Politechnika Warszawska
Wydział Elektroniki i Technik Informacyjnych

Warszawa, 20 grudnia 2016 r.

D z i e k a n a t

Uprzejmie informuję, że na Wydziale Elektroniki i Technik Informacyjnych Politechniki Warszawskiej odbędzie się w dniu 3 stycznia 2017 r. publiczna obrona rozprawy doktorskiej

mgr Omara Reyad

temat: "New Constructions of Elliptic Curves-based Pseudo-random Number Generators"

promotor – prof. dr hab. inż. Zbigniew Kotulski z Politechniki Warszawskiej

recenzenci:
dr hab. inż. Janusz Stokłosa, prof. w Wyższej Szkole Bankowej w Poznaniu
dr hab. inż. Jerzy Pejaś, prof. Zachodniopomorskiego Uniwersytetu Technologicznego w Szczecinie

Obrona odbędzie się w dniu 3 stycznia 2017 r. w sali 116 na Wydziale Elektroniki i Technik Informacyjnych – Gmach im. Janusza Groszkowskiego, Warszawa, ul. Nowowiejska 15/19; początek godz. 10.30.

Po adresem: **www.elka.pw.edu.pl/Wydzial/Rada-Wydzialu/Harmonogram-obron-doktorskich-streszczenia-i-recenzje** zapewniony jest na stronie Wydziału dostęp do tekstów streszczenia rozprawy i recenzji, jak również do tekstu rozprawy umieszczonej w Bazie Wiedzy Politechniki Warszawskiej.

Dziekan

prof. dr hab. inż. Krzysztof Zaremba

Mgr Omar Reyad

“New Constructions of Elliptic Curves-based Pseudo-random Number Generators”

“Nowe konstrukcje generatorów liczb pseudolosowych oparte na krzywych eliptycznych”

promotor: prof. dr hab. Inż. Zbigniew Kotulski

Celem niniejszej pracy jest wykorzystanie krzywych eliptycznych nad ciałami skończonymi (F_p lub F_{2^m}) do skonstruowania nowych generatorów liczb pseudolosowych i ich wszechstronne przebadanie. W celu wygenerowania sekwencji liczb o dobrych właściwościach losowych, zaproponowano nowe konstrukcje wykorzystujące łącznie pseudolosowe cechy dodawania punktów krzywej eliptycznej i pseudolosowe cechy chaotycznych dyskretnych układów dynamicznych. Konstrukcje te oparte są na generatorach liczb pseudolosowych działających na krzywych eliptycznych wzbudzanych przez chaotyczne układy dynamiczne (ang. Chaos-Driven Elliptic Curve Pseudo-Random Number Generator, C-D ECPRNG). Układy takie wykorzystują korzyści jakie daje chaotyczny generator ciągów binarnych aby poprawić jakość generatora działającego na krzywej eliptycznej. Dodanie efektu chaosu definiuje nową rodzinę generatorów ECPRNG. Chaotyczny generator liczb losowych jest szybki, statystycznie doskonały i kryptograficznie bezpieczny. Oddziałując na ECPRNG zwiększa jego losowość i (teoretycznie) wydłuża jego okres do nieskończoności. W pracy zbadano właściwości losowości nowych konstrukcji i stwierdzono, że przechodzą testy w NIST dla losowości pakietów (we wskazanych zakresie), przez co spełniają współczesne standardy bezpieczeństwa. W rozprawie przedstawiono także dwa praktyczne zastosowania nowych generatorów C-D ECPRNG do szyfrowania danych (odpowiednie kodowanie i szyfrowanie obrazów na krzywej eliptycznej i kodowanie i szyfrowanie tekstu jawnego ASCII). Są to bezpieczne systemy szyfrowania obrazu za pomocą sekwencji kluczy wygenerowanych z C-D ECPRNG nad ciałami skończonych (F_p i F_{2^m}). Analiza statystyczna i analiza różnicowa kryptogramów wykazały, że zaproponowane systemy dają odpowiednie zabezpieczenie poufności obrazów cyfrowych i takie szyfrowanie jest skuteczniejsze w stosunku do innych konkurencyjnych algorytmów znanych z literatury. Badania przeprowadzono dla trzech rodzajów jawnej wiadomości: kodu ASCII, skali szarości i obrazu RGB. W każdym z tych przypadków potwierdzono skuteczność proponowanej metody zabezpieczeń. Pośrednio potwierdza to dobrą jakość nowej konstrukcji generatora C-D ECPRNG.

Szczecin, dn. 28 listopada 2016 r.

dr hab. inż. Jerzy Pejaś
Katedra Inżynierii Oprogramowania
Wydział Informatyki
Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

KWESTIONARIUSZ- RECENZJA ROZPRAWY DOKTORSKIEJ DLA RADY WYDZIAŁU ELEKTRONIKI I TECHNIK INFORMACYJNYCH POLITECHNIKI WARSZAWSKIEJ

Tytuł rozprawy: New Constructions of Elliptic Curves-based Pseudo-random Number Generators

Autor rozprawy: mgr Omar Reyad

1. **Jakie zagadnienie naukowe jest rozpatrzone w pracy /teza rozprawy/ i czy zostało ono dostatecznie jasno sformułowane przez autora? Jaki charakter ma rozprawa (teoretyczny, doświadczalny, inny)?**

   Przedmiotem recenzowanej rozprawy doktorskiej są generatory pseudolosowych ciągów binarnych. Chociaż konstruowanie dobrych generatorów pseudolosowych ciągów binarnych jest przedmiotem badań prowadzonych od bardzo wielu lat, to problematyka ta jest nadal aktualna, zwłaszcza w obszarze kryptograficznych zabezpieczeń informacji. Bez dostępu do generatorów o wysokiej jakości, spełniających bardzo silne wymagania sformułowane, na przykład, w specyfikacji NSIT SP 800-22r1a (*A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*) i normie ISO/IEC 18031 (*Information technology -- Security techniques -- Random bit generation*), trudno jest za pomocą operacji kryptograficznych uzyskać wysoki poziom zabezpieczeń informacji przechowywanej i przetwarzanej w komputerach lub przesyłanej w sieci.

