Position based cryptography

Mots clés :
- Directeur de thèse : jean-pierre TILLICH
- Co-encadrant(s) :
- Unité de recherche : INRIA-Paris
- École doctorale : École Doctorale Informatique, Télécommunications, Électronique de Paris
- Domaine scientifique principal: Divers

Résumé du projet de recherche (Langue 1)

Position-based quantum cryptography is a recent line of work where the position of the legitimate party acts as their only credential. The simplest such primitive is position verification, where honest parties can prove that they lie at a given spatial position at a certain time. While a general no-go theorem was established (both in the classical and in the quantum settings [1, 2]), it turns out that in the quantum case, the best attacks seem to require unreasonable resources: an amount of entanglement exponential (or even doubly exponential) in some parameters of the problem. Clearly, if such bounds can be proven to be optimal, then position-based quantum cryptography would become possible for any practical purposes, thereby opening the way to many completely new applications. The main goal of this PhD is to devise simple, practical protocols that provably require a large amount of entanglement to break. A natural solution consists in increasing the number of verifiers, without requiring them to send entangled states. A second challenge will be to investigate security in a realistic scenario where (classical) computation takes time and where the communication channels are imperfect. [1] N. Chandran, V. Goyal, R. Moriarty, R. Ostrovsky, “Position based cryptography”. In Advances in Cryptology-CRYPTO 2009, pp. 391-407, Springer Berlin Heidelberg (2009). [2] H. Buhrman, N. Chandran, S. Fehr, R. Gelles, V. Goyal, R. Ostrovsky, C. Schaffner, “Position-Based Quantum Cryptography: Impossibility and Constructions”. Advances in Cryptology–CRYPTO 2011, pp. 429-446, Springer Berlin Heidelberg (2011).

Résumé du projet de recherche (Langue 2)

The program of this thesis is to explore the very recent field of quantum position-based cryptography and to devise protocols that are practical despite the existence of a general no-go theorem. To this end, one possibility is to put natural restrictions on potential adversaries, for instance that they cannot share an arbitrary amount of entanglement. This work will be mainly theoretical, but collaborations with experimental groups in Paris are possible if certain protocols prove reasonably easy to implement.

Informations complémentaires (Langue 1)

This position is open to all nationalities. The candidate must have good command over written and spoken English.