International Journal of Engineering Research in Electronic and Communication Engineering (IJERECE) Vol 3, Issue 4, April 2016

Reconfigurable Hardware Design of Hybrid System with Compact Memory for Secured Communication

[1] Reshmi Krishna Prasad, [2] Asha A S
[1] PG Student [VLSI and ES] [2] Assistant professor,
Department of ECE, TKM Institute of Technology, Kollam
[1] reshmiideepak@gmail.com [2] ashaprasobh@gmail.com

***Abstract*— Cryptosystem is one of the most discussed areas in today's digital scenario. The increasing use of pervasive devices in the field of electronics has raised the concerns about security. In embedded applications, implementing a full-fledged cryptographic environment would not be practical because of the constraints like security, power dissipation, area and cost. Due to these constraints, the focus is on using lightweight cryptography that needs as less memory space as possible. The main criteria for the lightweight cipher are to have high security and less memory space. The lightweight cryptography is a biometric key generation algorithm with the combination of PRESENT algorithm with group instruction permutation. The developed lightweight algorithm is implemented with biometric system i.e. finger print scanning. This is used to ensure the high security to avoid fake, repeated voting etc. It also enhances the accuracy and speed of the process. The system utilizes the RFID card as an identification card for each voter. Each voter ID card contains a unique ID number with corresponding fingerprints stored in the database .The system uses thumb impression for voter identification since it is unique for each individual. Thus it would have an edge over the present day voting systems. The system confirm that the voting rights are accessed only by a legitimate user. In this, creation of a database consisting of unique ID number and thumb impressions of all the eligible voters in a constituency is done as a pre-poll procedure. During election, RFID card is used for initial authentication. Once the authentication succeeds, the thumb impression of the voter is entered as input to the system. This is then compared with the available records in the database. Access to cast a vote is granted if the particular pattern matches with anyone in the available record. In case the pattern does not match with the records of the database or in case of repetition, access to cast a vote is denied or the vote gets rejected and total vote count is done. The designing language is MATLAB, VHDL and embedded C. The code is synthesized and simulated using Xilinx ISE 13.2 and is implemented using FPGA and Microcontroller.**

***Index Terms*— Fingerprint, Lightweight cryptography, PRESENT, RFID**

I. INTRODUCTION

In embedded systems, data security plays the central role in the design. In communication networks, the data transmission security is a critical problem. A communication system is consistent when it provides high level of security. Normally, users exchange personal sensitive information or documents and it need security, integrity, authenticity and confidentiality of the exchanged data. Significant amount of data is exchanged every second over a non secured channel, which cannot be safe. Therefore, it is necessary to protect the data from attackers or hackers. To protect the data new biometric cryptography is used.

Embedded systems provide critical functions that could be disrupt by malignant parties. When the system sends or receives responsive or critical information using public networks or communications, there is possibility of potential attacks. It is necessary to provide central security functions such as data confidentiality, data integrity, and user authentication. Data confidentiality protects the information from undesired eavesdroppers. Data integrity assured as the data has not been changed illegitimately. User authentication confirms that the information is sent and received by appropriate parties rather than masqueraders. These basic security functions are required for many embedded systems used in voting, medical, sensing, automotive, financial and many other applications proper output port. Then VA will allocate the available

