ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

Design of Block Cryptographic Processor Using VLIW Architecture

Poornima K V S [1], Sukumar B S[2]

P.G. Student, Department of ECE, CBIT College, Kolar, Karnataka, India[1]

Asst. Professor, Department of ECE, CBIT College, Kolar, Karnataka, India[2]

ABSTRACT: Data security is the everyday requirement in this digital world. This digital data is prone to intrusion activities hence it needs to be secured. Cryptographic algorithms are one of the best options to secure the digital data stream. Flexible and efficient implementation of block ciphers is critical to achieve information security processing. Existing implementations of block cipher like FPGA, GPP and cryptographic ASIC provide wide range of support but there are limited in factors like processing speed and flexibility. This paper proposes an approach for flexible implementation of block cipher. The proposed processor not only flexibly accomplishes the combination of multiple basic cryptographic operations, but also realizes dynamic configuration for cryptographic processing units. The AES algorithm is considered because of its high end applications and VLIW platform to meet the high speed requirements.

KEYWORD: Cryptographic algorithm, Block Cipher, VLIW.

I. INTRODUCTION

Security forms the backbone of today's digital world. Today most of the sensitive data is stored digitally. Bank accounts, medical records and personal emails are some categories where the data must kept secured; this has made cryptography an important and necessary research topic. In specific cryptography is a method of processing and transmitting data in a particular form so that for whom it is intended can read/process the data[1].

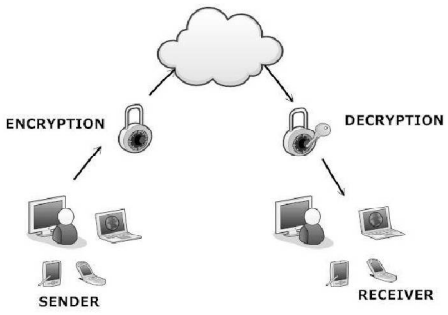

Figure 1: Basic Cryptographic Operation[1]

There are mainly two types of cryptographic systems used for security purpose. One is Symmetric key algorithm (also known as Private Key algorithm) and other is Asymmetric key algorithm (also known as Public key algorithm).The symmetric key algorithm uses same key for encryption and decryption of a message like Advanced Encryption Standard (AES), Data Encryption Standard (DES).The asymmetric key algorithm use one key for encryption of a message and a different key for the decryption of same message. Asymmetric algorithms also called *public key algorithms*, use different keys for encryption and decryption. One key is called *public key* and can be handed

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

out to all communication partners without compromising security. The second key, however, must be kept private and is therefore called *private key*. Public key algorithms are designed in a way that a message encrypted with someone's public key can only be decrypted with that person's private key and vice versa. Private Key algorithm due to having high throughput is suitable for data communication, and public key algorithm with much lower throughput are suitable for key exchange. The class of symmetric algorithms divides further into stream ciphers and block ciphers. As the name suggests, stream ciphers operate on a stream of data; depending on the context such a stream can be either be a stream of bits or bytes. Block ciphers, in contrast, operate on data chunks of certain size which means that a message distributes over a number of blocks. The size of these blocks is determined by the selected algorithm and algorithm configuration. The size of these blocks is determined by the selected algorithm and algorithm configuration. In case of DES, which is the first standardized crypto algorithm, block size is 64-bit. Advanced Encryption Standard (AES), a Federal Information Processing Standard (FIPS), is an approved cryptographic algorithm that can be used as private key algorithm [2].

In 1980, Josh Fisher invented the VLIW processor. Very Long Instruction Word defines the architecture of processor. In VLIW, compiler scheduled the each instructions and instructions are consists of grouped multiple independent operations. VLIW processor has multiple independent functional units. The main goal of VLIW design is to reduce the hardware complexity, better performance and reduced power consumption. In VLIW compiler assigned the function units and corresponds to position within the instruction packet. Therefore VLIW architecture is suitable for digital signal processing applications and also used in compression or decompression of image and speech data of processing

In this paper, the reconfigurable VLIW processor for block ciphers which improves the performance of block cipher implementation by clock cryptographic method is proposed.

II. RELATED WORK

Block Ciphers can be designed in the following approaches

- The General purpose processor (GPP), which higher flexibility, but less throughput, it won't meet high speed encryption requirements.
- Cryptographic Application specific Integrated circuits (ASIC), here throughput is enough, put less flexibility and low configurability.
- Much reconfigurable architectures were found for block ciphers, but block ciphers are having multiple operations, but configuration of the architecture is complex.
- Application specific instruction processor (ASIP) Supports high speed cryptographic algorithms, but when it compares to reconfigurable architecture, it is very difficult and complex to operate the multiple cryptographic based specific instruction set.

