Prof. dr hab. Maciej Liśkiewicz
Institute of Theoretical Computer Science
University of Lübeck
Ratzeburger Allee 160,
23538 Lübeck, Germany
Tel. +49 451 3101 5312
maciej.liskiewicz@uni-luebeck.de

Lubeka, 24.09.2026

Recenzja rozprawy doktorskiej mgra Grzegorza Fabiańskiego pt.
An Analysis of Security of Blockchain Protocols and the Role of Formal Methods

Analiza protokołów kryptograficznych, w szczególności złożonych i zdecentralizowanych systemów blockchain, ma kluczowe znaczenie praktyczne, a zarazem stanowi istotne wyzwanie badawcze, ponieważ systemy te muszą zapewniać bezpieczeństwo w nieprzewidywalnych i potencjalnie wrogich środowiskach. W swojej rozprawie doktorskiej Grzegorz Fabiański podejmuje tę problematykę, uzyskując zarówno wyniki negatywne, wskazujące na ograniczenia istniejących rozwiązań, jak i wyniki pozytywne, prowadzące do formalnej weryfikacji oraz dowodów poprawności protokołów kryptograficznych. Tematyka rozprawy wpisuje się w aktualny i intensywnie rozwijany nurt badań w dziedzinie kryptografii, a zaprezentowane wyniki spotkały się z zainteresowaniem środowiska naukowego, czego potwierdzeniem są publikacje przedstawiające wyniki zawarte w rozprawie na trzech wiodących konferencjach w tej dziedzinie.

W części rozprawy poświęconej wynikom negatywnym (rozdział 3) Pan Fabiański poddaje analizie protokoły Plasma, należące do popularnych rozwiązań służących skalowaniu technologii blockchain wykorzystywanej w Ethereum. Autor wskazuje na pewne nieuniknione ograniczenia tego podejścia, pokazując, że w każdym systemie typu Plasma przeciwnik może: (1) zmusić uczciwych uczestników do częstej komunikacji z blockchainem, mimo że nie zamierzali oni podejmować takich interakcji (zjawisko to określa się mianem „masowego wyjścia" – *mass exit*); lub (2) sprawić, że uczciwy uczestnik chcący opuścić system będzie musiał w krótkim czasie przesłać do blockchaina dużą ilość danych. Przeciwdziałanie tym atakom w praktyce jest szczególnie trudne ze względu na brak możliwości jednoznacznego przypisania winy w przypadku wystąpienia awarii (*uniquely attributable faults*). Oznacza to, że inteligentny kontrakt nie jest w stanie ustalić, który z uczestników działa w złej wierze, a tym samym nie może obciążyć go kosztami związanymi z koniecznością interakcji z blockchainem. Ciekawym wnioskiem wynikającym z przeprowadzonej analizy jest pokazanie, że nie jest możliwe jednoczesne uzyskanie korzyści oferowanych przez dwa najważniejsze warianty protokołu Plasma: Plasma Cash oraz Fungible Plasma.

W dowodzie głównego wyniku skonstruowano scenariusz probabilistyczny, oznaczony przez *Exp(V)*, obejmujący dwie epoki działania protokołu Plasma. Opisuje on zachowanie systemu w sytuacji, gdy część użytkowników, wybranych losowo, zostaje odcięta przez przeciwnika od dostępu do operatora. W dalszej analizie konstrukcja ta umożliwia przeciwnikowi odpowiedni dobór koalicji nieuczciwych użytkowników. Scenariusz ten pozwala oszacować, z dużym prawdopodobieństwem, minimalną ilość danych, które użytkownicy muszą przekazać do maszyny kontraktowej, aby skutecznie przeprowadzić procedurę wyjścia i bezpiecznie odzyskać swoje środki.

Warto podkreślić, że przedstawiony dowód nie wymaga przyjmowania żadnych założeń z zakresu teorii złożoności obliczeniowej. Oznacza to, że uzyskane dolne ograniczenia obowiązują również bez takich założeń.

W rozdziale 4 autor przedstawia formalną analizę właściwości bezpieczeństwa sieci Lightning Network (LN) – powszechnie uznawanej za najważniejsze i sprawdzone w praktyce rozwiązanie skalujące warstwy 2 dla Bitcoina. W tym celu posłużono się uproszczonym modelem LN, ograniczając się do analizy pojedynczego dwupartyjnego kanału. Główny wynik dowodzi, że LN zawsze gwarantuje bezpieczeństwo środków należących do uczciwych użytkowników. Wynik ten osiągnięto za pomocą metody formalnej weryfikacji, która obejmowała: (1) opracowanie formalnej implementacji protokołu LN, (2) sformułowanie pożądanych celów bezpieczeństwa oraz (3) dostarczenie sprawdzalnego maszynowo dowodu na to, że cele te są spełnione w każdym scenariuszu. Omawiany w tej części system został zbudowany z wykorzystaniem Why3, platformy typu open source służącej do dedukcyjnej weryfikacji programów.

