International Journal of Innovative Computing, Information and Control
Volume **3**, Number **3**, June **2007**

ICIC International ©2007 ISSN 1349-4198
pp. 751–759

A NEW S-BOX STRUCTURE NAMED AFFINE-POWER-AFFINE

Lingguo Cui

School of Information Science and Technology
Beijing Institute of Technology
5 South Zhongguancun Street, Beijing 100081, P. R. China
lgcui2001@163.com

Yuanda Cao

School of Computer Science and Technology
Beijing Institute of Technology
5 South Zhongguancun Street, Beijing 100081, P. R. China
ydcao@bit.edu.cn

Received July 2006; revised November 2006

Abstract. *In this paper, we consider the problem of the simple algebraic structure of the Advanced Encryption Standard (AES) S-box, in which only 9 terms are involved in the algebraic expression, while its inverse S-box involves 255 terms. By resolving the reason why the algebraic expressions of AES-like S-boxes are so simple, the upper bound of items involved in the algebraic expressions of AES-like S-boxes is presented. Then, a new S-box structure named Affine-Power-Affine (APA) is designed such that the algebraic complexity is increased. With the APA structure, the algebraic complexity of the improved AES S-box is increased from 9 to 253, and its inverse S-box keeps 255. Furthermore, other good cryptographic characteristics of AES S-box are inherited.*
Keywords: S-box, AES, APA, Algebraic complexity

1. **Introduction.** Since Rijndael [1], the Substitution-Permutation Network (SPN) block cipher algorithm designed by Joan Danmen and Vincent Rijmen, was selected by NIST as the Advanced Encryption Standard (AES) on Oct. 2, 2000, many cryptanalysts have increased their interest in attacking the algorithm. It has been recognized that Rijndael has the security against differential cryptanalysis (DC) [2] and linear cryptanalysis (LC) [3] which are the most well known attacks on block ciphers. Because of the strict algebraic structure of AES S-box, many people focus on the algebraic attack [4, 5], which may be a successful method with the development of algebraic methods [15, 16]. As the only nonlinear part of the network, S-box is a critical element of any SPN and it determines the performance of the whole block cipher. So, many researchers devote time to analyze and improve the S-box of AES [6, 7, 8, 9].

Although the algebraic expression of AES inverse S-box involves 255 items, there are only 9 items involved in the algebraic expression of AES S-box, which makes AES S-box be suspected. In the reference [6], the reasons why AES S-box has only 9 items but the inverse S-box has 255 items are explained with the algebraic method that the component of the field element can be expressed by a simple polynomial with the element itself as the variable over GF(2^8). In this paper, we not only resolve the reason why the algebraic