Legnica, 26 lipca 2016 r.

dr hab. inż. Wojciech Kordecki,
Państwowa Wyższa Szkoła Zawodowa
im. Witelona w Legnicy
ul. Sejmowa 5
59-220 Legnica
e-mail: wojciech.kordecki@pwsz-legnica.eu

Recenzja rozprawy doktorskiej
mgr. Łukasza Nitschke p.t.

Bezpieczeństwo protokołów w środowisku o ograniczonym zaufaniu

Zawartość rozprawy

Rozprawa doktorska mgr. Łukasza Nitsche składa się ze wstępu, czterech rozdziałów, posumowania i dodatku. We wstępie autor w wielkim skrócie przedstawia zawartość rozprawy. W pierwszym rozdziale autor przedstawia podstawowe pojęcia, omawia krótko lecz wyczerpująco podstawowe narzędzia kryptograficzne oraz problem bezpiecznej platformy. Rozdział drugi poświęcony jest sieciom mieszającym. Stanowi on podstawę dla przedstawianych dalej wyników własnych. W szczególności autor przedstawił metody weryfikujące działanie sieci oraz zapewnienie integralności wiadomości przesyłanych przez sieć. Szczegółowo autor przedstawił w punkcie 2.3 procedurę RPC. Następnie, w punkcie 2.4 autor przedstawił wpływ procedur RPC na poziom anonimowości. W punkcie 2.5 przedstawiono dwuetapowy wariant tej procedury wraz ze szczegółową analizą. Na tej podstawie autor podał własną, ulepszoną wersję tej procedury.

Rozdział trzeci poświęcony zagadnieniu wyborów elektronicznych, zawiera w większości wyniki własne autora. Punkt 3.1 jest przeglądem dotychczasowej wiedzy o wyborach przez internet, zaś punkt 3.2 zawiera przegląd najczęściej omawianych w literaturze protokołów. W punkcie 3.3 autor przedstawia własne wyniki dotyczące protokołów opartych na zaufanym sprzęcie. Omówiono

protokół oparty na kartach chipowych z ekranem. Teoretyczne własności zostały podsumowane w dwóch ciekawych własnościach, jako fakty 3.3.1 i 3.3.2. Wyniki z tego punktu zostały opublikowane w roku 2008. Punkt 3.4 zawiera omówienie protokołu opartego na papierowych kartach do głosowania. Punkt 3.4.6 zawiera również propozycje uogólnień. Wyniki z tego punktu zostały opublikowane również w roku 2008. W punkcie 3.5 zostały przedstawione systemy głosownia dla małych grup wyborców.

Rozdział czwarty poświęcony jest bardzo ważnym i mającym bezpośrednie zastosowania zagadnieniom egzaminów zdalnych (autor używa nazwy „egzaminy elektroniczne"). W dwóch pierwszych punktach scharakteryzowano takie systemy egzaminów oraz podano przegląd istniejących rozwiązań. Treść tych punktów pochodzi z dwóch prac przeglądowych, których doktorant jest współautorem. Ostatni, trzeci punkt poświęcony protokołom opartym na dwuetapowym mieszaniu, zawiera wyniki własne, przygotowane do publikacji.

Dodatek stanowi integralną i bardzo ważną część rozprawy. Przedstawiono w nim w sposób ścisły niezbędny aparat matematyczny uzupełniający jej rozważania. Jednakże w pracy nie zauważyłem bezpośredniego powołania się na wyniki przedstawione w tym dodatku.

Ocena wartości rozprawy doktorskiej

Rozprawa doktorska mgr. Łukasza Nitschke jest napisana ładną polszczyzną, z dbałością o logiczną strukturę. Zwraca też uwagę bardzo elegancki skład i starannie wykonane rysunki.

Jako przykład dbałości o logiczną strukturę a zarazem dbałości o czytelność, może służyć cały rozdział 1, a zwłaszcza punkt 1.1. Podane w nim ścisłe definicje uzupełnione są uwagami, które ułatwiają ich rozumienie, zwłaszcza jak sądzę, czytelnikom mniej oswojonym ze specyficzna terminologią informatyczną. Aczkolwiek rozdział ten nie zawiera własnych wyników, to trzeba go ocenić jako bardzo wartościową część rozprawy.

Prawie cały rozdział drugi, podobnie jak pierwszy, zawiera w zasadzie wyniki z literatury. Omówienie sieci mieszających jest bardzo staranne i wyczerpujące. Szczególną uwagę poświęcono procedurze RPC, istotnie wykorzystywaną w dalszych częściach rozprawy. Odpowiedni dobór definicji, twierdzeń i lema-

tów sprawia, że rozprawa staje się samowystarczalna w tym sensie, że czytelnik nie jest zmuszany do żmudnego wyszukiwania źródeł. Całość ilustrują dobrze dobrane rysunki, ułatwiające zrozumienie treści matematycznej. Kończący ten rozdział punkt 2.5.3 zawiera własną propozycję poprawienia dwuetapowej procedury RPC2.