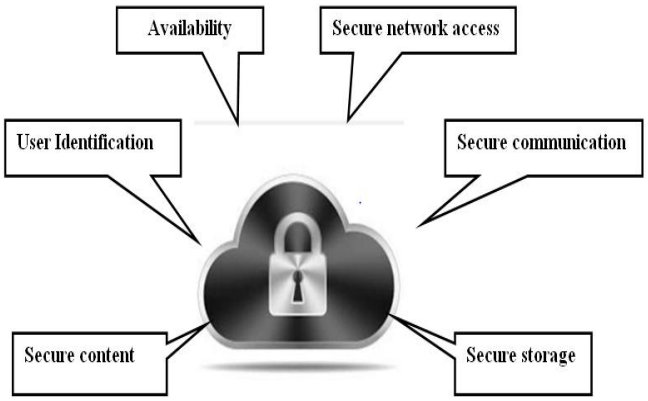


Fig.1. Embedded system requirements

The common security requirements of embedded systems from an end-user perspective is shown in Fig.1. Before few years, the major driver of the digital economy is PC. Recently, there has been a shift towards IT applications realized as embedded systems. The increasing use of pervasive devices in the field of electronics has raised the concerns about security. From low-end systems such as wireless handsets, networked sensors, and smart cards to high-end systems such as network routers, gateways, firewalls, and storage and web servers etc need to deal with security in one form or another. Technological advances that have spurred the development of the electronic systems have also ushered in seemingly parallel trends in the erudite of attacks. The technology of embedded system is fast improving and systems are becoming more and more advanced and very less attention is being given to its security. The main reasons behind this include the high sensitivity of costs, area and power dissipation. Due to these constraints, the focus is on using lightweight cryptography that needs as less memory space as possible. The main criterion for the lightweight cipher is to have less memory space and that which would result into a less Gate Equivalent (GEs) count without compromising the requirement of security. In response, the security solutions are being developed for providing robustness, protection from attacks, and recovery capabilities.

There are several requirements and challenges in the implementation of cryptographic systems. Mainly the performance of the algorithms is often crucial. Slow running cryptographic algorithms are translated into consumer dissatisfaction and inconvenience. Since traditionally, higher speeds were achieved through custom hardware devices, fast running encryption might mean high product costs. Guaranteeing security is a formidable challenge in addition to the performance requirements. A new biometric algorithm has been developed known as Lightweight cryptography. Algorithm is an interesting field that strikes the perfect balance in providing security, low-power consumption, higher throughput and compactness. Lightweight cryptography is a hybrid cryptosystem with key generation using an image and PRESENT algorithm with group instruction permutation. PRESENT algorithm is a form of SP (Substitution and Permutation) network has both the property Confusion and Diffusion.

The lightweight cryptographic algorithm is introduced in the biometric voting system. Here, the algorithm is implemented in the biometric system to ensure security using finger print scanning [1]. This is used to ensure the high security for avoiding avoid fake, repeated voting etc. It will also enhance the accuracy and speed of the process.

II. EXISTING TECHNIQUE FOR SECURED COMMUNICATION

Cryptography is a method that has been developed for transferring data securely. Cryptography now plays an increasingly important role in modern society, and it is essential to solve problems that involve secrecy, authentication, integrity, and dishonest entities. In digital communication, the information are sent through the wires or air and thus it is not from eavesdropping .Due to this, confidentiality of the transferring data is of extreme importance. Encryption is a process to transform the data to be sent to encrypted data using a key. The key is only known to the sender and receiver but the encryption process may not be confidential. The original data is obtained from decryption process. A modern information theory concept was first published by Claude Elmwood Shannon in 1948. The basic two basic types of encryption are symmetric and asymmetric encryption [5]. Data Encryption Standard (DES) [5] is the block cipher algorithm that takes a fixed length string of plain text bit and converts it through a series of sophisticated operations into another cipher text bit string of the same length. It is not highly secured due to Feistel Network and relatively slow operation. DES encryption is breakable through Brute Force attack. DES was succeed by AES. Advanced Encryption Standard (AES) is based on a design principle known as a substitution-permutation network. It is fast in both software and hardware. Like DES, AES does not use a Feistel network. AES has a key size of 128, 192, or 256 bit. The block size has a maximum of 256 bit but the key size has no theoretical maximum. AES is

secured but not suitable for embedded devices due to the high power consumption and larger footprint.

Lightweight Block Ciphers has been development due to resource-constrained and sensitive electronic and communication applications (and the advent of Internet of Things) [3].The lightweight block cipher has been used in many aspects of our lives, such as access control, parking management, identification, and goods tracking. The sensitivity of these applications makes lightweight cryptography necessary to reach acceptable confidentiality. It is necessary that every developer of lightweight cryptography has to cope-up with the trade-off between security, costs, and performance. The main criterion for the lightweight cipher is to have less memory space without compromising the requirement of strong security properties and that which would result into a less Gate Equivalent (GEs) count for an efficient hardware implementation. The design to be made with 1000–2000 gate equivalents (GEs) [3] for an ISO/IEC standard on lightweight cryptography out of that only 300–1800 GEs would be available for security aspects. In the past few years many algorithms have been designed and implemented in the field of pervasive computing. For security applications, total GEs available would be approx 2000–3000. These lightweight versions consume around 2200 GEs for encryption. Alternative to this approach of modifying an existing block cipher and to have an efficient hardware model, is an entirely new structure that has been designed called "PRESENT".PRESENT is a block cipher with Substitution Permutation network based on 80 bit or 128 bit key size and 64 bit block size. PRESENT [3] operates 31 rounds and its various variants need 2520 to 3010 GEs to provide adequate security levels. For ultra small applications with 1000 GEs, PRESENT [6] is also available. PRESENT is

