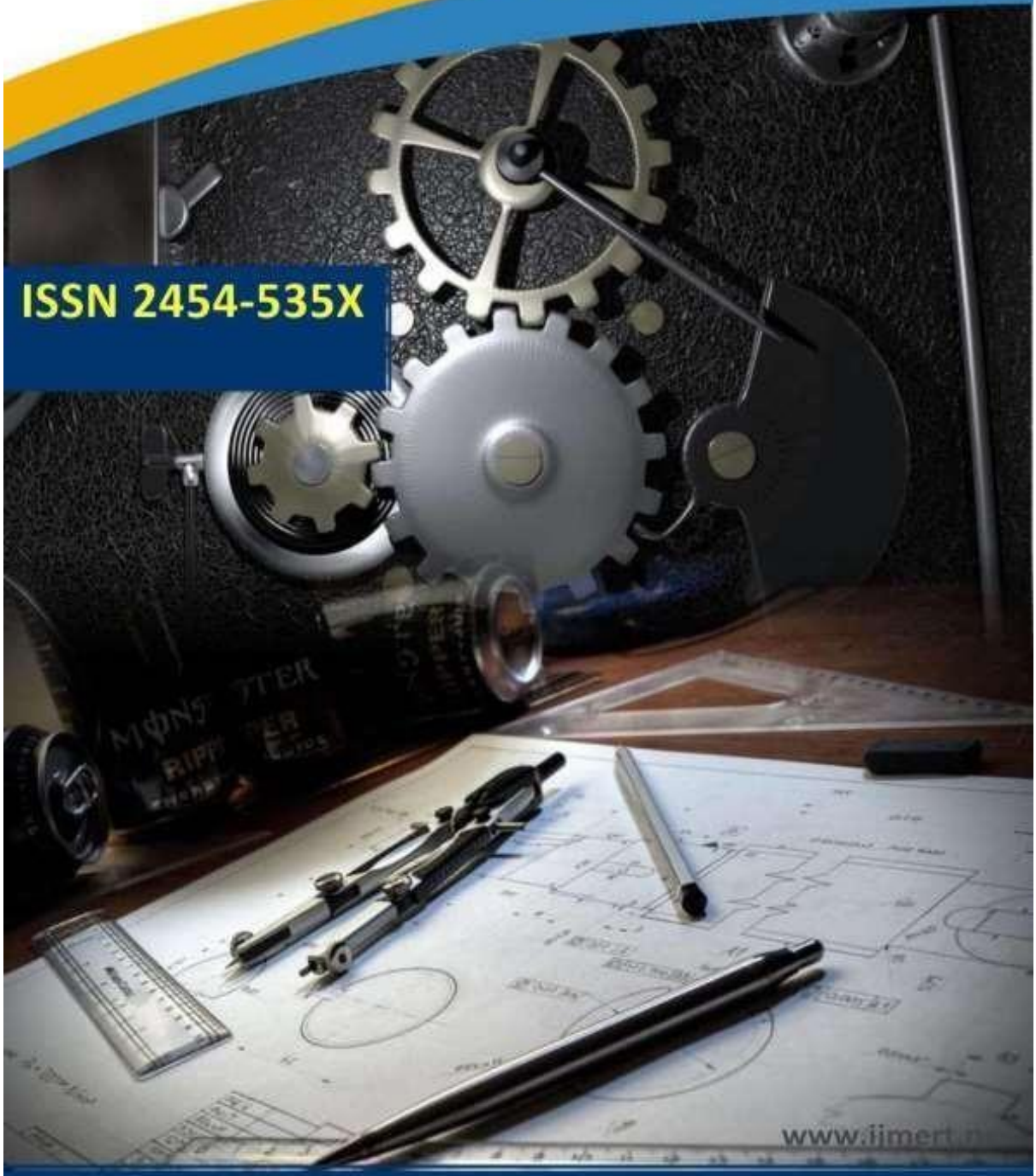
# International Journal of Mechanical Engineering Research and Technology

ISSN 2454-535X





Email ID: info.ijmert@gmail.com or editor@ijmert.net

International Journal of Mechanical Engineering Research and Technology
ISSN 2454 – 5X
http://www.ijmert.com
Vol.14 Issue. 4, Dec 2022

