

## Abstract

Quantum computing is the study of what we can and cannot do with quantum computers: computers operating based on the laws of quantum mechanics. This thesis is a collection of seven papers, dealing with three aspects of quantum computing: non-locality, cryptography and complexity.

### Nonlocality

Quantum nonlocality refers to the fact that, using a resource called *quantum entanglement*, two participants who are physically separated and unable to communicate can exhibit correlations that cannot be produced without entanglement. This gives rise to *nonlocal games*, which are multi-player cooperative games for which quantum players (who share entanglement) have an advantage over classical players (who share only classical information). A *pseudo-telepathy* game is a special case of a nonlocal game for which quantum players have a *perfect* winning strategy. The first paper in this thesis, *On the power of non-local boxes*, is a study of quantum correlations (which are *non-signalling*, *i.e.* they do not allow faster-than-light communication), as well as *superquantum* correlations (which are also non-signalling, but “stronger” than those predicted by quantum mechanics). We consider the simulation of pseudo-telepathy winning strategies with the *nonlocal box* (which can be seen as the most basic superquantum correlation), revealing that nonlocality and entanglement are different resources. Before our work, it was common to equate these two notions. The second paper, *Classical, quantum and non-signalling resources in bipartite games*, shows that the problem of deciding if a fixed game has a perfect classical winning strategy is **NP**-complete, while deciding if a perfect strategy exists with superquantum correlations is in **P**. We also establish links with the Bell-Kochen-Specker theorem, orthogonality graphs and two-prover interactive proofs.

Quantum nonlocality is a phenomenon that we can, in theory, witness in the laboratory. Many experiments have been performed, but none so far have simultaneously closed all experimental loopholes. There is currently a substantial scientific effort to achieve the perfect laboratory experiment. Yet not all experimental setups are created equally: the third and fourth paper of this thesis, *Entanglement swapping, light cones and elements of reality* and *On the logical structure of Bell theorems*, show that recent proposals have classical explanations, and thus do nothing to aid in our comprehension of the quantum world. This work is scientifically valuable, since it tells us that we should not invest in the proposed lines of research.

## Classical and quantum cryptography

The groundbreaking work of Peter Shor in 1995 established that quantum computers can efficiently factor large integers, thus rendering most modern cryptographic systems insecure. But what quantum computers break, they also fix: Bennett and Brassard had already given in 1984 a protocol for key distribution whose security is based only on the laws of quantum mechanics.

In a world with quantum computers, it seems like the only way to ensure perfect security in cryptographic tasks is to do away with computational assumptions (such as the apparent difficulty of factoring): this is the realm of information-theoretic security. In the fifth paper of this thesis, *Information-theoretic security without an honest majority* we give protocols to accomplish a series of six private distributed tasks (in particular, *vote* and *anonymous message transmission*), while ensuring information-theoretic security. Then, in *Anonymous quantum communication*, we give a protocol which, within a group, allows a sender to transfer a quantum message to a receiver of his choosing. The protocol ensures information-theoretic anonymity for the sender and the receiver as well as information-theoretic privacy for the message.

## Complexity in the measurement-based model

Finally, in *Parallelizing quantum circuits*, we study the depth complexity of quantum circuits, giving an automated technique for the parallelization of quantum circuits. The development of parallel (low-depth) quantum circuits seems almost essential if we wish to implement quantum algorithms in the near future with available technology. Quantum information is usually unstable, hence we can only operate on it for a very short period of time. Parallel circuits maximize the use of this fragile quantum information. Our method is based on the recent paradigm for quantum computing called the *measurement-based model*.

**Key words:** quantum information processing, pseudo-telepathy, nonlocal boxes, Bell's theorem, multi-party computation, information-theoretic security, anonymity, quantum depth complexity, measurement-based quantum computing, measurement calculus.