

Quantum Public-Key Cryptography

Georgios M. Nikolopoulos

Institute of Electronic Structure and Laser, FORTH, P. O. Box 1527, Heraklion 711 10, Crete, Greece

nikolg@iesl.forth.gr

Abstract

Quantum key-distribution (QKD) is the most mature field of quantum information processing. While certain QKD prototypes have entered the market, the deployment of QKD technology is hindered by various road blocks including the problem of key management. This presentation deals with quantum public-key (asymmetric) cryptography, which may provide a way out of this stumbling block.

Motivation

Today, the establishment of a secret key between two parties can be achieved by means of QKD protocols. By virtue of fundamental principles of quantum mechanics that do not allow passive monitoring and cloning of unknown quantum states, QKD protocols provide a solution to the *key-distribution problem* even in the presence of the most powerful adversaries. Nevertheless, the *key management* remains one of the main drawbacks of symmetric encryption schemes. In particular, the problem pertains to large networks where each entity needs a secret key with every other entity. Hence, the total number of secret keys scales quadratically with the number of users in the network.

One solution to the key-management problem is the use of an unconditionally trusted third party which is burdened with the key management and acts as a key-distribution center. The main problem with this solution, however, is that the center itself becomes an attractive target, while a compromised center renders immediately all communications insecure. An alternative solution to the key-management problem is provided by conventional public-key cryptosystems which are very flexible but, offer computational security only.

We discuss the prospect of quantum public-key cryptography (QPKC), which combines the provable security of QKD protocols with the flexibility of conventional public-key encryption schemes. The development of such a cryptosystem requires the existence of *quantum trapdoor one-way functions*, i.e., functions that are "easy" to compute, but "hard" to invert without some additional information (the so-called trapdoor information). Moreover, the one-way property of these functions has to rely on fundamental principles of quantum theory, rather than unproven computational assumptions.

QPKC based on single-qubit rotations

The presented cryptosystem relies on single-qubit rotations, thus allowing for comparison with existing QKD protocols. Each participant has to generate a pair of keys: a *private key*, which is purely classical, and a *public key*, which involves a number of qubits prepared independently in states specified by the private key. The sender (Bob) encrypts his message on the recipient's (Alice's) public key by rotating the state of its qubits. Alice can extract the message from the cipher state by means of quantum operations, which are determined by the private key.

Eavesdropping

In the context of asymmetric cryptosystems, the primary objective of a potential adversary (Eve) is to recover the message, from the cipher state intended for Alice. On the other hand, there is always a more ambitious objective pertaining to the recover of Alice's private key. A cryptosystem is considered to be broken with accomplishment of any of the two objectives, but in the latter case the adversary has access to all of the messages sent to Alice. Given that in an asymmetric cryptosystem multiple copies of the public key can be issued simultaneously, Eve may launch new powerful attacks to accomplish her objectives. We discuss the security of the presented cryptosystem against various types of attacks, and derive bounds on the number of public keys and the message length, so that security is guaranteed.

Outlook

The prospect of QPKC remains largely unexplored up to now. We hope that our results and discussion will stimulate further investigations on these topics, so that light is shed on crucial questions, pertaining to the power and the limitations of QPKC. Moreover, such investigations might lead to the development of practical public-key cryptosystems, or other provably secure quantum cryptographic primitives.

References

1. G. M. Nikolopoulos, Phys. Rev. A, 77 (2008), 032348