dr hab. Marek Klonowski
prof. ndzw. PWr
++48 692 842 272
Marek.Klonowski@pwr.edu.pl

Wrocław, 02.03.2018

Recenzja poprawionej rozprawy doktorskiej Pana mgra Michała Zająca

Niniejszym stwierdzam, że poprawiona wersja rozprawy doktorskiej Pana Michała Zająca spełnia ustawowe oraz zwyczajowe wymagania do nadania stopnia doktora i wnioskuję o dopuszczenie Kandydata do dalszych etapów przewodu doktorskiego.

Uwagi wstępne

Niniejszy dokument stanowi uzupełnienie recenzji z dnia 12.01.2016 i omawia przede wszystkim zmiany jakie zostały wprowadzone w nowej wersji.

Należy przede wszystkim zauważyć, że zmiany te są znaczne. Mimo, że struktura rozprawy, jak i główne tezy pozostały bez zmian, znacząca część tekstu została radykalnie zmieniona. Ogólnie prezentacja jest obecnie na zadowalającym poziomie i umożliwia zrozumienie uzyskanych wyników.

Ocena zmian i uwagi do kolejnych rozdziałów

Rozdział pierwszy zmienił swoją strukturę; został oczyszczony z trywializmów oraz wzbogacony o bardziej zrozumiałe opisy koncepcji zawartych w dalszej części rozprawy.

- s. 14 ostania linijka: some -> any ?

Rozdział drugi, który przedstawia podstawowe definicje dotyczące podstawowych protokołów kryptograficznych został rozszerzony i uspójniony. Jednocześnie zrezygnowano z prezentacji zbędnych przykładów, zastępując je bardziej adekwatnymi. Mimo, że przedstawione koncepcje pochodzą z różnych źródeł, całość wydaje się spójna. Nadal jednak można odnieść wrażenie, że część treści tu zawartych jest zbędna. Niektóre z faktów zaczerpniętych z obcych prac została udowodniona. Nie są jasne kryteria wyboru faktów, które zostały zamieszczone wraz z dowodami. Przyjęte definicje są naturalne, choć w przypadku analizy prywatności wybór ten nie jest oczywisty i zapewne mógłby być głębiej umotywowany.

- s. 47 Ostatnie zdanie przed Theorem 3 niezrozumiałe.

Rozdział trzeci zawierający nowe wyniki dotyczące koncepcji budowy BRM opartej o prywatne (niejednostajne) dane, został znacząco poprawiony. W obecnej formie, biorąc pod uwagę techniczną trudność rozumowań, można uznać, że wyniki te zostały zapisane w sposób nie odbiegający od wielu publikacji z tej tematyki. Pewien problem stanowi dowód Theorem 13, gdzie niejasny pozostaje zapis analizy gry. Nie ma jednak wątpliwości, że samo rozumowanie jest poprawne.

Uwagę zwraca także nowy Podrozdział 3.8, który prezentuje parametry protokołów w odniesieniu do rzeczywistych systemów. Przedstawione tu fakty jednak nie przekonują co do praktycznego znaczenia zaprezentowanych protokołów. Brakuje bowiem odniesienia do najistotniejszej, a przynajmniej najbardziej problematycznej, kwestii - rozkładu D. Potrzeba by było określić, na ile typowe dane przechowywane w urządzeniach, takich jak telefon komórkowy, spełniają założenia przyjętego modelu. Taka analiza wydaje się być bardzo trudna, o ile w ogóle możliwa. Niemniej pojawienie się rozważań zawartych w Podrozdziale 3.8 należy przyjąć z uznaniem.

Rozdział czwarty , który przedstawia wykorzystanie podejścia z poprzedniego rozdziału do budowy schematów kryptograficznych (podpis cyfrowy i schemat uwierzytelniania), w obecnej formie nie budzi większych zastrzeżeń. Zmiany w stosunku do pierwotnej wersji są znaczne. Zdecydowana większość uwag została w satysfakcjonujący sposób uwzględniona.

Ocena wyników

Poprawiona wersja rozprawy doktorskiej jest możliwa do oceny. Prezentacja wyników, mimo pewnych mankamentów, jest na zadowalającym poziomie. Ciągle można wytknąć dość liczne, drobne błędy formalne (np. traktowanie listy

jako zbioru, brak podawania założeń dotyczących zakresu użytych parametrów w twierdzeniach). Nie są to jednak usterki znaczące.

