Propozycja Tematu Pracy Magisterskiej: Wykorzystanie zk-Proof do Nowej Metody Autentykacji

Filip Gumuła

8 lutego 2025

1 Wprowadzenie

Celem pracy magisterskiej jest opracowanie nowej metody autentykacji użytkowników w systemach informatycznych z wykorzystaniem zero-knowledge proofs (zk-Proof), w szczególności SNARK oraz języka Noir. Tradycyjne metody autentykacji, oparte na przesyłaniu haseł lub innych danych wrażliwych do serwera, są podatne na liczne zagrożenia, takie jak przechwytywanie, ataki typu phishing czy naruszenia danych. Niniejsza praca proponuje innowacyjne podejście, w którym użytkownik udowadnia swoją tożsamość za pomocą zk-Proof, bez konieczności ujawniania jakichkolwiek danych wrażliwych.

W ramach tej pracy szczególną uwagę poświęcono wykorzystaniu Noir jako języka do definiowania i generowania dowodów SNARK oraz jego integracji z Garaga do efektywnej weryfikacji proofów. Noir, jako dedykowane narzędzie dla zero-knowledge proofs, umożliwia wydajne oraz intuicyjne tworzenie systemów kryptograficznych, a jego kompatybilność z SNARK pozwala na skuteczne wdrożenie w praktycznych rozwiązaniach. Kluczowym celem jest zaprojektowanie oraz implementacja systemu autentykacji, który może być wykorzystywany w różnych środowiskach, takich jak zdecentralizowane aplikacje (dApps), systemy logowania bez hasła czy protokoły identyfikacji cyfrowej.

Podsumowując, praca ta koncentruje się na zastosowaniu SNARK w procesach autentykacji, przy jednoczesnym wykorzystaniu Noir do definiowania i generowania dowodów zk. Efektem końcowym będzie działający prototyp, który umożliwi użytkownikom bezpieczne uwierzytelnianie bez konieczności przesyłania haseł

2 Teoretyczne Podstawy zk-Proof

2.1 Wprowadzenie do kryptografii

Kryptografia to dziedzina zajmująca się metodami zabezpieczania informacji poprzez ich matematyczne przekształcenie. Jej celem jest uniemożliwienie dostępu do danych osobom nieuprawnionym, przy jednoczesnym zachowaniu ich dostępności dla osób posiadających odpowiednie uprawnienia. Początki kryptografii sięgają starożytności, kiedy stosowano podstawowe techniki szyfrowania oparte na zamianie lub przestawieniu znaków.

Współczesna kryptografia obejmuje szeroki zakres zagadnień, w tym szyfrowanie symetryczne i asymetryczne, funkcje skrótu oraz techniki bardziej zaawansowane, jak dowody wiedzy zerowej (Zero-Knowledge Proofs, zk-Proofs). Stosuje się ją nie tylko do ochrony poufnych danych, ale także do zapewnienia integralności i autentyczności informacji, co jest kluczowe w dzisiejszym cyfrowym świecie.

2.1.1 Kluczowe zasady kryptografii

Kryptografia opiera się na kilku podstawowych zasadach, które zapewniają bezpieczeństwo informacji:

- **Poufność (Confidentiality)** – tylko uprawnione osoby mogą odczytać zaszyfrowane dane.
- **Integralność (Integrity)** – zapewnia, że dane nie zostały zmienione lub sfałszowane w trakcie transmisji.
- **Autentyczność (Authenticity)** – pozwala zweryfikować, czy nadawca wiadomości jest tym, za kogo się podaje.
- **Niezaprzeczalność (Non-repudiation)** – zapobiega zaprzeczeniu przez nadawcę, że wysłał określoną wiadomość.

2.1.2 Historia kryptografii

Rozwój kryptografii można podzielić na kilka głównych etapów:

- **Kryptografia klasyczna** – obejmuje metody stosowane od starożytności do XX wieku. Przykładem jest szyfr Cezara, który polegał na przesunięciu każdej litery w alfabecie o ustaloną liczbę miejsc.
- **Kryptografia mechaniczna** – w XX wieku rozwinięto bardziej skomplikowane systemy szyfrowania, np. Enigmę, maszynę wirnikową używaną przez armię niemiecką w czasie II wojny światowej.
- **Kryptografia współczesna** – obecnie opiera się na zaawansowanych metodach matematycznych i obliczeniowych, w tym szyfrowaniu asymetrycznym oraz kryptografii postkwantowej.

