HHL and its impact to post-quantum cryptography

Supervisor Joaquin Garcia-Alfaro[2]
Lab/Team TSP/SAMOVAR

HHL (short for Harrow-Hassidim-Lloyd) is a quantum-accelerated algorithm, expected to solve systems of linear equations exponentially faster than classical algorithms, under certain conditions. The combination of HHL with some other recent computing advancements, including quantum machine learning and search meta-heuristics, could lead to some of these unknown conditions. Their potential disruption to post-quantum cryptography requires from further research.

Expected deliverables/milestones

- 1. Simple description of the HHL algorithm and its potential applications;
- 2. Analysis of PQC algorithms that can be affected by the computational speedup of HHL, or combinations of HHL with additional techniques;
- 3. Implementation of a PoC to validate uncovered findings;
- 4. Paper-like manuscript reporting all the work.

[2] garcia_a@telecom-sudparis.eu