Recent trends on Boolean Functions

Sihem Mesnager, University of Paris VIII

Lecture 1 **On hyper-bent functions**

Hyper-bent Boolean functions were introduced in 2001 by Youssef and Gong (and initially proposed by Golomb and Gong in 1999 as a component of S-boxes) to ensure the security of symmetric cryptosystems but no cryptographic attack has been identified till 2016. Hyper-bent functions have properties still stronger than the well-known bent functions which were already studied by Dillon and Rothaus more than four decades ago. Hyper-bent functions are very rare and whose classification is still elusive. Therefore, not only their characterization, but also their generation are challenging problems. In the context of filtered LFSRs, Canteaut and Rotella showed at the 2016 FSE conference that when considering fast correlation attacks, the relevant criterion should no longer be nonlinearity, but rather generalized nonlinearity. Indeed, they showed that if $f + Tr(\lambda x^k)$ (where "Tr" stands for the absolute trace function over F_{2^n}) is biased, then we can apply a fast correlation attack to recover x_0^k where x_0 denotes the initial state. If k is coprime to $2^n - 1$, then the attack recovers the initial state. Moreover, the case when k is not coprime to $2^n - 1$ also leads to another attack and a new criterion to evaluate the security of filtered LFSR. The new criterion given on filtered LFSRs has thus revived interest in the topic of hyperbent functions. In this talk, we shall give a complete survey on all what is known on hyper-bent Boolean functions. We will also present very recent results (2018-2019) on hyper-bent functions in arbitrary characteristic as well as generalized hyper-bent functions. Albert's classification of the possible endomorphism algebras of abelian varieties (if time permits, I'll also touch upon Shimura's more precise results and the theory of complex multiplication).

Lecture 2 **On plateaued functions**

Plateaued functions are very important cryptographic functions due to their various desirable cryptographic characteristics. We point out that plateaued functions are more general than bent functions (that is, functions with maximum nonlinearity).

Some Boolean plateaued functions have large nonlinearity, which provides protection against fast correlation attacks when they are used as combiners or filters in stream ciphers, and contributes, when they are the component functions of the substitution boxes in block ciphers, to protection against linear cryptanalysis. P-ary plateaued functions have attracted recently some attention in the literature and many activities on generalized p-ary functions have been carried out. The first aim of this talk is to present several various tools to handle the plateaued-ness property of p-ary functions in order to clarify their structure. The second aim of the talk is present an overview on various notions of plateaued functions. We shall discuss weakly regular plateaued functions, generalized plateaued functions and admissible plateaued functions.

Lecture 3 **On Boolean functions with restricted input**

Recently, Carlet, Méaux and Rotella have studied the main cryptographic features of Boolean functions when, for a given number n of variables, the input to these functions is restricted to some subset E of $\mathbb{F}_2^n$. Their study includes the particular case when E equals the set of vectors of fixed Hamming weight, which is important in the robustness of the Boolean function involved in the FLIP stream cipher. In this talk, we will present a complete state-of-the-art on Boolean functions with restricted input. We shall discuss the nonlinearity of Boolean functions with restricted input and present recent results related to the analysis of this nonlinearity improving the upper bound given by Carlet et al.

Lecture 4 **On boomerang uniformity of S-boxes**

At Eurocrypt'18, Cid, Huang, Peyrin, Sasaki, and Song introduced a new tool called Boomerang Connectivity Table (BCT) for measuring the resistance of a block cipher against the boomerang attack which is an important cryptanalysis technique introduced by Wagner in 1999 against block ciphers.

Next, an important parameter (related to the BCT for cryptographic Sboxes) called boomerang uniformity has been introduced. The purpose of this talk is to present a complete state-of-the-art on boomerang uniformity of vectorial Boolean functions (or Sboxes) as well as recent results in this topic.