Prof. dr hab. inż. Franciszek Seredyński
Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie
Wydział Matematyczno – Przyrodniczy. Szkoła Nauk Ścisłych
ul. Wóycickiego 1/3, 01-938 Warszawa

Warszawa, 5.11.2013

RECENZJA

rozprawy doktorskiej mgr inż. Piotra Sucha nt.
„Szyfrowanie z użyciem automatów komórkowych dwuwymiarowych"

1. Problematyka naukowa oraz przedmiot rozprawy

Gwałtowny rozwój technologii komunikacyjno-informatycznych związanych z Internetem oraz sieciami mobilnymi i bezprzewodowymi i związanych z nimi usług opartych na wymianie informacji, takich jak e-biznes, e-bankowość, e-urząd, itp., spowodowały, że bezpieczeństwo przekazywanej informacji staje się jednym z kluczowych zagadnień nauki, a kryptografia stała się jedną z czołowych dziedzin informatyki. Rozwój współczesnej kryptografii odbywa się w warunkach swoistego wyścigu między rosnącą odpornością tworzonych standardów kryptograficznych na ataki kryptograficzne, a rozwojem mocy obliczeniowych współczesnych komputerów, która może być wykorzystana do złamania tych algorytmów. Z drugiej strony można też obserwować rozszerzanie się wachlarza zastosowań kryptografii i wymogów co do algorytmów kryptograficznych. Dziś kryptografia jest stosowana nie tylko do szyfrowania bardzo ważnych informacji i danych (duże wymagania kryptograficzne), ale również do szyfrowania, np. rozmów telefonicznych w sieciach komórkowych, czy też do szyfrowania danych przesyłanych między współpracującymi urzadzeniami (umiarkowane wymagania kryptograficzne). Z tych właśnie powodów, pomimo istnienia klasycznych narzędzi kryptograficznych wykorzystujących określone działy matematyki, poszukuje się dzisiaj nowych perspektywicznych narzędzi i algorytmów kryptograficznych zapewniających określony poziom bezpieczeństwa kryptograficznego, ale też jednocześnie charakteryzujących się umiarkowanym czasem przetwarzania.

Recenzowana rozprawa doktorska mgr inż. Piotra Sucha wpisuje się dobrze w ten nurt poszukiwań nowych metod i narzędzi kryptograficznych. W swojej pracy skupia się on na eksploracji możliwości stosowania dla celów kryptograficznych narzędzia jakim są automaty komórkowe (AK). AK były już w przeszłości stosowane w kryptografii i wciąż uważane są za obiecujące narzędzie do tworzenia takich algorytmów, zarówno z powodu swoich możliwości obliczeniowych jak też z powodu możliwości efektywnej obliczeniowo implementacji.

Doktorant zaproponował w swojej rozprawie oryginalną konstrukcję algorytmu szyfrującego opartego na koncepcji AK. Przeprowadził szereg badań teoretyczno-eksperymentalnych i pokazał wysoką jakość proponowanego rozwiązania na tle rozwiązań aktualnie znanych w literaturze. Postawiony w rozprawie cel został ściśle określony oraz w pełni osiągnięty. Rozważane w rozprawie zagadnienia są aktualne i w istotny sposób wpisują się w obszar informatyki. Rozprawa może zatem być przedstawiona jako monografia doktorska w dziedzinie informatyki.

2. Treść rozprawy

Rozprawa jest poprzedzona Wstępem, po którym następuje 6 numerowanych rozdziałów, Podsumowanie, Bibliografia zawierająca 38 pozycji literaturowych oraz Załączniki. Całość pracy obejmuje 89 stron i ma ona charakter teoretyczno-eksperymentalny. Wyniki własne doktoranta przedstawione są w rozdziałach 3,4, 5 i 6.

Dwa pierwsze bardzo krótkie 2-stronicowe rozdziały prezentują odpowiednio: koncepcję AK (Rozdział 1) oraz zastosowania AK w kryptografii (Rozdział 2).

W Rozdziale 3 doktorant przedstawił własną autorską koncepcję algorytmu szyfrującego 2DCARotate z kluczem tajnym. Algorytm ten całkowicie oparty jest na paradygmacie obliczeniowym, które oferują AK. Konstrukcja algorytmu jest niewątpliwie interesująca i nowatorska. Algorytm szyfrujący wykorzystuje trzy AK: automat główny CACrypt (AK odwracalny) służący do szyfrowania to 2-wymiarowy AK, dwa pozostałe AK automaty jednowymiarowe CALink (AK nieodwracalny) i CATop (AK odwracalny) mające charakter pomocniczy.

