International Journal of Advanced Multidisciplinary Research
ISSN: 2393-8870
www.ijarm.com
DOI: 10.22192/ijamr
Volume 5, Issue 11 -2018

Research Article
DOI: http://dx.doi.org/10.22192/ijamr.2018.05.11.012

Block Cipher Midori Encryption and Decryption with Fault Detection Technique

Dr. R. Venkadesh, Dr. A. V. Prathap kumar, K.Yoganand
Dhanalakshmi Srinivasan Engineering College, Perambalur

Keywords

Light weight cryptography; AES; block cipher midori; fault detection; Interleaved parity generation;

Abstract

To design short-term security based applications, there is an essential need of high-performance, low cost and area-efficient VLSI implementation of lightweight ciphers. Achieving secure high-performance implementations for constrained applications such as implantable and wearable medical devices are a priority in efficient block ciphers. However, security of these algorithms is not guaranteed in the presence of malicious and natural faults. The use of appropriate fault detection schemes for the encryption /decryption makes it robust to internal defects and fault attacks. A new lightweight block cipher Midori, has been proposed that optimizes the energy consumption besides having low latency and hardware complexity. In block cipher Midorian interleaved parity generation scheme for fault detection of and detection is introduced. By using this technique we can detect multi bit errors.

I. Introduction

With the introduction of the computer, the need of automated tools for protecting files and other information stored on the computer became mandatory. The major change that affected security is the introduction of distributed systems and the use of networks and communications facilities for carrying data between terminal user and computer. Encryption is fundamental to computer security.

A. Cryptography

Cryptography is a science that applies complex mathematics and logic to design strong encryption methods. When a message is sent using cryptography, it is changed (or encrypted) before it is sent. The method of changing text is called a "code" or, more precisely, a "cipher". The changed text is called "cipher text". The change makes the message hard to read. Someone who wants to read it must change it back (or decrypt it). A key is a piece of information (a parameter) that determines the functional output of a cryptographic algorithm. Cryptography is used to achieve the following goals: *Confidentiality ,Data integrity, Authentication.*

B. Lighweight Cryptography

Lightweight cryptography plays an essential role for achieving high security with low area and low energy consumption in many sensitive applications such as secure embedded systems, wireless Nano sensors, radio-frequency identification (RFID) tags, and implantable and wearable medical devices. Recently, a new lightweight block cipher, Midori, has been proposed that optimizes the energy consumption besides having low latency and hardware complexity. Midori provides acceptable security level with optimal energy consumption .

C. Need for fault detection

A unique characteristic of th cryptographic circuits is their very high sensitivity to faults. Even a single data bit fault in an encryption or decryption circuit will, in most cases, spread quickly and result in a totally scrambled output (an almost random pattern). There is, therefore, a need to prevent such faults.The existing system is advanced encryption standard(AES). The fault detection scheme used in aes is parity checking. Here Interleaved parity generation scheme is used to detect faults. By using this scheme, it is possible to to detect multi bit errors in the data. But it is not possible with the parity check.

II. Preliminaries

A . AES

The Advanced Encryption Standard, or AES, is a symmetric block cipher chosen by the U.S. government to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits.

B . AES algorithm

1. *Key Expansions*—round keys are derived from the cipher key using Rijndael'skey schedule. AES requires a separate 128-bit round key block for each round plus one more.

2. Initial Round

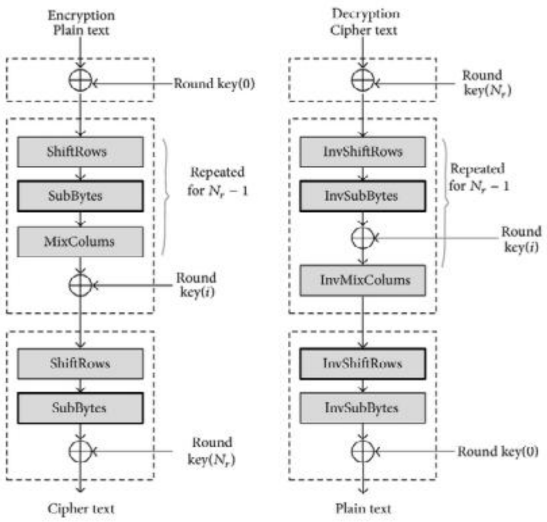


Fig1: AES structure

AddRoundKey—each byte of the state is combined with a block of the round key using bitwise xor.