2.1.3 Kluczowe pojęcia w kryptografii

Szyfrowanie i deszyfrowanie Szyfrowanie to proces przekształcania informacji w sposób, który czyni ją nieczytelną bez odpowiedniego klucza. Deszyfrowanie jest odwrotnym procesem, umożliwiającym odzyskanie oryginalnej treści.

Istnieją dwa główne typy szyfrowania:

- **Szyfrowanie symetryczne** – ten sam klucz służy zarówno do szyfrowania, jak i deszyfrowania (np. algorytm AES).
- **Szyfrowanie asymetryczne** – wykorzystuje parę kluczy: publiczny (do szyfrowania) i prywatny (do deszyfrowania). Przykładem jest algorytm RSA.

Funkcje skrótu Funkcje skrótu (np. SHA-256) przekształcają dowolne dane wejściowe w ciąg znaków o ustalonej długości, w sposób, który jest jednokierunkowy – tzn. nie da się łatwo odzyskać oryginalnej wartości na podstawie skrótu. Są one szeroko stosowane w kryptografii, np. do weryfikacji integralności danych.

Funkcje skrótu znajdują także zastosowanie w strukturach danych takich jak **drzewa Merkle**. Drzewa Merkle to hierarchiczne struktury, w których każdy węzeł jest funkcją skrótu swoich potomków. Zapewniają one integralność i spójność dużych zbiorów danych, umożliwiając efektywną i bezpieczną weryfikację poprawności danych w systemach rozproszonych, takich jak blockchain.

Zero-Knowledge Proofs (zk-Proofs) Jednym z bardziej zaawansowanych zastosowań kryptografii są dowody wiedzy zerowej. Pozwalają one jednej stronie (proverowi) wykazać, że posiada pewną informację, bez konieczności jej ujawniania. Technika ta znajduje zastosowanie m.in. w systemach prywatności blockchain i uwierzytelnianiu bez haseł.

2.1.4 Zastosowania kryptografii

Kryptografia znajduje zastosowanie w wielu dziedzinach technologii i bezpieczeństwa informacyjnego:

- **Bezpieczna komunikacja** – np. szyfrowanie transmisji internetowej za pomocą protokołów takich jak TLS/SSL (HTTPS).
- **Podpisy cyfrowe** – stosowane do zapewnienia autentyczności dokumentów elektronicznych.
- **Zabezpieczenia w bankowości** – np. w systemach 3D Secure oraz EMV chipach kart płatniczych.
- **Kryptografia w blockchain** – np. wykorzystanie funkcji skrótu i dowodów zk-Proofs do zapewnienia prywatności transakcji.
- **Kryptografia postkwantowa** – rozwijana w celu ochrony danych przed atakami komputerów kwantowych.

2.2 Zero-Knowledge Proofs: definicje i właściwości

Dowody z wiedzą zerową (ang. *Zero-Knowledge Proofs*, ZKP) to protokoły kryptograficzne, które umożliwiają jednej stronie (nazywanej *dowodzącym*) przekonanie innej strony (nazywanej *weryfikatorem*) o prawdziwości pewnego twierdzenia, nie ujawniając przy tym żadnych dodatkowych informacji poza faktem, że twierdzenie to jest prawdziwe [3].

2.2.1 Formalne właściwości ZKP

Aby protokół mógł być uznany za dowód z wiedzą zerową, musi spełniać trzy kluczowe właściwości [2]:

- **Kompletność (ang. *Completeness*)** – jeśli twierdzenie jest prawdziwe, uczciwy weryfikator zostanie przekonany przez uczciwego dowodzącego.
- **Poprawność (ang. *Soundness*)** – jeśli twierdzenie jest fałszywe, żaden nieuczciwy dowodzący nie zdoła przekonać uczciwego weryfikatora o jego prawdziwości.
- **Wiedza zerowa (ang. *Zero-Knowledge*)** – weryfikator nie uzyskuje żadnych informacji poza faktem, że twierdzenie jest prawdziwe.

