INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE
ISSN: 2057-5688

Design and Implementation of Encryption/Decryption Architectures for BFV Homomorphic Encryption Scheme

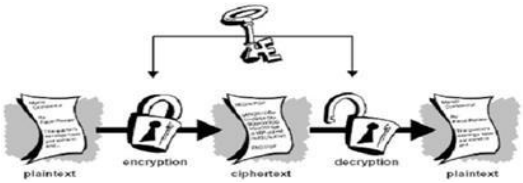
B.AKHILA[1], G.LAKSHMI BHARATH[2], B.UMAKANTH[3]
[1]PG Student, Dept of ECE, SITS, Kadapa, AP, India.
[2]Assistant Professor, Dept of ECE, SITS, Kadapa, AP, India.
[3]Assistant Professor, Dept of ECE, SV College of Engineering, Kadapa, AP, India.

Abstract—

Fully homomorphic encryption (FHE) is a technique that allows computations on encrypted data without the need for decryption and it provides privacy in various applications such as privacy-preserving cloud computing. In this article, we present two hardware architectures optimized for accelerating the encryption and decryption operations of the Brakerski/Fan-Vercauteren (BFV) homomorphic encryption scheme with high-performance polynomial multipliers. For proof of concept, we utilize our architectures in a hardware/software code sign accelerator framework, in which encryption and decryption operations are offloaded to an FPGA device, while the rest of operations in the BFV scheme are executed in software running on an off-the-shelf desktop computer. Specifically, our accelerator framework is optimized to accelerate Simple Encrypted Arithmetic Library (SEAL), developed by the Cryptography Research Group at Microsoft Research. The hardware part of the proposed framework targets the XILINX VIRTEX-7 FPGA device, which communicates with its software part via a peripheral component interconnect express (PCIe) connection. For proof of concept, we implemented our designs targeting 1024- degree polynomials with 8-bit and 32-bit coefficients for plaintext and ciphertext, respectively. The proposed framework achieves almost 12× and 7× latency speedups, including I/O operations for the offloaded encryption and decryption operations, respectively, compared to their pure software implementations.

I. INTRODUCTION

Since there is an evolution of wireless communication, the encrypting of data are major concern as shown in figure 1.Encryptions is the process of transfer of input text data (plain text) into the unintelligent data (cipher text) with the help of well algorithm are defined but U.S. government adopted that be used in the federal departments and agencies for protecting the important Information. According to the specifications of AES On October 2000, the NIST (national Institute of standard and technology) announced that AES encrypting algorithm as the best from other encrypting technique in the field of security, performance, efficiency, implementation capability and simplicity. Cryptography is the recognition and avoidance from the fraud and other illegal activity. The proposed AES design is the symmetric-key cryptography which involves the secret key that is only known by the user, which having the same number of bits as the palin text i.e. 128 bits. It considered that the secret key for the encryption and decryption of block of data. As for the symmetry system the secret key must be shared between the sender and the receiver for the communications purpose decrypt data. The AES process is realizing in ATM, intelligence card and magnetism card.



Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called attackers. Cryptology embraces both cryptography and cryptanalysis growth is a focal limit in math exercises subject to this assignment,

ISSN: 2057-5688

for instance, Multiply and Accumulate (MAC)and inner thing are among a bit of the regularly used Computation Intensive Math Functions (CIAF)currently realized in various Digital Signal Processing (DSP)applications, for instance, convolution, Fast Fourier Transform (FFT), isolating and in chip in its math and justification unit. Since increase overpowers the execution time of most DSP estimations, so there is a need of quick multiplier. At this moment, increment time is so far the prevalent factor in choosing the direction procedure length of a DSP chip.

a) Problem Statement

In conventional IP forwarding, the router uses a longest-prefix match on the destination IP address to determine where to forward a packet. With MPLS, labels are attached to packets at the ingress point to an MPLS network. Within the network, the labels are used to route the packets, without regard to the original packet header information. These labels can be stacked as a last in first out (LIFO) label stack, enabling MPLS flows to be combined for transport and separated later for distribution. Current proposed protocols for MPLS security, Behringer [2] and Senevirathne et al. [3] discuss two approaches to securing MPLS. Behringer [2] makes the assumption that the core MPLS network is "trusted and provided in a secure manner." We make no such assumption in our work. We assume that only the MPLS nodes themselves are secure. The physical links connecting the nodes are assumed to not be secure – we protect them using our protocol. Senevirathne et al. [3] proposes an encryption approach using a modified version of IPsec. IPsec is defined by the IETF [4], and is an all-purpose encryption protocol that includes key distribution, authentication for the IP header, and authentication and encryption for the IP payload. Senevirathne et al.

