SCIENCES & BIOENGINEERING SCIENCES

The Research Group
Mathematics & Data Science

has the honor to invite you to the public defence of the PhD thesis of

Carlo Emerencia

to obtain the degree of Doctor of Sciences

Title of the PhD thesis:

A mathematical approach to post-quantum cryptography

Promotor:
Prof. dr. Ann Dooms

The defence will take place on

Wednesday, September 18, 2024 at 4:00 p.m in auditorium I.0.03

The defense can be followed through a live stream:
https://us02web.zoom.us/j/85675641513?pwd=2NHyPTBrAaowYDOZx1O9WsyTkbKrhX.1

Members of the jury

Prof. dr. Jan De Beule (VUB, chair)
Prof. dr. Leandro Vendramin (VUB, secretary)
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 obtained his Bachelor degree in Mathematics in 2016 and his Master degree in Fundamental Mathematics in 2018 at the Vrije Universiteit Brussel, graduating magna cum laude. Afterwards, he started as an assistant at the Mathematics & Data Science department of the Faculty of Sciences and Bio-Engineering Sciences. He combined his teaching assignment with doctoral research at the research group DIMA under the supervision of prof. dr. Ann Dooms. His research on the Hidden Subgroup Problem and quantum algorithms has been published in peer-reviewed international journals and has been presented at international events.

Abstract of the PhD research

Most modern daily used cryptosystems, like RSA, have their security based upon difficult mathematical problems, such as prime decomposition for large integers. These so-called public-key cryptosystems are currently safe because there are no known efficient algorithms to solve their underlying problems on a classical computer. However, the soon expected availability of quantum computers threatens their security due to a discovery by Shor. In 1994 he developed a quantum algorithm that solves the integer factorisation problem within polynomial time. It was soon discovered that his approach was generalizable to Diffie-Hellman based cryptosystems. As it turns out that almost all practical cryptosystems are instances of a general group-theoretical problem, called the Hidden Subgroup Problem, creating quantum attacks for it has become an active field of research.

In my PhD thesis, I investigated this group-theoretical generalisation of integer factorisation. Though already solved for different platform groups, such as abelian, and Hamiltonian groups and certain semidirect products, the problem remains open in general for nonabelian groups.

In my research I analyzed the Hidden Subgroup Problem by reducing more general cases to these previous cases allowing me to advance the state-of-the-art and propose promising avenues for further research. I also investigated to what extent Shor's algorithm can be used to attack other post-quantum candidate cryptosystems, such as those based on group rings.