Wiskunde in de cryptografie

Dit themanummer van het *Nieuw Archief voor Wiskunde* staat in het teken van de wiskunde achter cryptografie. Alhoewel van oudsher methoden voor de geheimhouding van berichten tegen derde partijen en voor de authenticiteit van berichten de meest belangrijke voorbeelden van cryptografie zijn, bestudeert de moderne cryptografie een grotere verscheidenheid aan problemen die veiligheid tegen kwaadaardige entiteiten vergen, en probeert die op te lossen met efficiënte algoritmen.

Een dergelijk voorbeeld is *secure computation*, waarbij een groep personen berekeningen wil uitvoeren over ieders geheime invoer waarbij iedereen slechts de uitkomst leert, zeg de som van individuele stemmen. Hoewel iedereen samenwerkt om deze uitkomst te berekenen, leert niemand enig andere informatie dan de uitkomst, zelfs indien een beperkte deelgroep kwaadaardig samenwerkt.

De meest klassieke richting binnen de cryptografie is symmetrische cryptografie. Het idee binnen symmetrische cryptografie is dat entiteiten een geheime sleutel delen en deze gebruiken voor communicatie. De symmetrische versleutelingsalgoritmen zijn met afstand de meest efficiënte binnen de cryptografie. Veiligheid van symmetrische cryptografische systemen wordt tegenwoordig ondersteund met generieke veiligheidsbewijzen en met cryptanalyse, dat zwakheden in de veiligheid van dergelijke oplossingen probeert aan te tonen. Dit nummer bevat drie artikelen over moderne symmetrische cryptografie. Joan Daemen geeft een uiteenzetting van permutatie-gebaseerde cryptografie, en hoe deze vernieuwde richting de toekomst van symmetrische cryptografie kan waarborgen. Bart Mennink behandelt het aspect van veiligheid van versleutelingsalgoritmen en de relatie tussen cryptografie en de verjaardagsparadox. Berry Schoenmakers legt uit hoe je optimaal een hash chain kunt gebruiken voor authenticatie.

Sinds de verschijning van het Turing-award winnende resultaat van Whitfield Diffie en Martin Hellman uit 1976 vormt publieke-sleutelcryptografie een belangrijke richting binnen de cryptografie. Het basisidee binnen deze richting is dat iedere geheime sleutel gepaard gaat met een publieke (niet-geheime) sleutel: een buitenstaander kan de publieke sleutel gebruiken om data te versleutelen op dusdanige wijze dat alleen de eigenaar van de geheime sleutel de gegevens kan ontsleutelen. Robert Granger beschrijft het probleem van discrete logaritmes, legt het belang van deze voor de cryptografie uit, en geeft een uiteenzetting van enkele recente doorbraken en records in het berekenen van discrete logaritmes. Eric Verheul en Bart Jacobs tonen aan hoe de klassieke ElGamal-publieke-sleutelversleuteling gebruikt kan worden voor privacybeschermende versleuteling en authenticatie, en leggen uit hoe dit protocol gebruikt gaat worden in het Nederlandse eID-systeem.

De — momenteel nog theoretische — kwantumcomputers bieden veel nieuwe mogelijkheden voor cryptanalyse. Alhoewel symmetrische cryptografie enigszins weerbaar is tegen kwantumcomputers (in veel gevallen voldoet het om de sleutellengte te verdubbelen), hebben kwantumcomputers de potentie om vernietigende aanvallen op de voornaamste schema's voor publieke-sleutelcryptografie te realiseren: een algoritme van Shor uit 1994 kan bijvoorbeeld het discrete-logaritmeprobleem in polynomiale tijd oplossen. Léo Ducas behandelt bepaalde vormen van rooster-gebaseerde versleuteling, en wat voor invloed kwantumcomputers hierop kunnen hebben.

Een alternatieve richting is om kwantumtechnieken effectief te gebruiken om cryptografie mee te *bedrijven*. Christian Schaffner geeft een toegankelijke uiteenzetting over wat kwantumcryptografie behelst en hoe het veilige communicatie in de aanwezigheid van kwantumaanvallers mogelijk maakt. David Elkouss behandelt vormen van kwantumsleuteluitwisseling waarvan de veiligheid niet afhangt van de gebruikte kwantumapparatuur. Matthijs Coster bekijkt supersinguliere elliptische krommen, en hoe deze gebruikt kunnen worden voor sleuteluitwisseling.

Bart Mennink, *Radboud Universiteit Nijmegen, en CWI, Amsterdam*
Marc Stevens, *CWI, Amsterdam*
gastredacteuren