II. EXISITING SYSTEM

Here, we first present our Montgomery modular multiplier hardware architecture and its implementation. We then explain two encryption/decryption hardware architectures implementing the iterative and the four-step Cooley-Tukey NTT algorithms for polynomial multiplication operation, respectively. Henceforth, they are shortly referred to as the iterative hardware and the four-step hardware, Here, we first present our Montgomery modular multiplier hardware architecture and its implementation. We then explain two encryption/decryption hardware architectures implementing the iterative and the four-step Cooley-Tukey NTT algorithms for polynomial multiplication operation, respectively. Henceforth, they are shortly referred to as the iterative hardware and the four-step hardware, respectively.

III. PROPOSED SYSTEM

In this proposed system we can work on internal blocks like adder and multiplier Extension: vedic multiplier with koggestone adder which fast in process compare to other Architure will be same but this blocks is multiplier and adder block is replaced with extension work of adder and multiplier.

3.1 Kogge stone adder

Kogge stone adder is a parallel prefix type of carry look forward adders. It comprises of four vertical stages, every vertical phase of Kogge stone adder creates an engender and produce bit. It is considered as the quickest adder and it is broadly utilized in businesses for superior of arithmetic circuits. In Kogge stone adder carrys are registered quick by processing them in parallel at the expense of expanded territory. Kogge stone adder is adder which is having low delay.

a) Multipliers

The most basic type of the increase comprises of joining two numbers, the multiplier and the multiplicand, to shape the last item. The essential augmentation can be accomplished through the conventional paper and pencil technique, disentangled to radix 2.'

b) Multiplication Algorithm

From the above dialog it very well may be reasoned that the augmentation of two paired numbers has now changed in to the expansion of two twofold numbers. Considering this the increase of two double numbers might be detailed as pursues, i) If the Least Significant Bit of the multiplier is '1', the aggregator (at first set as '0') is included with the multiplicand. ii) Shift the multiplier and aggregator one piece to one side. iii) If the Least Significant Bit of the multiplier is '0', at that point just move the multiplier and aggregator

ISSN: 2057-5688

one piece to one side. iv) Repeat steps (i) to (iii) till every one of the bits in the multiplier are inspected.

c) Power Optimization in Multipliers

Power decrease in multipliers should be possible at all plan levels beginning from the innovation level to the framework level. In the multipliers, the incomplete item age, decrease and last stages are structured as a combinational plan. They have a huge plan with high entryway thickness, in certainty high transistor thickness. Clearly this huge dynamic region gives space to have extensive power utilization. In the combinational structure, the exchanging movement chooses the power scattering. Consequently, the power scattering in the multipliers can be diminished by limiting the exchanging exercises. Another effective methodology is by decreasing the quantity of fractional items created in the multiplier structure and their wiring. Duplication is a fundamental necessity in the present high complex processors. Parallel increase is performed by a two-level activity, the age of the halfway items and their collection.

d) Proposed Hybrid Vedic Multiplier

The multipliers are the core of any fast-computational gadgets. In the multiplier circuits, the measure of the multiplier chooses the quantity of adders being utilized. Consequently, the power utilization relies upon the quantity of adder squares utilized and the methodology pursued to interface the adder squares to play out the increase activity. Since all the constant applications utilize the multipliers as their center component, the multipliers are the significant power devouring squares. Ordinarily bigger squares are constructed utilizing different littler squares and power streamlining is centered around these littler squares. The proposed hybrid Vedic multiplier, the 4-bit adder is replaced by Kogge stone adder and results are analyzed. Then the proposed multiplier design was synthesized using the same technology and compared with the designs synthesized by the tool. The comparisons are made in terms of area, delay and power.

