Dowody z wiedzą zerową (Zero-knowledge proofs)

Jolanta Marzec-Ballesteros, specjalność cyberbezpieczeństwo

1. Charakterystyka obszaru badawczego

   Dowody z wiedzą zerową to metody, które służą weryfikowaniu czy dana osoba posiada pewną informację bez jej ujawnienia. Co więcej, wymaga się by danych uzyskanych przy takiej weryfikacji nie można było wykorzystać w celu przekonania osoby trzeciej o posiadaniu owej informacji. W zależności od rodzaju informacji i zastosowania wykorzystuje się różne techniki matematyczno-informatyczne: arytmetykę modularną, podpisy cyfrowe, dzielenie sekretów i in. Jednym z problemów jest sama konstrukcja dowodu z wiedzą zerową dla danego typu informacji.

   Ze względu na to, że dowody z wiedzą zerową często stanowią jeden ze składników protokołów kryptograficznych, ich znajomość jest nieodzowna dla przyszłego absolwenta cyberbezpieczeństwa.

2. Motywacja

   Dowody z wiedzą zerową mają zastosowanie w różnych obszarach; między innymi przy uwierzytelnianiu (np. na potrzeby głosowania, dostępu do bazy danych, itp.); w sieciach blockchain; do zapewnienia, że pracownik postępuje uczciwie i wg ustalonych procedur; w protokole wykorzystywanym przez kryptowalutę Firo. Z tego względu rozważa się wielorakie scenariusze: gdy zachodzi interakcja pomiędzy osobą weryfikowaną i osobami weryfikującymi bądź nie; a jeśli tak, to - gdy część osób ze sobą współpracuje i działa nieuczciwie – kiedy można zagwarantować prawdomówność osoby weryfikowanej? czy można wykryć osoby nieuczciwe? Jaka jest złożoność obliczeniowa danego procesu weryfikacji i czy można ją poprawić? Które metody będzie można stosować w dobie komputerów kwantowych?

3. Obecny poziom badań

   Artykuł [2] z 2022 roku w zwięzły sposób opisuje dynamiczną historię dowodów z wiedzą zerową. Pojawiają się tam częściowe odpowiedzi na niektóre z wyżej postawionych pytań oraz możliwe naturalne kierunki dalszej pracy naukowej.

4. Tematyka badawcza

   Tematyka badawcza będzie dostosowana do zainteresowań studenta. Może to być np. porównanie różnych dowodów z wiedzą zerową lub dokładne opisanie protokołu w którym wybrany typ dowodu się pojawia. Mile widziana będzie implementacja wybranych narzędzi.

5. Wymagania odnośnie członków projektu

   Kandydaci powinni mieć podstawową wiedzę z zakresu algebry, teorii liczb i kryptografii.

6. Literatura

[1] Nigel P. Smart, *Cryptography Made Simple*, Springer, 2016.
Dostępne online: https://mog.dog/files/SP2019/Cryptography%20Made%20Simple.pdf

[2] Carsten Baum et al., *Feta: Efficient Threshold Designated-Verifier Zero-Knowledge Proofs*. W: Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS '22), November 7–11, 2022, Los Angeles, CA, USA. ACM, New York, NY, USA.
Dostępne online: https://cosicdatabase.esat.kuleuven.be/backend/publications/files/conferencepaper/3470

[3] Jean-Jacques Quisquater, Louis C. Guillou, Thomas A. Berson, *How to Explain Zero-Knowledge Protocols to Your Children*. W: G. Brassard (ed.), Advances in cryptology - CRYPTO `89: Proceedings, Lecture notes in computer science, nr 435, Springer, 1990.
Dostępne online: https://pages.cs.wisc.edu/~mkowalcz/628.pdf