   Rozprawa doktorska ma charakter teoretyczno-doświadczalny, której rezultaty mają duże znaczenie praktyczne w projektowaniu wydajnych generatorów pseudolosowych ciągów

binarnych oraz zastosowaniu ich w nowych algorytmach szyfrowych (przykłady takich zastosowań autor przedstawił w pracy w rozdz. 10 i 11).

Pewną wadą rozprawy jest brak jawnie sformułowanego problemu naukowego, na przykład w formie postawionej tezy pracy. Utrudnia to nieco ocenę merytorycznej wartości pracy. Pośrednio, na podstawie przedstawionego streszczenia pracy oraz rozdz. 1.2, można przyjąć, że teza pracy została zdefiniowana następująco: *generator pseudolosowych ciągów binarnych oparty na krzywych eliptycznych pobudzanych przez chaotyczne dyskretne systemy dynamiczne posiada lepsze własności losowości oraz dłuższy okres dla ustalonego rozmiaru ciała skończonego aniżeli generatory wykorzystujące oddzielnie pseudolosowe cechy operacji na krzywej eliptycznej i pseudolosowe cechy chaotycznych dyskretnych systemów dynamicznych*.

Takie sformułowanie tezy znajduje odzwierciedlenie także w podsumowaniu pracy (rozdz. 12), w którym doktorant dodatkowo podkreśla, że zaproponowane w pracy połączenie dwóch odmiennych sposobów generowania pseudolosowych ciągów binarnych ma wpływ na przyspieszenie pracy generatora. Ta cecha jest szczególnie widoczna wtedy, gdy celem jest wygenerowanie ciągu bitów o ustalonej długości. Wynika to z tego, że krzywą eliptyczną wykorzystywaną w generatorze można wtedy zbudować nad mniejszym ciałem skończonym, co w efekcie powadzi do redukcji złożoności obliczeniowej generatora.

2. Czy w rozprawie przeprowadzono w sposób właściwy analizę źródeł / w tym literatury światowej, stanu wiedzy i zastosowań w przemyśle /świadczący o dostatecznej wiedzy autora. Czy wnioski z przeglądu źródeł sformułowano w sposób jasny i przekonywujący?

Recenzowana rozprawa doktorska została przygotowana w języku angielskim. Na jej zawartość składa się jedenaście rozdziałów, streszczenie (w języku angielskim i polskim), podsumowanie pracy oraz obszerna bibliografia obejmującej 197 pozycji literaturowych. Całość pracy obejmuje 151 stron. Wyniki własne doktoranta przedstawione są w rozdziałach 8, 9, 10 i 11 oraz częściowo w rozdz. 6 i 7.

Przedstawiona przez doktoranta analiza źródeł obejmuje sześć obszarów wiedzy: krzywe eliptyczne, odwzorowania chaotyczne, generatory pseudolosowych ciągów binarnych, testy statystyczne, różne techniki szyfrowania obrazów oraz metody kodowania wiadomości. W oparciu o przywołane w pracy źródła doktorant wprowadza definicje ciał skończonych, formułuje pojęcie krzywej eliptycznej oraz operacje arytmetyczne na punktach tej krzywej, dokonuje selekcji testów statystycznych, omawia generatory losowych ciągów binarnych opartych na krzywych eliptycznych i odwzorowaniach chaotycznych, i finalnie przytacza przykłady algorytmów stosowanych do szyfrowania obrazów oraz metody kodowania wiadomości, w tym przede wszystkim metodę Koblitz'a.

Przywoływane źródła stosowane są głównie do opisu wiedzy ogólnej (np. rozdz. 2, 3 i 5). Stąd uzasadniony jest w ich przypadku brak analiz i podsumowań. Jednak z punktu widzenia stanu wiedzy w zakresie tematyki powiązanej z pracą najważniejsze są analizy literaturowe dotyczące generatorów pseudolosowych ciągów binarnych oraz technik szyfrowania obrazów i kodowania wiadomości przedstawione w rozdz. 5, 6, 7, 9, 10, 11. Analizy te doktorant prowadzi w sposób, który można uznać za dość ciekawy. Nie umieszcza ich, bowiem w jednym lub dwóch rozdziałach pracy, ale zwykle przed opisem autorskich wyników badań. Widać to szczególnie w przypadku analizy stanu wiedzy

dotyczącego technik szyfrowania obrazów (rozdz. 9 i rozdz. 10). Takie podejście stanowi dobre wprowadzenie do tematyki rozdziału i pozwala na zrozumienie idei prezentowanych przez autora, ale nie określa szerszego kontekstu i powiązania wprowadzanych idei z istniejącym stanem wiedzy.