Lightweight Algorithm	Block Size	Key Length	GEs
HIGHT	64	128	3048
mCrypton	64	64 96 128	2420 2681 3758
SEA	96	96	3758
TEA	64	128	2355
ICEBERG	64	128	7732
CLEFIA	128	128	2488
PRESENT	64	128	1884

Fig.2. Gate Equalent Count of Lightweighted Algorithm

The ISO/IEC standard for lightweight cryptography and one of the leanest lightweight algorithms design. To achieve less GEs, CLEFIA [9], [10] is one more compact algorithm developed by SONY but results in a higher memory requirement. Mostly block ciphers have been published like HIGHT [7], mCrypton [6], SEA [6], TEA [8] and ICEBERG [9] for small devices like RFID and these are summarized in Fig.2 with respect to their GEs.

The aim of this paper is to provide adequate security for applications like pervasive computing with compact cipher with The research work focused on a compact hardware implementation of the cipher. The idea of Electronic Voting Machines (EVMs) is introduced by the Chief Election Commissioner in 1977.The EVMs was formulate and designed by Election Commission of India in collaboration with Bharat Electronics Limited (BEL) and Electronics Corporation of India Limited ECIL. An EVM consists of two units, Control Unit and Balloting Unit. The two units are joined by a five-meter cable [2]. The main problem with EVM which is currently in use is security problems and illegal voting. Security problems mean one can tamper the results after the polling by changing the program installed in the EVM and. By replacing a small part of the machine with a look-a like component that can be silently instructed to steal a percentage of the votes in favor of a chosen candidate. Illegal Voting (Rigging) means the very commonly known problem and is faced in every electoral procedure. Normally, one candidate casts the votes of all the members or few amount of members in the electoral list illegally. The problem of rigging can be eradicated by giving a unique id to every user so that one person can cast his vote only once. That unique id is RFID card number and Fingerprint of each individual [2].

The rest of the paper is organized as follows. Section III describes the System architecture and section IV describes the hardware implementation. The result is described in section V and finally describes the conclusion of the project.

III. SYSTEM ARCHITECTURE

The aim of the project is to provide adequate security for the digital systems. The lightweight cryptography is a biometric algorithm combination of PRESENT algorithm with group instruction permutation. The developed algorithm is highly secure and need only less area when compared with Advanced Encryption Standard (AES). The biometric cryptographic algorithm is used to design an electronic voting machine by using the RFID card authentication and fingerprint identification method to eradicate defrauding of the manual voting system by multiple votes. The entire structure of the project is shown in the Fig.3. The project

consists of following modules:

- Fingerprint Enrollment
- Lightweight Encryption
- Parity Matrix Code Error Correction
- RFID Card Verification
- Fingerprint Authentication

