Tomasz Jurdziński
Wydział Matematyki i Informatyki
Instytut Informatyki
Uniwersytet Wrocławski

Wrocław, 28 lipca 2020

Recenzja rozprawy doktorskiej mgr. Krzysztofa Grininga zatytułowanej "Privacy-Preserving Protocols in Unreliable Distributed Systems"

Pan Krzysztof Grining złożył rozprawę doktorską poświęconą tematyce agregacji danych z zachowaniem prywatności modelowanej poprzez pojęcia prywatności różnicowej (ang. differential privacy) i jej wariantowi nazywanemu prywatnością „bezszumową" (ang. noiseless privacy). Wyniki badawcze przedstawione w rozprawie zostały wcześniej opublikowane w sprawozdaniach międzynarodowych konferencji ACNS, TrustCom, AsiaCCS oraz w czasopismach naukowych International Journal of Information Security i Journal of Complex Networks.

Zawartość rozprawy

Rozprawę zaczyna rozdział wprowadzający w tematykę oraz przedstawiający wykorzystywane narzędzia matematyczne. Właściwe wyniki badawcze opisane są w rozdziałach 2 – 4. W krótkim rozdziale piątym znajduje się podsumowanie wyników rozprawy wraz z sugestiami odnośnie ich znaczenia i zastosowań. Poniżej przedstawiam krótkie omówienie rezultatów przedstawionych w rozprawie. Z uwagi na złożoność wykorzystywanych modeli i czynionych założeń, poniższe omówienie opisuje wyniki na ogólnym poziomie, pomijając niektóre istotne szczegóły.

Rozdział 2 – protokoły agregacji

W rozdziale drugim autor zajmuje się analizą i konstrukcją pewnych protokołów zapewniania prywatności różnicowej w środowisku sieciowym. Pierwsza część rozdziału poświęcona jest analizie znanego protokołu agregacji (sumy) n oryginalnych wartości o nazwie Binary Protocol. Zakłada się tutaj, że pewna liczba użytkowników κ jest nieaktywna, np. wskutek działania adwersarza. W oryginalnym artykule (z FC 2012) pokazano asymptotyczne logarytmiczne ze względu na n ograniczenie górne na błąd wyniku agregacji dla tego protokołu przy stałych wartościach pozostałych parametrów. W rozprawie przeprowadzona została bardziej precyzyjna analiza wielkości błędu Binary Protocol, która pozwoliła na wyprowadzenie dość dokładnych ograniczeń dolnych na wielkość błędu. Wymagało to zastosowania **zaawansowanych** narzędzi probabilistyki i dokładnej analizy kombinatorycznej dla oszacowania częstości występowania zdarzeń zwiększających oczekiwany błąd wyniku agregacji. Korzystając z tych nowych ograniczeń doktorant przeanalizował wielkości błędów dla (niewielkich) wartości parametrów n, κ występujących w praktycznych zastosowaniach. Przeprowadzone analizy i obliczenia wykazały, że uzyskane błędy są stosunkowo duże i mogą stanowić przeszkodę w praktycznych zastosowaniach protokołu.

Wyniki dotyczące Binary Protocol stanowiły motywację do badań zaprezentowanych w drugiej części rozdziału 2 – konstrukcji i analizy nowego protokołu agregacji, nazwanego PAALC (od ang. Precise Aggregation Algorithm with Local Communication). Przystępując do tego zadania **zmieniono** założenia odnośnie komunikacji. Do zaimplementowania Binary Protocol