Główny wynik zaprezentowany w pracy wymagał niemałych umiejętności technicznych. Przedstawione konstrukcje oparte są o mechanizmy bardzo często eksploatowane w kryptografii czy teorii bezpieczeństwa komputerowego (drzewa Merkla, grafy o własności ekspansji czy mechanizmy typowe dla BRM), chociaż ich połączenie nie jest oczywiste i wymagało pewnej pomysłowości. Co więcej analiza takich konstrukcji wymagała widocznego wysiłku. Szczególnie widać to w rozdziale czwartym gdzie z pozoru oczywiste wykorzystanie drzew Merkle'a związane było z nieoczywistą analizą działania protokołu.

Z drugiej strony, oryginalnych wyników jest stosunkowo mało (watro nadmienić, że Pan Michał Zając jest współautorem też innych prac, nie zawartych w przedstawionej rozprawie doktorskiej). Poza tym, przedstawione konstrukcje w obecnej formie wydają się cięgle daleki od faktycznych zastosowań. Nie jest jasne, na ile dane przechowywane w pamięciach popularnych urządzeń spełniają założenia modelu. Kolejną przeszkodą ,w drodze do zastosowań pomysłów zawartych w pracy, jest uwzględnienie dynamicznego charakteru danych. Dlatego na główny wynik pracy patrzyłbym raczej jak na rozbudowę paradygmatu BRM w kierunku użycia danych niejednostajnych.

Mimo uwag krytycznych ocena wyników naukowych jest pozytywna: rozprawa wskazuje na to, że Doktorant bardzo dobrze opanował zaawansowane techniki kryptograficzne i potrafi stosować je do rozwiązywania naturalnych problemów. Co więcej zaprezentowane wyniki, nawet jeśli nie nadają się do bezpośredniego zastosowania w rzeczywistych systemach, wykonują poważny krok w stronę użycia technik wyrosłych z BRM w rzeczywistości.

Podsumowanie

Przedstawiona rozprawa doktorska zawiera istotne pod względem teoretycznym wyniki z pewnym potencjałem do wykorzystania w rzeczywistych systemach informacyjnych. Liczba nowych wyników nie jest duża (rozdział trzeci oraz częściowo czwarty), jednak uznać należy że całość spełnia zwyczajowe wymagania stawiane rozprawom doktorskim w tym względzie.

Dodajmy, że Autor wykazał się znaczącymi umiejętnościami technicznymi - problematyka rozprawy jest trudna a zaprezentowane rozumowania wymagały szerokiej wiedzy dotyczącej analizy protokołów kryptograficznych.

Ponadto, prezentacja w obecnej wersji rozprawy stoi na zadowalającym poziomie.

Wszystko to pozwala uznać przedstawioną dysertację za wystarczającą, aby rekomendować dopuszczenie Kandydata do dalszych etapów przewodu doktorskiego.

dr hab. Marek Klonowski
prof. ndzw. PWr
++48 692 842 272
Marek.Klonowski@pwr.edu.pl

Wrocław, 02.03.2016

Recenzja rozprawy doktorskiej Pana mgra Michała Zająca

Niniejszym wnioskuję o skierowanie rozprawy doktorskiej mgra Michała Zająca do poprawy.

Uwagi wstępne

Niniejsza recenzja powstała na podstawie następujących dokumentów:

1. rozprawy doktorskiej w języku angielskim,
2. autoreferatu w języku polskim,
3. oświadczenia dotyczącego udziału Pana Michała Zająca w zaprezentowanych w rozprawie wynikach (z datą 02.02.2016), która stanowi załącznik do niniejszej recenzji. Dokument został dostarczony dnia 08.03.2016.

Recenzja jest sporządzona w oparciu o Ustawę z dnia 14 marca 2003 o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki z późniejszymi zmianami na gruncie tzw. „starego trybu".

Klasyfikacja wyników do dziedziny *informatyka* w ramach nauk matematycznych jest prawidłowa.

Tematyka i struktura pracy

Wyniki przedstawione w rozprawie *Effective Cryptographic Protocols with Limited Computational Power and Memory* pokazują jak można budować protokoły kryptograficzne w modelu *Bounded Retrieval Model* (BRM) bez podstawowego ograniczenia jakim jest poświęcenie bardzo dużej pamięci na klucz prywatny.