Autor uwzględnia dwa standardowe cele bezpieczeństwa: *funds security* (Definicja 4.3.1), zgodnie z którym każda ze stron może w dowolnym momencie zamknąć kanał i przenieść należne jej środki do głównego łańcucha bloków, oraz *liveness*, zgodnie z którym zasilenie kanału i realizacja płatności między dwiema uczciwymi stronami zawsze kończą się powodzeniem w określonym czasie. W rozprawie Autor dowodzi jedynie własności *funds security*. Ponieważ naruszenie tej własności wiąże się ze znacznie poważniejszymi konsekwencjami niż naruszenie własności *liveness*, przyjęte podejście stanowi uzasadniony kompromis między złożonością dowodu a praktycznym znaczeniem uzyskanego rezultatu.

Formalna weryfikacja protokołu LN była już przedmiotem wcześniejszych prac. W szczególności publikacja Grundmanna i Hartensteina (preprint arXiv 2023) zawiera wyniki bardzo zbliżone do tych przedstawionych w rozdziale 3. W pewnym stopniu ogranicza to nowatorski charakter rezultatów uzyskanych w tej części rozprawy.

Należy jednak podkreślić, że – jak omówiono w przedłożonej rozprawie – podejście Autora różni się pod kilkoma względami od podejścia przedstawionego w pracy Grundmanna i Hartensteina. W szczególności, w przeciwieństwie do systemu dowodzenia dedukcyjnego Why3, zastosowanego przez Pana Fabiańskiego, który umożliwia formalne dowodzenie własności dla nieskończonej liczby stanów, metoda *model checking* w języku TLA+, wykorzystana przez Grundmanna i Hartensteina, wymaga

ograniczenia analizowanego systemu do skończonej liczby akcji, aby uniknąć eksplozji przestrzeni stanów.

W rozdziale 5 przedstawiono formalnie zweryfikowane w języku Lean 4 środowisko służące do przekształcania symbolicznych dowodów bezpieczeństwa protokołów kryptograficznych w dowody ich bezpieczeństwa w modelu obliczeniowym. Zaproponowane rozwiązanie łączy dwa komplementarne podejścia: podejście symboliczne, które umożliwia stosunkowo prostą formalną specyfikację i weryfikację w modelu Dolev-Yao, lecz abstrahuje od pełnych możliwości realistycznego przeciwnika, oraz podejście obliczeniowe, zapewniające gwarancje bezpieczeństwa wobec realistycznych przeciwników, ale wymagające znacznie bardziej złożonych dowodów i ich formalizacji. Istotnym wkładem przedstawionego w dysertacji rozwiązania jest opracowanie i formalna weryfikacja przejścia pomiędzy tymi dwoma podejściami. Działanie zaproponowanego środowiska zilustrowano na przykładzie techniki *Garbled Circuits*, odgrywającej kluczową rolę w realizacji bezpiecznych obliczeń wielopartyjnych.

Zaproponowane podejście opiera się na pracy Micciancio (EUROCRYPT 2010), w której przedstawiono wykorzystanie ko-indukcji (zamiast indukcji) do symbolicznego wnioskowania o wiedzy przeciwnika w sposób ściśle powiązany z kryptografią obliczeniową. Na tej podstawie autor formalizuje w języku Lean 4 wyrażenia symboliczne reprezentujące wiadomości w transkryptach protokołów oraz przeprowadza dowód twierdzenia o poprawności (*Computational Soundness Theorem*), zgodnie z którym spełnienie symbolicznych gwarancji bezpieczeństwa implikuje bezpieczeństwo obliczeniowe. Mówiąc dokładniej, twierdzenie to stwierdza, że wyrażeniom nie-rozróżnialnym symbolicznie odpowiadają rozkłady nierozróżnialne obliczeniowo, przy założeniu, że bazowy schemat szyfrowania jest bezpieczny w sensie IND-CPA. Formalne sformułowanie twierdzenia oraz jego dowód przedstawiono w języku Lean 4.

