Posudek vedoucího bakalářské práce

Název: Integrální útoky na blokové šifry SIMON
Autorka: Kieu Trang Phamová

Shrnutí obsahu práce

Předložená práce je věnována zkoumání bitové dělící vlastnosti jako jednoho z možných prostředků integrální kryptografie. Pozornost je rovněž věnována vybraným aspektům této třídy integrálních útoků na šifry typu SIMON.

Text je vedle úvodu a závěru rozdělen do čtyř stručných kapitol. První část představuje hlavní pojmy práce a druhá se věnuje standardní formulaci pojmu dělící vlastnost. Třetí kapitola motivuje a zavádí bitovou dělící vlastnost jako jemnější prostředek umožňující integrální útoky na dané schéma. Jádro práce tvoří čtvrtá kapitola, v níž jsou detailně dokázány vlastnosti propagace bitové dělící vlastnosti.

Celkové hodnocení práce

Téma práce. Téma práce je kompilační. Od studentky vyžadovalo porozumění odbornému textu, jeho zpracování a doplnění o příklady a některé důkazy. Zadání bylo podle mého mínění studentkou naplněno.

Vlastní příspěvek. Hlavní příspěvek předložené práce spočívá v provedení tří vlastních studentčiných důkazů propagačních pravidel ve čtvrté kapitole práce.

Matematická úroveň. Ačkoli studentka občas zápolí s jazykem i formou, jak danou teorii prezentovat, je matematická úroveň práce uspokojivá a formulace jsou korektní .

Práce se zdroji. Třebaže je práce primárně kompilační, text formulačně závislý na zdrojích zásadně není.

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

Připomínky a otázky

S připomínkami, které jsem vznášel průběžně k pracovním verzím textu, se studentka vyrovnala a v předloženém textu jsem už významnější nedostatky nenalezl.

Závěr

Práce Kieu Trang Phamové *Integrální útoky na blokové šifry SIMON* podle mého názoru splnila zadání a doporučuji ji uznat jako bakalářskou.

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

Jan Žemlička
Katedra algebry
21.6.2021