2.2.2 Intuicyjny przykład – Jaskinia Ali Baby

Jednym z najbardziej znanych przykładów ilustrujących działanie dowodów z wiedzą zerową jest tzw. *Jaskinia Ali Baby* [1]. W tym scenariuszu występują dwie postacie: Tina (weryfikator) oraz Sam (dowodzący).

Podczas wspólnej wyprawy odkrywają oni jaskinię, w której znajdują się dwa wejścia prowadzące do dwóch różnych ścieżek – A i B. Wewnątrz znajduje się ukryte przejście zamknięte

magicznymi drzwiami, które można otworzyć jedynie za pomocą tajnego hasła, znanego wyłącznie Samowi.

Celem eksperymentu jest przekonanie Tiny, że Sam faktycznie zna hasło otwierające drzwi, bez konieczności jego ujawniania. Aby tego dokonać, Sam wchodzi do jaskini, wybierając losową ścieżkę A lub B, natomiast Tina pozostaje na zewnątrz, nie wiedząc, którą drogą podążył. Następnie Tina losowo wskazuje, którą ścieżką Sam ma powrócić. Jeśli Sam wybrał ścieżkę A, ale Tina zażądała, aby wyszedł ścieżką B, jedynym sposobem na spełnienie tego warunku jest faktyczna znajomość hasła do drzwi.

Proces ten można powtórzyć wielokrotnie, aby zmniejszyć prawdopodobieństwo przypadkowego trafienia przez Sama na właściwą drogę. Po dostatecznej liczbie powtórzeń Tina nabiera wysokiego stopnia pewności, że Sam rzeczywiście zna hasło, nie mając jednak dostępu do samej jego treści. Ten mechanizm odzwierciedla sposób, w jaki działają dowody z wiedzą zerową w kryptografii – umożliwiają one weryfikację prawdziwości twierdzenia bez ujawniania żadnych dodatkowych informacji poza faktem, że twierdzenie to jest prawdziwe [1].

Jak przykład spełnia trzy cechy ZKP? Przykład Jaskini Ali Baby doskonale ilustruje trzy podstawowe właściwości dowodów wiedzy zerowej:

- **Kompletność (ang. Completeness)** – Jeśli Sam rzeczywiście zna hasło do drzwi, zawsze będzie w stanie przejść z jednej ścieżki na drugą i spełnić wymaganie Tiny. Oznacza to, że uczciwy dowodzący (Sam) zawsze przekona uczciwego weryfikatora (Tinę).
- **Poprawność (ang. Soundness)** – Jeśli Sam nie zna hasła, nie jest w stanie przejść na drugą stronę i wrócić zgodnie z żądaniem Tiny. Teoretycznie może próbować zgadywać, ale szansa, że za każdym razem zgadnie poprawnie, maleje wykładniczo z każdym kolejnym powtórzeniem eksperymentu. Ostatecznie fałszywy dowodzący nie będzie w stanie oszukać weryfikatora.
- **Wiedza zerowa (ang. Zero-Knowledge)** – W trakcie całego procesu Tina nie zdobywa żadnej dodatkowej informacji poza faktem, że Sam rzeczywiście zna hasło. Sam nie ujawnia treści hasła ani żadnych wskazówek, które mogłyby pomóc Tinie je odtworzyć.

W rzeczywistych zastosowaniach kryptograficznych ZKP działa na podobnej zasadzie, wykorzystując obliczeniowe schematy dowodzenia wiedzy bez ujawniania samego sekretu. Systemy te bazują na funkcjach matematycznych i kryptograficznych obwodach logicznych, w których dowodzący może wykazać znajomość pewnych wartości bez ich bezpośredniego ujawnienia [2].

