

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 6836594, Pages 296-299

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 the security of LBlock lightweight algorithm using bit permutation (Conference Paper)

Aldabbagh, S.S.M.^{ac} [✉](#), Shaikhli, I.F.T.A.^b [✉](#)

^aDepartment of Information Systems, IIUM, Kuala Lumpur, Malaysia

^bDepartment of Computer Science, IIUM, Kuala Lumpur, Malaysia

^cUniversity of Mosul, Iraq

Abstract

[View references \(25\)](#)

Lightweight block cipher algorithms are important for constrained environment. LBlock uses word permutation to do the diffusion while this research uses bit permutation to increase the number of active Substitution box (S-box). The number of active S-box is a regular method to evaluate the security against linear and differential attacks. The bit permutation method is described in this research with analysis and discussion. The preliminary results show that the proposed algorithm has 32 active S-box for 13 rounds which is higher than 32 active S-box for 15 rounds of LBlock algorithm. Also, we can conclude that the proposed algorithm is better than LBlock algorithm in the perspective of security. © 2013 IEEE.

Author keywords

Active S-box LBlock lightweight block cipher linear cryptanalysis and differential cryptanalysis

Indexed keywords

Engineering controlled terms: Computer science Cryptography Security of data

Active S-box

Bit permutation

Differential attacks

Differential cryptanalysis

Lightweight block ciphers

Substitution Box(S Box)

Engineering main heading: Algorithms

ISBN: 978-147992758-6

DOI: 10.1109/ACSAT.2013.65

Document Type: Conference Paper

Metrics

0 Citations in Scopus

0 Field-Weighted Citation Impact



PlumX Metrics

Usage, Captures, Mentions, Social Media and Citations beyond Scopus.

Cited by 0 documents

Inform me when this document is cited in Scopus:

[Set citation alert >](#)

[Set citation feed >](#)

Related documents

Key-dependent S-box in lightweight block ciphers

Mahmood Aldabbagh, S.S. , Al Shaikhli, I.F.T. , Reza Zaba, M. (2014) *Journal of Theoretical and Applied Information Technology*

Improving PRESENT lightweight algorithm

Aldabbagh, S.S.M. , Shaikhli, I.F.T.A. (2014) *Proceedings - 2013 International Conference on Advanced Computer Science Applications and Technologies, ACSAT 2013*

Related-key impossible differential attack on reduced round LBlock

Zhan, Y.-J. , Guan, J. , Ding, L. (2012) *Dianzi Yu Xinxuebao/Journal of Electronics and Information Technology*

View all related documents based on references