POSUDEK VEDOUCÍHO DIPLOMOVÉ PRÁCE "PROBABILITY TESTING AND APPLICATION OF STATISTICAL TESTS IN CRYPTOGRAPHY"

PETRA NIŽNANSKÉHO

Jedná se o druhou verzi, neboť verzi první se autor rozhodl přepracovat. Z původní verze práce vynechal některé pasáže a soustředil se výhradně na aplikaci statických testů k hodnocení generátorů pseudonáhodných posloupností.

První kapitola je přehledem použitých statistických metod. Nejedná se o podrobný výklad, ale spíše o informativní popis bez odvození a důkazů. Je ponecháno na čtenáři, aby si podrobnosti potřebné k pochopení této úvodní kapitoly doplnil. Uvedené shrnutí je však věcně správné. Druhá kapitola je popisem několika statistických testů, které autor zamýšlí aplikovat k testování náhodnosti binárních posloupností. V této kapitole také navrhuje dva nové testy (Prime number test) a (Irreducible polynomial test). Ve třetí kapitole autor volí několik přirozených transformací binárních posloupností (např. cyklickou permutaci, komplement) a empiricky zkoumá, jak tyto transformace aplikované na binární posloupnosti ovlivní výsledky statistických testů popsaných v předchozí kapitole. Čtvrtá kapitola popisuje testy založené na faktu, že „generátor binárních posloupností je pseudonáhodným generátorem právě když nelze předpovídat další bity jím generovaných posloupností" a variantách výše uvedených statistických testů. V poslední kapitole jsou testy popsané ve druhé a čtvrté kapitole testovány posloupnosti generované pomocí generátorů jež byly vybranými kandidáty na hašovací funkci SHA-3 (nebo posloupnosti od takto generovaných posloupností odvozené).

Jak plyne z předchozího, jádrem práce je popis statistických testů pseudonáhodných generátorů a jejich variant. Autor se přitom neomezil jen na popis používaných testů, ale snažil se navrhnout i testy vlastní. Práce je prakticky orientovaná, studované testy jsou implementovány a použity v konkrétních případech. Teoretická analýza použitých testů je přítomna jen omezeně. Nejsem si ale jist, zdali existuje solidní teoretický základ používaných testů. Pokus o jeho vytvoření by dle mého názoru značně překračoval to, co lze od diplomové práce očekávat. Práce je psána anglicky; myslím, že na slušné úrovni. Celkem se domnívám, že splňuje požadavky kladené na dipomovou práci a jako diplomovou práci ji doporučuji uznat.

Mgr. Pavel Růžička, Ph.D.