Posudek bakalářské práce

předložené na Matematicko-fyzikální fakultě
Univerzity Karlovy v Praze

☐ posudek vedoucího ☒ **posudek oponenta**

Autor/ka: Martin Suchan

Název práce: Porovnání současných a nových našívacích funkcí

Studijní program a obor: Informatika, Programování

Rok odevzdání: 2007

Jméno a tituly ~~vedoucího~~/oponenta: Daniel Joščák, Mgr.

Pracoviště: Katedra Algebry

	excelentní	**odpovídající**	**slabší**	**nevyhovující**
Náročnost zadaného tématu		x		
Míra splnění zadání	x			
Struktura textové části práce	x			
Jazyková a typografická úroveň	x			
Analýza		x		
Vývojová dokumentace			x	
Uživatelská dokumentace		x		
Kvalita zpracování softwarové části		x		
Stabilita aplikace		x		

Nejvýznamnější klady: Súhrny prehľad takéhoto počtu používaných ale aj menej používaných hašovacích funkcií spolu s krátkou analýzou bezpečnosti a naprogramovaním všetkých popísaných funkcií si vyžaduje veľkú orientáciu v odbore, výborné programátorské schopnosti a značné množstvo času. Téma práce je nanajvýš aktuálna. Významným počinom je naprogramovanie a popis 3 nových algoritmov (DN hash, Grindahl, Radiogatun), ktoré je nezávislé od autorov týchto algoritmov a umožňuje ich porovnanie. Ukazuje to na schopnosť autora reagovať na posledné výsledky v obore. Kladne hodnotím aj nástroj pre diferenčnú kryptoanalýzu a krokovanie hašovacích funkcií, ktorý je dobrou pomôckou pri skúmaní implementovaných hashovacích funkcií.

Nejzávažnější nedostatky: Vážne nedostatky som v práci nenašiel. Uvediem niekoľko postrehov a odporúčaní. V kap. 1.6 by bolo vhodné využitie hašovacích funkcií popísať na konkrétnych príkladoch, nie je zrejmé ako sa hašovacie funkcie v daných situáciách používajú a prečo. V kap. 2 u obrázkov kompresných funkcií by bolo vhodnejšie uviesť, že ide o jeden „krok" kompresnej funkcie. Nesúhlasí popis funkcie SHA-2 a obr. 5. Jednotlivé stavebné bloky kompresných funkcií (napr. nelineárne funkcie) by bolo zaujímavé popísať presnejšie, prípadne pokúsiť sa výber stavebných blokov zdôvodniť. Autor prípadne mohol uviesť viac subjektívnych postrehov k jednotlivým algoritmom. Za nedostatok považujem vývojovú dokumentáciu k projektu, k niektorým funkciám (Radiogatun) chýba odkaz na zdroj v samotnom kóde. Ako istú náhradu za vývojovú dokumentáciu však môžeme považovať samotný text bakalárskej práce, ktorý jednotlivé funkcie popisuje dostatočne.

Další poznámky: Neštandardne pôsobí používanie tučného fontu (bold) pre matematický text a vzorce. V zozname použitej literatúry chýba u niektorých položiek (napr. 29, 32, 41, 42) podrobnejšia referencia (napr. url).

	výborně	**velmi dobře**	**dobře**	**neprospěl/a**
Návrh známky	**x**			

Datum: 16. 6. 2007

Podpis: [redacted]