

## Jury Member Report – Doctor of Philosophy thesis.


**Name of Candidate:** Elena Egorova

**PhD Program:** Computational and Data Science and Engineering

**Title of Thesis:** Signature Codes for Multiple Access Channels, Digital Fingerprinting Codes and Symmetric Group Testing

**Supervisor:** Prof. Grigory Kabatyansky

**Name of the Reviewer:** Eitan Yaakobi

|   |   |
|---|---|
| <p>I confirm the absence of any conflict of interest</p> <p>(Alternatively, Reviewer can formulate a possible conflict)</p> | <p><b>Signature:</b></p>  <p><b>Date: 28-03-2020</b></p> |
|---|---|

*The purpose of this report is to obtain an independent review from the members of PhD defense Jury before the thesis defense. The members of PhD defense Jury are asked to submit signed copy of the report at least 30 days prior the thesis defense. The Reviewers are asked to bring a copy of the completed report to the thesis defense and to discuss the contents of each report with each other before the thesis defense.*

*If the reviewers have any queries about the thesis which they wish to raise in advance, please contact the Chair of the Jury.*

### Reviewer's Report

Reviewers report should contain the following items:

- Brief evaluation of the thesis quality and overall structure of the dissertation.
- The relevance of the topic of dissertation work to its actual content
- The relevance of the methods used in the dissertation
- The scientific significance of the results obtained and their compliance with the international level and current state of the art
- The relevance of the obtained results to applications (if applicable)
- The quality of publications

The summary of issues to be addressed before/during the thesis defense

It is my great pleasure to write this report on the doctoral thesis by Elena Egorova. This Thesis, as far I've read, was initiated by the problem of constructing families of good multimedia fingerprinting codes since the rate of all previously known families of such codes tends to zero with growing code length that shouldn't be according to information theory. Elena has solved this problem rather easy by establishing a strong relationship between signature codes for the so-called A-channel, which is one of the studied cases of a MAC, and multimedia fingerprinting codes. It was possible to stop here and try to improve this result but Elena has chosen other, more interesting and difficult way to develop the theory of signature codes for different multiple access channels.

This Thesis has several major contributions. First, new upper and lower bounds are presented on the rate of signature codes for A-channel, B-channel and their modifications. Second, new constructions of the corresponding signature codes for A-channel and their efficient decoding algorithms. Third, results on the noisy setup of these channels in the form of an upper bound on the rate of signature codes for A-channel with noise. Fourth and and lastly, applications to digital fingerprinting codes and symmetric group testing. This includes also the new class of signature codes for the weighted adder channel, fingerprinting cods with simplified tracing traitors based on minimum distance decoding, and new upper bound for the minimal number of tests in symmetric group testing with adversarial noise.

The most impressive and technically difficult result, in my opinion, which she obtained on this way is upper and lower bounds on the rate of best signature codes for B-channel case of a MAC (Chapter 3 of the Thesis). Since the B-channel is the "largest" channel in some partial order, which Elena introduced on the set of multiple access channels, then the corresponding upper bound is valid for any multiple access channel. Another interesting and useful result is a new construction of a family of signature codes for the A-channel with polynomial complexity which allows immediately to receive a family of multimedia fingerprinting codes capable to find a malicious coalition with just polylog complexity (in the total number of users).

Elena introduced another, non-discrete, model of multimedia fingerprinting which provides to a dealer of a system more information (because avoiding quantization), show that this model can be considered as so-called weighted binary adder channel and finally constructed a family of fingerprinting codes with very high rate, namely, of order  $1/t$  instead of  $1/t^2$  for the ordinary (or quantized) model. It is worth to note that the corresponding codes are famous families of binary error-correcting codes, like Goppa or BCH codes. Unfortunately, there is no efficient decoding/tracing algorithm to find the corresponding coalition of malicious users what is one of a most interesting open question arising from the dissertation.

There are also interesting results, which follow from the previously known relationships between signature codes and non-adaptive group testing. In particular, this is the proposed application of results on A-channel toward symmetric group testing. By the way, I would like to note that signature codes for weighted binary adder channel are the same as non-adaptive search for counterfeit coins of unknown and different weights on a spring scale. And the corresponding comparison should be given.

Finally, I would to conclude that the Thesis is clearly written, all results belong to Elena Egorova and are properly published, in particular in three journal publications. For all these reasons, I recommend that the candidate should defend the thesis by means of a formal thesis defense.

**Provisional Recommendation**

*I recommend that the candidate should defend the thesis by means of a formal thesis defense*

*I recommend that the candidate should defend the thesis by means of a formal thesis defense only after appropriate changes would be introduced in candidate's thesis according to the recommendations of the present report*

*The thesis is not acceptable and I recommend that the candidate be exempt from the formal thesis defense*