Abstract

RC6 is a symmetric block cipher that possesses remarkable features, e.g., simple structure, Feistel structure and supporting for different block size, key length and number of rounds. However, some recent studies show that this cipher is subject to several cryptanalyses such as statistical attack, linear cryptanalysis, correlation attack and brute force attack. This paper proposes an enhancement version dubbed Chaotic Key Based RC6 (CKBRC6) that makes use of the Logistic map to generate round keys. Comprehensive assessments for the security of our proposal and fair comparisons between it and RC6 demonstrate the outperformance of the former in the domain of image encryption.

References

1. "3.5 million photos shared every minute in 2016 | Deloitte UK", Deloitte United Kingdom, 2018. [Online]. Available: https://www2.deloitte.com/uk/en/pages/press-releases/articles/3-point-5-million-photos-shared-e
1. Digital Image Encryption using Logistic Chaotic Key-based RC6

2. Zhang, X.; Wang, and Y. Zhang, "The visual internet of things system based on depth camera," in Proceedings of the Chinese Intelligent Automation Conference (CIAC ‘13), vol. 255, pp. 447–455, Yangzhou, China, 2013.

3. Chen, Chen, Ren, Yuzhuo, Kuo, C.-C. Jay, Big Visual Data Analysis, Scene Classification and Geometric Labeling, Springer Briefs in Signal Processing, 2016.

4. "3.5 million photos shared every minute in 2016 | Deloitte UK", Deloitte United Kingdom, 2018. [Online]. Available: https://www2.deloitte.com/uk/en/pages/press-releases/articles/3-point-5-million-photos-shared-every-minute.html. [Accessed: 05- Jun- 2018].

5. “Cyber Incident & Breach Trends Report - Online Trust Alliance”, Online Trust Alliance, 2018. [Online]. Available: https://www.otalliance.org/system/files/files/initiative/documents/ota_cyber_incident_trends_report_jan2018.pdf. [Accessed: 05- Jun- 2018].

6. Encrypted Traffic Analytics, Cisco Systems, 2018. [Online]. Available: https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/nb-09-encryptd-traf-anlytics-wp-cte-en.pdf. [Accessed: 05- Jun- 2018].

7. R. Rivest, M. Robshaw, R. Sidney, and Y.L. Yin, “The RC6 Block Cipher,” NIST AES Proposal, 1998.

8. R.L. Rivest, “The RC5 Encryption Algorithm,” Fast Software Encryption, 2nd International Workshop Proceedings, Springer-Verlag, pp. 86–96, 1995.

9. Miyaji A., Takano Y. “On the Success Probability of χ2-attack on RC6”. In Boyd C., González Nieto J.M. (eds) Information Security and Privacy. ACISP 2005. Lecture Notes in Computer Science, vol 3574. Springer, Berlin, Heidelberg, 2007.

10. H. Gilbert, H. Handschuh, A. Joux, and S. Vaudenay, “A Statistical Attack on RC6”, FSE 2000, LNCS 1978(2000), Springer-Verlag, 64–74, 2000.

11. L. Knudsen and W. Meier, “Correlations in RC6 with a reduced number of rounds”, FSE 2000, LNCS 1978, Springer-Verlag, 94–108, 2000.

12. A. Miyaji and M. Nonaka, “Cryptanalysis of the Reduced-Round RC6”, ICICS 2002, LNCS 2513, Springer-Verlag, 480–494, 2002.

13. N. Isogai, T. Matsunaka, and A. Miyaji, “Optimized χ2-attack against RC6”, ANCS 2003, LNCS 2846, Springer-Verlag, 2003.

14. S. Contini, R. Rivest, M. Robshaw, and Y. Yin, “The Security of the RC6 Block Cipher. v 1.0.”, 1998.

15. T. Shimoyama, M. Takenaka, and T. Koshiba, “Multiple linear cryptanalysis of a reduced round RC6," FSE 2002, LNCS 2365, Springer-Verlag, 76–88, 2002.

16. Boyar. J.. “Inferring sequences produced by a linear congruential generator missing low-order bits.” Journal of Cryptology, 1, 177–184, 1989.

17. Brickell, E.F. and A.M. Odlyzko. “Cryptanalysis: A survey of recent results.” Contemporary Cryptology: The Science of Information Integrity, 501–540, IEEE Press, Piscataway, NJ, 1992.

18. Frieze, A.M., J. Hastad, R. Kannan, J.C. Lagarias, and A. Shamir. “Reconstructing truncated integer variables satisfying linear congruence.” SIAM Journal on Computing, 17, 262–280, 1992.

19. Krawczyk, H.. “How to predict congruential generators.” Journal of Algorithms, 13, 527–545, 1992.
20. Plumstead, J.B. “Inferring a sequence generated by a linear congruence.” Proceedings of the IEEE 23rd Annual Symposium on Foundations of Computer Science. IEEE Press, New York, 153–159, 1982.
21. Plumstead, J.B.. “Inferring a sequence produced by a linear congruence.” Advances in Cryptology—CRYPTO’82, Lecture Notes in Computer Science, eds. D. Chaum, R.L. Rivest, and A.T. Sherman. Plenum Press, New York, 317–319, 1983.
22. Stern, J. “Secret linear congruential generators are not cryptographically secure.” Proceedings of the IEEE 28th Annual Symposium on Foundations of Computer Science. IEEE Press, New York, 421–426, 1987.
23. G. Alvarez, S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems", Int. J. Bifurcation Chaos, vol. 16, no. 8, pp. 2129-2151, 2006.
24. Marcel Ausloos, Michel Dirickx, “The Logistic Map and the Route to Chaos: From the Beginnings to Modern Applications”, Springer Science & Business Media. 2016.
25. R. Bose, A. Banerjee, "Implementing symmetric cryptography using chaos functions", Proc. 7th Int. Conf. Advanced Commun. Comp. (ADCOM), pp. 318-321, 1999.
26. Routo Terada and Eduardo T. Ueda. 2009. “A new version of the RC6 algorithm, stronger against
27. 

Index Terms

Computer Science Security

Keywords

RC6, Logistic map, Chaotic encryption key.