# DESIGN AND IMPLEMENTATION OF AREA EFFICIENT LATTICE BASED CRYPTOGRAPHY

*[1] Dr. C. Jaja Kumar, [2] K. Sanjeev Rao, [3] N. Ramesh Babu*

[1] Professor, Department of ECE, AM Reddy Memorial College 0f Engineering and Technology, Andhra Pradesh 522601

[2] Associate Professor, Department of ECE, AM Reddy Memorial College 0f Engineering and Technology, Andhra Pradesh 522601

[3] Assistant Professor, Department of ECE, AM Reddy Memorial College 0f Engineering and Technology, Andhra Pradesh 522601

**ABSTRACT: With a recent increase in the advancement of the technology, computer system and it's sensitive data are getting exhibited to unauthorized users, with steadily corroding the fundamentals of computer security. This, in fact, demanded fundamental innovations that require several cryptographic paradigms and security protocol. The interest in lattice-based cryptography is increasing due to its quantum resistance and its provable security under some worst-case hardness assumptions. As this is a relatively new topic, the search for efficient hardware architectures for lattice based cryptographic building blocks is still an active area of research. Therefore implementation of hardware efficient lattice based cryptography is proposed in this project. This lattice based cryptography architecture is implemented by using the Number Transform Theory (NTT) for area optimizations to the most critical and insensitive operation applications. The proposed hardware architectures can reduce slice usage, number of utilized memory blocks and total memory accesses by using a simplified address generation, improved memory organization. Compared to prior work, with similar performance the proposed hardware architectures can save number of occupied slices, used memory blocks and can fit into smallest Xilinx Spartan-6 FPGA.**

**KEYWORDS: Cryptography, lattice-based cryptography, Memory usage, Number Transform Theory (NTT), Xilinx.**

## I. INTRODUCTION

The impending realization of scalable quantum computers will have a significant impact on today's security infrastructure. With the advent of powerful quantum computers public key cryptographic schemes will become vulnerable to quantumalgorithm, undermining the security current communications systems.

Post-quantum (or quantum-resistant) cryptography is an active research area, endeavoring to develop novel and quantum resistant public key cryptography. Amongst the various classes of quantum-resistant cryptography schemes, lattice-based cryptography is emerging as one of the most viable options. Its efficient implementation on software and on commodity hardware has already been shown to compete and even excel the performance of current classical security public-key schemes. This work discusses the next step in terms of their practical deployment, i.e., addressing the physical security of lattice-based cryptographic implementations [1].

These public-key schemes are used in today's security infrastructure to provide public-key encryption and (authenticated) key exchange [2]. Reacting to this urgency, much research is now being conducted into quantum-resilient or post quantum cryptography of the various flavors of quantum-resilient cryptography proposed to date, lattice-based cryptography (LBC) stands out for various reasons. Firstly, these schemes offer security proofs based on NP- hard problems with average-case to worst- case hardness. Secondly, in addition to being quantum-age secure, the LBCimplementations are notable for their efficiency, primarily due to their inherent linear algebra based matrix/ vector operations on integers. Thirdly, LBC constructions offer extended functionality for advanced security services such as identity-based encryption (IBE) attribute-based encryption (ABE) and fully-

International Journal of Mechanical Engineering Research and Technology
ISSN 2454 – 5X
http://www.ijmert.com
Vol.14 Issue. 4, Dec 2022

Homomorphism encryption (FHE), in addition to the basic classical cryptographic primitives (encryption, signatures, key exchange solutions) needed in a quantum age [3].

There are three classes of lattices that are relevant for cryptography. Schemes that are based on LWE are standard or random lattice-based schemes [4]. These schemes have in common that they require computations with large matrices that either need a lot of memory or require costly on-the-fly computations. A further issue with standard lattice-based schemes is that they require matrix-vector multiplication with quadratic complexity. Ideal or ring lattice-based schemes are an alternative to standard lattices. The major difference between these classes of lattices is that the matrix that is used in standard lattices is represented by a single row in ring lattices. The remaining rows are generated by cyclic shifts of thefirst row. Therefore ideal lattice-based schemes are more efficient as they require less memory and the main arithmetic operation is polynomial multiplication instead of matrix-vector multiplication. With the help of the number-theoretic transform (NTT) polynomial multiplication can be accelerated to have a complexity of O(n logn).