W modelu tym zakłada się, że adwersarz może przejąć kontrolę nad urządzeniem zawierającym klucz prywatny, ale ze względu na rozmiar klucza, nie będzie w stanie przejąć i wykorzystać istotnej jego części. Model ten jest naturalny i w ostatnich latach cieszy się dużym zainteresowaniem wśród kryptologów. Ogromny klucz stanowi jednak istotną przeszkodę w stosowaniu tego typu rozwiązań w praktyce - szczególnie w przypadku urządzeń mobilnych o ograniczonej pamięci, która musiałaby w dużej części być przeznaczona właśnie na klucz.

Główny pomysł zaprezentowany w rozprawie jest następujący - ponieważ klucz w modelu BRM jest bardzo dużych rozmiarów, użyjmy nie losowego ciągu bitów, a danych które i tak są przechowywane zazwyczaj w pamięci. Dokładniej, Autor pokazuje, jak można wykorzystać dane i tak gromadzone przez użytkowników (np. prywatne zdjęcia, dokumenty, pliki multimedialne) w charakterze klucza. Tu jednak powstają dwa problemy. Po pierwsze, taki klucz nie jest ciągiem losowym wybranym z rozkładu jednostajnego, co w oczywisty sposób może obniżyć poziom bezpieczeństwa systemu. Po drugie, w przyjmowanym modelu, gdy klucz może zostać częściowo ujawniony, ujawnia się też osobiste dane użytkowników, co skutkuje zagrożeniem prywatności.

Zaprezentowane rozwiązanie opiera się na pomyśle, aby „wzmocnić losowość" wykorzystując konstrukcję opartą na tzw. *disperserach*. Dzięki temu, jeśli źródło jest odpowiednio losowe (w sensie tzw. *min-entropii*), odpowiednia funkcja deterministyczna wzmacnia je na tyle, że może ono być wykorzystywane w schematach BRM jako klucz prywatny. Co istotne, schemat z zamienionym kluczem będzie oferował niemal taki sam poziom bezpieczeństwa (zmniejszenie parametrów bezpieczeństwa jedynie o kontrolowalną wartość w stosunku do klucza wybranego z rozkładu jednostajnego). Jednocześnie takie przetworzenie danych zapewnia prywatność oryginalnych danych, zdefiniowaną w dość naturalny sposób. Opis tego pomysłu wraz z odpowiednimi konstrukcjami zawarte są w **rozdziale trzecim**.

Inne oryginalne wyniki znajdują się w **rozdziale czwartym**, gdzie Autor pokazuje jak wykorzystać zaprezentowaną wcześniej konstrukcję do zbudowania schematu podpisu cyfrowego oraz protokołu uwierzytelniania za pomocą standardowych konstrukcji.

Rozdział piąty stanowi lakoniczne podsumowanie rozprawy i nakreślenie otwartych problemów. **Dwa pierwsze** rozdziały nie zawierają oryginalnych wyników, a są jedynie wprowadzeniem w tematykę i przedstawiają motywację dla prowadzonych badań.

Ocena wyników rozprawy

Znaczenie wyników

Bez wątpienia najistotniejszym osiągnięciem naukowym i intelektualnym rozprawy są wyniki rozdziału trzeciego. Choć idea „wzmacniania losowości" pojawiała się często wcześniej w literaturze, w kontekście BRM pomysł ten jest nowy, szczególnie istotny i bardzo naturalny. Jednocześnie jego realizacja na podstawie „typowych danych" użytkowników wymaga zastosowania bardziej subtelnej analizy, w szczególności wzięcia pod uwagę zagrożenia prywatności. W rozprawie stwierdzono, że wynik rozdziału trzeciego stanowi rozwiązanie najistotniejszego problemu związanego z badaniami nad modelem BMR. Jestem skłonny się z tym stwierdzeniem zgodzić. Konstrukcję *dispersera* oparto o funkcję haszującą, którą później, w analizie traktowano jako wyrocznię losową. W rozprawie przekonująco pokazano, że postawionego problemu nie da się rozwiązać za pomocą klasycznych, narzucających się metod (np. ekstraktorów o podobnych własnościach). Konstrukcja i przeprowadzona analiza, mimo że osiągnięte zostały za pomocą połączenia technik z kilku innych prac, wymagały dużych umiejętności technicznych i sporej pomysłowości. Godne podkreślenia jest to, że metoda jest ogólna - generyczny schemat można wykorzystać podmieniając klucz w różnych protokołach w BRM, w taki sposób że gwarancje bezpieczeństwa oryginalnego protokołu są jedynie zmniejszone o kontrolowalną wartość. Warto też podkreślić, że metoda jest możliwa (przynajmniej w teorii) do implementacji, bo wszelkie konstrukcje podane są *explicite* (poza funkcją haszującą, która jest traktowana jako wyrocznia losowa). Nie jest to oczywiste w przypadku konstrukcji grafowych. Wynik ten, poza rozprawą, zawarty jest w raporcie technicznym napisanym przez Doktoranta z czterema innymi osobami. Z potwierdzonej przez Promotora deklaracji Doktoranta stanowiącej załącznik do recenzji dowiadujemy się, że wkład Pana Michała Zająca obejmował