2.2.3 Rodzaje dowodów z wiedzą zerową

Dowody z wiedzą zerową dzielą się na dwa główne typy [2] [4]:

- **Interaktywne dowody z wiedzą zerową** – Interaktywne dowody wiedzy zerowej (iZKP) to protokoły kryptograficzne, w których dowodzący (prover) i weryfikator (verifier) prowadzą wymianę komunikatów, aby udowodnić znajomość pewnej informacji bez jej ujawniania. W trakcie tej interakcji weryfikator zadaje pytania, a dowodzący musi na nie odpowiedzieć, dostarczając dowód znajomości sekretnej wartości. Jednym z najczęściej stosowanych interaktywnych protokołów ZKP jest schemat Fiat-Shamira. Polega on na tym, że weryfikator generuje losową wartość, którą wysyła jako wyzwanie do dowodzącego. Dowodzący następnie musi użyć swojej sekretnej wiedzy, aby wygenerować odpowiednią odpowiedź, którą weryfikator może sprawdzić. Jeśli odpowiedź jest poprawna, weryfikator akceptuje dowód i interakcja zostaje zakończona.

- **Nieinteraktywne dowody z wiedzą zerową (NIZK)** – Nieinteraktywne dowody wiedzy zerowej (niZKP) to protokoły, które nie wymagają interakcji pomiędzy dowodzącym a weryfikatorem. Zamiast tego, dowodzący generuje pojedynczy dowód, który może być zweryfikowany przez weryfikatora w dowolnym czasie, bez potrzeby dodatkowej komunikacji. Jednym z najczęściej stosowanych nieinteraktywnych protokołów ZKP jest SNARK (Succinct Non-Interactive Argument of Knowledge). SNARK wykorzystuje zaawansowane algorytmy matematyczne, aby wygenerować krótki, skondensowany dowód, który może być łatwo i szybko zweryfikowany.

2.2.4 Zaufany Setup [5]

Zaufany setup (ang. Trusted Setup) to proces inicjalizacyjny, w którym generowane są klucze kryptograficzne używane w niektórych systemach dowodów zerowej wiedzy (ZKP). Kluczowym celem tego procesu jest wygenerowanie zestawu parametrów, które umożliwią późniejsze tworzenie i weryfikację dowodów. Niektóre rodzaje ZKP, np. SNARKs, wymagają specjalnych parametrów kryptograficznych do tworzenia dowodów. Jeśli osoba lub organizacja, która generuje te parametry, zachowa ich pełną wersję, mogłaby stworzyć fałszywe dowody. Z tego powodu ważne jest, aby proces generowania kluczy był przeprowadzony w sposób bezpieczny i transparentny.

Jak działa Trusted Setup?

1. Wybór generatora – Proces zaczyna się od wyboru publicznych wartości matematycznych, takich jak generator grupy kryptograficznej.
2. Obliczanie parametrów – Tworzony jest zestaw parametrów publicznych oraz tajnych wartości, które umożliwiają generowanie dowodów.
3. Zniszczenie wartości tajnych – Aby system był bezpieczny, wartości tajne muszą zostać bezpowrotnie usunięte.

Jeśli osoba lub grupa, która przeprowadziła Trusted Setup, nie zniszczy tajnych wartości, mogłaby w przyszłości wygenerować fałszywe dowody, które wyglądałyby jak prawdziwe. To stanowi zagrożenie dla bezpieczeństwa systemu.

Jak można uniknąć problemu Trusted Setup?

- Multi-Party Computation (MPC) – zamiast jednej osoby, setup przeprowadza wiele niezależnych uczestników, a każdy generuje tylko część parametrów. Jeśli choć jedna osoba jest uczciwa, system pozostaje bezpieczny.
- Zk-STARKs zamiast zk-SNARKs – STARKs eliminują potrzebę Trusted Setup, wykorzystując inne mechanizmy matematyczne, np. funkcje mieszające zamiast krzywych eliptycznych.