## II. LITERATURE SURVEY

In [5], Valencia et al. discuss the vulnerability of R-LWE encryption against fault attacks. The work explored several possible fault injection effects, including single bit flip, single bit zeroing, and skip instructions and examines the consequences and the possibility of recover secret data. In [6], Espitau et al. investigated the implication of early Loop abort Faults for various stages of lattice based signature schemes including BLISS, GLP, TESLA and the GPV scheme. For BLISS (and the rest of the Fiat-Shamir family signatures), an early termination of the generation loop for the random commitment element (y1) enables a full recovery of the secret key value s1. For GPV signature schemes too, reconstruction of the entire secret key is possible by an early loop abort fault considered for the Gaussian sample generation during signature calculation.

In [7], Bindel et al. investigated the vulnerability and resistance of multiple lattice-based signature schemes including BLISS, ringTESLA and GLP signatures. They considered the first order randomizing, zeroing, and skipping faults and found effective attacks against all the signature schemes. All three schemes were found vulnerable against zeroing faults during the signing and verification, against skipping faults during the key generation, against two kinds of skipping faults during the verification. The work also suggested optimized code modifications as countermeasures against these attacks. Yuan et al. [8] reported a new type ofhardware AES implementation has been reported. In this paper Masked SBox for AES approach is discussed. Different types of masking that are used in practise according to masking functions are Boolean masking, Additive masking, Multiplicative masking and mixed masking.

In another implementation work (Borkar et al., [9]), the AES algorithm has been implemented using XCV600BG560-6 FPGA. The maximum operating frequency reported in this work is 140.390MHz. An encryption/decryption throughput of 352 Mbits/second has been obtained during the AES implementation. This method which uses Ciper FeedBack (CFB) mode for block encryption and decryption, consumes 1853 slices and 391 Bonded IOBs of Virtex FPGA considered for implementation. The

International Journal of Mechanical Engineering Research and Technology
ISSN 2454 – 5X
http://www.ijmert.com
Vol.14 Issue. 4, Dec 2022

hardware consumption is 26% of the total capacity of FPGA. Although FPGA-based cryptographic algorithm implementation has been widely studied during the past few years, a thorough comparative study of published implementations has not been presented, at least to the authors‟ knowledge. The article by Wollinger et al.
[10] included a review of implementations, but otherwise the article concentrated more on security questions of FPGAs as implementation platforms. In this article, implementations of cryptographic algorithms are compared in terms of speed, area and implementation techniques. Finally, certain conclusions on cryptographic algorithm implementation on FPGAs are presented.

## III. PROPOSED SYSTEM

Lattice-Based Cryptography uses high-dimensional geometric structures to hide information, creating problems that are considered impossible to solve without the key even by universal fault-tolerant quantum computers. The proposed lattice-based cryptography is implemented with area optimizations for the most critical and computationally-intensive operation in polynomial multiplication using the Number Theoretic Transform (NTT). In this paper, main aim is to design a lightweight hardware implementation of Lattice-Based Cryptography, which uses a small amount of resources but also guarantees security.

Plain text is the binary data bits in its natural format and in a readable form. Plain text is human-readable and extremely vulnerable from a confidentiality perspective. Plain text is also called clear text. Plain text is a message or data that has not been turned into a secret. Cipher Text is the altered form of plaintext data so as to be unreadable for anyone except the intended recipients. In other words, it has been turned into a secret. An eavesdropper or an attacker seeing the ciphertext would be unable to easily read the message or determine its content.

