Meggido a Papadimitriou [Theor. Comput. Sci., 1991] definovali třídu TFNP, která je tvořena vyhledávacími problémy, pro které řešení vždy existuje a lze je testovat v polynomiálním čase. V této práci studujeme, zdali lze různé problémy redukovat na problémy z TFNP. Problémy, jejichž redukovatelnost do TFNP studujeme, mají společnou vlastnost, že všechny jejich instance mají jednoznačné řešení (pokud nějaké řešení vůbec existuje).

V první části této práce studujeme problém zvaný ARRIVAL, který se poprvé objevil v článku Dohrau, Gärtner, Kohler, Matoušek a Welzl [A Journey Through Discrete Mathemathics: A tribute to Jiří Matoušek, 2017]. ARRIVAL je následující rozhodovací problém: Máme dán orientovaný graf, po kterém se pohybuje vláček podle předepsaných pravidel, a ptáme se, jestli vláček někdy dojede do předem určeného vrcholu. Prvně vylepšíme výsledek Dohrau a kol., kteří ukázali, že tento problém je v NP $\cap$ coNP. Ukážeme, že existuje jednoznačný certifikát pro náležení do jazyka a tedy dokážeme, že ARRIVAL je v UP $\cap$ coUP.

Dále budeme studovat vyhledávací variantu problému ARRIVAL, při které máme určit kolikrát vláček projel po každé hraně grafu. Jak ukázal Karthik C. S. [Inf. Process. Lett., 2017], vyhledávací varianta ARRIVAL je ve třídě PLS. My tento výsledek vylepšíme a ukážeme redukci z problému ARRIVAL na problém End-Of-Metered-line (problém definovaný v článku Hubáček a Yogev [SIAM J. Comput., 2020]) a tak ukážeme, že ARRIVAL je ve třídě CLS.

Ve druhé půlce této práce studujeme, je-li možné ukázat těžkost v TFNP na základě kryptografických předpokladů. Prvně vyloučíme, takzvané plně black-box konstrukce TFNP problémů, které jsou těžké v nejhorším případě, na základě problémů v UP, které jsou těžké v průměru. Tím pádem také vyloučíme vytváření těžkých TFNP problémů z problémů v NP, které jsou těžké v průměru. Poté budeme uvažovat více strukturovaný předpoklad prostých jednosměrných funkcí (které implikují problém v UP, který je těžký v průměru). Ukážeme, že dokonce ani v tomto případě není možné vytvářet těžké (v nejhorším případě) instance TFNP problémů alespoň za předpokladu, že redukce z prosté jednosměrné funkce je "jednoduchá". Přesněji řečeno, redukce je "jednoduchá", pokud její dotazy na TFNP instance jsou neadaptivní a nezávislé na volbě jednosměrné funkce vzhledem k níž redukce běží. Poznamenejme, že existují "jednoduché" konstrukce z jiných kryptografických předpokladů (například z hash funkcí rezistentních vůči kolizím), a proto věříme, že naše omezení na redukci jsou přirozené.