Wadą przedstawianych opisów i analiz jest brak uzasadniania dokonywanych wyborów. Na przykład w rozdz. 5 zostały omówione wybrane struktury generatorów opartych na krzywych eliptycznych, ale nie umieszczono tam podsumowania i wskazania przynajmniej pożądanych cech struktury generatora, który będzie przedmiotem dalszych badań. Podobne zastrzeżenie dotyczy rozdz. 6, w którym bez uzasadnienia do badań wybrano trzy odwzorowania chaotyczne. Zdecydowanym wyjątkiem na tym tle jest rozdz. 7, w którym doktorant bardzo uważnie przyjrzał się parametrom wybranych krzywych eliptycznych i przebadał ich wpływ na losowość oraz okres generatorów opartych na tych krzywych.

Rozległość przywoływanej literatury oraz omawianych na jej podstawie zagadnień świadczy o dobrej, pogłębionej wiedzy autora. Niemniej można odczuwać brak w pracy szerszego przeglądu generatorów losowych ciągów binarnych i ich struktur, w tym generatorów zalecanych przez ISO/IEC 18031 i NSIT NIST SP 800-90Ar1, czy też inne organizacje normalizacyjne, klasyfikacji generatorów, a także analizy metod konstruowania generatorów mieszanych i hybrydowych. Umieszczenie w pracy tego typu analiz i opisów pozwoliłoby na bardziej precyzyjne określenie celu poszukiwania i konstruowania nowych generatorów losowych ciągów binarnych. Jednak z punktu widzenia przyjętej przeze mnie tezy pracy uwaga ta nie jest aż tak istotna, ponieważ doktorant musiał przede wszystkim wykazać, że zaproponowane podejście do konstruowania generatorów pozwala na uzyskanie generatorów o lepszej losowości i dłuższych okresach niż wchodzące w jego skład generatory bazowe. Oczywiście nie oznacza to, że autor nie przeoczył przez to innej ciekawej struktury generatora.

3. Czy autor rozwiązał postawione zagadnienia, czy użył właściwej do tego metody i czy przyjęte założenia są uzasadnione?

W mojej ocenie, postawiony w pracy problem zaprojektowania nowych generatorów pseudolosowych ciągów binarnych opartych na krzywych eliptycznych nad ciałami skończonymi (F_p lub F_{2^m}) i pobudzanych przez chaotyczne systemy dynamiczne został w pełni rozwiązany. Należy zatem także uznać, że sformułowana (w sposób niejawny) teza pracy została uzasadniona.

Dobór właściwych rozwiązań oparto na rozważaniach teoretycznych, a do ich uzasadnienia metody eksperymentalne. Podejście teoretyczne zastosowano przede wszystkim do oceny zachowania się chaotycznych dyskretnych systemów dynamicznych implementowanych w cyfrowych systemach obliczeniowych o skończonej reprezentacji liczb. W takich przypadkach systemy chaotyczne ulegają często dynamicznej degradacji, której objawem jest skrócenie długości okresu, utrata ergodyczności, niska złożoność liniową, degradacja rozkładów losowych oraz silna korelacja.

Doktorant słusznie zauważył, że jeśli w cyfrowym systemie obliczeniowym generowane wyjście zależy od stanu systemu i jego wejścia zmienianego w kolejnych iteracjach, to pomimo skończonej reprezentacji liczb system będzie pozwalał na generowanie (teoretycznie) nieskończonej sekwencji liczb bez wpadania w cykl nawet wtedy, gdy stany systemu będą się powtarzały. Co więcej, w przypadku różnych stanów

początkowych sekwencje te będą się różniły także wtedy, gdy wejścia do systemu będą w każdym z przypadków takie same. Stwierdzenie to doktorant przeniósł na generator oparty na chaotycznym dyskretnym systemie dynamicznym i pokazał, że dla dwóch różnych ziaren możemy z prawdopodobieństwem jeden otrzymać dwie różne sekwencje bitów. Co prawda przedstawiony w pracy formalny dowód jest powieleniem dowodu przestawionego w cytowanej pracy [53], ale powielenie to można uznać za zasadne z punktu widzenia celu pracy.

Ocena jakości zaprojektowanych generatorów opartych na idei pobudzania jednego systemu za pomocą innego polegała na ich zamodelowaniu, wygenerowaniu odpowiedniej próbki ciągów binarnych, a następnie zastosowaniu testów statystycznych NSIT SP 800-22r1a do oceny wygenerowanych pseudolosowych ciągów binarnych. Takie podejście do projektowania jest metodycznie poprawne i stosowane zwykle w przypadku podobnych problemów. Podejście to pozwoliło doktorantowi na uzasadnienie stwierdzenia, że generatory oparte na krzywych eliptycznych z modulacją chaotyczną pozwalają na uzyskanie dłuższych sekwencji bitów niż w przypadku braku modulacji. W praktyce oznacza to, że w przypadku konieczności wygenerowania ustalonej liczby pseudolosowych bitów można dobrać ciało skończone o odpowiednio niskim rzędzie, nad którym pracuje krzywa eliptyczna i tym samym obniżyć złożoność obliczeniową generatora.

4. Na czym polega oryginalność rozprawy, co stanowi samodzielny i oryginalny dorobek autora, jaka jest pozycja rozprawy w stosunku do stanu wiedzy czy poziomu techniki reprezentowanych przez literaturę światową?

