

OPONENTNÍ POSUDEK ZÁVĚREČNÉ KVALIFIKAČNÍ PRÁCE

Autor závěrečné práce: David Salač

Název práce: Distributed application for cryptanalysis of public-key cryptosystems

Oponent práce Martin Plešinger

Pracoviště oponenta Katedra matematiky a didaktiky matematiky, FP, TUL

A. Kvalita abstraktu, klíčová slova odpovídají náplni práce	Výborně (1)
B. Rozsah a zpracování rešerše	Velmi dobře (2)
C. Řešení práce po teoretické stránce	Výborně mínus (1-)
D. Vhodnost, přiměřenost použité metodiky	Výborně (1)
E. Úroveň zpracování výsledků a diskuse	Výborně mínus (1-)
F. Vlastní přínos k řešené problematice	Výborně mínus (1-)
G. Formulace závěru práce	Výborně mínus (1-)
H. Splnění zadání (cílů) práce	Splněno
I. Skladba, správnost a úplnost citací literárních údajů	Velmi dobře (2)
J. Typografická a jazyková úroveň (vč. pravopisu)	Výborně mínus (1-)
K. Formální náležitosti práce (struktura textu, řazení kapitol, přehlednost ilustrací)	Výborně mínus (1-)

Komentáře či připomínky:

V první řadě bych rád vyzdvihl fakt, že práce je psaná anglicky a v LaTeXu, což (bohužel ani jedno) není v našich zeměpisných šířkách a délkách obvyklé. Angličtina vykazuje jisté rezervy, stejně jako celková formální úprava práce (překlepy, typografické záležitosti, drobné nekonzistence v matematickém značení, atp.; za všechny bych uvedl např. chybu v nadpisu kapitoly 2.3 (str. 18), kde skutečně nemusela být přehlédnuta).

Uvědomuji si, že práce není primárně matematická, přesto by si některá matematická tvrzení zasloužila upřesnit (chybějící předpoklady; náznaky důkazů tam, kde jsou užitečné / důležité). Text místy vykazuje jistou nevyváženost: ze začátku jsou matematická tvrzení (i netriviální) předkládána plynule v "plain-textu" (což nevádí), ale v kap. 2.6 (str. 24) se náhle vynoří dvě definice, věta a lemma diskutující relativně běžné matematické objekty. Proč? Domnívám se, že je to dáno prací s různými prameny. Už na první pohled ne zcela zřejmých tvrzení (např. pro jak velká čísla je ten který algoritmus ještě vhodný) bych uvítal detailnější odkazy do literatury, aby si čtenář mohl udělat lepší představu o kontextu, ve kterém byly takové odhady odvozeny.

K popisu implementace ani k implementaci samotné nemám žádné vážnější výhrady.

...pokračuje na straně 2

Celkové zhodnocení:

Téma je velmi aktuální s řadou otevřených výzev a zasloužilo by si, dle mého názoru, i mnohem delší a systematictější práci. Text je i přes shora uvedené výhrady solidní, doplněný reálnou implementací a základními experimenty. Celkově práci doporučuji k obhajobě a navrhuji hodnocení kvalifikačním stupněm "výborně minus".

Otázky k obhajobě:

1. V kapitole 2.6.1 (str. 26) je zmíněn blokový Lanczosův algoritmus. Tušíte, k čemu se zde používá?
2. Kapitola 2 končí zmínkou Shorova algoritmu (mimořádně bez odkazu na literaturu; str. 27), který je vhodný pro implementaci na tzv. kvantových počítačích, které zatím nemáme. Nebylo by možné jejich chod, nebo alespoň chod algoritmu emulovat na klasickém počítači (čistě z důvodů ilustrace jak algoritmus pracuje)?
3. V kapitole 5 se používá jeden až tři výpočetní uzly. Bylo by lepší větší počet výpočetních uzlů alespoň emulovat, případně použít služeb některého z dostupných výpočetních clusterů / superpočítačů (např. IT4I Salomon v Ostravě). Jak očekáváte, že bude záviset čas výpočtu na počtu výpočetních uzlů?

Celková klasifikace:

Práce splňuje požadavky na udělení akademického titulu, a proto ji doporučuji k obhajobě

Navrhuji tuto práci klasifikovat stupněm Výborně minus (1-)

V Liberci

dne 1. června 2017

Podpisem současně potvrzuji, že nejsem v žádném osobním vztahu k autorovi práce

.....

podpis oponenta