


[NIEUWS](#) | [AUTEURS](#) | [PARTNERS](#) | [DOSSIERS](#) | [AGENDA](#) | [VACATURES](#)

15-08-2019

CWI-onderzoeker ontwerpt bekroond algoritme voor cryptografie



Deel dit bericht



CWI-onderzoeker Benjamin Wesolowski heeft een nieuw ingrediënt ontwikkeld voor cryptografische loterijmachines en ontving hiervoor de Best Young Researcher Paper Award tijdens Eurocrypt 2019. Zijn resultaten kunnen worden gebruikt voor duurzamere blockchaintechnologie.

Het genereren van willekeurige getallen is een berucht gevoelig probleem voor computers. Het wordt nog lastiger als veel partijen de garantie willen hebben dat niemand vals kan spelen. Dit probleem speelt ook bij nationale loterijen: een winnaar moet willekeurig gekozen worden en alle deelnemers moeten ervan overtuigd zijn dat het selectieproces eerlijk is en dat er niet met de ballenmachine van de loterij is geknoeid.

Cryptografieonderzoek

Dele analogieën van loterijmachines spelen een belangrijke rol in gedecentraliseerde systemen zoals cryptovaluta. In zo'n context kan het aantal betrokken partijen erg groot zijn en het met een uitdaging zijn om consensus te bereiken over een volstrekt willekeurig getal. In 2015 werd een oplossing voorgesteld door Arjen Lenstra, hoogleraar aan de École technique fédérale de Lausanne, Zwitserland (EPFL) en CWI-onderzoeker Benjamin Wesolowski. Het bestaat uit het vrijwillig vertragen van het proces om volstrekt willekeurige getallen te genereren, dankzij een operatie die zorgvuldig is ontworpen om alleen langzaam kunnen worden berekend: een 'verifieerbare vertragingfunctie' (Engels: verifiable delay function) of VDF.

Voordat er was er echter geen bevredigende constructie van een VDF bekend; ook al zou het veel tijd moeten kosten om die te berekenen (een heel leger van computers zou niet sneller mogen gaan), toch zou iedereen efficiënt moeten kunnen controleren of het resultaat correct is. Die situatie veranderde toen onafhankelijk van elkaar, met een tussenpoos van twee dagen, twee constructies werden voorgesteld: één door Wesolowski, en één door Krzysztof Pietrzak, hoogleraar aan IST Austria. Wesolowski's oplossing werd gepresenteerd op de Eurocrypt 2019-conferentie, waar hij er de Best Young Researcher Paper Award voor ontving. Eurocrypt is samen met CRYPTO de belangrijkste conferentie ter wereld voor cryptografieonderzoek.

Energieverbruik

Deze fundamentele nieuwe constructie heeft interesse gewekt in de gemeenschap van blockchaintechnologie en veel platforms hebben plannen om VDF's in hun infrastructuur te integreren. Ze zijn met name een belangrijk ingrediënt voor het ontwerpen van veilige

MEEST GELEZEN BLOGS | CASES

05/06 Cag Gemini presenteert World FinTech Report 2019

15/06 Bedrijven betalen loyale IT'er minder dan jobhopper

31/05 Willem Meints brengt boek uit over neurale netwerken

17/07 Cag Gemini: Cybersecurity zet in op kunstmatige intelligentie

30/07 Blockchain technology and data access to connected cars



Techniques for problem analysis, business requirements, gap analysis, improvement approaches and other skills



VACATURES

Adobe Campaign Developer | A.S. Watson | Renswoude

IT Network Security Engineer | A.S. Watson | Renswoude

Siebel CRM Developer | A.S. Watson | Netherlands (near Utrecht)

Software Tester | A.S. Watson | Renswoude

Oracle Middleware Developer | DPA IT | Apeldoorn

Oracle Middleware Developer | DPA IT | Rotterdam

.Net front-end Developer | DPA IT | Rotterdam

.Net front-end Developer | DPA IT | Den Haag