Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 116 (2017) 401–407

Procedia Computer Science

www.elsevier.com/locate/procedia

2nd International Conference on Computer Science and Computational Intelligence 2017, ICCSCI 2017, 13-14 October 2017, Bali, Indonesia

IMPROVEMENT OF ADVANCED ENCRYPTION STANDARD ALGORITHM WITH SHIFT ROW AND S.BOX MODIFICATION MAPPING IN MIX COLUMN

Rizky Riyaldhi[a], Rojali[a], Aditya Kurniawan[b,*]

[a]*Mathmematics Department, School of Computer Science, Bina Nusantara Univesity,Jakarta 11480, Indonesia*
[b]*Computer Science Department, School of Computer Science, Bina Nusantara Univesity,Jakarta 11480, Indonesia*

Abstract

Cyber Security has become rising issue in recent years where encryption is one of solution and has an important role in data protection. Encryption algorithms that widely used in information security are asymmetric and symmetric. Advanced Encryption Standard (AES) is one of symmetric encryption that most used often and the most secure encryption today. However, AES encryption has slow computation. Our experiment show that both of algorithms combination needs 3.045 milliseconds for 1024 bytes of data and increase 3-4 milliseconds for 2048 bytes of data and so on. This paper proposes a novelty method to improve AES algorithm with Shift Row and S.Box modification for Mix Column transformation. The result show that our optimization has reduced 3 milliseconds and continue to increase as the number of bytes increases. Percentage average of the optimization is 86.143%.

Peer-review under responsibility of the scientific committee of the 2nd International Conference on Computer Science and Computational Intelligence 2017.

Keywords: Advanced Encryption Standard, Optimization, Array Shiftrow

1. Introduction

The Advanced Encryption Standard (AES) was introduced by Rijndael who come from US National Institute of Standards and Technology competition in 2001 [1]. AES encryption is the solution for Data Encryption Standard (DES) aging problem [2]. Rijndanel symmetric block cipher standard version which can encrypt and decrypt plaintext 128 bits blocks using key with 128-bit, 192-bit, or 256-bit size. The Rijndael cipher has simple structure and suitable to 8-bit and 32-bit processing. The cipher has numbers round of plaintext transformation. Key length determines how many rounds to be executed. The key with 128-bit use 10 rounds, 192-bit use 12 rounds, and 256-bit use 14 rounds [3].

* Corresponding author
E-mail address: adkurniawan@binus.edu

1877-0509
Peer-review under responsibility of the scientific committee of the 2nd International Conference on Computer Science and Computational Intelligence 2017.
10.1016/j.procs.2017.10.079

Stalling explain AES arithmetics operations are addition, subtraction, multiplication,and division on finite field $GF(2^8)$. Performance of AES operations is depending on size of key length[3]. Each round has four transformations differently: *Sub Bytes, Shift Rows, Mix Column, and Add Round Key*. Each transformation takes any sixteen byte block which as 4 x 4 matrix and produce matrix output with same dimension. Next subsection will explained the simulation process of AES using simple example so that optimization part will be shown clearly.

Most of AES improvement has been done in domain hardware recently. Satoh et.al optimize AES by using circuit CMOS standard cell library[4]. Ahmad et. al use combinational logic that implemented by using truth table on Virtex II FPGA chip[5]. Daemen et. al use 32-bit data as basis data unit in AES transformation that improve the execution performance[6]. Intel using AES-NI extended instruction set to improve AES algorithm significantly[7]. There are many other hardware implementation for AES optimization[8,9,10,11].

2. AES Algorithm

AES key that will be used is 128-bit with 16 length of character. Character of key and plaintext will be transformed into hexadecimal that shown on table 1. Key characters will call state key when this key will be proceeding on first round and data characters would called state data.

Table 1: AES Key and Sample Data

Key	b	i	n	a	n	u	s	a	n	t	a	r	a	1	2	3
Hex	62	69	6E	61	6E	75	73	61	6E	74	61	72	61	31	32	33
Plain Text	T	w	o		O	n	e		N	i	n	e		T	w	o
Hex	54	77	6F	20	4F	6E	65	20	4E	69	6E	65	20	54	77	6F

The hexadecimal public key key will be transformed into 4 x 4 matrix dimension in Equation 1 as follows:

$$\begin{bmatrix} K_{0,0} & K_{0,1} & K_{0,2} & K_{0,3} \\ K_{1,0} & K_{1,1} & K_{1,2} & K_{1,3} \\ K_{2,0} & K_{2,1} & K_{2,2} & K_{2,3} \\ K_{3,0} & K_{3,1} & K_{3,2} & K_{3,3} \end{bmatrix} = \begin{bmatrix} 62 & 6E & 6E & 61 \\ 69 & 75 & 74 & 31 \\ 6E & 73 & 61 & 32 \\ 61 & 61 & 72 & 33 \end{bmatrix} \quad (1)$$

Key will be processed with four steps transformation stage[12] that mention above:

1. *Sub Bytes* -Transformation process for a non-linear byte substitution using S.box lookup table
2. *Shift Rows* - Cyclical shifting process for key matrix in each row
3. *Mix Column* - Dot matrix operation combine with XOR using matrix finite field $GF(2^8)$ and Galois Field.
4. *Add Round Key* - XOR addition operation for round key with state data

SubBytes are steps of byte to byte substitution using Rijndael's S.Box lookup table[13]. The table has 16x16 dimension where its contain hexadecimal characters. The hexadecimal is a replacement byte for a given input key state byte. SubBytes process can be seen on Fig. 1. For example, matrix element $K_{0,1}$ has $6E$ value. The 6 value used as a row coordinate and the E value used as column coordinate on S.Box lookup table. The lookup result for the value is $9F$. It is important that key and plaintext characters have to transform to hexadecimal for fit AES encryption and decryption process.

A Shift Row is arranging elements of state key matrix which performs a circular shift each row. The circular shift length is different every each row. The first row is never moved over. Second row move one first element to the right at last element. Third row move two first elements to the right at last element and the last row move three first elements. Shift row process can be seen on Fig 2. For example, element $K_{1,0}$ to be switched to the last element and three others element will come forward to the left, so the composition in the new state of matrix at second row will be $\{K_{1,1}, K_{1,2}, K_{1,3}, K_{1,0}\}$.