Warszawa, 03.06.2020

Prof. dr hab. Adam Wierzbicki
Polsko-Japońska Akademia
Technik Komputerowych

OPINIA
O ROZPRAWIE DOKTORSKIEJ

MGR KRZYSZTOFA GRININGA

"PRIVACY-PRESERVING PROTOCOLS IN UNRELIABLE DISTRIBUTED SYSTEMS"

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

   Rozprawa dotyczy zagadnienia projektowania protokołów agregacji danych z wielu niezależnych źródeł w systemie rozproszonym, przy zachowaniu prywatności danych pochodzących z indywidualnych źródeł. Szczególnie, rozprawa skupia się na zapewnieniu „prywatności różnicowej" (ang. *„differential privacy"*), czyli własności protokołów agregacji polegającej na tym, że znając wynik protokołu, nie da się określić wartości danych żadnego indywidualnego uczestnika protokołu (z dostateczną dokładnością). Pojęcie prywatności różnicowej jest sformalizowanym matematycznie modelem prywatności. Rozprawa dotyczy również innego modelu prywatności – „prywatności bez szumów" (ang. *„noiseless privacy"*).

   Rozpatrywane zagadnienie naukowe jest sformułowane ogólnie we wprowadzeniu:

   „In this thesis we focus on privacy-preserving protocols in distributed systems. This is due to the importance of such systems and their growing amount, for example mobile users, IoT, smart metering, autonomous vehicles and many others.

   Most interesting, and practically useful, case is when the system is unreliable, i.e., some of the nodes can fail either randomly or due to some malicious entity. We propose a various approaches, both by devising a new protocol and by proposing a slightly modified model to improve privacy in such systems."

   Jest to jednak sformułowanie nieprecyzyjne, albowiem autor skupia się na ograniczonym przypadku, w którym obliczana funkcja agregacji jest funkcją sumy danych, a w dodatku zbiór uczestników protokołu jest znany i nie ulega zmianom.

   Rozprawa ma charakter teoretyczny.

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?**

Przegląd literatury (rozdział 1.3), opis stanu wiedzy oraz wnioski z przeglądu literatury (a właściwiej ich brak) stanowią najsłabszy element rozprawy. W moim odczuciu, analiza literatury opisana w rozprawie nie spełnia standardów pracy naukowej i wymaga poprawy.

Rozprawa ma zaledwie 73 pozycje bibliograficzne. W przeglądzie literatury autor przekierowuje czytelnika do opublikowanych artykułów w celu uzupełnienia bibliografii: *„In this section we present some of the most important papers related to this thesis. For more references one can see our papers mentioned in Subsection 1.1."* Jest to, moim zdaniem, niewłaściwe podejście, albowiem rozprawa doktorska nie ma ograniczeń objętościowych i powinna zawierać wyczerpujący przegląd literatury.

W przeglądzie literatury autor pomija całe dziedziny badań w zakresie informatyki, które mają silne związki z rozpatrywanym problemem badawczym. Pierwszą taką dziedziną są technologie blockchain. Zapytanie do serwisu Google Scholar w dniu 2.06.2020: ``*blockchain "differential privacy"*'' zwraca 1210 wyników (684 z nich od 2019 roku). Rozprawa nie zawiera słowa kluczowego blockchain. Poniższe publikacje nie są cytowane w pracy:

1. Yang, M., Margheri, A., Hu, R., & Sassone, V. (2018). Differentially private data sharing in a cloud federation with blockchain. *IEEE Cloud Computing*, *5*(6), 69-79.
2. Zyskind, G., & Nathan, O. (2015, May). Decentralizing privacy: Using blockchain to protect personal data. In *2015 IEEE Security and Privacy Workshops* (pp. 180-184). IEEE. (praca ma 1250 cytowań na Google Scholar)
3. Gai, K., Wu, Y., Zhu, L., Qiu, M., & Shen, M. (2019). Privacy-preserving energy trading using consortium blockchain in smart grid. *IEEE Transactions on Industrial Informatics*, *15*(6), 3548-3558.
4. Chen, X., Ji, J., Luo, C., Liao, W., & Li, P. (2018, December). When machine learning meets blockchain: A decentralized, privacy-preserving and secure design. In *2018 IEEE International Conference on Big Data (Big Data)* (pp. 1178-1187). IEEE.
5. Samuel, O., Javaid, N., Awais, M., Ahmed, Z., Imran, M., & Guizani, M. (2019, July). A blockchain model for fair data sharing in deregulated smart grids. In *IEEE Global Communications Conference (GLOBCOM 2019)*.
6. Zhao, Y., Zhao, J., Kang, J., Zhang, Z., Niyato, D., & Shi, S. (2020). A Blockchain-Based Approach for Saving and Tracking Differential-Privacy Cost. *arXiv preprint arXiv:2001.09259*.
7. Hassan, M. U., Rehmani, M. H., & Chen, J. (2019). Differential Privacy in Blockhain Technology: A Futuristic Approach. *arXiv preprint arXiv:1910.04316*.
8. Nagar, A. (2019). Privacy-Preserving Blockchain Based Federated Learning with Differential Data Sharing. *arXiv preprint arXiv:1912.04859*.