Wynik ten stanowi nietrywialne rozwinięcie podejścia zapoczątkowanego przez Abadiego i Rogawaya. Dzięki wykorzystaniu obliczeniowo poprawnej analizy symbolicznej rozwiązanie to łączy zalety obu podejść: stosunkowo proste dowody nierozróżnialności oparte na operacjach symbolicznych oraz silne gwarancje bezpieczeństwa wobec przeciwników dysponujących realistycznymi możliwościami obliczeniowymi.

Jako przykład niestandardowego zastosowania proponowanego podejścia autor formalizuje symboliczny dowód bezpieczeństwa procedury implementującej technikę *Garbled Circuits*. W połączeniu z twierdzeniem o poprawności obliczeniowej pozwala to uzyskać zmechanizowany w Lean 4 dowód bezpieczeństwa tej techniki w modelu obliczeniowym, uzyskany poprzez formalnie zweryfikowane przejście od dowodu symbolicznego do bezpieczeństwa obliczeniowego. Istotnym aspektem tego wyniku nie jest samo zmechanizowanie dowodu bezpieczeństwa techniki *Garbled Circuits*, które było przedmiotem wcześniejszych prac, lecz wykorzystanie go jako przykładu zastosowania formalnie zweryfikowanego w Lean 4 przejścia od bezpieczeństwa symbolicznego do bezpieczeństwa obliczeniowego.

Rozprawa jest napisana w sposób czytelny i poprawny językowo, a przedstawiony materiał został opracowany precyzyjnie. Rozdziały 1. i 2. zawierają uwagi wstępne oraz podsumowanie uzyskanych wyników. W rozdziale 3. opisano protokół Plasma oraz

przedstawiono główny wynik wraz z klasycznym dowodem matematycznym, przeprowadzonym bez wykorzystania narzędzi metod formalnych, a także nakreślono motywację do prowadzenia badań w tej dziedzinie. Pewnym mankamentem prezentacji jest natomiast fakt, że w odniesieniu do niektórych szczegółów, takich jak specyfika opisu eksperymentu *Exp(V)*, czytelnik odsyłany jest do pełnej wersji materiału omawianego w tej części pracy. Rozdział 4, przedstawiający wyniki dotyczące formalnej weryfikacji protokołu LN, jest napisany w sposób bardzo techniczny, co w pewnym stopniu wynika z natury zastosowanego podejścia. Wydaje się, że wybór narzędzia Why3 do specyfikacji i weryfikacji jest trafny i należycie uzasadniony. Materiał zawarty w rozdziale 5, dotyczący formalizacji obliczeniowo bezpiecznej kryptografii symbolicznej w języku Lean 4, został przedstawiony w sposób niezwykle klarowny, interesujący i przystępny, również dla czytelników nieposiadających biegłej znajomości języka Lean 4.

Konkluzja

Podsumowując, rozprawa doktorska przedstawia interesujące i wartościowe wyniki dotyczące analizy protokołów blockchain oraz zastosowania metod formalnych w kryptografii. Uzyskane rezultaty pozwalają precyzyjnie wskazać ograniczenia popularnych rozwiązań służących skalowaniu sieci blockchain i stanowią cenny i oryginalny wkład zarówno w rozwój metod formalnych stosowanych w kryptografii, jak i w analizę bezpieczeństwa protokołów blockchain. Osiągnięcia te spotkały się z uznaniem środowiska naukowego, czego potwierdzeniem jest publikacja prac przedstawiających wyniki zawarte w rozdziałach 3, 4 i 5 na trzech wiodących konferencjach w tej dziedzinie: *Innovations in Theoretical Computer Science Conference* (ITCS, 2021), *Financial Cryptography and Data Security* (FC, 2025) oraz *Computer Security Foundations Symposium* (CSF, 2026). Przedłożona rozprawa potwierdza, że kandydat posiada ogólną wiedzę teoretyczną w zakresie kryptografii oraz umiejętność samodzielnego prowadzenia pracy naukowej w tej dziedzinie.

Oceniając bardzo pozytywnie wartość naukową przedłożonej rozprawy doktorskiej, stwierdzam, że w sposób wystarczający spełnia ona wszystkie kryteria stawiane rozprawom doktorskim określone w Ustawie z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2024 r. poz. 1571 z późn. zm.). Na tej podstawie wnioskuję o dopuszczenie mgra Grzegorza Fabiańskiego do dalszych etapów postępowania w sprawie nadania stopnia doktora w dziedzinie nauk ścisłych i przyrodniczych, w dyscyplinie informatyka.

Maciej Liśkiewicz