prof. UAM dr hab. Jerzy Szymański
Wydział Matematyki i Informatyki
Uniwersytet im. Adama Mickiewicza w Poznaniu

Poznań, 18 lipca 2016 roku

Recenzja pracy doktorskiej mgra Łukasza Nitschke pt. „Bezpieczeństwo protokołów w środowisku o ograniczonym zaufaniu"

1. Omówienie zawartości pracy

Praca doktorska mgra Łukasza Nitschke dotyczy zagadnień związanych z bezpieczeństwem protokołów, liczy 149 stron i składa się ze wstępu, czterech rozdziałów merytorycznych, podsumowania, dodatku oraz spisu literatury, który obejmuje 76 pozycji (w tym pięciu, których mgr Łukasz Nitschke jest autorem lub współautorem).

Jednostronicowy „Wstęp" jest krótkim przewodnikiem po zawartości całej pracy.

W rozdziale 1 zatytułowanym „Bezpieczeństwo obliczeń" Autor przedstawia definicje i narzędzia kryptograficzne wykorzystywane dalej w pracy. Przedstawione definicje są bardzo precyzyjne, starannie zredagowane i spójne zarówno logicznie jak i stylowo. Przedstawione narzędzia kryptograficzne mimo, że standardowe opisane są precyzyjnie, wykorzystując sukcesywnie wcześniej zdefiniowane pojęcia. Jedyne zastrzeżenie do tej części może dotyczyć bardzo zwartej i suchej prezentacji, którą można jednak uzasadnić nie odstępowaniem od typowych dla tej dziedziny pojęć.

Rozdział 2 zatytułowany „Sieci mieszające" poświęcony jest przedstawieniu ich definicji i własności. Podstawowym zadaniem sieci mieszającej jest uniemożliwienie powiązania przesłanych wiadomości z ich nadawcami nie zniekształcając po drodze żadnej z wiadomości. Idea takiej sieci po raz pierwszy pojawiła się w pracy Davida Chauma w 1981 roku i od tego czasu pojawiło się wiele pomysłów usprawniających je i poprawiających

ich własności. Jeden z takich pomysłów pochodzi od Autora i jest związany z dwukrotnym przejściem przez tę samą sieć z zachowaniem zarówno własności anonimizujących jak i bezpieczeństwa.

W rozdziale 3 zatytułowanym „Wybory elektroniczne" poświęconemu przedstawieniu rozwiązań kryptograficznych mających zastosowanie w wyborach elektronicznych Autor omawia i analizuje wymagania jakie stawia się przed systemem do głosowania a następnie przedstawia istniejące rozwiązania. W tej części pracy Autor prezentuje również dwa swoje rozwiązania: jedno oparte o karty chipowe z ekranem, a drugie o papierowe karty do głosowania. Oba rozwiązania zostały przez Autora publikowane. Prezentacja własnych rozwiązań jest bardzo precyzyjna i dobrze uzasadniona. Omawiane są zarówno problemy poprawności i bezpieczeństwa takiego systemu jak również problemy związane ze złożonością obliczeniową i pamięciową.

W rozdziale 4 zatytułowanym „Egzaminy elektroniczne" Autor przedstawił zastosowanie metod kryptograficznych w modnym od wielu lat temacie e-learningu, a dokładniej w zdalnym egzaminowaniu. Ponownie zdefiniowane są wymagania stawiane systemom zdalnego egzaminowania oraz przegląd istniejących rozwiązań. Ważną częścią tego rozdziału jest przedstawienie własnego rozwiązania opartego o dwuetapowe sieci mieszające. Ponownie zaprezentowane bardzo starannie.

W krótkim podsumowaniu Autor pokazuje ważność i użyteczność omawianych wyników oraz zwraca uwagę na swój wkład w tę tematykę.

Pracę kończy dodatek „Analiza rozkładów brzegowych i łącznych w procedurze częściowego sprawdzania," który zawiera rozważania dotyczące rozkładów brzegowych i łącznych w zależności od liczby wiadomości i serwerów. Rozważania tu przedstawione poparte są dowodami, niestety nie w pełni rozwiązują problem.

