Summary of the project:

Quantum cryptography offers unprecedented levels of security but is susceptible to implementation level attacks, which exploit the differences between the theoretical model of the devices and their physical realization. Moreover, some hacking attacks can artificially induce such differences. This results in a situation in which the current generation of quantum technology is less trustworthy than the well-tested classical solutions. A new version of quantum cryptography – device independent can solve this problem as it is, by definition, impervious to physical flaws. Its name stems from the fact that inner workings of the hardware are not taken into account when testing security. The probability distribution of outputs being the only figure of merit.

Unfortunately, state-of-the-art device independent experiments are many orders of magnitude too slow and work at much shorter distances than required for practical purposes. The aim of the project is to improve the theoretical background that device independent quantum cryptography is based on, to such a level that it becomes feasible in real life applications. We will achieve this by investigating new nonclassicality tests which are the foundation of whole quantum cryptography, streamlining security proofs and inventing new experimental setups.

Relevance to the topic addressed in the call:

Security and Privacy in Decentralised and Distributed Systems is impossible without secure communication and private random numbers which are exactly the components that we improve in our project. The specific target outcomes of the call that our project addresses are:

1. Design of hybrid software-hardware security and privacy solutions – The nature of device independent quantum cryptography is the study of the interplay between the hardware and the software. We will create new hardware ideas and design protocols tailored for this equipment.

2. Design of verification models for real-world applications of privacy and security solutions –Most of the tasks of our project boil down to development of methods for verifying how far the real-world version of a particular device is from the ideal case.