Chapter 6

CRYPTOGRAPHY

INTRODUCTION

Secure communication is one of the areas of key importance for modern society in which quantum information transmission and processing seems to be able to bring significant contributions. For example, quantum cryptography may be the main defence against quantum code breaking in the future.

An important new feature of quantum cryptography is that security of quantum key generation and quantum cryptographic protocols is based on a more reliable fact, on the laws of nature as revealed by quantum mechanics, than in the case of classical cryptography, whose security is based on unproven assumptions concerning the computational hardness of some algorithmic problems.

It is difficult to overemphasize the importance of quantum cryptography for an understanding and utilization of quantum information processing. Quantum cryptography was the first area in which quantum laws were directly exploited to bring an essential advantage in information processing.

Closely related are quantum teleportation and quantum superdense coding—special ways of the transmission of quantum or classical information using one of the most puzzling phenomena of the quantum world—non-locality features of the quantum entanglement.

LEARNING OBJECTIVES

The aim of the chapter is to learn:

1. several methods of secret key generation by two parties;
2. a method of multiparty secret key generation;
3. the unconditional security of quantum key generation;
4. the basic quantum cryptographic protocols;
5. the problems related to the security of quantum cryptographic protocols;
6. the main principles, circuits and some applications of quantum teleportation;
7. the quantum superdense coding procedure.