3. Rounds

- Sub Bytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
- Shift Rows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
- MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.

4. Final Round (no MixColumns).

D . AES fault detection

The faults that accidently or maliciously occur in the hardware implementations of the Advanced Encryption Standard (AES) may cause erroneous encrypted/decrypted output. The use of appropriate fault detection schemes for the AES makes it robust to internal defects and fault attacks. In AES fault detection is done by parity check as shown below.

Consider a **Message - 1011**

the parity check is shown below

1 EXOR 0 = 1 1 EXOR 1 = 0 0 EXOR 1 = 1

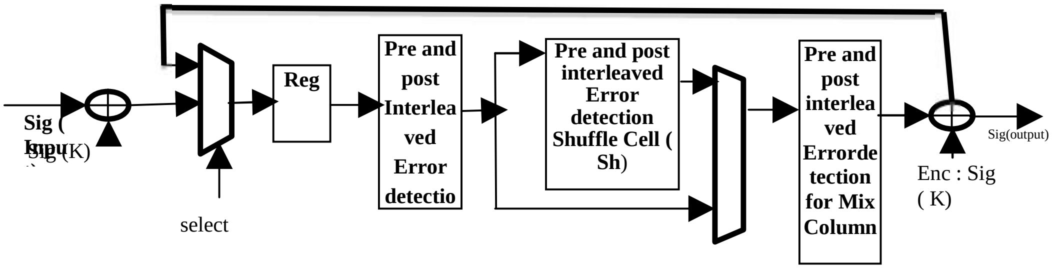
and the parity check for the **Corrupted message – 1101** is

1 EXOR 1 = 0 0 EXOR 0 = 0 0 EXOR 1 = 1

Here the two outputs are same,cannot detect the multi bit errors in AES.

III. Block cipher midori and proposed error detection scheme

proposed system is block cipher Midori .it is a symmetric key cipher which occupies less area and also consumes less power.Midori consists of two parts, i.e., data processing and key scheduling modules. The plaintext input and the cipher text output, which are 64 bits or 128 bits in width, are divided into 4-bit and 8-bit cells, respectively. Two variants of Midori, Midori64 and Midori128, are a 64-bit block cipher and a 128-bit block cipher with the same key length of 128 bits corresponding to 16 and 20 number of rounds, respectively. Block cipher midori block digram shown below:


Sig (Input
Sig (K)
select
Reg
Pre and post Interleaved Error detectio
Pre and post interleaved Error detection Shuffle Cell (Sh)
Pre and post interleaved Errordetection for Mix Column
Enc : Sig (K)
Sig(output)

The input is a single 128 bit block both for decryption and encryption and is known as the in matrix. This block is copied into a state array which is modified at each stage of the algorithm and then copied to an output matrix. A plain text is combined with the secret key as the input to the multiplexer. Input and key are combined by exor operation.A feedback signal is also given as the input to the mux. The time delay between two signals are reduced by mux.it is known as block compensation. The output of the mux is stored in a register temporarily.

A .inner workings of a round

The algorithm begins with an add round key stage followed by 9 rounds of four stages and a tenth round of three stages. This applies for both encryption and decryption with the exception that each stage of a round the decryption algorithm is the inverse of its counterpart in the encryption algorithm.

The four stages are as follows: Substitute bytes, Shift rows , Mix columns, Add round key.

B. Fault detection scheme for block cipher midori

In our proposed system Interleaved parity generation is used forfault detection. It also helps to reduces transport error. It is method of error monitoring and in each block error is detected.

