OPIS OBSZARU BADAWCZEGO W RAMACH KONKURSU IDUB 078

Secure multi-party computation

Maciej Grześkowiak, specjalność cyberbezpieczeństwo

1. Charakterystyka obszaru badawczego

   Grupa n osób użytkuje pewien system informatyczny. Załóżmy, że każdy użytkownik u_i posiada swój tajny sekret $x_i \in \{0,1\}^k$ oraz, że wszystkim z nich znana jest ustalona funkcja $f : \{0,1\}^{nk} \to \{0,1\}^m$. Rozważmy taki protokół kryptograficzny, w którym po jego zakończeniu każdemu użytkownikowi sytemu wartość $f(x_1, \ldots, x_n)$ będzie znana i jednocześnie osoby u_i nie uzyskały żadnych informacji o sekretach x_j, dla $j \neq i$, poza tym co można wywnioskować z wartości funkcji f. Protokół powinien również działać bez udziału trzeciej strony, której musieliby zaufać wszyscy użytkownicy systemu. Protokoły, które spełniają powyższe warunki należą do szerokiej klasy konstrukcji kryptograficznych zwanych *secure multi-party computation.*

2. Motywacja

   Okazuje się, że z punktu widzenia metodologii dotyczącej projektowania bezpiecznych protokołów kryptograficznych wiele konstrukcji można sprowadzić do przypadku *secure multi-party computation.* Dla przykładu, w protokole identyfikacji wymagamy, aby użytkownik A, który posiada sekret x oraz publiczną funkcję $f(x)$, przekonał stronę B o tym, że zna x bez ujawniania żadnych informacji o sekrecie x. W podobny sposób możemy sformalizować inne protokoły np.: schemat uzgadniania wspólnego sekretu na otwartym kanale, który jest odporny przed podsłuchującym adwersarzem, protokół anonimowego dostępu do bazy danych, bezpieczne i uczciwe konstrukcje prywatnych aukcji internetowych, czy protokoły anonimowych wyborów elektronicznych. Wnikliwe poznanie zagadnień związanych *secure multi-party computation* będzie z pewnością wielkim atutem przyszłego absolwenta cyberbezpieczeństwa.

3. Obecny poziom badań

   Dynamiczny rozwój wielu współczesnych technologii informatycznych takich, jak: sztuczna inteligencja, blockchain, technologie kwantowe, powoduje potrzebę rewizji i udoskonalenia istniejących protokołów kryptograficznych, w tym opartych na *secure multi-party computation* oraz odkrywa szeroki horyzont do znajdowania nowych zastosowań kryptografii we współczesnym świecie technologii informatycznych.

4. Tematyka badawcza

   Proponowana tematyka badawcza obejmuje obliczenia na zaszyfrowanych obwodach logicznych (*garbled circuits*), protokoły z rodziny *oblivious transfer* oraz *proof of knowledge.*

5. Wymagania odnośnie członków projektu

   Kandydaci powinni mieć ukończony kurs elementów algebry i teorii liczb oraz posiadać umiejętność programowania.

6. Literatura

1. Sophia Yakoubov, A Gentle Introduction to Yao's Garbled Circuits `https://web.mit.edu/sonka89/www/papers/2017ygc.pdf`

2. Moni Naor, Benny Pinkas, Effcient oblivious transfer protocols, SODA '01, Proceedings of the twelfth annual ACM-SIAM symposium on Discrete algorithms, 448–457, 2001.