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~~: doc. RNDr. Jiří Tůma, DrSc.

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: Implemetace řady nejužívanějších hašovacích funkcí jako nejnovějších návrhů připravovaných pro celosvětové hledání nového standardu pro hašovací funkce a porovnání rychlosti těchto implementací. Toto porovnání sice nevychází z optimalizovných implementací, vzájemný poměr rychlostí u autorových implemetací a u optimalizovných implementací tam, kde jsou k dispozici, vychází přibližně stejně.

Dalším kladem je velmi užitečný program Visualhash pro sledování binárních a modulárních rozdílů registrů při dvou paralelních výpočtech téže hašovací funkce. Bude pro nás výbornou pomůckou při dalším zkoumání existence kolizí, zejména v hašovací funkci MD5.

Nejzávažnější nedostatky:

Výhrady mám poze k některým poněkud nepřesným formulacím. Jako poněkud nešťastnou považuj formulaci v definici hašovací funkce hned v prvním odstavci na str. 6, *že pro libovolně zvolené* $y\in Y$ *není možné najít takovou hodnotu* $x\in X$, *že* $y=f(x)$. Podobně i pro kolize. Až o tři odstavce dále je vysvětleno, že nemožností se myslí výpočetní nemožnost v současně době.

V anglických termínech uváděných dole na str. 6 by mělo být *resistance* místo *resistant*.

Otázkou je rovněž, jak rozumět výrazu, že *bezkoliznost hašovací funkce je nejsilnější požadavek*. Vzhledem k tomu, že první odhalenou slabinou užívaných hašovacích funkcí je práve existence kolizí, a že z této existence neplyne možnost hledat druhé vzory nebo dokonce možnost invertovat hašovací funkci, raději bych požadavek neexistence rychlého algoritmu pro hledání kolizí považoval za nejslabší požadavek na hašovací funkce.

Na straně 7 ve druhém odstavci se tvrdí, že hašovací funkce s délkou 128 bitů má obor hodnot 2^{128} možných hašů. Pokud vím, tak i u běžných funkcí jako je třeba MD5 to není dokázáno. Uvedené číslo je pouze horním odhadem.

Také bych byl opatrnější při formulaci, že v *množině* ***n*** *náhodných hašů nejsou žádné dva stejné*. V množině nikdy nejsou dva prvky stejné. Správnější formulace by mohla být např. *mezi* ***n*** *náhodnými hodnotami hašovací funkce nejsou dvě stejné*.

Výraz *vstupní blok dat pro hašovací funkci* také může vést k nedorozumění. Vstupní data jsou totož rozdělena na bloky pevné velikosti, např. 512 bitů u MD5. Výraz vstupní blok dat bez dalšího vysvětleni tak může být chápán jako blok dané velikosti, na které se vstupní data dělí.

V části 1.**6. Kryptografické využití hašovacích funkcí** zcela schází použití v elektronických podpisových schématech.

V přehledu alhoritmů pro hledání kolizí u MD4 schází zmínka o výsledcích prezentovaných na letošní konferenci *Fast Software Encryption*, kde k nalzení kolize stačí méně než dva výpočty hodnoty MD4.

Také formulace *Funkce SHA-0 se od SHA-1 liší jen přidáním jedné bitové rotace v expanzní funkci* je poněkud nedbalá. V SHA-1 je v expanzní funci přidána rotace o 1 bit.

V odevzdané implementaci programu Visualhash, které je součástí práce, je chyba ve výpočtu hodnoty modulárního rozdílu dvou registrů. Po upozornění pan Suchan chybu rychle opravil, takže současná verze, kterou mám k dipozici, již chybu neobsahuje.

Práce neobsahuje samostatnou vývojovou dokumentaci. Jde o práci převážně teoretickou, proto je za vývojovou dokumentaci možno částečně považovat samotný text bakalářské práce. Knihovna hašovacích funkcí je tvořena samostatnými implementacemi jednotlivých funkcí a vyžadovalal přípravu spíše v podobě vyhledání specifikací jednotlivých funkcí včetně návrhů nejnovějších funkcí. Tato příprava je v práci dobře sledovatelná.

Další poznámky: Na tomto místě bych rád vyzdvihnul naprostou samostatnost pana Suchana při vypracování bakalářské práce.

Díky této samostatnosti v práci zůstalo několik formulačních nepřesností, případně opomenutí. V žádném případě to ale hodnotu práce nesnižuje.

Hodnocení excelentní mi přijde jako zcela mimořádné, se kterým by se mělo trochu šetřit. Proto jsem v předchozí tabulce označil většinou hodnocení odpovídající. To ale nic nemění na tom, že jde o práci velmi kvalitní.

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

Datum: 11.6.2007

Podpis: