ABSTRACT

Boolean functions play a fundamental role in the design of symmetric key primitives, particularly in stream ciphers, which have become significant in lightweight cryptographic applications due to their low computational complexity. In EUROCRYPT 2016, Méaux et al. introduced a stream cipher, FLIP, which is based on a filter permutator, where the input to the filtering Boolean function is restricted to constant Hamming weight vectors $x \in \mathbb{F}_2^n$. In this thesis, we focus on the construction of Weightwise Almost Perfectly Balanced (WAPB) and Weightwise Perfectly Balanced (WPB) Boolean functions, which exhibit (almost) balance over the sets $\mathsf{E}_{k,n} = \{x \in \mathbb{F}_2^n : \mathsf{w_H}(x) = k\}$ for all $0 \leq k \leq n$. These functions are of particular interest in the context of FLIP cipher framework.

The following provides a brief description of our work on the construction and analysis of the WAPB/WPB Boolean functions.

1. We present several constructions of WAPB Boolean functions based on Siegenthaler's method. We introduce a new class of WAPB Boolean functions, known as *complementary weightwise almost perfectly balanced (CWAPB)* Boolean functions, and identify the necessary and sufficient conditions under which the function is special WAPB (SWAPB) as defined by Gini and Méaux in their INDOCRYPT 2022 paper.

   Specifically, we propose a method for constructing a class of n variable WAPB functions by extending the support of a known n_0 variable WAPB Boolean function, where $n = n_0 2^m$ for some integer m, with n_0 being odd. This approach, combined with an elegant construction of WPB functions proposed by Mesnager and Su, gives a generalized framework for constructing WAPB functions that is applicable for arbitrary n.

2. For two Boolean functions $f : \mathbb{F}_2^m \to \mathbb{F}_2$ and $g : \mathbb{F}_2^n \to \mathbb{F}_2$, we define the direct sum $h(x, y) = f(x) + g(y)$ as a Boolean function over $\mathbb{F}_2^{m+n}$ for $x \in \mathbb{F}_2^m$ and $y \in \mathbb{F}_2^n$. We study the direct sum construction of WAPB and WPB Boolean functions and establish a general condition under which the direct sum h results in a WAPB/WPB Boolean function. Given f and g each being either WAPB or WPB, we investigate two cases under which h is WAPB or WPB. Our findings refine the earlier result by

Carlet et al. on the construction of WPB functions and compute the weight of h over $\mathsf{E}_{k,n}$ for $k \in [1, n-1]$ earlier proved by Zhu et al. that the direct sum of several WPB functions.

We propose a recursive construction of WPB functions based on direct sum and establish an upper bound to the algebraic immunity of the resulting functions. The constructed functions also exhibit high nonlinearity over $\mathbb{F}_2^n$. Furthermore, we define another subclass of WAPB functions called *alternating WAPB (AWAPB)*, which enable a recursive direct sum construction method for generating WAPB functions.

3. We propose a general construction method for a class of WAPB Boolean functions based on the action of a cyclic permutation group $P = \langle \pi \rangle$, where $\pi \in \mathbb{S}_n$ is a permutation on n elements, acting on $\mathbb{F}_2^n$. In particular, we studied the WAPB/WPB Boolean functions generated due to the action of two significant permutation groups, $\langle \psi \rangle$ and $\langle \sigma \rangle$, where ψ is a distinct binary-cycle permutation and σ is a rotation. When $n = 2^m$ for $m > 0$, a particular case of this construction is a WPB Boolean function in 2^m variables, proposed by Liu and Mesnager in Design, Codes and Cryptography, 2019. We evaluate the nonlinearity and weighted nonlinearities of the functions obtained from this construction, and as a result, the derived bounds improve upon those established by Liu and Mesnager. We theoretically analyze the cryptographic properties of the WAPB functions derived from these permutations and experimentally evaluate their nonlinearity parameters for n between 4 and 10.