Pomysł na problem naukowy badany w pracy jest prosty: wziąć dwa różne mechanizmy generowania pseudolosowych ciągów binarnych, połączyć je i zbadać ich właściwości, np. właściwości statystyczne, długość okresu, złożoność obliczeniową. Łączenie jest sposobem na zwiększenie długości okresu i poprawy właściwości statystycznych generatorów. Jednak nieprzemyślane kombinacje lub mieszanie mechanizmów generowania nie daje gwarancji poprawy. Dlatego bardzo ważne jest rozumienie struktury otrzymanego generatora i formalne lub eksperymentalne pokazanie, że otrzymany generator posiada oczekiwane własności.

Idea łączenia generatorów znana jest w literaturze[1,2] i stosowana w praktyce (np. ISO/IEC 18031). W przypadku recenzowanej pracy nowością jest nie jest więc samo łączenie generatorów, ale propozycja połączenia dwóch deterministycznych generatorów, z których jeden bazuje na strukturach algebraicznych (krzywych eliptycznych nad ciałem skończonym), drugi z kolei na dyskretnych systemach dynamicznych o własnościach chaotycznych. Oddzielnie każdy z nich ma dobre własności losowości, w połączeniu ze sobą własności te mogą być lepsze (np. prowadzić do zwiększenia losowości, teoretycznie dowolnego wydłużenia okresu do nieskończoności). Zaproponowane w pracy połączenie generatorów jest niespotykane w literaturze i należy je zaliczyć do oryginalnego dorobku autora, nawet jeśli nie bez znaczenia jest w tym udział promotora, z którym doktorant opublikował kilka znaczących prac.

[1] Zhou Y, Hua Z, Pun CM, Chen CL: *Cascade Chaotic System With Applications*. IEEE Transactions on Cybernetics, Vol. 45, No. 9, September 2015, str. 2001-2012

[2] L'Ecuyer, P. (1996a). *Combined multiple recursive random number generators*. Operations Research, 44(5):816–822

Struktura proponowanych w pracy generatorów deterministycznych składa się ze źródła entropii (ziarna), wejścia pobudzającego (rolę tę odgrywa chaotyczny dyskretny system dynamiczny), funkcji zmiany stanu generatora oraz funkcji generującej wyjściowe pseudolosowe ciągi binarne. Autor rozważa trzy różne odwzorowania chaotyczne (równania (6.5)-(6.7)), dwie funkcje zmiany stanu generatora (równania (8.1) i (8.2)) oraz dwadzieścia trzy funkcje wyjściowe (równania (8.4) i tab. 8.7). W efekcie uzyskana liczba struktur generatorów jest imponująca i wymagała od autora wykonania wielu eksperymentów, które pozwoliły mu na wybór tych struktur, które mają odpowiednie własności statystyczne, są kryptograficznie bezpieczne, mają długie okresy oraz mogą być efektywne obliczeniowo po obniżeniu rzędu ciała skończonego, nad którym działa wybrana krzywa eliptyczna.

Dodatkowym oryginalnym dorobkiem autora, także na tle aktualnego stanu wiedzy, są zaproponowane w pracy dwa zastosowania opracowanych generatorów pseudolosowych ciągów binarnych. Pierwsze zastosowanie dotyczy generatorów w schematach szyfrowania obrazów, drugie z kolei odwzorowania wiadomości jawnych i ich kodowania o oparciu o metodę Koblitz'a.

Potwierdzeniem wartości i oryginalności wyników uzyskanych przez doktoranta są dwa artykuły opublikowane w czasopiśmie *Applied Mathematics & Information Sciences* oraz sześć artykułów dostępnych w materiałach dobrych konferencji międzynarodowych. Wszystkie artykuły zostały opublikowane w latach 2014-2016.

5. Czy autor wykazał umiejętność poprawnego i przekonywującego przedstawienia uzyskanych przez siebie wyników /zwięzłość, jasność, poprawność redakcyjna rozprawy/?

Analiza układu rozprawy oraz jej zawartości wskazuje na: (a) poprawne określenie obszaru badań, (b) solidną podstawę metodyczną prowadzonych badań, uzyskaną dzięki dobremu wprowadzeniu aparatu pojęciowego związanego z krzywymi eliptycznymi, odwzorowaniami chaotycznymi i ich zastosowaniami do generowania pseudolosowych ciągów binarnych oraz (c) dużą swobodę autora w projektowaniu szerokiej gamy nowych generatorów pseudolosowych ciągów binarnych, a następnie w eksperymentalnym badaniu ich właściwości.

Autor bardzo dobrze porusza się w obszarze badań statystycznych własności generatorów, w tym w szczególności generatorów zaprojektowanych i przedstawionych w pracy. Wyniki tych badań zostały przedstawione w formie czytelnych tabel i/lub rysunków. Wadą są czasami lakoniczne komentarze i wnioski. Na przykład, w rozdz. 8.3.2 autor nie wiąże uzyskanych wyników z funkcjami wyjściowymi generatora przedstawionymi w tab. 8.7 i nie uzasadnia, dlaczego w porównaniu z funkcją wyrażoną zależnością (8.4) w niektórych przypadkach nie uzyskano poprawy jakości generatora.

Z całą pewnością merytorycznie najciekawszą częścią pracy jest rozdział ósmy. Rozdział ten, chociaż krótki, spina w całość analizy oraz wyniki cząstkowe przedstawione we wcześniejszych rozdziałach rozprawy i, pomijając uwagi, o których wspomniałem w poprzednim akapicie, jest „przekonywującym przedstawieniem uzyskanych wyników". Szkoda, że znaczenia tego rozdziału nie podkreślił sam autor chociażby podczas omawiania struktury pracy.