Autor rozprawy wiele uwagi poświęca protokołowi "Binary Protocol", opisanemu w publikacji:
Chan, T. H. H., Shi, E., & Song, D. (2012, February). Privacy-preserving stream aggregation with fault tolerance. In *International Conference on Financial Cryptography and Data Security* (pp. 200-214). Springer, Berlin, Heidelberg.

Rozdział 2 rozprawy jest poświęcony udoskonaleniom tego protokołu. Jednakże nawet w tak wąskim zakresie, autor nie przeprowadził wyczerpującej analizy literatury. Zapytanie w serwisie Google Scholar (01.06.2020) o prace cytujące artykuł (Chan, 2012) zwraca 161 wyników. Ograniczenie do prac od 2019 roku zwraca 22 wyniki. Spośród nich, następujące publikacje nie są cytowane w rozprawie:

9. Truex, S., Baracaldo, N., Anwar, A., Steinke, T., Ludwig, H., Zhang, R., & Zhou, Y. (2019, November). A hybrid approach to privacy-preserving federated learning. In *Proceedings of the 12th ACM Workshop on Artificial Intelligence and Security* (pp. 1-11).
10. Munz, R. (2019). Towards Usability in Private Data Analytics. (rozprawa doktorska z grudnia, 2019 roku na Politechnice Kaiserslautern)
11. Rane, S., Bindschaedler, V., Brito, A. E., Uzun, E., & Rao, V. (2019). *U.S. Patent No. 10,223,547*. Washington, DC: U.S. Patent and Trademark Office.
12. Kairouz, P., McMahan, H. B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A. N., ... & d'Oliveira, R. G. (2019). Advances and open problems in federated learning. *arXiv preprint arXiv:1912.04977*. (przegląd literatury zawierający 438 pozycji)

Ostatnia pozycje (Kairouz, 2019) jest przeglądem literatury dotyczącej prywatności różnicowej, na który autor mógł się powołać i który może wykorzystać do poprawy własnej analizy literatury. Pozycja (Munz, 2019) jest rozprawą doktorską, poświęconą zbliżonemu zagadnieniu badawczemu.

Prace autora zmierzają do wykorzystania lokalnej komunikacji do poprawy protokołów zapewniających prywatność różnicową. Także i w tym zakresie przegląd literatury nie jest wystarczający. Zapytanie do Google Scholar (01.06.2020): ``*"differential privacy" "local communication"*'' zwraca 67 wyników. Poniższe publikacje nie są cytowane w pracy:

13. Zhu, J., Xu, C., Guan, J., & Wu, D. O. (2018). Differentially private distributed online algorithms over time-varying directed networks. *IEEE Transactions on Signal and Information Processing over Networks*, *4*(1), 4-17.
14. Friedman, A., Sharfman, I., Keren, D., & Schuster, A. (2014, February). Privacy-Preserving Distributed Stream Monitoring. In *NDSS* (pp. 1-12).
15. Beimel, A., Kasiviswanathan, S. P., & Nissim, K. (2010, February). Bounds on the sample complexity for private learning and private data release. In *Theory of Cryptography Conference* (pp. 437-454). Springer, Berlin, Heidelberg.
16. Khandade, N. V., & Nargundi, S. Hiding User Privacy in Location Based Services Through Clustering.

