Cryptanalysis of AES using FPGA Implementation

Mrs. Priyanka Holambe[#1], Prof. Ms. Harshali D. Zodpe [*2]

[#]Dept. of Electronics and Telecommunication Engineering
Maharashtra Institute of Technology, Pune – 411038, India,
[*] Dept. of Electronics and Telecommunication Engineering
Maharashtra Institute of Technology, Pune – 411038, India

Abstract: *In an age of technological advancements, security and privacy plays an important role in day to day communication. Cryptanalysis of modern cryptography algorithm involves massive and parallel computations. In absence of the mathematical breakthroughs to a cryptanalytical problem, a promising way to tackle these computations is to build special purpose hardware which will provide better cost-performance ratio. In this paper, the cryptanalysis of AES algorithm using brute force attack is used as a proof of concept. The basic concept is to create multiple instances of the design which can be instantiated simultaneously so that the solution space is exposed at a faster rate. For implementation of AES, Spartan-6 (XC6LX9) device is used. FPGA implementation of the AES requiring 1918 slices on a Xilinx Spartan3 (XC3S50) device, while achieving throughput of 1114.624 Mbps. Time required for cryptanalysis of AES is reduced from seconds to miliseconds as 3 multiple instances of design are instantiated parallel. The low-cost implementation and moderate throughput makes it practically suitable for low resource security applications.[1]*

Keywords— *AES, FPGA, VHDL, Cryptanalysis, Brute-Force Attack, Cipher Key.*

I. INTRODUCTION TO CRYPTANALYSIS

With the advance high speed electronic communication there is more information than ever to protect. The constant increase of information transmitted electronically has led to an increased reliance on cryptography. The security of symmetric and asymmetric ciphers is usually determined by the size of their key-length. Hence when designing a cryptosystem, the key-length must be chosen according to the assumed computational capabilities of an attacker. Cryptanalysis of modern cryptographic algorithms involves massive and parallel computations. Cryptanalysis is the study of retrieving the plain-text without knowledge of the valid key. In the absence of mathematical breakthroughs to a cryptanalytical problem, a promising way to tackle these computations is to build special-purpose hardware which will provide better cost-performance ratio.

There are different types of cryptanalysis, such as classical, algebraic attack, pre-existing attack, side channel attack, brute-force attack etc…

A. Brute-Force Attack

Brute-force attack is a strategy which can be used against any encryption data. This attack is being used when attacker can't take advantages of other any leak information from encryption. This applies every possible key from key space until the correct key is not obtained. The resources required brute-force attack increases exponentially as length of key increases. The length of key decides practical feasibility of performing Brute-force attack. The bottleneck for brute-force attack is time, as length of the key increase. Only by using the brute-force attack AES is breakable.

This paper is organized as follows: Section I is the Introduction to Cryptanalysis, Section II is Advanced Encryption Standard, it gives the detail explanation of AES algorithm and its operations. Section III gives proposed cryptanalysis of AES system requirements, specifications, design and implementation. Section IV gives results and conclusion V scope of future work.

II. ADVANCED ENCRYPTION STANDARD

The *Advanced Encryption Standard (AES)* is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2002. Originally called Rijndael, the cipher was developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, who submitted to the AES selection process. AES has been adopted by the U.S. government and is now used worldwide. It supersedes the Data Encryption Standard (DES). The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data.

A. AES Alogrithm

The AES is a symmetric block cipher that is used to encrypt and decrypt data. It consists of 128 bits input and support 128, 192 and 256 bits key length. These 128 bits are organized into 4x4 matrix referred as "state. The key size used for an AES specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the cipher-text. The feature of AES with different key is shown in Table I.

TABLE I

AES FEATURES WITH DIFFERENT KEY LENGTH

	Block Size	Key Length	No. of Rounds
AES_128	4	4	10
AES_192	4	6	12
AES_256	4	8	14

The AES algorithm consists of four major transformations. These transformations are:

- Byte Substitution
- Shift Row Transformation
- Mix Column Transformation
- Addition of Round Key
- Key Expansion

The AES Encryption and decryption process include the above mentioned transformations applied consecutively over the state, for a fixed number of rounds. The number of rounds depends on the key length used. The transformations for encryption and decryption are as follows. [5]

1. *AES encryption*

Encryption is simply conversion of raw data referred as plain text to encrypted or encoded data referred as cipher text.

