Skoltech
Skolkovo Institute of Science and Technology

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: Alexey Frolov

I confirm the absence of any conflict of interest (Alternatively, Reviewer can formulate a possible conflict)	**Signature:**  **Date: 28-03-2020**

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

The PhD thesis of Elena Egorova, entitled “Signature codes for multiple access channels (MACs), digital fingerprinting codes and symmetric group testing”, is devoted to the study of uniquely decodable codes (signature codes) for the case of partial activity of users for special classes of channels, namely MAC with and without intensity information, or the so-called A-channel and B-channel, and some their generalizations and applications. The thesis consists of introduction, 4 chapters and conclusion.

In the first chapter the author describes not only three, at first glance, looking rather different areas of research, namely signature codes for MACs, digital fingerprinting codes and group testing, but shows very deep relationships among them. I would like to draw attention to introduced in the Thesis a partial order on MACs, what makes the set of MACs a poset and allows to derive some results almost for free!

In the second chapter, the signature codes for A-channel are investigated. A-channel is also known as the multi-frequency channel without intensity information. It was introduced in the paper of Chang and Wolf almost forty years ago. The input of the channel is the value of q-ary alphabet $Q = \{0, 1, \ldots, q-1\}$ and the output is the union of inputs. The author is interested in the parameters of the best signature codes for this channel. First, Elena explains interconnections among signature codes, disjunctive, cover-free and separating codes and even with non-adaptive group testing. In this part, Elena demonstrates deep understanding of the topic. Then, Elena considers an interesting problem of decoding at least one of active users, which is important for digital fingerprinting. Finally, Elena investigates A-channel with noise and provides us with the bounds for this case.

The third chapter is devoted to investigation of B-channel or the multi-frequency channel with intensity information and its modification, called weighted adder channel. In the case of B-channel the receiver has not only the set of transmitted symbols but also their multiplicities, i.e., how often a given symbol (frequency) was used. It is clear that this channel provides us with maximal possible information. Elena proves new lower and upper bounds for the rate of the best signature codes for B-channel. For the weighted adder channel she consider a more general case when the output of the channel can be disturbed by adversarial noise and show how ordinary error-correcting codes, like Goppa and BCH codes, can be applied to solve the problem. An interesting connection with compressed sensing is also established.

The fourth chapter is devoted to applications. I will focus on digital fingerprinting only as this problem is of extremely high importance for the digital world. Assume we want to redistribute some content in between users (e.g. a movie) and be able to check if a user illegally shares his digital copy. In order to do this, we add different watermarks (binary strings) to different copies. At the same time, the users can form coalitions and create fake watermarks from existing ones. Elena found a way to deal with this problem. This approach is based on signature codes developed of the previous chapters.

Finally, the summary of my review is as follows. Elena obtained significant scientific results compliant with the international level and current state of the art. This statement is proved by high level publications at top level international conferences, like IEEE International Symposium on Information Theory, and in WoS journals (Problems of Information Transmission and two papers in Designs, Codes and Cryptography).

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*