Posudek vedoucího diplomové práce
Testy generátorů pseudonáhodných čísel
Olhy Jurečkové

Proudová šifra je symetrická šifra, kterou si lze představit tak, že zprávu (posloupnost bitů) bit po bitu vyxorujeme s výstupem pseudonáhodného generátoru, tedy algoritmu, který z tajného klíče délky n vyprodukuje posloupnost bitů délky $l(n) > n$. Každý, kdo má k dispozici stejný generátor, je pak schopen snadno zprávu dešifrovat. Bezpečnost proudové šifry se odvíjí od kvality použitého generátoru, v optimálním případě by se bezpečnost blížila Vernamově šifře One-Time Pad, přičemž proudové šifry umožňují šifrovat mnohem delší zprávy než je délka klíče.

V předložené práci jsou představeny statistické testy pseudonáhodných generátorů založené většinou na testu dobré shody. Ve třetí kapitole jsou to klasické testy frekvenční monobit test, poker test a runs test, které jsou součástí balíku statistických testů NIST. Čtvrtá kapitola ukazuje testy založené na zkoumání algebraické normální formy booleovských funkcí, v páté kapitole jsou pak testy korelační - dobře navržený generátor by neměl mít statisticky významnou korelaci mezi vstupem a výstupem. Šestá kapitola obsahuje návrh na využití pseudonáhodných generátorů pro Pollardovu rho metodu (zde jenom ve verzi pro faktorizace, zajímavější by to mohlo být pro diskrétní logaritmy).

Některé testy byly naimplementovány a změřeny pro generátory představené ve druhé kapitole.

Práce je napsána velmi pečlivě a srozumitelně, autorka zpracovala větší množství zdrojů do logicky strukturovaného textu. Po formální stránce lze vytknout jenom drobnosti. Jediným podstatným nedostatkem práce je její malá matematická náročnost, úvahy v práci uvedené detailněji jsou víceméně elementární. I když práce měla být především rukodělné povahy, její těžiště mělo být zejména v experimentech s různými testy a porovnávání získaných výsledků, nějaký obtížnější, byt' převzatý, související výsledek mohl být zařazen.

Tento problém je daný částečně povahou tématu - řada prací publikovaných na toto téma má srovnatelnou obtížnost, částečně je pak způsoben mou neschopností (nejen) nagenerovat dobré zadání - původním záměrem bylo studium projektu eStream (soutěž pro proudové šifry, která proběhla v letech 2004 - 2008) a pochopit metodiku vyhodnocování navržených šifer. Tato cesta se bohužel ukázala neprůchodná.

K zamyšlení jsou ještě výsledky měření v sedmé kapitole. Ty jsem viděl až po odevzdání práce, proto je připomínkuju až nyní.

- Dalo by se očekávat, že mnohý generátor bude mít navrženou maximální délku keystreamu, který lze generovat. Je tato skutečnost zohledněna v uvedených testech?
- Pro testování výkonu Pollardovy rho metody bylo lepší volit n ve tvaru součinu dvou zhruba stejně velkých prvočísel. Počet iterací by měl v průměru vyjít jako (malý) násobek odmocniny z nejmenšího prvočíselného dělitele. Z naměřených hodnot se zdá, že při využití šifer Decim a Geffe toto platit nebude. To pochopitelně může být způsobeno řadou faktorů. Nicméně, bylo by možné modifikovat uvedený postup tak, aby Geffe a Decim neprošly testem hypotézy 'posloupnost $f(x_0), ff(x_0), fff(x_0), \ldots$' splňuje narozeninový paradox (místo složeného čísla n bychom mohli uvažovat vhodnou mocninu dvou)?

Celkově si myslím, že předložená práce splnila zadání, doporučuji ji uznat jako diplomovou s hodnocením *velmi dobře*.

V Praze, 1. 9. 2015

Pavel Příhoda