Popularnym i znanym podejściem do budowy protokołów wykorzystujących lokalną komunikację są protokoły plotkujące (ang. *„gossiping protocols"*). Autor wydaje się nie znać tego pojęcia, które nie występuje w rozprawie. Zapytanie do Google Scholar: ``*gossiping "differential privacy"*'' zwraca 288 wyników. Rozprawa nie zawiera słowa kluczowego „gossiping". Poniższe publikacje nie są cytowane w pracy:

17. Hanzely, F., Konečný, J., Loizou, N., Richtárik, P., & Grishchenko, D. (2017). Privacy preserving randomized gossip algorithms. arXiv preprint arXiv:1706.07636.
18. Liu, Y., Liu, J., & Basar, T. (2018, December). Differentially private gossip gradient descent. In *2018 IEEE Conference on Decision and Control (CDC)* (pp. 2777-2782). IEEE.
19. Hegedűs, I., & Jelasity, M. (2017). Differentially private linear models for gossip learning through data perturbation. *OPEN JOURNAL OF INTERNET OF THINGS*, *3*(1), 62-74.
20. Foner, L. (1995, March). Clustering and Information Sharing in an Ecology of Cooperating Agents, or How to Gossip without Spilling the Beans. In *Proceedings of the Conference on Computers, Freedom, and Privacy'95 Student Paper Winner.*
21. Bellet, A., Guerraoui, R., & Hendrikx, H. (2019). Who started this rumor? Quantifying the natural differential privacy guarantees of gossip protocols. *arXiv preprint arXiv:1902.07138.*
22. Huang, Y., & Dai, H. (2019). Quantifying Differential Privacy of Gossip Protocols in General Networks. *arXiv preprint arXiv:1905.07598.*

W proponowanym przez siebie protokole (rozdział 2) autor używa metod kryptografii homomorficznej. Jednakże także i w zakresie użycia kryptografii homomorficznej do zapewnienia prywatności różnicowej, autor nie przeanalizował istotnej literatury. Następująca praca:

23. Halevi, S., Lindell, Y., & Pinkas, B. (2011, August). Secure computation on the web: Computing without simultaneous interaction. In Annual Cryptology Conference (pp. 132-150). Springer, Berlin, Heidelberg.
poświęcona jest zastosowaniom kryptografii homomorficznej do zapewnienia prywatności w protokole klient-serwer.

Recenzent nie przesądza o tym, że powyższe publikacje opisują prace konkurencyjne do wyników autora. Jednakże tak duże braki w przeglądzie literatury uniemożliwiają stwierdzenie, czy autor w swojej pracy uwzględnił konkurencyjne rozwiązania i porównał z nimi swoje wyniki. Co więcej, przegląd literatury powinien przedstawić również prace pokrewne, które wnoszą dodatkową wiedzę dotyczącą zagadnienia badawczego, na przykład pokazując inne metody badawcze bądź obszary zastosowań.
Recenzent jest przekonany o tym, że szersza lektura prac naukowych z pokrewnych tematów będzie z korzyścią dla przyszłych badań prowadzonych przez doktoranta. Przykładem takich korzyści może być lepsze uzasadnienie istotności problemu badawczego poprzez odniesienie do prac, które mogą stosować wyniki uzyskana przez doktoranta – zobacz punkt 7 recenzji.

3. **Czy autor rozwiązał postawione zagadnienia, czy użył właściwej do tego metody i czy przyjęte założenia są uzasadnione?**
Autor posługuje się głównie metodą analizy matematycznej. Przyjmuje w tym celu wiele założeń, które nie są jasno przedstawione we wprowadzeniu do rozprawy. Pierwszym z nich jest ograniczenie funkcji agregacji do funkcji sumy indywidualnych danych. Jest to ograniczenie dopuszczalne, albowiem wiele zastosowań korzysta głównie z funkcji sumy. Jednakże autor czyni inne założenia, na przykład, że zbiór uczestników protokołu jest znany i niezmienny. Jest to dość ograniczające założenie w kontekście systemów rozproszonych, bowiem wyklucza otwarte systemy rozproszone, a także użycie takich technologii jak multicast. Co więcej, w połączeniu z poprzednim założeniem, założenie to daje daleko idące konsekwencje: niemożliwe jest użycie metod zaproponowanych przez autora do obliczania średnich ruchomych, w których średnia jest aktualizowana o nowe wartości pozyskiwane od nowych uczestników protokołu. W rozprawie brak jest wyczerpującej dyskusji poczynionych założeń i wynikających z nich ograniczeń wyników uzyskanych przez autora.

