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

Volume 139
-
Number 1

Year of Publication: 2016

Authors:

Ahmed M. Rayan, Ahmed A. Abdel-Hafez, Ismail Mohamed Hafez

10.5120/ijca2016908849
{bibtex}2016908849.bib{/bibtex}

## Abstract

In 1997 The National Institute of Standards and Technology (NIST) started a process to select a symmetric-key encryption algorithm instead of DES. NIST determined the evaluation criteria that would be used to compare the candidate algorithms depending on the analyses and comments received, NIST selected five finalist algorithms (RC6, MARS, Rijndael, Serpent and Twofish). At the end, NIST selected Rijndael as the proposed Advanced Encryption Standard algorithm (AES). Although Twofish algorithm based on Feistel structure and possesses a large security margin, it has some drawbacks as The Twofish structure is not easy to analyses, the mixing of various operations makes it hard to give a clean analysis and forces us to use approximation techniques. Moreover, The use of key-dependent S-Boxes adds complexity and greatly increase the effort required to write automated tools to search for characteristics (differentials, linear, …) of the structure. In this paper a proposal of a new Secure Symmetric-key Encryption (SSE) algorithm based on Feistel structure is produced to overcome the previous drawbacks and produce a provable secure algorithm.

## References

1. A. Biryukov, D. Wagner. “Slide Attacks,” Fast software Encryption (FSE’99), volume 1636, lecture notes in computer science, pp.245-259, springer, 1999.
2. P. JUNOD, Statistical Cryptanalysis of Block Ciphers (Lausanne, EPFL, 2005).
3. C. E. Shannon, “Communication theory of secrecy systems,” Bell System Technical Journal, vol. 28, pp. 656–715, Oct. 1949.
4. S. Harris1, C. Adams2, “Key-Dependent S-Box Manipulations” Selected Areas in Cryptography (SAC '99) Proceedings, LNCS 1556, Springer, 1999.
5. M. Matsui, R. Zuccherato,” Selected Areas in Cryptography,” 10th Annual International Workshop, SAC 2003, Ottawa, Canada, August 2003.
6. K. Gupta, I. Ghosh Ray, “On Constructions of MDS Matrices from Companion Matrices for Lightweight Cryptography,” CD -ARES 2013 Workshops, MoCrySEn, pp. 29-43, Springer 2013.
7. P. S. L. M. Barreto and V. Rijmen, “The ANUBIS block cipher,” 1st NESSIE Workshop, Heverlee, Belgium, Nov. 2000.
8. B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson, “Twofish: A 128-bit Block Cipher,” AES Round 1 Technical Evaluation CD-1: Documentation, National Institute of Standards and Technology, Aug 1998.
9. J. Nechvatal, E. Barker, D. Dodson, M. Dworkin, J. Foti and E. Roback,” Status report on the first round of the development of the advanced encryption standard,” Journal of Research of the NIST, vol. 104, no 5, Nechvatal et al., Sep-Oct, 1999.
10. S. Murphy, M. Robshaw,” Differential Cryptanalysis, Key- Dependent S-Boxes and Twofish,” Codes and Cryptography, Vol. 27, pp. 229-255, 2002.
11. B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson,” Twofish: A 128-bit Block Cipher,” Counterpane Systems, USA, AES submission, 15 June, 1998.
12. Top500 List - June 2015. http://www.top500.org/list/2015/06/
13. H. M. Heys, S. E. Tavares, “The Design of Substitution-Permutation Networks Resistant to Differential and Linear Cryptanalysis,” Proceedings of 2nd ACM Conference on Computer and Communications Security, Fairfax, Virginia, pp. 148–155, 1994.
14. H. M. Heys, S. E. Tavares, “Avalanche Characteristics of Substitution - Permutation Encryption Networks,” IEEE Trans. Comp., Vol. 44, pp. 1131-1139, Sept 1995.
15. ] M. Matsui, “ Linear cryptanalysis method for DES cipher,” in Advances in Cryptology -EUROCRYPT'93, Lecture Notes in Computer Science 765, Springer-Verlag, pp. 386–397, 1994.
16. X. Lai, “Higher order derivatives and differential cryptanalysis,” Communications and Cryptology, pp.227-233, Kluwer Academic Publishers, 1994.
17. L.R. Knudsen, “Truncated and Higher Order Differentials,” Fast Software Encryption, 2nd International Workshop Proceedings, pp. 196– 211, Springer- Verlag, 1995.
18. T. Jakobsen and L.R. Knudsen, “The interpolation attack on block ciphers,” Fast Software Encryption, LNCS 1267, pp. 28-40, Springer- Verlag, 1997.
19. G. Piret, M. Ciet, J. Quisquater, “Related key and slide attacks: Analysis, connections, and improvements,” Proceedings of the 23rd Symposium on IT in Benelux, pp. 315-325, 2002.

## Index Terms

Computer Science Algorithms

## Keywords

Symmetric-key cryptography; Block Ciphers; Substitution- Box; Diffusive Components; MDS; branch number.