Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 10, October 2014, pg.208 – 218

RESEARCH ARTICLE

PERFORMANCE ANALYSIS OF RECONFIGURABLE CRYPTO PROCESSOR FOR SECURITY AND PRIVACY IN COMMUNICATION NETWORKS

Mr. A.Kaleel Rahuman[1], Dr. G.Athisha[2]

[1,2] Department of Electronics and Communication Engineering
PSNA College of Engineering and Technology, Dindigul, TamilNadu, India
[1] kaleel23@gmail.com ; [2] gathisha@yahoo.com

Abstract— Recently, the number of electronic devices handling confidential information has increased. In these devices, encryption is applied to protect the confidential information. Therefore, technologies to incorporate cryptographic circuits into these cards have become important. In this work we wish to design the highly securable processor with less power consumption. Cryptographic transformations of AES, 3DES, RC5 are analysed based on the factors like, power consumption, memory usage, speed, number of input/outputs, memory usage. As a result, the algorithm with less power consumption and memory is implemented for designing low power, highly securable crypto processor. These algorithms are computationally intensive, consuming significant power. This paper presents these three algorithms with regard to VHDL and the FPGA. Xilinx software is used for simulation and optimization of the synthesizable VHDL code. Synthesizing and implementation (i.e. Translate, Map and Place and Route) of the code is carried out on Xilinx - Project Navigator, ISE 12.1 suite. All the transformations of both Encryption and Decryption are simulated using an iterative design approach in order to minimize the hardware consumption. Xilinx XC3S200 device of Spartan Family is used for hardware evaluation.

Keywords— Advanced Encryption Standard, Data Encryption Standard, Triple DES, Rivest cipher (RC), FPGA

I. INTRODUCTION

In past few years, wireless communications has been fast increasing with many devices like laptops, PDAs, and Pocket PCs. Individuals are using wireless technology for private communications, for mobile, E-commerce, emails and business interactions. Wireless networking resources have been started as initiatives towards a network of a future world without wires. Studies indicate that the growth of wireless networks is being restricted by their perceived in security [1]. The increasing of wireless systems provides malicious entities greater incentives to step up their efforts to gain unauthorized access to the information being exchanged over the wireless link.

Security is important for wireless networks, mainly because the communications signals are openly available as they propagate through the air. The amount of security required by the system may depend on the organization using the wireless network.

Important information such as account numbers is recorded on magnetic tapes on the back of credit and cash cards. Because magnetic tapes can be forged easily, integrated circuit (IC) chips (cryptographic circuits) have been used in recent years. Therefore, technologies to incorporate cryptographic circuits into these cards have become important. A financial company would require very strong security techniques to prevent unauthorized users and maintain information confidentiality. The hot-spots networks may require that only legitimate users access the network and may not require confidentiality and data integrity.

The study of the energy consumption of the encryption schemes in wireless devices are essential in design of energy efficient security protocols customized to the wireless environment. A key limitation in wireless devices is the battery capacity, while memory and processor technologies double with the introduction of every new semiconductor generation (roughly every 18 months) [3]; battery technology is increasing at the much slower rate of 5%-10% per year. This is causing a gap to form between the power required and the battery available.

Symmetric keys encryption or secret key encryption, only one key is used to encrypt and decrypt data. Strength of Symmetric key encryption depends on the size of key used. There are many examples of strong and weak keys of cryptography algorithms likeRC2, DES, 3DES, RC6, Blowfish, and AES. RC2 uses one 64-bit key .DES uses one 64-bits key. Triple DES (3DES) uses three 64-bits keys while AES uses various (128,192,256) bits keys. Blowfish uses various (32-448); default 128bits, while RC6 is used various (128,192,256) bits keys.

This paper examines a method for evaluating performance of selected symmetric encryption of various algorithms on the factors like, power consumption, memory usage, speed, number of input/outputs, and memory usage for wireless devices. A wireless device is limited in resources such as less memory, less processing power and limited power supply. Power is subjected to the problem of energy consumption due to encryption algorithms. Battery technology is increasing at slower rate than other technologies. We need a way to make decisions about energy consumption and security to reduce the consumption of battery powered devices. This study evaluates three different encryption algorithms used or suggested for wireless networks namely; AES, 3DES, and RC5.

II. RC5

Rivest Cipher 5 (RC5) encryption algorithm is a fast symmetric block cipher suitable for hardware or software implementations.RC5 has a variable word size, a variable number of rounds, and a variable length secret key. It consists of three components: a key expansion algorithm, an encryption algorithm and a decryption algorithm .The plaintext input to RC5 consists of two w bit words, which we denote, A and B. RC5 uses an expanded key table, S (0, 1…t-1) consisting of t =2(r+1) w bit words. The key expansion algorithm initializes S from the user's given secret key parameter K.

We assume that the input block is given in two w bit registers A and B. key expansion array is S (0, 1….T-1).