Rozprawa jest napisana na dobrym poziomie językowym, zdania są zrozumiałe i poprawnie formułowane.

6. Jakie są słabe strony rozprawy i jej główne wady?

Niewątpliwie, pomimo wymienionych powyżej zalet pracy, można w niej wskazać także słabsze miejsca i na tej podstawie sformułować pewne uwagi o charakterze dyskusyjnym. Są to:

(a) autor rozprawy w jawny sposób nie sformułował tezy pracy, co utrudnia, chociaż nie uniemożliwia określenie *oryginalnego rozwiązania problemu naukowego* w rozumieniu Art. 13.1 Ustawy *o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki*; na podstawie wprowadzenia do rozprawy, a także jej podsumowania sformułowałem propozycję przykładowej tezy, która odnosi się do głównego osiągnięcia autora, tj. do oryginalnej rodziny generatorów pseudolosowych ciągów binarnych; w tym kontekście sformułowana przeze mnie teza może osłabić dorobek autora dotyczący propozycji algorytmów szyfrowania obrazów oraz kodowania wiadomości i rodzić pytanie o sens umieszczenia w pracy rozdz. 9, 10 i 11;

(b) w pracy brakuje przedstawienia ogólnej struktury proponowanej rodziny generatorów pseudolosowych ciągów binarnych; utrudnia to ocenę różnic pomiędzy poszczególnymi konstrukcjami, a także analizę uzyskanych wyników i formułowanych przez autora wniosków;

(c) dowody poprawności generatorów bazują na eksperymentach; w niektórych przypadkach doktorant mógł rozważyć zastosowanie bardziej formalnego podejścia do analizy właściwości uzyskanych generatorów, np. do oszacowania ich okresów;

(d) wadą pracy jest brak pseudokodów proponowanych w pracy algorytmów (generatorów, funkcji szyfrujących i deszyfrujących, metod kodowania wiadomości); obecność pseudokodów ułatwiłaby analizę poprawności i bezpieczeństwa algorytmów;

(e) autor nie porównuje właściwości nowych konstrukcji generatorów z innymi praktycznymi realizacjami generatorów, np. opisanymi w specyfikacji NIST SP 800-90Ar1; tego typu porównanie pozwoliłoby na pełniejszą ocenę wyników przedstawionych w pracy.

Do wad pracy należy zaliczyć także sygnalizowany już wcześniej brak uzasadniana przez autora swoich wyborów. Oprócz podanych już przykładów wada ta dotyczy także rozdz. 8, w którym autor nie uzasadnia proponowanych tam struktur generatorów, zwłaszcza tych przedstawionych w tab.8.7. Stąd można przyjąć, że propozycje przedstawione w tab. 8.7 są wynikiem dogłębnych przemyśleń autora, wynikające ze studiów literaturowych i licznych eksperymentów lub po prostu kombinacją wszystkich możliwych komponentów. Wskazanie i uzasadnienie sposobów podejmowania przez autora swoich decyzji z pewnością wpłynęłoby na jeszcze lepszy odbiór i ocenę pracy.

Dodatkowo, w pracy można znaleźć i wytknąć drobne usterki o charakterze błędów edycyjnych lub formalnych. Są to między innymi:

(a) str. 5, 3 akapit od góry: dwukrotnie użyto słowa „spowodowało”;

(b) w niektórych opisach brakuje objaśnień stosowanych oznaczeń lub odwołania się do literatury, np. str. 60, pierwszy akapit od dołu, oznaczenie $\sigma(S)$; oznaczenia te są

zwykle oczywiste, ale studiujący pracę nie powinien zaprzątać sobie tym głowy;

(c) str. 64, 1 akapit od góry: zbędne słowo „all”;

(d) str. 64, 1 akapit od dołu: powinno być "-(2^L – 1) to +(2^{L-1} – 1)";

(e) można znaleźć miejsca w pracy, np. rozdz. 6.4.3, 6.4.4 i 6.55, które autor dosłowne przytacza z literatury bez jawnego wskazania tego faktu; co prawda, autor wskazuje źródło, ale przytoczony tekst nie ma znamion cytatu;

(f) str. 80 (ostatni akapit) i str. 82 (tytuł rozdz. 8.2.4): jak należy rozmieć pojęcia „chaotic modulation” i „chaotic switching”?;

(g) str. 94, 18 linia od góry: jest „select-plaintext attack”, powinno być „chosen-plaintext attack”;

(h) str. 99, rozdz. 10.2: brak wskazania typu szyfru zaproponowanego do szyfrowania/deszyfrowania obrazów; czy jest to szyfr blokowy, czy też strumieniowy (w rozdz. 10.3 wyraźnie został wskazany szyfr strumieniowy)?

(i) str.11, rozdz. 10.4: brak dokładnych obliczeń i uzasadnienia długości kluczy oraz wymiaru przestrzeni kluczy;

(j) str.133 i dalsze, spis literatury: brak alfabetycznego uporządkowania literatury; utrudnia to wyszukanie publikacji konkretnego autora/autorów.

Należy zauważyć, że wskazane uwagi dyskusyjne, usterki edycyjne oraz formalne nie wpływają w istotny sposób na moją merytoryczną ocenę pracy jako całości.