C. Interleaved parity generation

This scheme is used to detect multibit errors. A Simple example showing the operation of interleaved parity generation scheme is shown below:

Consider a message 1011. Then divide the total bits in message into two as shown below

Even parity – 11 and Odd parity – 01

Then do parity checking as shown below

1 EXOR 1 - 0 0 EXOR 1 –1

Now consider the Corrupted message be1101. Then divide message bits into two.

Odd parity - 10and even parity – 10 and the corresponding parity check is

EXOR 1 – 1 1 EXOR 1 – 0

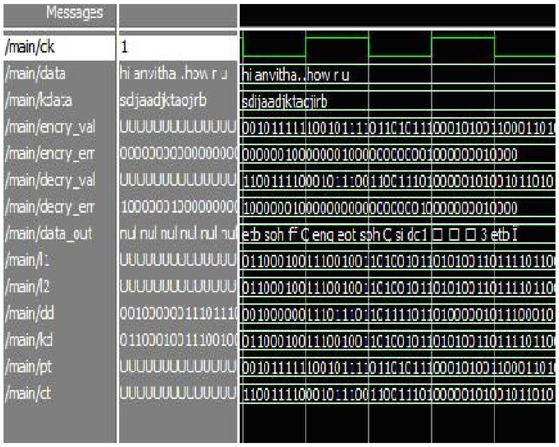
Here the Outputs of the parity check are different.so error is detected.

D . Advantages

- It can able to detect multiple bit errors
- Less faults in encrypted cipher text data
- Reduce the hardware complexity
- Improve the secuirity and accuracy level

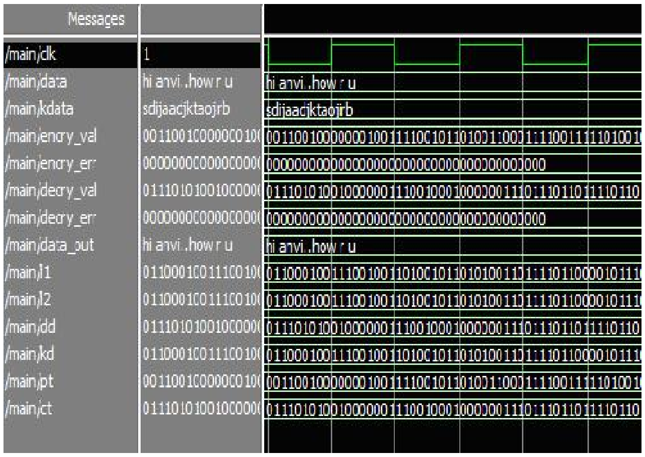
IV . Experimental Result

Encryption and decryption output:



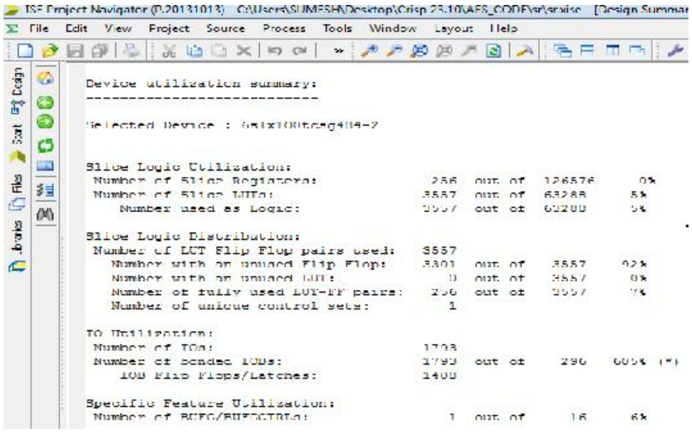
```
Messages
/main/ck          1                   
/main/data        hi anvitha .how r u    hi anvitha..how r u
/main/kdata       sdjaadjktaojrb         sdijaadjktaqjirb
/main/encry_val   UUUUUUUUUUUUUU      0010111111001011110110101110001010011000110
/main/encry_err   0000000000000000    000000100000001000000000001000000000010000
/main/decry_val   UUUUUUUUUUUUUU      1100111100010111001100111010000010100101101
/main/decry_err   1000000010000000    1000000100000000000000000100000000010000
/main/data_out    nul nul nul nul nul nul  etb soh ff Ç enq eot soh Ç si dc1 □ □ □ 3 etb Ï
/main/l1          UUUUUUUUUUUUUU      0110001001110010011010010110101001101111011
/main/l2          UUUUUUUUUUUUUU      0110001001110010011010010110101001101111011
/main/dd          00100000011101111   0010000001110111011011101101000001011100010
/main/kd          01100010011100100   0110001001110010011010010110101001101111011
/main/pt          UUUUUUUUUUUUUU      0010111111001011110110101110001010011000110
/main/ct          UUUUUUUUUUUUUU      1100111100010111001100111010000010100101101
```