To encrypt:

$A=A+S_o$

$B=B+S_1$

For i=1 to r;

$A= ((A \oplus B)<<<B) +S_{21}$

$B= ((B \oplus A) <<<A) +S_{22}$

The output is the register's A and B.

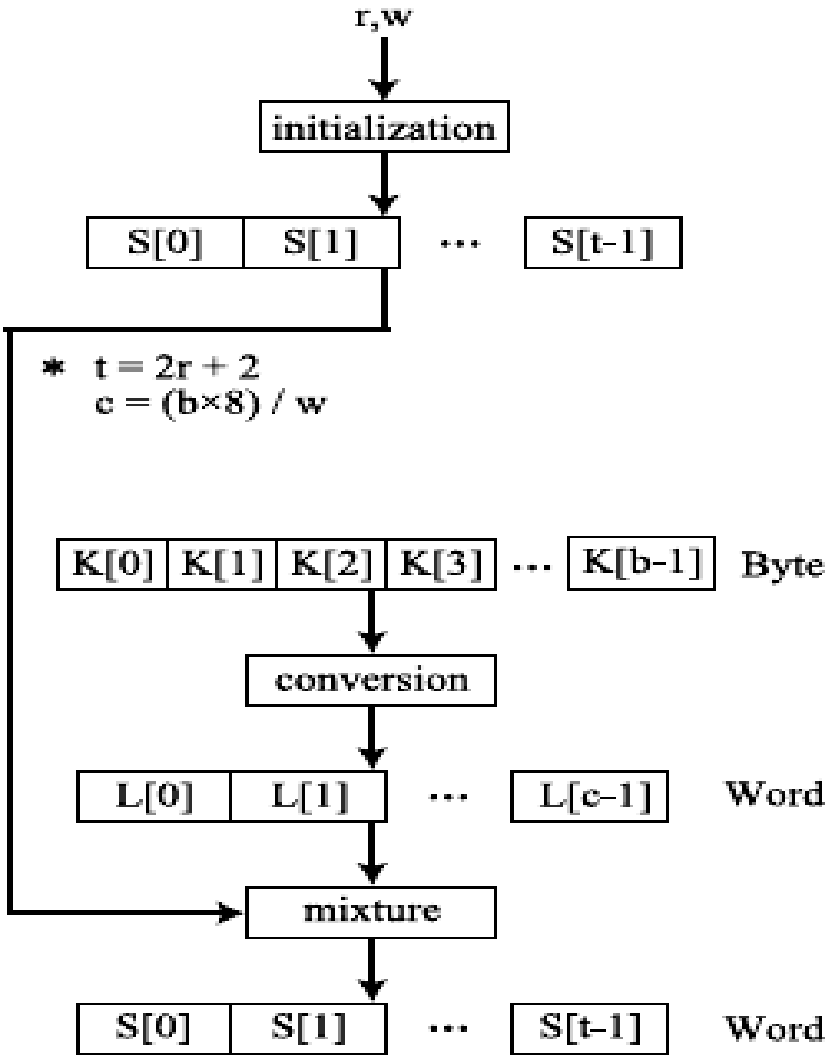


Figure 1.Generation of secondary key

To decrypt:

For i= r down to 1;

B= ((B-S22)>>>A)⊕A

A= ((A-S21)>>>B)⊕B

B=B-S1

A=A-S0

The symbol ">>>" is a right circular shift.

Sub-key generation: In this step, two constants P and Q are used. The array of sub-keys to be generated is called as S. The first sub-key S [O] is initialized with the value of P. Each next sub-key S[I], S[2] ... is calculated on the basis of the previous sub-key and the constant value Q, using the addition mod 2^32 operations. The process is done 2(r+l) - 1 times where r is the number of rounds. Here r= 12.So sub-keys S[O], S[1], ... S[25] are generated.

Sub-key mixing: In this stage, the sub-keys S[O],S[1] ... are mixed with the sub portions of the original key,i.e. L[O],L[I] ... L[c],where c is the last sub-key position in the original key..

A distinguishing feature of RC5 is its heavy use of data dependent rotations. The amount of rotation performed is dependent on the input data and is not predetermined. The encryption, decryption routines are very simple.