wystarczy, aby uczestnicy protokołu (n posiadaczy agregowanych wartości) mieli możliwość jednokrotnego przesłania wiadomości do centralnego „agregatora". W rozprawie przyjęto naturalny model środowiska rozproszonego, w którym uczestnicy tworzą sieć modelowaną poprzez graf prosty umożliwiający bezpośrednią dwustronną komunikację między sąsiadami w grafie. Przyjęto też założenie, że połączenia komunikacyjne modelowane przez krawędzie w grafie są bezpieczne (niemożliwe jest podsłuchanie komunikacji z zewnątrz). Dla takiego środowiska zaprojektowany został protokół agregujący indywidualne wartości dwustopniowo: najpierw w mniejszych grupach, następnie zagregowane wartości z grup zbierane są globalnie. Protokół wykorzystuje znane schematy szyfrowania asymetrycznego i przy standardowych założeniach kryptograficznych pokazane zostały bardzo dobre własności prywatności protokołu PAALC. Główny trik umożliwiający zmniejszenie ryzyka kumulacji błędów dodawanych na potrzeby prywatności polega na dodawaniu do przesyłanych wartości losowych elementów $x_v^{v'}$ odpowiadających wszystkim skierowanym krawędziom (v, v') grafu połączeń. Dzięki temu, że węzły przesyłają sąsiadom te losowe wartości i umieszczają w swoich sumach wartości odpowiadające zarówno krawędziom wychodzącym jak i wchodzącym z różnym znakiem, wartości $x_v^{v'}$ znikają w procesie agregacji. Pewnym mankamentem PAALC jest niska ochrona prywatności węzłów znajdujących się w bardzo małych grupach/składowych, powstałych wskutek adwersarialnego uszkodzenia κ wybranych wierzchołków grafu.

Na końcu rozdziału 2 przedstawione zostało eksperymentalne porównanie działania obu protokołów dla różnych zakresów wartości κ i innych parametrów, na rzeczywistych danych złożonych z $n = 4039$ wierzchołków pochodzących z sieci Facebook (zbiór danych SNAP ze Stanford University). Rezultaty potwierdziły wcześniejsze wyniki analityczne wynikające po części z różnych modeli komunikacji: błąd wyniku algorytmu PAALC jest istotnie mniejszy od błędu Binary Protocol i nie rośnie wraz ze wzrostem liczby nie κ. Osobny wykres potwierdza duży rozmiar największego spójnego komponentu grafu po usunięciu κ wierzchołków przy niewielkich wartościach κ. Wierzchołki w tym komponencie mają największą gwarancję prywatności.

Rozdział 3 – zwiększanie spójności grafu na potrzeby prywatnych protokołów agregacji

Tematyka rozdziału 3 w naturalny sposób wynika z zagrożeń prywatności, jakie pociąga za sobą agregacja w środowisku sieciowym rozważanym w rozdziale drugim, w szczególności z użyciem protokołu PAALC. Głównym zagrożeniem w PAALC jest ograniczenie prywatności części wierzchołków poprzez wyłączenie/usunięcie κ węzłów prowadzące do podziału grafu sieci na wiele rozłączne składowe spójności.

Jako sposób na zapobieżenie powyższemu zagrożeniu zaproponowano w rozdziale 3 różne metody wzmacniania spójności grafu polegające na dodawaniu nowych krawędzi przy wykorzystaniu lokalnej komunikacji. Dokładniej, zaproponowane zostały trzy różne metody dodawania nowych krawędzi tak, że każdy wierzchołek sieci może wybrać k nowych krawędzi prowadzących do wierzchołków w odległości dwa lub do sąsiadów tzw. fat nodes, dla ustalonej wartości parametru k. Krawędzie dodawane są w sposób losowy zgodnie z rozkładem definiującym każdą z trzech metod o skrótowych nazwach 2SFF (wybór losowego sąsiada mojego sąsiada, rozkład jednostajny), A3F (wybór losowego sąsiada losowego fat node), 2S3F (wybór losowego sąsiada mojego sąsiada, prawdopodobieństwa proporcjonalne do stopni sąsiadów). Na potrzeby potencjalnych praktycznych scenariuszy przyjęto, że wierzchołki grafu mogą indywidualnie podejmować decyzje o udziale lub braku udziału w procesie rozszerzania grafu o nowe krawędzie.

