Quantum information processing has been introduced as the new solution to many problems which appear in classical computer science. Two main applications were proposed and are still being developed: quantum protocols, which possess the level of security unachievable for protocols based on classical information, and quantum algorithms, which can break speed limitations of conventional computers. In the second case, the best known algorithms are Shor's algorithm, which can factorize numbers in polynomial time, and Grover's algorithm for database search which achieves square root complexity.

While the excitement in the area of quantum computing is fully justified by the new theoretical developments, year by year scientists have discovered new limitations of quantum computing devices. In particular, unitary operation decomposition provides a number of problems including applications to hardware with fixed topology. Moreover, quantum algorithms have been proved to be fragile to noise, which may impact the results of the computation. This resulted in the development of a new branch of quantum computing, namely the theory of quantum error-correcting codes. This aspect became even more critical when first commercial quantum computing systems became available. Furthermore, for quantum cryptographic protocols, hardware attacks, based on the security holes of conventional electronics, have been discovered. This demonstrated that the theoretical security confirmed by the laws of physics in the ideal environment could be insecure in the real-world applications.

The main novelty of the presented project is the approach to the analysis of quantum algorithms based on the study of the input data. Using this approach we will characterize the applicability of quantum algorithms in real-world scenarios, taking into account that algorithms are exposed to attacks, including those based on providing malicious data.

Since quantum spatial search has been well analysed in the context of efficiency, we plan to use this family of algorithms as the starting point of the project. We will consider complexity attacks based on exceptional configuration and on the imprecise implementation of the algorithm. We will introduce the formal description of the resilience of the family of quantum algorithms based on quantum spatial search and provide the connection between the structure of the underlying network and the ability to perform an algorithmic attack on the algorithm. We will describe how the knowledge about the attack can be used to reduce the impact of the algorithmic attack and how the efficiency of the attack depends on the random graph model used to describe the data. Thus, our work provides the connection between the structure of the graph and the computational complexity of quantum algorithms.