International Journal of Technology and Engineering System (IJTES)
©gopalax-Publisher of International Journals
ISSN: 0976-1345 pp. 24-28
available at : www.ijcns.com
Vol 3.No.1 Jan- March 2012

Hybrid Cryptographic Processor for Dynamic Configurations

K.S.Samyuktha[1],N.Magadevi[2]
[1]Scholar,M.E,S.A.Engineering College,Anna University of Technology,Chennai
[2]Assistant Professor ,S.A.Engineering College,Anna University of Technology,Chennai.
[1]samyucse_1705@yahoo.co.in,[2]mahadevinirmalkumar@gmail.com

Abstract— **Protecting the digital data through encryption using tools and external codes are highly cost effective and also results in performance degradation. To achieve much efficiency in encryption a reconfigurable cryptographic microprocessor is designed in this project to offer maximum digital security. A typical CPU unit with RAM, ALU, PC, Register bank and Buses are designed as prioritized units for utilizing the Cryptographic co-processors which consists of Parallel Processing Unit, Bit permutation unit, sequencing cache and Byte permutation units. The Rijndael, DES and hybrid units are also included as co-processors to play the role of encryption and decryption. A sophisticated instruction sets have been derived to issue control signals to the main processor to initiate and control cryptographic operations. The design of hybrid unit combines the effect of bit permutation and .The incoming 16 bit data is divided into 4 blocks each containing 16 bits in it. Different pair of algorithms are implemented for each block. Depending on whether the block is odd or even, the corresponding algorithm in a pair will be selected for encryption and this key note is saved in look up table maintained by the processor alone.During decryption the processor refers the look up table for encryption technique and performs the corresponding decryption to retrieve the original data. By means of .reconfiguring the processor with the selection of various co-processors the robustness of security is achieved efficiently in high speed with the minimum resources.**

. The RTL Description is done in ModelSim using Verilog HDL and the results are synthesized in Synopsys. The performance evaluation of this processing design will be analyzed through a programmable FPGA kit.Thus in this project a Hybrid architecture is proposed in which the advantage of symmetric cryptotography is used.The proposed technique presents an emerging reconfigurable hardware that delivers a high performance for cryptographic algorithms.

Keywords:Reconfigurable Cryptography,security

1. INTRODUCTION

The art of protecting information by transforming it(encrypting it)into an unreadable format,called ciphertext. Only those who possess a secret key can decipher(DECRYPT)the message into plaintext.Encrypted messages can sometimes be broken by cryptanalysis,also called code breaking,although modern cryptography techniques are virtually unbreakable. Cryptographic services are required across variety of platforms in a wide range of applications such as secure access. Generally most of cryptography algorithms are implemented in software,but software implementation cannot offer the physical security for the key. Software is OS dependent and also exposed to viruses and hackers attacks that may interrupt the OS running on the general computer.If execution on general purpose processor of the algorithm because CPU lacks of instructions of modular arithmetic with operations on very large operands.Different applications of the data encryption algorithm may require different speed and area trade-offs.Some applications such as smartcard and cellular phone,require a small area.Cryptographic processors faced by some of the problems include lack of adaptability to new encryption algorithm,larger area,more power,hugecost. Hardware cryptographic devices can be securely encapsulated to prevent any modification of the implemented algorithm.this paper presents into symmetric key systems that use a single key that both the sender and receipent have,and public key systems that use two keys,a public key known to everyone and a private key that only the receipent of the messages uses

2. CIPHER MODELS

Symmetric cipher models:It is also referred as conventional encryption. Symmetric encryption is a form of cryptosystem in which encryption and decryption are performed using the same key. Symmetric cryptography is susceptible to plain text attacks and linear cryptanalysis meaning that they are hackable and at times simple to decode. With careful planning of the coding and functions of the cryptographic process these threats can be greatly reduced. Asymmetric cryptography uses different encryption keys for encryption and decryption. In this case an end user on a network, public or private, has a pair of keys; one for encryption and one for decryption. These keys are labelled or known as a public and a private key; in this instance the private key cannot be derived from the public key.

