Multi-party quantum cryptographic primitives in realistic environments

Résumé du projet de recherche (Langue 1)

In an increasingly connected and globalized world, the notions of security and privacy are an imperative, henceforth making cryptography a very important research field. In the not so far future, adversaries are likely to possess the ability to perform computations on quantum computers that would enable them to break most of the commonly used security systems. It is, therefore, an urgency to strengthen the foundations of cryptography, in order to make them sufficient for a world where quantum computation and communication is an available resource. Quantum computation has had a tremendous impact in the field of cryptography in the last decades. Shor’s algorithm for factoring shows that quantum computers are probably more powerful than classical ones, since factoring is assumed to be hard for any classical computer. Moreover, the ability to communicate over quantum channels has made it possible to revisit unconditionally secure cryptography, in particular in the context of secret key distribution. These developments have opened the way to using the power of quantum mechanical systems to achieve a level of security in computer and communication infrastructures that is impossible to achieve by any classical means. The proposed research project is situated at the heart of this exciting field. It has the goal to build upon the wealth of knowledge available for quantum key distribution to explore advanced quantum cryptographic primitives in a realistic setting, which involves practical components and multiple communication parties.

Résumé du projet de recherche (Langue 2)

Since the discovery of unconditionally secure key distribution, a series of works has investigated what other cryptographic primitives are possible or not in the quantum world. Such primitives have been mostly studied in an idealized setting, where there are no errors and losses in the communication channel. It is clear, however, that for the development of practical quantum cryptographic systems, it is important to consider a realistic setting. The main goal of this doctoral project is therefore to provide a general framework that will enable the theoretical study of quantum cryptographic primitives in a realistic scenario, i.e., in the presence of losses and errors, as well as to achieve their experimental implementation, ideally using standard telecommunication and fiber optic components. A second objective that will be pursued is the extension of the aforementioned ideas to the case of multi-party quantum networks. A network structure is indeed required to overcome the limitation imposed by the channel loss to the maximum communication distance between two parties and is better suited to a realistic scenario of communication systems for which point-to-point exchange links are not sufficient. It is therefore essential to conceive, study the security and implement adapted quantum protocols.

Informations complémentaires (Langue 1)

The doctoral candidate will benefit from the extended collaborations of the supervisors in the field of the research proposal in the context of ANR, European and bilateral (Canada, Japan) projects.

Informations complémentaires (Langue 2)

The research proposal belongs to the EDITE thematic area: L : algorithme, programmation de systèmes séquentiels ou répartis The proposal subject is situated at the frontier between computer science and physics; we therefore propose the co-supervision of the candidate by two scientists, Eleni Diamanti from LTCI – Télécom ParisTech and Iordanis Kerenidis from LRI – Université Paris-Sud XI, who belong in these two fields with common involvement and interest in quantum communication and quantum computation. The doctoral candidate should be motivated and have a varied background in most or all of the following areas: mathematics (including information theory), cryptography, physics (including quantum mechanics, optics), and computer science (including complexity theory and algorithms).