Scopus

Document details

Back to results | 1 of 1

Export Download Print E-mail Save to PDF Add to List More...

Full Text View at Publisher

Proceedings - 2013 International Conference on Advanced Computer Science Applications and Technologies, ACSAT 2013
2014, Article number 6836586, Pages 254-258
2nd International Conference on Advanced Computer Science Applications and Technologies, ACSAT 2013; Kuching, Sarawak; Malaysia; 23 December 2013 through 24 December 2013; Category numberP5234; Code 106250

Improving PRESENT lightweight algorithm (Conference Paper)

Aldabbagh, S.S.M.[ac], Shaikhli, I.F.T.A.[b]

[a]Department of Information Systems, IIUM, Kuala Lumpur, Malaysia
[b]Department of Computer Science, IIUM, Kuala Lumpur, Malaysia
[c]University of Mosul, Iraq

Abstract

View references (15)

Lightweight block cipher algorithms are vital for constrained environment. Substitution box (S-box) is the essential constituent of many lightweight block cipher algorithms and it is the only nonlinear part. It is proficient to create confusion in the plaintext during the process of encryption. In this research, a new way of key dependent S-box is proposed by choosing one S-box out of 16 good S-boxes. Preliminary analysis of linear and differential cryptanalysis is showing that the proposed algorithm is more secure than fixed PRESENT S-box. Also, the complexity of the PRESENT S - box in each round is 28 while the complexity of the proposed algorithm S-box is 212 in each round. © 2013 IEEE.

Author keywords

Key Dependent S-box linear cryptanalysis and differential cryptanalysis PRESENT lightweight block cipher S-box

Indexed keywords

Engineering controlled terms: Computer science Cryptography Lyapunov methods Security of data

Differential cryptanalysis
Key Dependent S-box
Lightweight block ciphers
Plaintext
Preliminary analysis
S-box S-boxes
Substitution Box(S Box)

Engineering main heading: Algorithms

ISBN: 978-147992758-6 **DOI:** 10.1109/ACSAT.2013.57
Document Type: Conference Paper