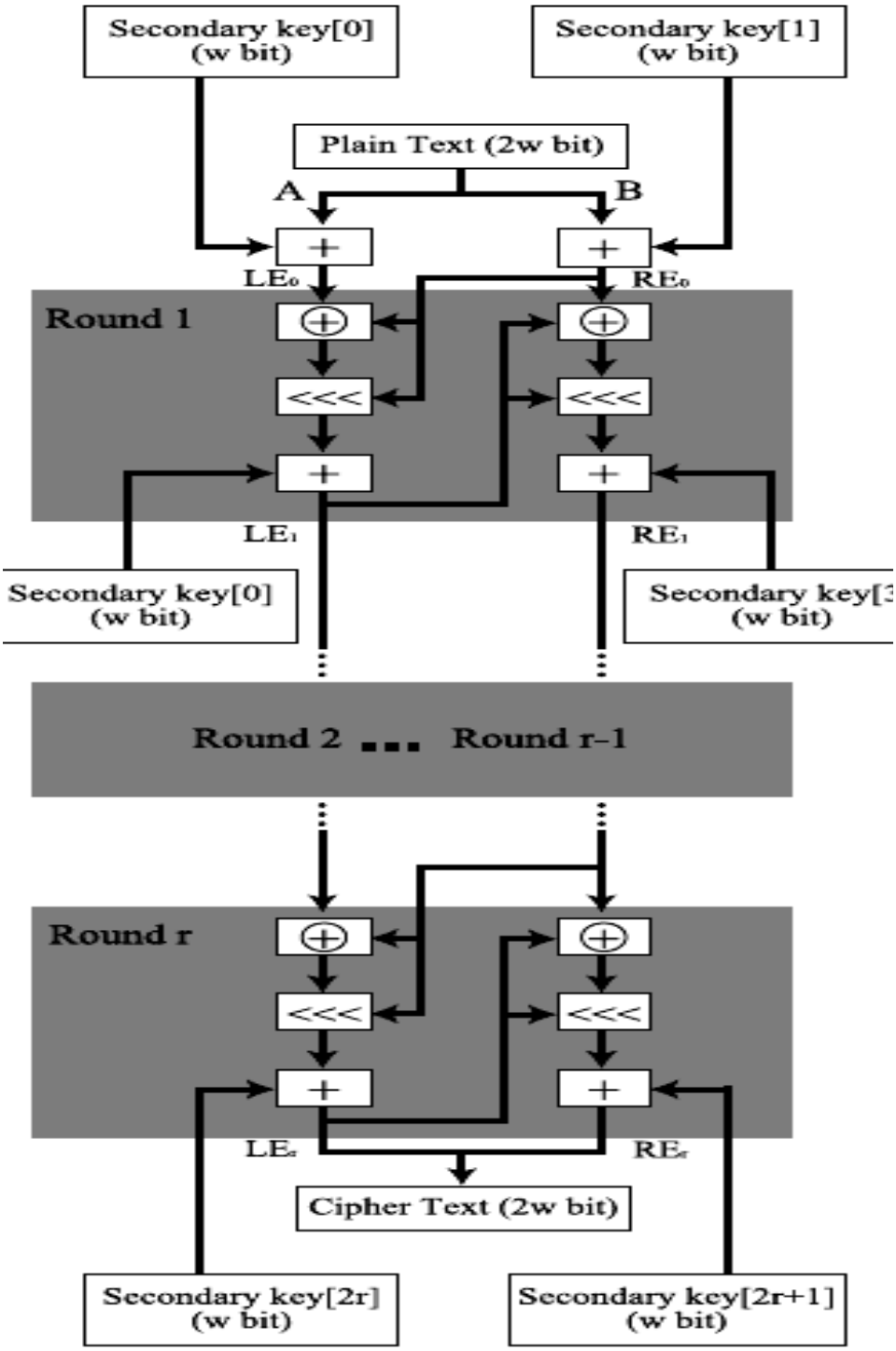


Figure 2. Encryption process of RC5

III.DES

Data Encryption Standard (DES) is a block cipher; it encrypts data in 64 bit blocks. DES is a symmetric algorithm; the same algorithm and key are used for both encryption and decryption. The key length is 56 bits.(the key is usually expressed as a 64 bit number, but every eighth bit is used for parity checking and is ignored. These parity bits are the LSB of the key bytes).they can be any 56 bit number and can be changed at any time. A handful numbers are considered weak keys, but they can easily be avoided. All security rests within the key.

This algorithm is a combination of two techniques of encryption, confusion and diffusion. DES has 16 rounds; it applies the same combination of techniques [6].

IV. AES

Advanced Encryption Standard (AES) is an encryption standard, based on a design principle known as a Substitution permutation network. It is fast in both software and hardware, is relatively easy to implement, and requires little memory. Unlike its predecessor, DES, AES does not use a Feistel network. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits.

1) Sub Byte Transformation - a nonlinear transformation applied to the elements of the matrix. This first step in each round is a simple substitution, when implemented as a Look up Table (LUT). It operates independently on each byte of state using S-box. The byte, s [i, j] become s'[i, j] through a defined substitution table.

