Posudek na bakalářskou práci

Adam Christov, Statistické testy hašovacích (= žvýkacích) funkcí

Cílem práce Adama Christova bylo jednak ověřit elementárními statistickými testy, že hašovací funkce MD5 má vlastnosti náhodného orákula, a dále ověřit nebo popřít nezávislost postačujících podmínek v různých implementacích algoritmu Wangové a dalších pro nalezení kolizí v této hašovací funkci.

Po popisu MD5 v první kapitole autor uvádí popis tří různých generátorů náhodných bitů (jeden vlastní) a výsledky testů náhodnosti a nezávislosti jednotlivých bitů v hodnotě kompresní funkce pro MD5. Dále uvádí test senzitivity výsledku kompresní funkce na změnu jednoho bitu vstupního bloku. První dva testy potvrzují, že kompresní funkce pro MD5 má vlastnosti náhodného orákula. Jsou to očekávané výsledky, nalezení jakékoliv závislosti v těchto testech by totiž ihned znamenalo oslabení kryptografických vlastností této funkce. Test senzitivity rovněž dává očekávané normální rozdělení množství bitů výstupu, které se změní po změně jednoho bitu vstupu.

Ve třetí části autor popisuje princip algoritmu Wangové a jeho zpřesnění a urychlení v pracích Klímy a Stevense.

Hlavní výsledky práce jsou obsažené ve čtvrté kapitole. Autor zde potvrzuje, že všechny podmínky v obou implementacích jsou splněné s pravděpodobností ½ až na podmínky, u kterých je pravděpodobnost na první pohled výrazně menší. Opravdu zajímavé je pak zjištění, že obě implementace obsahují dvojici podmínek (různých v různých implementacích), které nejsou nezávislé. Absence vysvětlení této závislosti je jedinou drobnou vadou této práce, je však třeba dodat, že to nebylo v zadání.

Práci lze stěží něco vytknout. Je napsána pečlivě, formulace jsou jasné a korektní, zadání práce bylo plně splněno.

Proto navrhuji práci přijmout jako práci bakalářskou a hodnotit ji známkou *výborně*

Doc. RNDr. Jiří Tůma, DrSc.
vedoucí práce

V Praze, 5.9.2006