- Byte substitution

It is a nonlinear substitution of bytes that operates independently applied on State matrix. It include two steps: first, executing the inverse of multiplication on finite field GF (2^8) with irreducible polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$, then apply the transformation defined by

$$\begin{bmatrix} b'0 \\ b'1 \\ b'2 \\ b'3 \\ b'4 \\ b'5 \\ b'6 \\ b'7 \end{bmatrix} = \begin{bmatrix} 1&0&0&0&1&1&1&1 \\ 1&1&0&0&0&1&1&1 \\ 1&1&1&0&0&0&1&1 \\ 1&1&1&1&0&0&0&1 \\ 1&1&1&1&1&0&0&0 \\ 0&1&1&1&1&1&0&0 \\ 0&0&1&1&1&1&1&0 \\ 0&0&0&1&1&1&1&1 \end{bmatrix} \begin{bmatrix} b0 \\ b1 \\ b2 \\ b3 \\ b4 \\ b5 \\ b6 \\ b7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

Figure.1. Matrix Notation for S- Box

- Shift Row Transformation

It performs cyclic shift of rows in the state matrix. The shift is performed over different offsets.

- Mix Column Transformation

In this transformation, each column of the state matrix is treated as four term polynomial. The columns are considered as polynomial over GF (2^8) and multiplied by modulo $x^4 + 1$ with fixed term polynomial $a(x) = \{03\} x^3 + \{01\} x^2 + \{01\} x + \{02\}$.

- Addition of Round Keys

In this transformation, a Round Key is added to each byte of state matrix by simple bitwise XOR operation.

- Key Expansion

In AES, there are a number of rounds, each needing its own key, so the actual key is ``stretched out'' and transformed to give portions of key for each round.

2. *AES Decryption*

Decryption is the reverse process to convert cipher text into the plain text. The decryption algorithm is very similar to the encryption algorithm except it uses inverses of the subroutines and they are executed in a slightly different order. 128 bit cipher text is converted into plaintext by the application of the inverse of the four transformations. Addition of round key is same for both encryption and decryption. The last round of both data and key are the first round inputs for the decryption process. [5]

The overall AES encryption and decryption process is described by Figure. 2.

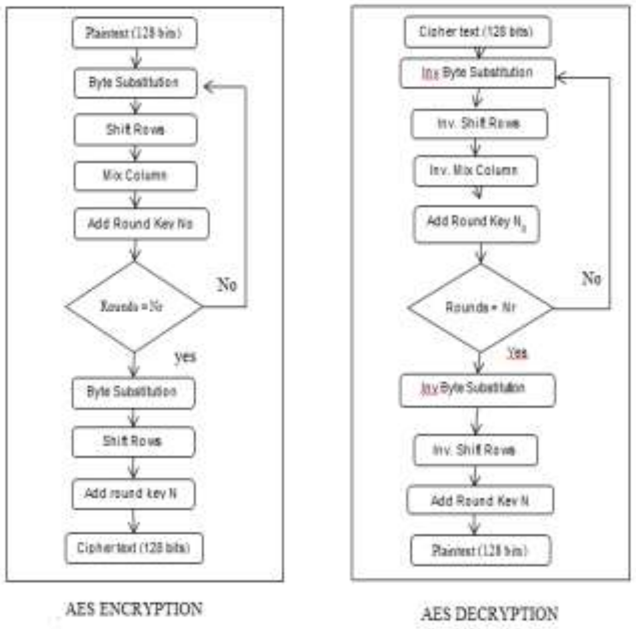


Figure 2. AES Encryption and Decryption

III. Implementation of cryptanalysis of AES on SPARTAN-6 Board

A. Overall System Design

In this paper Cryptanalysis of AES-128 for single and three parallel instances is implemented at the description level using Verilog Hardware Descriptive Language (VHDL). This program is written in Xilinx ISE 14.1 Project Navigator and simulated using ISE Simulator and implemented using FPGA Spartan-6Board.

Figure 3 shows the proposed system design for AES Cryptanalysis.

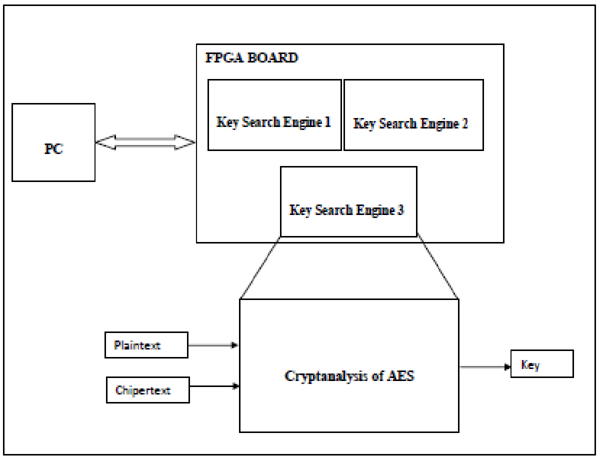


Figure. 3: System Block Diagram for Cryptanalysis of AES using FPGA

Computer is interfaced with the FPGA board, here Spartan-6 by using USB cable which also provides power supply to the kit. FPGA board has three key search engines. Each key search engine has VHDL programmed cryptanalysis of AES instances. Plaintext and ciphertext both are inputs required for cryptanalysis of AES's module which is VHDL program. These instances of key search engine are instantiated parallel to find the output key. Computer shows this output key and time required finding the key, generated from the FPGA Spartan-6 board.