Istnieje wiele implementacji dowodów z wiedzą zerową, z których każda ma swoje unikalne cechy, wady i zalety. Różnią się one m.in. rozmiarem dowodu, czasem generowania dowodu, czasem weryfikacji oraz wymaganym poziomem interakcji [2]. Do najważniejszych należą:

- **zk-SNARKs** (ang. *Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge*) – dowody, które są niewielkich rozmiarów i łatwe do weryfikacji. Generują kryptograficzny dowód przy użyciu krzywych eliptycznych, co jest bardziej efektywne pod względem zużycia gazu w porównaniu do metod opartych na funkcjach haszujących stosowanych w STARKs. Są wykorzystywane m.in. w kryptowalutach zapewniających prywatność, takich jak Zcash.

- **zk-STARKs** (ang. *Zero-Knowledge Scalable Transparent Arguments of Knowledge*) – eliminują potrzebę zaufanego setupu i są odporne na ataki kwantowe. STARKs wymagają minimalnej interakcji między dowodzącym a weryfikatorem, co czyni je szybszymi niż SNARKs. Dzięki temu są stosowane w skalowalnych rozwiązaniach dla blockchain, takich jak StarkNet.
- **PLONK** (ang. *Permutations over Lagrange-bases for Oecumenical Noninteractive arguments of Knowledge*) – wykorzystuje uniwersalny zaufany setup, który może być używany z dowolnym programem i obsługiwać dużą liczbę uczestników. PLONK jest bardziej elastyczny niż SNARKs, a jego popularność rośnie w systemach zk-rollups.
- **Bulletproofs** – krótkie, nieinteraktywne dowody zerowej wiedzy, które nie wymagają zaufanego setupu. Zostały zaprojektowane w celu umożliwienia prywatnych transakcji w kryptowalutach. Wykorzystywane są m.in. w Monero do ukrywania wartości transakcji.

Technologie te znajdują zastosowanie w wielu projektach zero-knowledge, takich jak StarkNet, ZKsync czy Loopring, które wdrażają rozwiązania zapewniające skalowalność i prywatność w blockchain [2].

Dowody z wiedzą zerową mają szerokie zastosowanie w różnych obszarach kryptografii:

- **Blockchain i kryptowaluty** – prywatne transakcje w Zcash (zk-SNARKs) oraz optymalizacja Layer 2 w Ethereum (zk-Rollups).
- **Uwierzytelnianie bez haseł** – systemy takie jak FIDO2 mogą korzystać z ZKP do zapewnienia tożsamości użytkownika bez ujawniania haseł.
- **Bezpieczne głosowanie elektroniczne** – systemy e-voting mogą wykorzystywać ZKP do weryfikacji głosów bez ujawniania ich treści.

2.3 Rozdział 3: Projekt Systemu Autentykacji

- Wymagania systemowe
- Architektura systemu
- Wybór algorytmów kryptograficznych: Pedersen/Poseidon
- Mechanizm challenge-response

2.4 Rozdział 4: Implementacja

- Środowisko programistyczne i narzędzia
- Implementacja po stronie przeglądarki: obliczanie hash i generowanie zk-Proof
- Implementacja po stronie serwera: weryfikacja zk-Proof
- Integracja z istniejącymi systemami autentykacji

2.5 Rozdział 5: Testowanie i Walidacja

- Scenariusze testowe
- Bezpieczeństwo systemu
- Wydajność i skalowalność
- Porównanie z tradycyjnymi metodami autentykacji

2.6 Rozdział 6: Dyskusja

- Zalety i wady proponowanego rozwiązania
- Możliwości dalszego rozwoju
- Potencjalne zagrożenia i sposoby ich mitigacji

2.7 Rozdział 7: Podsumowanie

- Wnioski
- Osiągnięcia pracy
- Przyszłe kierunki badań

Literatura

[1] 101 Blockchains. Zero-knowledge proof example – the ali baba cave, 2023. Dostęp: 01-02-2025.

[2] Chainlink. Zero-knowledge proof (zkp) — explained, 2023. Dostęp: 01-02-2025.

[3] Marcin Karbowski. *Podstawy kryptografii*. Helion, 2015.

[4] NFTing. Zero-knowledge proof: Interactive vs. non-interactive, 2023. Dostęp: 01-02-2025.

[5] Panther Team. Understanding trusted setups: A guide, 2022. Dostęp: 01-02-2025.