Cyber Security VHDL Design of Superscalar Homomorphic Encryption: A Review

Chandra Kant Maurya[1] Abhishek Singh[2]
[1]M.Tech Scholar [2]Assistant Professor
[1,2]Department of Electronics and Communication Engineering
[1,2]Gyan Ganga Institute of Technology and Science, Jabalpur, MP, India

Abstract— with today's Cyber Networks it is possible to transmit both voice and data, including e-mail, pictures and video. Importance of security issues is higher in current data Cyber Networks than in previous systems because users are provided with mechanisms to accomplish very crucial operations such as banking transactions and sharing of confidential business information, which require high levels of protection. Cyber Network Security and cryptography in high speed Cyber Networks demands for specific hardware in order to match up with fast cloud systems. In cryptographic module, Dual key Homomorphic, a symmetric key block cipher is been designed as algorithm for implementation in cyber security. Design goal is to increase data encryption rate i.e. throughput to a substantial value so that design may be used as a cryptographic processor in high speed Cyber Network applications. 2^n+1 modulo multiplier is a main element in Homomorphic encryption of cloud system.

Keywords: VHDL, Cyber Security, cloud System, modulo multiplier, cryptography, Homomorphic encryption

I. INTRODUCTION

The nature of information that flows throughout modern data communications Cyber Networks has evolved noticeably since early years of first generation systems, when only voice sessions were possible. Weaknesses in security architectures allow successful eavesdropping, message tampering and masquerading attacks to occur, with disastrous consequences for end users, companies and other organizations. With today's Cyber Networks it is possible to transmit both voice and data, including e-mail, pictures and video. importance of security issues is higher in current data Cyber Networks than in previous systems because users are provided with mechanisms to accomplish very crucial operations such as banking transactions and sharing of confidential business information, which require high levels of protection. Weaknesses in security architectures allow successful eavesdropping, message tampering and masquerading attacks to occur, with disastrous consequences for end users, companies and other organizations.

Cloud computing is a prototype as enabling ubiquitous, convenient, on-demand Cyber Network ingress to a shared pool of configurable computing resources (e.g., Cyber Networks, servers, storage, applications, and services). Authorization, Authentication, Encryption, Key and Identity Management various from conventional information technologies, in cloud computing deployment of virtual machines, IP addresses and resources are dynamic [13]. Authorization, authentication and identity management have to be configured with effects from this dynamism in way of synchronization. While achieving this configuration, data privacy is also indispensable. and way of achieving data privacy a well-defined, well configured and well-maintained key management.

II. INTERNATIONAL DATA ENCRYPTION ALGORITHM (IDEA)

International Data Encryption Algorithm (IDEA) is a block Homomorphic cipher technique designed by Mr. Xuejia Lai and James L. Massey [7] of ETH-Zurich and was first introduce in 1991. It is a modified version of an earlier cipher, PES (Proposed Encryption Standard); IDEA-Homomorphic was known as at initially IPES (Improved PES). Dual key Homomorphic was used as symmetric dual key cryptography in initial version of Pretty Good Privacy cryptosystem (PGPC).

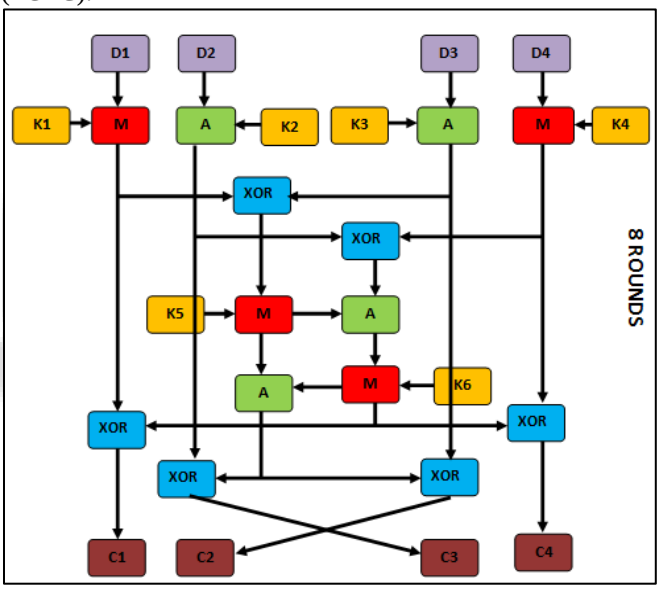

Fig. 1: IDEA-Homomorphic Encryption system

IDEA-Homomorphic was to develop as a strong encryption algorithm, which could replace DES procedure developed in U.S.A. in seventies data transfer. It is also good to know that it fully avoids use of any lookup tables or Substitution-boxes (SBOX). famous PGP email and file encryption product was designed by Phil Zimmermann, uses Dual key Homomorphic as its original choice for data encryption based for its proven design and its well reputation. Dual key Homomorphic encryption algorithm provides very high level security just not based on keeping algorithm a secret, however upon ignorance of secret key

- It is completely specified and easy to understood
- It is public
- It is good for use in a huge range of applications
- It may be economical and easy to implement in electronic components (FPGA Chip)
- It may be used proficiently
- It may be exported world wide

– It is patent protected to prevent fraud and piracy and unauthentic use.