The modeling process utilized in this project is the bottom-up approach. This means that the leaf components in the design hierarchy were developed first and the higher-level modules were constructed by instantiating their subcomponents and connecting them with the internal signals. All the modules in the design hierarchy were modeled in behavioral style, but the root module consisted of data flow modeling as well to implement the four major cipher transformations.

For the Cryptanalysis of AES design, a software model was initially developed in VHDL which would read a binary input and then output the encoded bit stream into another binary output. It gives the output key search for plaintext and cipher text.

B. System Implementation

The top module of the program (Single instance AES-128 Cryptanalysis) is simulated by using ISE simulator available with the Xilinx 14.1 ISE Design suite. Once the design is placed and routed, the Post placed and routed design is simulated and the output is cross checked with reference to the standard documentation available for AES. Then it is implemented on the FPGA board (XC6SLX9 CSG324). Same is done for the three parallel instances AES-128 cryptanalysis.

C. Requirements

- Hardware selection
  FPGA is used here because of its ability of re-programmable, and a shorter time to market and lower non-recurring engineering costs. FPGAs combine the best parts of ASICs and processor-based systems.

- Software selection
  1. Xilinx ISE 14.1: It is a software tool produced by Xilinx for synthesis and analysis of HDL designs, enabling the developer to synthesize their designs, perform timing analysis, examine RTL diagrams, simulate a design's reaction to different stimuli, and configure the target device with the programmer. Xilinx 14.1 supports Spartan-6 boards.
  2. Mimas V2: It is used to download VHDL Xilinx program in Spartan-6 board with port selection option.
  3. Visual Basic: Using Visual Basic we can see only required parameters in a single window and it is flexible to add or remove the parameters in window.

D. Specifications

1. 128 bit Plaintext and 128 bit Chiphertext-Input
2. AES algorithm
3. 128-bit key Variable - Output
4. Hardware used – Spartan-6 FPGA Board
5. Software used – Xilinx ISE 14.1, Mimas V2, Visual Basic (VB).

E. Simulation Results

The simulation results for the AES 128 bit for encryption and decryption are obtained from ISE simulator are as shown in Fig. 4-5. These results are verified from AES standard documentation.

The simulation results for single and three instances cryptanalysis of AES are obtained as shown in Figure 6-7.

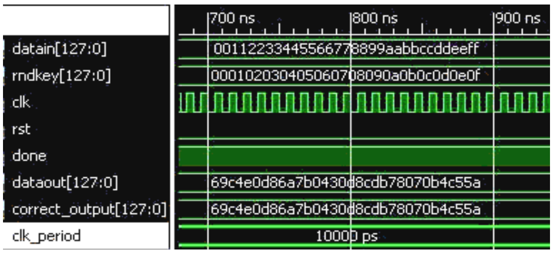

700 ns
800 ns
900 ns
datain[127:0]
00112233445566778899aabbccddeeff
rndkey[127:0]
000102030405060708090a0b0c0d0e0f
clk
rst
done
dataout[127:0]
69c4e0d86a7b0430d8cdb78070b4c55a
correct_output[127:0]
69c4e0d86a7b0430d8cdb78070b4c55a
clk_period
10000 ps

Figure. 4. Simulation Result for AES-128 Encryption

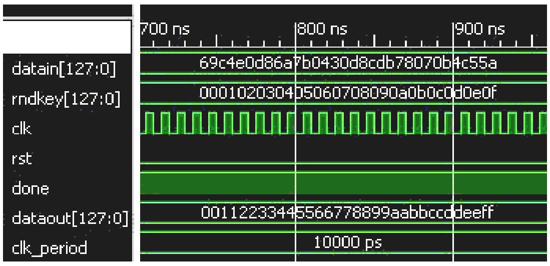

700 ns
800 ns
900 ns
datain[127:0]
69c4e0d86a7b0430d8cdb78070b4c55a
rndkey[127:0]
000102030405060708090a0b0c0d0e0f
clk
rst
done
dataout[127:0]
00112233445566778899aabbccddeeff
clk_period
10000 ps