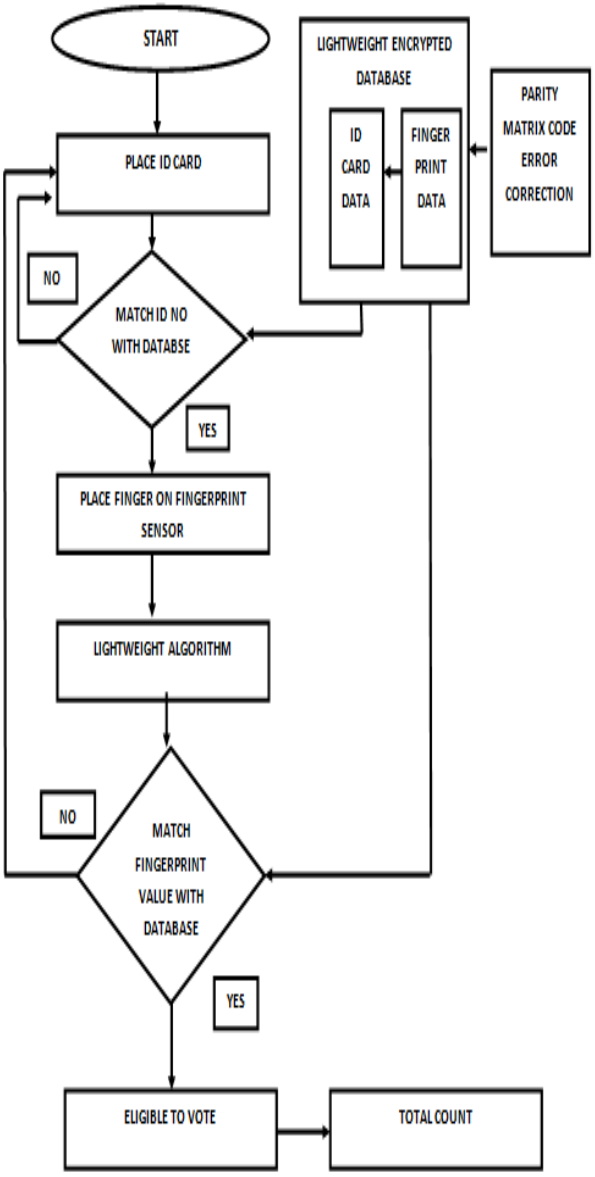


Fig.3. Project Flow

A. Fingerprint Enrollment

Biometrics is a process used to measure and analyze a person's unique characteristics. There are two types of biometrics namely behavioral and physical. Behavioral biometrics is commonly used for verification whereas physical biometrics is used for either identification or verification. Here fingerprint enrollment process is performed first and stored in the database. Enrollment refers to the process of capturing a fingerprint image, extracting relevant data, creating a data with user information, and storing the data to memory. Fig.4 shows the finger enrollment process to store the data in the database.

B. Lightweight Encryption Algorithm

Lightweight algorithm is a biometric cryptographic hybrid system with combination of PRESENT and key generation. The basic block diagram of the lightweight algorithm is shown in the Fig.5. To provide a high security and low cost, there is need to have a lightweight crypto algorithm whose coverage area would be less. PRESENT algorithm is ISO/IEC standardized. PRESENT is a substitution and permutation network with 64-bit iterated symmetric block cipher. PRESENT was designed to allow fast and compact implementation in hardware and software. The plain text bit is 128 and key has two variants, one with an 80-bit key and one with a 128-bit key. The plain text and key run in 31 rounds and each round has three layers, a substitution layer, a permutation layer and a key addition layer.

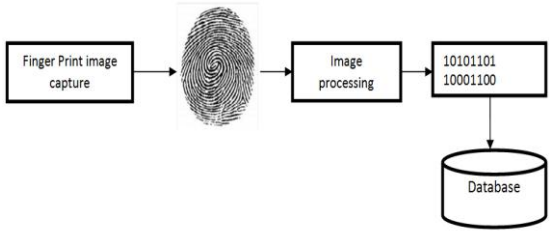


Fig.4. Fingerprint Enrollment Process

C. Substitution and Permutation:

The substitution layer comprises 30 S-boxes with 128 bit input and 128 bit output. Substitution operation used in PRESENT is given in the below Fig.6 and it shows the movement of bit S (i) to bit position P (i). In P-layer group instruction operation (GRP) is performed. GRP algorithm can generate different values from a given integer sequence. In