III. LITERATURE SURVEY

1) Sujoy Sinha Roy et al [1] design a custom co-processor for the computationally expensive operations of the well-known Fan-Vercauteren (FV) Homomorphic encryption scheme on the FPGA, and make the Arm processor a server for executing different Homomorphic applications in the cloud, using this FPGA-based co-processor. they use the most recent arithmetic and algorithmic optimization techniques and perform design space exploration on different levels of the implementation hierarchy. In particular we apply circuit-level and block-level pipeline strategies to boost the clock frequency and increase the throughput respectively. To reduce computation latency, they use parallel processing at all levels. Starting from the highly optimized building blocks, we gradually build our multi-core multi-processor architecture for computing. We implemented and tested our optimized domain specific programmable architecture on a single Xilinx Zynq UltraScale+ MPSoC ZCU102 Evaluation Kit. At 200 MHz FPGA-clock, their implementation achieves over 13x speedup with respect to a highly optimized software implementation of the FV Homomorphic encryption scheme on an Intel i5 processor running at 1.8 GHz.
2) Zhe Liu et al [2] propose a vector version of Iterative Number Theoretic Transform (NTT) for high-speed computation of polynomial multiplication on ARM NEON platforms and a 32-bit variant of SAMS2 technique for fast reduction. For MSP430 architecture, we propose an optimized SWAMS2 reduction technique, which consists of five different basic operations, including Shifting, Swapping, Addition, as well as two Multiplication Subtractions. Regarding of the sampling from the discrete Gaussian distribution, we adopt Knuth-Yao sampler, accompanied with optimized methods such as Look-Up Table (LUT) and byte-scanning.
3) yang su et al [3] presented a fast implementation of levelled fully Homomorphic encryption scheme BGV. In order to reduce the computation latency and improve the performance, we applied both circuit-level and block-level pipeline strategies to improve clock frequency, and as a result, enhance the processing speed of polynomial multipliers and Homomorphic evaluation functions. At the same time, multiple polynomial multipliers and modular reduction units were deployed in parallel to further improve the hardware performance. Finally, they implemented and tested our architecture on a Virtex UltraScale FPGA platform. Running at 150MHz, their implementation achieved 4.60x~9.49x speedup with respect to the optimized software implementation on Intel i7 processor running at 3.1GHz for Homomorphic encryption and decryption.

Author	Brief	Journal	Results
Sujoy Sinha Roy et al [1]	They design an new Parallel Architecture for Homomorphic Encryption for could based secure data storage. they implemented the design on Zynq-7 FPGA and used Xilinx Vivado for design and simulations.	IEEE proceeding in 2019	0.362 Second for Send cipher text and Receive result cipher text in 0.18 sec. 200 MHz speed of encryption achieved. 63522 LUT's of Zynq-7 FPGA for Encryption engine
Zhe Liu et al [2]	They design a Ring-LWE Encryption engine on IoT ARM-NEON processors and used high level language for design Efficient Software system.	IEEE transactions 2017	Encryption cycles require are 149,400 with 32-bit ARM-NEON processors
Yang Su et al [3]	They design Ring-LWE Fully Homomorphic Encryption for cloud system secure data storage and fast access. they use FPGA-based Hardware Accelerator and design a Leveled encryption module.	IEEE Access 2020	95854 LUT's of Virtex UltraScale FPGA with 150MHz

Table 1: Literature Summary

The main objectives of presented work is to design, synthesize and verify functionality of each modules of Dual key Homomorphic that are highly computationally importance and are highly challenging to make them really work as an isolated module in a very high speed secure Cyber Network. As per earlier work done on modulo $(2^N + 1)$ multiplier for Dual key IDEA-Homomorphic cipher system, there was no enough space for very high speed operation or area reduction up to mark. Also previous work discussed that there were no clear theory for power optimization which is important area in current situation. problem areas for my research work are hardware implementation of cipher system on FPGA to reduce number of logic gates and provide faster efficiency. The main objective of presented work is implementation and optimization of FPGA based of unique new Modulo Multiplier $(2^N + 1)$ Design for High Speed Secured Cyber Network system by application of symmetric dual key dual key IDEA-Homomorphic cryptography. Multiplier is most time and space consuming operation any computation. research work is implementation with help of Xilinx software and FPGA Zybo Zynq-7000.

IV. TOOL & LANGUAGE

VHDL is Hardware Description Language [6] that may be used to model a digital system at many levels of abstraction, ranging from algorithmic level to gate level. HDL simulators are better than gate level simulators for 2 reasons: portable model development, & ability to design complicated test

benches that react to outputs from model under test. Vivado Design Suite[19] is a software suite produced by Xilinx for synthesis and analysis of HDL designs, superseding Xilinx ISE with additional features for system on a chip development and high-level synthesis. Vivado represents a ground-up rewrite and re-thinking of the entire design flow (compared to ISE).