2. Ocena pracy

Wyniki uzyskane przez Autora w rozprawie dotyczą konstruowania, dowodzenia poprawności oraz bezpieczeństwa protokołów związanych z wyborami elektronicznymi oraz z e-egzaminami. Spełnienie wszystkich wymogów związanych z tymi tematami jest bardzo trudne, a niektóre z nich tworzą wrażenie wzajemnie sprzecznych (np. anonimowość z weryfikowalnością, a ta z kolei z niemożliwością sprzedawania głosów). Nowoczesne protokoły kryptograficzne pozwalają jednak spełnić te wymogi w zadawalającym stopniu. Nadal jednak problemem jest to, że o wykorzystaniu takich systemów decydują politycy a nie kryptolodzy.

Pierwszy z protokołów wyborczych zaproponowany przez Autora związany jest z za-

stosowaniem specjalnych urządzeń - kart chipowych z ekranem. Wyświetlacz na karcie m.in. upewnia głosującego, ze oddał właściwy głos. Dodatkowo zaproponowana tablica ogłoszeń zapewnia możliwość weryfikacji poprawnego policzenia głosu.

Drugi autorski protokół związany jest z papierowymi kartami do głosowania. Jest on modyfikacją protokołu Prêt à Voter.

W końcu trzeci protokół zaproponowany przez Autora dotyczy egzaminowania elektonicznego i zrealizowany jest przez dwuetapowe mieszanie.

Aby zbudować i przeanalizować powyższe protokoły Autor sprawnie posługuje się pojęciami i technikami zarówno matematycznymi (kryptografia, rachunek prawdopodobieństwa, matematyka dyskretna), jak i informatycznymi (algorytmika, złożoność obliczeniowa, bezpieczeństwo systemów). Jego protokoły są bardzo pomysłowe a uzyskane wyniki dają istotnie ulepszenie w stosunku do istniejących rozwiązań. Uzasadnienie ich poprawności, bezpieczeństwa i innych własności mimo, że wykorzystuje standardowe narzędzia, wymagało dużej wiedzy, pomysłowości i sprawności technicznej.

Pewien niedosyt sprawiła zbytnia „skromność" Autora. Czytając pracę trudno dociec, które wyniki są własne. Można to poznać jedynie po braku powoływania się na autorów oraz z krótkich informacji we Wstępie i Podsumowaniu. Ze swej natury praca doktorska powinna eksponować wyniki autora. Brakuje również informacji o dalszych losach prezentowanych wyników (np. prace dotyczące elektronicznych wyborów ukazały się w 2008 roku i potem były analizowane i cytowane).

Przechodząc do ogólnej oceny wyników zawartych w rozprawie pragnę stwierdzić, że uzyskując je Autor wykazał się nieprzeciętną pomysłowością, pracowitością, sprawnością techniczną i uporem w przezwyciężaniu trudności technicznych. Mimo, ze praca powstawała w bardzo długim okresie czasu to udało zachować się pewną spójność. Autor wykazał się dużą pomysłowością i umiejętnością rozwiązywania praktycznych problemów informatycznych, potrafił również do analizy swoich rozwiązań zastosować zaawansowany aparat matematyczny.

Mgr Łukasz Nitschke opublikował wyniki prezentowane w pracy w pięciu pracach oraz przedstawiał je na kilku konferencjach zarówno krajowych, jak i międzynarodowych. Brał również czynny udział w kilku grantach naukowych dotyczących kryptografii.

Reasumując, wyniki uzyskane w recenzowanej pracy doktorskiej oceniam wysoko. Sądzę, że omawiana rozprawa doktorska stanowi istotny wkład w rozwój teorii wyborów i egzaminów elektronicznych.

3. Uwagi redakcyjne

Praca napisana jest bardzo staranie zarówno pod względem logicznym jak i redakcyjnym. Poza drobnymi literówkami (jak np. str 9_8: powinno być „był" zamiast „być"; str 53^2 „pod uwagę" a nie „pod wagę", itp) nie wpływającymi na ocenę pracy, nie znalazłem żadnych istotnych błędów.

4. Konkluzja

Uważam, że przedstawiona do oceny rozprawa „Bezpieczeństwo protokołów w środowisku o ograniczonym zaufaniu" spełnia wymogi ustawowe stawiane pracom doktorskim i może stanowić podstawę do nadania mgrowi Łukaszowi Nitschke stopnia naukowego doktora nauk matematycznych, w dziedzinie informatyka. W związku z tym wnoszę o dopuszczenie rozprawy doktorskiej mgra Łukasza Nitschke do publicznej obrony.

Jerzy Szymański