WETENSCHAPPEN & BIO-INGENIEURSWETENSCHAPPEN

De Onderzoeksgroep
Wiskunde & Data Science

nodigt U graag uit op de openbare verdediging van het proefschrift van

Carlo Emerencia

ter behaling van de graad van Doctor in de wetenschappen

Titel van het proefschrift:

A mathematical approach to post-quantum cryptography

Promotor:
Prof. dr. Ann Dooms

De verdediging heeft plaats op

Woensdag 18 september 2024 om 16u in aula I0.03

De verdediging kan ook online gevolgd worden via:
https://us02web.zoom.us/j/85675641513?pwd=2NHyPTBrAaowYDOZx1O9WsyTkbKrhX.1

Samenstelling van de jury

Prof. dr. Jan De Beule (VUB, voorzitter)
Prof. dr. Leandro Vendramin (VUB, secretaris)
Prof. dr. An Braeken (VUB)
Prof. dr. Angel del Rio (Universidad de Murcia, ES)
Prof. dr. Gabor Ivanyos (Institute for Computer Science and Control, HU)

Curriculum vitae

Carlo Emerencia behaalde zijn Bachelor diploma Wiskunde in 2016 en zijn Master diploma Fundamentele Wiskunde in 2018 aan de Vrije Universiteit Brussel, met grote onderscheiding. Nadien is hij gestart als assistent in de vakgroep Wiskunde & Data Science van de faculteit Wetenschappen en Bio-Ingenieurswetenschappen. Hij combineerde het lesgeven met onderzoek binnen de onderzoeksgroep DIMA onder begeleiding van prof. Dr. Ann Dooms. Zijn onderzoek naar het Verborgen Deelgroep Probleem en kwantumalgoritmen werd gepubliceerd in peer-reviewed internationale tijdschriften en gepresenteerd op internationale evenementen.

Abstract van het doctoraatsonderzoek

Voor moderne hedendaags gebruikte cryptosystemen, zoals RSA, is de veiligheid gebaseerd op moeilijke wiskundige problemen, zoals priemontbinding voor grote gehele getallen. Deze zogenaamde public-key cryptosystemen zijn nog steeds veilig vanwege het feit dat er nog geen klassieke efficiënte algoritmen gekend zijn om deze problemen op te lossen. Echter, de snel verwachte beschikbaarheid van kwantumcomputers bedreigt de veiligheid van deze cryptosystemen door een ontdekking van Shor. In 1994 ontwikkelde hij een kwantumalgoritme dat binnen polynomiale tijd gehele getallen kan ontbinden in priemfactoren. Al vlug werd ontdekt dat zijn aanpak veralgemeenbaar was naar Diffie-Hellman gebaseerde cryptosystemen. Naarmate er bleek dat bijna alle praktische cryptosystemen specifieke gevallen zijn van een algemeen groeptheoretisch probleem, genaamd het Verborgen Deelgroep Probleem, werd het ontwerpen van kwantumaanvallen voor dit probleem een actief onderzoeksgebied.

In mijn thesis heb ik deze groep-theoretische veralgemening van ontbinding in priemfactoren bestudeerd. Hoewel het al opgelost is voor bepaalde soorten groepen, zoals abelse groepen, Hamiltoniaanse groepen en bepaalde semidirecte producten, blijft het een open probleem in het algemeen voor niet-abelse groepen.

In mijn onderzoek analyseerde ik het Verborgen Deelgroep Probleem door algemenere gevallen te reduceren tot één van deze voorgaande gevallen, wat mij toeliet om de huidige state-of-the-art te verbeteren en om enkele veelbelovende richtingen voor verder onderzoek voor te stellen. Ook heb ik onderzocht in welke mate Shor's algoritme gebruikt kan worden om andere post-kwantum kandidaat cryptosystemen aan te vallen, waaronder deze gebaseerd op groepringen.