FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

# Posudek oponenta závěrečné práce

| | |
|---|---|
| **Oponent práce:** | Mgr. Tomáš Rabas |
| **Student:** | Bc. Jiří Hájek |
| **Název práce:** | Testování náhodnosti proudové šifry Elephant |
| **Obor / specializace:** | Počítačová bezpečnost |
| **Vytvořeno dne:** | 4. června 2023 |

## Hodnotící kritéria

### 1. Splnění zadání

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

Instructions:
"1. Describe the Elephant cipher from the LWC project and at least five tests from the NIST Statistical Test Suite."
- Šifra Elephant byla s jednou lehkou výhradou dobře popsána. Testů NIST bylo popsáno a vysvětleno i s příklady celých 10.
"2. Describe and implement the Monomial for testing the randomness of binary sequences. "
- Monominální test byl popsán a vysvětlen v kapitole 4.2 opět i s příkladem.
V práci jsem nenalezl, zda je její implementace převzata či je vlastní.
"3. Apply the above tests to the Elephant cipher and compare the results."
- Všechny testy byly aplikovány na šifru Elephant a výsledky porovnány.
"4. In addition, try applying the Cube testers on the Elephant cipher."
- Cube tester byl také popsán a zároveň i aplikován na šifru Elephant.

### 2. Písemná část práce 90 /100 (A)

Práce je až na výjimky velmi dobře čitelná a danou problematiku dobře a pochopitelně předává čtenáři i za pomoci mnoho vlastních příkladů, pomocí kterých vysvětluje všechny koncepty.
Zdroje se zdají být dobře citovány, u většiny kapitol je autorem přiznáno odkud vzal inspiraci pomocí "adopted from".

Drobné nedostatky či nejasnosti:
1) V kapitole 1.1.3 je v tvrzení 2 použit termín periodická posloupnost, která není předtím

definovaná (a odlišena např. od částečně periodické posloupnosti). I přesto, že čtenář tuto definici může znát, vzhledem k tomu, že je zásadní pro dané tvrzení ("sekvence je periodická právě tehdy když..."), doporučil bych ji doplnit.
2) V kapitole 1.1.3 v příkladu 1 jsou 3 početní chyby kdy zřejmě došlo k záměně posunu x3 ≪ 7 za rotaci x3 ≪ 7.
3) V kapitole 1.1.4 se využívá konsenzus posouvání LFSR doleva, kdežto v kapitole 1.1.3 se dle Figure 1.3 a cvičení 1 používá LFSR s posunutím vpravo. Pro čtenáře by bylo mírně čitelnější, kdyby byla konvence směru zachována.
4) a) V kapitole 1.3 je napsáno u popisu šifry Elephant, že "where encryption is performed using counter mode".
Counter mode je obvykle použit pro blokové šifry. Zde by chtělo dovysvětlit jak je to myšleno pro tuto proudovou šifru.
Z jejího popisu není zřejmé, kde/co je použito jako čítač (counter) a jak se zvyšuje.
b) Podobně jako v bodě a, chtělo by čtenáři vysvětlit pojem "counter sum MAC function" příkladem a při popisu šifry jeho naplnění případně vysvětlit.
Soudím, že jsou obě tvrzení pouze převzaty z [4])
5) V kapitole 1.1.4 je poměrně podrobně vysvětlena generická houbovitá konstrukce (https://keccak.team/sponge_duplex.html.). To působí dojmem, že šifra Elephant ji nějakým způsobem využívá, byť to není přímo napsáno. Bohužel pak není vyjasněno jak (např. upřesnění rate r a kapacity c, jak probíhá absorbční a squeezing fáze u šifry Elephant) a z podrobnější popisu šifry v kapitole 1.3 to neplyne.
6) V kapitole 4.1.1 jsou definovány poměrně náročné abstraktní pojmy a vzorečky, které nemusí nutně čtenář znát. Oproti zbytku práce, která je velmi vstřícná vzhledem k pochopení čtenářem, je tahle kapitole trochu uspěchána a chtěla by více rozepsat a čtenáři přiblížit.
7) V kapitole 5.2 je psáno "As for the nonce, we wish to find a subset of input bits that is likely to receive less mixing during the nonce setup process than other bits [11].
This is likely to be either at the beginning or the end of the nonce bit-vector [11]."
- Není mi jasné, jak to vychází ze zdroje [11], kde autoři "present results of tests performed on eSTREAM proposals", mezi které ale Elephant nepatřil, a domnívám se, že to závisí od schématu šifry a nelze to zobecnit.
8) V kapitole 5.1 je pro 0.001105 a 0.004236 použit popis "very low p-values". Domnívám se, že je to příliš silné slovo pro tyto hodnoty (i přestože je níže napsáno, že to není "major issue"), obzvláště když v kapitole 5.2 je p-hodnota 0.0023 označena za "relatively high".
9) V conclusion se píše: "After that, we presented the results of our tests. Dumbo passed the vast majority of tests from NIST's STS,
failing only two out of ten iterations of the runs test and one iteration of the random excursions test".
- domnívám se, že je zde oponuto testování prvních dvou keystreamů s klíčem ks1 a ks2. V takto obecném shrnutí testování, by měly být zahrnuty, jinak to uměle snižuje kvalitu šifry Elephant. (Kapitola 5.1: "Keystreams ks1 and ks2 passed all of the tests, while ks3 failed the Runs test and one of the eight Random excursions tests.")
V případě runs testu by pak správné shrnutí mělo znít "2 z 30 testů neprošly", nikoli "2 z 10 testů neprošly".

## 3. Nepísemná část, přílohy

90 /100 (A)

### 4. Hodnocení výsledků, jejich využitelnost 90 /100 (A)

Byla podána poměrně robustní statistická analýza šifry Elephant, která byla vážným kandidátem na standard v Lightweight cryptography.
I přesto, že byla testována její nejslabší varianta (s 112 bity bezpečnosti a limitem na množství šifrovaných dat 2^46 bloků) v plné formě (není oslabena např. nižším počtem iterací vnitřní permutace Spongent-pi), student narazil na zajímavé výsledky u balančního testu u Cube testeru.
Považuji to za poměrně kvalitní výsledek sloužící k dalšímu hodnocení bezpečnosti tohoto kryptosystému.

## Celkové hodnocení 90 /100 (A)

Student splnil celé zadání a to i včetně bodů, které nebyly nutné (Cube tester, vícero testů NIST).
Z práce bylo vidět snahu autora pochopit a následně dobře vysvětlit problematiku, které se práce týká.
Oceňuji velké množství příkladů i dobře čitelný výklad.
Práci lze považovat za velmi kvalitní.

## Otázky k obhajobě

Pro statistické testy NIST STS student použil implementaci z https://github.com/arcetri/sts.
Jak student implementoval d-monomial test a Cube tester - pomocí vlastní nebo cizí implementace?

# 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.