Oponentský posudek diplomové práce

Jana Divišová: Kryptografie založená na mřížkách

Práce se zabývá využitím mřížek v kryptografii a kryptoanalýze. Podává přehled kryptografických systémů založených na složitosti SVP a CVP a kryptografických útoků na některé kryptosystémy založených na algoritmu LLL. Vlastním přínosem autorky je implementace jednoho z kryptosystémů založeného na mřížkách (NTRU) a jeho srovnání s RSA pro různé velikosti zpráv a klíčů. Práce je podle mého názoru velmi dobrá, po obsahové i jazykové stránce. Rešeršní část vyžadovala studium mnoha zdrojů.

Poznámky:

- Práce se přirozeně nevyhla překlepům a nepřesnostem. Příklady drobných nepřesností: V definicích 2.3 a 2.4 by mělo být „libovolný *nenulový* vektor mřížky"; na začátku sekce 3.1.3 je zmíněno, že šifrování 1 probíhá stejně a šifrování 0 se liší, správně je to naopak. O-notace je používaná příliš vágně, například definice 3.10, 3.13 nedávají podle mého názoru bez bližšího vysvětlení smysl.

- V některých částech by bylo pro srozumitelnost textu potřeba přidat vysvětlení. Následují konkrétní příklady. V důkazu Lemma 3.3. je argument „protože T a v jsou celočíselné, tak i $T^{-1}v$ je celočíselné", což není obecně pravda – potřebujeme vědět, že T^{-1} je celočíslná, a to je potřeba zdůvodnit (nebo aspoň zmínit). Na začátku se mřížky definují nad reálnými čísly, v kapitole o NTRU kryptosystému se bez varování začíná pracovat z mřížkami nad jiným okruhem. Není nijak vysvětlen výzkam operace definované v Definici 3.5. (tj. že se jedná o násobení polynomů v daném okruhu). Na straně 29 dole je psáno "Protože se jedná o nejmenší vektor nalezený LLL algoritmem, pak jeho prvních $t-1$ souřadnic splňuje...", přitom následný odhad využívá vlastnost LLL algoritmu, která není nikde dříve zmíněná.

- Zajímalo by mě, jak knihovna NTL řeší počítání modulo $x^n - 1$ – v 5.1. se zmiňuje, že počítání modulo f lze urychlit předpočítáním informací o f, co se stane pro $f = x^n - 1$?

Předloženou diplomovou práci doporučuji k obhajobě a navrhuji ohodnotit stupněm výborně.

V Praze dne 17.5.2010

Mgr. Libor Barto, Ph.D.