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

Filip Gumuła

January 27, 2025

Celem pracy magisterskiej jest opracowanie nowej metody autentykacji użytkowników w systemach informatycznych z wykorzystaniem zero-knowledge proofs (zk-Proof), w szczególności algorytmu STARK. Tradycyjne metody autentykacji, oparte na przesyłaniu hasła na serwer, są podatne na różnorodne ataki. Praca ta proponuje innowacyjne podejście, w którym użytkownik udowadnia znajomość swojego hasła bez konieczności przesyłania go wprost.

W ramach tej pracy, szczególną uwagę poświęcono Stwo Proverowi, który jest szybkim, otwartoźródłowym proverem, który implementuje przełomowy protokół Circle STARK. Dzięki temu, Stwo odblokowuje pełny potencjał wysoce efektywnego liczby pierwszej Mersenne'a M31, przynosząc korzyści w przestrzeni zk-proof i blockchain. Kluczowe cechy Stwo Prover, takie jak Circle STARK, otwartoźródłowość, skalowalność i kompatybilność, są istotne dla opracowywanej metody autentykacji, oferując niezrównaną wydajność dowodzenia.

Podsumowując, Stwo Prover i jego wykorzystanie w kontekście zero-knowledge proofs stanowi kluczowy element tej pracy magisterskiej, oferując nową, bezpieczniejszą i bardziej efektywną metodę autentykacji użytkowników w systemach informatycznych.

1 Wstępny Plan Pracy

1.1 Rozdział 1: Wprowadzenie

2 Wprowadzenie

Współczesne systemy informatyczne odgrywają kluczową rolę w codziennym życiu, umożliwiając szybki dostęp do usług finansowych, platform społecznościowych oraz innych aplikacji o krytycznym znaczeniu. Wraz z rosnącą zależnością od technologii, pojawia się także coraz większe zapotrzebowanie na bezpieczne i wydajne metody autentykacji użytkowników. Tradycyjne podejścia, oparte na przesyłaniu hasła do serwera, choć szeroko stosowane, niosą ze sobą szereg ryzyk, takich jak przechwytywanie danych czy ich kradzież.

Celem niniejszej pracy jest opracowanie nowoczesnej metody autentykacji użytkowników z wykorzystaniem koncepcji *zero-knowledge proofs* (zk-Proof), w szczególności algorytmu STARK. Zero-knowledge proofs to zaawansowana technika kryptograficzna, która pozwala na udowodnienie prawdziwości pewnych informacji bez konieczności ich ujawniania. W kontekście autentykacji użytkowników oznacza to możliwość potwierdzenia tożsamości bez przesyłania danych wrażliwych, takich jak hasła.

W pracy szczególny nacisk położono na wykorzystanie narzędzia *Stwo Prover*, które implementuje protokół Circle STARK. Rozwiązanie to charakteryzuje się wysoką wydajnością,

skalowalnością oraz otwartoźródłowym charakterem, co czyni je atrakcyjnym wyborem do zastosowań praktycznych. Dzięki innowacyjnym funkcjom, takim jak wykorzystanie liczby pierwszej Mersenne'a M31, Stwo Prover oferuje nowe możliwości w przestrzeni zk-Proof, blockchain i autentykacji.

Rozdział ten stanowi wprowadzenie do problematyki pracy, omawia jej główne cele oraz znaczenie praktyczne. W kolejnych częściach pracy szczegółowo omówione zostaną teoretyczne podstawy kryptografii zk-Proof, projekt systemu autentykacji, implementacja proponowanego rozwiązania oraz jego testowanie i walidacja. Ostatecznie praca ta ma na celu przedstawienie efektywnego i bezpiecznego podejścia do autentykacji użytkowników, które może znaleźć zastosowanie w wielu różnych dziedzinach.

2.1 Rozdział 2: Teoretyczne Podstawy zk-Proof

- Wprowadzenie do kryptografii
- Zero-Knowledge Proofs: definicje i właściwości
- Algorytm STARK: zasady działania
- Stwo Prover: opis i właściwości
- Przegląd istniejących rozwiązań i ich ograniczenia

2.2 Rozdział 3: Projekt Systemu Autentykacji

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

2.3 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

2.4 Rozdział 5: Testowanie i Walidacja

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

2.5 Rozdział 6: Dyskusja

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

2.6 Rozdział 7: Podsumowanie

- Wnioski
- Osiągnięcia pracy
- Przyszłe kierunki badań

Bibliografia

Załączniki

Opis Wybranych Narzędzi i Bibliotek:

- STEW
- Cartridge Oasis
- Stone Prover
- State Channel Framework
- Rust Programming Language
- WebAssembly
- Yew Framework