POLSKO-JAPOŃSKA WYŻSZA SZKOŁA TECHNIK KOMPUTEROWYCH

ポーランド日本情報工科大学

Warszawa, 19 sierpnia 2010 r.

prof. dr hab. Witold Kosiński
Polsko-Japońska Wyższa Szkoła
Technik Komputerowych, Warszawa
Uniwersytet Kazimierza Wielkiego
Bydgoszcz

Opinia na temat rozprawy doktorskiej mgra Mirosława Szabana :

Zastosowanie automatów komórkowych w kryptografii z kluczem symetrycznym

Niniejszą recenzję przygotowałem na zlecenie Rady Wydziału Informatyki Polsko-Japońskiej Wyższej Szkoły Techniki Komputerowych, która prowadzi przewód doktorski mgra Mirosława Szabana. Promotorem rozprawy jest dr habil. inż. Franciszek Seredyński, profesor PJWSTK.

Uwagi wstępne

Koniec ubiegłego wieku i początek obecnego to czas, kiedy kryptologia stała się dostępną i powszechną dyscypliną naukową. Powstaje wiele publikacji na temat kryptografii, dokonuje sie rozstrzygnięć kolejnego konkursu na nowy standard szyfrowania, w Polsce oraz na świecie organizowane są konferencje naukowe tematycznie związane z bezpieczeństwem informacji.

Szyfrowanie jest sposobem ochrony informacji przed zinterpretowaniem ich przez osoby niepowołane. Jednocześnie jest to jedyny znany i skuteczny sposób realizacji ochrony informacji przesyłanej w sieci, kanałami otwartymi. W szyfrowaniu informacji wykorzystuje się szyfry - tj. rodzinę przekształceń służących do nadawania informacji postaci niezrozumiałej lub bezużytecznej dla napastnika. Z szyfrowaniem związane są takie pojęcia jak: nauka o szyfrach, nauka o konstruowaniu i stosowaniu szyfrów, zwana kryptografią i kryptoanaliza - nauka o łamaniu szyfrów. Sam proces szyfrowania polega na przekształceniu za pomocą funkcji oraz hasła szyfrowania (tzw. klucza) informacji jawnej w inną zwaną kryptogramem lub tekstem zaszyfrowanym. Proces odwrotny, nazywany deszyfrowaniem, polega na tym, że kryptogram jest przekształcany z powrotem w oryginalną informację jawną za pomocą pewnej funkcji matematycznej i klucza.

Przedstawiona do recenzji rozprawa doktorska odnosi się do wymienionych działów, zajmuje się jednak głownie konstrukcją automatów komórkowych (AK), które byłaby w stanie wspomagać algorytmy z kluczem symetrycznym.

ul. Koszykowa 86, 02-008 Warszawa; tel: (+22) 58-44-500, fax: (+22) 58-44-501;
e-mail: pjwstk@pjwstk.edu.pl; www.pjwstk.edu.pl

Automaty komórkowe należą do podstawowych narzędzi inteligencji obliczeniowej, znanej dotąd pod nazwą sztucznej inteligencji. Skoro wspomina się sztuczną inteligencję, to pojawia się bezpośrednie skojarzenie do jej wykorzystania w kryptoanalizie, łamaniu szyfrów czy wydobywanie z szyfrogramów tekstów oryginalnych, ukrytych. Autor niniejszej rozprawy nie poszedł w tym kierunku. Zaproponował coś innego.

Głównym celem rozprawy, stawianym przez Doktoranta, jest wykazanie możliwości efektywnego zastosowania automatów komórkowych w szyfrowaniu blokowym i strumieniowym. W tym celu Doktorant skupia się na rozwiązaniu dwóch zagadnień: proponuje nową postać skrzynki podstawieniowej w szyfrach blokowych, której konstrukcja wykorzystuje jednowymiarowy jednorodny AK, oraz proponuje konstrukcję jednowymiarowego niejednorodnego (tj. z działajacymi co najmniej dwoma regułami aktualzacji stanów) AK służącego jako generator liczb pseudolosowych - pełniących rolę kluczy na użytek szyfrowania strumieniowego. Dla obu proponowanych rozwiązań doktorant przeprowadza intensywne badania teoretyczno-eksperymentalne i pokazuje wysoką jakość tych rozwiazań na tle rozwiązań aktualnie proponowanych w literaturze.

