International Journal of Innovative Computing, Information and Control
Volume **7**, Number **5(A)**, May **2011**

ICIC International ©2011 ISSN 1349-4198
pp. **2291–2302**

AN IMPROVED AES S-BOX AND ITS PERFORMANCE ANALYSIS

Jie Cui[1,2], Liusheng Huang[1], Hong Zhong[2], Chinchen Chang[3] and Wei Yang[1]

[1]National High Performance Computing Center at Hefei and
Department of Computer Science and Technology
University of Science and Technology of China
No. 96, Jinzhai Rd., Hefei 230026, P. R. China
lshuang@ustc.edu.cn; { cuijie; smartyw }@mail.ustc.edu.cn

[2]School of Computer Science and Technology
AnHui University
No. 3, Feixi Rd., Hefei 230039, P. R. China
zhongh@ahu.edu.cn

[3]Department of Computer Science and Information Engineering
Feng Chia University
Taichung 40724, Taiwan
alan3c@gmail.com

Received January 2010; revised May 2010

Abstract. *S-box is a unique nonlinear operation in Rijndael, one encryption algorithm chosen as AES, and it determines the performance of AES. In this paper, the weaknesses in complexity and security of AES S-box are analyzed. We propose to increase the complexity and security of AES S-box by modifying the affine transformation and adding an affine transformation. Performance analysis demonstrates that the improved AES S-box has following cryptographic properties: the affine transformation period is increased from 4 to the most 16, the iterative period is increased from less than 88 to the most 256, and the distance to SAC is reduced from 432 to 372. Moreover, the number of terms in the improved AES S-box algebraic expression is increased from 9 to 255, and its inverse S-box keeps almost the same as AES inverse S-box. Comparison results suggest that the improved AES S-box has better performance and can readily be applied to AES.*
Keywords: AES, Rijndael, Affine transformation, Inverse S-box

1. **Introduction.** Since Rijndael algorithm was chosen by NIST as an advanced encryption standard (AES) on October 2, 2000, much attention has been attracted to it and many methods have been proposed to attack it [1,2,10]. But there has never been successful attack on the full AES up to now. As the only nonlinear operation of AES, S-box plays a crucial role against various attacks.

The cryptanalysis of the cryptographic strength of Rijndael has not stopped after the announcement and official publication of the AES [11-16,19]. Biryukov et al. [10] proposed a distinguisher and related-key attack on the full AES-256. Wang [5] noted that AES S-box affine transformation period is 4, and it does not achieve the most 16. Wang et al. [6,17,18] studied AES S-box structure and pointed out that the iterative period of AES S-box has short-period phenomenon, and all the periods are less than 88. Murphy and Robshaw [3] analyzed AES S-box algebraic expression and indicated that the algebraic expression of AES S-box is very simple and only 9 terms are involved. Much work has concentrated on AES S-box, such as the latest significant progress [7] which illustrated the reason why AES S-box algebraic expression is so simple and proposed an improved S-box, and the algebraic expression of the S-box involves 255 terms, so the complexity