# Report on "Projective polynomials and the S-Boxes of Streebog and Kuznyechik"

The thesis is on the analysis of the S-Box of the recent cipher Kuznyechik and the hash function Streebog. Perrin [Per19] showed that the S-Box permutation (called $\pi$ overall the thesis) can be understood in a simple way that uses substructures of the finite field $\mathbb{F}_{2^8}$, namely the additive substructures (i.e., vector space of half dimension) $\mathbb{F}_2^4$ and its cosets; and the multiplicative substructures (i.e., multiplicative group of the subfield of index two) $\mathbb{F}_{2^4}^\times$ and its cosets. This analysis hints that $\pi$ has an apparent resemblance to the so-called *fractional projective permutations* with certain parameters [Go22]. The goal of the thesis is to explain these two notions (i.e., Perrin's paper and the fractional projective permutations) in detail and design and implement an experiment to decide whether the S-Box $\pi$ is "equivalent" to a fractional projective permutation.

The student starts by a preliminary chapter where she explains the notions like cipher, hash function etc. and the mathematical and cryptographical concepts used in the thesis. In the second chapter, she explains [Per19] in detail. One requirement of the thesis which was accomplished was to rewrite the results in a less "engineering" notation with more mathematical detail (on selected parts) than the original paper. The third chapter contains the main results. The student starts by explaining the classification result on fractional projective polynomials (FPP) [Go22]. Then the experiment is explained in ample detail. Some invariants of Boolean functions are used to minimize the work done to check whether there exists an FPP equivalent to $\pi$ or not. These invariants are explained in Section 3.3. The experiment requires a lot of details to be taken care of which are all done in this section. These include affine equivalence, the notion of fractional jump etc. Finally, the results are interpreted in the final section.

Although the results of the experiment is negative, the thesis answers a very natural question whether $\pi$ is equivalent to one of the FPPs. A positive result might have lead to a cryptanalysis of the ciphers, since the form of FPPs are well-structured.

The thesis could be written in a way that is better organized. It must be quite difficult to understand for a reader who is not well-versed on the subject matter. At least, the goal could be more clearly explained. For instance the following explanation (or a similar one) could be mentioned early in the thesis, even in the Introduction.

> **Goal:** Let $\Pi : \mathbb{P}^1(\mathbb{F}) \to \mathbb{P}^1(\mathbb{F})$ be an FPP. Suppose that $\Pi(\infty) = \gamma$ and $\Pi(\beta) = \infty$. We would like to show that the "fractional jump" function $FJ(\Pi) : \mathbb{F} \to \mathbb{F}$ (which maps $FJ(\Pi) : \beta \mapsto \gamma$ and behaves exactly as $\Pi$ on the other values) is not "equivalent" to the S-Box $\pi$, for every FPP $\Pi$. (The notion of "equivalence" is explained in the thesis quite well.)

A similar explanation was given in the text (see Eq (3.2)), however it is buried in the text. In my opinion, although many parts of the thesis explained in a correct way, it could have been done in an easier way to help the clarity of the text.

A few formal errors:

- Observation 1: + should be multiplication.
- (p. 39) alpha

**Topic of the thesis:** The thesis combines cryptography (Block Ciphers and Hash Functions) and mathematics (Möbius transformation, Permutation Rational Functions, Boolean Functions). Thus the topic is very suitable for a thesis.

**Mathematical content:** The mathematical content is suitable.

**Citations/References:** Many sources are used which are cited carefully overall the thesis.

**Student's contribution:** Student first explains two recent publications: [Per19] in detail and parts of [Gol22]. She designs and implements experiments to check whether the hypothesis that "$\pi$ is equivalent to an FPP" is correct. During the process she solves several mathematical problems to ensure the correctness and to improve the efficiency of the experiment.

The use of English is good overall the thesis but could be improved. For instance:

- (p. 5) there must exists
- lenght, bitsting
- Analogically should be analogously
- to encrypt longer messages than k bits: messages longer than $k$ bits.
- (p. 20) choose a fixed coordinates
- One should use ‘ ’ and “ ” for quotation marks

**Conclusion:** I believe the thesis deserves to be recognized as a successful thesis. Although the novelty of the thesis cannot be viewed as outstanding, it solves a meaningful question in a nice way. The shortcomings of the thesis are minor in my opinion. I will inform the committee of my suggested grade.