Posudek vedoucího bakalářské práce

Název: Využití invertibilních prvků mřížky v ověření s nulovou znalostí
Autorka: Karolína Kučerová

Shrnutí obsahu práce

Cílem předložené práce byl matematický popis a ověření korektnosti kryptografického protokolu založeného na počítání v okruhu $\mathbb{Z}_p[x]/(x^n + 1)$.

Text je rozdělen kromě úvodu a závěru do tří kapitol. Hlavním úkolem první kapitoly je vedle zavedení potřebných pojmů a jejich ilustrací na příkladech ověření invertibility prvků okruhu $\mathbb{Z}_p[x]/(x^n + 1)$ s malou normou pro vhodné parametry. Druhá část práce se zabývá popisem a důkazem korektnosti dvou variant algoritmu LWE (learning with errors) a Fiatova-Shamirova protokolu ověření s nulovou znalostí. Třetí část textu prezentuje protokol ověřitelného šifrování včetně ověření jeho korektnosti založený na aparátu předchozích dvou kapitol.

Celkové hodnocení práce

Téma práce. Téma práce byla primárně kompilační, od studentky vyžadovalo především porozumění několika odborným textů, výběr témat, jejich zpracování a doplnění o příklady a detaily důkazů. Zadání bylo podle mého mínění studentkou úspěšně naplněno.

Vlastní příspěvek. Hlavní příspěvek předložené práce spočívá v v matematicky přesné formulaci metody ověřitelného šifrování. Za pozornost stojí především vlastní provedení kompletních důkazů invertibilty prvků okruhu $\mathbb{Z}_p[x]/(x^n + 1)$ pro vhodné parametry.

Matematická úroveň. Matematická úroveň textu práce je dobrá a formulace, ač občas poněkud kostrbaté, jsou vesměs korektní a srozumitelné. Jasnosti kapitol věnovaných popisu algoritmů by podle mého mínění prospělo poněkud podrobnější vysvětlení nebo ilustrační příklad protokolů využívajících prezentované algoritmy.

Práce se zdroji. Třebaže je práce primárně kompilační a opírá o několik článků, není na žádném z nich formulačně závislá.

Formální úprava. Formální náležitosti práce podle mého mínění nezasluhují podstatnější výtky a množství jazykových nepřesností je přiměřené rozsahu textu.

Připomínky a otázky

1. předposlední řádek českého abstraktu - vypadl název Fiatova-Shamirova protokolu.
2. strana 4 - Definice 4 a 5 by měly být vysloveny pro komutativní okruhy.
3. strana 6 - v Definici 6 by mělo být řečeno, že operace na T jsou restrikcí operací z U.
4. strana 10 - Okruh z příkladu je řádu 5^8 nikoli řádu $40 = 5 \cdot 8$.
5. strany 18 - důkaz Tvrzení 10 by si zasluhoval aspoň trochu podrobnější komentář.

Závěr

Práce Karolíny Kučerové *Využití invertibilních prvků mřížky v ověření s nulovou znalostí* podle mého názoru splnila zadání a doporučuji ji uznat jako bakalářskou.

Návrh klasifikace vedoucí práce sdělí předsedovi zkušební (sub)komise.

Jan Žemlička
Katedra algebry
5.9.2022