DOOR MARIE BETH VAN EGMOND
EN ALEX SANGERS

Gezamenlijke witwasdetectie met Secure Multi-Party Computation

Nederlandse banken hebben een taak en verantwoordelijkheid in de bestrijding van financiële criminaliteit. Toezicht op witwassen is de afgelopen jaren verder aangescherpt en er zijn allerlei grote boetes uitgedeeld aan Nederlandse banken voor het niet voldoen aan wetgeving.

Om witwassen aan te pakken wordt er de laatste jaren flink ingezet op meer antiwitwasanalisten. Zo werken er bij de Nederlandse banken duizenden medewerkers (de zogenaamde *due diligence*) die ongebruikelijke transacties monitoren.[1] Om deze ongebruikelijke transacties te vinden, werken de banken steeds meer met (machine learning) algoritmes in plaats van regelgebaseerde detectie. Door algoritmes uit te voeren op transactienetwerken kan meer inzicht verkregen worden in criminele geldstromen.

Een beperking bij het uitvoeren van deze algoritmes is echter dat elke bank slechts zicht heeft op de in- en uitgaande betalingen van zijn eigen rekeninghouders. Over de rekeninghouders van andere banken mogen zij wegens privacywetgeving niet zomaar informatie ontvangen. Ook de transacties tussen andere banken blijven buiten het zicht. Hierdoor blijven veel criminele geldstromen verborgen. Met technieken zoals Secure Multi-Party Computation (MPC) kunnen banken echter wél algoritmes uitvoeren op het gehele transactienetwerk.

M.A.N.E. van Egmond MSc (links) is onderzoeker; A. Sangers MSc is projectmanager. Beiden werken ze bij TNO aan Privacy Enhancing Technologieën.

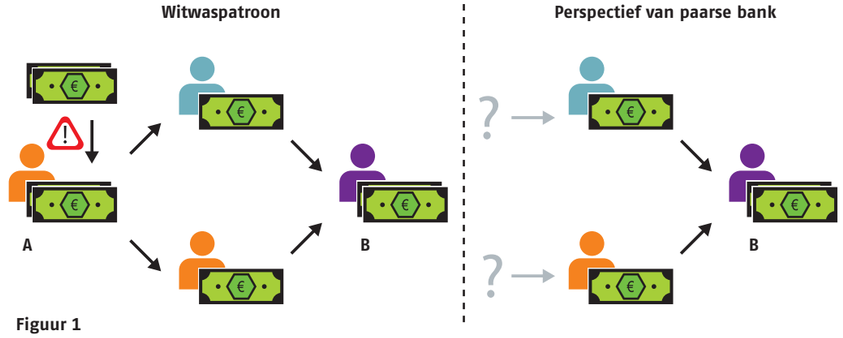
SECURE MULTI-PARTY COMPUTATION (MPC)

Stel dat twee miljonairs willen weten wie van hen de rijkste is, zonder hun vermogen met elkaar te delen. Ze kunnen hiervoor een derde persoon in vertrouwen nemen. Deze persoon kan de miljonairs dan vertellen wie de rijkste is. In de praktijk is zo'n *Trusted Third Party* of TTP echter niet altijd beschikbaar of erg kostbaar.
Met behulp van MPC kunnen de miljonairs samen een berekening uitvoeren, met als einduitkomst wie van hen de rijkste is, met de zekerheid dat zij niet elkaars vermogen leren.
MPC is een verzamelnaam voor technieken waarbij gezamenlijk veilig berekeningen kunnen worden uitgevoerd door meerdere partijen. Het zijn wiskundige protocollen die de TTP vervangen en met wiskundige zekerheid privacy van de input én juistheid van de uitkomst garanderen. MPC biedt een oplossing voor als men wil samenwerken maar geen gevoelige data wil delen.

> OOK MPC-TECHNIEKEN WORDEN INTERNATIONAAL ERKEND ALS VEELBELOVEND IN DE STRIJD TEGEN FINANCIËLE MISDAAD

MPC TEGEN FINANCIËLE MISDAAD

Ook Nederlandse banken willen samenwerken en (transactie)data delen, maar mogen of kunnen dat niet altijd, bijvoorbeeld door privacywetgeving of in verband met de vertrouwensband met klanten. Ook hier bestaan TTPs; bijvoorbeeld Transaction Monitoring Netherlands (TMNL)[2], waar gepseudonimiseerde datasets van vijf banken gecombineerd en geanalyseerd worden.
Ook MPC-technieken worden internationaal erkend als veelbelovend in de strijd tegen financiële misdaad, onder andere door het World Economic Forum[3]. TNO doet al een aantal jaar onderzoek naar de inzet van MPC ten behoeve van detectie van financiële misdaad, meest recent in samenwerking met Rabobank en ABN Amro. In dit onderzoek is vastgesteld dat het voor de banken belangrijk is om crimineel geld door het gezamenlijke netwerk heen te kunnen volgen. Dit heeft geleid tot de ontwikkeling van het *risicopropagatie*-algoritme.



