Mgr. Marek Sýs Ph.D.
Fakulta informatiky
Masarykova univerzita
Botanická 68a, 602 00 Brno

POSUDEK DIPLOMOVÉ PRÁCE

Student: Michal Hajas
Název: Analysis of pseudorandom number generators based on lightweight cryptographic primitives
Vedoucí: Petr Švenda
Oponent: Marek Sýs

Zpráva: Cieľom práce bolo zmapovať rôzne typy náhodných generátorov a najbežnejšie typy útokov proti nim. Z praktického hľadiska si práca kladie za cieľ pridať vybrané krypto-funkcie do existujúceho nástroja CryptStreams a otestovať výstup z hľadiska náhodnosti.
Práca je delená celkovo do 5 kapitol. Za krátkym úvodom nasleduje kapitola venovaná pseudonáhodným generátorom (PRNG), ich celkovej charakteristike a požiadavkám na ne kladené. Kapitola sa zameriava na PRNG konštruované na báze kryptografických funkcií.
Kapitola popisuje útoky na PRNG resp. analýzy (lineárna a diferenciálna) funkcie a analýzy produkovaného výstupu za pomoci batérií testov náhodnosti.
Ďalšia kapitola sa detailne venuje nástroju CryptoStreams, ktorým možno jednoducho generovať dáta pomocou veľkého množstva kryptografických funkcií. Kapitola prezentuje výsledky unit testov jednotlivých funkcií a diskusiu k problematickým funkciám. Študent tu taktiež popisuje experiment zameraný na testovanie náhodnosti dát vygenerovaných pomocou vstupných dát rôzneho typu. Testovanie náhodnosti bolo realizované pomocou štandardných batérií testov a nového parametrizovaného testu BoolTest. Ďalej sú tu popísané rôzne PRNG, ktoré boli pridané do CryptoStreams, a ktoré boli v rámci experimentu otestované. Jedná sa konkrétne o 6 „čistých“ PRNG (napr. LCG, XorShift, Mersenne Twister) a 19 generátorov postavených na „jednoduchých“ krypto-primitívach.
V ďalšej kapitole sa nachádzajú výsledky (a ich interpretácia) viacerých experimentov zameraných na zistenie miery bezpečnosti jednotlivých funckcií, úspešnosť testov náhodnosti, vzájomné porovnanie jednotlivých batérií z TestU01 a porovnanie jednotlivých kofigurácií BoolTestu.

Práca ako celok je na veľmi dobre úrovni. Je vidieť, že študent venoval netriviálne množstvo času samotnému text, kde spracoval vhodným spôsobom 65 zdrojov. Najviac oceňujem praktickú časť práce, ktorá bola z časového hľadiska omnoho náročnejšia. Bolo doimplementovaných a otestovaných 25 funkcií čo znamenalo vygenerovať a stovky GB dát. Treba taktiež oceniť prehľadne spracované výsledky experimentov. Prepokladám, že budú samotné výsledky budú neskôr spracované do vedeckého článku. Práca splnila zadanie.

Práca má len málo negatív. Medzi ne patrí: obrázky 3.1, 3.2 s nulovou informačnou hodnotou, časť venovaná lineárnej a diferenciálnej kryptoanalýze je zbytočná a mohla byť vynechaná,
Po gramatickej stránke je práca dobrá, rovnako tak úroveň angličtiny. Nachádza sa tu minimálne množstvo gramatických chýb. Po formálnej stránke je kvalita práce taktiež dobrá.
Hodnocení: Doporučujem prácu uznať ako prácu diplomovú s hodnotením **A**

Datum: 17.1.2019

Marek Sýs