7. Jaka jest przydatność rozprawy dla nauk technicznych?

Wyniki uzyskane w pracy mają duże praktyczne znaczenie. Można wskazać przynajmniej dwa powody tego stanu rzeczy. Po pierwsze, opracowane deterministyczne generatory pseudolosowych ciągów binarnych można wykorzystać w kryptograficznych metodach ochrony informacji. Bez dobrych generatorów trudno jest uzyskać wysokiej jakości klucze kryptograficzne, parametry algorytmów szyfrowych, w końcu zaszyfrować wiadomość lub też realizować protokoły uwierzytelniania

Po drugie, problem poszukiwania nowych technik konstrukcji generatorów o dobrych własnościach losowości i odpornych na ataki jest ciągle aktualny. W szczególności dotyczy to łączonych generatorów, które bazują na komponentach o „naturalnej” losowości takich jak krzywe eliptyczne i dyskretne chaotyczne systemy dynamiczne. Jest to praktyczna realizacja idei powszechnie stosowanej w kryptografii, zgodnie z którą silne przekształcenia szyfrujące można składać ze słabych algorytmów szyfrowych (przykładem takiego podejścia jest algorytm 3DES zbudowany na bazie algorytmu DES).

8. Do której z następujących kategorii Recenzent zalicza rozprawę?

W swojej pracy doktorant przedstawił rodzinę nowych konstrukcji generatorów pseudolosowych ciągów binarnych łączących cechy generatorów opartych na krzywych eliptycznych i generatorów opartych na chaotycznych dyskretnych systemów dynamicznych i za pomocą testów NSIT SP 800-22r1a uzasadnił, że mają one pożądane właściwości statystyczne i właściwości bezpieczeństwa.

Przedstawione powyżej uwagi merytoryczne i formalne nie umniejszają osiągnięć doktoranta, ani nie podważają praktycznej przydatności proponowanych generatorów oraz metody badania ich własności, w tym własności bezpieczeństwa. Przedstawioną mi do oceny rozprawę oceniam pozytywnie, zarówno z uwagi na aktualność i ważność

tematyki rozprawy, jak również wiedzę autora oraz znajomość literatury z zakresu metod projektowania i badania generatorów pseudolosowych ciągów binarnych.

Uważam, że autor zrealizował cel rozprawy oraz wykazał się umiejętnościami i odpowiednim przygotowaniem do samodzielnej pracy naukowej w dyscyplinie informatyka. Na tej podstawie stwierdzam, że przedstawiona do oceny rozprawa doktorska mgra Omara Reyad pt. „New Constructions of Elliptic Curves-based Pseudo-random Number Generators" **spełnia wymagania stawiane rozprawom doktorskim** w Ustawie *o stopniach naukowych i tytule naukowym* z dnia 14 marca 2003 roku (Dz. U. nr 65/2003, poz. 595 z późn. zmn.) i wnoszę o dopuszczenie jej Autora do publicznej obrony.

Jerzy Pejaś

dr hab. inż. Janusz Stokłosa
prof. nadzw.
w Wyższej Szkole Bankowej w Poznaniu

Poznań, 25 listopada 2016 r.

RECENZJA ROZPRAWY DOKTORSKIEJ DLA RADY WYDZIAŁU ELEKTRONIKI I TECHNIK INFORMACYJNYCH POLITECHNIKI WARSZAWSKIEJ

Tytuł rozprawy:

New Constructions of Elliptic Curves-based Pseudo-Random Generators

(Nowe konstrukcje generatorów pseudolosowych na podstawie krzywych eliptycznych)

Autor rozprawy: **mgr Omar Reyad**

1. W recenzowanej dysertacji doktorskiej mgr Omar Reyad zaproponował nowy schemat konstrukcji generatorów pseudolosowych polegający na połączeniu generatorów liczb pseudolosowych pracujących na krzywych eliptycznych z chaotycznymi układami dynamicznymi. Autor wziął pod uwagę krzywe eliptyczne nad ciałem $\mathbb{F}_p$, gdzie p jest liczbą pierwszą, oraz krzywe nad $\mathbb{F}_{2^m}$, $m > 1$. Poprzez wykorzystanie do sterownia takich generatorów chaotycznych sekwencji addytywnych i multiplikatywnych zdefiniował nową rodzinę generatorów pseudolosowych. Autor jasno sformułował cel rozprawy. Wykonując badania zaproponowanych generatorów wykazał ich użyteczność. Opracowane przez siebie generatory zastosował do szyfrowania obrazów i tekstów. Rozprawa ma charakter teoretyczno-obliczeniowy.

2. W rozprawie mgr Reyad przedstawił stan wiedzy w zakresie niezbędnym do uzasadnienia nowości uzyskanych przez siebie wyników. W szczególności przytoczył podstawowe pojęcia dotyczące ciał skończonych i krzywych eliptycznych, skomentował podstawowe zestawy testów statystycznych stosowane w kryptografii. Omówił znane z literatury generatory liczb pseudolosowych na krzywych eliptycznych, a także konstrukcje chaotycznych generatorów liczb pseudolosowych i ich właściwości. Przedstawił również zasady wyboru parametrów domenowych dla krzywych eliptycznych nad $\mathbb{F}_p$ oraz $\mathbb{F}_{2^m}$, rekomendowane przez Certicom Research. Dokonał przeglądu literatury w zakresie szyfro-

wania obrazów. Poświęcił uwagę metodom przekształcania oryginalnych wiadomości jawnych w wartości liczbowe, w szczególności kodowaniu Koblitza. Analiza źródeł została przeprowadzona w rozprawie w sposób właściwy. Odzwierciedla stan wiedzy zawartej w literaturze światowej. Wykaz cytowanej literatury jest obszerny, składa się z 197 pozycji.