Asymmetric cipher models: The asymmetrical cryptography method has been proven to be secure against computationally limited intruders. The security is a mathematical definition based upon the application of said encryption. Essentially, asymmetric encryption is as good as its applied use; this is defined by the method in which the data is encrypted and for what use. The most common form of asymmetrical encryption is in the application of sending messages where the sender encodes and the receiving party decodes the message by using a random key generated by the public key of the sender. Asymmetric key encryption uses different keys for encryption and decryption. These two keys are mathematically related and they form a key pair. One of these two keys should be kept private, called private-key, and the other can be made public (it can even be sent in mail), called public-key. Hence this is also called Public Key Encryption.

3. RELATED WORKS

Implementing a unified field reconfigurable processor delivers a rapid increase in communication and network applications,cryptography has become a crucial issue to ensure the security of transmitted data.Experimental results shows that the high hardware utilization.Implementing public-key cryptosystems on a general purpose processor(GPP) is flexible.A drawback of GPP realization is that it generally results in lowerthroughput rate and largser power consumption.In existing systems an application specipic integrated circuits solution generally leads to higher throughput rate at lower cost,but it is inflexible.because it is limited subset of cryptosystems.

Implemennting a bit permutation instructions for software cryptography proposed a permutation is widely used in cryptographic algorithms.However,it is not well supported in existing instruction sets. Data Encryption Standard proposed the selective application of technological and related procedural safeguards is an important responsibility of every federal organization in providing adequate security to its electronic data systems.

DES is being made available for use by federal agencies within the context of a total security program consisting OS physical security procedures,good information management and network access controls.Implementing in micro-code based architectures can be adopted to program or optimized cryptography operations in microcode read-only memories or lookup tables for enhancing the extensibility of cryptographic processors. The advantages of reconfigurable cryptographic processors include area and power effieciency,flexibility,algorithm upgradability, cost and resource efficiency and high throughput. The proposed technique of reconfigurable cryptographic processor supports two algorithms namely Advanced Encryption Standard(AES) and Data Encryption Standard(DES).

In this paper the reconfigurable cryptographic processor design is implemented on hardware with key stored in a Ram,which can make not only a forward key scheduling for encryption but also a reversed key scheduling for decryption.Therefore compared to software implementation,hardware implementation enhances the physical security as well as higher speed.Also intruders cannot easity attack,interrupt or modify its operation.

4. IMPLEMENTATION

Our implementation is restricted to the following scope of work:

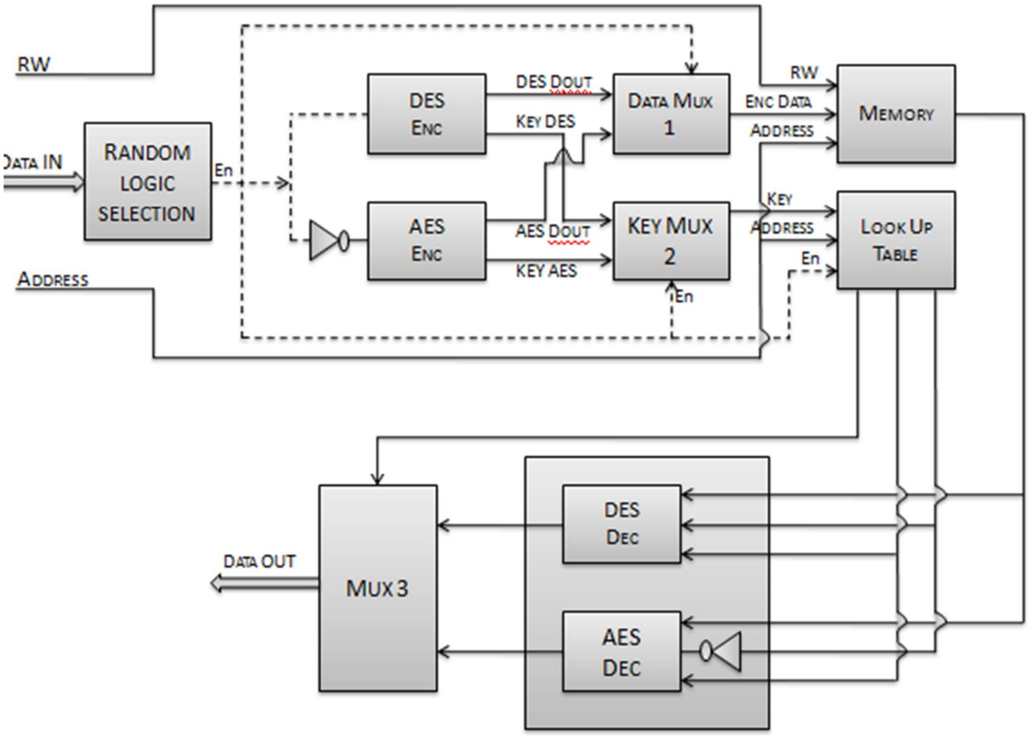
(a) The research is only to design fixed data block and key sizes using only AES and DES.