Doktorant na wstępie tego rozdziału przedstawia motywacje powstania opracowanego algorytmu szyfrującego, które związane są z koncepcjami wcześniejszych prac Horwarda Gutowitza. Przedstawia główne założenia algorytmu szyfrującego i jego ideę w postaci trzech współpracujących ze sobą AK oraz prezentuje sam algorytm w postaci pseudokodu. Następnie szczegółowo omawia podstawową kwestię związaną z każdym z tych automatów, a mianowicie budowę reguł AK odpowiedzialnych za zmianę stanu automatów. Kolejnymi kwestiami omawianymi w tym rozdziale to budowa klucza szyfrującego/deszyfrującego oraz przygotowanie automatów do szyfrowania. Rozdział kończy się omówieniem trzech faz działania algorytmu: fazy szyfrującej, fazy przełączającej oraz fazy rozpraszającej.

Kolejny rozdział, Rozdział 4 poświęcony jest statystycznej analizie proponowanego algorytmu szyfrującego. Rozdział ten rozpoczyna się od przeglądu kilkunastu testów statystycznych stosowanych powszechnie do oceny jakości statystycznej pseudolosowych danych. Następnie doktorant omawia oprogramowanie Access zawierające grupę testów przeznaczonych do weryfikacji modułów kryptograficznych, opracowane przez National Institute of Standards and Technology (NIST). Oprogramowanie to zostało użyte przez niego do wykonania testów statystycznych. Zostały przedstawione wyniki wykonanych testów, dla których danymi wejściowymi były dane generowane przez zaproponowany algorytm szyfrujący. Dane te były uzyskane dla różnych parametrów algorytmu szyfrującego, co pozwoliło na ustalenie optymalnych parametrów algorytmu. Następnie tym samym narzędziem przetestowane znane aktualnie algorytmy szyfrujące, takie jak DES, 3DES, BlowFish oraz Rijandel. Porównanie tych wyników z wynikami uzyskanymi dla opracowanego algorytmu szyfrującego pozwoliło ustalić, że jakość zaproponowanego szyfru nie odbiega od jakości znanych standardów kryptograficznych, lub jest wyższe w przypadku porównania go z szyfrem BlowFish. Proponowany algorytm szyfrujący został też przetestowany z użyciem oprogramowania realizującego tzw. metodę gradacyjną opracowaną w IPIPAN. Wyniki przeprowadzonych testów tą metodą potwierdziły wyniki uzyskane wcześniej z użyciem narzędzia Access.

Rozdział 5 to krótki 4-stronicowy rozdział poświęcony kryptoanalizie autorskiego algorytmu szyfrującego. Doktorant zrealizował program, który określa stopień nieliniowości przekształceń geometrycznych w fazie rozpraszania algorytmu szyfrującego i zadeklarował bardzo wysoką nieliniowość uzyskaną w trakcie obliczeń. Zawarte w rozprawie elementy analizy liniowej i różnicowej algorytmu szyfrującego również prowadzą do pozytywnych konkluzji dotyczących algorytmu.

W ostatnim numerowanym rozdziale, Rozdziale 6, Doktorant rozważał możliwości sprzętowej realizacji algorytmu szyfrującego. Automaty komórkowe, które są środowiskiem obliczeniowym wykorzystanym do stworzenia koncepcji algorytmu szyfrującego, charakteryzują się tzw. masową równoległością i doskonale nadają się do wykonywania w środowisku obliczeń równoległych, bądź do realizacji sprzętowej z użyciem układów FPGA. Doktorant wykorzystał język VHDL służący do komputerowego projektowania układów cyfrowych typu FPGA, w celu opisu algorytmu szyfru-

jącego i uzyskał w ten sposób model sprzętowy algorytmu umożliwiający badanie jego wydajności w przypadku sprzętowej realizacji. Przeprowadzone badania pozwoliły stwierdzić, że implementacja sprzętowa algorytmu umożliwiłaby przyśpieszenie obliczeń o jeden lub nawet dwa rzędy wielkości w stosunku do realizacji algorytmu na maszynie sekwencyjnej.

Rozprawa kończy się podsumowaniem uzyskanych wyników i wnioskami uzyskanymi na podstawie analizy wyników.

