International Journal of Innovative Computing, Information and Control
Volume **5**, Number **5**, May **2009**

ICIC International ©2009 ISSN 1349-4198
pp. 1253–1264

A TRANSPOSITIONAL ADVANCED ENCRYPTION STANDARD (AES) RESISTS 3-ROUND SQUARE ATTACK

Yi-Shiung Yeh[1], Chen-Yu Lee[1], Ting-Yu Huang[1] and Chu-Hsing Lin[2]

[1]Department of Computer Science
National Chiao-Tung University
1001 Ta-Hsueh Road, HsinChu, Taiwan 30050, Taiwan
{ ysyeh; chenyu; tingyu }@cs.nctu.edu.tw

[2]Department of Computer Science and Information Engineering
Tunghai University
181 Taichung Harbor Road, Section 3 Taichung 40704, Taiwan
chlin@thu.edu.tw

Received December 2007; revised June 2008

Abstract. *In this paper, an advanced encryption standard (AES) variant is proposed that is resistant to linear cryptanalysis, differential cryptanalysis, and the square attack. We replace some procedures in the round function of AES and take the bit as the operation unit to foil the square attack. Also, we apply linear cryptanalysis and differential cryptanalysis to the proposed cipher. The proposed cipher is shown to be superior to AES in many aspects.*

Keywords: AES, Square attack, Feistel structure, Differential cryptanalysis, Linear cryptanalysis

1. Introduction.

On October 2, 2000, the National Institute of Standards and Technology (NIST) announced that Rijndael had been selected as the proposed Advanced Encryption Standard (AES) and began the process of making it the official standard. On November 26, 2001, NIST announced the AES as Federal Information Processing Standards Publication 197 (FIPS PUB 197). The National Security Agency (NSA) stated all AES finalists, including Rijndael, were secure enough for US government non-classified data. In June 2003, the US government announced that AES should be used for classified information.

The AES algorithm is specified with a fixed block size of 128bits and a key size of 128, 192, or 256bits. It is capable of using any key and block size for all multiples of 32bits. The key is expanded using Rijndael's key schedule. Most AES computations are done in a special finite field. AES operates on a 4×4 array of bytes called the state. For encryption, each round of AES (except for the last round, which omits the *MixColumns* stage) consists of four stages.

The four stages of AES are explained as follows

- *SubByte* – a non-linear substitution step where each byte is replaced with another according to a lookup table.
- *ShiftRow* – a transposition step where each row of the state is shifted cyclically by a certain number of offsets.
- *MixColumn* – a mixing operation that operates on the columns of the state and combines the four bytes in each column using a linear transformation.
- *AddRoundKey* – each byte of the state is combined with the round key; each round key is derived from the cipher key using a key schedule algorithm.