Fitness Landscape Analysis for Cryptographic Boolean Functions

Boolean functions (i.e. mappings from n-bit strings to a single output bit) play a fundamental role in the design of symmetric ciphers. Often, the security of a cipher model can be reduced to the analysis of the cryptographic properties of the underlying Boolean functions. However, due to the super-exponential size of the search space, it is unfeasible to exhaustively search for the Boolean functions with the best combination of cryptographic properties. Hence, one often resorts to metaheuristic optimization techniques, such as Genetic Algorithms (GA), to efficiently find Boolean functions with a good trade-off of cryptographic properties [1]. A common problem with this approach is to parametrize the components of the GA (e.g. crossover operators, initialization strategy, etc.) with respect to the characteristics of the search landscape of Boolean functions, to avoid getting stuck in local optima. This entails understanding the graph structure of the local optima within the search landscape, which can be done by using Fitness Landscape Analysis (FLA) techniques [2].

The aim of this project is to implement and test a local search algorithm to sample the fitness landscape of Boolean functions, focusing on the cryptographic properties of balancedness and nonlinearity. The goal is to run local search from a large random sample of Boolean functions in order to construct a Local Optima Network for this fitness landscape, from which insights can be gained concerning the parametrization of GA.

References

[1] M. Djurasevic, D. Jakobovic, L. Mariot, S. Picek: A survey of metaheuristic algorithms for the design of cryptographic Boolean functions. Cryptogr. Commun. 15(6): 1171-1197 (2023)

[2] D. Jakobovic, S. Picek, M. S. R. Martins, M. Wagner: Toward more efficient heuristic construction of Boolean functions. Appl. Soft Comput. 107: 107327 (2021)