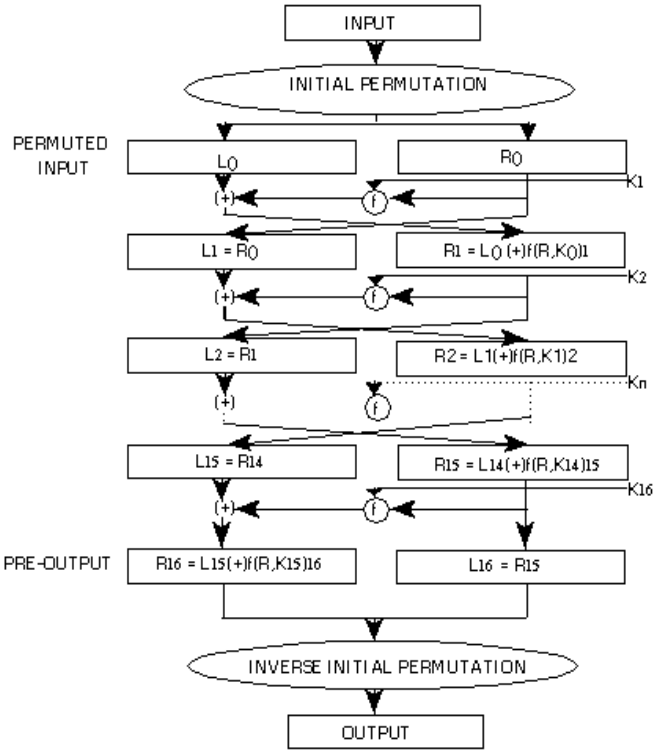


Figure 3. Outline of DES algorithm

2) Shift Rows Transformation - a cyclical shift operation with constant offsets, applied to the rows of the matrix. This second step in each round is permutation of rows by left circular shift; the first (leftmost, high order) i elements of row i are shifted around to the end (rightmost, low order).

3) Mix Columns Transformation - the third step is a resource intensive transformation on the columns of state under which the four elements of each column are multiplied by a polynomial, essentially diffusing each element of the column over all four elements of that column.

4) Add Round Key Transformation - performs modulo 2 (XOR) operations with the round key, which is obtained from the initial key by a key expansion procedure. The encryption flow starts with the addition of the initial key to the plaintext. Then the iteration continues for (Nr - 1) rounds (Nr being the total number of rounds). In last round the Mix Column step is bypassed.

V. PROPOSED ALGORITHM

In order to realize high-speed processing and area reduction, this study introduces arithmetic processes suitable for hardware during encryption and decryption. First, a shift process used for encryption is replaced by a bit selection process. Because of this substitution, the shift process can be realized in wiring. The mixture process usually requires t x 3 = 78calculations. The proposed architecture divides the processing by inserting a register between calculations and introducing a loop process, which reduce the required calculations to 26.Dividing the processing of each round enables high speed processing. As Fig. 2 shows, RC5's round processing enciphers a 64-bit plaintext. The results are shown in table 1 and table 2 However, the actual

processing is performed every 32 bits. Therefore, the round is divided into the left and right parts to perform left and right processing with two clock signals, which raises the operating frequency and improves latency.

Table 1.Normal method of RC5 algorithm

	Used	Available	Utilization
No of slices	[N/A]	4800	[N/A]
No of LUTs	16300	19200	85%
No of FF's	554	19200	2%

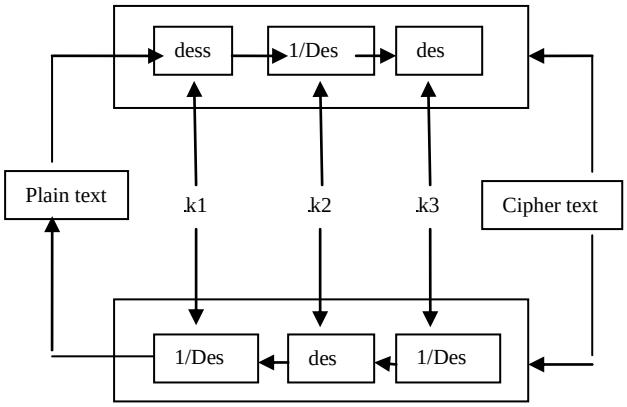
Table 2. Proposed method of RC5 algorithm

Resources	Used	Available	Utilization
No of slices	2488	4800	51%
No of LUTs	8893	19200	46%
No of FFs	2281	19200	11%

DES is the most widely used symmetric algorithm in the world, despite claims that the key length is too short. Ever since DES was first announced, controversy has raged about whether 56 bits is long enough to guarantee security. The key length argument goes like this. Assuming that the only feasible attack on DES is to try each key in turn until the right one is found, then 1,000,000 machines each capable of testing 1,000,000 keys per second would find (on average) one key every 12 hours. Most reasonable people might find this rather comforting and a good measure of the strength of the algorithm. Those who consider the exhaustive key-search attack to be a real possibility (and to be fair the technology to do such a search is becoming a reality) can overcome the problem by using double or triple length keys.

Use of multiple length keys leads us to the Triple-DES algorithm, in which DES is applied three times. Triple DES is simply another mode of DES operation. It takes three 64-bit keys, for an overall key length of 192 bits. In Private Encryption, you simply type in the entire 192-bit (24 character) key rather than entering each of the three keys individually. The Triple DES DLL then breaks the user provided key into three sub keys, padding the keys if necessary so they are each 64 bits long. The procedure for encryption is exactly the same as regular DES, but it is repeated three times. Hence the name Triple DES, The data is encrypted with the first key, decrypted with the second key, and finally encrypted again with the third key. Triple DES, also known as 3DES. Consequently, Triple DES runs three times slower than standard DES, but is much more secure if used properly. The procedure for decrypting something is the same as the procedure for encryption, except it is executed in reverse.