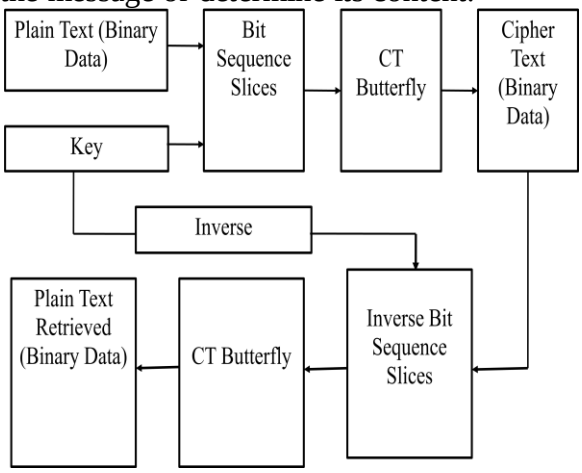



**Fig. 1: BLOCK DIAGRAM OF PROPOSED LATTICE BASED CRYPTOGRAPHY ARCHITECTURE**

To implement the costly polynomial multiplication, we use the number theoretic transform (NTT). Rather than using the block RAM, the proposed design is implemented with distributed RAM (i.e., LUTM (Look Up Table Memory), which can achieve high frequency and throughput. There are log n stages, and at each stage a total of n values are evaluated. At each iteration of the inner loop two values are generated as in a Cooley-Tukey (CT) radix-2 butterfly, hence it takes (n/2)(log n) iterations to complete the NTT operation ofa polynomial with n coefficients. CT Butterfly executes the CT radix-2 butterfly. After the NTT of two vectors are calculated, point-wise multiplication and the inverse NTT should also be computed. The key observation is that during system tasks there are sequential multiplications of the coefficients by the powers of $\varphi$, $\varphi^{-1}$, $\omega$ and
$\omega^{-1}$. During the execution of the 1st system task, the first coefficients $a_c$,$b_o$ will be multiplied by $\varphi^0$, the second coefficients $a_1$, $b_1$, by $\varphi^1$, and so on, up to the multiplication of the last coefficients by $\varphi^{n-1}$. The input polynomial coefficients are supplied to the

International Journal of Mechanical Engineering Research and Technology
ISSN 2454 – 5X
http://www.ijmert.com
Vol.14 Issue. 4, Dec 2022

Hardware in an interleaved fashion and operands are generated by the multipliers on-the-fly.

The classic CT Butterfly architecture is used in the NTT of polynomial coefficients. At each execution of the CT Butterfly, two coefficients should be read out from the bit sequence slices and also two output coefficients should be written back to the bit sequence slices. This corresponds to four bit sequence slices accesses at each clock cycle. Moreover, this also requires the generationof two read and two write addresses. Even with the bit sequence slices s configured as dual-port, the four accesses requires duplication of each bit sequence slices. The key observation is that most of the system tasks will be performed on the same coefficients of two polynomials. If a coefficient pair of two polynomials $\{a_i, b_i\}$ will be multiplied with the same power $\varphi^1$, then that pair will be transformed using the same powers of w and the pair will also be point-wise multiplied. Instead of storing the coefficients of two polynomials in separate bit sequence slices and executing these system tasks on the first polynomial and then to the second polynomial, we can store two coefficient pairs of the polynomials in the same address and apply execution of the system task in a concurrently-interleaved fashion.

## IV. RESULTS

The Xilinx design environment was used to implement and examine the developed algorithm. The architecture of proposed algorithm is shown in Fig. 2 and Fig. 3. The below Fig. 2 and Fig. 3 shows the RTL schematic and technology schematic of Proposed lattice based cryptography algorithm. RTL schematic is thecombination of inputs and outputs. Register-transfer logic deliberation is utilized inequipment portrayal dialects (HDLs) like Verilog and VHDL to make elevated level portrayals of a circuit, from which lower-level portrayals and at last genuine wiring can be determined. Structure at the RTL level is run of the mill practice in present day advanced plan.

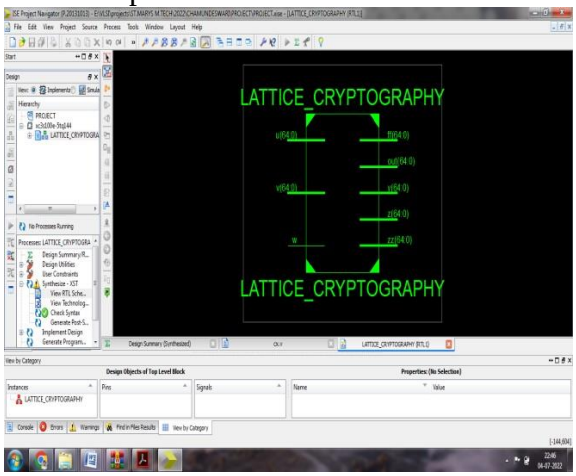



**Fig. 2: RTL SCHEMATIC OF PROPOSED METHOD**

The combination of Look up tables, K-Map, Truth Tables & equations is the Technology schematic. The Fig. 3 represents the proposed system Technology schematic. After optimization & technology targetingphase of synthesis process the Technology schematic was generated. Schematic showing the design in terms of optimizedlogic elements for the Xilinx target device orexample, the logic elements are carry logic, I/O buffers, LUTs & other specified technology components.

