Posudek oponenta bakalářské práce

Název: Problém LWE a bezpečnost schémat pro výměnu klíče
Autor: Jan Václavek

Shrnutí obsahu práce

Předložený text Jana Václavka se zabývá otázkou využitelnosti problému LWE v postkvantové kryptografii. Kromě úvodu, závěru a přehledu základní použité termilogie a notace sestává ze čtyř věcných částí. První z nich je věnována přehledu potřebných výsledků z teorie mříží, jejím hlavním přínosem je vyřešení čtyř cvičení popisujících vztah mezi minimální vzdáleností a pokrývajícím poloměrem mříží a dále vyslovení algoritmických problémů na mřížích, které se o pojem minimální vzdálenosti opírají. Další část čtenáři vysvětluje centrální pojem práce, jímž je problém LWE, včetně souhrnu nezbytných faktů a pojmů z teorie pravděpodobnosti. Následující kapitola obsahuje hlavní výsledek práce, který představuje prezentace důkazu redukce problému BDD_Λ na jednu z variant problému LWE. Stručná závěrečná kapitola nastiňuje konstrukci a bezpečnost schématu pro výměnu tajného bitu založeného právě na LWE.

Celkové hodnocení práce

Téma práce. Téma bylo poměrně obtížné, neboť od studenta vyžadovalo porozumění několika oblastem matematiky překračující standardní znalosti bakalářského studenta oboru Obecná matematika (teorie mříží, kryptografie a kryptografické využití teorie pravděpodobnosti, elementy teorie složitosti), přesto bylo zvládnutelné a svým charakterem vhodné pro zpracování v bakalářské práci. Zadání bylo podle mého mínění studentem zdařile naplněno.

Vlastní příspěvek. Práce je kompilací většího množství zdrojů doplněná o vyřešení několika cvičení a některé netriviální detaily v důkazech (například Lemma 14).

Matematická úroveň. Matematická úroveň práce je velmi dobrá a formulace jsou vesměs korektní. Výběr dokazovaných tvrzení je dobře motivovaný a prezentované důkazy jsou srozumitelné.

Práce se zdroji. Práce vedle samostatného vyřešení několika cvičení zpracovává a doplňuje teorii převzatou z několik zdrojů, na nichž není formulačně závislá.

Formální úprava. Po formální stránce nezasluhuje práce zásadní výtky, jazykových nepřesností a omylů je v textu množství přiměřené jeho rozsahu a výsledný text se velmi dobře čte.

Připomínky a otázky

1. V komentáři za Definicí 8 pracujete s nejbližším celočíselným vektorem $\lfloor \mathbf{B}^{-1}\mathbf{w} \rceil$, ačkoli toto značení na straně 3 zavádíte jen pro reálná čísla.
2. V jakém smyslu považujete za *prostor* množinu $\mathrm{span}(\Lambda') + c\mathbf{b}_m$ v důkazu Cvičení 1?
3. V důkazu Cvičení 2 bychom měli mluvit spíše o uzavřenosti Λ' na opačné prvky než na *inverzní* prvky.

Závěr

Práce „Problém LWE a bezpečnost schémat pro výměnu klíče" podle mého mínění beze zbytku splnila zadání a doporučuji ji uznat jako bakalářskou.

Návrh klasifikace oponent sdělí předsedovi zkušební (sub)komise.

Jan Žemlička
Katedra algebry
5.6.2019