Evolution in Networks and Computer Communications Journal
Number 2 - Article 2

Year of Publication: 2011

Authors:

Nikesh Bajaj

{bibtex}encc010.bib{/bibtex}

Abstract

The Global System for Mobile communication, GSM voice calls are encrypted using a family of algorithms collectively called A5. A5/1 is the stream cipher which encrypts the information transmitted from mobile user. Initially A5 algorithm was kept secret to ensure the security but as algorithm was disclosed many cryptanalytic attacks were proposed and proved the A5 algorithm cryptographically weak. In this paper, proposed enhanced A5/1 is described and it's analysis with different parameters is done. Enhanced A5/1 is proposed to make it robust and resistive to the attacks. Modification is done in two ways (1) feedback tapping mechanism which is enhanced by variable taps for LFSR (Linear Feedback Shift Register) and random shuffling of

LFSRs, which increases the complexity of the algorithm without compromising the properties of randomness and (2) clocking rule. The modification has been proposed keeping the ease of implementation in mind. This modified algorithm has been simulated in MATLAB and tested its randomness properties by 'Randomness test suit' given by NIST-National Institute of Standard and Technology and obtained satisfactory results. Further analysis of A5/1 is done by varying it's parameters to achieve better results.

Reference

1. G. Rose, A précis of new attacks on GSM encryption, Qualcomm, Australia, 10 september 2003.
2. R. Mita, G. Palumbo and M. Poli, Pseudo-random sequence generators with improved inviolability performance, IEE Proceedings of Circuits, Devices and Systems, vol. 153, pp 375-382, 2006.
3. J. Golic, Cryptanalysis of alleged A5 stream cipher, Advances in Cryptology, proceedings of EUROCRYPT'97, LNCS, vol. 1233, pp. 239–255, Springer-Verlag, 1997.
4. A. Biryukov, A. Shamir, and D. Wagner, Real time cryptanalysis of A5/1 on a PC, Advances in Cryptology, proceedings of Fast Software Encryption'00, LNCS, pp. 1–18, Springer-Verlag, 2001.
5. E. Biham, and O. Dunkelman, Cryptanalysis of the A5/1 GSM stream cipher, Progress in Cryptology, proceedings of INDOCRYPT'00, LNCS, pp. 43–51, Springer-Verlag, 2000.
6. P. Ekdahl, and T. Johansson, Another attack on A5/1, IEEE Transactions on Information Theory, vol. 49, pp. 284-289, 2003.
7. A. Maximov, T. Johansson, and S. Babbage, An improved correlation attack on A5/1, proceedings of SAC 2004, LNCS, vol. 3357, pp. 1–18, Springer-Verlag, 2005.
8. E. Barkan, and E. Biham, Conditional estimators: an effective attack on A5/1, proceedings of SAC 2005, LNCS, vol. 3897, pp. 1–19, Springer-Verlag, 2006.
9. S. E. AlAschkar and M. T. El-Hadidi, Known attacks for the A5/1 algorithm: a tutorial, International Conference on Information and Communications Technology (ICICT'03), pp. 229-251, 2003.
10. B. Schneier, Applied Cryptography, protocols algorithm and souce code in c, Second edition, John Wiley & Sons Inc.
11. Andrew Rukhin et all, NIST, A Statistical Test Suit for random and pseudorandom number generators for cryptographic applications. NIST Special Publication 800-22 , with revisions dated May 15, 2001.
12. Recommendation GSM 02.09, European Telecommunications Standards Institute (ETSI), Security aspects.
13. M. Galanis, P. Kitsos, G. Kostopoulos, N. Sklavos, O. Koufopavlou and C. E. Goutis, Comparison of the hardware architectures and FPGA implementations of stream ciphers, proceedings of the 11th IEEE International Conference on Electronics, Circuits and Systems (ICECS'04), pp. 571- 574, 2004.
14. W. Ahmad, O, Farooq and Izharuddin, Stream Ciphering using a novel Pseudo-Random generator, the ICFAI University Journal of Electronics Engineering, vol 1, No.1, 2008.
15. A. Braeken, Cryptographic properties of boolean functions and s-boxes, Katholieke

Universiteit Leuven, Belgium, Ph.D Thesis, March 2006.

Index Terms

Computer Science Communications

Key words

A5/1

GSM security

stream cipher

randomness tests