Abstract. In this paper, we investigate the existence and invariant of algebraic attacks, which have been recently shown as an important cryptanalysis method for symmetric-key cryptographical systems. For a given boolean function f in n variables and two positive integers d and e, we observe that the sufficient condition $d + e \geq n$, shown in [8] or [9], cannot guarantee the existence of a function g with $deg(g) \leq d$ such that $deg(fg) \leq e$ where $fg \neq 0$. Based on this observation, we find a sufficient and necessary condition for the existence of such a multiplier g, which also yields an algorithm to construct them. The algorithm is more efficient when the polynomial basis is employed for linearization than the boolean basis is employed. We then introduce the concept of *invariants* of algebraic attacks in terms of the algebraic security criterion, proposed by Courtois and Meier in 2003, and characterize these invariants. Applying this criterion to the hyper-bent functions, we derive that for a randomly selected boolean function g, the probability of the degree of fg is greater than or equal to $deg(f) = n/2$ is close to 1 where f is a given hyper-bent function in n variables. The tool for establishing our assertions in this paper is to use the (discrete) Fourier transform of boolean functions in terms of technics of analysis of pseudo-random sequences.
Key words. Algebraic attacks, low degree approximation, linearization, (discrete) Fourier transform, invariant, and hyper-bent function.