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?**

Samodzielny dorobek autora rozprawy jest udokumentowany w pięciu publikacjach:

A. Krzysztof Grining and Marek Klonowski, Towards extending noiseless privacy: Dependent data and more practical approach, Proceedings of the 12th ACM on Asia Conference on Computer and Communications Security (AsiaCCS), 2017, pp. 546–560. Konferencja ma rangę B w rankingu Core, co oznacza uzyskanie **70 punktów** w ranking ministerialnym.
B. Krzysztof Grining, Marek Klonowski, and Małgorzata Sulkowska, How to cooperate locally to improve global privacy in social networks? On amplification of privacy preserving data aggregation, Proceedings of the 16th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2017, pp. 464–471. Konferencja ma rangę A w rankingu Core, co oznacza uzyskanie **140 punktów** w ranking ministerialnym.
C. Krzysztof Grining, Marek Klonowski, and Małgorzata Sulkowska, Stronger trust and privacy in social networks via local cooperation, Journal of Complex Networks (2019). Czasopismo figuruje na ministerialnej liście czasopism i ma **100 punktów**.
D. Krzysztof Grining, Marek Klonowski, and Piotr Syga, Practical fault-tolerant data aggregation, International Conference on Applied Cryptography and Network Security (ACNS), Springer, 2016, pp. 386–404. Konferencja ma rangę B w rankingu Core, co oznacza uzyskanie **70 punktów** w ranking ministerialnym.
E. Krzysztof Grining, Marek Klonowski, and Piotr Syga, On practical privacy preserving fault tolerant data aggregation, International Journal of Information Security 18 (2019), no. 3, pp. 285–304. Czasopismo figuruje na ministerialnej liście czasopism i ma **100 punktów**.

Należy zwrócić uwagę, że doktorant jest pierwszym autorem każdej z tych publikacji. W serwisie Google Scholar prace doktoranta mają 13 cytowań (H-indeks 2). Podsumowując stwierdzam, że doktorant ma dostateczny samodzielny dorobek badawczy do obrony doktoratu.

Do najbardziej oryginalnych wyników rozprawy należą prace autora nad modelem „noiseless privacy". Autor uogólnił wyniki uzyskana dla tego modelu, które zakładały całkowitą niezależność agregowanych wartości, a uzyskane rezultaty były wyłącznie asymptotyczne. W rozprawie opisano wyniki nie tylko dla danych niezależnych, ale również takich z lokalnymi zależnościami. Ponadto wyniki autora dotyczą dowolnych rozkładów, a do ich zastosowania potrzebne jest oszacowanie trzech pierwszych momentów z rozkładu danych, oszacowania na liczbę użytkowników, których dane adwersarz posiada oraz, w przypadku danych zależnych, oszacowanie na wielkość największego zależnego podzbioru. W rozprawie przedstawione są wyniki konkretne (nieasymptotyczne), a przez to bardziej dokładne w praktycznych zastosowaniach.

Jednakże wobec niewystarczającej analizy pokrewnej literatury, trudno jest ocenić oryginalność wkładu autora do współczesnego stanu wiedzy. Recenzent musi w tym zakresie zaufać recenzentom prac opublikowanych przez autora na konferencjach i w czasopismach.

5. **Czy autor wykazał umiejętność poprawnego i przekonywującego przedstawienie uzyskanych przez siebie wyników (zwięzłość, jasność, poprawność redakcyjna rozprawy)?**
   Autor posługuje się dobrym i jasnym językiem, a język angielski w rozprawie jest poprawny. Rozprawa ma prosty i przejrzysty układ. Jednakże wstęp i zakończenie rozprawy pozostawiają wiele do życzenia – zobacz następny punkt.

6. **Jakie są słabe strony rozprawy i jej główne wady?**
   Najsłabszym elementem rozprawy jest przegląd literatury, który w odczuciu recenzenta nie spełnia standardów pracy naukowej. Pominięcie tak znacznej ilości pokrewnych prac oraz całych dziedzin badań blisko związanych z zagadnieniem badawczym autora jest nieprofesjonalne. Recenzent oczekuje od autora istotnej poprawy przeglądu literatury oraz sformułowania wniosków z tego przeglądu, które wyraźnie uzasadnią innowacyjność wyników opisanych w rozprawie.

