Warszawa, dn. 01. 06. 2022 r.

dr hab. inż. Andrzej Paszkiewicz
Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni
DKWOC
ul. gen broni Tadeusza Buka 1
05-119 Legionowo

RECENZJA

Przedmiotem recenzji jest rozprawa doktorska P. mgr. inż. Olgi DZIĘGIELEWSKIEJ na temat: „*Extending selected statistical disclosure control models with adaptive metrics and evaluation framework*" napisana w języku angielskim (po polsku „*Rozszerzenie wybranych modeli sterowania ujawnianiem danych statystycznych o metryki adaptacyjne i mechanizm oceny*"). Praca została napisana pod kierunkiem P. prof. dr hab. inż. Bolesława Szafrańskiego z Wydziału Cybernetyki Wojskowej Akademii Technicznej.

1. Kontekst społeczny i cywilizacyjny rozprawy i jej ważność w świetle współcześnie prowadzonych badań

Do niedawna aparat statystyki matematycznej w odniesieniu do zgromadzonych danych był stosowany w kierunku pozyskania jak największej ilości informacji o danych, poszukiwania korelacji między określonymi ich podzbiorami i trendów rozmaitych zjawisk opisywanych przez zbiory danych statystycznych w funkcji czasu. Typowymi przykładami takiego wykorzystania jest np. badanie średniej długości życia człowieka i jej rozwarstwienie w kierunku płci, miejsca zamieszkania czy wykonywanego zawodu, skuteczność stosowania rozmaitych leków czy średni czas bezawaryjnej pracy systemu technicznego. Poprzez umiejętną analizę danych statystycznych przechowywanych w bazach danych, zwłaszcza przy wadliwych mechanizmach zabezpieczeń, można jednak pozyskać cenne informacje o konkretnych obiektach, których zbierane dane dotyczą, w szczególności ich jednoznacznej identyfikacji i wzajemnych powiązań między nimi, czego zapewne chcielibyśmy uniknąć. Informacja na temat genomu, czy przekroju chorób społeczeństwa żyjącego na określonym

terenie jest cenną rzeczą ale już ta sama informacja w odniesieniu do konkretnego człowieka jest niepożądana, zwłaszcza w obcych rękach, i może być dla niego rzeczą niebezpieczną.

W ciągu ostatnich dwudziestu lat burzliwie rozwijająca się informatyka dostarczyła wielu narzędzi i metod pozwalających na dokonywanie zakupów przez Internet, załatwianie spraw urzędowych, wykonywanie przelewów z własnego konta na konto innych obywateli czy firm, bez potrzeby bezpośredniego odwiedzania banków i straty czasu spędzanego w kolejkach. Najnowsze rozwiązania w zakresie *claud computing* pozwalają także na założenie „w chmurze" własnej firmy i korzystanie do jej administrowania z dostarczonych narzędzi za niewielką opłatą bez potrzeby kosztownego inwestowania w sprzęt, zatrudniania ludzi, wynajmowanie pomieszczeń, zakładanie baz danych etc. Ciemniejszą stroną tej nowej rzeczywistości może być obawa związana z przejęciem wrażliwych danych, śledzeniem łańcuchów dostaw w przypadku firm, nieuprawnionym korzystaniem z wyników cudzej pracy, czy po prostu złośliwym zniszczeniem naszych zasobów, przechowywanych nie wiadomo gdzie w cyberprzestrzeni.

