On the Univariate and Algebraic Degrees of Iterated Power Functions

Clémence Bouvier[1,2], Anne Canteaut[2], and Léo Perrin[2]

[1] Sorbonne Université, France
[2] Inria, France
clemence.bouvier@inria.fr, anne.canteaut@inria.fr, leo.perrin@inria.fr

Abstract. New symmetric primitives are being designed to address a novel set of design criteria. Instead of being executed on regular processors or smartcards, they are instead intended to be run in abstract settings such as multi-party computations. This implies in particular that these new primitives are described using operations over large finite fields. As the number of primitives grows, it is important to better understand the properties of these operations.

In this paper, we investigate the algebraic degree of one of the first such block ciphers, namely MiMC. It is composed of many iterations of a simple round function, which consists of an addition and of a low-degree power permutation applied to the full state, usually $x \mapsto x^3$. We show in particular that, while the *univariate* degree increases predictably with the number of rounds, the *algebraic* degree (aka multivariate degree) has a much more complex behaviour, and simply stays constant during some rounds. Such *plateaus* slow down slightly the growth of the algebraic degree.

We present a full investigation of this behaviour. First, we prove some lower and upper bounds for the algebraic degree of an arbitrary number of iterations of MiMC and of its inverse. Then, we combine theoretical arguments with simulations to prove that the upper bound is tight for up to 16265 rounds. Using these results, we improve the higher-order differential attack presented by the authors of MiMC to cover one or two more rounds.