



SAT-based S-Box Search

Advisor: **Manfred Scheucher** and **Maria Eichlseder**

Motivation

Substitution boxes (**S-boxes**) are the small non-linear look-up tables used in many symmetric primitives (block/stream ciphers and hash functions). Good S-boxes aim for low differential uniformity (APN is optimal), high nonlinearity, and an appropriate algebraic degree to resist classical attacks such as **differential and linear cryptanalysis**. When searching for S-boxes, many candidates are essentially the same up to simple input/output changes. Two standard ways to capture isomorphisms are **extended-affine (EA)** and the more general **CCZ equivalence**. Treating equivalent S-boxes as one object drastically reduces the search space.

In this project, we start from an existing **SAT/CNF formulation** with a partial symmetry breaking and extend it with dynamic symmetry breaking so that EA/CCZ equivalences are detected and pruned during the solving process (via the **IPASIR-UP** interface to the **CaDiCaL** SAT solver). Besides reconstructing and validating known results—such as the canonical 4-bit class list and Dillon’s 6-bit APN permutation—a longer-term goal is to address more challenging open problems.

Goals and Tasks

-  Familiarize with S-boxes, EA/CCZ equivalence and preserved properties
-  Familiarize with SAT & CNF modeling, interactive propagation and clause injection via IPASIR-UP/CaDiCaL
-  Reproduce & verify existing results
-  Run exploratory/experimental searches for new results.

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$S(x)$	4	11	31	20	26	21	9	2	27	5	8	18	29	3	6	28
x	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
$S(x)$	30	19	7	14	0	13	17	24	16	12	1	25	22	10	15	23

Example: the 6-bit S-box of Ascon

Literature

- > [C. Carlet](#)
Vectorial Boolean Functions for Cryptography
[Boolean Models and Methods in Mathematics, Computer Science, and Engineering](#)
2010
<https://www.math.univ-paris13.fr/~carlet/chap-vectorial-fcts-corr.pdf>

Courses & Deliverables

- ☒ **Master Project**
Project code
Report
Presentation
 - OR –
 - ☒ **Master’s Thesis**
Initial presentation
Project code
Thesis (60+ pages)
Final presentation

Recommended if you’re studying

- ☒ CS ☒ ICE ☒ SEM

Prerequisites

- > *Cryptography*
- > Interest in Mathematics/Logic
- > Programming (C++/Python/SageMath)

Advisor Contact

maria.eichlseder@tugraz.at