3. Autor trafnie wybrał obszar badań. Podstawą analizy wszystkich przedstawionych rozwiązań były eksperymenty obliczeniowe polegające badaniu właściwości statystycznych proponowanych rozwiązań. Wykonano:

a. Testy NIST dla binarnych generatorów chaotycznych z uwzględnieniem trzech rodzajów odwzorowań (tabela 6.1).
b. Testy $\chi 2$ dla punktów krzywych eliptycznych nad $\mathbb{F}_{271}$, $\mathbb{F}_{521}$ oraz $\mathbb{F}_{1031}$ opisanych równaniem Weierstrassa (3.4) o zmiennych parametrach domenowych (a,b) dla dwóch rodzajów generatorów: kongruencyjnego liniowego (5.1) i chaotycznego (tabele 7.1–7.3).
c. Testy NIST dla punktów krzywych eliptycznych nad ciałem $\mathbb{F}_{733}$ oraz $\mathbb{F}_{5477}$ opisanych równaniem Weierstrassa (8.5), po przekształceniu punktów krzywej eliptycznej będącym konkatenacją pięciu najmniej znaczących bitów współrzędnych punktów generowanych przez sekwencje addytywne i multiplikatywne o długości nie większej niż 2^{16} (tabela 8.2–8.5 dla krzywej nad GF(733)); w przypadku krzywej nad $\mathbb{F}_{5477}$) wyniki skomentowano nie przytaczając rezultatów w formie tabelarycznej.
d. Testy NIST dla sekwencji addytywnych uzyskanych z uwzględnianych naprzemiennie punktów dwóch krzywych, nad $\mathbb{F}_{29}$ i $\mathbb{F}_{53}$ (tabela 8.6).
e. Testy NIST dla generatorów chaotycznych na krzywych eliptycznych nad $\mathbb{F}_{2^8}$ opisanych równaniem (8.7) dla 22 różnych schematów generowania sekwencji addytywnych; dla 6 z nich rezultaty zamieszczono w tabelach 8.8–8.10.

Dla generatorów na krzywych eliptycznych nad $\mathbb{F}_p$ o ustalonych parametrach domenowych przeprowadzone eksperymenty obliczeniowe pozwoliły skonstruować 10 schematów generowania kluczy – z wykorzystaniem generatora chaotycznego – do algorytmu szyfrowania obrazów.

Szyfrowano dwa obrazy: czarno-biały przedstawiający dziewczynę o imieniu Lena (standardowy obraz testowy) oraz odcisk palca. Dla obydwu przypadków wykonano: analizę entropii i analizę korelacyjną (tabela 10.2 i 10.3), testy losowości NIST, analizę wrażliwości na atak różnicowy, analizę histogramów (rys. 10.3-10.4). Zilustrowano (rys. 10.1 i 10.2) rezultaty szyfrowania obydwu obrazów kluczami wygenerowanymi przez zaproponowane generatory.

Podobnie rzecz się ma z generatorami na krzywych eliptycznych nad $\mathbb{F}_{2^m}$. W tym przypadku skonstruowano 14 schematów generowania kluczy. Dla opisanych powyżej dwu obrazów wykonano także analizę entropii i analizę korelacyjną (tabela 10.4 i 10.5),

testy losowości NIST, analizę wrażliwości na atak różnicowy, analizę histogramów (rys. 10.7–10.8). Zilustrowano (rys. 10.1 i 10.2) rezultaty szyfrowania obydwu obrazów kluczami wygenerowanymi przez zaproponowane generatory.

Rezultaty wykonanych analiz, w tym również analizy liczności przestrzeni kluczy (ze względu na atak poprzez przeszukiwanie wyczerpujące klucza) potwierdziły zasadność przyjętych założeń, w rezultacie czego została opracowana nowa metoda generowania kluczy kryptograficznych.

Ważną rolę w przypadku każdej metody szyfrowania odgrywa przekształcenie wiadomości oryginalnej (np. tekstu, obrazu, dźwięku) w wartość dającą się przetworzyć (np. blok bitów, liczba naturalna, punkt na krzywej eliptycznej) przez algorytm szyfrujący. Autor zaproponował metodę odwzorowywania pikseli w punkty krzywej eliptycznej (tab. 11.5) i zilustrował proces szyfrowania obrazu Leny czarno-białego (tab. 11.6) i RGB (tab. 11.7–11.10). Porównał także rezultaty szyfrowania punktów krzywej eliptycznej zakodowanych (i) metodą Koblitza oraz (ii) metodą zaproponowaną przez siebie w rozprawie (rys. 11.2). Podobne porównanie zostało wykonane dla odwzorowania w punkty krzywej eliptycznej (i) znaków kodu ASCII oraz (ii) obrazu RGB (rys. 11.3).

4. W rozprawie zaproponowano autorskie rozwiązanie problemu generowania liczb pseudolosowych w oparciu o krzywe eliptyczne wzbudzane przez chaotyczne układy dynamiczne. Poprzez dodanie efektu chaosu została zdefiniowana nowa rodzina generatorów. Autor zaproponował także dwa pola zastosowań opracowanych przez siebie generatorów: (i) kodowanie i szyfrowanie obrazów oraz (ii) szyfrowanie tekstów zakodowanych za pomocą ASCII.