(b) The research is limited to design,to simulate,to verify the design correctness,to synthesize using synopsys tools and verify the results.

(c) Use the test vectors based on NIST.

5. RECONFIGURABLE CRYPTOGRAPHIC PROCESSOR ARCHITECTURE.

The proposed Reconfigurable cryptographic Processor is similar to traditional micro-programmed Processor architecture.The processor works only in the stand alone mode where the user has freedom to select an algorithm.Architectural optimization schemes are explored to improve hardware utilization,and specifically resource sharing among different arithmetic algorithms is iimplemented to reduce the overall hardware requirements..To protect the digital data through encryption using tools and external codes are highly cost effective and also results in performance degradation.To achieve much efficiency in encryption a reconfigurable cryptographic processor is designed in this paper to offer maximum digital security.With the conventional design of AES and DES standards as supporting co-processors,a logic module is also implemented in the design to ensure the robustness of this processor design to serve all kind of encryption and decryption needs.The performance evaluation of this processing design will be analyzed through a programmable FPGA kit.Thus in this paper a hybrid architecture is proposed in which the symmetric algorithm is used.Symmetric cryptography processor has the limitation of single key security but comparatively has the advantage of low area,resource and power consumption.For implementation AES and DES cryptography encryption is combined to mutuate a reconfigurable instruction driven processor.Even though the processor is increased a multiple pipelined architecture can be implemented in future work to reduce the hardware cost.



Reconfigurable Cryptographic processor Block Diagram

6.RECONFIGURABLEARCHITECTURE

Reconfigurable computing is a computer architecture combining some of the flexibility of software with the high performance of hardware by processing with very flexible high speed computing fabrics like field-programmable gate arrays (FPGAs). The principal difference when compared to using ordinary microprocessors is the ability to make substantial changes to the data path itself in addition to the control flow. On the other hand, the main difference with custom hardware, i.e. application-specific integrated circuits (ASICs) is the possibility to adapt the hardware during runtime by "loading" a new circuit on the reconfigurable fabric.The reconfigurable computers can be categorized in two classes of architectures: hybrid computer and fully FPGA based computers. Both architectures are designed to transport the benefits of reconfigurable logic to large scale computing. They can be used in traditional CPU cluster computers and network infra structures.The hybrid computer combine a single or a couple of reconfigurable logic chip, FPGAs, with a standard microprocessor CPU by exchanging e.g. one CPU of a multi CPU board with a FPGA,also known as hybrid-core computing,or adding a PCI or PCI Express based FPGA expansion card to the computer.This architectural compromise results in a reduced scalability of hybrid computers and raises their power consumption

In computer science lookup table is a datastructure usually an array or associative array often used to replace a runtime consumption with a simpler array indexing operation savings in terms of processing time can be significant, since retrieving a value from memory is often faster than undergoing an 'expensive' computation or input/output operation. The tables may be precalculated and stored in static program storage or calculated as part of a programs initialization phase. Lookup tables are also used extensively to validate input values by matching against a list of valid (or invalid) items in an array and, in some programming languages, may include pointer functions (or offsets to labels) to process the matching input

Hardware LUTs

In digital logic, an *n*-bit lookup table can be implemented with a multiplexer whose select lines are the inputs of the LUT and whose inputs are constants. An *n*-bit LUT can encode any *n*-input Boolean function by modeling such functions as truth tables. This is an efficient way of encoding Boolean logic functions, and LUTs with 4-6 bits of input are in fact the key component of modern FPGAs.

A.Multiplexer

A Multiplexer (or mux) is a device that selects one of several analog or digittal input signals and forwards the selected input into a single line. A multiplexer of 2^n inputs has n select lines, which are used to select which input line to send to the output.Multiplexers are mainly used to increase the amount of data that can be sent over the network with in a certain amount of time and bandwidth.A multiplexer is also called as a data selector.