Na szczęście również w ostatnich kilkunastu latach pojawiły się za sprawą rozwoju informatyki dwa genialne rozwiązania, pozwalające widzieć naszą „*cyberprzyszłość*" nieco bardziej optymistycznie. Pierwszą jaskółką może być przełomowa praca doktorska Craige'a Gentry obroniona w 2009 roku na Uniwersytecie Stanforda (Craig Gentry. *Fully homomorphic encryption scheme.* PhD thesis, Stanford University , 2009. Praca w formie skróconej została opublikowana jako *Fully homomorphic encryption using ideal lattices*. In Michael Mitzenmacher, editor, *Proceedings of the 41st Annual ACM Symposium on Theory of Computing, STOC 2009, pp. 169-178. ACM, 2009*). Wyniki prac Gentry'ego pozwalają na konstrukcję metody przetwarzania danych w postaci zaszyfrowanej. Zatem obawa nieuprawnionego wykorzystania umieszczonych w chmurze danych została teoretycznie zażegnana. Teoretycznie, ponieważ złożoność zaproponowanej metody jest na razie zbyt duża aby można ją było wykorzystać w praktyce.

Drugą przełomową pracą, uhonorowaną prestiżową nagrodą Gödla za 2017 rok, jest praca zbiorowa dotycząca prywatności różnicowej zespołu autorskiego: Cynthia Dwork, Kobbi Nissim i Adam Smith (patrz. C. Dwork, K. Nissim, A. Smith, *Calibrating Noise to Sensitivity in Private Data Analysis*, Journal of Privacy and Confidentiality, vol. 7, iss. 3, 2016. Wstępna wersja tej pracy była opublikowana w Theory of Cryptography, TCC 2006). Kluczową rolę w opracowaniu teorii prywatności różnicowej odegrała Cynthia Dwork, która tym problemem zajmowała się już kilka lat wcześniej. Recenzowana dysertacja w istotny sposób jest zakorzeniona w pracach związanych z prywatnością różnicową. Metody statystyki

matematycznej zostały tam wykorzystane w kierunku nietypowym, mianowicie poprzez domieszkowanie szumu o określonym rozkładzie prawdopodobieństwa podczas odczytywania danych z bazy (w niektórych przypadkach podczas wpisywania danych do bazy), dane są nieczułe pod kątem wycieku informacji o pojedynczych obiektach, gdy atak jest wykonywany serią kwerend za pomocą minimalnie zmodyfikowanych parametrów zapytań. Badania przeprowadzone przez p. mgr inż. Olgę Dzięgielewską są na czasie i bardzo dobrze wpisują się w nurt współcześnie prowadzonych badań.

2. Struktura i tezy rozprawy doktorskiej

Praca posiada stosunkowo zwarty charakter, składa się z dziewięciu rozdziałów nie wliczając bibliografii liczącej 59 pozycji literatury, cytowanej w różnych miejscach przedłożonej rozprawy. Są to w większości pozycje świeże, które pojawiły się w ciągu ostatnich kilku lat. Jedynie trzy spośród cytowanych pozycji literatury pochodzą z lat osiemdziesiątych ub. wieku i należą do klasyki związanej z ochroną statystycznych baz danych czy też ochroną informacji w ogólności (np. klasyczna pozycja Dorothy E. Robbling Denning). Wśród cytowanych prac znalazły się także cztery prace, których autorką lub współautorką jest Doktorantka.

Rozdział 1. *Introduction*, zawiera krótki opis zawartości wszystkich następujących po nim rozdziałów. Dodatkowo znalazł się w nim spis terminów używanych w pracy, skrótów oraz ich definicje, lista rysunków oraz tablic. To bardzo ułatwia dalszą lekturę przedłożonej pracy. Rozdział 2 *Statistical Databases Security,* stanowi krótkie wprowadzenie i definicje dotyczące statystycznych baz danych, w tym także odnosi się do dokumentów ustawowych regulujących porządek prawny, ochronę danych przechowywanych w tych bazach w Polsce, Unii Europejskiej i Stanach Zjednoczonych. Rozdział 3, *Research Problem* formułuje zadanie badawcze podjęte do realizacji w ramach pracy oraz tezy. *Jest nią stwierdzenie mówiące, że metody sterowania ujawnianiem danych statystycznych rozszerzone o metryki adaptacyjne zdefiniowane przez Doktorantkę w metodyce VIOLAS są w stanie skutecznie zapobiegać atakom przy pomocy wnioskowania.* W rozdziale tym Doktorantka formułuje także cztery kryteria bezpieczeństwa. Są nimi *statistical confidentiality*, *statistical integrity*, *statistical accuracy* i *statistical transparency*. Obszerny rozdział czwarty *Risk Assessment for Statistical Inference Attacks* podejmuje problematykę oszacowania ryzyka ataków wnioskowaniem statystycznym, według mojego odczucia jest to jeden z najciekawiej napisanych fragmentów pracy. Rozdział piąty *VIOLAS FRAMEWORK for EVALUATING DISCLOSURE CONTROL*

