Document details

Proceedings - 2015 4th International Conference on Advanced Computer Science Applications and Technologies, ACSAT 2015
25 May 2016, Article number 7478736, Pages 159-164
4th International Conference on Advanced Computer Science Applications and Technologies, ACSAT 2015; Kuala Lumpur; Malaysia; 8 December 2015 through 10 December 2015; Category numberP5790; Code 121882

Enhancing Lightweight Block Cipher Algorithm OLBCA through Decreasing Cost Factor (Conference Paper)

Al-Dabbagh, S.S.M.[a], Shaikhli, I.F.T.A.[b], Al-Enezi, K.A.[b], Alyaqoup, M.J.[c]

[a]Department of Computer Science, University of Mosul, Iraq
[b]Department of Computer Science, IIUM, Malaysia
[c]Technology and Infrastructure Department, Central Agency for Information Technology, Kuwait

Abstract

View references (18)

Lightweight block cipher algorithms are vital for constrained environment. There are three factors should be considered when you design lightweight block cipher algorithm which are security, performance and cost. In this paper, we have improved the cost factor of OLBCA algorithm by decreasing the number of Substitution box (S-box) without a major effect on other factors. Also, we have applied three attacks, which are differential, integral and boomerang attacks. From the result, it can be seen that our proposed algorithm has less cost than other algorithms and still secured. © 2015 IEEE.

SciVal Topic Prominence

Topic: Cryptography | Security of data | impossible differentials

Prominence percentile: 92.288

Author keywords

Differential cryptanalysis | Integral cryptanalysis and Boomerang cryptanalysis | Lightweight block cipher | Permutation Network | Substitution

Indexed keywords

Engineering controlled terms: Costs | Cryptography | Security of data | Substitution reactions

Engineering uncontrolled terms: Boomerang attack | Cost factors | Differential cryptanalysis | Integral cryptanalysis | Lightweight block ciphers | Permutation network | Substitution Box(S Box)

Engineering main heading: Algorithms

ISBN: 978-150900424-9
Source Type: Conference Proceeding
Original language: English
DOI: 10.1109/ACSAT.2015.11
Document Type: Conference Paper
Sponsors:
Publisher: Institute of Electrical and Electronics Engineers Inc.

References (18)

View in search results format >

1 Panasenko, S., Smagin, S.
Lightweight Cryptography: Underlying principles and approaches
(2011) *International Journal of Computer Theory and Engineering*, 3 (4). Cited 18 times.

2 Salim, S., Taha, I.
Lightweight block Ciphers: Comparative study
(2012) *Journal of Advanced Computer Science and Technology Research (JACSTR)*, 2, pp. 159-165. Cited 9 times.

3 Borghoff, J., Canteaut, A., Güneysu, T., Kavun, E.B., Knezevic, M., Knudsen, L.R., Leander, G., (...), Yalçin, T.
PRINCE - A low-latency block cipher for pervasive computing applications (Open Access)

(2012) *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 7658 LNCS, pp. 208-225. Cited 286 times.
http://springerlink.com.ezproxy.um.edu.my/content/0302-9743/copyright/2005/
ISBN: 978-364234960-7
doi: 10.1007/978-3-642-34961-4_14

View at Publisher

4 Knudsen, L., Leander, G., Poschmann, A., Robshaw, M.J.B.
PRINTcipher: A block cipher for IC-printing (Open Access)

(2010) *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 6225 LNCS, pp. 16-32. Cited 141 times.
ISBN: 3642150306; 978-364215030-2
doi: 10.1007/978-3-642-15031-9_2

View at Publisher

5 Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurin, Y., (...), Vikkelsoe, C.
PRESENT: An ultra-lightweight block cipher

(2007) *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 4727 LNCS, pp. 450-466. Cited 1060 times.
ISBN: 978-354074734-5

View at Publisher

6 Lim, C.H., Korkishko, T.
MCrypton - A lightweight block cipher for security of low-cost RFID tags and sensors

(2005) *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 3786 LNCS, pp. 243-258. Cited 140 times.
ISBN: 3540310126; 978-354031012-9