ENCIPHERING



DECIPHERING

Figure 4. Block Diagram of TDES

If we consider a triple length key to consist of three 56-bit keys K1, K2, K3 then encryption is as follows:
•Encrypt with K1
•Decrypt with K2
•Encrypt with K

Decryption is the reverse process:
•Decrypt with K3
•Encrypt with K2
•Decrypt with K1

Setting K3 equal to K1 in these processes gives us a double length key K1, K2. Setting K1, K2 andK3 all equal to K has the same effect as using a single-length (56-bit key). Thus it is possible for a system using triple-DES to be compatible with a system using single-DES. DES operates on a 64 – bit block of plain text [3]. After an initial permutation the block is broken into a right half and left half, each 32 – bits long. Then there are 16 rounds of identical operations, called Function f, in which the data are combined with the key. After the sixteenth round, the right and left halves are joined, and a final permutation (the inverse of the initial permutation) finishes off the algorithm. DES operates on a 64 – bit block of plaintext. After an initial permutation the block is broken into a right half and left half, each 32 – bits long. Then there are 16 rounds of identical operations, called Function f, in which the data are combined with the key. After the sixteenth round, the right and left halves are joined, and a final permutation (the inverse of the initial permutation) finishes off the algorithm. In each the key bits are shifted, and then 48 – bits are selected from round the 56 –bits of the key. The right half of the data is expanded to 48 – bits via an expansion permutation, combined with 48 –bits of a shifted and permuted key via an XOR, sent through 8 S- boxes producing 32- new bits, and permuted again.

Like DES, data is encrypted and decrypted in 64-bit chunks. Unfortunately, there are some weak keys that one should be aware of: if all three keys, the first and second keys, or the second and third keys are the same, then the encryption procedure is essentially the same as standard DES. This situation is to be avoided because it is the same as using a really slow version of regular DES [4]. Note that although the input key for DES is 64 bits long, the actual key used by DES is only 56 bits in length. The least significant (right-most) bit in each byte is a parity bit, and should be set so that there are always an odd number of 1s in every byte. These parity bits are ignored, so only the seven most significant bits of each byte are used, resulting in a key length of 56 bits. This means that the effective key strength for Triple DES is actually 168 bits because each of the three keys contains 8 parity bits that are not used during the encryption process.

The basic architecture unrolls only one full cipher round, and iteratively loops data through this round until the entire encryption or decryption transformation is completed. Only one block of data is processed at a time making it equally suited for feedback and non-feedback modes of operation. The proposed architecture achieves good performance and occupies less area than previously reported designs. This compact design was developed by thorough examination of each of the component of the AES algorithm and matching them into the architecture of the FPGA. The demonstrated implementation fits in a very inexpensive, off-the-shelf Xilinx Spartan 3 XC3S120 FPGA, which cost starts below $10 per unit. Only 50% of the logic resources available in this device were utilized, leaving enough area for additional glue logic. This implementation can encrypt and decrypt data streams up to 166 Mbps. The encryption speed, functionality, and cost make this solution perfectly practical in the world of embedded systems and wireless communication

Table 3.TDES simulation results

Device	Area		Max.clock freq[MHz]	Throughput[Mbps]
	CLB slices	Block RAMs		
Existing implementation [XC2S100]	200	3	60	138
Proposed implementation [XC3S120]	150	3	50	120

Table 4.combined implementation results

ATTRIBUTE	RC5	TDES	AES
Freq of operation	140MHz	100MHz	300MHz
No of slices	180	155	75
speed	7.25 ns	9 ns	5 ns
No of FFs	123	158	334
No of input outputs	230.	354	540

VI. VLSI IMPLEMENTATION AND SIMULATION RESULTS

The goal for this design was to create a low-cost implementation of AES, TDES, RC5 in the FPGA targeted for real life applications. Much of the previous research targets state-of-the-art technologies forgetting that the individual cost of those devices ranges in hundreds of US dollars. We shifted our attention to older technologies and smaller devices. Xilinx. produces two low-cost families of devices called Spartan II, and Spartan III.

