

## OFERTA PRACY

**Nazwa stanowiska:** magistrant

**Dziedzina:** informatyka

**Sposób wynagradzania (wynagrodzenie w ramach umowy o pracę/stypendium):** stypendium

**Liczba ofert pracy:** 4

**Kwota wynagrodzenia/stypendium:** 2.500 PLN netto

**Data rozpoczęcia pracy:** 1 grudnia 2019

**Okres zatrudnienia:** 6 miesięcy

**Instytucja (zakład/instytut/wydział/uczelnia/instytucja, miasto):** Wydział Matematyki, Informatyki i Mechaniki, Uniwersytet Warszawski

**Imię i nazwisko laureata kierującego projektem:** Stefan Dziembowski

**Tytuł projektu:** Kryptograficzne metody obrony przed nieuczciwymi producentami sprzętu elektronicznego

**Opis projektu:** Celem projektu jest stworzenie mechanizmów obrony przed zagrożeniami wynikającymi z outsourcingu produkcji układów scalonych. Zlecenie wytwarzania sprzętu elektronicznego firmom zewnętrznym jest obecnie bardzo częsta praktyką, a typowymi wykonawcami tych zleceń są firmy umiejscowione za granicą (głównie w Chinach i na Tajwanie). Jest to bardzo niepokojące, zwłaszcza, jeśli wziąć pod uwagę ogromne uzależnienie współczesnego społeczeństwa od urządzeń elektronicznych oraz ich obecność w bardzo dużej liczbie urządzeń otaczających człowieka.

Ze względu na złożoność tych układów sprawdzenie czy zewnętrzny producent wytworzył je prawidłowo jest z reguły bardzo trudne. Dlatego nieuczciwy producent może zmienić działanie urządzenia, poprzez wprowadzenie do niego złośliwych modyfikacji, nazywanych sprzętowymi końmi trojańskim. Tak zmodyfikowane urządzenie może spowodować znaczne szkody dla jego użytkowników poprzez nieprawidłowe działanie lub kradzież prywatnych danych. Innym zagrożeniem powiązaniem ze zjawiskiem outsourcingu produkcji sprzętu elektronicznego jest kradzież własności intelektualnej i piractwo.

Przeciwdziałanie zagrożeniom związanym z outsourcingiem produkcji układów scalonych jest od kilku lat intensywnym tematem badań w środowisku naukowym zajmującym się bezpieczeństwem sprzętowym. Z reguły w pracach z tej tematyki nie były stosowane zaawansowane metody kryptograficzne. W naszym projekcie spojrzymy na ten problem z punktu widzenia kryptograficznego. Inaczej mówiąc, zaproponujemy rozwiązania używające najnowszych technik kryptograficznych, oraz zastosujemy metodologię stosowaną w kryptografii w celu analizy własności zaproponowanych rozwiązań.

### Zadania:

1. Prowadzenie prac naukowych w tematyce projektu.
2. Spisywanie uzyskanych wyników oraz ich prezentacja na seminariach i konferencjach naukowych.
3. Współpraca z innymi członkami zespołu oraz z partnerami zagranicznymi

### Oczekiwania wobec kandydatów:

1. Dobra znajomość matematyki oraz informatyki teoretycznej.
2. Znajomość języka angielskiego.
3. Entuzjazm do prowadzenia badań podstawowych w informatyce.

### Lista wymaganych dokumentów

1. Życiorys
2. Lista ocen ze studiów licencjackich i magisterskich

**Dodatkowe informacje o rekrutacji (np. strona www):** <http://www.crypto.edu.pl/positions/trojans-msc-position>

**Adres przesyłania zgłoszeń:** <https://goo.gl/forms/TABqfFvd7EL93x4c2>

**Termin nadsyłania zgłoszeń:** 15 listopada 2019

Prosimy o zamieszczenie następującej klauzuli:

„Wyrażam zgodę na przetwarzanie moich danych osobowych dla potrzeb niezbędnych do realizacji procesu rekrutacji zgodnie z Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych ( Dz. U. z 2016 r. poz. 922 z późn. zm.)”