- dowód lematu 8 na podstawie idei Promotora;
- udział w pomyśle wykorzystania *Guessing game*;
- dowód lematu 9;
- opracowanie symulatora w dowodzie twierdzenia 10;
- dowód twierdzenia 12.

Wnioskując na podstawie deklaracji, **udział Doktoranta w opracowaniu głównego wyniku jest istotny**. Dotyczy to zarówno strony technicznej, jak i koncepcyjnej.

Pewne znaczenie mają także wyniki rozdziału czwartego, gdzie pokazano oparty na pomysłach poprzedniego rozdziału schemat podpisu cyfrowego oraz protokół uwierzytelniania. Idee te są stosunkowo prostymi i standardowymi rozwinięciami poprzedniego pomysłu (poprzez zastosowanie drzew Merkle'a, czy protokołu Fiata-Shamira), niemniej wymagały od Doktoranta umiejętności technicznych i nietrywialnej analizy.

Poza wskazanymi rozprawa nie zawiera innych, nowych wyników o znaczeniu naukowym.

Silne strony pracy

- Praca zawiera ważną, ciekawą koncepcję która stanowi ważny krok w stronę wykorzystania BRM w powszechnej praktyce. Sama koncepcja, mimo że bardzo mocno opiera się o znane techniki (np. funkcje kdf, bezpieczeństwo definiowane przez entropię), jest istotnym i niebanalnym rozszerzeniem dotychczasowego stanu wiedzy. Co więcej, potencjalnie może się przyczynić do spopularyzowania modelu BRM nawet na obszar rzeczywistych zastosowań.
- Przedstawiona analiza i konstrukcja wykorzystują dużą liczbę różnorodnych technik – także tych bardzo nowych. Co więcej metody te zostały użyte w sposób bardzo subtelny. Przykładowo, nie zastosowano na przykład standardowych ekstraktorów a tzw. *dispersery*. Co więcej, wybór ten w sposób bardzo przekonujący został uzasadniony w rozdziale 1.3.6. Podobnie, dobrze umotywowano zastosowanie w analizie modelu wyroczni losowej zamiast pozornie silniejszego modelu standardowego.
- Zastosowane modele bezpieczeństwa wydają się adekwatne do rzeczywistości, co nie jest zupełnie oczywiste wobec mnogości definicji prywatności.
- Główny wynik pracy wpisuje się w ważny, popularny i trudny nurt badań prowadzonych w wielu wiodących ośrodkach na świecie.

Słabe strony pracy

1. Bardzo podkreślaną wartością zaprezentowanego w rozprawie wyniku jest to, że mają one silne zakorzenienie w praktyce, w tym sensie że motywowane są względami praktycznymi i potrzebami rzeczywistych systemów. W autoreferacie zaznaczono nawet, że system ma być bezpieczny *„dla pewnych rozsądnych, spełnianych w świecie rzeczywistym paramentów "*. W rozprawie znajdziemy odwołanie do konkretnych systemów - między innymi urządzeń mobilnych, gdzie rzeczywiście pomysł na wykorzystanie istniejących danych jako klucza jest bardzo naturalny ze względu na ograniczoną pamięć. Podejście takie jest bardzo cenne, i nieczęste w przypadku doktoratów z dziedziny nauk matematycznych. Niemniej realizacja pomysłu to protokół, którego bezpieczeństwo zależy od **kilkunastu parametrów** - w tym od *min- entropii* danych D, które służą jako klucz, wielkości przechowywanych danych, użytej funkcji haszującej, epsilona, ograniczenia na liczbę zapytań do wyroczni, ograniczenia na wielkość wycieku danych etc... . Bezskutecznie próbowałem sobie wyobrazić jak taki system miałby działać i czy powszechnie przechowywane dane mają wystarczająco dobre własności potrzebne do użycia nowych schematów ? Jeśli tak, jaki musi być rozmiar klucza ? Szczególnie, że min-entropia wydaje się bardzo silna w sensie założeń modelu. Byłbym zobowiązany, gdyby Pan Michał Zając zechciał na ewentualnych dalszych etapach przewodu skomentować to zagadnienie.

