Quantum Cryptography Based on Orthogonal States

Lior Goldenberg and Lev Vaidman

School of Physics and Astronomy, Raymond and Beverly Sackler Faculty of Exact Sciences, Tel-Aviv University, Tel-Aviv 69978, Israel

(Received 23 February 1995)

All existing quantum cryptosystems use nonorthogonal states as the carriers of information. Nonorthogonal states cannot be cloned (duplicated) by an eavesdropper. As a result, any eavesdropping attempt must introduce errors in the transmission, and, therefore, can be detected by the legal users of the communication channel. Orthogonal states are not used in quantum cryptography, since they can be faithfully cloned without altering the transmitted data. We present a cryptographic scheme based on orthogonal states, which also assures the detection of any eavesdropper.

PACS numbers: 03.65.-w, 89.70.+c

A basic task in cryptography is exchanging a secret message between two users, traditionally called Alice and Bob, in a way that no other party can read it. The only known method to do this in a proven secure way is to use a “one-time pad,” which uses a previously shared secret information called a key. The key, a sequence of random bits, is used for encrypting the message. The encrypted message is completely confidential, even if transmitted via a public communication channel. Thus the security of any key-based cryptographic method depends ultimately on the secrecy of the key. All existing classical key-distribution cryptosystems are not proven to be secure; their secrecy is based on computational complexity assumptions which sometimes turn out to be false. In particular, some existing cryptosystems can be broken (in principle) due to new developments in quantum computation [1]. On the other hand, the secrecy of quantum cryptosystems is guaranteed by the fundamental laws of quantum mechanics. Any intervention of an eavesdropper, Eve, must leave some trace which can be detected by the legal users of the communication channel.

In the recent years many quantum cryptosystems have been suggested. All of these schemes use nonorthogonal states to encode the information. The first key-distribution scheme was presented by Bennett-Brassard [2] in 1984 (a variation of it has already been tested experimentally [3]). In this scheme Alice transmits single photons polarized along one of four possible directions, \( \perp, \leftrightarrow, \nearrow, \text{ or } \searrow \). The first two are orthogonal in one basis and the other two are orthogonal in another basis. The encoding is as follows: Alice chooses, at random, one of the four states and sends it to Bob. It is agreed that the states \( \leftrightarrow \) and \( \searrow \) stand for bit value 0, and the states \( \perp \) and \( \nearrow \) stand for bit value 1. Bob chooses, also at random, a basis, \( \oplus \) or \( \otimes \), and measures the polarization in that basis. If Alice and Bob choose the same basis, their results should be identical. If they choose different bases, their results are not correlated. By discussion over an insecure classical channel (which cannot be modified by an eavesdropper), Alice and Bob agree to discard all the cases where different bases were used (about half of the bits). The result should be two perfectly correlated strings, unless the transmission was disturbed. Any eavesdropping attempt must introduce errors in the transmission, since Eve does not know the polarization of each photon. Whenever Alice and Bob measure in one basis and Eve in the other basis, the correlation of the strings is destroyed.

The encoding in quantum cryptography was based on nonorthogonal states, since they cannot be cloned (duplicated) by an eavesdropper. Even an imperfect cloning attempt (intended to gain partial information) induces errors in the transmission, therefore, it is detectable. In general, any two nonorthogonal states can be used for quantum cryptography, as shown by Bennett [4]. On the other hand, orthogonal states can be faithfully cloned, so that Eve can copy the data without being noticed. For these