PhD thesis referee report: **Complexity of Dynamic Data Structures**, by Karel Kŕal.

Referee: Prof. Yuval Ishai, Computer Science Department, Technion

Summary:

The thesis studies problems related to sorting and hiding access patterns to data. Its technical chapters contain three distinct contributions: (1) improved upper bounds on the circuit complexity of sorting small integers, (2) improved lower bounds for oblivious RAM, and a (3) new algorithm for sorting in the RAM model which is significantly simpler to describe and analyze than the (slightly better) state-of-the-art algorithm.

Evaluation:

This is a strong thesis that advances the state of the art in a major way. All three contributions address important problems and are likely to find applications in several areas, including algorithms, cryptography, and complexity theory.

The first contribution is particularly appealing due to the pervasive use of sorting in algorithms and other areas of computer science. It should be noted that the circuit complexity of sorting has recently been a very active research area, in part because of its relation to secure sorting and oblivious RAM (the topic of the second contribution). The thesis not only improves over the very recent work of Asharov et al. from SODA 2021, but also obtains a conceptually simpler solution by using previous results in a black-box way. The solution is based on a novel implementation of a “fast counting” gadget that can be useful elsewhere.

The second contribution addresses a very important problem in cryptography and in a sense fills in a natural gap left by a celebrated lower bound of Larsen and Nielsen. The same chapter contains several other nice observations and results related to previous definitions of oblivious RAM from the literature.

The third contribution gives an elegant new sorting algorithm that, while slightly falling short of achieving the best known asymptotic complexity, is relatively easy to describe and analyze and may lead to further progress on this important problem.

The first two contributions were published in competitive peer-reviewed conferences (TCC and ICALP respectively).

The thesis is very well-written, contains a comprehensive treatment of prior related works, and spends a lot of effort on explaining the intuition behind the results.

Overall, the thesis proves the author’s ability for creative scientific work, and clearly meets the expected standards for a PhD dissertation in Computer Science.

Signed: Yuval Ishai