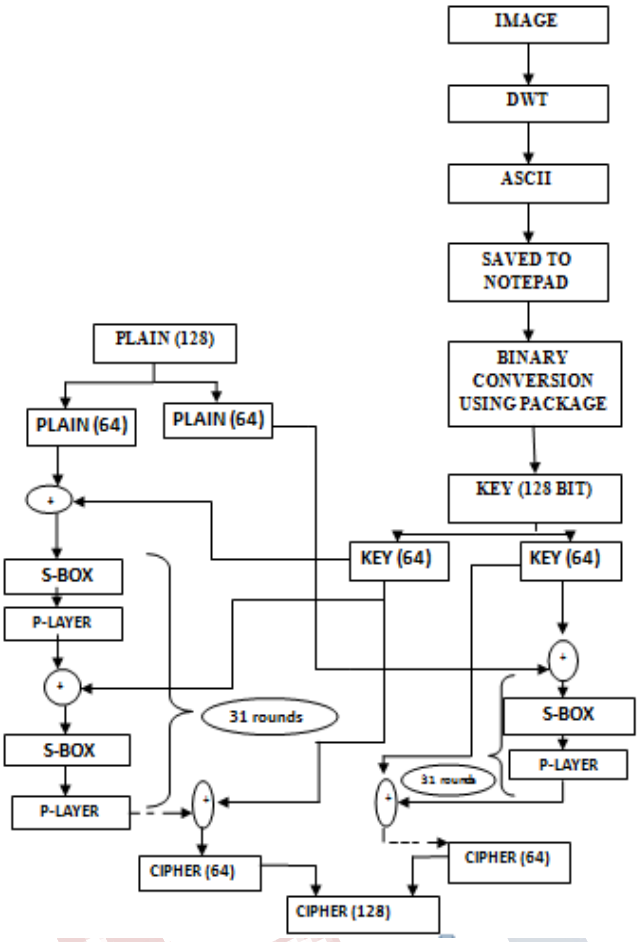


Fig.5. Lightweight Encryption Algorithm

S(i)	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
P(i)	0	16	32	48	1	17	33	49	2	18	34	50	3	19	35	51
S(i)	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
P(i)	4	20	36	52	5	21	37	53	6	22	38	54	7	23	39	55
S(i)	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
P(i)	8	24	40	56	9	25	41	57	10	26	42	58	11	27	43	59
S(i)	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
P(i)	12	28	44	60	13	29	45	61	14	30	46	62	15	31	47	63

Fig.6. Movement of bit S(i) to P(i)

This paper, 128 bit encryption is designed and P-layer operation is performed based on bit permutation instruction. Group instruction operation is a codeword's generation which is a universal design for n integers. The Fig. 7 shows the group instruction operation of a 8 bit in P-layer.

D. Key Generation:

The key generation is a process developed from an image .The block diagram of key generation is shown in the lightweight encryption Figure. In cryptography, key is a variable value that is applied to a string or block of unencrypted text to produce encrypted text or to decrypted text. Here key is generated from an image and DWT (Discrete Wavelet Transform) method is used to generate four images from a color image. Then randomly select any one of the image among the four and resize the image into required pixel value. Now the value generated is in binary ASCII format and written to the file in .txt format. The key generation is done in MATLABR2013a.

The 128 bit key generated from an image is divided into two 64 bit value. Similar way 128 bit plain text is divided into two 64 bit value. The 64 bit value of key is xored with the 64 bit value of plain text. The output is given to s-box and the substitution operation is performed. The output from s-box is given to the p-layer and group instruction operation is performed and the output is xored with another value of key which is stored in the key register. The process will continue for 31 rounds and cipher text with 128 bit is obtained.

E. Parity Matrix Code Error Correction

The parity matrix codes are block code with parity check matrices. It contains only very few number of non-zero entries. The H matrix guarantees both a decoding complexity and increases the linearity with the code length. The parity matrix codes are designed by creating a sparse parity-check

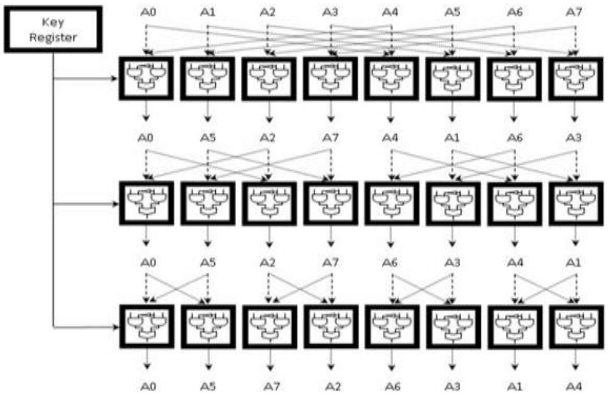


Fig.7. GRP operation of 8 bit in P-layer

Matrix initially and then determining a generator matrix for the code after that. The main difference between parity matrix codes and common block code is how they are decoded. For large block size, parity matrix codes are usually constructed by first studying the nature of decoders. Construction of specific parity matrix codes after this optimization are of two main types of techniques such as pseudo-random approaches for large block size, a random

