Analisis dan Pengembangan Algoritma Modifikasi Lightweight PRESENT Berdasarkan Ketahanan terhadap Potensi Improbable Differential Cryptanalysis = Analysis and Development of PRESENT Lightweight Modification Algorithm Base on Resistance to Potential Improbable Differential Cryptanalysis.

Afifah, author

Abstrak

ABSTRAK
Teknologi Internet of Things (IoT) menjadi salah satu kebutuhan yang terus meningkat, dan tentunya memunculkan risiko dan tantangan keamanan informasi. Mengingat serangan terhadap perangkat IoT juga semakin meningkat, aspek keamanan menjadi bagian utama dalam implementasi IoT salah satunya adalah teknik kriptografi. Dari segi teknik kriptografi, lightweight cryptography dibutuhkan untuk memenuhi aspek keamanan informasi sekaligus didesain untuk diterapkan pada perangkat IoT. PRESENT merupakan salah satu algoritma block cipher ultra lightweight yang banyak diimplementasikan karena telah teruji ringan dan cepat, serta termasuk dalam salah satu algoritma lightweight yang direkomendasikan pada standar ISO/IEC 29192-2. Namun beberapa peneliti telah melakukan analisis kelemahan algoritma PRESENT terhadap suatu cryptanalysis salah satunya adalah improbable differential cryptanalysis. Improbable differential cryptanalysis merupakan gabungan dari metode impossible differential characteristic dan differential characteristic. Metode improbable differential cryptanalysis ini memanfaatkan karakteristik unik berupa undisturbed bit dari s-box PRESENT untuk membentuk pola dalam melakukan analisis cryptanalysis. Oleh karena itu, pada penelitian ini dilakukan analisis dan pengembangan algoritma modifikasi PRESENT berdasarkan ketahanannya terhadap potensi improbable differential cryptanalysis. Modifikasi algoritma dilakukan dengan mengganti s-box PRESENT menggunakan 9 (sembilan) pilihan s-box yang meliputi 4 (empat) s-box SERPENT, s-box BORON, s-box KLEIN, s-box LED, s-box RECTANGLE, dan s-box NES. Analisa yang dilakukan menggunakan uji Strict Avalanche Criterion (SAC), uji Differential Approximation Probability (DAP), dan analisa terhadap probabilitas karakteristik improbable differential yang dapat dibentuk. Berdasarkan hasil penelitian, substitution box KLEIN menghasilkan nilai uji SAC dan DAP yang paling baik dibandingkan 9 s-box lainnya yaitu memiliki nilai SAC rata-rata sebesar 0.59375 dan nilai DAP tertinggi sebesar 0.25 sebanyak 15. Serta berdasarkan hasil analisa improbable differential, algoritma modifikasi PRESENT yang menggunakan s-box KLEIN memiliki probabilitas terendah yaitu sebesar . Hal ini menunjukkan bahwa algoritma modifikasi PRESENT menggunakan s-box KLEIN memiliki ketahanan yang lebih baik terhadap potensi dilakukannya improbable differential cryptanalysis.
<hr>
ABSTRACT
Internet of Things (IoT) technology increased for needed, and it raises risks and challenges of information security. Considering that attacks on IoT devices are increasing, security aspects become a part important in the implementation of IoT, one of which is cryptography. In terms of cryptography techniques, lightweight cryptography is needed to comply with the information security aspects and designed to be applied to IoT devices. PRESENT is one of the ultra-lightweight block cipher algorithms that has been implemented

because it has been tested small and fast. PRESENT is included in one of the lightweight algorithms recommended in the ISO/IEC 29192-2 standard, but some researchers have analyzed algorithm weaknesses. Improbable differential cryptanalysis is a combination of impossible differential characteristics and differential characteristics. This improbable differential cryptanalysis method uses a unique characteristic consisting of the uninterrupted bits of the PRESENT s-box to create a pattern for conducting cryptanalysis. Therefore, in this research, an analysis of the PRESENT modification algorithm is based on its resistance to improbable differential cryptanalysis potential. Algorithm modification is done by replacing PRESENT S-box using 9 (nine) s-box options, which include 4 (four) SERPENT s-boxes, BORON s-boxes, KLEIN s-boxes, LED s-boxes, RECTANGLE s-boxes, and NES s-boxes. The analysis is performed using Strict Avalanche Criterion (SAC) test, Differential Approximation Probability (DAP) test, and analysis of the probability of improbable differential characteristics that can be formed. Based on the results of the research, KLEIN substitution box produces the best SAC and DAP test values compared to 9 other s-boxes, which have an average SAC value of 0.59375 and the highest DAP value of 0.25 of 15. And based on the results of improbable differential analysis, PRESENT modification algorithm which use the KLEIN s-box has the lowest probability of. This shows that the PRESENT modification algorithm using the KLEIN s-box has better resistance to the potential for improbable differential cryptanalysis.