Fault-tolerant linear collision attack: A combination with correlation power analysis.


Summary: The framework of test of chain was presented by Bogdanov et al. in 2012, which combines collision attack with divide-and-conquer side-channel attacks. Its success rate highly depends on the correctness of the chain established from collision attack. In this paper, we construct a fault-tolerant chain which consists of 15 paths, and each path includes only one step. In order to decrease the misjudgments, we combine this chain with correlation power analysis, linear collision attack and search. So the fault-tolerant linear collision attack is proposed. Our experiments show that the new attack is more efficient than the method of Bogdanov et al. Furthermore, we give a fault-identification mechanism to find the positions of wrong key bytes, and thus the subsequent search space can be reduced a great deal. Finally, the choice of threshold in correlation power analysis is discussed in order to optimize our attack.

Keywords: power analysis attack; correlation power analysis; test of chain; linear collision attack
doi:10.1007/978-3-319-06320-1_18