METHODS zawiera wcześniej zapowiedzianą metodykę VIOLAS. W rozdziale szóstym *Extending Differential Privacy Model* zdefiniowano metryki w rozszerzonym modelu prywatności różnicowej i zaproponowano algorytm ich wyznaczania. Rozdział siódmy *Evaluation of the Metrics* zawiera pewne dywagacje dotyczące wprowadzonych metryk a także wyniki przeprowadzonych w niewielkiej skali obliczeń. Pomimo pewnych uchybień występujących w tym rozdziale (o czym później) jest to również jeden z ciekawiej napisanych fragmentów pracy. Rozdział ósmy *Application Considerations* zawiera luźne uwagi dotyczące aplikacji i wreszcie rozdział dziewiąty *Summary and Conclusions* podsumowuje całość pracy i wyniki w niej uzyskane.

3. Dostrzeżone błędy i uchybienia

Praca, pomimo lekkiej konstrukcji i stosunkowo niewielkiej objętości nie jest wolna od pewnych błędów i uchybień. Poniżej przedstawiam listę tych, które udało mi się wychwycić podczas jej lektury.

- Str. 53, wzór (15) – zbiór indeksów do których, do którego należy i, nie powinien zawierać elementu 0, inaczej jego liczność będzie równa n+1. Również zaraz po znaku równoważności <-> w tym wzorze zamiast q_n, powinno być q_i;
- Str. 53, wzór (17) - zbiór indeksów, do którego należy i nie powinien zawierać 0;
- Str. 54, wzór (18) – analogiczne uwagi jak do wzoru (15);
- Str. 54, wzór (19) – brak zamykającego nawiasu kwadratowego po prawej stronie nierówności;
- Str. 57, wzór (22) – zamiast operatora przypisania „=" powinien być operator porównania „==", jeżeli używamy konwencji języka C/C++. We wzorze (20) zapis jest prawidłowy;
- Str 60, wzór (29) – w zapisie normy powinien wystąpić indeks 1, inaczej będzie ona rozumiana jako "zwyczajna" norma euklidesowa, tymczasem jest to suma wartości bezwzględnych pomiędzy odpowiadającymi sobie współrzędnymi dwóch wektorów tej samej przestrzeni;
- Str. 68, wzór (31) dot. funkcji supp – brakuje zapisu „where T is a set of transactions …", który definiuje czym jest T;
- Str. 68, wzór (32) – w mianowniku brakuje nawiasu zamykającego;

