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.
12. Recommendation GSM 02.09, European Telecommunications Standards Institute (ETSI), Security aspects.
15. A. Braeken, Cryptographic properties of boolean functions and s-boxes, Katholieke
Effects of Parameters of Enhanced A5/1


Index Terms

Computer Science

Communications

Key words

A5/1

GSM security

stream cipher

randomness tests