New construction of highly nonlinear resilient S-boxes via linear codes

Haixia ZHAO, Yongzhuang WEI

Frontiers of Computer Science, DOI: 10.1007/s11704-020-0182-y

Problems & Ideas

- Problems of constructing highly nonlinear resilient S-boxes without concatenating a large number of $n/2$ variables affine subfunctions
  - How to construct the component functions of S-box?
  - How to construct S-boxes satisfy the above properties?
- Ideas: Following the idea of non-overlap spectra, two families of disjoint linear codes with different code lengths are utilized in the construction of the component functions
  - The component functions are constructed via disjoint linear codes
  - Basing on the component functions , S-boxes satisfy the above properties are constructed

Main Contributions

- **New construction of highly nonlinear resilient function via linear codes.**

An example of Boolean function f with 16 variables:
➢ The resilient order of f is 2 ➢ $N_f \geq 2^{15} - 2^9$ ➢ $\deg(f) \geq 11$

- **New construction of highly nonlinear resilient S-boxes via linear codes.**

An example of (16, 2) S-box F :
➢ The resilient order of F is 2, $N_F \geq 2^{15} - 2^9, \ \deg(F) \geq 11$ ➢ F contains 40 affine subfunctions with 8 variables, whose proportion of all subfunctions with other 8 variables kept fixed is $40 / 2^8 \approx 15.625\%$