Abstract:

In this work we study cryptanalysis one of the most current stream ciphers A5/1. The cipher is used to provide mobile communication privacy in the GSM cellular telephone standard. An essential element of the cipher A5/1 is LFSR(Linear feedback shift register) which is used in stream ciphers because it produces a sequence of bits with high periodicity, has good statistical properties and is easily analyzed using various algebraic methods. At work, we describe and implement three known-plaintext attacks on the cipher. The first two attacks are of the type Guess and Determine and the last one is correlation attack. The focus of the work is cryptanalysis by Golić, which assumes only 64 bits of plaintext. The character of implementation allows to split the work and use parallel-computing, making it possible to use the program in practice. At the end of the work we devote to correlation attack, that is considerably faster, but it assumes knowledge of the relatively large amount of plaintext.