PhD in Mathematics **Scholarship Title**	Development and security proof of Quantum Key Distribution protocols based on single particle entanglement (SP-QKD)
Contacts.:	Sonia Mazzucchi (sonia.mazzucchi@unitn.it) Silvio Ranise (silvio.ranise@unitn.it) Lorenzo Pavesi (lorenzo.pavesi@unitn.it)
Synthetic description of the activity and expected research outcome	The main goal of the PhD student's thesis work is the development, the security analysis as well as a critical evaluation of new quantum key distribution (QKD) protocols based on single-particle entanglement. Experiments will also be performed to validate the proposed QKD protocol. The project acronym is SP-QKD (which stands for Security Proof of QKD). Since one of the main issues affecting the security of QKD is the authentication of the two clients and the possibility of a "man in the middle attack", we plan to tackle this problem. On the one hand, we plan to propose some use-cases where the high security promised by QKD protocols is not significantly damaged by authentication issues. On the other hand, we plan to develop and analyze new protocols more robust under man-in-the-middle attacks by introducing a trusted arbiter, similarly to what is done in [Ma19]. Eventually, the developed protocols will be implemented with a fiber optics or a free space based set-up with the SPE sources available in the laboratories of the NanoLab. This will allow us to verify the protocol at different levels of abstraction, namely on design with possibly automated security analyses and on implementation with an experimental assessment of performance and security risks. Here, the PhD student will collaborate in assessing and evaluating the results of the analyses at the various levels of abstractions.
Ideal candidate (skills and competencies):	Interdisciplinary expertise is necessary to develop the project, including knowledge of modern cryptography, security analysis proofs, probability theory, quantum information theory and photonics. The PhD student enrolled in this project is assumed to be mainly a mathematician with an expertise in modern cryptography and security analysis, but he/she should be also able to collaborate with experimental physicists of the Nanoscience Laboratory based at the DF.