Referee's report on the Master Thesis
Projective polynomials and the S-Boxes of Streebog and Kuznyechik
by Marie Brožová

The submitted thesis studies S-box used in a construction of a hash function Streebog and also in a symmetric cipher Kuznyechik. This S-box is a permutation on a 256-element set and a general problem is to find some unexpected structure on this permutation which could be used to attack these cryptographic constructions.

The work is divided into three chapters - the first one with some introductory material, second one describing constructions of ciphers and also previous works on the S-box done by Perrin, Udovenko and Biryukov, namely the construction of mapping TKlog (Algorithm 4) which can be used to compute the S-box when its parameters are appropriately chosen.

The main part of the work is the third chapter where the author tries to find an expression of the S-box as a fractional q-projective function (or some modification of such a function). The main tool is Göloglu's characterization of q-projective permutations of a projective line up to projective equivalence (Theorem 16). This theorem gives a way how to search whether the S-box is affine equivalent to a fractional q-projective permutation by brute force but this way is not feasible in practice. The author therefore introduces some improvements based on decompositions of a Möbius transform and differential spectra.

In the end no q-projective permutation related to the S-box was found the author also suggests a general way how to search for q-projective permutations which are in some sense close to a given permutation.

The work contains also Attachments with details which were not neccessary for understanding the material in the thesis, also implementation used for the experiment introduced in the third chapter.

In my opinion the thesis contains interesting material, also the presentation is quite good. There are some misprints or imperfections which make some parts of the thesis hard to read. I list some of them below.

Overall I recommend the work to be accepted as Master thesis.

In Prague, August 30, 2024

Pavel Příhoda

Some comments

- Observation 1: In general α is not a generator of $\mathbb{F}_{2^m}^*$
- The proof of Theorem 3 should be written carefully: For example how can we conclude from the formula on page 13, case a. that this transformation does not change the Walsh spectrum?

- Notation 7: $c = 0, d = 1, a = 1$
- Observation 7: It could be proved that R is invertible.
- Diagram on page 28: I think boxes in the second row should be switched
- Algorithm 4: I think κ should be injective at least to make the argument below work.
- page 35: Image of κ is an affine subspace of $\mathbb{F}_2^8$.
- Algorithm 5: What does $\mathrm{Int}_4(y)^{-1}$ mean?
- Claim 12: W_{add} is should be introduced earlier than in the proof.
- Theorems 13,14: I think the objects should be shifted to correct structures.
- Notation 14: Is this notation correct? For example, ϵ_1 is an element of $\mathbb{L}$ but the domain of $\mathrm{tr}_{\mathbb{D}\setminus\mathbb{F}_2}$ is $\mathbb{D}$.
- page 48: Why are ϵ_q and ϵ_2 in $\mathbb{F}_{2^8}$? Also note that if $\omega \in \mathbb{F}_{2^{16}} \setminus \mathbb{F}_{2^8}$ then actually $\mathbb{F}_{2^{16}} = \mathbb{F}_{2^8}(\omega)$.
- page 51: I think that g_1, g_2 should be polynomials in x.
- page 55: $2 \times (2^{16} + 2^8 + 2^8 + 1) \neq 2^{18} + 2$
- the proof of Theorem 18 seems to be quite complicated. Could it be possible to check the equality element-wise?
- A.11: I think some speedup could be achieved if the spectrum of ψ is compared to the spectrum of π during its computation. When we learn that the spectra are different we can interrupt the computation.
- I think it would be very interesting if there was a 'small' example explaining how to use an S-box which can be expressed as a q-projective permutation to attack a cipher.