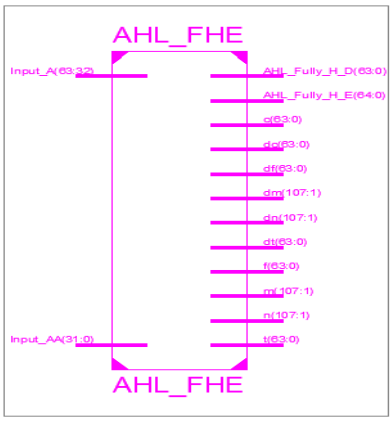

Fig. 3: RTL SCHEMATIC OF PROPOSED SYSTEM

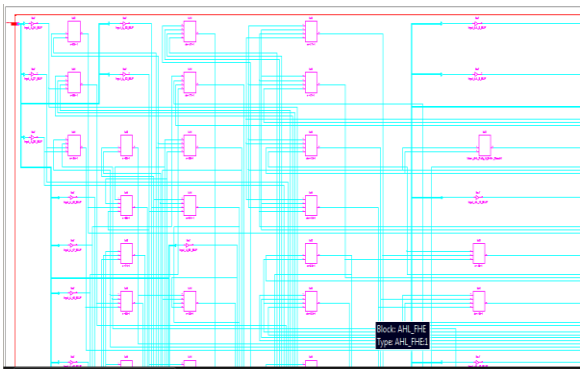

Fig. 4: TECHNOLOGY SCHEMATIC OF PROPOSED SYSTEM

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

Technology schematic is generated after the optimization and technology targeting phase of the synthesis process. It shows a representation of the design in terms of logic elements optimized to the target Xilinx device or "technology"; for example, in terms of LUTs, carry logic, I/O buffers, and other technology-specific components. Viewing this schematic allows you to see a technology-level representation of your HDL optimized for a specific Xilinx architecture, which might help you discover design issues early in the design process.

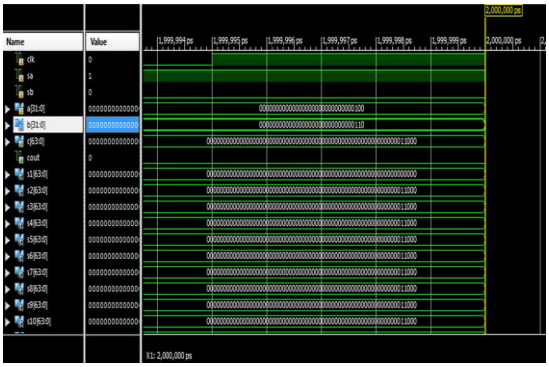

Fig. 5: OUTPUT WAVEFORM OF PROPOSED SYSTEM

VI. CONCLUSION

In this paper, design low complexity VLSI architecture of AHL Multiplier for Fully Homomorphic encryption was implemented. The proposed system was synthesized with an estimated core area. AHL Multiplier using Fully Homomorphic encryption performs the operation depend on the homomorphic conditions. From Experimental results it can observe that the proposed system is faster than CPU and provides security in efficient way.

VII. REFERENCES

[1] Jheng-Hao Ye and Ming-Der Shieh, "Low-Complexity VLSI Design of Large Integer Multipliers for Fully Homomorphic Encryption", 1063-8210 © 2018 IEEE.

[2] S. Koteshwara and A. Das, "Comparative study of authenticated encryption targeting lightweight IoT applications," IEEE Design Test, vol. 34, no. 4, pp. 26–33, Aug. 2017.

[3] C. Dobraunig, M. Eichlseder, S. Mangard, F. Mendel, and T. Unterluggauer, "ISAP–towards side-channel secure authenticated encryption," IACR Trans. Symmetric Cryptol., vol. 2017, no. 1, pp. 80–105, 2017.

[4] H. Böck, A. Zauner, S. Devlin, J. Somorovsky, and P. Jovanovic, "Nonce-disrespecting adversaries: Practical forgery attacks on GCM in TLS," in Proc. USENIX WOOT, 2016, pp. 1–11.

[5] P. G. Lopez et al., "Edge-centric computing: Vision and challenges," ACM SIGCOMM Comput. Commun. Rev., vol. 45, no. 5, pp. 37–42, Oct. 2015

[6] F. Abed, C. Forler, and S. Lucks, "General overview of the firstround CAESAR candidates for authenticated encryption," IACR Cryptol. ePrint, Tech. Rep. 2014/792, 2014.

[7] Nitesh Aggarwal, Cp Gupta, and Iti Sharma. 2014. Fully Homomorphic symmetric scheme without boot strapping. In Cloud Computing and Internet of Things (CCIOT), 2014 International Conference on.IEEE, 14–17.

[8] S Sobitha Ahila and KL Shunmuganathan. 2014. State Of Art in Homomorphic Encryption Schemes. International Journal of Engineering Research and Applications 4, 2 (2014), 37–43.

[9] D. McGrew and D. Bailey, AES-CCM Cipher Suites for Transport Layer Security (TLS), document RFC 6655, 2012.

[10] H. Handschuh and B. Preneel, "Key-recovery attacks on universal hash function

based MAC algorithms," in Proc. Annu. Int. Cryptol. Conf. Berlin, Germany: Springer, 2008, pp. 144–161.

NANDAM SANKEERTHANA
Completed diploma in Govt. Polythenic, Warangal and completed B.tech in kkr & ksr institute of technology and sciences, Guntur in A.P India.

Dr. K. RAJKAMAL completed B.Tech from JNTUK, Kakinada, Andhra Pradesh, India and Completed M.Tech., Ph.D from K L University, Guntur, Andhra Pradesh, India At present he is Working as Associate professor in the department of ECE, Guntur engineering college, Guntur, Andhra Pradesh, India. His area of interest is Antennas and VLSI.

M. APPARAO completed his B.Tech in V. R. Siddhartha Engineering College and M.Tech in Bharath University. Present working as Professor in Guntur Engineering College, Guntur, A.P, India