W dalszej części rozdziału analizowane są własności grafów uzyskanych przez dodanie nowych krawędzi przy założeniu, że oryginalny graf sieci został uzyskany wg modelu *preferential attachment graphs* (PDA). W analizie rozważano dwa scenariusze usuwania

wierzchołków z grafu przez adwersarza: w pierwszym scenariuszu zbiór usuniętych wierzchołków jest wybrany losowo z rozkładem jednostajnym, w drugim scenariuszu usuwane są wszystkie fat nodes (wierzchołki o stopniach $\Omega(n/\log n)$). Wśród konkretnych wyników m.in. zidentyfikowano parametry gwarantujące spójność rozszerzonego grafu po usunięciu wszystkich fat nodes a także zależności między wartościami standardowych parametrów a rozmiarami największych spójnych składowych w wynikowym grafie. Obliczenia przeprowadzone na potrzeby tych wyników korzystają m.in. z własności grafów losowanych zgodnie z modelem Erdős -Renyi jak i grafów PDA.

Wyniki analityczne zostały uzupełnione dość rozległymi symulacjami dla rzeczywistych danych z sieci społecznościowej Epinion (zbiór danych SNAP ze Stanford University). Rezultaty eksperymentów w dość przekonujący sposób ilustrują korzystny wpływ zastosowania poszczególnych algorytmów na rozmiar największej spójnej składowej w grafie uzyskanym po usunięciu wybranych wierzchołków dla różnych wartości parametru k określającego liczbę nowych krawędzi wybieranych przez wierzchołki uczestniczące w algorytmie „zagęszczania" grafu. Wpływ ten jest szczególnie istotny, gdy usuwany jest losowy podzbiór wierzchołków. Niemniej, również w przypadku usuwania fat nodes niektóre protokoły dają istotny postęp już przy niewielkiej liczbie k dodawanych nowych krawędzi przez każdy aktywny wierzchołek.

Być może **najciekawsze** wyniki eksperymentów dotyczą aspektu, który nie był analizowany formalnie – frakcji wierzchołków uczestniczących w algorytmie zagęszczania grafu, które znalazły się w największej spójnej składowej wynikowego grafu. Wykonane eksperymenty wskazują, że frakcja takich wierzchołków nie zmniejsza się istotnie wraz ze zmniejszeniem liczby wierzchołków uczestniczących w zagęszczaniu. Oznacza to, że wierzchołki nie-uczestniczące w algorytmie nie wpływają istotnie na bezpieczeństwo tych wierzchołków, które aktywnie rozszerzają graf o nowe krawędzie zgodnie z przyjętym protokołem.

Rozdział 4 – rozszerzenia noiseless privacy

Podczas gdy model prywatności różnicowej rozważany w rozdziałach 2 i 3 wymaga zachowania prywatności każdej agregowanej wartości nawet przy znanych („deterministycznych") wartościach pozostałych elementów, w rozdziale 4 autor zajmuje się agregacją w modelu noiseless privacy zakładającym losowość samych agregowanych danych.

Pierwszym naturalnym zagadnieniem badawczym rozważanym w tym rozdziale jest ustalenie parametrów ε i δ, dla których suma n niezależnych 0/1 zmiennych losowych $B(n,p)$ spełnia warunki (ε,δ)-noiseless-privacy. Jak zilustrowano na wykresie dla małych wartości n, uzyskane oszacowania dają istotnie lepsze wyniki od wcześniejszych asymptotycznych rezultatów z pracy wprowadzającej model noiseless privacy (z ASIACRYPT 2011).

