Posudek vedoucího bakalářské práce
Problém LWE a bezpečnost schémat pro výměnu klíče
Jana Václavka

Cílem práce bylo seznámení s problémem LWE a jeho možnými aplikacemi v kryptografii. Práce je rozdělena na pět kapitol. Druhá kapitola obsahuje základní pojmy teorie mříží, v sekci 2.3 autor vyřešil několik cvičení týkajících se vlastností pokrývajícího poloměru mříže. Formulaci několika variant problému LWE se věnuje kaitola 3. Zároveň jsou vysvětleny pojmy diskrétního Gaussova rozdělení na mříži a statistické vzdálenosti rozdělení pravděpodobnosti. Sekce 3.3 o statistické vzdálenosti je prezentována v obecnosti potřebné pro kapitolu 4, která představuje jádro celé práce. Jedná se o výsledky O. Regeva a C. Peikerta ukazující, jak lze některé výpočetní problémy na mřížích efektivně řešit pomocí vyhledávacího problému LWE. Závěrečná kapitola ukazuje návrh schématu pro výměnu klíče, které svou bezpečnost odvozuje od obtížnosti rozhodovacího problému LWE.

Přestože téma práce lze považovat za poměrně obtížné, autorovi se podařilo sepsat srozumitelný a čtivý text. Některá techničtější tvrzení potřebná pro uvedené redukce jsou uvedeny bez důkazu, autor se zaměřil hlavně na podstatu redukce, která dává do souvislosti LWE s problémy na mřížích. Tyto části důkazu jsou provedeny detailněji než v citovaných článcích. Jediný problém, kterého jsem si všimnul, je přeznačení symbolu $\mathbf{B}$ v důkazu Věty 18 - kde místo báze Λ^* značí tento symbol bázi Λ.

Celkově považuju práci Jana Václavka za velmi zdařilou a navrhuji ji uznat jako práci bakalářskou.

V Rychalticích, 15. 6. 2019

Pavel Příhoda