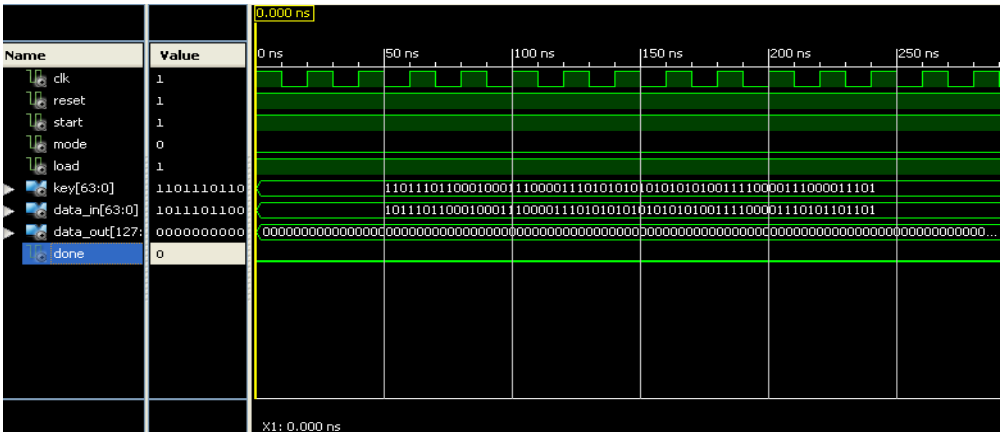


Figure 5.RC5 ENCRYPTION

Figure 5. represents the waveforms generated by the 64-bit encryption process. The inputs are clock of 240ns time period, Active High reset, and 64-bit state as a standard logic vector.

Encryption Process (Cipher):
AES block length/Plane Text = 64bits
Plane Text: 00112233445566778899aabbccddeeff
Key: 000102030405060708090a0b0c0d0e0f
Output/Cipher Text: 69c4e0d86a7b0430d8cdb78070b4c55a

Decryption Process (Inverse Cipher):
AES block length/Cipher Text = 64bits
Input /Cipher Text: 69c4e0d86a7b0430d8cdb78070b4c55a
Key: 000102030405060708090a0b0c0d0e0f
Output/Plain Text: 00112233445566778899aabbccddeeff

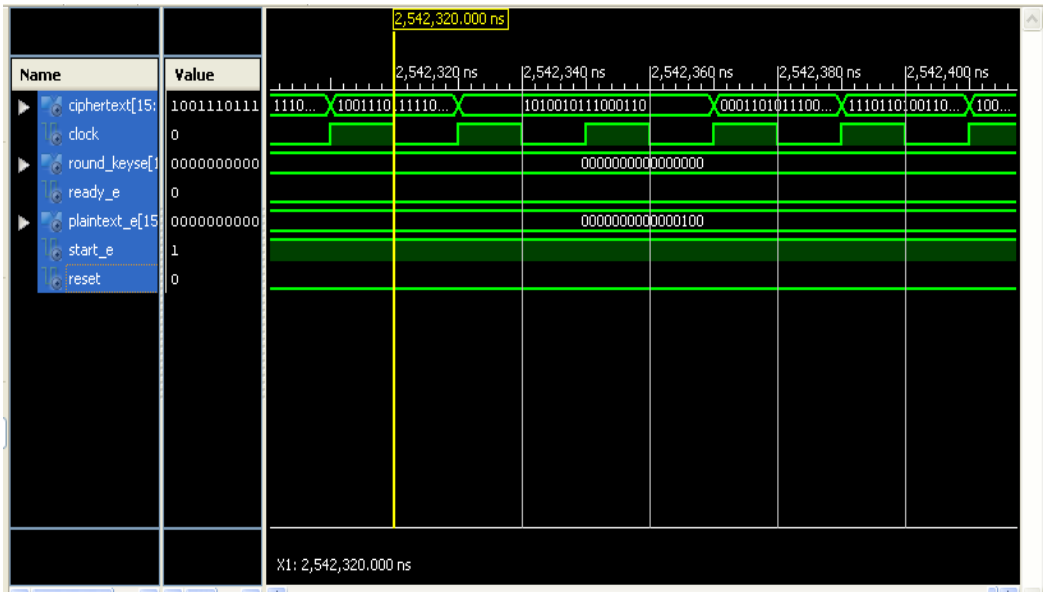


Figure 6. RC5 Decryption

The parameter that compares RC5 from the point of view of their hardware efficiency is Throughput. Encryption/Decryption Throughput = block size frequency/total clock cycles. Thus,
Throughput = 128 x140 MHz/51 = 352Mbits/sec.
Total number of clock cycles=51