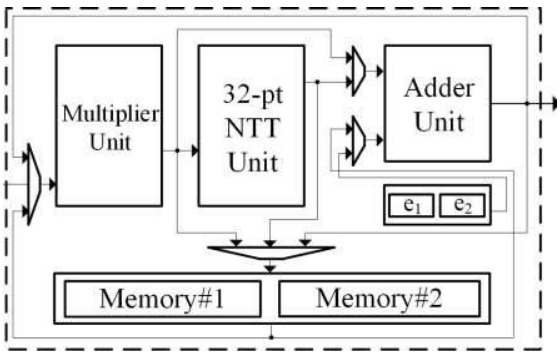
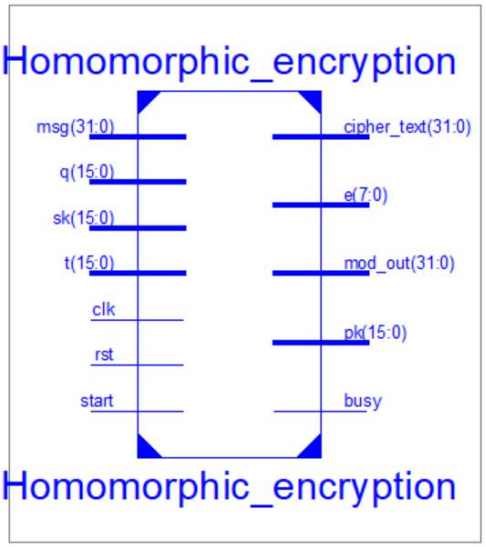


Figure: Proposed Method block Diagram

IV. RESULTS

Encryption and Decryption are the Important Part of Secured communication, In homomorphic Encryption Scheme Operation on Chiper Text can be easily done andwithout Need of any Decrypting First. The Architecture used gives better Results in computation speed, area, energy and power are of more Priority Outcome to be Accurate i.e., By Using ISE DESIGN SUITE Project Navigator, Xilinx 14.7 version in the simulation procedure the better Outputs are Achieved with Less Circuit Area With Low Power Consumption. The encryption operation should be verified that the given input message is encrypted perfectly or not .if any errors occur in the encryption operation then the samesteps happen.

RESULTS OF ENCRYPTION OPERATION:



INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE
ISSN: 2057-5688

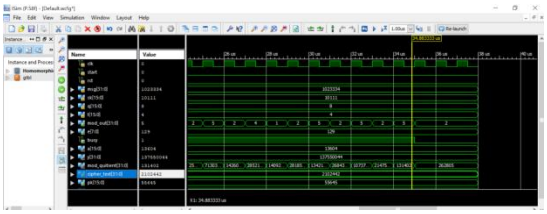
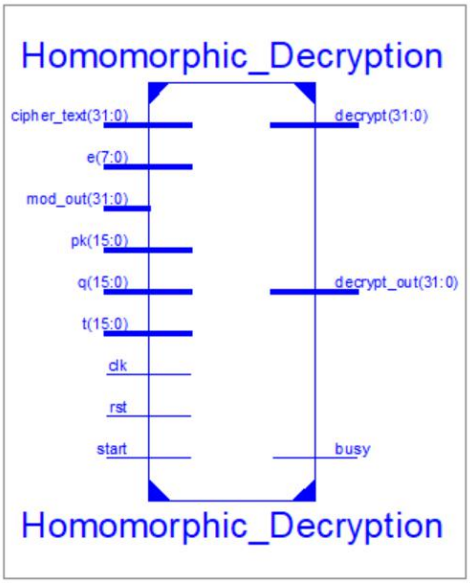


Figure: Results of Encryption Operation

After performing the encryption the received output message should be decrypted at the output end by performing decryption operation and the outputs of the decryption is shown below. The outputs of the encryption will be verified and the decryption operation should be performed which is shown in below. The outputs from the encryption operation should be verified that the given input message is encrypted perfectly or not. If any errors occur in the encryption operation then the same steps should be performed.

RESULTS OF DECRYPTION OPERATION:



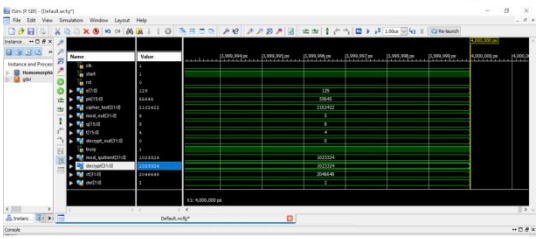


Figure: Results of Decryption Operation

The comparison table that shows the improved parameters for existing method to the proposed method is given below

```
--------------------------------------+-----------------------+--------+

Asynchronous Control Signals Information:
----------------------------------------
No asynchronous control signals found in this design

Timing Summary:
---------------
Speed Grade: -3

   Minimum period: 1.943ns (Maximum Frequency: 514.646MHz)
   Minimum input arrival time before clock: 28.582ns
   Maximum output required time after clock: 2.150ns
   Maximum combinational path delay: No path found

=========================================================================
```