   Chcę jednak zaznaczyć, że nawet jeśli taki model nie odpowiada żadnym konkretnym systemom rzeczywistym, ani takim które mogą w przewidywalnej przyszłości

się pojawić (co prawdę mówiąc podejrzewam), **wynik ten i tak pozostaje znaczący pod względem teoretycznym i stanowi pewien krok w stronę praktyki**.

2. Wynik rozdziału trzeciego dotyczy dwóch aspektów bezpieczeństwa. O ile definicja pierwszego, klasycznego nie budzi wątpliwości, o tyle definicja prywatności (sformułowana w definicji 11) prosi się o lepsze umotywowanie i umiejscowienie na tle bogatej literatury dotyczącej anonimowości czy silnie związanych prywatności oraz nierozróżnialności. Tu też warto zaznaczyć, że przyjęta definicja wydaje się w zasadzie w pełni akceptowalna ale w rozprawie doktorskiej należy się spodziewać szerszego komentarza i przedstawienia tła literaturowego.

3. W dowodzie lematu 8 nie jest dla mnie jasna nierówność $\alpha \leq 2^{\lambda}\beta$. Zapewne jest to argument typu union bound, jednak wymaga ono głębszego uzasadnienia.

4. Dowód lematu 9 jest wyjątkowo nieprzejrzyście napisany (końcowy akapit).

5. Definicja 11 jest nieprecyzyjna. O ile można zaakceptować brak formalnego wyjaśnienia czym jest „**Output**“ (bo taki zapis w niektórych pracach się stosuje), o tyle relacja $\approx_{\varepsilon}$ powinna być wyjaśniona w sposób akceptowalny dla nauk matematycznych. Ten zapis **nie** jest standardowy.

6. W wielu miejscach brakuje szerszego, bardziej rzetelnego opisu. Niektóre przykłady:

   - W definicji 4 znajdujemy właściwie kilka definicji kluczowych, i przynajmniej w części, niestandardowych pojęć opisanych dość lakonicznie. Należało je podzielić. Dodatkowym utrudnieniem jest też to, że samo EUG pojawia się dopiero na kolejnej stronie, w dodatku z innymi parametrami. W szczególności, czym jest funkcja ζ trzeba sobie dopowiedzieć na podstawie komentarza w kolejnym podrozdziale.
   - Pierwsza nierówność na str. 29 zdecydowanie wymaga komentarza.
   - Końcówka przykładu 14 niejasna. O jakim zdarzeniu mówi Autor ? Wskazana formuła zdaje się być zwykłą nierównością.
   - s. 41, twierdzenie 11: sam wzór jest trudny do zrozumienia, dodatkowo pojawia się definicja.
   - Brak podania źródeł w części definicji (np. w 2.8).
   - Czym jest z formalnego punktu widzenia k w przykładzie 12 ?
   - Rozdział 2.5: Chociaż pojęcie „zaniedbywalnie mały” (*negligible*) często pojawia się w literaturze kryptograficznej jako standardowe, jego wyjaśnienie powinno być umieszczone w rozprawie.

   To skrótowe podejście szczególnie razi na tle kilku pierwszych stron w tej niegrubej rozprawie przeznaczonych, nie wiedzieć czemu, na bardzo szczegółowe omówienie zagadnień prostych, luźno związanych z tematem rozprawy. Niektóre są wręcz zbędne (na przykład szczegółowy opis wybranych zabytków kryptografii) lub z powodzeniem mogłyby zostać zawarte w dwóch linijkach (przykłady z rozdziału pierwszego).

