Posudek oponenta bakalářské práce

Název: Integrální útok na blokové šifry Simon
Autor: Kieu Trang Phamová

Shrnutí obsahu práce

V první části práce jsou definovány blokové šifry, šifra SIMON a popsány integrální útoky. Zbytek práce směřuje k definici dělící vlastnosti a k závěrečné trojici tvrzení týkajících se zachovávání této vlastnosti při různých transformacích výchozí podmnožiny.

Celkové hodnocení práce: Studentce se nepodařilo naplnit požadavky zadaného tématu. Z práce není patrná souvislost dělících vlastností s kryptografickými útoky na blokové šifry. Studentka se omezila na vymezení kryptografických pojmů, definici dělících vlastností a formulaci a důkazy několika tvrzení, která tyto vlastnosti popisují. Prokázala tak schopnost formálně správně zformulovat a dokázat jednoduchá matematická tvrzení. Je-li to postačující k úspěšné obhajobě ponechám na rozhodnutí komise.

Téma práce.: Téma práce bylo stanoveno takto: „Hlavním cílem práce bude matematický popis útoku založeného na využití dělící vlastnosti (division property) a případně jeho srovnání s jinými verzemi integrálních útoků." Téma by odpovídalo požadavkům bakalářské práce. Požadavky vymezené tímto tématem však studentka splnila jen částečně. Prakticky se omezila na definici dělící vlastnosti a formulace a důkazy některých vztahů, které splňuje. Útoky na ní založené, stejně jako jejich srovnání s jinými verzemi integrálních útoků, v práci nejsou zpracovány.

Vlastní příspěvek.: Vlastním příspěvkem studentky jsou patrně podrobné důkazy závěrečných tvrzení.

Matematická úroveň.: Matematická úroveň práce je velmi slabá. V první části, kde jsou definovány blokové šifry, šifra SIMON a integrální útoky je řada nepřesností. Bez předchozí znalosti uvedené problematiky je velmi obtížné těmto pojmům porozumět. Například parametry v definici šifry SIMON rozměrově neodpovídají definici blokové šifry. Způsob šifrování a podstata integrálních útoků nejsou řádně vysvětleny. Ve zbytku práce jsou zavedeny a studovány dělící vlastnosti podmnožin $\mathbb{F}_2^n$. Souvislost s kryptografickou první částí není z práce patrná. Relativně přijatelná je poslední kapitola, kde je zformulováno a správně dokázáno několik tvrzení o dělící vlastnosti.

Práce se zdroji.: Zdroje jsou citovány v úvodních a závěrečných textech jednotlivých kapitol. V případě dokazovaných tvrzení v kapitole 4.3. si nejsem jist, nakolik jsou tato tvrzení převzata z literatury.

Formální úprava.: Formální úprava práce je uspokojová.

Závěr

Práci považuji za podprůměrnou. Domnívám se, že je na hranici uznatelnosti. Konečné rozhodnotí o tom, zda práci uznat jako práci baklářskou by mělo záviset na kvalitě závěrečné obhajoby.

Návrh klasifikace oponent sdělí předsedovi zkušební (sub)komise.

Jméno oponenta, podpis: Pavel Růžička
Pracoviště: Katedra Algebry
Datum: 23. 6. 2021