Digitale veiligheid

Cryptografie gaat met wiskunde witwassen te lijf

Beeld ThinkStock

Lisa Kohl rekent aan veilige digitale communicatie. Ze hoopt hiermee ook banken te kunnen helpen witwasfraude te bestrijden.

Elleke Bal 5 januari 2024, 10:03

Twee miljonairs willen weten wie het rijkste is, zonder prijs te geven hoeveel geld ze hebben. Kan dat? Met wiskunde valt dit probleem op te lossen. Daarvoor moeten de rijken samen een berekening uitvoeren met fictieve getallen, en minstens een deel van de berekening voor elkaar verborgen houden.

Wat de miljonairs moeten doen is een soort protocol opstellen, zoals: doe je vermogen min een willekeurig getal en stuur het resultaat naar de ander. Als ze vervolgens versleutelde stukjes van de oplossing naar een ander sturen, wordt het – met cryptografische technieken – mogelijk om te weten te komen welk bezit het grootste van de twee is, zonder dat ze hun echte vermogen hebben prijsgegeven.

Dit is ook het principe van *secure multiparty computation* (MPC): berekeningen maken met data van meerdere partijen, zonder dat die data gedeeld worden. En dat is de specialiteit van cryptograaf Lisa Kohl. Zij houdt zich bezig met de wiskunde achter digitale veiligheid, bij het Centrum Wiskunde & Informatica (CWI) in Amsterdam.

Geld langs bankrekeningen sluizen

In haar onderzoek werkt Kohl samen met TNO en banken aan het opsporen van witwasfraude. En daarvoor is MPC heel geschikt. Witwasfraude is een probleem dat de samenleving veel geld kost, vertelt Kohl. Jaarlijks wordt er naar schatting in Nederland alleen al zo'n 13 miljard euro witgewassen. Dat doen die criminelen onder meer door geld langs verschillende bankrekeningen wereldwijd te sluizen en zo een dwaalspoor te creëren.

Om die transacties in kaart te brengen, moeten banken hun transactienetwerken naast elkaar leggen. Het punt is: wetgeving verbiedt dat. Onder meer vanwege privacy en commerciële redenen is het ondenkbaar dat de ene bank met de andere bank gegevens deelt over klanten.

Met *multiparty computation* is het mogelijk dat banken toch kunnen zoeken in hun gezamenlijke transactienetwerken, om zo verdachte geldstromen op te sporen. Denk aan de miljonairs die een protocol volgen om tot een conclusie over hun rijkdom te komen. Dat doen banken met protocollen vol rekensommen die heen en weer worden gestuurd.

Lisa Kohl, cryptograaf bij het Centrum Wiskunde & Informatica Beeld Chiara Bellamoli

Multiparty computation is al mogelijk sinds de jarig tachtig, vertelt Kohl. Sindsdien is er, in haar woorden, een soort 'gereedschapskist' van wiskundige berekeningen ontwikkeld om te rekenen met geheimen zonder de onderliggende data te delen. Toch is het gereedschap nog niet goed genoeg. De sommen lopen stuk op de gigantische hoeveelheid transacties. Het gaat in het geval van banken immers niet om twee miljonairs, maar om miljoenen transacties.

"Opschalen is nog steeds een van de grote uitdagingen", zegt Kohl. Het toverwoord is dus efficiëntie: wiskundige foefjes vinden die een berekening sneller uitvoerbaar maken voor computers. En dat is iets waar het onderzoek van Kohl zich op richt. Ze heeft de afgelopen jaren al gewerkt aan een methode om een deel van de berekening vast offline uit te voeren voordat data uitgewisseld worden. Dat scheelt tijd en geld, en het vergroot de veiligheid omdat er minder gecommuniceerd hoeft te worden.

Willekeurige data comprimeren

Een knelpunt waar Kohl mee te maken krijgt in deze voorverwerkingsfase is dat er veel willekeurige vermenigvuldigingen nodig zijn om de geheime data te vermommen. Daarvoor heeft Kohl met haar collega's een generator voor willekeurige berekeningen gebouwd. Het resultaat ervan is dat die willekeurige data met een factor duizend gecomprimeerd kunnen worden. En dat scheelt enorm veel tijd, opslagruimte en geld.

Van onderzoeksfinancier NWO ontving Kohl onlangs een Veni-beurs om dit onderzoek voort te zetten, naar andere innovatieve manieren om MPC-berekeningen efficiënter te maken, zonder daarbij aan veiligheid in te boeten. Daarbij is naast efficiëntie vooral 'kwantumveiligheid' belangrijk. Want alle cryptografen doen momenteel hun werk met de komst van de kwantumcomputer in hun achterhoofd. Die superkrachtige computer zou een groot deel van de huidige wiskundige methodes om informatie te versleutelen kunnen gaan kraken. "Het blijft de vraag wanneer het zover is, maar we moeten er rekening mee houden", zegt Kohl.

En dat is precies het leuke aan cryptografie, vertelt Kohl. "In dit vakgebied kan je wiskunde gebruiken om heel urgente maatschappelijke problemen op te lossen."

Lees ook:

De wiskunde achter de grootte van drugskartels in Mexico, de vijfde grootste 'werkgever' van het land

Voor het eerst gebruikten onderzoekers wiskunde en statistieken om te kijken naar de grootte van de kartels en de aanwas van nieuwe rekruten.

wetenschap

Net binnen MEER

Liveblog Oorlog in Oekraïne

Druk op Scholz neemt toe om kruisraketten te leveren aan Oekraïne

Liveblog Oorlog Israël-Gaza

Unicef: Ondervoeding en ziekte bedreigen meer dan 1,1 miljoen kinderen in Gazastrook

Politiegeweld

Blanke politieagent in VS krijgt 14 maanden cel voor dood zwarte twintiger

Presidentsverkiezingen 2024

Hooggerechtshof VS beoordeelt in februari onverkiesbaarheid Trump

Energiewinning

Het gestage karwei om de belofte van **kernfusie** waar te maken

Dierenwelzijn

We herkennen een **blije kip** aan haar gekakel

Experiment

Het ruiken van een vrouwentraan heeft een meetbaar effect op mannen

Best gelezen MEER

1 **Drie jaar na de eerste coronaprik onderzoeken wetenschappers een...**

2 **Eigen zonnestroom eerst? Stop toch met die mythe**

MEER WETENSCHAP

Wilt u iets delen met Trouw?

Tip hier onze journalisten

Algemeen
Over ons
Contact met Trouw
Privacystatement
Abonnementsvoorwaarden
Gebruiksvoorwaarden
Cookiebeleid
Privacy-instellingen
Auteursrecht
Colofon

Service
Klantenservice
Mijn omgeving
Vakantieservice
Adverteren
Losse verkoop

Meer Trouw
Abonneren
Nieuwsbrieven
Digitale krant
Webwinkel
RSS-feeds
Facebook
Twitter
Android apps
iOS apps

Navigeer
Columnisten
Recensies
Archief