A cryptographic processor implements the cryptographic algorithms with hardware. A crypto processor is like a microprocessor which carries the cryptographic operations. Types of crypto processors are : smart cards, TPM, Hardware security modules. **Smartcards**: Cryptoprocessors input program instructions in encrypted form, decrypt the instructions to plain instructions which are then executed within the same crypto processor chip where the decrypted instructions are inaccessibly stored. By never revealing the decrypted program instructions, the crypto processor prevents tampering of programs by technicians who may have legitimate access to the sub system databus[3].

III. BLOCK CIPHERS

Many block ciphers may be characterized as Feistel networks. Feistel networks were invented by Feistel and are a general method of transforming a function into a permutation. The basic Feistel network divides the data into two

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

halves where one half operates upon the other. The f-function uses one of the halves of the data block and a key to create a pseudorandom bit stream that is used to encrypt or decrypt the other half of the data block.

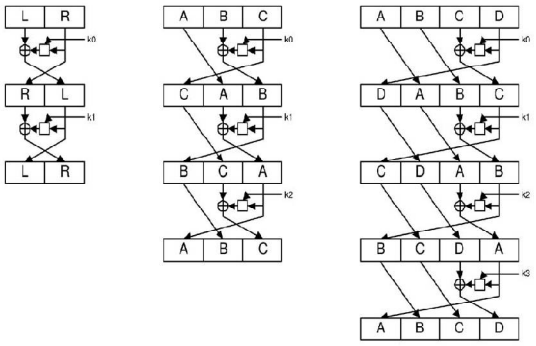

Figure 2: Block diagram for standard block ciphers [4]

Therefore, to encrypt or decrypt both halves requires two iterations of the Feistel network. A generalization of the basic Feistel network allows for the support of larger data blocks. Generalization occurs by considering the data swap as a circular right shift. This allows for the use of the same f-function, but requires multiple rounds to input all of the sub-blocks to the f-function. Fig. 2 from details the block diagram for block ciphers employing both the basic Feistel network and generalized Feistel networks of three and four blocks. The f-function is represented by the box and the ⊕symbol represents a bit-wise XOR operation. The f-function employs confusion and diffusion to obscure redundancies in a plaintext message.

Confusion obscures the relationship between the plaintext, the ciphertext, and the key. S-Box look-up tables are an example of a confusion operation. Diffusion spreads the influence of individual plaintext or key bits over as much of the ciphertext as possible. Expansion and permutation functions are examples of diffusion operations. The basic operations that may be found within an f-function include:

- . Bitwise XOR, AND, or OR.
- . Modular addition or subtraction.
- . Shift or rotation by a constant number of bits.
- . Data-dependent rotation by a variable number of bits.
- . Modular multiplication.
- . Multiplication in a Galois field.
- . Modular inversion.
- . Look-up-table substitution.

The most frequently implemented block cipher algorithms are DES and the AES candidates. The following summarizes block cipher implementations of AES algorithm in FPGAs and other reconfigurable logic. There are also a number of reconfigurable hardware-based implementations of public-key algorithms, many of which target elliptic curve cryptosystems due to the significantly reduced operand size as compared to other public-key algorithms, such as RSA[4].

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

IV. VLIW ARCHITECTURE

The Re-configurable 'VLIW' processor contains 4-modules:
1. Instruction-Fetch unit
2. Control-unit
3. Cluster execution-unit, and
4. Register-files.

In instruction-fetch module, the set of instructions can be sub-divided as 5-slots in which every slot have 4-block cryptographic-arithmetic instruction blocks and has single branch control-instruction block. Therefore, the instruction-fetch module will issue the 4-arithmetic instruction and single branch control-instruction in a single clock-cycle. Therefore "block-cryptographic arithmetic function, branch-control would be process in parallel manner.

There are 4-cluster execution units, 'Cluster-A', 'Cluster-B', 'Cluster-C', and 'Cluster-D'. The aim of every single cluster has 64 bit cryptographic function and 128 bit cryptographic function have to match with 2-clusters and 256 bit cryptographic function in 4-clusters. Every single cluster has number of re-configurable slot in cryptographic-operation module. From the analysis of 18 block-ciphers, the cluster has 9-kinds of operations:- 3-input Logic-operation, modular-addition operation, modular-multiplication operation, LUT-sbox, shift / rotation by constant-bits / variable number-bits, bit-permutation, 'Galois-field' multiplication, modular-inversion. Therefore every operation has different kinds of function modes. Consider Ex:- S-box operation has different 'AES' and 'DES' operation modes[5].