International Journal of Mechanical Engineering Research and Technology
ISSN 2454 – 5X
http://www.ijmert.com
Vol.14 Issue. 4, Dec 2022

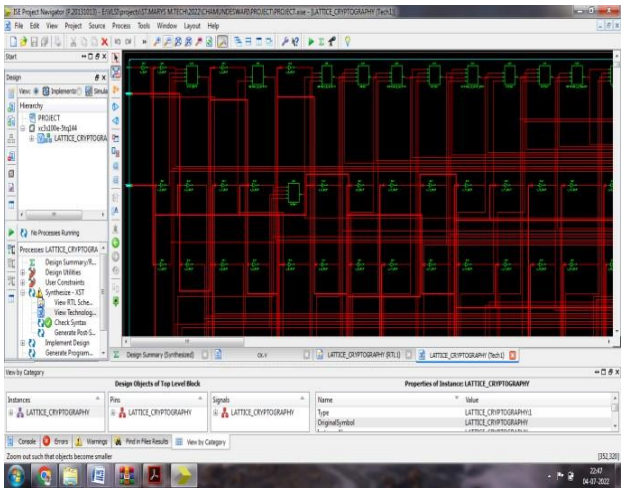


**Fig. 3: TECHNOLOGY SCHEMATIC OF PROPOSED METHOD**

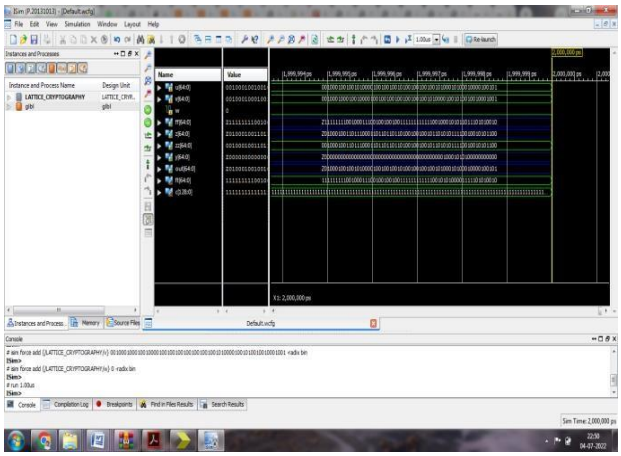


**Fig. 4: OUTPUT WAVEFORMS OF PROPOSED METHOD**

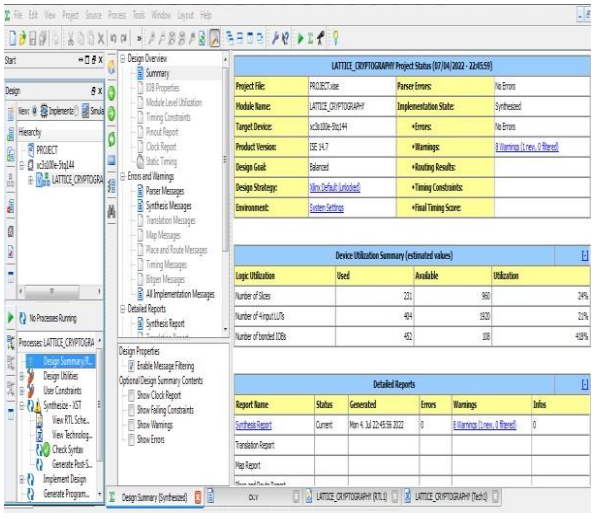


**Fig. 5: DEVICE UTILIZATION**

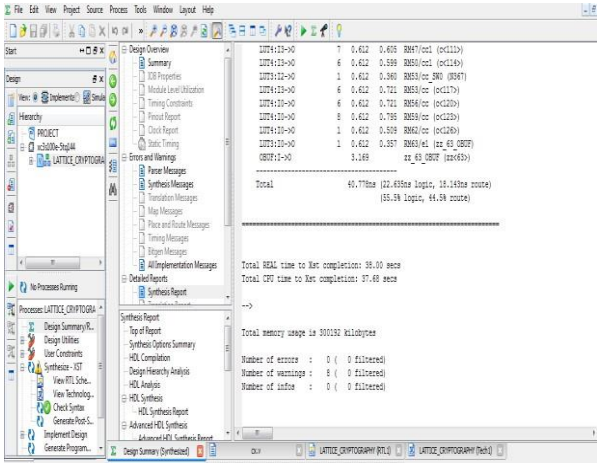


**Fig. 6: MEMORY UTILIZATION**

## V. CONCLUSION

In this project, design and implementation of hardware efficient lattice based cryptography was implemented. Thisconcept of lattices and its hardness is mainlyused as an update to the current cryptographic schemas. Lattice-based cryptography is a complex cryptic method which is meant to protect our data and secure us from cyber threats generated from the quantum computing system consisting of millions of bits. The lattice based cryptography was synthesized in FPGA technology with the VHDL experimental results, and this system provides security in efficient way & it is faster than CPU. The Lattice based cryptography taken small amount of hardware resources. Based on the overall performance analysis it can be concluded that this design provides betterperformance than others in terms of the area and the timing.

## VI. REFERENCES

[1] Y. Xing and S. Li, "An Efficient Implementation of the New Hope Key Exchange on FPGAs", IEEE Transactions on Circuits and Systems *I: Regular Papers*, vol. 67, no. 3, pp. 866-878, Mar. 2020.

[2] T. N. Tan and H. Lee, "High-secure fingerprint authentication system using ring-

International Journal of Mechanical Engineering Research and Technology
ISSN 2454 – 5X
http://www.ijmert.com
Vol.14 Issue. 4, Dec 2022

LWE cryptography", *IEEE Access*, vol. 7,pp. 23379-23387, Feb. 2019

