Stream Ciphers and Number Theory: Sidelńikov Sequences

Arne Winterhof

Johann Radon Institute for Computational and Applied Mathematics
Austrian Academy of Sciences (Linz)

Let $m_1, m_2, \ldots$ be a binary *message* represented as a string of bits, then a *cipher* consists of two processes: *encryption* and *decryption*. In a *stream cipher* each bit m_i is enciphered with the element k_i of a *keystream* $k_1, k_2, \ldots$ to $c_i \equiv m_i + k_i \bmod 2$. The *ciphertext* $c_1, c_2, \ldots$ can be converted back by adding the keystream to the ciphertext ($m_i \equiv c_i + k_i \bmod 2$).

The security of a stream cipher depends on the randomness properties of the keystream. The cryptographic properties of many classes of keystreams can be analyzed using number theoretic methods.

In this talk we analyze the following keystream introduced by Sidelńikov: Let q be an odd prime power, α a primitive element of the finite field $\mathbb{F}_q$, and let η denote the *quadratic character* of $\mathbb{F}_q$, i.e.,

$$\eta(\alpha^i) = (-1)^i, \quad i = 0, 1, \ldots, q-2,$$

and $\eta(0) = 0$. Then the *Sidelńikov sequence* is defined to be the $(q-1)$-periodic binary sequence (s_n) with

$$s_n = \begin{cases} 1 & \text{if } \eta(\alpha^n + 1) = -1, \\ 0 & \text{otherwise,} \end{cases} \qquad n = 0, 1, \ldots. \tag{1}$$

The *linear complexity* $L(a_n)$ of a binary sequence (a_n) is the smallest positive integer L such that there are constants $c_1, \ldots, c_L \in \{0, 1\}$ satisfying

$$a_n \equiv c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_L a_{n-L} \bmod 2 \quad \text{for all } n \geq L.$$

The Linear complexity provides information on the predictability and thus unsuitability for cryptography. Hence, a low linear complexity has turned out to be an undesirable feature of keystreams.

We determine the exact value of the linear complexity of the sequence (1) in many cases. The proofs are based on number theoretic results: bounds on *character sums* and formulas for *cyclotomic numbers*.

Besides linear complexity we also discuss *autocorrelation* properties of Sidelńikov sequences.