Posudek na bakalářskou práci

Jana Kučerová, Interaktivní důkazy

Práce Jany Kučerové se zabývá interaktivními důkazy, tj. kryptografickými protokoly, které slouží k tomu, aby jeden účastník protokolu přesvědčil druhého, že má nějakou znalost. Tyto protokoly především slouží k ověřování identity příslušného účastníka protokolu, který prokazuje, že má nějakou znalost, která pevně spojena s jeho identitou, například znalost svého privátního klíče.

Po stručné informaci, co je to kryptografický protokol, jsou ve třetí kapitole uvedeny některé matematické pojmy a tvrzení používané v dalším textu. Čtvrtá kapitola obsahuje popis několika základních stavebních prvků kryptografických protokolů, v páté kapitole jsou uvedené nezbytné definice z teorie Turingových strojů a závěrečná šestá kapitola obsahuje příklady interaktivních protokolů a posouzení jejich bezpečnosti.

Autorka téma zvládla velmi dobře, práce je napsaná přehledně a s pochopením podstaty věci.

Mám-li mít nějaké výhrady, pak by se týkaly některých matematických míst, nikoliv kryptografických. Tak například v Definici 3.4. není uvedené, z jaké množiny uvažujeme prvky v. Důkaz druhé části Důsledku 3.13. (existence čtyř kvadratických reziduí modulo pq, kde p a q jsou různá lichá prvočísla) je zbytečně složitý, stačilo vhodně použít Čínskou větu o zbytcích, Větu 3.12.

Tyto výhrady jsou ale drobností ve srovnání s tím, jak pečlivě je práce napsaná, s minimem překlepů a chyb.

Práce bohatě naplňuje požadavky na bakalářskou práci, proto ji navrhuji přijmout jako práci bakalářskou a hodnotit ji známkou **výborně.**

Doc. RNDr. Jiří Tůma, DrSc.
vedoucí práce

V Praze, 20.9.2006