Przedstawione w rozdziale trzecim dwa pierwsze punkty mają charakter przeglądowy i mają te same dobre cechy, co poprzednie rozdziały. Wybrane do nich fakty przedstawiają wszystkie informacje potrzebne dla sformułowania własnych wyników w punktach 3.3 – 3.5. Zwraca zwłaszcza uwagę sposób prezentacji protokołów w punktach 3.4 i 3.5.

Punkty 3.3 i 3.4 opierające się na już opublikowanych artykułach, mają podobną strukturę: założenia, opis protokołu, analiza poprawności i poziomu bezpieczeństwa. W obu punktach autor formułuje algorytmy i dokonuje analizy w sformalizowany, czyli matematyczny sposób, choć brak tu typowych dla prac matematycznych konstrukcji typu „twierdzenie – dowód", które zastąpione są ciągiem opisów przeplatanych wzorami i tabelami. Jest to jednak sposób często spotykany w pracach informatycznych i trudno go uznać za wadliwy, jeśli zachowuje odpowiedni poziom ścisłości. Uważam, że w recenzowanej rozprawie warunek ten jest spełniony.

Ostatni w tym rozdziale punkt 3.5 poświęcony jest bardzo ciekawemu zagadnieniu głosowania w małych grupach wyborców. Cały ten punkt ma charakter raczej opisowy i nie zawiera wyników, które sklasyfikowałbym jako „matematyczne". Nie oznacza to, że zawartość tego punktu oceniam jako mniej wartościową.

Ostatni, czwarty rozdział o tzw. „egzaminach elektronicznych" jest najobszerniejszą częścią z wynikami własnymi. Jednocześnie wyniki w nim przedstawione, aczkolwiek bardzo ciekawe, mają najbardziej „czysto informatyczny" charakter ze wszystkich wyników w rozprawie. Oznacza to, że w tej części wzory matematyczne służą wyłącznie do opisu procedur, a nie do ich analizy. Jest to też rozdział z wynikami, które mogą mieć bardzo bezpośrednie zastosowania w praktyce i to w codziennej praktyce uczelnianej.

Osobnej oceny wymaga Dodatek A mający charakter czysto matematyczny. Przedstawione w nim wyniki dotyczą pewnych problemów z zasadniczej części rozprawy. Uważam, że z punktu widzenia matematycznego jest to bardzo ciekawa, a więc nie tylko „dodatkowa" część rozprawy. Za najciekawsze i jednocześnie trudne uważam tu oszacowanie otrzymane w twierdzeniu A.2.1.

Uwagi krytyczne

W każdej pracy zawsze można znaleźć drobne błędy, których zauważenie wskazuje, że recenzent pracę starannie przeczytał. Niestety, autor nie dał mi tu wielu możliwości. Jedną z nielicznych jest brak numeru punktu, do którego autor odwołuje się na stronie 103. Nie bardzo podoba mi się też nadużywanie słowa „elektroniczny" jako synonimu słowa „zdalny", „na odległość" lub „przez internet". Jest to oczywiście mój subiektywny pogląd. Szkoda też, że powiązania pomiędzy zasadniczą częścią rozprawy a dodatkiem, nie jest określone *explicite*.

Powyższe uwagi dotyczą rzeczy jednak mało istotnych i w niczym nie wpływają na ocenę rozprawy.

Konkluzja

Rozprawy doktorskie z informatyki mogą być podstawą do uzyskania stopnia doktora nauk matematycznych w zakresie informatyki lub stopnia doktora nauk technicznych w zakresie informatyki. Różnica między tymi dwoma zakresami jest często rozmyta. Najpierw więc sprecyzuję ocenę, jaką recenzowana rozprawa wnosi do informatyki, abstrahując chwilowo, jakiej dziedziny nauk (matematycznych czy technicznych) ona dotyczy.

Z przedstawionych powyżej uwag wynika jednoznacznie, że ocena ta może być tylko bardzo dobra. Czy jest jednak podstawą do nadania stopnia doktora nauk matematycznych? Aby odpowiedzieć na to pytanie, zauważę najpierw, że rozprawa ma wyraźnie wyodrębnione cztery wątki:

1. wątek opisowy, w którym przedstawiono znane algorytmy, protokoły itp.,
2. wątek przedstawiające własne procedury, jednakże nie uzasadniający ich w klasyczny sposób poprzez twierdzenia i dowody,
3. ilościowo skromny, ale istotny wątek z twierdzeniami, lematami i dowodami, czyli wątek czysto matematyczny,
4. najskromniejszy, ale niepomijalny wątek „techniczny" – w którym na przykład używa się nazwy „karty chipowe z ekranem".

Strukturę taką i proporcje między tymi wątkami uważam za wyważone i właściwe, a wątek matematyczny jest wystarczająco istotny i ważny, aby recenzowana rozprawa była podstawą do nadania stopnia doktora nauk matematycznych.

Uważam że rozprawa doktorska mgr. Łukasza Nitschke spełnia wszelkie wymogi, zarówno ustawowe jak i zwyczajowe stawiane rozprawom doktorskim w dziedzinie nauk matematycznych w zakresie informatyki.

Wnoszę zatem o dopuszczenie mgr. Łukasza Nitschke do dalszych etapów przewodu doktorskiego.

Wojciech Kordecki