According to research, information technologies account for an insignificant percentage of energy consumption on Earth. In recent years, awareness has also increased that its resources should be used in a way friendly to the environment. At the same time, quantum information technology has joined the group of information technologies - a field that uses the laws of physics, specifically quantum mechanics, to process information. Quantum Information Theory has reached a high level of advancement in recent decades. With its development, many so-called quantum resources have been discovered and explored. By quantum resource, we mean the phenomenon by which, under certain circumstances, we get faster, more efficient, or more secure information processing. The list of known resources includes, among others, quantum entanglement, quantum coherence, Bell non-locality, quantum contextuality, secure randomness, and a cryptographic key secure against a quantum adversary, but it is constantly being extended. So far, it has usually been studied how to obtain a specific resource while accepting an arbitrarily high cost of its production. Last year, however, the Quantum Energy Initiative was established, aiming to estimate and minimize the consumption of physical resources by quantum technologies.

In spirit of this initiative, the first goal of this project is to design new protocols for obtaining quantum resources that are more friendly to the environment. This time, it will not be the only goal to obtain resources but also to minimize the energy cost of obtaining them. One of the many resources we will explore is the so-called "magic" that allows for universal quantum calculations, quantum coherence, and purity, understood as the ability to do thermodynamic work.

One of the most important in terms of its use of quantum resources, apart from the resources mentioned above and quantum entanglement, is also a cryptographic key that is safe against a quantum adversary. Depending on the level of security concern, i.e., trust in the manufacturer of the cryptographic device that generates the cryptographic key, we are talking about a key whose security depends or does not depend on the device. Interestingly, the cryptographic key theory has not been fully developed so far. The second goal of this project is to develop the cryptographic key theory first by calculating the security cost for two-chip quantum states. Secondly, we intend to find upper bounds on the multi-system cost of both quantum entanglement and a secure key. The most important factor indicating energy leakage in transforming quantum information is the irreversibility of creating a resource versus its distillation, i.e., obtaining a resource from its noisy version. Therefore, thirdly, we want to determine the amount of such irreversibility, which will allow us to estimate the energy cost depending on the technological cost of preparing qubits (units of quantum information) in the appropriate state. To this end, we will give new tight upper bounds on the distillable cryptographic key in various scenarios and lower bounds on the cost of creating states in security terms.

For over a dozen years, work has been ongoing on the implementation of the quantum Internet - a quantum network that would enable, among other things, secure communication and quantum computing in the cloud on an intercontinental scale, unlike the current commercial point-to-point connections on a metropolitan and continental scale. In anticipation of a technological breakthrough that will allow the implementation of the idea of the quantum Internet, we want to assess the cost of its various implementations in terms of a secure key in this project. The project's third goal is to determine whether, on an intercontinental scale, the amount of cryptographic key can exceed the amount of established pure entanglement. Depending on the result, the cost of a quantum network on an intercontinental scale will be estimated in terms of pure entanglement or a cryptographic key. The next sub-task will examine the cost of connections enabling secure conversations of network users and pose similar questions regarding the quantum network whose security does not depend on the device.

The above research project is largely pioneering. Its expected effects will include new, more ecological ways of processing quantum data, knowledge of the cheapest cryptographic scenario in terms of security, and an estimation of the cost of quantum Internet in terms of a secure cryptographic key. The development of knowledge about quantum resources is also expected. The broader vision of this project includes not only the study of the cost of quantum states and state-related resources but also the cost of quantum communication channels.