Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

OPONENTSKÝ POSUDEK BAKALÁŘSKÉ PRÁCE

Student: **Patrik Kováč** **Oponent:** **Ing. Petr Žáček, Ph.D.**

Studijní program: **Inženýrská informatika**
Studijní obor: **Softwarové inženýrství**
Akademický rok: **2021/2022**

Téma bakalářské práce: **Kryptoanalytické algoritmy pro kvantové počítače**

Hodnocení práce:		**A**	**B**	**C**	**D**	**E**	**F**
		Hodnocení: A – nejlepší; F - nevyhovující					
1.	Aktuálnost řešeného tématu	☒	☐	☐	☐	☐	☐
2.	Obtížnost zadaného úkolu	☒	☐	☐	☐	☐	☐
3.	Splnění všech bodů zadání	☐	☐	☒	☐	☐	☐
4.	Vhodnost zvolené metody řešení	☐	☐	☐	☒	☐	☐
5.	Logické členění práce	☐	☐	☐	☒	☐	☐
6.	Úroveň jazykového zpracování	☐	☐	☐	☒	☐	☐
7.	Formální úroveň práce	☐	☐	☐	☐	☒	☐
8.	Práce s literaturou a její citace	☐	☐	☐	☐	☒	☐
9.	Úroveň zpracování teoretické části	☐	☐	☐	☒	☐	☐
10.	Kvalita zpracování praktické části	☐	☐	☐	☐	☒	☐
11.	Dosažené výsledky práce	☐	☐	☐	☐	☒	☐
12.	Přínos práce a její využití	☐	☐	☐	☐	☒	☐

Celkové hodnocení práce:
Výsledná známka není průměrem výše uvedených hodnocení. Známku uvede oponent dle svého uvážení dle klasifikační stupnice ECTS:
A – výborně, B – velmi dobře, C – dobře, D – uspokojivě, E – dostatečně, F – nedostatečně.
Stupeň F znamená též „nedoporučuji práci k obhajobě“.

Předloženou bakalářskou práci doporučuji k obhajobě a navrhuji hodnocení

E - dostatečně.

V případě hodnocení stupněm „F – nedostatečně“ uveďte do připomínek a slovního vyjádření hlavní nedostatky práce a důvody tohoto hodnocení.

Otázky k obhajobě:
1. Můžete prosím rozvést rozdíl mezi hashovacím algoritmem a šifrovacím algoritmem ?
2. Podle vašeho textu není příliš jasné, jestli DSA je šifrovací algoritmus či ne. Můžete to prosím objasnit ?
3. Můžete prosím objasnit, zda lze pomocí kryptografie eliptických křivek generovat pseudonáhodná čísla ? viz kapitola 1.3.3.5
4. Lze pomocí QKD šifrovat ?
5. Jste si opravdu jistý, že jeden bit dokáže pojmout dva bity informace ? Viz kapitola 2.1.1
6. Je nebo není možné Simonův algoritmus aplikovat v kryptologii ?
7. K čemu slouží Diffie-Hellman ? Lze jej využít k šifrování, jak uvádíte v kapitole 4.3 ?

8. Jaký vliv má tedy příchod kvantových počítačů na bezpečnost symetrické kryptografie ?

Další připomínky, vyjádření, náměty k obhajobě práce (možno pokračovat i na další stránce):
Práce se věnovala velmi aktuálnímu a zajímavému tématu. Právě o to je větší škoda, jak téma student vypracoval, protože potenciál práce byl obrovský ... Právě na první pohled práce budí dojem, že byla sepsána za pár posledních dní před odevzdáním a následně poslána přímo do tisku… bez patřičné kontroly. Student mnohdy pouze překládá či parafrázuje dostupnou literaturu bez hlubšího zamyšlení a celkově je práce strukturována zmateně -> dokonce některé nadpisy neodpovídají dalšímu textu či se pak věci opakují (Nadpis kapitoly 5, kapitola 3.2 a pak kapitoly 4.1 a 4.2). Výsledkem je práce, kterou lze označit jako "hromadu" nelogicky "splácaných" dat s pochybnou informační hodnotou …. Navíc, spousta obsahu má v sobě chybné interpretace, chyby a chybně použitou terminologii … (viz otázky k obhajobě).

Co se týká praktických implementací Shorova a Groovrova algoritmu, tak zde je také hodnota skoro nulová, protože se jedná z 98 procent o stejný kód jako v uvedeném zdroji. Jedinou úpravou jsou řádky pro navázání spojení a přeložené komentáře do českého jazyka … Každopádně, je potřeba uvést, že jsou nad rámec zadání.

Po formální stránce se práce jeví opravdu "neuhlazeným" dojmem, obtížně se čte a často vícekrát popisují jednu věc pořád dokola, viz kapitola 2.1.1. Student si navíc v práci několikrát protiřečí -> uvádí jednu věc a pak ji následně v dalším textu vyvrací nebo popírá … (opět viz otázky k obhajobě).

Nicméně, i když je práce kvalitativně na pomezí uznání a obsahuje významné nedostatky, tak musím konstantovat, že všechny body zadání jsou splněny a doporučuji tedy práci k obhajobě. Po úspěšné obhajobě, s podmínkou zodpovězení všech otázek, doporučuji práci hodnotit stupněm E - dostatečně.

Datum 1. 6. 2022 Podpis oponenta bakalářské práce