Ministry of Higher Education and
Scientific Research
University of Mosul
College of Computer Science
and Mathematics
Department of Computer Science

Constructing S-Box Based on Chaotic Logistic Map and Jellyfish Search Algorithm

**A Thesis Submitted to the Council of the College of Computer Science and Mathematics
University of Mosul
As Partial Fulfillment of Requirements for the Degree of Master Science
in
Computer Science**

By

Hind Abdulghani Ahmed Al-Heayli

Supervised by

Dr . Sufyan Salim Al-Dabbagh -
Assistant Prof

2022 A.D **1443 A.H.**

Abstract

Substitution-Boxes (S-Boxes) are a key component of most block ciphers, and the robustness of the S-Boxes for preventing unauthorized access has a significant impact on the security of digital data in general. As a result, building a robust S-Box with a high nonlinearity score is seen as a substantial difficulty. On the other hand, because some devices have limited resources, lightweight security techniques are the best option for ensuring the security of such systems. For these reasons, it is important to have a cryptographically strong lightweight S-Box to help in reducing the processing and power overhead caused by block ciphers with traditional S-Box.

In this thesis, a new lightweight S-Box is designed to be used for resource-constraint devices. The logistic chaotic map was selected for initializing the S-Box population. With some modification and addition to the state-of-art Jellyfish optimization algorithm, it was possible to use it for optimizing the generated S-Boxes, in order to find a suitable strong S-Box that can satisfy the statistical design criteria.

The statistical analysis results of the proposed S-Box are compared to some of the recently designed S-Boxes in the literature, the comparison showed that the suggested S-Box has mostly equal, to better statistical attributes, which mark the suggested S-Box as a robust cryptographically and a good fit to be used for lightweight block cipher algorithms. All the functions of the three S-Boxes showed the maximum non-linearity of 4, and SAC values of 0.5027, 0.4978, and 0.5031 respectively, which have a very small margin to the perfect 0.5 desirable value.

The analysis results showed that the overall processing that cause power consumption of the network was slightly higher with the presence of the cipher using the proposed S-Box, especially when the ppm is low. As the ppm gets higher slightly more processing is needed which results in a very small margin increase in energy consumption that can be tolerated.

وزارة التعليم العالي والبحث العلمي
جامعة الموصل
كلية علوم الحاسوب والرياضيات
قسم علوم الحاسوب

بناء S-Box على أساس الخريطة اللوجيستية الفوضوية وخوارزمية البحث عن قنديل البحر

رسالة مقدمة
الى مجلس كلية علوم الحاسوب والرياضيات في جامعة الموصل
كجزء من متطلبات نيل شهادة ماجستير علوم في علوم الحاسوب
من قبل

هند عبد الغني أحمد الحيالي

بإشراف
الدكتور سفيان سالم الدباغ

1443هـ 2022م

الملخص

تعد صناديق الاستبدال (S–Boxes) مكونًا رئيسيًا لمعظم خوارزميات التشفير الكتلي، كما أن متانة S–Boxes لمنع الوصول غير المصرح به لها تأثير كبير على أمان البيانات الرقمية بشكل عام. نتيجة لذلك، يُنظر إلى بناء S–Box قوي مع درجة عالية من اللاخطية عالية على أنه عملية صعبة كثيراً. من ناحية أخرى، نظرًا لأن أجهزة إنترنت الأشياء لديها موارد محدودة، فإن تقنيات الأمان خفيفة الوزن هي الخيار الأفضل لضمان أمان هذه الأنظمة. لهذه الأسباب، من المهم أن يكون لديك S–Box قوي وخفيف الوزن من الناحية التشفيرية للمساعدة في تقليل المعالجة والطاقة الزائدة التي يسببها التشفير الكتلي مع صناديق التعويض التقليدية.

في هذه الأطروحة، تم تصميم S–Box خفيف الوزن جديد لاستخدامه في أجهزة إنترنت الأشياء مقيدة المصادر. تم اختيار الخريطة الفوضوية اللوجستية لتهيئة المجتمع الاولي من صناديق التعويض. مع بعض التعديلات والإضافة إلى خوارزمية تحسين قنديل البحر الحديثة، كان من الممكن استخدامها لتحسين صناديق التعويض المولدة، من أجل العثور على صندوق تعويض قوي مناسب يمكنه تلبية معايير التصميم الإحصائي.

تمت مقارنة نتائج التحليل الإحصائي لـ S–Box المقترحة مع بعض صناديق التعويض المصممة حديثًا، وأظهرت المقارنة أن S–Box المقترح يتساوى في الغالب، مع سمات إحصائية أفضل، والتي تميز S–Box المقترح باعتباره تشفيرًا قويًا ومناسبًا جيدًا لاستخدامه في خوارزميات تشفير الكتلة خفيفة الوزن. أظهرت جميع دوال الصندوق المقترح الحد الأقصى من الغير الخطي البالغ 4، وقيم SAC مساوية لـ 0.5027 و 0.4978 و 0.5031 على التوالي ، والتي لها هامش صغير جدًا إلى القيمة المثالية 0.5 المرغوبة.

أظهرت نتائج التحليل أن المعالجة الإجمالية التي تسببت في استهلاك الطاقة للشبكة كانت أعلى قليلاً مع وجود التشفير باستخدام S-Box المقترح، خاصةً عندما يكون معدل نقل البيانات منخفض. نظرًا لارتفاع جزء معدل نقل البيانات، هناك حاجة إلى مزيد من المعالجة مما يؤدي إلى زيادة هامش صغيرة جدًا في استهلاك الطاقة يمكن التغاضي عنها.