Posudek

☒vedoucího ❑oponenta
☒diplomové ❑bakalářské práce

Autorka: Barbora Galaczová

Název práce: Bezpečnost a použitelnost základních hashovacích funkcí, zejména MD-5, SHA-1 a SHA-2

Jméno vedoucího: Doc. RNDr. Jiří Tůma, DrSc

Matematická úroveň:
❑vynikající ❑velmi dobrá ❑průměrná ☒podprůměrná ❑nevyhovující

Grafická, jazyková a formální úroveň:
❑vynikající ❑velmi dobrá ☒průměrná ❑podprůměrná ❑nevyhovující

Výsledky:
❑originální ❑původní i převzaté ☒netriviální kompilace ☒citované z literatury ❑opsané

Použité metody:
❑nestandardní ☒standardní ❑obojí

Aplikovatelnost:
❑přínos pro teorii ❑přínos pro praxi ❑přínos pro praxi i teorii ☒bez přínosu ❑nedovedu posoudit

Věcné chyby:
❑téměř žádné ❑vzhledem k rozsahu a pojednávanému tématu přiměřený počet ☒méně podstatné četné ❑závažné

Tiskové chyby:
❑téměř žádné ❑vzhledem k rozsahu a pojednávanému tématu přiměřený počet ☒četné

Celková úroveň práce:
❑vynikající ❑velmi dobrá ☒průměrná ☒podprůměrná ❑nevyhovující

Práci
☒doporučuji ❑nedoporučuji
uznat jako diplomovou. Návrh klasifikace přikládám na zvláštním papíru.

Připomínky a vyjádření vedoucího:

Práce je výhradně kompilační a zpracovává literaturu až po rok 2008 včetně (dvě z prací vyšly tiskem až v roce 2009), pozdější práce s jedinou výjimkou nejsou uvažovány. Vzhledem k tomu, že bezpečnost hašovacích funkcí je velmi aktivní oblastí výzkumu, jde o významné omezení, které hodnotu práce snižuje.

Podrobně je popsána metoda hledání kolizí u funkcí MD-5 a SHA-1. V obou případech jde o značně netriviální postupy a jejich popis tvoří zhruba polovinu textu práce.
Práce je zatížena řadou drobných věcných chyb, které sice nebrání srozumitelnosti pro čtenáře, který je s problematikou obeznámen, ale patrně by způsobila problémy u někoho, kdo by se chtěl s problematikou pomocí této práce seznámit.

Jako příklad lze uvést definici váhy BSDR reprezentace na str. 7, kde je sice uvedena správná formule, ale slovní vysvětlení definice říká, že jde o součet nenulových hodnot, přestože formulka ukazuje, že jde o počet nenulových hodnot.

V některých částech je koncentrace drobných věcných chyb značná. Jako příklad lze uvést část 5.3. Mluví se zde v prvním odstavci o *útocích prvního řádu*, přestože jde o hledání kolizí. Dále se zde hovoří o hledání *kolizí druhého řádu*, ve skutečnosti jde ale o hledání druhého vzoru. Ani útoky prvního řádu ani kolize druhého řádu nepatří mezi definované pojmy.
V předposledním odstavci jsou dvě věty vzájemně ve sporu. Ve druhé větě má autorka patrně na mysli jednu z generických slabin Merkle-Damgardovy iterativní konstrukce hašovacích funkcí, která říká, že druhý vzoru pro dlouhé zprávy lze vždy najít rychleji než by tomu bylo při útoku hrubou silou. Vzhledem k tomu, že v práci jsou probírány výhradně funkce založené na Merkle-Damgardově konstrukci, bylo by vhodné uvést přehled generických slobain této konstrukce hned v úvodu práce.

V práci je řada překlepů, někde je terminologie používána dosti volně. Například je na některých místech zaměňována *inicializační hodnota* s *iniciační hodnotou*.

Větší pozornost také měla být věnována sjednocení značení při přebírání výsledků z literatury. Bitová rotace slov vlevo je značena *ROTL*, zatímco rotace vpravo je značena *RR*. Na str. 13 je místo symbolu pro xor náhle používán symbol pro tenzorový součin.

Poslední připomínka je ke způsobu uvádění referencí. V případě více než tří autorů práce autorka vždy uvádí pouze jméno prvního z nich a doplní *a kol*. V případě sborníků někde uvádí jména editorů, jinde je neuvádí.

Během obhajoby by autorka měla vysvětlit, proč zvolila při vlastní implementaci softwaru variantu modifikace jednotlivých bitů, která podle autorky způsobila, že její implementace je zhruba třináctkrát pomalejší, než implementace V. Klímy z roku 2006.

Místo, datum, podpis vedoucího:

Praha, 12.9.2011