# On the Properties of S-boxes

Léo Perrin

Monday, 18th of March 2013

S-boxes are key components of many symmetric cryptographic primitives. Among them, some block ciphers and hash functions are vulnerable to attacks based on differential cryptanalysis, a technique introduced by Biham and Shamir in the early 90's. Resistance against attacks from this family depends on the so-called differential properties of the S-boxes used.

When we consider S-boxes as functions over finite fields of characteristic 2, monomials turn out to be good candidates. In this Master's Thesis, we study the differential properties of a particular family of monomials, namely those with exponent $2^t - 1$. In particular, conjectures from Blondeau's PhD Thesis are proved.

More specifically, we derive the differential spectrum of monomials with exponent $2^t - 1$ for several values of $t$ using a method similar to the proof Blondeau *et al.* made of the spectrum of $x \mapsto x^7$. In the first part of the presentation, we provide the mathematical and cryptographic background necessary while a second one contains the proofs of the spectra we extracted. Finally, some observations which, among other things, connect this problem with the study of particular Dickson polynomials are mentioned in the last part.

**Keywords:** Symmetric cryptography, Differential uniformity, Differential spectrum, Kloosterman sum, Power function, Roots of trinomial, $x \mapsto x^{2^t-1}$, Dickson polynomial, Differential Cryptanalysis.