Design High Speed and Area Optimised dual Key Encryption using VHDL: A Review

1Neelam Soni, 2Shivam Solanki
1M.Tech Student, 2Asst.professor
Takshila Institute of Engineering and Technology, Jabalpur.

Abstract: **Arrange Security and double key cryptography in rapid systems requests for particular equipment to coordinate with the quick system. These equipment outlines are being created utilizing reconfigurable FPGA innovation to bolster mass calculation. In the cryptographic module, Dual key International Data Encryption Algorithm (IDEA), a symmetric key piece figure is been planned as the calculation for execution. The plan objective is to build the information encryption rate i.e. the throughput to a significant esteem so that the plan can be utilized as a cryptographic processor in fast system applications. Every one of the plans are coded utilizing HDL dialect VHDL and are integrated utilizing Xilinx ISE 9.2i for confirming their usefulness and working. Vertex IV ace FPGA is picked as the objective stage gadget for acknowledgment of the proposed plan. Our work is chiefly in view of outlining a proficient engineering (IP) for a cryptographic module for secure information trafficking and a system interruption identification framework for a rapid system. The entire outlines are coded utilizing VHDL dialect and are confirmed utilizing Xilinx-ISE test system for checking their usefulness.**

Keywords: **Field Programmable Gate Array (FPGA), International data encryption algorithm (IDEA), Network Intrusion Detection System (NIDS), Look up Table (LUT), VHSIC Hardware Description Language (VHDL)**

I-INTRODUCTION

Cryptography is study and routine of procedures of secure information correspondence in nearness of different gatherings. More points of interest, it is about creating and breaking down conventions that maintain a strategic distance from impact of foes and which are worry to different diverse viewpoints in data security, for example, information secrecy, validation, information honesty and non-revocation. Presently a day's double key cryptography converges controls of software engineering, arithmetic and electrical building. Uses of double key cryptography incorporate PC passwords, ATM cards and electronic trade. The fig 1.1 demonstrates a fundamental cryptographic model in which information which is to be transmitted is gone through encryption framework and yield so produced is called 'figure'. On getting terminal figure is unscrambled to get unique information.

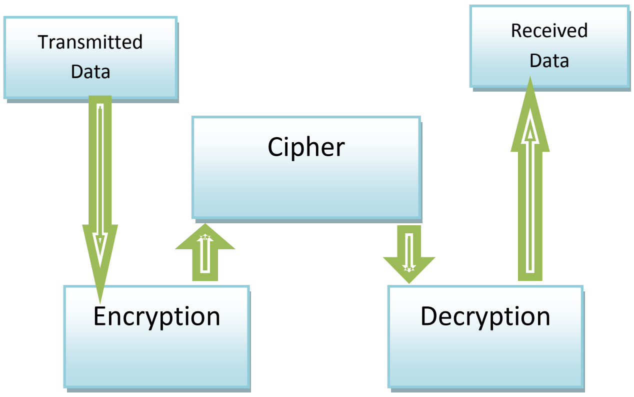

Figure 1 Basic Cryptographic model

II-LITERATURE SURVEY

Zhongyuan Hao et al [1] in this paper, plan and FPGA (Field Programmable Gate Array) execution of installed framework for time based IDEA encryption is displayed. By and by accessible encryption frameworks, experience the ill effects of Brute Force assault in which every single key mix are gone for to locate the right key. In such a case, the time taken for breaking the code relies on upon the framework utilized for cryptanalysis. In the proposed framework, time is utilized as a moment measurement of the key. That is, the right key entered at the right time is required for appropriate unscrambling. As their proposed framework needs simultaneous execution and continuous preparing, the framework is actualized utilizing Vertex 4 FPGA and the outcomes are displayed. LI Wei et al [2] An Efficient and adaptable usage of square figures is basic to accomplish data security handling. Existing execution techniques, for example, GPP, FPGA and cryptographic application-particular ASIC give the wide scope of support. In any case, these techniques couldn't accomplish a decent exchange off between fast handling and adaptability. In this paper, we exhibit a reconfigurable VLIW processor design focused at piece figure handling, examine fundamental operations and capacity qualities, and propose the multi-bunch enroll document structure for square figures. Ten sorts of square and hash figures were acknowledged in the processor. The encryption throughput of AES, DES, IDEA, and SHA-1 calculation is 1554Mbps, 448Mbps, 785Mbps, and 424Mbps individually; the test outcome demonstrates that our processor's encryption execution is essentially higher than different plans.