B.Lookup Tables

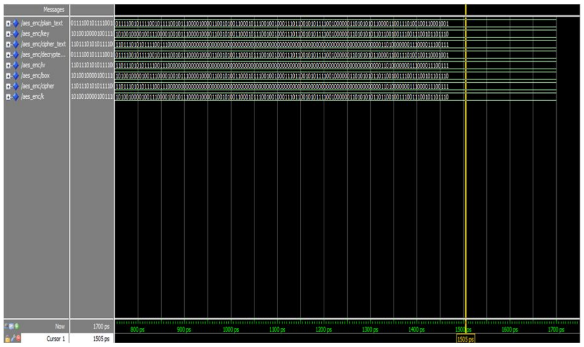
RAM is a form of computer data storage.Today it takes the form of integrated circuits that allow stored data to be accessed in any order with a worst case performance of constant time. Strictly speaking, modern types of DRAM are therefore not random access, as data is read in bursts, although the name DRAM / RAM has stuck. However, many types of SRAM, ROM, OTP, and NOR flash are still random access even in a strict sense. RAM is often associated with volatile types of memory where its stored information is lost if the power is removed. Many other types of non-volatile memory are RAM as well, including most types of ROM and a type of flash memory called NOR-Flash

AES ALGORITHM

The conventional design of AES as supporting co-processors,a logic module is also been implemented in the design to ensure the robustness of this processor design to serve all kind of encryption and decryption needs.

The Advanced Encryption Standard was published by NIST in 2001.AES is a symmetric block cipher.The Rijndael proposal for AES defined a cipher in which the block length and the key length can be independently specified to be 128,192,0r 256 bits.The AES specification uses the same three key size alternatives but

limits the block length to 128 bits.A number of AES parameters depend on the key length.Advanced Encryption Standard must be a 128 bits.Design simplicity is easy in AES.



```
Messages
/aes_enc/plain_text   01111001011110011
/aes_enc/key          10100100001001111
/aes_enc/cipher_text  11011101010111110
/aes_enc/decrypte...  01111001011110011
/aes_enc/iv           11011101010111110
/aes_enc/box          10100100001001111
/aes_enc/cipher       11011101010111110
/aes_enc/k            10100100001001111
Now                   1700 ps
Cursor 1              1505 ps
```

SIMULATION OF AES

Four different stages are used in AES:

Substitute bytes:Byte-by-Byte substitution.

Shift Rows:A simple permutation

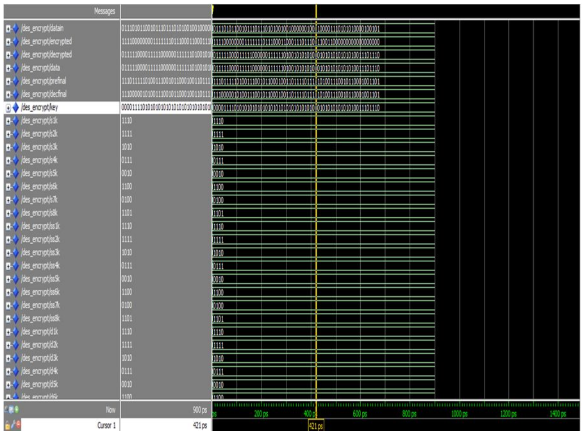
Mix Columns:A substitution that makes use of arithmetic over.

Add round key:A simple bitwise XOR of the current block with a portion of the expanded key.

DES ALGORITHM:

The overall scheme for DES encryption scheme,there are two inputs to the encryption scheme,there are two inputs to the encryption function:the plaintext to be encrypted and the key.Plaintext must be 64 bits in length and the key is 56 bits in length.The Data encryption standard algorithm is the most widely used encryption algorithm in the world.

