The Hidden Subgroup Problem

Carlo Emerencia

VUB

Modern daily used cryptosystems like RSA are still safe by the fact that there is no known classical efficient algorithm to factor large integers into primes. However, the soon expected availability of quantum computers threatens the security of these cryptosystems. More concretely, Shor's quantum algorithm for example solves the integer factorisation problem within polynomial time. In this talk, we introduce some basic notions about quantum computation and briefly explain how Shor's algorithm works. Afterwards, we discuss a group theoretical generalisation, called the Hidden Subgroup Problem, and give an overview of the current methods and algorithms that have been found to solve this problem in different cases, together with how our research contributes to the analysis of currently unsolved instances of the problem.

DIMA: Digital Mathematics
Carlo.Emerencia@vub.be