OPIS OBSZARU BADAWCZEGO W RAMACH KONKURSU IDUB 078

Dowody z wiedzą zerową

Jędrzej Garnek, specjalność cyberbezpieczeństwo

1. Charakterystyka obszaru badawczego

   Naukowo zajmuję się geometrią arytmetyczną, czyli dziedziną badającą rozwiązania równań wielomianowych za pomocą metod teorii liczb. Interesują mnie przede wszystkim takie obiekty jak krzywe i rozmaitości abelowe. Są to kluczowe obiekty z punktu widzenia współczesnej kryptografii (także postkwantowej) i są stosowane m.in. do uzgadniania kluczy, cyfrowych podpisów i generatorów pseudolosowych. Proponowany przeze mnie projekt badawczy dotyczy jednak bardziej arytmetycznych protokołów kryptograficznych, typu SNARK (ang. Succinct Non-interactive Argument of Knowledge), związanych z dowodami z wiedzą zerową. Dowody z wiedzą zerową pozwalają jednej stronie udowodnić drugiej, że zna pewne informacje, nie ujawniając jednak żadnych szczegółów na ich temat. SNARKi są szybkie do sprawdzenia („succint”), oraz "nieinteraktywne", co oznacza, że dowód może być przesłany jako pojedyncza wiadomość od nadawcy do odbiorcy, bez potrzeby dalszej komunikacji.
2. Motywacja

   Tematyka ta jest zaawansowanym i aktywnie badanym obszarem kryptografii. SNARKi znajdują zastosowanie w wielu dziedzinach, w tym w blockchainach i kryptowalutach, gdzie są używane do tworzenia efektywnych i prywatnych transakcji. Ponadto z tematyką SNARKów związane są rozmaite ciekawe problemy na pograniczu algebry oraz teorii liczb. Niektóre z najnowszych protokołów wykorzystują metody geometrii algebraicznej.

3. Obecny poziom badań i możliwości finansowania

   Jestem autorem kilku publikacji dotyczących problemów z dziedziny teorii liczb, algebry, geometrii algebraicznej. Nie dotyczą one stricte kryptografii, jednak moje umiejętności i doświadczenie w tych obszarach mogą być wartościowym wkładem w rozwój nowych metod, szczególnie tych pochodzących z geometrii algebraicznej. Badania te byłyby realizowane w ramach moich badań własnych. Potencjalne źródła finansowania: Study@Research.
4. Tematyka badawcza

   - Optymalizacja i implementacja istniejących protokołów typu SNARK: Badanie sposobów na poprawę wydajności SNARKów, zarówno pod względem rozmiaru dowodu, jak i czasu weryfikacji, jest kluczowe dla ich praktycznego zastosowania.
   - Bezpieczeństwo SNARKów: badanie potencjalnych ataków na SNARKi i sposobów ich zapobiegania, w tym analiza różnych modeli zagrożeń. Opracowywanie technik obronnych.
5. Wymagania odnośnie członków projektu

- szacowana liczba studentów: 2
- wymagania wstępne: znajomość podstawowych pojęć algebry i teorii liczb, znajomość języka angielskiego.

6. Literatura

[1] Thomas Chen, Hui Lu, Teeramet Kunpittaya, Alan Luo, A Review of zk-SNARKs, arXiv 2202.06877
[2] Hartwig Mayer, zk-SNARK explained: Basic Principles, skrypt dostępny pod tym linkiem
[3] Anca Nitulescu, zk-SNARKs: A Gentle Introduction, skrypt dostępny pod tym linkiem
[4] Edgar Gonzalez Fernandez, Guillermo Morales-Luna, and Feliu Sagols. "A zero-knowledge proof system with algebraic geometry techniques." Applied Sciences 10.2 (2020): 465.