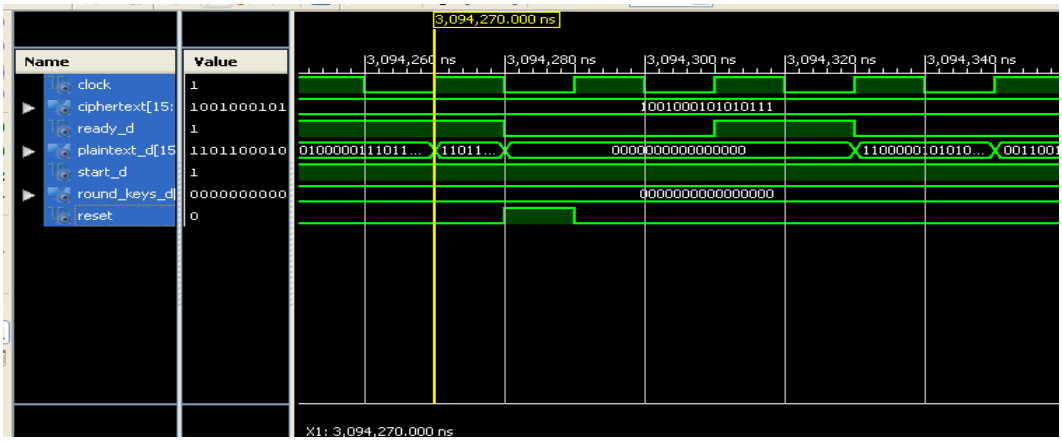


Figure 7.TDES Encryption

As DES will run through 16 iterations to achieve its desired cipher text (final output).With Triple DES, it will Encrypt-Decrypt-Encrypt the block and a completely different output is generated with a final combination. It's said that the security is 192 bit encryption, but also argued that regardless of the keys, the security is only 168 bit.

The FPGA family delivers high-performance, high-capacity programmable logic solutions. Dramatic increases in silicon efficiency result from optimizing the new architecture for place-and-route efficiency and exploiting an aggressive 5 layer-metal 0.22 µm CMOS process. These advances make Virtex FPGAs powerful and flexible alternatives to mask-programmed gate arrays. The Xilinx XC3S120 is chosen as target device for the implementation of TDES.

Table5. Device utilization summary of TDES Encryption

Allocated area	Used/available	Utilization in %
CLB slices	2943/33972	8
No. of LUTs	5802/67584	8
IOs	836	-
IOBs	384/684	56

FPGA device used: SPATRAN 3E XC3S120E

The proposed design is compared with other different design implementation in Xilinx FPGA device. The proposed device is implemented in XC3S120E to have sufficient memory to implement the entire three different rijndael algorithms. The maximum core frequency is 100 MHz Each round are completed in one clock cycle and one clock cycle for registering the input, so total clock cycle need for processing 128-bit data is 12 clocks. As a result 833.3 Mbps of throughput is achieved.

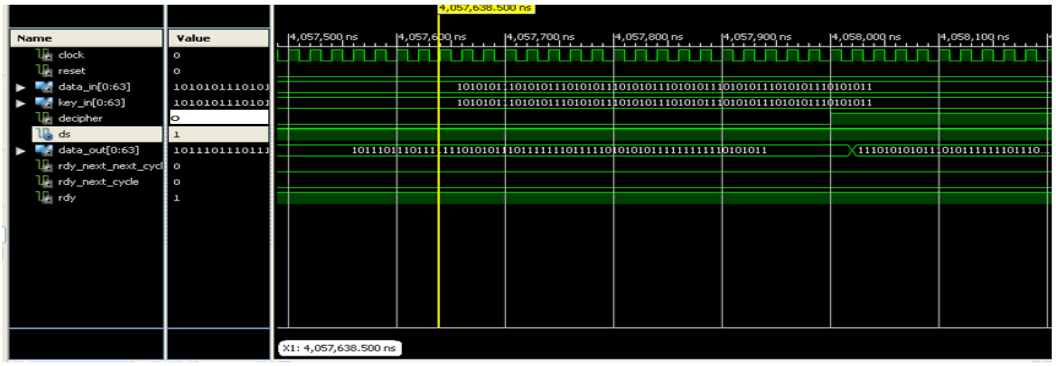


Figure 8.TDES Decryption

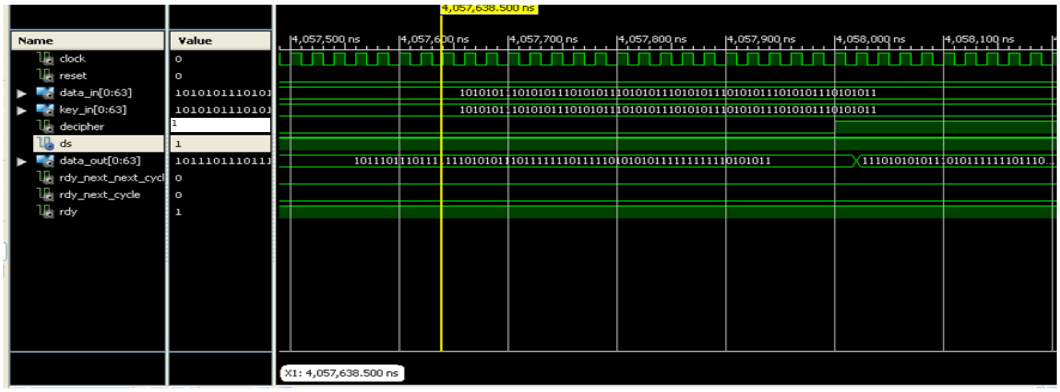


Figure 9.AES Integrated Output

AES encryption is an efficient scheme for both hardware and software implementation. As compare to software implementation, hardware implementation provides greater physical security and higher speed. Hardware implementation is useful in wireless security like military communication and mobile telephony where there is a greater emphasis on the speed of communication.

