


Alkhzaimi HA, Knudsen LR. **Cryptanalysis of Selected Block Ciphers.** Kgs. Lyngby: Technical University of Denmark (DTU), 2016. 140 p. (DTU Compute PHD-2015; No. 360).


Bogdanov A, Moradi A, Yalcin T. **Efficient and side-channel resistant authenticated encryption of FPGA bitstreams**. In Proceedings of 2012 International Conference on Reconfigurable Computing and FPGAs (ReConFig). IEEE. 2013. Available from, DOI: 10.1109/ReConFig.2012.6416743


Bogdanov A, Kavun EB, Tischhauser E, Yalcin T. Efficient reconfigurable hardware architecture for accurately computing success probability and data complexity of linear attacks. In International Conference on Reconfigurable Computing and FPGAs (ReConFig) 2012. IEEE. 2012. Available from, DOI: 10.1109/ReConFig.2012.6416744