Fault detection output:



```
Messages
/main/clk         1
/main/data        hi anvi .how r u       hi anvi .how r u
/main/kdata       sdijaacjktaojrb        sdijaacjktaojrb
/main/encry_val   00110010000000100   0011001000000010011110010110100110011110011110100
/main/encry_err   0000000000000000    0000000000000000000000000000000000000000
/main/decry_val   01110101001000000   0111010100100000011100100010000001110110110111110110
/main/decry_err   0000000000000000    0000000000000000000000000000000000000000
/main/data_out    hi anvi .how r u       hi anvi .how r u
/main/l1          01100010011100100   0110001001110010011010010110101001101110110000101111
/main/l2          01100010011100100   0110001001110010011010010110101001101110110000101111
/main/dd          01110101001000000   0111010100100000011100100010000001110110110111110110
/main/kd          01100010011100100   0110001001110010011010010110101001101110110000101111
/main/pt          00110010000000100   0011001000000010011110010110100110011110011110100
/main/ct          01110101001000000   0111010100100000011100100010000001110110110111110110
```

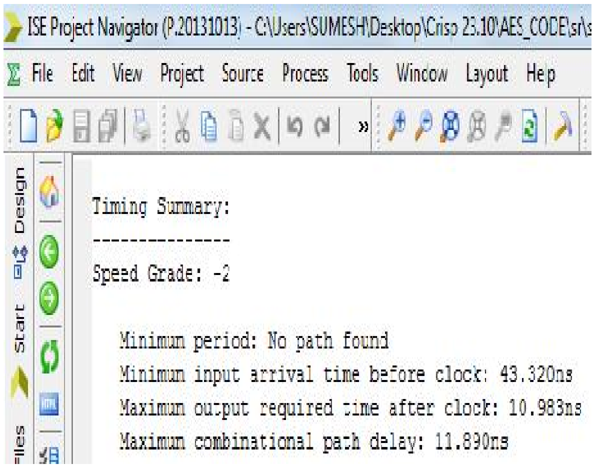
Area analysis :



ISE Project Navigator (P.20131013) C:\Users\SUMESH\Desktop\Crisp 23.10\AES_CODE\sr\sr.xise [Design Summar

```
Device utilization summary:
---------------------------

Selected Device : 6slx100tcsg484-2


Slice Logic Utilization:
 Number of Slice Registers:                256  out of  126576     0%
 Number of Slice LUTs:                    3557  out of   63288     5%
    Number used as Logic:                 3557  out of   63288     5%

Slice Logic Distribution:
 Number of LUT Flip Flop pairs used:      3557
   Number with an unused Flip Flop:       3301  out of    3557    92%
   Number with an unused LUT:                0  out of    3557     0%
   Number of fully used LUT-FF pairs:      256  out of    3557     7%
   Number of unique control sets:            1

IO Utilization:
 Number of IOs:                           1793
 Number of bonded IOBs:                   1793  out of     296   605% (*)
    IOB Flip Flops/Latches:               1400

Specific Feature Utilization:
 Number of BUFG/BUFGCTRLs:                   1  out of      16     6%
```

Time analysis:



