Jana Kučerová: Interaktivní důkazy

posudek oponenta

Jádro práce tvoří popis tří základních interaktivních důkazů pro prokazování identity, a to schématu pomocí kryptografie s veřejným klíčem, Fiat-Shamirova a Schnorr-Okamotova schématu (kap. 6). Prvních pět kapitol pak je věnováno potřebnému pozadí matematickému i z teorie složitosti. Práce je soběstačným výkladem této problematiky, která patří k základům kryptografie.

Práce je přehledná a čtivá, po jazykové stránce perfektní. Matematicky je také téměř bezchybná, jen na několika málo místech obsahuje drobné nejasnosti a nepřesnosti, keré jsem již s autorkou konzultoval (např. na str. 21 v definici (A,B)(x) nebo ve výkladu na str. 24). Jediným nedostatkem, který stojí za zmínku, je fakt, že některé části jsou poněkud technické a chybí trochu motivace a "lidský popis" některých formálních definic a tvrzení; občas by stálo za to uvést, k čemu se právě popisovaná věc později použije, co která podmínka znamená (např. v Definici 6.1, proč se v podmínce Spolehlivosti kvantifikuje přes *všechny* ITM?). Na srozumitelnost a korektnost práce ovšem tato místa vliv nemají. Také jsem nalezl pár nedomyšlených drobností, např. na konci sekce o Rabinově kryptosystému se tvrdí, že "Alice by byla hloupá", kdyby pro Boba dešifrovala jím zvolenou zašifrovanou zprávu pomocí svého tajného klíče (Bob pak má slušnou šanci získat Alicino heslo), ovšem o pár stránek dál (kap. 6.1) je popsán identifikační protokol, který takovou věc de facto Alici nařizuje.

Předloženou práci považuji za kvalitní, doporučuji ji uznat jako bakalářskou a navrhuji hodnocení stupněm **výborně.**

V Praze, 15.9.2006
David Stanovský