On Division Property and Degree Bounds

Aleksei Udovenko

Abstract

Computing or bounding the algebraic degree of iterated functions is a fundamental problem in Boolean functions. Especially important it is in symmetric-key cryptography, where a low algebraic degree of a cipher leads to the so-called integral distinguishers and key recovery attacks. Furthermore, fine-grained algebraic deficiencies such as missing monomials in the algebraic normal form can also be exploited and therefore need to be detected by the designers.

Techniques for estimating the algebraic degree and finding missing monomials significantly evolved in the recent decade. Classic approaches require only a small amount of information about the iterated functions, such as their algebraic degree, the algebraic degree of their compositional inverse, or the algebraic degree of their graph indicator. However, full knowledge of a function's structure leads to much more precise bounds. The state-of-the-art technique for exploiting this information is the so-called *division property*, alternatively described as *monomial trails*.

This talk will summarize the most influential degree bounds and show their relation to division property variants, as well as describe techniques for proving lower bounds.