construction that gives good decoding performance but complex encoders approach can be used to optimize the properties of small block size parity matrix codes. The main property of parity matrix codes depends on how they are to be applied. For a capacity approaching performance of low noise channel long code length or pseudo-random constructed irregular parity check matrices produces the performance closes to capacity. The important blocks of parity matrix codes are named as, variable node unit(VNU), check node unit(CNU) and sparse matrix. Sparse matrix includes the connections between VNUs and CNUs. The sparse matrix will be reduced and in such a manner that all the processes will be done in parallel. Input data sending will be divided into parts and is given to sparse matrix. Here every part will be processed in parallel. Thus total system complexity will be decreased. Here, parity matrix code is used for correcting the database value if any error occurs while fetching the data.

F. RFID Card Verification

The RFID card is a unique identification number which is used as the identification number of each voter, the information carried within the card is kept discrete and the data can only be manipulated during the initial set up procedure. RFID tag transmits the data to the RFID reader by throwing energy from the RFID reader's magnetic field. The advantage of RFID reader is that can detect a corresponding voltage drop across its antenna leads. So the tag can communicate binary information to the reader. Once the tag used for verification, it cannot be used by any other user.

E. Fingerprint Verification

Fingerprint identification is common biometric identification system because of the uniqueness & consistency over time. This is the operation of comparing a live fingerprint against the corresponding record stored during enrollment. The authentication result is returned based on whether the score was above a predefined threshold value. Fig.8 shows the authentication process. Once the matching is success the concern person is authenticated successfully. Based on the authentication total count is calculated.

IV. HARDWARE IMPLEMENTATION

The complete system can be considered as a package comprising of ATmega162 micro-controller, Spartan 3E FPGA, LCD, Fingerprint sensor R305, RFID card reader, keypad and RS 232. Working in group, these components provide the solution for the security problem of electronic voting system. The sections that follow the functionalities of the devices and describes how the system works together. Fig.9 shows the hardware implementation of the system.

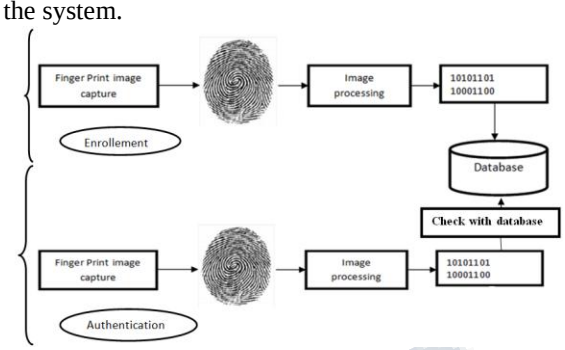


Fig.8. Fingerprint Authentication

A.RFID Card Reader

RFID is implemented to communicate information between a unique item and a system using radio waves. RFID system comprise of tags, RFID reader and at least one antenna. The tags are powered by electromagnetic induction through the RFID reader. Once the tag is powered, it responds by transmitting its unique information. In this project, five RFID tags have been used. Each and every tag contains the information related to individual voters. The individual information is stored in the microcontroller with respect to the fingerprint.When RFID tag shown to RFID reader, RFID reader activates the details of particular data of RFID tag which is pre loaded into micro controller memory. If that RFID tag information exist in the database of micro controller, then the person is eligible to fingerprint authentication. Else, our system goes to check next RFID Tag. In this way, entire authentication process goes on.