Zawartość rozprawy

Rozprawa skład się z 10 rozdziałów, bibliografi, która zawiera 164 pozycji, spisów rysunków, tablic oraz dwóch dodatków. Praca liczy 167 stron.

Rozdział 1 zawiera cel i zakres pracy, motywacje do podjęcia tematyki badawczej, będącej przedmiotem rozprawy. Tutaj też została sformułowana teza. Rozdział 2 to wprowadzenie podstaw teoretycznych z zakresu kryptologii, dotyczących wyników badań przedstawionych w tej pracy.

Rozdział 3 opisuje narzędzie jakim jest automat komórkowy. W rozdziale tym przedstawiona została definicja AK, sposób jego działania, a także klasyfikacja AK. Ponadto przedstawione zostały wybrane typy AK.

W rozdziale 4 zaprezentowano narzędzia (w postaci algorytmów heurystycznych), których użyto do poszukiwania konfiguracji początkowych oraz zbioru reguł AK. Do przeszukania ogromnej przestrzeni podzbiorów reguł AK, które w nim zastosowane mogłyby pełnić rolę generatorów kluczy stosowanych w szyfrach strumieniowych, użyto algorytmu genetycznego. Podobnie, przy pomocy algorytmu największego wzrostu przeszukano ogromną przestrzeń konfiguracji początkowych AK stanowiących element zaproponowanej skrzynki podstawieniowej konstruowanej z użyciem AK.

Rozdział 5 rozprawy porusza zagadnienie zastosowania AK w szyfrowaniu blokowym. Zaproponowano w nim użycie AK jako narzędzia mogącego

zastąpić skrzynki podstawieniowe. AK posiadające własności obliczeniowe ekwiwalentne uniwersalnej maszynie Turinga może realizować w szczególności funkcje boolowskie, występujące w analizie skrzynek podstawieniowych. Doktorant proponuje konstrukcję skrzynki podstawieniowej w pełni realizowanej przez AK, dla którego znalezione i przetestowane reguły uzyskują wysokie wartości funkcji nieliniowości, autokorelacji, balansu i dSAC.

W rozdziale 6 porównano skrzynki podstawieniowe realizowane z użyciem AK utworzone zgodnie z konstrukcją zaproponowaną w rozdziale 5, ze skrzynkami podstawieniowymi w postaci tablic używanych w algorytmie DES oraz skrzynkami równoważnymi skrzynkom algorytmu AES. Doktorant wykazał, iż elementarne AK realizujące skrzynki podstawieniowe charakteryzują się wartościami funkcji testujących przewyższającymi wartości osiągane przez klasyczne skrzynki podstawieniowe.

Rozdział 7 zawiera analizę własności skrzynek podstawieniowych o liczbie bitów wyjściowych mniejszej od liczby bitów wejściowych oraz wpływ na ich własności kryptograficzne zależności pomiędzy liczbą bitów w blokach wejściowym i wyjściowym. Przedstawiono też wyniki analizy skalowalności skrzynek podstawieniowych w pełni realizowanych przez AK. Porównano uzyskane wyniki z wynikami uzyskiwanymi dla współcześnie tworzonych w postaci tablic skrzynek podstawieniowych.

W rozdziale 8 przedstawiono propozycję zastosowania AK w tworzeniu dynamicznych skrzynek podstawieniowych. Pod tym kątem przeprowadzono analizę parametrów AK, a następnie zaproponowano konstrukcję dynamicznych skrzynek podstawieniowych realizowanych przez AK. Ponadto przeprowadzono analizę własności kryptograficznych dynamicznych skrzynek podstawieniowych w pełni realizowanych przez AK zgodnie z zaproponowaną konstrukcją.