Wykonując analizę entropii i analizę korelacyjną zaszyfrowanych obrazów zaproponowanymi przez siebie schematami generowania kluczy Autor dokonał porównania uzyskanych wyników ze znanymi z literatury. Porównanie to wypada na korzyść rozwiązań zaproponowanych w rozprawie.

W rozdziale 12.1.1 Autor zwraca uwagę na fakt, że wyniki zreferowane w rozprawie były wcześniej częściowo publikowane. Omawia zawartość ośmiu artykułów współautorskich: dwóch w czasopismach, pięciu w materiałach konferencji międzynarodowych, jednego złożonego do publikacji.

5. Rozprawa napisana jest językiem precyzyjnym, zwięzłym, na ogół jasnym. Główna wątpliwość kryjąca się pod określeniem „na ogół" dotyczy algorytmu szyfrowania obrazów i znaków ASCII. Nie znalazłem wyraźnego stwierdzenia jaki algorytm został przez Autora użyty. Nie wyjaśnia tego ani stwierdzenie sformułowane na str. 99_{5-4}, ani na str. 100^{3-4} rozprawy.

6. Co do słabych stron rozprawy, to nie ma ich wiele:
   a. W dysertacji zabrakło mi podsumowania w postaci algorytmu, choćby za pomocą uproszczonego schematu blokowego, procesu projektowania generato-

rów liczb pseudolosowych pracujących na krzywych eliptycznych z chaotycznymi układami dynamicznymi.

b. Istotną niepewność wskazałem w p. 4 tej recenzji; dotyczy ona braku wyraźnego wskazania stosowanego algorytmu szyfrowania.

c. Sposób cytowania literatury polegający na przypisywaniu kolejnym cytowanym po raz pierwszy pozycjom kolejnych liczb naturalnych jest bardzo wygodny dla autora lecz wielce niewygodny dla czytelnika. Uważam, że spis literatury powinien być wykonany alfabetycznie, np. zgodnie z systemem harwardzkim cytowań (wygodnym zarówno dla autora, jak i czytelnika).

d. Usterek spostrzegłem niewiele, jednak na niektóre chciałbym zwrócić uwagę:
– str. 14_2 i str. 79^9: nie jest jasne co rozumie się pod pojęciem generatora „statystycznie doskonałego" (*statistically perfect*),
– str. 18, rozdz. 22: definiując ciało skończone Autor korzysta słusznie z arytmetyki modularnej, natomiast w przykładzie 1 stosuje (nie wprowadzoną) relację kongruencji dwóch liczb, co na str. 20_{12} prowadzi do fałszywego stwierdzenia, że $-1 \in \mathbb{F}_2 = \{0,1\}$,
– na str. 27 omówiony jest najpierw geometryczny sposób wyznaczania sumy dwóch punktów na krzywej eliptycznej określonej nad zbiorem liczb rzeczywistych, po którym następuje nieuprawniona moim zdaniem konstatacja, że z tej interpretacji geometrycznej można wyprowadzić formuły obowiązujące w ciele algebraicznym $\mathbb{F}_p$,
– na str. 30_2 Autor rozdziela niesłusznie kryptografię na krzywych eliptycznych od algorytmów podpisu cyfrowego na krzywych eliptycznych,
– w przytoczonym twierdzeniu Hassego (wzór (3.18) na str. 31) powinna być nierówność nieostra,
– w algorytmach 2, 3 i 4 na str. 36 i 37, a także na str. 39_1, 40^1 oraz 41^9, punkt w nieskończoności oznaczono symbolem ∞ zamiast O, ponadto w algorytmach 2 i 3 w linii 1 powinno być $k_{l-1} = 1$, natomiast w algorytmie 4 w linii 1 brak jest rozkładu liczny k na postać binarną (podobnie w algorytmie 5 na str. 38),
– na str. 55_{2-1} użyto niezdefiniowanego określenia „złożoność strukturalna"; jak tutaj rozumiana jest złożoność strukturalna?,
– na str. 60_7 brak jest objaśnienia znaczenia symbolu σ,
– na str. 71^{13-14} nie jest jasne stwierdzenie odnoszące się do algorytmu SHA.

Wymienione uwagi nie umniejszają osiągnięć merytorycznych Doktoranta.

7. Wyniki uzyskanych przez mgr. Omara Reyada w zakresie projektowania generatorów pseudolosowych są oryginalne i wartościowe. Zaproponowany w rozprawie nowy schemat konstrukcji generatorów pseudolosowych polegający na połączeniu generatorów

liczb pseudolosowych pracujących na krzywych eliptycznych z chaotycznymi układami dynamicznymi jest nowatorski.

8. Reasumując stwierdzam, że:
   - tematyka rozprawa jest aktualna i bardzo ważna,
   - Autor rozwiązał zdefiniowany przez siebie problem naukowy i użył do tego celu odpowiednich metod,
   - rozprawa świadczy o dużej wiedzy Autora w zakresie projektowania generatorów pseudolosowych oraz znajomości literatury z tego zakresu.

Uważam, że przedstawiona mi do recenzji dysertacja doktorska spełnia wymagania stawiane rozprawom doktorskim w Ustawie o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki z dnia 14 marca 2003 r. (Dz. U. nr 65, poz. 595). Wnoszę o dopuszczenie mgr. Omara Reyada do publicznej obrony rozprawy.