

Kryptografie založená na polookruzích je jedním z možných řešení, jak přistupovat k schématům s veřejným klíčem v postkvantové kryptografii. V naší práci se budeme zabývat jedním konkrétním polookruhem – tropickou algebrou. Prozkoumáme jedno konkrétní schéma dohody na klíči – Stickelův protokol upravený pro použití v polookruzích. Přestože na toto schéma byl již navržen útok, tak jsme tento algoritmus naimplementovali a především určili jeho složitost. Dále navrhujeme další varianty Stickelova protokolu a zkoumáme jejich potenciál pro praktické využití. Během tohoto výzkumu jsme narazili na teorii chování mocnin tropických matic, proto jsme se snažili udělat její přehled pro použití v kryptografii založené na maticích nad tropickou algebrou.