Table 1: literature work

Author	Brief	Results
Zhongyuan Hao et al [1]	FPGA implementation of IDEA encryption is presented, used as a second dimension of the key. That is, the correct key entered at the correct time is needed for proper decryption	Vertex4, 11342 slice at 1.06 Mhz
LI Wei , ZENG et al [2]	Reconfigurable VLIW processor architecture targeted at block cipher processing for AES, DES, IDEA, and SHA-1 algorithm	Vertex4, 11589 slice at 0.982 Mhz

Problem Statement: The accessible Encryption techniques like AES, DES, Blowfish, and RSA and so forth are adequate however require loads of time and territory and power prerequisite like for this another encryption strategy is been created and exhibited in the proposal work which is very secure (profoundly torrential slide) , exceedingly throughput (less calculation time) as look at existing encryption strategies. The fundamental point of proposed work is to configuration, reproduce and confirm the usefulness of proposed encryption strategy which is very computationally costly and are exceptionally testing in other accessible techniques. To create proposed act as a free module in a rapid secure system. This can be said in explained as: When privacy concerns, the thought process is to outline an improved design for Encryption which is profoundly perplexing with less region and time necessity.

Zhongyuan Hao et al. [1] they presume that, 64 bit size of the key gives sufficient level of security right now, because of the expansion in the speed of the framework with most recent innovations in the IC manufacture houses, the key size should be expanded relatively. Their proposed plot gives an option strategy in which the quality of the IDEA calculation is kept up with no alteration yet at the same the framework can't guard against savage compel assault all the more enthusiastically because of straightforwardness.

LI Wei et al [2] Open test vector was received by capacity recreation, and the way that reproduction results and test vector information are can't be checked the rightness of framework rationale capacities. Their plan does not have the quickest speed; notwithstanding it accomplishes the adjust of speed and assets under the preface of guaranteeing encryption and unscrambling speed.

III-METHODOLOGY

Dual key IDEA is a symmetric, secret-key block cipher. The keys for both encryption and decryption must be kept secret from unauthorized persons. Since the two keys are symmetric, one can divide the decryption key from the encryption one or vice versa.

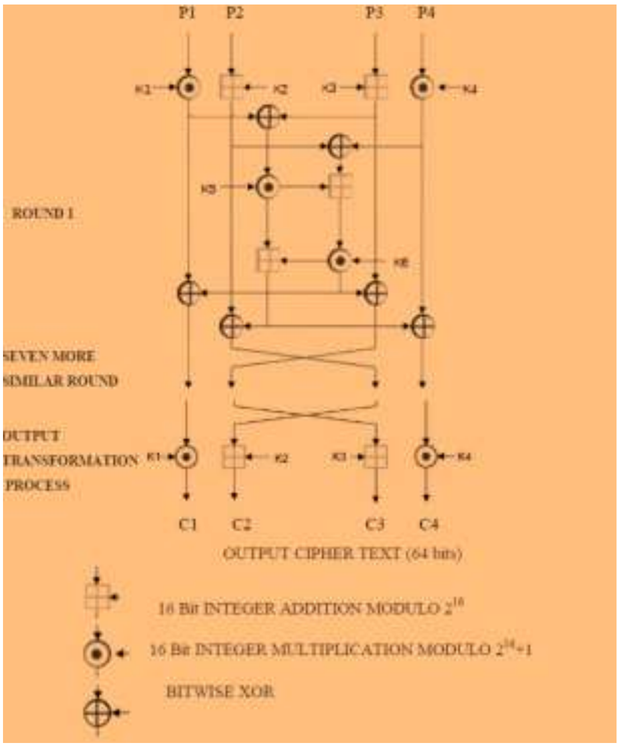
P1
P2
P3
P4
K1
K2
K3
K4
K5
K6
ROUND 1
SEVEN MORE
SIMILAR ROUND
OUTPUT
TRANSFORMATION
PROCESS
K1
K2
K3
K4
C1
C2
C3
C4
OUTPUT CIPHER TEXT (64 bits)
16 Bit INTEGER ADDITION MODULO 2^16
16 Bit INTEGER MULTIPLICATION MODULO 2^16+1
BITWISE XOR

Figure 2 International Data Encryption Algorithm (IDEA)

The extent of the key is settled to be 128 bits and the measure of the information piece which can be taken care of in one encryption/unscrambling procedure is settled to 64 bits. All information operations in the Dual key IDEA figure are in 16-bit unsigned whole numbers. When preparing information which is not a whole number numerous of 64-bit square, cushioning is required. The security of Dual key IDEA calculation [4] depends on the blending of three various types of mathematical operations: EX-OR, expansion and secluded duplication. Double key IDEA is based upon a fundamental capacity, which is iterated eight circumstances. The principal emphasis works on the info 64-bit plain content piece and the progressive cycles work on the 64-bit obstruct from the past cycle. After the last emphasis, a last change step creates the 64-bit figure square. The calculation structure has been picked to such an extent that, with the special case that distinctive key sub-squares are utilized, the encryption procedure is indistinguishable to the decoding procedure. Double key IDEA utilizes both disarray and dissemination to encode the data.Three mathematical gatherings, EX-OR, expansion modulo 216, and increase modulo (2^{16} + 1), are mixed, and they are all easily implemented in both hardware and software. All these operations operate on 16-bit sub-blocks.