Następnie analiza noiseless privacy zostaje przeprowadzona dla sumy niezależnych zmiennych losowych o być może różnych rozkładach. Kolejnym krokiem jest rozważenie sytuacji, gdy co prawda agregowane wartości są losowe, ale dopuszcza się ograniczoną zależność między nimi. Podane w twierdzeniach 12 i 13 oszacowania dla takich założeń uzyskane są z pomocą narzędzi do szacowania odległości między rozkładami losowymi w różnych miarach – twierdzenia Berry'ego-Essena i metody Steina. Te wyniki zostały z kolei uogólnione na scenariusz „hybrydowy", w którym adwersarz może znać liniową frakcję agregowanych wartości tak jak w standardowym modelu differential privacy a pozostałe są losowe, tak jak w modelu noiseless privacy. Oszacowania dla takich założeń zostały przedstawione w twierdzeniach 14 i 15. W rozdziale 4.6 rozważana jest z kolei sytuacja, w której losowość samych danych zostaje połączona z losowymi zaburzeniami agregowanych wartości, stosowanymi w standardowym modelu prywatności różnicowej. Aplikując wcześniej używane techniki autor formułuje pewne ograniczenia na parametry prywatności w tym modelu i ilustruje je prostym przykładem.

Ocena rozprawy

Ogólna ocena merytoryczna

Rozprawa podejmuje aktualne, intensywnie badane i istotne dla zastosowań narzędzi informatycznych tematy. Duży wysiłek włożony został w odpowiednie wymodelowanie studiowanych problemów, aby uzyskane wyniki miały nie tylko teoretyczno-poznawcze znaczenie, ale także potencjał aplikacyjny. Za cel postawiono sobie również dokładne, nie tylko asymptotyczne, oszacowanie niektórych wartości decydujących o praktycznej przydatności badanych protokołów i algorytmów. Realizacja tak postawionych celów wymagała pogłębionej wiedzy i umiejętności z różnych obszarów matematyki i informatyki. Wśród stosowanych narzędzi i technik znajdują się m.in. asymetryczne protokoły kryptograficzne dopasowane do wymagań agregacji danych, analiza własności grafów losowych wg rozkładów Erdős–Renyi oraz preferential attachment model, analiza własności zmiennych losowych z wykorzystaniem funkcji charakterystycznych dodatniej składowej, analiza rozkładów (sum) zmiennych losowych z wykorzystaniem nierówności Chernoffa, twierdzenia Waldta, szacowanie odległości między rozkładami losowymi z użyciem twierdzenia Barry'ego-Essena, metody Steina. Choć każde z tych narzędzi z osobna może być zapewne uznane za standardowe w pewnym środowisku badawczym, stosowanie ich wszystkich w jednej rozprawie z informatyki jest dość unikalne. Dlatego też wysoko oceniam przygotowanie merytoryczne autora, ogólną wiedzę, sprawność rachunkową i umiejętność stosowania zróżnicowanych narzędzi matematycznych w problematyce informatycznej.

Pozytywnym wyróżnikiem ocenianej rozprawy jest również spójność tematyczna odzwierciedlająca jasno zarysowany i konsekwentnie realizowany plan badawczy. Wszystkie rezultaty wychodzą od standardowego pojęcia prywatności w agregacji danych i studiowane są różne aspekty i scenariusze istotne dla realizacji tego celu. Konsekwencja w realizacji tak zarysowanego planu zasługuje na uznanie.

W mojej subiektywnej ocenie drobnym mankamentem rozprawy jest przewaga działań związanych z modelowaniem problemów nad poszukiwaniem kompletnych rozwiązań. W efekcie same wyniki z rozprawy mają być może nieco bardziej techniczny niż poznawczy charakter. Uzyskiwane rozwiązania zazwyczaj nie wymagają wysoce zaawansowanych rozumowań, trudność leży raczej w konieczności stosowania zróżnicowanych i zaawansowanych technik i narzędzi. Mam też drobne wątpliwości odnośnie ścisłości dwóch rozumowań, o czym dokładniej piszę poniżej. Niezależnie od tych częściowo krytycznych uwag chciałbym podkreślić, że właściwie wszystkie rezultaty przedstawione w rozprawie zyskały pewne zainteresowanie środowiska zajmującego się bezpieczeństwem informacji i komunikacji i przeszły weryfikację tego środowiska, co potwierdzone jest akceptacją rezultatów na konkurencyjne recenzowane międzynarodowe konferencje i publikacjami w środowiskowych czasopismach naukowych.

