A MODIFIED STREAM GENERATOR FOR THE GSM ENCRYPTION ALGORITHMS A5/1 AND A5/2 (ThuPmOR9)

Author(s) :

Imran Erguler (Dogus University, Turkey)
Emin Anarim (Bogazici University, Turkey)

Abstract :

A5/1 and A5/2 are the GSM encryption algorithms that protect user data transmission over air. However, both of the A5/1 and A5/2 were cryptanalized by using different attack techniques such as time−memory trade off, divide and conquer and correlation attacks. In this study, we present a modified version of the A5/1 and A5/2 with offering security improvements to the vulnerabilities of the algorithms. By changing just the clocking mechanism of the shift registers used in the algorithms, it is shown that known attacks techniques become impractical.

Menu