7. Str. 49 nie jest wyjaśnione z jakiego zbioru elementy wektora $\mathbf{v}$ są losowane.

8. Twierdzenie 15 jak rozumiem jest przepisane z innej pracy. Nie wydaje mi się to koniecznie. Niemniej jeśli Autor postanowił je w rozprawie umieścić, powinien ujednolicić notację, a przynajmniej wyjaśnić na przykład czym jest $negl$ a także zdefiniować nowe symbole, które przywędrowały z obcej pracy.

9. Rozdział 4.5 jest bardzo skrótowy. Trudno podpowiedzieć po jego lekturze, ile konkretnie użytkownik musi wykonać wywołań funkcji haszującej i ile bitów przesłać przy zmianie x bitów swoich danych.

10. Notacja jest nieprzemyślana.

    - Przykładem może być tu wprowadzony 1.3.2 symbol SD, który nigdy później nie zostaje użyty.
    - Można zauważyć, że wiele symboli nie zostało zdefiniowanych. Przykłady to: ε-close (s. 17), $\approx_\varepsilon$, $\rightleftharpoons$ (s. 42), $\mathcal{U}_n$, PPT. Niektóre z nich **nie są standardowe** w literaturze kryptograficznej, nie mówiąc nawet o informatyce jako dyscyplinie w ogóle. Co prawda w większości przypadków można z kontekstu domyśleć się ich znaczenia - choćby z treści dowodów. Niemniej jest to w mojej ocenie istotne uchybienie, które bardzo utrudnia przeanalizowanie, i tak niełatwego rozumowania.
    - Notacja jest jakby zapożyczona z różnych źródeł, nieujednolicona. Autor niektóre zbiory, wydaje się analogiczne, reprezentuje zupełnie innymi symbolami. Zbiór możliwych wiadomości raz reprezentowany przez dwuwyrazowy napis frakturą - rozdział 4.3, raz klasycznym pismem ozdobnym $\mathcal{M}$ (przykład 12) a czasami w ogóle nie jest oznaczany.

11. Rozwiązania z rozdziału czwartego, w świetle wyników z rozdziału trzeciego są koncepcyjnie standardowe, wręcz klasyczne. Zastosowanie drzewa Merkle'a czy protokółu Fiata–Shamira trudno określić jako pomysłowe, bo mają po lat trzydzieści ze sporym okładem. Przyznać jednak trzeba, że pełna analiza wymagała wysiłku, znajomości technik które jednak zostały poprawnie zastosowane, co dobrze o Doktorancie świadczy.

12. Biorąc pod uwagę deklarację udziału w opracowaniu głównego wyniku, rezultatów jest stosunkowo mało, jak na typową rozprawę w dyscyplinie informatyka. Całościowy wkład Doktoranta określiłbym jako zadowalający.

Uchybienia pomniejsze

Rozprawa jest niedopracowana na poziomie edycyjno-prezentacyjnym. Wskazać można bardzo liczne literówki, oczywiste błędy czy niekonsekwencje. Ich obecność co prawda nie uniemożliwia zrozumienia przekazu, jednak ich obfitość znacząco utrudnia lekturę.

Oczywiste błędy językowe świadczą o tym, że rozprawa **nie została poddana jakiejkolwiek korekcie, nawet automatycznej**.

Przykłady:

