This thesis is devoted to several important problems that arise in the context of design and analysis of key-stream generators for stream ciphers. First, we analyze two common building blocks that are used in key-stream generators. These are nonlinear logical functions and clock-controlled linear feedback shift registers (LFSR). A newly introduced tensor transform and its instances prove to be helpful for analyzing the security of the functions. Special cases of this approach not only provide easy proofs for known important relations in the theory of algebraic normal, numerical normal and Walsh transforms, but also allow to establish some new properties of these transforms. We also propose a new type of tensor transform, the so-called probabilistic transform, giving an important insight in certain probabilistic properties of Boolean functions that are discussed. Another new type of tensor transform that we propose, is the weight transform. It relates a Boolean function to the weights of its subfunctions. We also introduce a tensor transform over an arbitrary finite field that allows a generalization of the algebraic normal and Walsh transforms to the case of functions over GF($q$).

Further, we study correlation properties of Boolean functions. We show how correlation coefficients that provide an estimate for correlation dependencies of a Boolean function, can be obtained from its weight transform. It is proved that the number of fixed-order product terms in the ANF of a balanced Boolean function depends on its correlation coefficients. We also prove that highly resilient Boolean functions can not be approximated with a function that is nondegenerate on few variables. A new probabilistic function of a Boolean function is also introduced. This function estimates the probabilistic distribution of output bits of the function if the distribution of the arguments, the function depends on, is known. We suggest a characteristic for a balanced Boolean function that measures its ability to compensate a nonuniform distribution of the input. Resilient functions are proved to have good compensating qualities.

The other building block being analyzed is a clock-controlled LFSR. We estimate the period of its output sequence when the feedback polynomial is irreducible and the structure of the control sequence is arbitrary. A sufficient condition for this period to reach its maximal value is formulated. Some specific configurations of clock-controlled arrangements with a maximal period of the output sequence are defined. Relevant recommendations for estimating the linear complexity are also presented.

Moving slightly away from building blocks, we construct a key-stream generator based on the one suggested by Geffe. Unlike the Geffe generator that has three binary input $m$-sequences, this generator runs over the field GF($q$) and combines multiple inputs having arbitrary periods. In particular, this implies that clock-controlled shift registers can be used as inputs. The original Geffe generator can not be used for key-stream generation since its combining function is zero-order correlation immune and correlation attacks can easily be applied. Using clock-controlled registers and multiple inputs makes the new generator immune against fast correlation attacks and less susceptible to basic attacks. We analyze some relevant algebraic properties of the suggested generator.

Finally, we develop several statistical attacks on stream ciphers. Our first algorithm uses invariant statistical tests to implement the fast correlation attack on the initial state of the LFSR which output is XORed with the random noise. The other algorithm tests a ciphertext for key-stream overlaps. This is done by constructing nonrandomized and randomized most powerful tests. If the cryptanalyst is dealing with blocks of key-stream or ciphertext then it may be helpful to use statistical procedures for selecting the most probable outcomes from the multinomial population. We construct new procedures that are based on the calculation of reduced frequencies. That makes them more efficient when the total number of outcomes is big compared to the amount of memory available. Theoretical results obtained include the limit distribution for reduced frequencies.