Zynq-7000 SoC FPGA module: The Zynq-7000 SoC[18] family integrates the software programmability of an ARM-based processor with the hardware programmability of an FPGA, enabling key analytics and hardware acceleration while integrating CPU, DSP, ASSP, and mixed signal functionality on a single device.

V. Conclusion

One may conclude on behalf of literature survey for which we have gone through many research papers, books, Datasheets of EDA tools and references mansion in this paper that presented work is a better cryptograph procedure in terms of area and throughput, as known dual key cryptography is just a overhead for any system and it should not took many of area or time so presented work may be solution for same as presented work necessary very less area and time as compare to other existing work in same research area. As known dual key cryptography is just an overhead for any system and it should not took many of time so presented work is a solution for same as presented necessary very less time and highly security (i.e. high avalanche effect) as compare to other existing work in same category. One may conclude that presented encryption procedure has fastest among available methods such as AES, DES and RSA. presented technique is also faster than procedure developed by researchers of [2], [5] and [1]. total avalanche observed for presented technique is 76% which is best among all procedure available hence presented work is a better cryptograph procedure in terms of throughput and security level.

As electronic communications grow in importance, there is also an increasing need for data protection. Encryption ensures that: Only authorized persons may access information. Data cannot be amended or manipulated by unauthorized persons. Unbreakable crypt system warrants military strength security level.

References

[1] S. Sinha Roy, F. Turan, K. Jarvinen, F. Vercauteren and I. Verbauwhede, "FPGA-Based High-Performance Parallel Architecture for Homomorphic Computing on Encrypted Data," 2019 IEEE International Symposium on High Performance Computer Architecture (HPCA), Washington, DC, USA, 2019, pp. 387-398, doi: 10.1109/HPCA.2019.00052.

[2] Z. Liu, R. Azarderakhsh, H. Kim and H. Seo, "Efficient Software Implementation of Ring-LWE Encryption on IoT Processors," in IEEE Transactions on Computers, vol. 69, no. 10, pp. 1424-1433, 1 Oct. 2020, doi: 10.1109/TC.2017.2750146.

[3] Y. Su, B. Yang, C. Yang and L. Tian, "FPGA-Based Hardware Accelerator for Leveled Ring-LWE Fully Homomorphic Encryption," in IEEE Access, vol. 8, pp. 168008-168025, 2020, doi: 10.1109/ACCESS. 2020.3023255.

[4] Y. Fan, G. Zhao, W. Shang, J. Shang, W. Lin and Z. Wang, "A Preliminary Design for Authenticity of IoT Big Data in Cloud Computing," 2020 29th International Conference on Computer Communications and Networks (ICCCN), Honolulu, HI, USA, 2020, pp. 1-2, doi: 10.1109/ICCCN49398.2020.9209646.

[5] Zhongyuan Hao, Wei Guo, Jizeng Wei, Dual Processing Engine Architecture to Speed Up Optimal Ate Pairing on FPGA Platform, 2016 IEEE/Trustcom/BigDataSE/ISPA, DOI: 10.1109/TrustCom.2016.0113, ISSN: 2324-9013

[6] LI Wei , ZENG Xiaoyang , NAN Longmei , CHEN Tao , DAI Zibin , A reconfigurable block cryptographic processor based on VLIW architecture, China Communications (Volume: 13, Issue: 1, Jan. 2016), DOI: 10.1109/CC.2016.7405707, Page(s): 91 – 99, ISSN: 1673-5447

[7] Based on character of cloud storage string encryption and cipher text retrieval of string research, 2016 4th International Conference on Cloud Computing and Intelligence Systems (CCIS), DOI: 10.1109/ CCIS.2016.7790293

[8] International Data Encryption Algorithm, swiss encryption technology, and HOMOMORPHIC logo are trademarks of MediaCrypt AG, Switzerland, Patent protection EU: 0 482 154 B1

[9] Harivans Pratap Singh, Shweta Verma, Shailendra Mishra, Secure-International Data Encryption Algorithm, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 2, problem 2, February 2013, ISSN (Online): 2278 – 8875

[10] nick hoffman, a simplified Homomorphic algorithm, online documents, http://citeseerx.ist.psu.edu/viewdoc /download?doi=10.1.1.501.2662&rep=rep1&type=pdf

[11] Sandipan Basu, international data encryption algorithm (idea) a typical illustration, Volume 2, No. 7, July 2011 Journal of Global Research in Computer Science REVIEW ARTICLE Available Online at www.jgrcs.info, JGRCS 2010

[12] Oleg Vyshnyvetshkey, sebistian gulloex, Homomorphic block cipher final presentation, RIT cryptographic course, 2012

[13] Wikipedia documents, https://en.wikipedia.org/wiki/ International_Data_ Encryption Algorithm

[14] Xilinx documents, https://www.xilinx.com/products/m design-tools/Vivado-design-suite.html

[15] Vertex 4 VLX 200 FPGA datasheet, https://www.xilinx.com/support/documentation /datasheets/ds112.pdf

[16] NPTL lectures on VHDL, http://nptel.ac.in /courses/117108040

