Publicatie : Elektronica
Datum : 28 feb 2017
cm2 : 160
Pagina : 25
Advertentiewaarde : € 750,00
Regio : Nederland
Frequentie : 8x per jaar
Oplage : 4.834

Yfke Dulek wint scriptieprijs voor versleuteling qubits voor kwantumcomputer

Yfke Dulek (Universiteit van Amsterdam) ontvangt de Ngi-NGN Informatie Scriptieprijs voor Informatica en Informatiekunde 2016 (5000 euro). Haar scriptie Quantum homomorphic encryption for polynomial-sized circuits gaat over een bijzondere versleutelingsmethode die ze in haar masteronderzoek heeft ontwikkeld. Hiermee kunnen derden in de toekomst berekeningen op versleutelde kwantumdata uitvoeren zonder deze data te hoeven decoderen. Toekomstige kwantumcomputers zijn gebaseerd op de regels van de kwantummechanica en kunnen bepaalde rekentaken vele malen sneller uitvoeren dan de huidige computers. Ze zijn zo radicaal anders dan gewone computers, dat de hardware en software opnieuw ontwikkeld moeten worden. Zo werken kwantumcomputers niet met bits (enen en nullen) maar met qubits.

Yfke deed onderzoek naar het versleutelen (encryptie) van die qubits. Net als de gegevens die nu op onze computers staan, willen we de gegevens op de harde schijf van een kwantumcomputer goed beveiligen. Maar de gangbare encryptiemethoden, die voor gewone bits ontworpen zijn, werken niet op qubits. Yfke ontwikkelde een encryptiemethode waarmee met versleutelde gegevens kan worden gerekend door derden, zonder dat zij die gegevens te weten kunnen komen. Dit is bijvoorbeeld nuttig wanneer men door een externe partij (bijvoorbeeld een supercomputer of de cloud) berekeningen wil laten uitvoeren op gevoelige data. In 2009 is ontdekt dat deze 'homomorfische' encryptie voor gewone bits mogelijk is. Sindsdien heeft men geprobeerd eenzelfde soort encryptie te ontwerpen voor qubits, maar bleef men vastlopen op dezelfde stap. Yfke zet met haar onderzoek die laatste stap en bewijst daarmee het bestaan van een homomorfische encryptiemethode voor kwantumdata. Ze voerde het onderzoek uit in samenwerking met dr. Christian Schaffner en dr. Florian Speelman.

De jury vindt haar onderzoek indrukwekkend, omdat ze meerdere belangrijke resultaten boekt op het gebied van de kwantumcryptografie en vragen beantwoordt die belangrijke cryptologen in recente literatuur hebben gesteld. Onlangs is Yfke Dulek gestart met een promotietraject in de kwantumencryptografie aan het CWI en zet ze haar onderzoek voort bij de Algorithms & Complexity groep.

De Ngi-NGN Informatie Scriptieprijzen worden op 28 november uitgereikt door Maarten Emons, bestuurslid van het Ngi-NGN Platform voor IT-professionals. De jurering was in handen van de Koninkijke Hollandse Maatschappij der Wetenschappen te Haarlem, die nog tal van andere belangrijke wetenschappelijke prijzen toekent. (http://www.hollmij.nl/)