Szczecin, 11.07.2022

STRESZCZENIE ROZPRAWY DOKTORSKIEJ

Metody oceny jakości algorytmów generowania kluczy rundowych w szyfrach blokowych

Autor: mgr inż. Michał Apolinarski
Promotor: dr hab. inż. Krzysztof Chmiel
Promotor pomocniczy: dr inż. Anna Grocholewska-Czuryło

Algorytmy generowania kluczy rundowych wykorzystywane są w szyfrach blokowych do wygenerowania z klucza głównego (przeważnie o długości pomiędzy 64 a 256 bitów), zbioru kluczy rundowych wykorzystywanych następnie, w rundach (iteracjach), właściwego procesu szyfrowania lub deszyfrowania. Istotną cechą jest to, aby wygenerowane przez ten algorytm klucze rundowe posiadały właściwości statystyczne zbliżone do ciągów losowych, co wpływa na proces kryptoanalizy szyfru.

Do oceny właściwości statystycznych ciągów pseudolosowych (za takie ciągi należy uznać szyfrogram oraz klucze rundowe), zastosowanie mają różnego rodzaju testy statystyczne, m.in. testy NIST SP800-22 wykorzystane w konkursie na standard AES do oceny szyfrów blokowych.

W rozprawie wykorzystano testy NIST SP800-22 do oceny algorytmów generowania kluczy rundowych, na podstawie sekwencji kluczy rundowych, o długości kilkuset lub kilku tysięcy bitów dla pojedynczej wartości klucza głównego.

Projektując algorytm generowania kluczy rundowych należy znaleźć kompromis pomiędzy szybkością generowania kluczy, a bezpieczeństwem, w szczególności kiedy projektowany szyfr ma być „lekki" (ang. *lightweight*) czyli stosowany w środowisku o małych, ograniczonych zasobach, np. karta RFID. Przy takich ograniczeniach problematyczne staje się określenie optymalnych struktur spełniających zadane kryteria. Zatem podczas projektowania algorytmu generowania kluczy rundowych warto rozważyć i przetestować różne warianty zastosowanych operacji, np. rotacji (cyklicznego przesunięcia), permutacji, podstawień, stałych lub innych przekształceń.

Celem rozprawy jest zaproponowanie wykorzystania testów statystycznych oraz analizy skupień, jako elementu wspomagającego i wzbogacającego ocenę konstrukcji algorytmów generowania kluczy rundowych w szyfrach blokowych. Poszczególne zadania cząstkowe zrealizowane w rozprawie to:

- Opracowanie metody testowania i oceny algorytmów generowania kluczy rundowych opartej na testach statystycznych oraz analizie skupień.
- Przegląd i analiza różnych konstrukcji algorytmów generowania kluczy rundowych szyfrów blokowych (m.in. DES, LOKI97, KASUMI, AES (Rijndael), Serpent, PP-1, PP-2, IDEA, RC6, Speck).
- Ocena teoretyczna oraz praktyczna jakości wybranych algorytmów generowania kluczy rundowych.

11.07.2022