PROTECTED COMMUNICATION IN THE GSM STANDART

Yu.B. Nechaev, B.N. Voronkov, Ye.S. Dolbilova,
A.V. Dudchenko

In the view of low crypto steadfastness of crypto algorithm A5/1, its modification is offered. This modification allows to increase key space and to ensure protection against attack based on plain or fitted text. For this purpose, supplementary cryptographic transformations based on finite field theory are realized on plain text and produced pseudorandom sequence.