



**FACULTY
OF MATHEMATICS
AND PHYSICS**
Charles University



August 20, 2021

Advisor's report on the doctoral thesis of Mgr. Veronika Slívová

The central theme of the doctoral thesis of Mgr. Veronika Slívová is the computational complexity of total search problems with a unique solution. Specifically, the thesis presents new results aiming to identify the limits on the power of efficient algorithms for such structured search problems by employing techniques from algorithm design and cryptography. The results contribute to a research area which has recently been very active. To this end, the thesis presents results in two main directions. In the first direction, the thesis establishes an improved upper bound on the computational complexity of a natural reachability problem in graphs. In the second direction, the thesis establishes an apparent limitation for proving cryptographic lower bounds for this class of search problems under weak and, in particular, unstructured cryptographic assumptions. I must stress that the second direction aims at generalizing and pushing further seminal impossibility results in theoretical cryptography and, as such, presents novel techniques towards a challenging goal of establishing black-box impossibility results in the context of the complexity class TFNP.

The core of the results was already presented in top-tier conferences in theoretical computer science such as ICALP and TCC. Besides the results contained in her thesis, Mgr. Veronika Slívová has published other results with her coauthors, while making a substantial contribution to each of her published works. During her Ph.D. studies, she clearly and continuously demonstrated her ability to carry out and disseminate independent and original research in computer science, clearly qualifying her, in my opinion, for the Ph.D. degree.

It is my pleasure to strongly recommend accepting the submitted thesis as a doctoral thesis and awarding Mgr. Veronika Slívová with the Ph.D. degree.

Sincerely,

Mgr. Pavel Hubáček, Ph.D.
Assistant Professor