[3] W. Liu, S. Fan, A. Khalid, C. Rafferty and M. O'Neil, "Optimized schoolbook polynomial multiplication for compact lattice-based cryptography on FPGA", *IEEE Trans. Very Large Scale Integr., (VLSI) Syst.*, vol. 27, no. 10, pp. 2459-2463, Oct. 2019.

[4] D. Liu, C. Zhang, H. Lin, Y. Chen and M. Zhang, "A resource-efficient and side-channel secure hardware implementation of ring-LWE cryptographic processor", *IEEE Trans. Circuits Syst. I Reg. Papers*, vol. 66, no. 4, pp. 1474-1483, Apr. 2018.

[5] Felipe Valencia, Tobias Oder, Tim Güneysu, and Francesco Regazzoni, "Exploring the Vulnerability of R-LWE Encryption to Fault Attacks. 5th Workshop on Cryptography and Security in Computing Systems", - Workshop - HiPEAC (2018)

[6] Thomas Espitau, Pierre-Alain Fouque, Benoît Gérard, and Mehdi Tibouchi. 2016. Loop-abort faults on lattice-based Fiat-Shamir and hash-and-sign signatures. In International Conference on Selected Areas in Cryptography. Springer, 140–158.

[7] Nina Bindel, Johannes Buchmann, and Juliane Krämer, "Lattice-based signature schemes and their sensitivity to fault attacks", In Fault Diagnosis and Tolerance in Cryptography (FDTC), 2016 Workshop on, IEEE, 63–77.

[8] Yuan, Z., Y. Wang, J. Li, R. Li and W. Zhao, 2011. FPGA based optimization for masked AES implementation. Proceedingsof the 2011 IEEE 54th International Midwest Symposium on Circuits and Systems (MWSCAS), August 7-10, 2011,
Seoul, pp: 1-4

[9] Borkar, A.M., R.V. Kshirsagar and M.V.Vyawahare,2011,FPGAimplementation of AES algorithm. Proceedings of the 2011 3rd International Conference on Electronics Computer Technology (ICECT), April 8-10, 2011, Kanyakumari, pp: 401-405

[10] Wollinger, T., Guajardo, J., and Paar, C.: „Security on FPGAs: state of the art implementations and attacks", ACM Trans. Embed. Comput. Syst., 2004, 3, pp. 534–574