Rozdział 9 rozprawy zawiera opis metod i wyniki poszukiwania reguł elementarnego AK, które spełniać będą kryteria stawiane szyfrom strumieniowym. Na użytek poszukiwań utworzony został AG bazujący na zaadoptowanych odpowiednio operatorach klasycznych. Przeprowadzone eksperymenty wyłoniły zestawy reguł, które zastosowane w jednowymiarowym niejednorodnym AK mogłyby pełnić rolę generatorów kluczy stosowanych w szyfrach strumieniowych kryptografii z kluczem symetrycznym. Generator skonstruowany z użyciem AK i wyselekcjonowanych zbiorów reguł spełnia wymagania stawiane generatorom liczb pseudolosowych (PRNG). Doktorant po przeprowadzeniu testów stwierdził, że ciągi generowane przez AK z użyciem wyselekcjonowanych zbiorów reguł przeszły pomyślnie testy FIPS PUB 140-2 publikowane przez National Institute of Standards and Technology (NIST) określające przynależność do grupy PRNG. Potwierdził tym, że AK z wyselekcjonowanymi zbiorami reguł mogą być stosowane jako generatory kluczy kryptograficznych.

Podsumowanie prowadzonych rozważań w całej pracy oraz przedstawienie obszarów, w których badania będą kontynuowane w przyszłości, składają się na Rozdział 10.

Ocena wyników rozprawy

Przedstawione przez Doktoranta metody z zakresu kryptologii wprowadzają czytelnika w podstawową treść rozprawy. W celu wykazania tezy pracy doktorant przeprowadza dość dokładną analizę istniejących modeli i klasyfikację automatów komórkowych. Przedstawia też analizę aktualnego stanu badań światowych w zakresie możliwości zastosowania automatów komórkowych w kryptologii. Następnie formułuje koncepcję wykorzystania AK do budowy szyfrów blokowych. To jest główny wynik pracy obok zaprezentowania algorytmów heurystycznych zastosowanych do poszukiwania konfiguracji początkowych oraz zbioru reguł AK, w ogromnej przestrzeni podzbiorów reguł AK. Obok tego wyniku Doktorant zaproponował i przebadał zestaw reguł dla jednowymiarowego niejednorodnego AK, który mogłyby pełnić rolę generatora kluczy stosowanych w szyfrach strumieniowych kryptografii z kluczem symetrycznym.

Do najważniejszych osiągnięć rozprawy chciałbym zaliczyć:

- konstrukcja skrzynki podstawieniowej z użyciem jednowymiarowego, jednorodnego automatu komórkowego oraz analizy kryteriów ich konstrukcji (podrozdział 5.3) i egzekucji, w tym
  - wyselekcjonowanie przykładowych skrzynek podstawieniowych o bloku wejściowym złożonym z 6 bitów i bloku wyjściowym złożonym z 4 bitów (podrozdział 6.2) oraz o bloku wejściowym i wyjściowym złożonym z 8 bitów (podrozdział 6.3) osiągających najlepsze z uzyskanych wartości własności kryptograficznych,
  - konstrukcja skrzynki podstawieniowej równoważnej tablicom algorytmu AES o bloku wejściowym i wyjściowym złożonym z 8 bitów (podrozdział 6.3),

- wykazanie, ze jakość skrzynek podstawieniowych skonstruowanych z użyciem jednowymiarowego, jednorodnego automatu komórkowego rośnie wraz ze wzrostem liczby jej bitów wejściowych (podrozdział 7.3),

- konstrukcja dynamicznej skrzynki podstawieniowej (generatora skrzynek podstawieniowych) z użyciem jednowymiarowego, jednorodnego automatu komórkowego (podrozdział 8.2) oraz analiza jej własności o wyselekcjonowanie przykładowych skrzynek podstawieniowych o bloku

wejściowym i wyjściowym złożonym z 8 bitów (podrozdział 8.3), wygenerowanych przez generator skrzynek podstawieniowych, osiągających najlepsze z uzyskanych wartości własności kryptograficznych,

- konstrukcja generatora pseudolosowych ciągów bitowych z użyciem jednowymiarowego, niejednorodnego automatu komórkowego i wyselekcjonowanie, przy użyciu algorytmu genetycznego, zbioru właściwych reguł (funkcji przejścia) jednowymiarowego, niejednorodnego automatu komórkowego, dla których ciągi bitowe generowane przez skonstruowany generator spełniają testy wchodzące w skład standardu FIPS Pub 140-2 (podrozdział 9.4).

Rozprawa dowodzi dużej pomysłowości i biegłego opanowania programowania przez doktoranta. Na zakończenie recenzji stwierdzam, że rozprawa mgr. Mirosława SZABANA zawiera oryginalny dorobek naukowy, a wyniki w niej zamieszczone niosą do uprawianej przez Niego dyscypliny naukowej bardzo wartościowy wkład.

