

Lecturer: Samed Bajrić, University of Primorska

Title: On Generalized Bent Functions With Dillon's Exponents

Abstract: In this talk we investigate the possibility of constructing bent functions over fields with odd characteristic. We show that the necessary and sufficient bent conditions for both the Boolean function of the form $f(x) = \text{Tr}_1^{2k}(x^{2^k-1} + ax^{r(2^k-1)})$ and the associated mapping $F(x) = \text{Tr}_k^{2k}(x^{2^k-1} + ax^{r(2^k-1)})$, where $F : GF(p^{2k}) \rightarrow GF(p^k)$, are very similar and can be expressed in terms of the image of a set V used in the direct sum decomposition of $GF(p^{2k})$. Furthermore, we observe that multiple output bent functions are easily constructed using the Maiorana-McFarland method.