ISE Project Navigator (P.20131013) - C:\Users\SUMESH\Desktop\Crisp 23.10\AES_CODE\sr\s

```
Timing Summary:
---------------
Speed Grade: -2

   Minimum period: No path found
   Minimum input arrival time before clock: 43.320ns
   Maximum output required time after clock: 10.983ns
   Maximum combinational path delay: 11.890ns
```

Conclusion

This paper proposed anfault diagnosis scheme for the energy-efficient lightweight block cipher Midori. Programs are developed for encryption of a plain text. encryption and decyption of the plain text are analysed by simulation in Modelsim. It is identified that by the addition of fault in the encryption and decryption process, Midori block cipher is able to detect the fault. While comparing the area and time delay of the midori block cipher and AES, it is understood that a block cipher midori is more energy efficient and consumes less power than existing system.

More reliable architectures for Midori are achieved through the proposed detection schemes and they can be tailored based on the objectives in terms of reliability and overhead tolerance. The modification that is going to include in the project in future is to implement a fault correction technique using hamming code for block cipher midori. The proposed design will be done on FPGA.

References

[1] M. Mozaffari- Kermani, M. Zhang, A. Raghunathan, and N. K. Jha, “Emerging frontiers in embedded security,” in Proc. Conf. VLSI Design, Jan. 2013, pp. 203–208.

[2] T. Eisenbarth, S. Kumar, C. Paar, and L. Uhsadel, “A survey of lightweight-cryptography implementations,” IEEE Des. Test Comput., vol. 24, no. 6, pp. 522–533, Jun. 2007.

[3] S. Banik et al., “Midori: A block cipher for low energy (extended version),” in Proc. Cryptol. ePrint Arch., 2015, pp. 411–436. A.Moradi and T. Schneider. (2016). Side-Channel Analysis Protection and Low-Latency in Action-Case Study of PRINCE and Midori. [Online]. Available: https://eprint.iacr.org/2016/481.pdf

[4] M. Mozaffari Kermani, R. Azarderakhsh, C.-Y. Lee, and S. Bayat-Sarmadi, “Reliable concurrent error detection architectures for extended Euclidean-based division over GF(2m),” IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 22, no. 5, pp. 995–1003, May 2014.

[5] S. Ali, X. Guo, R. Karri, and D. Mukhopadhyay, “Fault attacks on AES and their countermeasures,” in Secure System Design Trustable Computing. Springer, 2016, pp. 163–208.

[6] X. Guo and R. Karri, “Recomputing with permuted operands: A concur- rent error detection approach,” IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst., vol. 32, no. 10, pp. 1595–1608, Oct. 2013.

[7] M. Mozaffari-Kermani, R. Azarderakhsh, and A. Aghaie, “Fault detec- tion architectures for post-quantum cryptographic stateless hash-based secure signatures benchmarked on ASIC,” ACM Trans. Embedded Comput. Syst., to be published.

[8] M. Mozaffari-Kermani and R. Azarderakhsh, “Efficient fault diagno- sis schemes for reliable lightweight cryptographic ISO/IEC standard CLEFIA benchmarked on ASIC and FPGA,” IEEE Trans. Ind. Electron., vol. 60, no. 12, pp. 5925–5932, Dec. 2013.

[9] X. Guo, D. Mukhopadhyay, C. Jin, and R. Karri, “Security analysis of concurrent error detection against differential fault analysis,” J. Crypto- graph. Eng., vol. 5, no. 3, pp. 153–169, 2015.

[10] R. Karri, G. Kuznetsov, and M. Goessel, “Parity-based concurrent error detection of substitution-permutation network block ciphers,” in Proc. Cryptograph. Hardw. Embedded Syst., 2003, pp. 113–124.

Access this Article in Online

Quick Response Code	Website: www.ijarm.com Subject: Computer Sciences Engineering

DOI:10.22192/ijamr.2018.05.11.012

How to cite this article:
R. Venkadesh, A. V. Prathap kumar, K.Yoganand. (2018). Block Cipher Midori Encryption and Decryption with Fault Detection Technique. Int. J. Adv. Multidiscip. Res. 5(11): 104-108.
DOI: http://dx.doi.org/10.22192/ijamr.2018.05.11.012