Since the creation of DES,many other algorithms have emerged which are based on design principles similar to DES.DES works on bits,on binary numbers –the 0s and 1s common to digital computers.



```
Messages
/des_encrypt/datain     0111010110010111011101010010010000
/des_encrypt/encrypted  1111000000001111110111000110001110
/des_encrypt/decrypted  0111110000111110000000111111010010
/des_encrypt/data       0111110000111110000000111111010010
/des_encrypt/prefinal   1110111110100111001011000100110111
/des_encrypt/decfinal   1110000010100111001011000100110111
/des_encrypt/key        0000111101010101010101010101010101
/des_encrypt/s1k        1110
/des_encrypt/s2k        1111
/des_encrypt/s3k        1010
/des_encrypt/s4k        0111
/des_encrypt/s5k        0010
/des_encrypt/s6k        1100
/des_encrypt/s7k        0100
/des_encrypt/s8k        1101
/des_encrypt/ss1k       1110
/des_encrypt/ss2k       1111
/des_encrypt/ss3k       1010
/des_encrypt/ss4k       0111
/des_encrypt/ss5k       0010
/des_encrypt/ss6k       1100
/des_encrypt/ss7k       0100
/des_encrypt/ss8k       1101
/des_encrypt/d1k        1110
/des_encrypt/d2k        1111
/des_encrypt/d3k        1010
/des_encrypt/d4k        0111
/des_encrypt/d5k        0010
/des_encrypt/d6k        1100
Now                     900 ps
Cursor 1                421 ps
```

SIMULATION OF DES

7. CONCLUSION AND FUTUREWORK:

AES and DES algorithm is simulated with various input data by modelsim.Features of this project security wise the processor offers a provision to encrypt the data by mixing the algorithms AES and DES,Reconfigurable cryptography,Highly portable.

Thus in this paper proposed a Hybrid reconfigurable cryptographic processor using AES and DES.In future enhancement,we can implement our own algorithms by using the same architecture.

ACKNOWLEDGEMENT

I must thankful to Mrs.UMARANI SRIKANTH.M.E.,(Ph.D) Head of the Department, PG studies and project coordinator Mrs N.MAGADEVI.M.E Assistant Professor, Department of PG studies, without whose guidance and patience, this dissertation would not be possible. And engineering, project panel members, Professors of the Department of Electrical and Electronics Engineering for their consistent encouragement and ideas.

REFERENCES

1. Tsuyoshi Hamada, Khaled Benkrid, Keigo Nitadori and Makoto Taiji, "A c comparative study on ASIC, FPGAs, GPUs and general purpose processors in the O(N2) gravitational Nbody simulation", NASAIESA Coriference on Adaptive Hardware and Systems, 2009
2. Mancia Anguita, Javier D'laz, Eduardo Ros, and F. Javier Fem'andez-Baldomero, "Optimization Strategies for HighPerformance Computing of Optical-Flow in General-Purpose Processors", IEEE Transactions On Circuits And Systems For Video Technology, Vol. 19, No. 10, October 2009
3. Dejan Markovic, Borivoje Nikolic, and Robert W. Brodersen,"Power and Area Minimization for

Multidimensional Signal Processing", IEEE Journal Of Solid-State Circuits, Vol. 42, No. 4, April 2007

4. M. Ernst, S. Klupsch, O. Hauck, and S. A. Huss, "Rapid Prototyping for Hardware Accelerated Elliptic Curve Public Key Cryptosystems", 1074-600901,2001
5. Joan Daemen and Vincent Rijmen, The Design of Rijndael:AES - The Advanced Encryption Standard (Information Security and Cryptography), Springer Series.
6. AES secured Hardware Cryptography lecture series from Virginia Tech.
7. Hua Li, Jianzhou Li and Jing Yang, "An efficient and reconfigurable architecture for RC5" Coriference on Electrical and Computer Engineering, 2005, Page(s): 1648 -1651
8. May itani, and Hassan Diab, "Reconfigurable Computing For RC6 cryptography", Proceedings of the IEEEIACS International Conference on Pervasive Services (ICPS'04)
9. Ronald L. Rivest, 'The RC5 Encryption Algorithm",Proceedings of the 1994 Leuven Workshop on Fast Software Encryption (Springer 1995), pages 86-96
10. Ronald L. Rivest, MJ.B. Robshaw, R. Sidney, and Y.L. Yin,'The RC6 Block Cipher", Posted at RSA's RC6 page,(Version 1.1; August 20, 1998).
11. Symth, N. ; McLoone, M.; McCanny, lV., " Reconfigurable Processor for Public-Key Cryptography", IEEE Workshop on Signal Processing Systems Design and Implementation,2005.
12. Rajesh Kannan Megalingam, Iype P Joseph, Gautham P, parthasarathy R, Deepu K B, Mithun Muralidharan Nair, Amrita Vishwa Vidyapeetham”, Reconfigurable Cryptographic Processor for Multiple Crypto-AlgorithmsReconfigurable Cryptographic Processor for Multiple Crypto-Algorithms,january2011