Figure: Delays

```
Asynchronous Control Signals Information:
----------------------------------------
No asynchronous control signals found in this design

Timing Summary:
---------------
Speed Grade: -3

   Minimum period: 1.943ns (Maximum Frequency: 514.646MHz)
   Minimum input arrival time before clock: 27.715ns
   Maximum output required time after clock: 2.150ns
   Maximum combinational path delay: No path found

Timing Details:
```

Figure: Existing delay

Table: Comparison for Existing Method and the Proposed Method

Parameters	Existing Method	Proposed Method
Clock Frequency	200 MHz	514.64 MHz
LUT	800	526
Slice Registers	726	105
Delay (ns)	5.0	1.943

The comparison table that shows the improved parameters for existing method to the proposed method is given above. From the above table it is observed that the delay in the proposed method is lessthan the existing method, this results in the performance of the architectures used in this applications.

CONCLUSION

Here this Project We Can Reduce the Power Consumption and Delay by Using Vedic Multiplier and K oggestone Adder which is Fast in Performance**.** The greater values of frequency will results in the reduction in delay. So the performance of the system will be increased. And also the number of LUT's used in this project will alsobe reduced. This work can be used Further for 128 bits, 256 bits, can be Implemented by Further Different Multipliers and Fastest Adder to Increase the Performance of the Circuit. Finally, with small modifications, the core arithmetic units in our accelerator can be used to implement ring

ISSN: 2057-5688

arithmetic with larger ring degrees and modulus sizes. Currently, we are working on such new design based on our current architecture which reduce the power Consumption with Parrallel prefix adder (like Kogge stone Adder), and the results will be presented in our future work.

REFERENCES

[1] Albrecht, M. R. (2017). On dual lattice attacks against small-secret LWE and parameter choices in HE lib and SEAL. In J. Coron & J. B. Nielsen (Eds.), EUROCRYPT 2017, parii (Vol.10211, pp. 103–129).Springer, Heidelberg.

[2] Martin R. Albrecht, Robert Fitzpatrick, and Flori an Gopfert: On the Efficacy of Solving by Reduction to Unique-SVP. In Hyang-Sook Lee and Dong-Guk Han, editors, ICISC 13, volume 8565 of LNCS, pages293-310.Springer, November2014

[3] Albrecht, M. R., Göpfert, F., Virdia, F., &Wunderer, T. (2017). Revisiting the expected cost of solving uSVP and applications to LWE. In T.Takagi & T.Peyrin (Eds.), ASIACRYPT2017, part i(Vol.10624, pp.297–322). Springer, Heidelberg

[4] Martin R. Albrecht, Rachel Player and Sam Scott. On the concrete hardness of Learning with Errors. Journal of Mathematical Cryptology. Volume 9, Issue 3.

[5] Alkim, E., Ducas,L., Pöppelmann,T., & Schwabe, P. (2016). Post-quantum key exchange-A new hope. In T.Holz & S. Savage (Eds.), 25thUSENIX security Alperin Sheriff, J.,Peikert, C.: Faster boots trapping with polynomial error. In: Garay, J.A., Gennaro, R.(eds.) CRYPTO2014. LNCS, vol.8616, pp. 297–314.

[6] László Babai: On Lovász' lattice reduction and the nearest lattice point problem, Combinatorica, 6(1):1-3,1986.

[7] Becker, A., Ducas,L., Gama,N., & Laarhoven,T. (2016). New directions in nearest neighbor searching with applications to lattice sieving. In R. Krauthgamer (Ed.), 27thsoda (pp.10–24). ACM-SIAM.

[8] W. Castryck, I. Iliashenko, F. Vercauteren, Provably weak instances of ring-lwe revisited.In:Eurocrypt2016. vol.9665, pp.147–167. Springer(2016)

[9] W. Castryck, I. Iliashenko, F. Vercauteren, On error distributions in ring-based LWE. LMS Journal of Computation and Mathematics 19(A), 130–145 (2016) 7.

[10] Y. Chen, P.Q. Nguyen. BKZ 2.0: Better Lattice Security Estimates. In: Lee D.H., Wang X.(eds) Advances in Cryptology – ASIACRYPT 2011. ASIACRYPT.