On the number of inequivalent APN functions

Yue Zhou

September, 2021

Department of Mathematics, National University of Defense Technology,
410073 Changsha, China

A function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is called *almost perfect nonlinear* (APN, for short), if the map

$$x \mapsto f(x+a) - f(x),$$

is 2-to-1 for each nonzero $a \in \mathbb{F}_{2^n}$.

APN functions play an important role in the design of block ciphers as they offer the strongest resistance against differential cryptanalysis. In this talk, first I will give an overview of the construction of known APN functions. Then we will look at a construction by Taniguchi (2019) and will show that it provides at least $\frac{\varphi(m)}{2}\left\lceil\frac{2^m+1}{3m}\right\rceil$ inequivalent APN functions on $\mathbb{F}_{2^{2m}}$, where φ denotes Euler's totient function. This is a great improvement of previous results: for even m, the best known lower bound has been $\frac{\varphi(m)}{2}\left(\lfloor\frac{m}{4}\rfloor+1\right)$, for odd m, there has been no such lower bound at all. In the end, I will also propose some open questions.

This talk is based on two joint works with Christian Kaspers at Otto-von-Guericke University of Magdeburg.