- Pewne są obiekty nadmiarowe - przy stosowanej dalej konwencji, że się utożsamia zm. losową z jej rozkładem wprowadzanie zm. $\mathcal{Y}$ (s. 19) nie jest celowe.
- Widać także brak spójności - ta sama funkcja raz jest oznaczana jako SD (s. 16) a raz Δ (s. 30). Raz Autor pisze $\mathcal{U}_n$, a raz U_n. W tym ostatnim przypadku, czytelnik nie może wykluczyć, że pierwszy symbol to zm. losowa a drugi to jej rozkład. Ale i to powinno być *expressis verbis* wyrażone. Nawet i przy takim założeniu trudno pewne przypadki użycia wyjaśnić (twierdzenie 11 oraz definicja 16)
- Brak spójności w bibliografii, występują oczywiste błędy - między innymi fragmenty tytułów tworzące „dodatkowych" autorów (np $[HLWO06]$), dane niekompletne (np. $[BDK+11]$).
- Przy niektórych zapożyczonych definicjach należy wskazać źródła - np. przy definicji 8.
- Str 52, pierwszy podpunkt punktu 1. używa dwa razy symbolu R w **różnych** znaczeniach. Żadne z tych znaczeń nie zostało wyjaśnione.
- Zarówno w Autoreferacie, jak i Rozprawie w kilku miejscach jest i a powinno być $\{i\}$. Chyba, że Autor używa innych konwencji teoriomnogościowych, ale i to wymagałoby komentarza.
- W kilu miejscach w rozdziale 3 jest równość zamiast słabej nierówności co dodatkowo utrudnia śledzenie i tak niełatwego dowodu.
- Poza brakami widać też pewną nadmiarowość - symbol $p(x)$ jest wyjaśniany w definicji 5 oraz definicji 8.
- Gdy jest mowa o wielomianowej liczbie, czasem podaje się względem czego, a czasem nie.
- W rozdziale 2.4 protokół identyfikacji zostaje przedstawiony w postaci definicji 3. Kilka linijek dalej w rozdziale 2.5 znajduje się protokół podpisu. Mimo analogicznej sytuacji, wyszczególnionej definicji podpisu nie ma. Ponadto w 2.4 pojawia się symbol Π, który właściwie nie jest potrzebny a powoduje, że zrozumienie tekstu staje się trudniejsze.
- Znaczenie Δ_λ powinno być lepiej przedstawione.

„Autoreferat" Na kilka osobnych uwag zasługuje Autoreferat. Jak na swoją małą objętość zawiera **liczne** błędy stylistyczne, językowe i **bardzo liczne** literówki. Zdarzają się niepoprawne gramatycznie zdania. Tłumaczenia są bardzo dyskusyjne (np. *dystans statystyczny, black-boksowy*) a sama polityka tłumaczenia specjalistycznych terminów jest niekonsekwentna bo wiele z nich nie zostało przetłumaczonych w ogóle.

Autor w Autoreferacie powiela wiele uchybień z rozprawy, dodaje jednak też nowe np. na str. 6. niejasne sformułowanie na temat zmiennej losowej D. Ogólnie, tekst ten robi wrażenie jakby nie był nigdy przez Autora przeczytany i z pewnością nie powinien być przekazany jakiemukolwiek czytelnikowi. Wydaje się, że dokładne omówienie Autoreferatu wykracza poza obowiązki recenzenta. Poza tym jego treść nie wpływa na moją merytoryczną ocenę wyników.

Wątpliwości

Poniżej wskazuję na kilka szczegółów, które wzbudziły moje (być może niesłuszne) wątpliwości.

- Sens rozdziału 2.2 nie jest do końca jasny. Wydaje się, że dla dalszego toku rozumowania wystarczyłby komentarz, że λ może zależeć od długości klucza lub nie, w zależności od modelu. W szczególności nie jest dla mnie jasna uwaga o funkcji p.
- Czy rzeczywiście potrzebna jest definicja 1 ? Zdaje się, że dalej właściwie jest w pełni zastępowana definicją 2.
- W 2.4 wydaje się, że bardziej właściwie będzie protokół ten nazwać uwierzytelnianiem (*authentication*) a nie identyfikacją ?
- W 2.2 Autor wprowadza funkcje f_i, które się później pojawiają jedynie w 3.1 i zdają się nie mieć żadnego znaczenia dla dalszego rozumowania. Może wystarczy uwaga o sumie bitów dostępnych adwersarzowi ?

Konkluzja - dalsze etapy

Ogólna ocena przedłożonej rozprawy jest trudna. Z jednej strony **mamy ciekawy, ważny wynik który w istotnej części jest dziełem Doktoranta**. Jego prezentacja w rozprawie jednak dość wyraźnie odbiega od przyjętego standardu. Jestem przekonany, że wyniki naukowe Pana Zająca zasługują na doktorat. Niemniej w mojej ocenie należy wcześniej poprawić rozprawę, też aby strona formalna nie pozostawiała żadnych wątpliwości co do poprawności rozumowań.

Niezależnie, w przypadku gdyby Autoreferat miał być publicznie dostępny, sugerowałbym Komisji zwrócenie się do Pana Michała Zająca z prośbą o zdecydowaną poprawę, przynajmniej w warstwie językowej, tego dokumentu.