Quantum Public-Key Cryptosystems

Tatsuaki Okamoto[1], Keisuke Tanaka[2], and Shigenori Uchiyama[1]

[1] NTT Laboratories
1-1 Hikari-no-oka Yokosuka-shi, Kanagawa 239-0847, Japan
fax: +81-468-59-3858
{okamoto, uchiyama}@isl.ntt.co.jp
[2] Dept. of Mathematical and Computing Sciences
Tokyo Institute of Technology
1-12-1 Ookayama Meguro-ku, Tokyo 152-8552, Japan
fax: +81-3-5734-2714
keisuke@is.titech.ac.jp

Abstract

This paper presents a new paradigm of cryptography, *quantum public-key cryptosystems* consisting of *quantum public-key encryption* and *quantum digital signatures*. In quantum public-key cryptosystems, all parties, including senders, receivers, and adversaries, are modeled as *quantum* (probabilistic) polynomial-time Turing (QPT) machines, and only classical channels (i.e., no quantum channels) are employed. A *quantum trapdoor one-way function*, f, plays an essential role in our system, in which a QPT machine can compute f with high probability, any QPT machine can invert f with negligible probability, and a QPT machine with trapdoor data can invert f.

This paper also proposes a concrete scheme for quantum public-key cryptosystems: a quantum public-key encryption scheme or quantum trapdoor one-way function. The security of our schemes is based on the computational assumption that a class of subset-sum problems is intractable against any QPT machine. Our scheme is very efficient and practical if Shor's discrete logarithm algorithm is efficiently realized on a quantum Turing machine.

Keywords: one-way functions, public-key cryptosystems, digital signatures, knapsack-type cryptosystems