Meggido and Papadimitriou [Theor. Comput. Sci., 1991] introduced the class TFNP of search problems for which a solution always exists and is polynomially verifiable. In this thesis, we study the possibility of reducing different problems into problems in TFNP. The property which is in common for problems, for which we study the reducibility to TFNP, is that all instances of these problems have a unique solution (if there is any solution present).

In the first part of this thesis, we study a problem called ARRIVAL, which was introduced by Dohrau, Gärtner, Kohler, Matoušek and Welzl [A Journey Through Discrete Mathemathics: A Tribute to Jiří Matoušek, 2017]. ARRIVAL is the following decisional problem: Given a graph in which a train is moving according to prescribed rules does the train arrive to a given vertex? We first improve the result of Dohrau et al. who showed that the problem is in NP $\cap$ coNP. We show that there exists a unique certificate for being in the language and, thus, prove that it lies in UP $\cap$ coUP.

We also study the search version of the ARRIVAL problem, which asks for the transcript of number of traversals for each edge. It was known that the search version lies in PLS, which was proven by Karthik C. S. [Inf. Process. Lett., 2017]. We improve this result by showing a reduction from ARRIVAL to End-Of-Metered-Line (a problem introduced by Hubáček and Yogev [SIAM J. Comput., 2020]) and, thus, prove that it lies in the class CLS.

In the second half of this thesis, we study the possibility of showing hardness in TFNP based on cryptographic assumptions. We first rule out a fully black-box construction of a worst-case hard TFNP problem from a hard-on-average UP problem. Thus, we also rule out constructions of hard TFNP problems from hard-on-average problems in NP. Then, we consider more structured assumption of injective one-way functions (which imply a hard-on-average problem in UP). We show that, even in this case, it is not possible to construct a worst-case hard TFNP problem assuming that the reduction from injective one-way functions (OWF) is "simple". More precisely, a security reduction is "simple" if it queries the TFNP instances non-adaptively and independently on the one-way function with respect to which it is running. Note that there are known "simple" constructions based on other cryptographic assumptions (such as collision resistant hash functions) and, thus, we believe that our restrictions on the security reduction are natural.