Warszawa, 12.09.2023

Dr hab. inż. Michał Kruk, prof. SGGW

Instytut Informatyki Technicznej

Szkoła Główna Gospodarstwa Wiejskiego w Warszawie

ul. Nowoursynowska 159

02-776 Warszawa

Recenzja rozprawy doktorskiej mgr. inż. Piotra Witkowskiego

Tytuł rozprawy: Metody szyfrowania danych w sieciach komputerowych z wykorzystaniem informacji kodowanych w sieci elektroenergetycznej

Autor rozprawy: mgr inż. Piotr Witkowski

Promotor: dr hab. inż. Jarosław Zygarlicki, prof. Uczelni

Promotor pomocniczy: dr hab. inż. Aleksandra Kawala-Sterniuk, prof. Uczelni

1. Cel, teza i zakres pracy

Celem pracy jest opracowanie metody generacji liczb losowych, bazującej na entropii zmienności częstotliwości harmonicznej podstawowej napięcia sygnału elektroenergetycznego. Dodatkowo proponowana metoda ma zostać zabezpieczona poprzez zastosowanie filtrów o zadanych parametrach. Opisywana metoda ma mieć zastosowanie w szeroko pojętej kryptografii np. do generowania kluczy. Doktorant za cel postawił sobie nie tylko opracowanie samej metody, ale również stworzenie całego i kompletnego systemu o nią opartego.

Autor postawił następującą tezę:

Wykorzystanie zmiennych w czasie globalnych parametrów rejestrowanych w sieci elektroenergetycznej umożliwia tworzenie niepowtarzalnych kluczy szyfrujących, zwiększających bezpieczeństwo danych przesyłanych w sieciach komputerowych.

W moim przekonaniu zarówno cel pracy jak i teza sformułowane są jasno i prawidłowo. Co bardzo ważne, autor ma również z góry przewidzianą metodę weryfikacji stworzonego systemu, którą są testy NIST. Takie podejście pozwala na ścisłe i precyzyjne określenie wartości proponowanej metody.

2. Struktura pracy

Praca mgr. Witkowskiego składa się z 9 rozdziałów, które zajmują 127 stron.

Rozdział 1 opisuje cel i zakres pracy. Jak napisano w pkt. 1 niniejszej recenzji cel jest jasno sformułowany, a jego weryfikacja nie podlega dyskusji. Również przedstawiona teza zbudowana jest poprawnie.

Rozdział 2 zawiera wprowadzenie oraz uzasadnienie podjęcia opisywanej pracy badawczej. Doktorant we wprowadzeniu przedstawił w sposób klarowny główne etapy pracy, a w uzasadnieniu wykazał, że kolejna metoda generowania liczb losowych jest potrzebna. Rozdział oparty jest o odwołania literaturowe co dodatkowo wzmacnia uzasadnienie podjęcia takiej, a nie innej pracy badawczej.

Rozdział 3 przedstawia studium literaturowe. Rozdział ten oceniam wysoko i uważam go za mocną stronę pracy. Opisywana literatura jest nowa, a ilość zamieszczonych pozycji, których jest 101 oznacza, że doktorant mocno przebadał opisywany przez siebie temat. Dodatkowo, opisy zawarte w rozdziale świadczą, że autor faktycznie do wykazanych prac zajrzał, a nie wykazał je tylko w opracowaniu.

Rozdział 4 zawiera projekt i opis działania systemu. W moim przekonaniu rozdział ten jak na pracę badawczą, którą jest rozprawa doktorska jest za bardzo rozbudowany. Zbyt dokładnie przedstawiono w postaci UML działanie systemu, jednocześnie rozbudowane diagramy zawierają małą czcionkę i są nieczytelne (np. 4.6, 4.7, 5.1…). Uważam, że szczegółowa część tego opisu mogłaby zostać pominięta lub umieszczona na końcu w postaci dodatku. Oczywiście w żaden sposób nie dyskwalifikuje to zawartego w rozdziale opisu, który pozwala czytelnikowi na staranne zrozumienie zasady działania stworzonego systemu.

Rozdział 5 przedstawia metodologię badawczą. Doktorant opisał w nim szczegółowo poszczególne urządzenia pomiarowe i ich parametry. Metodologię słusznie podzielił na 3 etapy, co ułatwia jej zrozumienie. W etapie 1 opisywany jest pomiar i synchronizacja przebiegów napięć z dwóch lokalizacji, w etapie 2 przedstawia estymację przecięcia z osią czasu harmonicznej podstawowej, a etap 3 opisuje filtrację i zestawienie ze sobą wygenerowanych ciągów liczbowych.

Rozdział 6 jest weryfikacją uzyskanych rezultatów poprzez zastosowanie testów NIST. W pracy doktorant zastosował 5 z 15 proponowanych testów. Niniejszy rozdział przedstawia same wyniki bez dodatkowej interpretacji, która ma miejsce w rozdziale 7.

Rozdział 7 zatytułowany *Podsumowanie* jest interpretacją wyników uzyskanych w rozdziale 6 oraz porównaniem z wynikami osiąganymi przez innych autorów. W mojej ocenie rozdział ten stanowi mocną część pracy, gdyż pokazuje, że autor potrafi w odpowiedni sposób bronić swoich rezultatów odwołując się m.in. do pozycji literaturowych.

