Posudek oponenta k bakalářské práci
Využití invertibilních prvků mřížky v ověření s nulovou znalostí
Karolíny Kučerové

Předložená práce se zabývá protokolem z článku V. Lyubashevsky a G. Neven, *One shot verifiable encryption from lattices*. Vlastní protokol je poměrně komplikovaný, v principu kombinuje okruhové LWE a Fiat-Shamirovo schéma (obě metody jsou detailně představeny ve druhé kapitole). Práce se věnuje pouze důkazu koreknosti schématu, nikoli důkazu jeho bezpečnosti (kapitola 3). Matematický základ je pak doplněn v první kapitole, pro důkaz koreknosti je pak důležité Lemma 7 ukazující že všechny nenulové prvky malých norem jsou v okruhu $\mathbb{Z}_q[x]/(x^n+1)$ pro vhodné volby n a q invertibilní.

Autorce se podařilo schéma poměrně dobře vysvětlit. Vzhledem k tomu, že se v práci nevěnuje bezpečnosti ani efektivitě dešifrovacího Algoritmu 7, bylo asi možné schéma trochu zjednodušit do podoby, na které by bylo možné princip důkazu koreknosti demonstrovat asi o něco snadněji. Například Algoritmus 5 mění rozdělení náhodné veličiny $\mathbf{z}$, z dalšího textu však není jasné proč to vlastně dělá. Podobně se nastavují paramtery na straně 24 nahoře, přičemž v důkazu se využívá pouze $p(2k_2+2) < \frac{q}{2J}$.

Po formální stránce je práce napsaná pečlivě s minimem překlepů. Některé definice a tvrzení v první kapitole obsahují drobné nedostatky ve formulacích (viz připomínky níže).

Celkově si myslím, že práce splnila zadání a doporučuji ji proto uznat jako bakalářskou.

V Praze, 6. 9. 2022

Pavel Příhoda

Konkrétní připomínky k práci:

- Definice 4: $I \neq \emptyset$
- Definice 14: $f \neq 0$
- Tvrzení 2: n je použito ve dvou různých významech. Dále chybí předpoklad p nedělí stupeň polynomu. Aby bylo tvrzení $x^n - 1 = \prod_{k|n} Q_k$ formálně správné, měly by všechny množiny $E_{(k)}$ ležet ve společném tělese (což se asi implicitně předpokládá).
- Definice 18: Definice obsahuje vlastně 2 definice mřížky. Jednu pomocí báze a jednu 'bez souřadnicovou' jako diskrétní podgrupu v $\mathbb{R}^n$.
- Tvrzení 4: Nerovnost $(a_i + b_i)^2 \leq a_i^2 + b_i^2$ vypadá dost podezřele.

- Příklad na straně 10: Okruh má 5^8 prvků.
- Lemma 5: Jde o řád prvku v grupě $\mathbb{Z}^*_{2^{\kappa+2}}$.
- strana 24, poznámka dole: ... potřebovat, aby pro všechny *nenulové* prvky ...
- strana 28: Ve výrazu $p(\overline{r}s_2 + \overline{e'} + \overline{e}s_1)$ má pravděpodobně být $-\overline{e}s_1$ (soudě dle výpočtu na straně 17)
- Asi by bylo dobré vysvětlit pojem *jednorázové ověření*.