Figuur 1

RISICOPROPAGATIE

In Figuur 1 zien we een voorbeeld van een versimpeld witwaspatroon. In het linker plaatje zien we dat rekeninghouder A (bij de oranje bank) een grote som cash geld ontvangt. Vervolgens wordt dit geld doorgesluisd via de blauwe en oranje bank naar rekeninghouder B bij de paarse bank. Het doel van het risicopropagatie-algoritme is om dit soort verdachte geldstromen te detecteren.
In het algoritme heeft elke rekeninghouder een initiële risicoscore, vastgesteld door de desbetreffende bank. De scores worden bijvoorbeeld gebaseerd op het ontvangen van grote bedragen cash of crypto of relaties met hoog-risico landen. In één iteratie van het algoritme worden de risicoscores van elke rekeninghouder bijgewerkt, gebruikmakend van de (gewogen) inkomende scores in het transactienetwerk. Als een rekeninghouder veel geld ontvangt van een rekeninghouder met een hogere (respectievelijk lagere) score, zal zijn eigen score dus toenemen (respectievelijk afnemen).

> MPC BIEDT MOGELIJKHEDEN OM HET ALGORITME WEL UIT TE VOEREN ZONDER GEVOELIGE DATA PRIJS TE HOEVEN GEVEN

Als we dit idee toepassen op het voorbeeld, zal dus de score van rekeninghouder A initieel hoog zijn, vanwege de grote cash storting. De scores van de twee tussenliggende rekeninghouders zullen dan, door toedoen van de hoge score van rekeninghouder A, na één iteratie van het algoritme worden verhoogd. In een volgende iteratie zal dan ook de score van de paarse rekeninghouder hoger worden, wat aanleiding kan zijn voor verder onderzoek.

Het risicopropagatie-algoritme kan echter niet zomaar worden uitgevoerd. Er is geen enkele partij met zicht op het grotere geheel en de risicoscores kunnen ook niet zonder meer gedeeld worden tussen de banken. Gelukkig biedt MPC mogelijkheden om het algoritme decentraal uit te voeren en de benodigde inzichten te verkrijgen, zonder gevoelige data prijs te hoeven geven.

RISICOPROPAGATIE MET VERSLEUTELDE SCORES

Eén techniek uit de MPC-gereedschapskist is Additieve Homomorfe Encryptie (AHE). Encryptie (of versleuteling) van data zorgt ervoor dat er niets over de data achterhaald kan worden zonder de geheime sleutel. Homomorfe encryptie staat echter toe om berekeningen te doen op versleutelde data, dus zonder de data tussendoor te ontsleutelen.
We gebruiken AHE om de risicopropagatie versleuteld uit te voeren. Om één iteratie van het algoritme uit te voeren, moeten de banken die meedoen de relevante risicoscores (homomorf) versleuteld met elkaar delen. Dankzij de eigenschappen van AHE, kunnen alle banken de benodigde berekeningen voor de risicopropagatie uitvoeren op de ontvangen versleutelde risicoscores. Het resultaat is een versleutelde, bijgewerkte risicoscore. Met medewerking (en dus toestemming) van andere banken kan dan (een deel van) deze nieuwe risicoscores worden onthuld aan de desbetreffende bank. Een andere optie is om niet één maar enkele iteraties uit te voeren met de nog versleutelde risicoscores. In Figuur 1 wordt na twee iteraties de nieuwe score van rekeninghouder B aan de paarse bank onthuld. De paarse bank leert dan de verhoogde score van zijn rekeninghouder. Dankzij AHE kan dit op een decentrale manier en dus zonder de precieze scores van de andere bankrekeningen te leren.

RESULTATEN & TOEKOMST

In samenwerking met ABN Amro en Rabobank heeft TNO de waarde en mogelijkheid van het gezamenlijk uitvoeren van dit algoritme laten zien; gebruikmakend van nepdata die witwaspatronen bevat. De code voor dit algoritme heeft TNO open source gepubliceerd.[4]

In een volgend project (*Alliance for Privacy-Preserving Detection of Financial Crime*) start TNO een pilot met echte transactiedata, samen met Nederlandse banken en het Centrum voor Wiskunde en Informatica (CWI). Er zijn hier nog meer dan genoeg uitdagingen, bijvoorbeeld de juridische interpretatie van deze nieuwe technologie. Zo moet er een Privacy Impact Assessment opgesteld worden, waarbij er ook gezamenlijke verantwoordelijkheid voor de verwerking van (persoons)-gegevens geldt. Deze pilot brengt ons een stap dichter bij ons uiteindelijke doel; financiële criminaliteit bestrijden, terwijl de privacy van klanten gewaarborgd wordt. ■

De onderzoeksactiviteiten die tot dit resultaat hebben geleid zijn gefinancierd door ABN Amro, Rabobank, PPS-toeslag Onderzoek van het ministerie van Economische Zaken en Klimaat en TNO's AppI.AI programma.

1 – 'Detecting financial crime and money laundering'. ABN website. Detecting financial crime and money laundering – ABN AMRO Clearing

2 – www.tmnl.nl

3 – Whitepaper World Economic Forum 'The Next Generation of Data Sharing in Financial Services: Using Privacy Enhancing Techniques to Unlock New Value'.

4 – Open source risicopropagatie door TNO MPC Lab : https://github.com/TNO-MPC/protocols.risk_propagation