{tag} {/tag}International Journal of Computer Applications
Foundation of Computer Science (FCS), NY, USA

Volume 166
-
Number 8

Year of Publication: 2017

Authors:

Sufyan Salim Mahmood AlDabbagh

10.5120/ijca2017914088

{bibtex}2017914088.bib{/bibtex}

Abstract

Lightweight block cipher algorithms are vital for constrained environment. There are many applications need secured lightweight block cipher algorithm like credit card, E-passport and etc. This paper will propose 32-bit lightweight block cipher algorithm. It will apply two attacks differential and boomerang attack. The results will show that the proposed algorithm is resistance to these attacks.

References

1. Panasenko, S., & Smagin, S., “Lightweight Cryptography: Underlying Principles and Approaches”, International Journal of Computer Theory and Engineering, Vol 3 No.4, (2011).
2. S. Salim and I. Taha, "Lightweight block ciphers: comparative study," Journal of Advanced Computer Science and Technology Research (JACSTR), vol. 2, pp. 159-165, 2012.
3. J. Borghoff, et al., "PRINCE – A Low-Latency Block Cipher for Pervasive Computing Applications," in Advances in Cryptology – ASIACRYPT 2012. vol. 7658, Springer Berlin

Heidelberg, 2012, pp. 208-225.

4. L. Knudsen, et al., "PRINTcipher: A Block Cipher for IC-Printing," in Cryptographic Hardware and Embedded Systems, CHES 2010. vol. 6225, Springer Berlin Heidelberg, 2010, pp. 16-32.

5. A. Bogdanov, L. Knudsen, G. Leander, C. Paar, A. Poschmann, M. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT: An Ultra-Lightweight Block Cipher Cryptographic Hardware and Embedded Systems - CHES 2007." Vol. 4727, Springer Berlin / Heidelberg, 2007, pp. 450-466.

6. C. Lim and T. Korkishko, "mCrypton – A Lightweight Block Cipher for Security of Low-Cost RFID Tags and Sensors Information Security Applications." Vol. 3786, Springer Berlin / Heidelberg, 2006, pp. 243-258.

7. Z. Gong, S. Nikova, and Y. Law, "KLEIN: A New Family of Lightweight Block Ciphers RFID. Security and Privacy." Vol. 7055, Springer Berlin / Heidelberg, 2012, pp. 1-18.

8. W. Wu and L. Zhang, "LBlock: A Lightweight Block Cipher Applied Cryptography and Network Security." Vol. 6715, Springer Berlin / Heidelberg, 2011, pp. 327-344.

9. T. Suzaki, et al., "TWINE: A Lightweight Block Cipher for Multiple Platforms," in Selected Areas in Cryptography. vol. 7707, Springer Berlin Heidelberg, 2013, pp. 339-354.

10. J. Guo, T. Peyrin, A. Poschmann, and M. Robshaw, "The LED Block Cipher Cryptographic Hardware and Embedded Systems – CHES 2011." Vol. 6917, Springer Berlin / Heidelberg, 2011, pp. 326-341.

11. S. Panasenko and S. Smagin, "Lightweight cryptography: Underlying principles and approaches," International Journal of Computer Theory and Engineering, vol. 3, pp. 516-520, 2011.

12. E. Biham and A. Shamir, "Differential Cryptanalysis of DES Variants," in Differential Cryptanalysis of the Data Encryption Standard, ed: Springer, 1993, pp. 33-77.

13. J.-S. Kang, et al., "Practical and provable security against differential and linear cryptanalysis for substitution-permutation networks," ETRI journal, vol. 23, pp. 158-167, 2001.

14. E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," Journal of CRYPTOLOGY, vol. 4, pp. 3-72, 1991.

15. D. Wagner, "The boomerang attack," in Fast Software Encryption, 1999, pp. 156-170.

16. S. S. M. Aldabbagh, et al., " Lightweight Block Cipher Algorithms: Review Paper" in International Journal of Enhanced Research in Science, Technology & Engineering ISSN: 2319-7463, Vol. 5 Issue 5, May-2016.

Index Terms

Computer Science Security

Keywords

Lightweight block cipher, Substitution, Permutation Network, Differential cryptanalysis and Boomerang cryptanalysis.