- Str. 68, wzór (33) – nadmiarowy nawias rozpoczynający (w mianowniku funkcji lift;
- Str. 81, 7 wiersz od dołu – nadmiarowy symbol |X| w odwzorowaniu M : $N^{|X|}$ -> R;
- Str. 81, 7 wiersz od dołu – w przyjętym zapisie powinno być ε - differentially zamiast (ε,δ) – differentially;
- Str. 81, wiersz 5 od dołu – patrz uwaga do wiersza 7 od dołu na tej samej stronie;
- Str. 82. od góry aż do końca sekcji. Zawarty tu tekst jest próbą wyrażenia treści zawartych w Stwierdzeniu 2. 1 i wcześniejszym Twierdzeniu z cytowanej pracy źródłowej Dwork & Roth *The Algorithmic Foundations of Differential Privacy*, 2014. Twierdzenia zawarte w pracy źródłowej są prawdziwe przy odpowiednich, subtelnych założeniach, tymczasem pozbawienie ich formy rygorystycznych twierdzeń powoduje, że zapisany tu tekst zatracił pierwotne walory spójności i uciekł w niepożądanym kierunku;
- W zapisach pseudokodu algorytmów (patrz Str. 72-73, 75, 77), warto byłoby trzymać się jakiejś przyzwoitej konwencji np. wziętej z jęz. C/C++ z wykorzystywanymi tam nawiasami czy w innych konwencjach pseudo-Pascala z wytłuszczaniem słów kluczowych, czy ostatnio modnej konwencji, w której zaznacza się początek i koniec pętli. W przeciwnym przypadku trudno się w tym wszystkim „połapać". Jest to szczególnie trudne przy długich komentarzach, które zaburzają interpretacje naturalnie stosowanych „wcięć". Recenzent poświęcił dużo czasu żeby zbadać strukturę i poprawność opisywanych algorytmów;
- Warto nadmienić, że zagadnienie SLI DERIVATION, str. 56-58, może być sprowadzone do analizy funkcji czterech lub pięciu zmiennych i poszukiwania jej wartości ekstremalnych na zbiorze wypukłym.

4. Język pracy

Praca została konsekwentnie napisana w języku angielskim. Ze względu na tematykę jest to język dość hermetyczny, używany przez wąskie grono specjalistów, skupiony wokół pojęć związanych bezpośrednio z tematyką dysertacji. W trakcie lektury kilku początkowych rozdziałów pracy zastanawiałem się nad sensownością, czy motywacją, która skłoniła Autorkę do napisania pracy w języku obcym i czy nie stanowi to aby dodatkowego utrudnienia i ryzyka, związanego z możliwością niezamierzonego „wstrzyknięcia" szumu

statystycznego (używając terminologii zawartej w dysertacji) w postaci błędów. Dopiero pod koniec lektury pracy zdałem sobie sprawę, że jest wręcz odwrotnie. Ponieważ praca dotyczy dziedziny (differential privacy), która dopiero od niedawna stawia swoje pierwsze kroki, więc nie mogła doczekać się normatywnego tłumaczenia pojęć na język polski. Co więcej Autorka musiałaby wymyślić i zaproponować adekwatną terminologię w języku polskim, co nie byłoby rzeczą łatwą. Łatwiej więc jest korzystać z gotowych wzorców językowych już funkcjonujących w języku, w którym zostały napisane prace źródłowe. Jako pewien niewielki mankament pracy uważam brak w niej streszczenia po polsku. Mogłoby ono stanowić zachętę do przeczytania jej z chwilą, gdy znajdzie się w odpowiedniej bazie danych.

Nie zajmowałem się oceną jakości języka, w którym została praca napisana. Jest on bowiem środkiem do wyrażania myśli a nie jej celem.

5. Podsumowanie

Podsumowując, uważam, że praca „*Extending selected statistical disclosure control models with adaptive metrics and evaluation framework*" napisana przez P. mgr inż. Olgę Dzięgielewską w przedstawionej formie **spełnia wymagania przewidziane dla rozpraw doktorskich w aktualnie obowiązującej ustawie i stawiam wniosek o przyjęcie jej jako rozprawy doktorskiej i dopuszczenie jej Autorki do publicznej obrony**.

Jednocześnie chciałbym przeprosić Promotora i Doktorantkę, za przekroczenie limitu przydzielonego mi czasu na wykonanie recenzji, które choć niezbyt wielkie, w okresie przedwakacyjnym, mogło być zupełnie inaczej odczuwane po obydwu stronach. Z drugiej strony wyrażam również swoje podziękowanie, za złożenie mi propozycji zrecenzowania niniejszej rozprawy doktorskiej, dzięki czemu mogłem, przy okazji, bez obawy utraty czasu, zapoznać się z ważnymi pracami dotyczącymi prywatności różnicowej, będącymi kamieniami milowymi, wyznaczającymi kierunki rozwoju naszej współczesnej cywilizacji cyfrowej.