Należy na zakończenie tego punktu stwierdzić, że teza pracy o istnieniu alternatywego dla obecnie powszechnego podejścia do konstruowania skrzynek podstawieniowych i szyfrowania strumieniowego wykorzystującego jednowymiarowe, jednorodne i niejednorodne automaty komórkowe, jednego z narzędzi inteligencji obliczeniowej, została wykazana.

Uwagi krytyczne i dyskusyjne

1. Mam kilka pytań do początkowych rozdziałów:
   1. str. 21-23 opis działania skrzynek podstawieniowych nie należy do mocnej strony części wstepnej.
   2. str. 35 przedstawiając reguły Doktorant nie przedstawił jasno problemu warunków brzegowych, ograniczając się od razu tylko do cyklicznego automatu.
   3. str. 55 do wzoru (5.8) brak komentarza o możliwości znikania lewej strony, tj. wartości funkcji $\hat{F}_f(\omega)$ dla pewnych ω, skoro wyrazy sumy mogą przyjmować wartości -1 i1.
   4. str. 10, w.9 o.d. występuje błąd merytoryczny wypowiedzi w zdaniu :*Odnalezione zbiory reguł spełniają wymagania stawiane PRNG.* Powinno być: *Generator liczb pseudolosowych skonstruowany z użyciem AK i wyselekcjonowanych reguł spełnia wymagania stawiane PRNG.*
   5. str. 10, w.3 o.d. występuje: *...z w takcie...*, a powinno być: *w trakcie...*.
   6. str. 33 (i dalszych: 34, 37, 39, 41, 63, 127, 137) błedne użycie apos-

trofu w odmianie imienia i nazwiska Stephen Wolfram , np. w pracy występuje Stephen'a Wolfram'a, a jest to błędne.

2. W rozdziale 9 Doktorant proponuje konstrukcję generatora liczb pseudolosowych z użyciem AK, jednakże nie prezentuje formalnie takiej konstrukcji, jak to wykonał w rozdziale 5 w przypadku konstrukcji skrzynki podstawieniowej realizowanej z użyciem AK.

3. Może warto byłoby przeprowadzić kryptoanalizę skrzynek podstawieniowych konstruowanych z użyciem AK przedstawionych w rozdziałach 5-8, co mogłoby mieć dodatkowy obraz jakości takich konstrukcji.

4. Recenzent chciałby zobaczyć zaimplementowany algorytm szyfrująco–deszyfrujący realizowany z użyciem konstrukcji zaproponowanych w rozprawie, a także porównanie go pod względem jakości oraz czasu szyfrowania-deszyfrowania z szyframi klasycznymi i znanymi dzisiaj.

Proszę o ustosunkowanie się do tych uwag. Powyższe uwagi nie mają wpływu na moją wysoką ocenę pracy.

Uwagi końcowe

Przesłana do mnie do recenzji rozprawa doktorska mgr. Mirosława SZABANA p.t. Zastosowanie automatów komórkowych w kryptografii z kluczem symetrycznym promotorstwa dr. hab. Franciszka Seredyńskiego, prof. PJWSTK, spełnia wszystkie wymogi stawiane rozprawom doktorskim (Ustawa o stopniach naukowych i o tytule naukowym oraz o stopniach i tytule w zakresie sztuki z dnia 14 marca 2003 roku, Dziennik Ustaw Nr 65, poz. 595) w dziedzinie nauk technicznych w dyscyplinie informatyka. W związku z tym wnioskuję o dopuszczenie doktoranta Pana mgra Mirosława Szabana do dalszych etapów przewodu doktorskiego.

Ponadto wnoszę o wyróżnienie tej rozprawy ze względu na uzyskanie przez Doktoranta znaczących rezultatów oraz opublikowanie (bądź przyjęcie do druku) części z nich w dwóch czasopismach z tzw. listy filadelfijskiej Journal of Supercomputing i Journal of Cellular Automata, opublikowanie 3 artykułów w serii LNCS, wydawnictwa Springer, jak też opublikowanie kilkunastu artykułów w materiałach znanych międzynarodowych konferencji naukowych.

Witold Kosiński