Siedlce, dnia 26.05.2008

mgr Mirosław Szaban
Akademia Podlaska w Siedlcach
Instytut Informatyki
Zakład Systemów Operacyjnych
ul. Sienkiewicza 51
08-110 Siedlce

Autoreferat

Rozprawa doktorska poświęcona jest zastosowaniu *Automatów Komórkowych (AK)* w różnych dziedzinach kryptografii z kluczem symetrycznym. Głównym celem mojej pracy jest wykazanie możliwości efektywnego zastosowania AK w szyfrowaniu strumieniowym i blokowym.

We współczesnym świecie, kiedy jednym z najcenniejszych "surowców" jest informacja, zachodzi potrzeba jej skutecznej ochrony. Wartość informacji jest tym większa im szybciej zostanie wykorzystana. Rozwój technologii przekazywania informacji, w szczególności informacji elektronicznej oraz przesyłania jej przez globalną sieć umożliwia błyskawiczne przekazywanie danych. Niestety, globalna sieć jest siecią niezabezpieczoną, a usługi przekazywania informacji cechują się różnym stopniem bezpieczeństwa. Powszechnie znanym jest fakt, iż nie istnieje usługa całkowicie bezpieczna. Zatem wartość usług przesyłania informacji wyznaczana jest przez stopień trudności jej złamania. Im trudniej i dłużej przebiega proces odczytania przechwyconej i zaszyfrowanej wiadomości, tym wyższą jakość kryptograficzną prezentuje algorytm szyfrujący wykorzystywany przez usługi transportu danych.

Klasyczne algorytmy szyfrująco-deszyfrujące cechują się dużym zużyciem czasu działania i/lub pochłanianiem ogromnych ilości zasobów sprzętowych. W tym celu niezbędne jest zastąpienie ich nowymi technikami kryptograficznymi pozwalającymi szybko, przy małym zużyciu zasobów sprzętowych a przede wszystkim skutecznie zabezpieczyć cenne dane przed ich pobieraniem, przetwarzaniem i upublicznianiem. W rozprawie doktorskiej rozpatrywane będą metody poprawiające skuteczność działania algorytmów ochrony rosnącej ilości danych elektronicznych, zabezpieczania szybko rozwijających się metod transakcji elektronicznych, także mogących mieć zastosowanie w coraz częściej pojawiającym się użyciu podpisów elektronicznych.

W rozprawie doktorskiej, do poszukiwania AK właściwych odpowiednim technikom kryptograficznym, posłużą różne metody poszukiwań między innymi techniki heurystyczne ze szczególnym uwzględnieniem *Algorytmu Genetycznego (AG)*.

W pierwszej części rozprawy będą przedstawione wiadomości i definicje niezbędne w dalszych częściach rozprawy. Wprowadzone zostaną definicje AK i reguł AK oraz opis i prezentacja działania. Opisane zostaną techniki kryptograficzne, w kontekście, których stosowane są proponowane AK. Końcową część rozdziału stanowić będą opisy heurystycznych metod poszukiwania rozwiązań w problemach NP-trudnych, głównie opis AG.

Rozdział drugi rozprawy przedstawia poszukiwanie właściwych reguł klasycznego automatu komórkowego, które w nim zastosowane spełniać będą zdefiniowane własności szyfrów strumieniowych. Przestrzeń reguł stosowanych w klasycznych AK jest przestrzenią ogromną i problem jej przeszukania należy do klasy

problemów NP-trudnych. W tym celu jedyne skuteczne metody to metody heurystyczne. Dlatego utworzony został algorytm genetyczny bazujący na zaadoptowanych odpowiednio klasycznych operatorach genetycznych w celu znalezienia odpowiednich reguł AK. Nowym elementem pojawiającym się w algorytmie jest budowa osobnika populacji. W dotychczas znanych pracach osobnikami algorytmów genetycznych były osobniki jednoelementowe (jednochromosomowe), w badaniach pojawiły się osobniki algorytmu genetycznego złożone z wielu elementów (reguł - chromosomów). Przeprowadzone eksperymenty (z użyciem właściwie skonfigurowanego AG) wyszukania reguł AK, wyłoniły zestawy reguł niejednorodnych AK, które mogłyby pełnić rolę generatorów kluczy stosowanych w szyfrach strumieniowych, kryptografii z kluczem symetrycznym. Odnalezione zbiory reguł spełniają wymagania stawiane generatorom liczb pseudolosowych. Zbiory te przeszły pomyślnie testy FIPS PUB 140-2 publikowane przez NIST (National Institute of Standards and Technology), określające przynależność do grupy generatorów pseudolosowych, co stanowi, iż mogą być stosowane jako generatory kluczy kryptograficznych. Dodatkowym efektem badań jest wykazanie istnienia i wskazanie zestawów reguł, których nie należy stosować, gdyż ich użycie w AK prowadzi do wygenerowania słabych kryptograficznie kluczy.

Rozdział trzeci rozprawy porusza zagadnienie zastosowania AK w szyfrowaniu blokowym. Zaproponowano użycie AK jako narzędzia mogącego zastąpić S-bloki (S-box'y). Automat komórkowy jako narzędzie równoważne Uniwersalnej Maszynie Turing'a może wykonać każde obliczenia Boolowskie, a operacje wykonywane przez S-bloki są oparte na operacjach na funkcjach Boolowskich. Wykazano, iż klasyczne jednorodne AK (AK z jedną regułą) posiadają właściwości przewyższające własności klasycznych S-bloków. Znaleziono i przetestowano reguły AK, które spełniają własności *Nieliniowości* i *Autokorelacji*, a wartości uzyskane dla tych własności są lepsze niż w klasycznych S-blokach. Opisano i porównano wyniki współcześnie tworzonych Tablic S-bloków z otrzymanymi rozwiązaniami dla S-bloków opartych na AK i stwierdzono wyższą jakość działania AK jako S-bloku. Poza tym, AK pozwala na wykonywanie funkcji przypisanych S-blokom bez potrzeby tworzenia Tablicy S-bloku, (co miało miejsce w algorytmie DES, czy też, AES), które to zadanie jest zadaniem czasochłonnym i kosztochłonnym.

Kolejne badania skupiają się wokół uzyskania coraz lepszych wyników AK jako S-bloków, ze szczególnym uwzględnieniem niejednorodnych i odwracalnych AK. Ponadto przeprowadzone zostaną badania mające na celu sprawdzenie innych własności S-bloków dla S-bloków opartych na AK, oraz zastosowanie AK jako dynamicznych S-bloków.