Quantum computers seem to have capabilities which go beyond those of classical computers. A particular example which is important for cryptography is that quantum computers are able to factor numbers much faster than what seems possible on classical machines.

In order to actually build quantum computers it is necessary to build sufficiently accurate hardware, which is a big challenge. In Part I of this thesis we prove lower bounds on the accuracy of the hardware needed to do quantum computation. We also present a similar result for classical computers.

One resource that quantum computers have but classical computers do not have is entanglement. In Part II of this thesis we study certain general aspects of entanglement in terms of quantum XOR games and non-locality.

Part I: Limits on fault-tolerant quantum and classical computation

At the moment, quantum algorithms are only fast in theory, since we are a long way from building quantum computers large enough to solve large instances of these problems (for example factoring). This is despite a decade-long, concentrated effort by experimental physicists. The reason is that quantum computers must be built from very small components in order to exhibit quantum properties. Building and operating on these small components is hard and is probably not possible without faults. Faulty devices are also called “noisy”. Rather surprisingly, it is still possible to do arbitrarily long quantum computation even if the physical devices used are not perfect but slightly noisy. Unfortunately, currently it is not possible to build hardware which is accurate enough to allow large-scale quantum computation.

In Part I of this thesis we show minimum requirements on the accuracy of quantum hardware, by proving upper bounds on the amount of noise tolerable for fault-tolerant quantum computation. We show the following upper bounds on the tolerable noise rates:
1. In Chapter 3 we consider circuits with arbitrary gates of fan-in at most \( k \), in which each wire is subject to more than \( 1 - 1/k \) erasure noise. We show that already after a constant amount of time it is impossible to distinguish any two input states by a single-qubit measurement. For polynomial-size circuits it is impossible to distinguish any two input states by measurements on all qubits after time which is logarithmic in the size of the circuit.

2. In Chapter 4 we analyze circuits built with almost perfect 1-qubit gates and arbitrary \( k \)-qubit unitaries in which all incoming wires are subject to at least \( 1 - \sqrt{2^{1/k} - 1} \) depolarizing noise. We show that after a constant amount of time no single-qubit measurement can distinguish any two input states. For the interesting case \( k = 2 \) our bound becomes 35.7%.

3. In Chapter 5 we show that circuits built from stabilizer gates (Hadamard gate, Phase gate, CNOT, measurements in the computational basis, preparation of computational basis states) and arbitrary 1-qubit gates with depolarizing noise at least \( \hat{\theta} = (6 - 2\sqrt{2})/7 \approx 45\% \) can be efficiently simulated on a classical computer.

In Chapter 4 we analyze noise in classical computation. Faults happen in modern computers so rarely that the problem of error-correction and fault-tolerance is nowadays essentially ignored. However, if hardware engineers continue to shrink the size of components, faults will become more likely and it will be important to know how to cope with them.

4. We show a threshold on the tolerable noise for computation by formulas with \( \epsilon \)-noisy 2-input gates: Fault-tolerant classical computation is possible if and only if \( \epsilon < (3 - \sqrt{7})/4 \approx 8.856\% \).

Part II: Entanglement and interactive proof systems

In Chapter 7 we consider games played between a verifier and two (possibly entangled) provers. In these games the verifier sends questions to the provers, who win if they can answer them correctly. Games like this are the basis of all multiprover interactive proof systems, but they also have many other applications. For certain types of games, namely quantum XOR games, we show a perfect parallel repetition theorem: The provers’ optimal success probability for winning a collection of quantum XOR games played simultaneously is equal to the product of the success probabilities of the individual games. This is a remarkable feature of entanglement, since for classical XOR games a perfect parallel repetition theorem does not hold. Further, quantum XOR games are the only kind of games which are currently known to obey a perfect parallel repetition theorem.

In Chapter 8 we analyze a different feature of entanglement. Entanglement allows two separated parties to exhibit non-local correlations, i.e., correlations
that cannot be explained by any classical local hidden-variable model. Tsirelson proved an upper bound on the strength of these correlations, using the quantum mechanical axioms. His bound is known as Tsirelson’s bound. In Chapter 8 we show that a weaker version of Tsirelson’s bound can be derived from some general plausible assumptions about the world, without invoking the axioms of quantum mechanics themselves. The aim is to explain certain surprising consequences of quantum mechanics, using plausible assumptions about the real world. The assumption we use is the following: Two separated parties Alice and Bob need to communicate in general more than one bit, in order to compute the value of a Boolean function for which some of the input bits are in Alice’s possession and some in Bob’s.