UNIWERSYTET WARSZAWSKI

Biuro Prasowe

21.04.2020

PROF. STEFAN DZIEMBOWSKI LAUREATEM NAGRODY COPERNICUS

Modele zabezpieczania danych przed niepowołanym dostępem, matematyczne podstawy kryptowalut, kryptograficzne aspekty inteligentnych kontraktów i inne zagadnienia z zakresu kryptografii i bezpieczeństwa IT to obszary, wokół których koncentruje się wieloletnia współpraca prof. Stefana Dziembowskiego i prof. Sebastiana Fausta z Technische Universität Darmstadt. Za – będące jej efektem – wybitne zasługi naukowcy zostali wyróżnieni Nagrodą „Nicolaus Copernicus".

Prof. Stefan Dziembowski z Wydziału Matematyki, Informatyki i Mechaniki UW oraz prof. Sebastian Faust z Technische Universität Darmstadt prowadzą wspólne badania nad podstawami i zastosowaniami kryptografii oraz bezpieczeństwa IT. Znacząco wpłynęły one na systemy używane w świecie rzeczywistym. Prace współtworzone przez naukowców prezentowane są na licznych wiodących konferencjach, wśród których wymienić można np. Crypto, ACM CCS oraz IEEE Security and Privacy. Publikowane są również w czasopismach.

Jedna z ich wspólnych prac w 2014 roku zdobyła nagrodę Best Paper Award na konferencji Eurocrypt, zaliczanej do grona najbardziej prestiżowych corocznych tego rodzaju wydarzeń poświęconych kryptografii. Publikacja ta, zatytułowana „Unifying Leakage Models: from Probing Attacks to Noisy Leakage", znacząco przyczyniła się do ogólnego poznania metod obrony przed tzw. atakami typu „side-channel". Ataki te są uważane za jedne z największych zagrożeń dla praktycznych systemów bezpieczeństwa.

Ważny obszar ich współpracy naukowej dotyczy też technologii blockchain i kryptowalut. W szczególności zaproponowali oni pojęcie tzw. „dowodów przestrzeni" (ang. „proofs of space"), które oferują bardziej „ekologiczną" alternatywę dla wydobywania kryptowalut niż ta wykorzystywana w Bitcoinie. Przedstawiona przez badaczy technologia jest obecnie wdrażana w komercyjnych projektach blockchainowych. Prof. prof. Dziembowski i Faust stworzyli również system „Perun", który umożliwia wykonywanie aplikacji blockchainowych w czasie rzeczywistym. Oprócz opublikowania kilku znaczących prac na ten temat, pracują oni obecnie nad wdrożeniem tej technologii w postaci projektu typu open source zintegrowanego z istniejącymi platformami blockchainowymi.

Trwająca ponad 10 lat współpraca prof. prof. Dziembowskiego i Fausta zaowocowała wybitnymi zasługami dla rozwoju badań nad kryptografią i bezpieczeństwem danych. Naukowcy zostali wyróżnieni Polsko-Niemiecką Nagrodą „Nicolaus Copernicus", przyznawaną co dwa lata przez Fundację na rzecz Nauki Polskiej (FNP) oraz Deutsche Forschungsgemeinschaft (DFG). Współpraca profesorów finansowana jest m.in. przez FNP oraz prywatną Ethereum Foundation.

Podczas każdej z organizowanych od 2006 roku edycji konkursu wyróżnienie otrzymuje para naukowców: jeden z Polski, drugi z Niemiec. Jak głosi regulamin, „od nagrodzonych uczonych oczekuje się, by mieli szczególne zasługi dla współpracy niemiecko-polskiej, łącząc w sposób

Krakowskie Przedmieście 26/28, Pałac Kazimierzowski, pokój 11
tel.: 22 55 24 066
e-mail: media@uw.edu.pl

komplementarny różne doświadczenia, wiedzę i zasoby w celu wspólnego rozwiązywania problemów badawczych. Wyniki takiej współpracy powinny mieć potencjał, aby otwierać nowe perspektywy w swoich dziedzinach badawczych lub innych domenach nauki, oraz wnosić wyjątkowy wkład w rozwój obu narodów".

Wysokość nagrody wynosi 200 tys. euro – po 100 tys. euro dla każdego z laureatów. Środki te powinny zostać wykorzystane przez naukowców na rzecz dalszego rozwoju współpracy polsko-niemieckiej.

Prof. Stefan Dziembowski jest pracownikiem Instytutu Informatyki UW. Na Uniwersytecie pod jego kierownictwem działa zespół badaczy z WMIM, których prace dotyczą m.in. kryptograficznych aspektów cyfrowej waluty bitcoin. Badacz związany był z kilkoma zagranicznymi instytucjami naukowymi. Stopień doktora uzyskał na Uniwersytecie Aarhus w Danii. Następnie odbył staże podoktorskie na Politechnice Federalnej w Zurychu (ETH), w instytucie Włoskiej Narodowej Rady ds. Badań Naukowych w Pizie oraz na Uniwersytecie „Sapienza" w Rzymie. Jako pracownik tej uczelni w 2007 roku otrzymał „Starting Grant" ERC. Wkrótce realizację projektu badawczego pt. „Cryptography and no-trusted machines" przeniósł na Uniwersytet Warszawski. Jednocześnie stał się pierwszym na UW laureatem tej prestiżowej nagrody.

W marcu 2020 roku ERC wyróżniła naukowca po raz kolejny – przyznając mu tym razem „Advanced Grant" w wysokości ponad 2,4 mln euro na realizację projektu pt. „Smart-Contract Protocols: Theory for Applications" (PROCONTRA). Prof. Dziembowski jest też laureatem wielu innych grantów i stypendiów, w tym „Welcome" i „Team" FNP.

Prof. Sebastian Faust jest pracownikiem Technische Universität Darmstadt i szefem grupy kryptografii stosowanej. Po ukończeniu doktoratu na Katolickim Uniwersytecie w Leuven w Belgii odbył staż podoktorski na Uniwersytecie Aarhus w Danii, a potem na Politechnice Federalnej w Lozannie (EPFL) w Szwajcarii, na stypendium Marie Curie. Następnie wrócił do Niemiec na Uniwersytet Ruhry w Bochum, gdzie został zatrudniony jako adiunkt w ramach programu Emmy Noether Research finansowanego przez fundację DFG. Od 2017 roku jest profesorem zwyczajnym na Politechnice w Darmstadt. W swoich badaniach koncentruje się na kryptografii, technologii blockchain i bezpieczeństwie IT.