Talk Title: Factoring with oracles

Abstract: The integer factoring problem is assumed to be hard in classical non-quantum computing. We can ask which hint (given by some oracle) would be enough to factor some classes of numbers. The aim of the talk is to describe some of these oracles and their properties. Some of these come from public key cryptography, some others are purely number theoretical. As an example, can we factor a number given the value of its Euler totient function value? We will shed some light on this oracle using the LLL algorithm.