3. Najistotniejsze osiągnięcia przedstawione w rozprawie

Rozprawa doktorska mgra inż. Piotra Sucha zawiera nowe, oryginalne wyniki zastosowania automatów komórkowych w kryptografii z kluczem symetrycznym. Do najistotniejszych osiągnięć rozprawy zaliczyć należy:

- opracowanie nowego algorytmu szyfrowania z kluczem symetrycznym bazującego na koncepcjach jedno- oraz dwuwymiarowego automatu komórkowego oraz opracowanie operacji rozpraszania informacji w szyfrogramie, realizowanych z użyciem tych automatów
- zbadanie własności statystycznych ciągów szyfrogramu i wykazanie wysokiej jakości tworzonych szyfrogramów, porównywalnej z jakością szyfrogramów uzyskiwanych z użyciem znanych standardów kryptograficznych
- utworzenie z użyciem języka VHDL modelu symulacyjnego sprzętowej realizacji algorytmu kryptograficznego i wykazanie wysokiej wydajności takiej potencjalnej sprzętowej realizacji algorytmu.

4. Uwagi merytoryczne

W trakcie czytania rozprawy doktorskiej nasuwa się szereg uwagi, na które chciałbym uzyskać wyjaśnienie:

- W rozdziale 4 „Testy jakości" doktorant przechodzi od sekcji 4.1 Rodzaje testów do sekcji 4.2 Strategia wykonania testów, gdzie skupia się na technicznym opisie danych wejściowych/danych wynikowych oprogramowania Access zrealizowanego w NIST (brak tu odsyłacza do źródła skąd pobrano to oprogramowanie) pomijając kwestię jakie testy statystyczne są wykonywane przez to oprogramowanie; można się domyślać, że prawdopodobnie grupa trzecia i czwarta klasyfikacji wyników podanej na str. 37 dotyczy odpowiednio testów przedstawionych w sekcjach 4.1.15 i 4.1.16; nie jest jasne natomiast o jakie testy statystyczne chodzi w przypadku grupy pierwszej i drugiej; doktorant opisując wspomniane cztery grupy wyników, pisze: „Test ten generuje 148 wyników ...(grupa 2), podobnie jest dla innych grup – o jakie to wyniki chodzi ? Nie ma żadnego komentarza dotyczącego tych wyników.

- Przedstawione w postaci wykresów na rys. 19 – 47 wyniki testów są mało czytelne i brakuje do nich wyczerpujących komentarzy; nie jest jasne np. co jest na osiach X tych wykresów i dlaczego wartości podane na osi Y zmieniają się w zależności od testu i wykresu; podpisy pod rysunkami są mało informatywne, np. „Rys. 19. Testy 15"; jak doktorant rozumie pojęcie „zdany/niezdany test" ?

- Amerykańska instytucja NIST, którą doktorant przywołuje publikuje regularnie dokumenty np. FIPS 140-2, FIPS 140-3, FIPS 200 dotyczące, między innymi, minimalnych wymagań i zestawu testów dla generatorów liczb pseudolosowych używanych w kryptografii; czy istnieje jakiś związek między użytym oprogramowaniem Access a tymi dokumentami ?

- Nie jest jasne w jaki sposób doktorant obliczał w Rozdziale 5 wartość nieliniowości- podana na str. 67 definicja nieliniowości funkcji binarnej jest ogólna i niezbyt nadaje się do obliczeń numerycznych, a podany kod programu obliczeń nieliniowości jest użyteczny dla komputerów, ale nie dla ludzi; do obliczenia nieliniowości potrzebne są odpowiednio zdefiniowane funkcje boolowskie; definicja takiej funkcji przez doktoranta w postaci zdania (str. 67): „Funkcja boolowska zdefiniowana jako obroty kwadratem ma sześć argumentów i jeden bit wyniku" daleko odbiega od w miarę precyzyjnej definicji; doktorant nie wyjaśnia jak interpretuje wartość nieliniowości w kontekście algorytmu kryptograficznego; doktorant ostatecznie podaje liczbę 24 jako wynik obliczeń nieliniowości; co oznacza ta liczba i jaki jest zakres wartości nieliniowości dla tego algorytmu ?; jakiej konfiguracji algorytmu szyfrującego ta wartość dotyczy, bo przecież algorytm szyfrujący ma wiele parametrów, które wpływają na wartości nieliniowości i w związku z tym charakteryzuje się zakresem wartości nieliniowości.

