CS553 Cryptography

BitBees

Question 9

The objective is to minimize the number of active s-boxes in the trail. Hence, the objective function of the LP-Problem would be $\Sigma_{i\in[0,5],j\in[0,4]}a_{ij}$, where a_{ij} denotes the j^{th} s-box in the i^{th} round.

Constraints are set to obey the following conditions:

- If an s-box has a non-zero input, it is active.
- If a_{ij} is 1, s-box has non-zero input.
- Input difference must result in output difference and vice-versa.
- At least one s-box must be active.

In the MILP model described above, the model attempts to simply minimize the number of active s-boxes by possibly considering invalid transitions through the s-box too. This is because no constraints have been set to consider the s-box properties.

This would mean that our optimizer may not return a valid solution, as is the case when it is run on the "Sypher004" described in the lectures. Here are how the files are organized:

- milp_sypher004.lp - The LP file to sypher004 discussed in class.
- bitbees_milp_sypher004.lp - The LP file to sypher004 implemented the BitBees way
- sypher004.sol - Solution file to Gurobi optimized milp_sypher004.lp
- bitbees_sypher004.sol - Solution file to Gurobi optimized bitbees_milp_sypher004.lp