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

Evaluating the Resistances of Lightweight Block Cipher Algorithms to Linear and Differential Cryptanalysis

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

Mohammed Eid Khamees Salim Al-Shammary

Supervised by

Assist. prof. Dr. Sufyan Salim Mahmood Al-Dabbagh

2023 A.D **1444 A.H.**

Abstract

With the increasing of using the Internet and the applications that use it, it has become necessary to use technologies that maintain the confidentiality of data transmitted over the network. Encryption is one of the most important forms of maintaining the confidentiality of data sent over the network from one party to the other. A lightweight block cipher is one of the most important methods used to achieve this purpose, especially in Internet of Things (IoT) applications. The robustness of cipher systems depends on the implemented substitution box (S-Box) in the structure of the cipher system. Therefore, S-Box inputs and outputs are an important factor in cryptanalysis. Many attacks have been implemented with different methods to estimate the strength of these systems such as differential and linear cryptanalysis.

In this thesis, the resistance of some commonly used lightweight block ciphers in many applications to differential and linear cryptanalysis (DDT and LAT) is tested. These algorithms were characterized using a 4x4 S-Box. The S-Box of all these encoders has 4 inputs and 4 outputs.

After the practical application of differential and linear analysis on the selected algorithms, the tables gave corresponding results in evaluating the resistance of each algorithm. The results clearly show that TWINE, PRINCE, and KLEIN Lightweight Block Cipher are more robust than other lightweight block ciphers against linear and differential cryptanalysis. While the algorithm was GIFT relatively weaker than the rest of the systems in its resistance to linear and differential analysis.

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

تقييم مقاومة خوارزميات التشفير الكتلي الخفيف الوزن لتحليل التشفير الخطي والتفاضلي

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

من قبل
محمد عيد خميس سالم الشمري

بإشراف
أ.م.د سفيان سالم محمود الدباغ

٢٠٢٣ م ١٤٤٤ هـ

الخلاصة

مع تزايد استخدام شبكة الانترنيت والتطبيقات التي تستخدمها أصبح من الضروري استخدام تقنيات تحافظ على سرية البيانات المرسلة عبر الشبكة. يعد التشفير بأنواعه أحد اهم اشكال الحفاظ على سرية البيانات المرسلة عبر الشبكة من طرف الى اخر. اذ يستخدم في تحقيق سرية وخصوصية البيانات. يعد التشفير الكتلي الخفيف الوزن أحد اهم الوسائل المستخدمة لتحقيق هذا الغرض وخاصة في تطبيقات انترنيت الاشياء. تعتمد متانة أنظمة التشفير على صندوق الاستبدال المنفذ (S-Box) في هيكل نظام التشفير. لذلك، تعد مدخلات ومخرجات S-Box عاملا مهمة في مجال تحليل التشفير. تم تنفيذ العديد من الهجمات بطرق مختلفة لتقدير قوة هذه الأنظمة مثل تحليل التشفير التفاضلي والخطي.

في هذه الرسالة تم اختبار مدى مقاومة بعض انظمة التشفير الكتلي خفيف الوزن المستخدمة بشكل شائع في العديد من التطبيقات مع كلا النوعين من تحليل التشفير التفاضلي والخطي (DDT وLAT). تميزت هذه الخوارزميات باستخدام 4x4 S-Box. يحتوي S-Box لجميع أنظمة التشفير هذه على ٤ مدخلات و٤ مخرجات.

بعد التطبيق العملي للتحليل التفاضلي والخطي على الخوارزميات التي تم اختيارها، أظهرت النتائج وجود تشابه كبير في مدى مقاومة الخوارزميات للتحليلين نسبة الى جدول التقريب الخطي وجدول التوزيع التفاضلي. حيث أظهرت أن TWINE و PRINCE و KLEIN Lightweight Block Cipher أقوى من بقية انظمة التشفير خفيفة الوزن الأخرى ضد تحليل التشفير الخطي والتفاضلي. بينما كانت خوارزميةGIFT أضعف نسبيا من باقي الانظمة في مقاومتها للتحليل الخطي والتفاضلي.