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

Filip Gumuła

June 21, 2024

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

- Cel pracy
- Zakres pracy
- Struktura pracy

1.2 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

1.3 Rozdział 3: Projekt Systemu Autentykacji

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

1.4 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

1.5 Rozdział 5: Testowanie i Walidacja

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

1.6 Rozdział 6: Dyskusja

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

1.7 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