Rozdział 8 zawiera wnioski końcowe i przedstawia osiągnięcia naukowe pracy.

Rozdział 9 jest spisem literatury cytowanej w rozprawie.

3. Główne osiągnięcia naukowe pracy

Tematyka rozprawy jest bardzo aktualna i istotna. W chwili obecnej bardzo ważnym aspektem jest zapewnienie poufności jak i integralności danych. Służą do tego algorytmy kryptograficzne oparte najczęściej na wygenerowanych liczbach losowych. Stworzenie jednego z takich generatorów proponuje doktorant. W mojej ocenie praca zawiera wartościowe, oryginalne osiągnięcia do których należą:

- opracowanie generatora liczb losowych, który bazuje na entropii częstotliwości panującej w sieci elektroenergetycznej;

- wykazanie, że entropia w częstotliwości sieci elektroenergetycznej posiada wystarczający chaos i nieporządek, aby móc być użyteczną przy generowaniu liczb losowych;

- rozpoczęciem badań na zmiennym w czasie kluczem częstotliwościowym, co może być naturalnym i ciągłym przejściem doktoranta do dalszej pracy naukowej.

4. Pytania i uwagi

W mojej ocenie do mocnych stron pracy zaliczyłbym:

- ciekawą tematykę badawczą oraz interdyscyplinarność pracy;
- dobrze zrobiony przegląd literatury, zawierający aktualne i nowe pozycje;
- ciekawa i dobra polemika wyników testów z wynikami w innych pracach. Doktorant pokazuje, że potrafi skutecznie bronić swoich wyników;
- jasne, przejrzyste i dokładne opisy metodologii badań oraz stworzonego systemu.

Z kolei słabymi stronami pracy są

- bardzo liczne błędy gramatyczne, ortograficzne i redaktorskie, katastrofalna wręcz interpunkcja;
- nieco za bardzo rozbudowana część opisu projektu i funkcjonowania systemu.

Uwagi szczegółowe:

„badan” - str. 8
„nie kryptograficzne” - str. 9
w pracy [8] nie ma wzoru 1.2 - str.10
„entropi” - str. 10
wzór 1.3 - brak oznaczeń q - str. 10
przecinki – „2021, roku”; przed który str. 11 - w całej pracy wrażenie, że autor umieszcza je losowo
„w prawdzie” - str. 13
niepotrzebny koniec zdania – „…EKG. Można” - str. 17
„pozwoliło eliminację” - brakuje "na" - str. 17
jest a, powinno być na - str. 17
„poza funkcjonalny” - str. 20
„informacji” - powinno być „informacjom” - str. 22
„niż” - powinno być „o” - str. 23
„Polega ona” - powinno być "polega na" str. 23

lokalizacjach - niepotrzebny koniec zdania - str. 23
„się literaturze” - powinno być "się na literaturze" - str. 23
„energii elektrownie” - str. 23
„artkule” - str. 24
„elektrycznych. Co czyni” - niepotrzebny koniec zdania - str. 25
„posiada” - niepotrzebne - str. 25
„trój obiektową” - str. 27
„nie zdominowanego” - str. 28
„najlepiej na podstawie o zegar światowy UTC” - str. 29
„zasadza działania” - str. 30
„www” - powinno być WWW - str. 31
„dostęp do korespondencji osobą(!) trzecim” - str. 63
„nr. 1” - powinno być „nr 1” - str. 67
„oddzielone dużymi odległościami geologicznie” - str. 69

str. 78 "lecz jeżeli na 50 rzutów wypadnie awers to wtedy oznacza to, że moneta mogła zostać odpowiednio spreparowana" - coś nie tak...

„... wypadły gorzej. Nie jest” - niepotrzebny koniec zdania - str. 113

W całej pracy - transformata Falkowa - powinno być transformata falkowa.

W trakcie lektury nasunęły mi się trzy pytania dotyczące rozprawy:

1. Autor pisze o parametrach filtra pasmowo-przepustowego (str. 67) i dolnoprzepustowego (str. 74). Dlaczego zastosował takie wartości, a nie inne? W jaki sposób wartości te zostały dobrane?
2. W pracy użyto 5 testów NIST spośród 15. Dlaczego akurat pięć? W jaki sposób i dlaczego dobrano akurat te 5 testów?
3. Str. 41 - *Parametry filtracji są przechowywane w hurtowni danych* - czy chodzi o hurtownię danych w sensie rozumienia systemu który ma umożliwić i wspierać działania z zakresu analizy biznesowej m.in. poprzez narzędzia OLAP?

5. Ocena końcowa rozprawy

Uważam, że rozprawa doktorska przedstawia oryginalne rozwiązanie zaprezentowanego w niej zagadnienia naukowego i projektowego. Autor podjął się rozwiązać problem, który ma istotne znaczenie praktyczne. Trafnie określił metodę weryfikacji osiągniętych wyników. Należy podkreślić, że praca ma charakter interdyscyplinarny, a autor musiał się wykazać wiedzą z kilku dyscyplin. Pomimo uchybień (zwłaszcza edytorskich) pracę oceniam wysoko i w mojej opinii w pełni spełnia ona wymogi stawiane rozprawom doktorskim i wnoszę o dopuszczenie do publicznej obrony.

Michał Kruk