B. Fingerprint Sensor

Finger print sensor R305 module with TTL UART interface for direct communication. For identifying the person, the system can store the finger print data in the module and can configure in 1:1 or 1: N mode. The finger print module can directly interface with 3v or 5v microcontroller. Here, Finger print sensor is used for enrollment and authentication purpose. The user need to go for second stage authentication when RFID tag authentication success. A finger print of every human is unique. After first stage verification, user need to put the thumb on fingerprint scanner. During enrollment stage, the fingerprint value is stored in the database which is in encrypted form. The lightweight algorithm is used for encrypting the data to provide high security. Once the thump pressed on the scanner, the fingerprint value will be converted to encrypted form and then the matching process

is performed. The concern user is eligible to vote, if the particular fingerprint matches with the fingerprint already stored in the FPGA which act as database. The fingerprint sensor and RFID card reader works based on relay driver circuit.

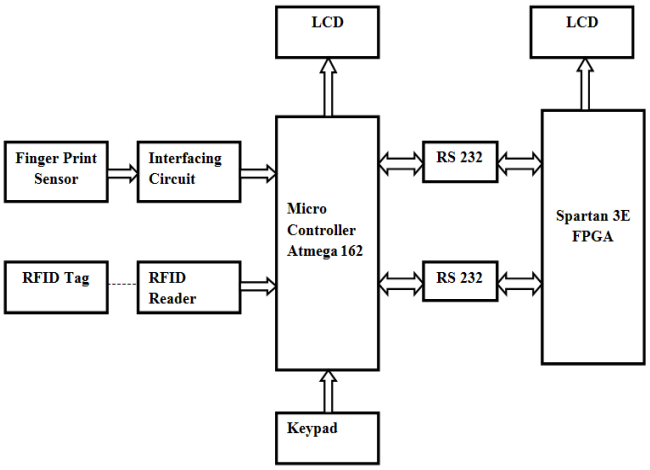


Fig.9. Hardware Implementation

C. AT mega 162 Microcontroller

ATmega162 is an extremely powerful and flexible microcontroller which controls the input and output devices of the project. ATmega162 has large instruction set with low power consumption and greater performance. When the RFID tag authentication is performed, proper message with success or failure is displayed using LCD. Once the process completed the finger print value is passed to the FPGA and the matching process is completed, the result is displayed again on LCD which is placed on the controller.

D. Spartan-3E FPGA

The Spartan 3E Field-Programmable Gate Arrays (FPGAs) is specifically designed to meet the needs of high volume, cost-sensitive consumer electronic applications. The fingerprint value is stored in FPGA in encrypted form. The cipher value at enrollment and authentication process is displayed on LCD which is placed on the FPGA.

E. LCD

Liquid Crystal Display (LCD) components are specialized for being used with the microcontroller and FPGA. LCD display is an output module which displays the respective messages based on the authentication.

F. RS 232

Serial Communication Interface is used for serial data transmission between controller and FPGA. The entire structure of hardware implementation is shown in Fig.10.