In each round of the 8 rounds of algorithm, the following sequences of events [1] are performed:

1. Multiply* P1 and K1
2. Add* P2 and K2
3. Add* P3 and K3
4. Multiply* P4 and K4
5. XOR the results of step 1 and step 3
6. XOR the results of step 2 and step 4
7. Multiply* the results of step 5 with K5
8. Add* the results of step 6 and step 7
9. Multiply* the results of step 8 with K6
10. Add* the results of step 7 and step 9
11. XOR the results of step 1 and step 9
12. XOR the results of step 3 and step 9
13. XOR the results of step 2 and step 10
14. XOR the results of step 4 and step 10

Sequence of events followed in the output transformation round:-

1. Multiply* R1 and K1
2. Add* R2 and K2
3. Add* R3 and K3
4. Multiply* R4 and K4

New Modulo (2^N + 1) multiplier: Binary numbers with n bits are denoted as

A= an-1an-2…..a0

in the following text, where

n-1
A= Σ 2^ia_i
i=0

Reduction of a number A modulo a number M (“A mod M”) can be accomplished by a division
(with the remainder as result) or by iteratively subtracting the modulus until A < M.

For modulo multiplication,

P = X .Y mod (2^n + 1)

The reduction modulo (2n+1) can be computed as:

A mod (2^n+1) = (A mod 2^n – A div 2^n) mod (2^n + 1)

Modulo (2^n + 1) multiplication using the normal number representation can be formulated as:

X.Y mod (2^n+1) = (X.Y mod 2^n – X.Y div 2^n) mod (2^n + 1)

As observed from the Dual key IDEA cipher algorithm there is four types of computation (2^n + 1) modulo multiplier, (2^n) modulo adder, XOR and shifter in key generation.

Out of these the ability to perform fast modulo 2^n+1 multiplication is then still a major challenge, particularly from a hardware point of view. Even though a modulo 2^n + 1 multiplier can be implemented using look-up tables, the memory requirements are a big constraint for large values of *n*. Hence, to avoid the exponential growth of the memory requirements several implementations based on combinational arithmetic circuits have been proposed.

First let for n=4
(2^n + 1) can be factorized in four forms below:-
R1=10001000
R2=01000100
R3=00100010
R4=00010001
R1, R2, R3 and R4 are possible four various factors of 2^4+1
Let if X=0110 and Y= 0101
Than XY= 011110
Possible solution with proposed method is =>
00011110 – 00010001 => 0000111
Observed ANS in only one step
Let if X=1110 and Y= 1101
Than XY= 10110110
Possible solution with proposed method is =>
10110110 – 10001000 => 00101110 - 00100010 => 00001100
Observed ANS in only two steps

Let if X=1010 and Y= 1101
Than XY= 10000010
Possible solution with proposed method is =>
10000010 – 01000100 => 00111110 - 00100010 => 00011100-00010001=>00001001
Observed ANS only in three steps it is MAX steps required with proposed architecture
The same approach is been used for 2^8+1 and 2^{16}+1 modulo multiplier

IV-CONCLUSION

One can finish up for writing study for which we have experienced many research papers, books, Datasheets of EDA apparatuses and references chateau in this paper proposed work is a superior cryptograph strategy regarding region and throughput, as known double key cryptography is only an overhead for any framework and it ought not required loads of range or investment so proposed work can be answer for the same as proposed work requires less zone and time as contrast with other existing work in a similar research zone.

Theory work can at long last infer that the speed of proposed Dual key IDEA figure generator module is better that past work done that are examine in writing survey, when range concerns proposed work is direct.

REFERENCES

[1] 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

[2] 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

[3] Based on the 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

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

[5] 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, Issue 2, February 2013, ISSN (Online): 2278 – 8875

[6] NICK HOFFMAN, A SIMPLIFIED IDEA ALGORITHM, online documents, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.501.2662&rep=rep1&type=pdf

[7] 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