

Question Number 10

Find the best 4-round trail for your Sypher004 using Gurobi. Concentrate on how the constraints for different rounds are to be generated taking care of your permutation layer. Submit your .lp and .sol files.

Recall: We are not taking the properties of the Sbox into consideration in the current MILP model.

Solution. Solution is in files directory.