5. Uwagi redakcyjne i edytorskie

Cechą charakterystyczną rozprawy z punktu widzenia języka oraz kwestii edytorskich jest jej bardzo duża skrótowość i lakoniczność i czasami mało precyzyjny język. Pewne rozdziały, jak np. rozdział 1, 2 oraz 5 są zbyt krótkie i przypominają sekcje artykułu. Czytając pracę zauważyłem tam następujące niedociągnięcia językowe bądź edytorskie:

- str. 8: „W pracy (Neumann, 1996) zdefiniował ..." – nieprawdziwy rok publikacji
- str. 11-13: lakoniczność, niekompletność i szereg nieprecyzyjnych pojęć w rozdziale 1 „Zasady budowy automatów komórkowych", brak odnośnika do literatury z której korzystał doktorant przygotowując ten rozdział, a w szczególności:
    - str. 11, podpis pod Rys. 1: „ Przykład automatu komórkowego wraz z jego stanami" – powinno być „Przykład binarnego automatu komórkowego"
    - str. 11, podpis pod Rys. 2. „Przykład otoczenia o wymiarze 1" – powinno być "Przykład sąsiedztwa o promieniu r =1"
    - brak informacji o takim pojęciu jak warunki brzegowe automatu
    - rysunki i tabele numeruje się zwykle wg. rozdziałów, a więc zamiast np. „Rys. 1" powinno być „Rys. 1.1"; opisy tabel daje się nad tabelami, a nie pod nimi
- str. 15-16: lakoniczność i szereg nieprecyzyjnych pojęć w rozdziale 2 „Automaty komórkowe w kryptologii"
    - z treści rozdziału wynika, że jego tytuł powinien brzmieć: „Automaty komórkowe w kryptografii"
    - bardzo skromny opis zastosowań AK w kryptografii, bez wskazania do jakich problemów kryptograficznych były one stosowane i z jakim skutkiem
    - str. 15: brak opisu zmiennych i oznaczeń we Wzorze 1 i Wzorze 2
    - str. 15: „zmiana bitu najbardziej odległego" – nieprecyzyjny opis

- str. 17, rozdział 3: „Nowy szyfr z automatami 2-wymiarowymi z obrotami" – niezgrabny, nieprecyzyjny tytuł
    - str. 17: „ilość reguł" – słowo „ilość" jest w całej pracy nieprawidłowo używane
    - str. 17/18 – rysunek powinien być całkowicie na jednej z tych stron, a jest przełamany na 2 części
    - str. 19: „automaty są niejednorodne" – brak wyjaśnienia co to oznacza
    - str. 19: „ma kształt podany, jak na Rys. 5" – niezgrabne określenie
    - str. 23: opis algorytmu zawiera taki krok: „przesuń się o jeden wiersz w dół" (?!)
- str. 31, rozdział 4, tytuł „Test jakości" – tytuł zbyt lakoniczny
    - str. 32: „z oczekiwanymi wynikam …" → „z oczekiwanymi wynikami …"
    - str. 18: „Wyznaczanie słów" – lakoniczny podpis pod rys. 18
    - str. 47: „Wyniki dla testów dla obrotów dwoma kwadratami i zewnętrznym" - niezręczne sformułowanie tytułu sekcji 4.3.5
    - str. 51, 52,61: „Radnom excursion" →"Random excursion".

6. Podsumowanie

Powyżej przedstawione uwagi merytoryczne oraz redakcyjne nie mają istotnego wpływu na jakość i wagę przedstawionych rozwiązań i nie obniżają wartości pracy. Doktorant zaproponował i zbadał interesujący algorytm kryptograficzny stosując w sposób twórczy metodologię automatów komórkowych. Uzyskane wyniki są interesujące zarówno dla kryptografii jak też dla obszaru wiedzy jaką reprezentują automaty komórkowe. Są one dobrą bazą startową do dalszych badań w zakresie bezpieczeństwa kryptograficznego z użyciem metodologii automatów komórkowych. Podsumowując, stwierdzam, że przedstawiona do oceny rozprawa doktorska mgr inż. Piotra Sucha pt.: „Szyfrowanie z użyciem automatów komórkowych dwuwymiarowych " spełnia wymagania stawiane rozprawom doktorskim przez obowiązującą ustawę o stopniach i tytule naukowym. W konsekwencji, może ona stać się przedmiotem publicznej obrony. Wnoszę zatem o dopuszczenie mgr inż. Piotra Sucha do dalszych etapów przewodu doktorskiego.