   Kolejnym słabym punktem jest brak w rozprawie rozdziałów lub sekcji poświęconych dyskusji ograniczeń uzyskanych wyników. Jest to szczególnie widoczne w zakończeniu (rozdział 5), które ma 2 strony długości. Autor powinien w zakończeniu podsumować uzyskane wyniki, wskazać ich ograniczenia i zaproponować kierunki przyszłych badań.

   Analiza wyników uzyskanych przez autora w każdym z rozdziałów nie porusza w ogóle zagadnienia złożoności obliczeniowej (bądź pamięciowej lub komunikacyjnej. W całej rozprawie, słowo kluczowe „complexity" nie występuje ani razu. Jest to uderzające w rozprawie z dziedziny informatyki (zobacz następny punkt). Analiza złożoności proponowanych przez autora protokołów wskazałaby wyraźnie na ich możliwe

zastosowania bądź ograniczenia. Czy protokoły proponowane przez autora można stosować na urządzeniach o ograniczonych zasobach obliczeniowych, bądź zasilanych baterią? Recenzent oczekuje od autora rozprawy uzupełnienia rozprawy o dyskusję złożoności obliczeniowej proponowanych protokołów.

7. **Jaka jest przydatność rozprawy dla Informatyki?**

Autor składa doktorat w dziedzinie Informatyki jako części nauk matematycznych. Należy jednak zaznaczyć, że nauki matematyczne dzielą się na teoretyczne i stosowane. Informatyka jest w opinii recenzenta nauką stosowaną, która może częściowo przynależeć do stosowanych nauk matematycznych. Autor zdaje sobie z tego sprawę, dlatego w wielu punktach swojej rozprawy i publikacji podejmuje próbę analizy i poprawy możliwości praktycznych zastosowań swoich rezultatów. W tym zakresie, autor ma pewne osiągnięcia, pomimo tego, że jego rozwiązania nie były implementowane ani testowane eksperymentalnie.

Pomimo tego, autor niedostatecznie uzasadnił potencjalne możliwości zastosowań wyników swoich badań, a co za tym – ich znaczenia dla Informatyki. Wiąże się to także z pobieżnym przeglądem literatury. Autor praktycznie zignorował takie obszary zastosowań jak *„federated learning"*, czyli rozproszone uczenie maszynowe z zachowaniem prywatności danych. Nawet ograniczone wyniki autora dotyczące obliczania funkcji sumy danych mogłyby mieć znaczenie dla tej dziedziny: zob. pracę (także nie cytowaną w rozprawie):

Bonawitz, K., Ivanov, V., Kreuter, B., Marcedone, A., McMahan, H. B., Patel, S., ... & Seth, K. (2017, October). Practical secure aggregation for privacy-preserving machine learning. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1175-1191).

Jak wiele podobnych, istotnych współcześnie pojęć w dziedzinie Informatyki (blockchain, gossiping protocols), pojęcie „federated learning" nie występuje w rozprawie.

Kolejnym, uderzającym przykładem braku odniesień do zastosowań jest kompletny brak analizy złożoności obliczeniowej, komunikacyjnej itd. w rozprawie. Z punktu widzenia recenzenta, jest to niedopuszczalne w rozprawie z dziedziny Informatyki.

Podsumowując – mimo starań autora, przydatność rozprawy dla Informatyki jest niedostatecznie uzasadniona.

WNIOSKI

Autor posiada dostateczny samodzielny dorobek badawczy, udokumentowany publikacjami w dobrych czasopismach i konferencjach naukowych. Rozprawa oparta jest na tych publikacjach, dlatego można przyjąć, że wyniki naukowe opisane w rozprawie spełniają wymogi stawiane rozprawom doktorskim, pomimo zastrzeżeń opisanych w tej recenzji.

Podsumowując stwierdzam, że **rozprawa spełnia wymagania stawiane rozprawom doktorskim przez obowiązujące przepisy, wymaga jednak znacznej poprawy.**

Prof. dr hab. Adam Wierzbicki