Figure. 5. Simulation Result for AES-128 Decryption

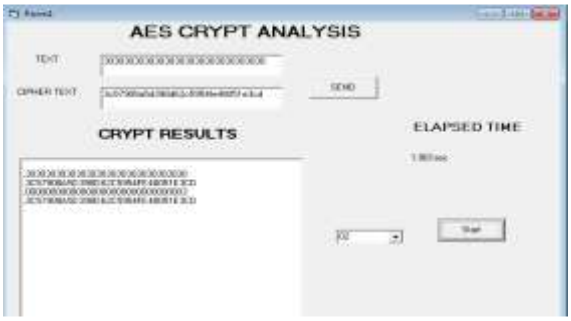


Figure. 6 Simulation Result of single Cryptanalysis of AES

Details of the simulation result of single cryptanalysis of AES.
Plaintext considered = 30303030303030303030303030303030
Ciphertext out = 3c57908a5d398d62c5954fe48051e3cd
Output key generated = 00000000000000000000000000000003
Elapsed time to generate the key with single instance is 1.061 sec.

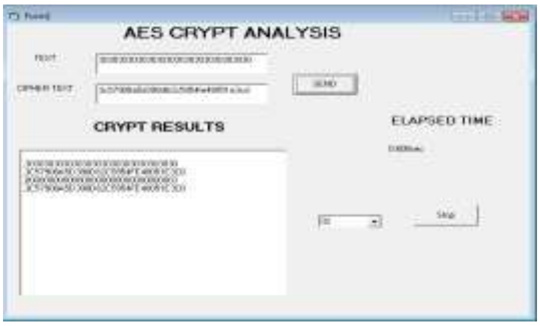


Figure. 7 Simulation Result of three parallel instances of Cryptanalysis of AES

Details of the simulation result of three instances of cryptanalysis of AES.
Plaintext considered = 30303030303030303030303030303030
Ciphertext out = 3c57908a5d398d62c5954fe48051e3cd
Output key generated = 00000000000000000000000000000003
Elapsed time to generate the key with single instance is 0.608 sec.

IV. RESULTS AND CONCLUSIONS

A. Results

Table 1 gives synthesis results with fastest and memory free AES-128 encryption. Synthesis comparison of AES encryption with other results [1]

Table 1
Synthesis Result Comparison

Parameters	Chodowis e & Gaj [6]	Rouvroy et al [7]	Pramstaller et al [8]	T Good & Benaissa [4]	Picoblaz e based [4]	Yong Sung Jeon et al [10]	Junfeng Chu Mohamme d Benaissia [1]	**This Design**
FPGA	Spartan II XC2S30-6	Spartan III XC3S50 -4	Virtex-E XCV1000 E	Spartan II XC2S15 -6	Spartan II XC2S15 -6	Spartan II XC2S30 -6	Spartan III XC3S50-5	**Spartan III XC3S50-5**
clock frquency (MHz)	60	70	161	67	90	66	45.642	**113.204**
Data Path	32	32	32	8	8	8	8	**3**
No. of clock cycles	44	46	92	3691	13546	352	160	**13**
Slices	222	163	1125	124	119	258	184	**1918**
No. of Block RAM's	3	3	0	2	2	0	0	**0**
Block RAM Size (kbits)	4	18	0	4	4	0	0	**0**
Bits of block RAM used	9600	34176	0	4480	10666	0	0	**0**
Total Equivalent Slices	522	1231	1125	264	452	258	184	**1918**
Throughput (Mbps)	166	208	215	2.2	0.71452	24	36.5	**1114.624**
Throughput/Slic e	318 kbps	169 kbps	191 kbps	8.3 kbps	1.9 kbps	93 kbps	198 kbps	**147.5 Mbps**
Summary	Best speed/ area	_	Fastest	ASIP	Software	_	Smallest	**Fastest & Memory Free**

Table2
Comparison of elapsed time required to find key

Sr. No.	Key(16 bytes)	Elapsed time required for single cryptanalysis (sec)	Elapsed time required for three cryptanalysis (sec)
1	00 0 … 0 0	0.39	0.39
2	0 00 …. 0 1	0.608	0.39
3	0 0 0.. .. 0 2	0.842	0.39
4	0 0 0 …0 3	1.061	0.608
5	0 0 0 .... 0 4	1.279	0.608
6	0 0 0 .. 0 5	1.528	0.608
7	0 0 0 … 0 6	1.747	0.843
8	0 0 0 … 0 7	1.982	0.843
9	0 0 0 .. ..0 8	2.199	0.843
10	0 0 0 .. 01 c	6.723	2.418
11	0 0 … ..0 f f	58.095	19.594
12	0 0.... 01 2 b	68.048	22.792

From the above results we can conclude that, as number of key search engines are increases time required to find key reduces. Table 1 is formed by collecting number of results of single and three instances of cryptanalysis AES, so collectively we can easily illustrate the result that time required to search the key is reduced as numbers of search engines are increased.

