Posudok oponenta na bakalársku prácu

Luskáš Fuchs, Generátory pseudonáhodných čísel a útoky na ně.

Predložená bakalárska práca sa zaoberá generátormi pseudonáhodných čísiel (postupností), pričom sa zameriava hlavne na generátory založené na lineárnych posuvných registroch.

V úvode práce sú popísané niektoré štatistické testy, ktoré sa používajú ako testy náhodnosti pre číselné postupnosti. Kapitola 1 popisuje základné vlastnosti lineárnych posuvných registrov (LFSR), ako aj stručný popis nelineárnych posuvných registrov. V kapitole 1 sú taktiez popísané 2 generátory založené na lineárnych posuvných registroch. Druhá časť prvej kapitoly obsahuje prehľad základných útokov na popísané generátory pseudonáhodných postupností. Kapitola 2 sa venuje popisu základov takzvaných algebraických útokov, ktoré boli v poslednej dobe úspešne aplikované na viacero prúdových šifier.

Dobrú úroveň práce narušujú iba viaceré nepresnosti a preklepy, ktorých zoznam je uvedený nižšie. Práca by pre ilustratívnosť taktiež mohla obsahovať popis väčšieho množstva generátorov presudonáhodných postupností (napríklad popis ďalších typov generátorov založených na LFSR).

Predložená práca spĺňuje požiadavky kladené na bakalársku prácu.
Navrhujem hodnotenie

výborný (1)

Mgr. Michal Hojsík
Oponent práce

Poznámky k práci:

Strana 7:
zlé rozdelenie slova obsiahly,
zlé rozdelenie slova neexistuje.

Strana 8:
- "geberátor" namiesto generátor,
- "Ak nami vygenerované postupnosti prejdú viacerými testami, budú nerozlíšiteľné od náhodných a generátor je tým pádom vhodný na kryptografické účely." Ak postupnosť prejde viacerými testami, neznamená to, že je nerozlíšiteľná, ale len to, že je nerozlíšiteľná pomocou daných testov.

Strana 11:
"Dôkaz tohoto tvrdenia sa mi bohužiaľ nepodarilo nikde nájsť a ani vymyslieť." Tento dôkaz sa preberal na studentskom kryptografickom seminári pre 3. ročník a je ho možné nájsť napríklad v knihe Finite fields, Rudolf Lidl, Harald Niederreiter, P.M. Colm., Cambridge University Press, 1997.

"Veta: ... v lineárnom čase ... " riesenie sústavy lineárnych rovníc (uvedené v dôkaze vety) má približne kubickú zložitosť.

Strana 13:
– "Ľubovoľní boolovskú funkciu ... " má byť "Ľubovoľnú boolovskú funkciu stupňa menšieho alebo rovného d ...".

Strana 15:
"ideálne s nesúdeiteľnými" má byť "nesúdeliteľnými".

Strana 16:
–"Inými slovami sa skartuje c_i bitov registra A" lepšie by bolo "c_i bitov výstupu registra A".

Strana 17:
"Veta: ... útočník potrebuje výpočetný čas ..." má byť "útočník potrebuje najviac ... ", alebo "existuje útok hrubou silou v čase ...". Veta totiž nedokazuje neexistenciu lepšieho útoku.

Strana 18:
– "potom vieme bit aktuálny bit" opakuje sa slovo bit.
"aj keď počet obrazov x_n, ktoré máme k dispozícii ... " má byť " ... počet vzorov x_n, ... ".

Strana 19:
– "Veta: ... k dispozícii je $O(l)$, ... " má byť $O(l_A)$.

Strana 23:
– "Pripomenieme, že i-ty bit výstupu generátora môžeme vyjadriť ..." nasleduje ale rovnica popisujúca výstup takzvaného filtrovacieho generátora o ktorom v práci nie je zmienka. Vyššie v práci sa spomína kombinačný generátor, rovnica ale popisuje filtrovací generátor.

Strana 24:
– V dôkaze vety je pre $C = A \cup B$ uvedená "rovnosť" "$|C| = |A| + |B|$", ktorá samozrejme neplatí, pretože zanedbáva prienik množín A a B, ktorý v danom prípade môže byť neprázdny.

Pri popise algebraických útokov by bolo vhodné poznamenať, že uvedené výpočty sa neodohrávajú v $GF(2)[x]$ ale vo faktor okruhu $GF(2)[x]/(x^2 - x)$.

Autor pri niektorých referenciách neuvádza ani vydavateľa, ani rok publikácie.