Drobne uwagi szczegółowe

Pewne drobne wątpliwości budzi krytyka protokołu Binary Protocol w oparciu o jego porównanie z PAALC na końcu rozdziału drugiego. Wydaje się jasne, że różnice w błędzie uzyskiwanym w obu protokołach wynikają zarówno z tego, że PAALC korzysta z bardziej rozbudowanego modelu komunikacji jak i z faktu, że PAALC nie gwarantuje prywatności użytkowników znajdujących się w małych spójnych składowych. Ponadto dla PAALC nie zostało wyprowadzone „analityczne" ograniczenie $o(n)$ na wielkość błędu.

Wydaje mi się również, że powołania na spójność grafów Erdös-Renyí z odpowiednio dużym prawdopodobieństwem losowania krawędzi w dowodach Lemma 4 i Theorem 8 to swego rodzaju skróty myślowe lub niedociągnięcia. Sposoby losowania grafów opisane w Lemma 4

i Theorem 8 nie zapewniają pełnej niezależności losowania każdej krawędzi. Dlatego nie jestem pewien czy można je traktować jak Erdös-Renyí graphs.

Redakcja rozprawy

Rozprawa jest bardzo dobrze przygotowana od strony redakcyjnej. Tekst rozprawy jest zrozumiały, adresowane problemy dobrze uzasadnione a wyniki zilustrowane licznymi przykładami. Pojawiające się nieliczne błędy lub omyłki nie wpływają na zrozumiałość prezentowanych treści, obliczeń bądź rozumowań. Na potrzeby ewentualnej dalszej redakcji wyników rozprawie, podaję kilka zauważonych drobnych błędów, omyłek i nieścisłości:

- str. 38, Fact 5: sformułowanie „moderate values" warto doprecyzować; tym bardziej, że ograniczenia na wartości n i ε są potrzebne w dowodzie;
- str. 47, Filling the ciphertext: wartość Enc nie zależy od sk'?
- str. 59: ograniczenie z góry na stopnie wierzchołków fat jest trochę nieintuicyjne, warto wyjaśnić;
- str. 73, dowód Theorem 10: dlaczego można przyjąć „We assume that at least (...) of them appeared after step n=2"?
- str. 105, Theorem 12: brak końcówki "M(X) is (ε, δ)-NP."

Podsumowanie

Rozprawa doktorska Krzysztofa Grininga jest rezultatem realizacji dobrze uzasadnionego i spójnego planu badawczego podejmującego istotną tematykę prywatności danych w procesie agregacji. Przedstawione wyniki dają nową wiedzę o znanych wcześniej protokołach agregacji zorientowanych na zachowanie prywatności jak i wprowadzają nowe modele prywatności i środowisk jej realizacji oraz odpowiednie rozwiązania. Rezultaty analityczne są uzupełnione instruktywnymi eksperymentami i symulacjami. Wyniki przedstawione w rozprawie zyskały zainteresowanie środowiska naukowego i zostały pozytywnie zweryfikowane, co potwierdzają publikacje w materiałach międzynarodowych konkurencyjnych konferencji i w czasopismach. W pracy nad rozprawą Pan Grining wykazał się dużą wiedzą i umiejętnościami posługiwania się zaawansowanymi narzędziami matematycznymi w rozwiązywaniu problemów informatycznych a także w identyfikowaniu i modelowaniu problemów. Uwzględniając te wszystkie pozytywne strony uzyskanych wyników **rozprawę oceniam pozytywnie,** niezależnie od przedstawionych wcześniej drobnych zastrzeżeń odnośnie charakteru atakowanych problemów badawczych i pojedynczych wątpliwości odnośnie ścisłości rozumowania.

W związku z powyższą opinią nie mam wątpliwości, że rozprawa Pana Krzysztofa Grininga spełnia ustawowe i zwyczajowe wymagania stawiane doktoratom w obszarze informatyki. Wnioskuję tym samym o **pozytywne** zaopiniowanie rozprawy i dopuszczenie do dalszych etapów przewodu doktorskiego.