FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

# Posudek oponenta závěrečné práce

| | |
|---|---|
| **Oponent práce:** | Ing. Josef Kokeš, Ph.D. |
| **Student:** | Bc. Daniel Minarovič |
| **Název práce:** | Algebraická kryptoanalýza zjednodušených variant šifry Grain-128AEAD |
| **Obor / specializace:** | Počítačová bezpečnost |
| **Vytvořeno dne:** | 15. května 2023 |

## Hodnotící kritéria

### 1. Splnění zadání

▸ [1] **zadání splněno**
[2] zadání splněno s menšími výhradami
[3] zadání splněno s většími výhradami
[4] zadání nesplněno

Všechny požadavky zmíněné v zadání můžeme v práci najít.

### 2. Písemná část práce 50 / 100 (E)

Hodnotit textovou část je pro mě obtížné, protože nemám takovou matematickou výbavu, abych dokázal posoudit faktickou správnost, a ani takovou technickou výbavu, abych mohl ověřit výsledky. Nezbývá mi tedy než věřit, že tuto část práce si zkontroloval vedoucí práce.
Nicméně, některé věci mě zaráží:
- Kapitola 1 je v podstatě jen proud definic a vět z knihy [4]. Nevšiml jsem si ničeho, co by bylo vlastním příspěvkem studenta. To by ještě nemuselo nutně vadit, problémem pro mě ale je, že nevím, proč vlastně kapitola v práci je: k pochopení čtenáři přispívá minimálně a nemohu se zbavit dojmu, že kdyby byl princip Groebnerových bází ponechán na úrovni "toho je nějaká magie, kterou spočítá nástroj Magma", tak by na tom čtenář byl zhruba stejně.
- Kapitola 2 je téměř doslovný překlad kapitoly 2 z článku [1].
- Kapitola 3 je velmi stručnou rešerší článků, které se zabývají technikami relevantními pro útoky na Grain. Nezdá se, že by články byly nějak uplatněny ve zbytku textu.
- Kapitola 4 popisuje některé implementační aspekty šifry, které nepovažuji za příliš podstatné. Klíčová je ale pro mě část 4.2, která se zabývá problematikou vytváření redukovaných variant šifry Grain. Bohužel celá tato část má jen něco málo přes jednu stránku a naprosto nevysvětluje, jak student k použité redukci přišel a proč je tato redukce validní. Zatímco práce s počtem šifrovacích rund mi dává smysl, zmenšení

vnitřního stavu prostým odříznutím "přebytečných" bitů a ponecháním všeho ostatního mi přijde krajně podezřelé - už jenom mám pochybnosti o tom, že tím zůstane zachována vlastnost použití primitivního polynomu (LFSR) nebo chování neprimitivního (NSFR). Toto je nutné vysvětlit, protože jinak výsledky stojí na vodě, vlastnosti šifry se tím mohou dramaticky měnit!
- Kapitola 5 je zajímavá a přináší výsledky, které mají hodnotu, ovšem za předpokladu, že řešení zvolené v části 4.2 je funkční. Student však mohl aspoň zběžně provést srovnání s útokem hrubou silou.
V bibliografii se nachází drobnější chyby, např. v názvu práce [23] (podle zdrojového kódu zřejmě neopravené chyby z copy&paste) nebo v URL [22].

### 3. Nepísemná část, přílohy 80 /100 (B)

Přiložené programové kódy nejsou příliš podstatné. Máme zde implementaci šifry v Pythonu, vyjádření téže šifry jako sady polynomů, skript pro provedení výpočtu v Magmě a skript pro vyhodnocení výsledků. Pro práci to naprosto stačí, hodnotit není moc co.

### 4. Hodnocení výsledků, jejich využitelnost 50 /100 (E)

Použitelnost výsledků se odvíjí od toho, zda je řešení z kapitoly 4.2 validní nebo ne. Osobně jsem k němu spíše skeptický, přinejmenším mi text práce nedává podklady pro to, abych mu věřil. Domnívám se, že po doplnění příslušných zdůvodnění by se práce mohla dobře uplatnit, minimálně jako podklad k rozhodování o tom, zda a jak používat zvolené techniky pro kryptoanalýzu podobných šifer.

## Celkové hodnocení 50 /100 (E)

Práce je nepochybně ambiciozní, jak co se týká tématu, tak jeho realizace. Problém vidím zejména v textové části, která od čtenáře očekává až příliš velkou znalost tématu a příslušných matematických principů a vůbec mu nepomáhá, pokud je nemá. Zároveň je z mého pohledu naprosto zásadní otázka, zda je zvolená metoda vytváření redukovaných variant šifry validní nebo ne. Pochybnosti také vyvolává, zda jsou kapitoly 1 a 2 vůbec přijatelné z pohledu citační etiky (zdroje jsou sice citovány, ale nepřipadá mi v pořádku, když je kapitola takřka doslovným překladem jednoho zdroje; jistě bylo možné doplnit aspoň vlastní komentáře studenta nebo jiných autorů). Za těchto okolností se spíše přikláním k tomu, že by bylo lepší textovou část práce přepracovat. Na druhou stranu musím uznat, že student odvedl značné množství vysoce specializované práce a že nedostatky v mých znalostech nejsou jeho chybou. Navrhuji proto práci hodnotit známkou E-dostatečně, s výhledem na zlepšení (klidně až na A), pokud student svoji práci před komisí obhájí.

## Otázky k obhajobě

Vysvětlete prosím, proč je vaše volba redukce šifry z kapitoly 4.2 validní. Jak pro LSFR tak pro NSFR.

# Instrukce

## Splnění zadání

Posuďte, zda předložená ZP dostatečně a v souladu se zadáním obsahově vymezuje cíle, správně je formuluje a v dostatečné kvalitě naplňuje. V komentáři uveďte body zadání, které nebyly splněny, posuďte závažnost, dopady a případně i příčiny jednotlivých nedostatků. Pokud zadání svou náročností vybočuje ze standardů pro daný typ práce nebo student případně vypracoval ZP nad rámec zadání, popište, jak se to projevilo na požadované kvalitě splnění zadání a jakým způsobem toto ovlivnilo výsledné hodnocení.

## Písemná část práce

Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části. Dále posuďte, zda předložená ZP je po věcné stránce v pořádku, případně vyskytují-li se v práci věcné chyby nebo nepřesnosti.

Zhodnoťte dále logickou strukturu ZP, návaznosti jednotlivých kapitol a pochopitelnost textu pro čtenáře. Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 52/2021, článek 3.

Posuďte, zda student využil a správně citoval relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami. Zhodnoťte, zda převzatý software a jiná autorská díla, byly v ZP použity v souladu s licenčními podmínkami.

## Nepísemná část, přílohy

Dle charakteru práce se případně vyjádřete k nepísemné části ZP. Například: SW dílo – kvalita vytvořeného programu a vhodnost a přiměřenost technologií, které byly využité od vývoje až po nasazení. HW – funkční vzorek – použité technologie a nástroje, Výzkumná a experimentální práce – opakovatelnost experimentů.

## Hodnocení výsledků, jejich využitelnost

Dle charakteru práce zhodnoťte možnosti nasazení výsledků práce v praxi nebo uveďte, zda výsledky ZP rozšiřují již publikované známé výsledky nebo přinášející zcela nové poznatky.

## Celkové hodnocení

Shrňte stránky ZP, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení nemusí být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích. Obecně platí, že bezvadně splněné zadání je hodnoceno klasifikačním stupněm A.