研究方向(x)：密码学与信息安全

➢ 优良密码性质的布尔函数构造

- ✓ 构造了三类具有优良密码学性质的布尔函数，这些函数不但代数免疫最优，而且在平衡性、代数次数、快速代数免疫度上都表现良好，特别是在非线性度上，将高出Lobanov界的部分从$O(k\cdot 2^k)$提升至$O(k^2\cdot 2^k)$。

➢ 布尔函数的代数免疫性质研究

- ✓ 证明两类重要布尔函数的仿射等价性，揭示其间的本质联系。
- ✓ 证明了涂-邓猜想在$w(t)=5$时成立。
- ✓ 证明了变元数量为2^m+2和2^m+3时择多函数的快速代数免疫度。

研究方向(x)：密码学与信息安全

- Y. Chen, F. Guo, J. Ruan. Constructing Odd-Variable RSBFs with Optimal Algebraic Immunity, Good Nonlinearity and Good Behavior Against Fast Algebraic Attacks. Discrete Applied Mathematics, 2019, vol 262, pp.1-12
- Y. Chen, L. Zhang, F. Guo, et al., Fast Algebraic Immunity of 2^m+2 & 2^m+3 variables Majority Function, Cryptology ePrint Archive, https://eprint.iacr.org/, Report 2019/286, 2019
- Y. Chen, J. Ruan, X. He, Constructing Even-variable RSBFs with Higher Nonlinearity, Optimal AI and Good FAI. Advances in Cryptology, ChinaCrypt 2019, pp.107-121
- Y. Chen, L. Zhang, D. Tang, et al., Translation Equivalence of Boolean Functions Expressed by Primitive Element. IEICE Trans. Fundam. Electron., Commun. Comput. Sci., 2019, E102-A(04): 672-675
- Y. Chen, F. Guo, H. Xiang, et al., Balanced Odd-variable RSBFs with Optimum AI, High Nonlinearity and Good Behavior Against FAAs. IEICE Trans. Fundam. Electron., Commun. Comput. Sci., 2019, E102-A(06): 818-824.
- Y. Chen, F. Guo, Z. Gong, et al., One Note about the Tu-Deng Conjecture in case w(*t*)=5. IEEE Access, 2019, vol 7, pp.13799-13802
- Y. Chen, L. Lin, L. Liao, et al., Constructing higher nonlinear odd-variable RSBFs with optimal AI and almost optimal FAI, IEEE Access, 2019, vol 7, pp.133335-133341