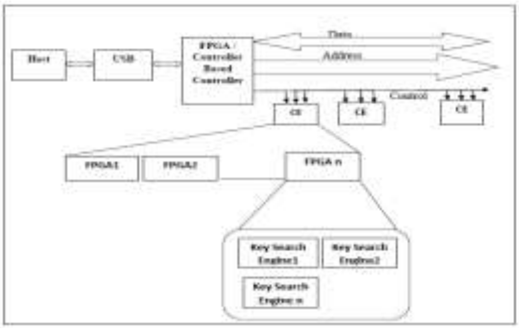
B. Conclusions

The proposed hardware-based cryptanalysis of AES system is designed to find the key, which is used to encrypt and decrypt data. Using AES-128 algorithm, implementation of cryptanalysis of AES is done on FPGA board; here Spartan-6 board is used. From the results of AES cryptanalysis it is clearly seen that as numbers of instances increases processing time to find key decreases. As the length of the key increases the processing time required to find output key is increases exponentially. From the results we can say that time increase from seconds to minutes, as length of key increases. Processing time to generate the output key reduces as the multiple instances of cryptanalysis are instantiated parallel as compared to single instance.

B. Scope for future work

In this project, a single FPGA board is used for implementation of Cryptanalysis of AES. Further, a system consisting of customized board with multiple FPGA's board and multiple such boards can be developed. All FPGA cards can be controlled by using a controller or another FPGA board.

Figure 8 shows proposed future scope block diagram for Cryptanalysis of AES.



ACKNOWLEDGMENT

We take this opportunity to express our sincere appreciation for the cooperation given by all the faculty and staff members of MIT, Pune to make this work a memorable experience.

REFERENCES

[1] Junfeng Chu , Mohammed Benaissa, "LOW AREA MEMORY-FREE FPGA IMPLEMENTA TION OF THE AES ALGO RITHM", 978-1-4673-2256-0/12/$31.00 c 2012 IEEE, PP.623-626.

[2] Alan Kaminsky, Michael Kurdziel, Stanislaw Radziszowski, "An Overview of Cryptanalysis Research for the Advanced Encryption Standard", 2010 Military Communications Conference - Unclassified Program - Cyber Security and Network Management 978-1-4244-8179-8/10/$26.00 ©2010 IEEE

[3] William Stallings, "Cryptography and Network Security Principles and Practices", Pearson Education, ISBN 81-7758-774-9,2007.

[4] T. Good and M. Benaissa, "AES on FPGA from the Fastest to the Smallest," LectureNotesinComputerScience,vol.3659,pp.427- 440, Sep. 2005.

[5] Federal Information Processing Standards Publication 197, "Advanced Encryption Standard (AES)"November26, 2001.

[6] P. Chodowiec, K. Gaj, Very Compact FPGA Implementation of the AES Algorithm, Cryptographic Hardware and Embedded Systems (CHES 2003), LNCS Vol. 2779, pp. 319 – 333, Spri nger - Verlag, October 2003.

[7] G. Rouvroy, F. X. Standaert, J. J. Quisquater, J. D. Legat, Compact and efficient encryption/decryption module for FPGA implementation of the AES Rijndael very well suited for small embedded applications, Procedings of the international conference on Information Technology: Coding and Computing 2004 (ITCC 2004), pp. 583 – 587, Vol. 2, April 2004.

[8] N. Pramstaller, S. Mangard, S. Dominikus, and J. Wolkerstorfer. Efficient AES implementations on ASICs and FPGAs. In Proc. 4th Conf. on the Advanced Encryption Standard (AES 2004), pp. 98 – 112, Bonn, Germany, May 10– 12, 2005.

[9] "Virtex-5 FPGA Data Sheet DS100 (v5.0)", February6, 2009.

[10] Y. S. Jeon, Y. J. Kim, and D. H. Lee, "A Compact Memory-Free Architecture for the Aes Algorithm Using Resource Sharing Methods," Journal of Circuits, Systems, and Computers, vol. 19, no. 5, p. 1109, 2010.

[11] http://en.wikipedia.org/wiki/AES

[12] http://en.wikipedia.org/wiki/FPGA

[13] http://en.wikipedia.org/wiki/spartan_6_FPGA