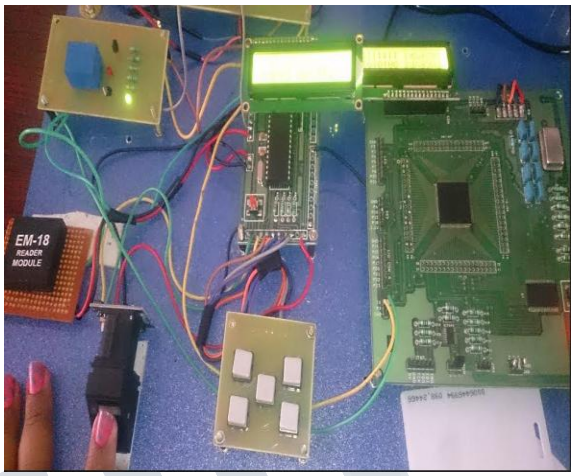


Fig.10. Implemented Hardware Block

V. EXPERIMENTAL RESULTS

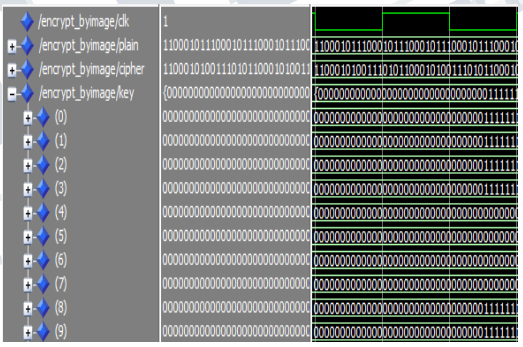


Fig.11. Simulation result of Lightweight Encryption

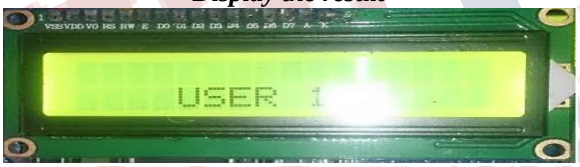
The modules are coded using embedded C and VHDL language and synthesized in Xilinx ISE 13.2 Design. In lightweight encryption algorithm, the plain text input and key generated from an image is xored and the obtained output is applied to a single s-box and shuffling operation is performed and the output from S-box is applied to P-layer and 7 stages operation is performed. The obtained output from P-layer is again xored with new key value which is stored in the key register and the output is obtained after 31 round processes. Fig.11 shows the simulation result of lightweight encryption algorithm.

Step 1
Enroll the User Finger

Step 2
Press the finger on the fingerprint scanner and displayed the result

Step 3
Show RFID card

Step4
Display the result



Step 5
Place your Finger

Step6
Failure Result

VI. CONCLUSION

The paper has presented the design and hardware implementation of voting system authentication which is based on RFID with fingerprint identification. The system ensures high security using Biometric Voting Method. The lightweight biometric algorithm is developed for high security. The system is perfectly convenient for almost all the voters. For physically handicapped, if we adopt face recognition based retinal scan method, we can solve the authentication problem up to 100%. The system is linked to database in order to avoid duplicate voting. The structure inter linked with three primary specifications namely enrollment, encryption and authentication. The problem of rigging can be eradicated by this system. The biometric algorithm can be used in many applications such as army, banking, medical etc.

REFERENCES

[1] Syed Mahmud Hasan, Arafa Mohd. Anis, Hamidur Rahman, Jennifer Sherry Alam, Sohel Islam Nabil, Md. Khalilur Rhaman, "Development of Electronic Voting Machine with the Inclusion of Near Field Communication ID Cards and Biometric Fingerprint Identifier," IEEE 17th Conf. on Computer and Information Technology, 22-23 December 2014.

[2] B. Madan Mohan Reddy, D. Srihari "RFID Based Biometric Voting Machine Linked To Aadhaar For Safe And Secure Voting" International Journal of Science, Engineering and Technology Research (IJSETR) Volume 4, Issue 4, April 2015.

[3] Gaurav Bansod, Nishchal Raval, Narayan Pisharoty " Implementation of a New Lightweight Encryption Design for Embedded Security" IEEE Trans. On Information Forensics and Security, vol. 10, no.1, January 2015.

[4] S.Sabeen, N. Bharathi Raja "Enhanced Memory Reliability Using Parity Matrix Code," International

Journal of Scientific & Engineering Research, Volume 5, Issue 4, April-2014.

[5] A. Juels and S. A. Weis, "Authenticating pervasing devices devices with human protocols," in Advances in Cryptology. Berlin Germany: Springer- Verlag, pp. 293-308, 2005.

[6] A . Bogdanov , " PRESENT- An ultra- lightweight block cipher," in Cryptographic Hardware and Embedded Systems (Lecture Notes in Computer Science), vol. 4727, Pp, 450- 466 Springer-Verlag, 2007.

[7] D. Hong, "HIGHT: A new block cipher suitable for low resource device," in Cryptographic Hardware and Embedded Systems (Lecture Notes in Computer Science), vol. 4249, l. Goubin and M. Matsui , Eds. Berlin, Germany : Springer- Verlag, pp 46- 59, 2006,.

[8] D. J. Wheeler and R. M Needham, " TEA, a tiny encryptin algorithm," in Fast Software Encryption, vol. 1008, Springer- Verlag 1994.

[9] F-X. Standaert, G. Rouvroy, Quisquater, and J-D. Legat, " ICEBERG: An involutional cipher efficient for block encryption in reconfigurable hardware," in Fast Software Encryption, B. Roy and W. Meier, Eds. Berlin Germany: Springer- Verlag, pp. 363- 366,2004.