Obliczenia weryfikowalne i dowody z wiedzą zerową

Maciej Grześkowiak, *specjalność cyberbezpieczeństwo*

1. **Charakterystyka problemu badawczego**. W wielu systemach dane wykorzystywane do raportowania, rozliczeń lub podejmowania decyzji są poufne (np. finansowe, biznesowe, przemysłowe, medyczne) albo objęte ograniczeniami dostępu. Jednocześnie rośnie potrzeba audytu i niezależnej weryfikacji poprawności wyników obliczeń wykonywanych na tych danych: statystyk, agregacji, klasyfikacji czy rozliczeń. Powstaje konflikt: jak sprawdzić, że wynik został wyliczony zgodnie z regułami, bez ujawniania danych wejściowych ani wrażliwych szczegółów procesu.

   Obszar badań dotyczy obliczeń weryfikowalnych (verifiable computation) oraz dowodów z wiedzą zerową (zero-knowledge proofs), które pozwalają wykazać poprawność obliczeń wobec weryfikatora, ujawniając jedynie kontrolowany zestaw informacji. W praktyce łączy się metody klasyczne (np. Σ-protokoły dla własności lokalnych) z systemami dowodów dla złożonych obliczeń (SNARK), co umożliwia skalowanie od prostych relacji do realistycznych raportów dla dużych zbiorów danych.

2. **Motywacja**. Motywacją są wymagania ochrony prywatności i poufności (prawne, kontraktowe, organizacyjne) oraz potrzeba budowy zaufania do raportów, rozliczeń i decyzji opartych o przetwarzanie danych. Podejścia VC/ZK mogą ograniczać zakres ujawnianych informacji, zwiększać wiarygodność wyników oraz redukować ryzyko manipulacji, błędów i sporów. Zastosowania obejmują m.in. audyt zewnętrzny, raportowanie zgodności, usługi chmurowe i systemy rozproszone.

3. **Planowane metody badawcze**

   - Analiza literatury i przegląd rozwiązań z obszaru obliczeń weryfikowalnych oraz dowodów ZK.
   - Projekt scenariuszy audytu: co jest publiczne/prywatne, kto generuje dowód i kto weryfikuje, oraz model zagrożeń.
   - Projekt mechanizmów integralności i zobowiązania do wyników (np. zobowiązania kryptograficzne, wersjonowanie).
   - Implementacja prototypów i ewaluacja kosztów: czas generacji i weryfikacji, rozmiar dowodu, ograniczenia wdrożeniowe.

4. **Tematy i opis projektów**

   - Prywatne raportowanie: publikacja statystyk z dowodem poprawności bez ujawniania danych medycznych pacjentów.
   - Audyt spójności: weryfikacja zgodności raportów dziennych i miesięcznych oraz ich oparcia o te same dane.

5. **Wymagania odnośnie członków projektu** Wymagana jest dobra samoorganizacja, gotowość do pracy zespołowej, podstawy matematyki dyskretnej i bezpieczeństwa informacji oraz umiejętność programowania i tworzenia prototypów. Wskazane (ale niekonieczne) jest wcześniejsze doświadczenie z narzędziami kryptograficznymi i projektowaniem API.

[1] J. Groth, *On the Size of Pairing-based Non-interactive Arguments*, 2016.

[2] S. Goldwasser, S. Micali, C. Rackoff, *The Knowledge Complexity of Interactive Proof Systems*, 1989.