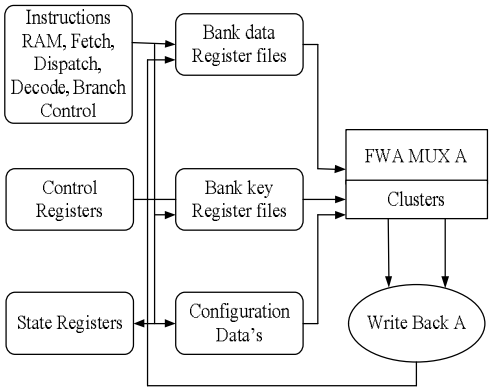

Figure.3: 'VLIW' Re-configurable architecture.

V. EXPERIMENTAL RESULTS

Once the system is designed it has to be verified using appropriate tools which supports for the design. Here as we are executing in Xilinx and simulated using and Implemented on Artix 7 FPGA Board. The executed system provides detailed description of result with their input and outputs. The design has been done using Verilog code, which stands as one of high descriptive language in VLSI.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

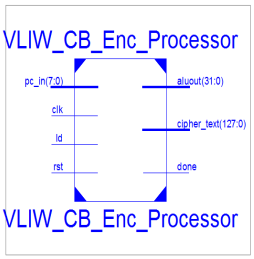

Figure.4 Cipher block encryption processor top Module

Logic Utilization	Used	Available	Utilization
Number of Slice Registers	556	126800	0%
Number of Slice LUTs	998	63400	1%
Number of fully used LUT-FF pairs	449	1105	40%
Number of bonded IOBs	172	210	81%
Number of Block RAM/FIFO	4	135	2%
Number of BUFG/BUFGCTRLs	1	32	3%

Figure.5. Cipher block encryption processor Design Summary

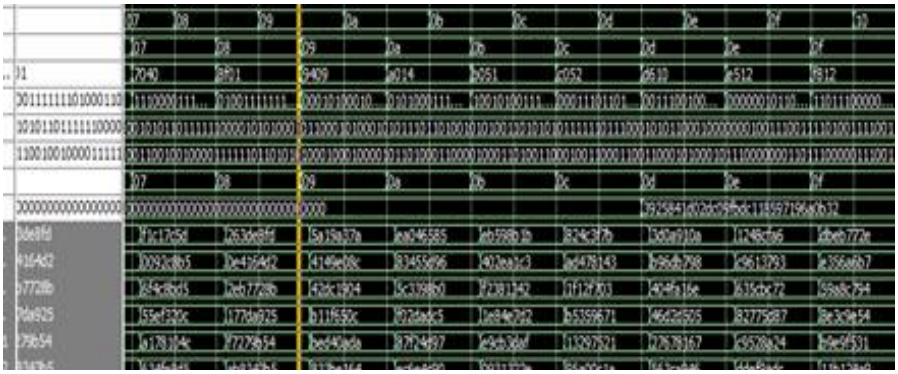

Figure 6: Test bench of crypto processor

V. CONCLUSION

The reconfigurable Block cryptographic processor is designed and implemented on FPGA. The Block cryptographic processor is majorly divided into two parts namely Encryption processor and decryption processor based on VLIW architecture which is executed the modules in pipelined manner. The processor includes mainly fetching unit decoding unit, instruction memory, data register and Execution unit. The processor architecture is completely flexible and efficient in hardware throughput, frequency and design area than other processor architectures.

REFERENCES

[1] " FPGA Implementation of High Security Hybrid Reconfigurable Cryptographic Processor with RSA and SEA", A. Chitra , K et al, International Journal of Scientific & Engineering Research, Volume 5, Issue 2, February-2014, ISSN 2229-5518

[2] "CRYPTONITE: A Programmable Crypto Processor Architecture For High-Bandwidth Applications[D]", Rainer Buchty, Institut f¨ur Informatik der Technischen Universit¨at M¨unchen

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

[3] Ross Anderson, Mike Bond, Jolyon Clulow, Sergei Skorobogatov, "Cryptographic processors – a survey", http://www.cl.cam.ac.uk/TechReports/ ISSN 1476-2986
[4] "An Instruction-Level Distributed Processor for Symmetric-Key Cryptography",
Adam J. Elbirt and Christ of Paar, IEEE Transactions on Parallel And Distributed Systems, VOL. 16, NO. 5, MAY 2005.
[5] LI Wei et al "A Reconfigurable block Cryptographic processor based on VLIW architecture", IEEE Publications, Jan 2016.