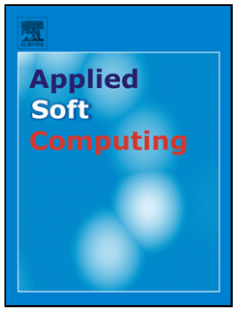

Title: Designing Bijective S-boxes Using Algorithm Portfolios with Limited Time Budgets

Author: Dimitris Souravlias Konstantinos E. Parsopoulos Gerasimos C. Meletiou

PII: S1568-4946(17)30330-7
DOI: http://dx.doi.org/doi:10.1016/j.asoc.2017.05.052
Reference: ASOC 4256

To appear in: *Applied Soft Computing*

Received date: 5-10-2016
Revised date: 13-4-2017
Accepted date: 26-5-2017

Please cite this article as: Dimitris Souravlias, Konstantinos E. Parsopoulos, Gerasimos C. Meletiou, Designing Bijective S-boxes Using Algorithm Portfolios with Limited Time Budgets, *<![CDATA[Applied Soft Computing Journal]]>* (2017), http://dx.doi.org/10.1016/j.asoc.2017.05.052

Designing Bijective S-boxes Using Algorithm Portfolios with Limited Time Budgets

Dimitris Souravlias[a], Konstantinos E. Parsopoulos[a], Gerasimos C. Meletiou[b]

[a]*Department of Computer Science and Engineering, University of Ioannina, GR-45110 Ioannina, Greece*
{dsouravl,kostasp}@cse.uoi.gr
[b]*Department of Agricultural Technology, Technological Education Institute of Epirus, GR-47100 Arta, Greece*
gmelet@teiep.gr

Abstract

Substitution boxes (S-boxes) are essential parts of symmetric-key cryptosystems. Designing S-boxes with satisfactory nonlinearity and autocorrelation properties is a challenging task for both theoretical algebraic methods and computational optimization algorithms. Algorithm Portfolios (APs) are algorithmic schemes where multiple copies of the same algorithm or different algorithms share the available computational resources, running concurrently or interchangeably on a number of processors. Recently, APs have gained increasing attention due to their remarkable efficiency in multidisciplinary applications. The present work is a preliminary study of parallel APs on the bijective S-boxes design problem. The proposed APs comprise two state-of-the-art heuristic algorithms, namely Simulated Annealing and Tabu Search, and they are parallelized according to the master-slave model without exchange of information among the constituent algorithms. The proposed APs are experimentally assessed on typical problem instances under limited time budgets. Different aspects of their performance is analyzed, suggesting that the considered APs are competitive in terms of solution quality and running time against their constituent algorithms as well as different approaches.

Keywords: Algorithm Portfolios, S-boxes, Optimization, Heuristics, Cryptography

1. Introduction

Substitution boxes (S-boxes) constitute essential parts of modern cryptographic applications. In essence, S-boxes are multi-input multi-ouput Boolean functions that map binary input to binary output values. S-boxes lie at the core of symmetric-key cryptographic algorithms. Specifically, they are used to conceal the relation between the input key and the encrypted output message. Therefore, they have crucial impact on the algorithm's security quality [1, 2].

The design of suitable S-boxes has been an active research area for several decades with significant applications in symmetric-key cryptography standards. A widely known example is the Data Encryption Standard (DES), which was introduced in 1977 and it is based on eight 6-input 4-output S-boxes [3]. DES has been proved to be vulnerable to crack attacks such as linear cryptanalysis and parallel brute-forcing. Thus, it was superseded by the Advanced Encryption Standard (AES). AES was proposed in 2000 and its implementation is also based on S-boxes [4]. Specifically, it employs a properly designed Rijndael S-box that is resistant to linear [5] and dif-