Minimum period: 13.038ns (Maximum Frequency: 76.699MHz) Maximum combinational path delay: 7.790ns. Minimum input arrival time before clock: 6.933ns. Max output required time after clock: 6.611ns. Encryption/Decryption Throughput = block size frequency/total clock cycles. Thus, 986.33MBits/sec.

The results shows that the hardware implementation of AES Algorithm is no doubt faster than the software implemented AES algorithm.

VII. CONCLUSIONS

In this paper the feasibility of creating a very compact, low-cost FPGA implementation of the AES was examined. The proposed folded architecture achieves good performance and occupies less area than previously reported designs. This compact design was developed by thorough examination of each of the components of the AES algorithm and matching them into the architecture of the FPGA. As DES will run

through 16 iterations to achieve its desired cipher text (final output).With Triple DES, it will Encrypt-Decrypt-Encrypt the block and a completely different output is generated with a final combination. It's said that the security is 192 bit encryption, but also argued that regardless of the keys, the security is only 168 bit. This debate is clearly beyond the scope of this article/writer. It's a safe but that Triple DES is exponentially stronger than the previous DES. After that, AES may supplant Triple DES as the default algorithm on most systems if it lives up to its expectations. But Triple DES will be kept around for compatibility reasons for many years after that. So the useful lifetime of Triple DES is far from over, even with the AES near completion.

For the foreseeable future Triple DES is an excellent and reliable choice for the security needs of highly sensitive information. The AES will be at least as strong as Triple DES and probably much faster. It's the industry mandate from Visa and MasterCard that's requiring ATM deployers to upgrade and/or replace their legacy terminals. In a nutshell, it's all lab out three waves of encryption, and it's designed to make ATM transactions more secure.

In this paper, we have presented a high performance parity based concurrent fault detection scheme for the AES using the S-box and the inverse S-box in composite fields. Using exhaustive searches, we have found the least complexity S-boxes and inverse S-boxes as well as their fault detection circuits. Our error simulation results show that very high error cover ages for the presented scheme are obtained. Moreover, a number of fault detection schemes from the literature have been implemented on ASIC and FPGA and compared with the ones presented here. Our implementations show that the optimum S-boxes and the inverse S-boxes using normal basis are more compact than the ones using polynomial basis. However, the ones using polynomial basis result in the fastest implementations. We have also implemented the AES encryption using the proposed fault detection scheme. The results of the ASIC and FPGA mapping show that the costs of the presented scheme are reasonable with acceptable post place and route delays.

REFERENCES

[1] Rajesh Kannan mega lingam, Gayathiri gopa Kumar," A VLSI implementation and analysis of cryptographic algorithms for security and privacy in communication networks", International conference on mechanical and electrical technology (ICMET) 2010.

[2] Brown.B (2003), "802.11: the security differences between b and i," "Potentials, IEEE Volume 22, Issue 4, pp23-27.

[3] Bruce.S. (2008) The Blowfish Encryption Algorithm available http://www.schneier.com/blowfish.html

[4] Daemen.J, and Rijmen.V (2001). "Rijndael: The Advanced Encryption Standard."D r.Dobb's Journal, PP. 137-139.

[5] El-Fishawy.N (2007)," Quality of Encryption Measurement of Bitmap Images with RC6, MRC6, and Rijndael's Block Cipher Algorithms", International Journal of Network Security, PP.241–251.

[6] Ruangchaijatupon.P, Krishnamurthy.P (2001), "Encryption and Power Consumption in Wireless LANs-N,'' The Third IEEE Workshop on Wireless LANs - Newton, Massachusetts.

[7] Shih.E, Cho.S, Ickes.N, Min.R, Sinha.A,Wang.A, and Chandrakasan.A(2001),"Physical layer driven protocol and algorithm design for energy-efficient wireless sensor networks," in Proceedings of The 7th ACM Annual International Conference on Mobile Computing and Networking (MobiCom),Rome, Italy,pp.272-287.

[8] Sinha.A and Chandrakasan.A.P(2001),"Joule Track A Web Based Tool for Software Energy Profiling," in the Proceedings of the 38th Design Automation Conference, Las Vegas, NV, USA, pp.220-225.

[9] Karygiannis.T and Owens.L (2002),"Wireless Network Security: 802.11, Bluetooth and Handheld Devices," special Publication 800-48.

[10] Federal Information Processing Standards Publication 140-1, "Security Requirements for Cryptographic Modules", U.S. Department of Commerce/NIST, Springfield, VA: NIST, 1994

[11] Kempf.J (2008),"Wireless Internet Security: Architecture and Protocols," CAMBRIDGE University Press.

[12] Lahiri.K, Raghunathan.A, Dey.S, and Panigrahi .D(2002), "Battery driven system design," a new frontier in low power design.

[13] NIST Special Publications 800-20, "Modes of Operation Validation System for the Triple Data Encryption Algorithm", National Institute of Standard and Technology, 2000.

[14] William stallings, cryptography and network security principles and practices.

[15] Dougles L Perry, VHDL Programming by example.

