

Desk copy

19 / Feb / 95

# Cryptography with Quantum Files

(or Quantum Cryptography without Quantum Channels)

E. Biham\* T. Mor†

## Abstract

Public key cryptography and quantum cryptography allow secure communication between two parties who share no secret data in advance. Public key cryptography provides security which relies on computational complexity assumptions, while quantum cryptography provides security which relies on the laws of quantum mechanics. A key tool of public key cryptography is a public file which holds the public keys of the users. Any user is allowed to access the public key of any other user, and can use it to communicate and authenticate the communication with the other user. In this paper we define new notions of files, which are used to combine the advantages of public key cryptography and quantum cryptography. We suggest a particular quantum cryptosystem, in which correlations between quantum states are created by the center upon request. Our system is particularly adequate to form a network of many users, and *any* two users who have quantum keys (even in different centers) can communicate securely. Even the center(s) cannot gain any information on the transmitted messages. In this system, quantum channels are not required.

## 1 Introduction

The only known method to exchange secret information through a communication channel in a proven secure way, is to use the one-time pad. In this technique, the data is mixed with a random secret key (known only to both users) and the result is sent through the communication channel. The randomness of the key ensures that the encoded message is also completely random and thus totally unintelligible to a potential eavesdropper. Safety can be guaranteed only if the secret key is used once.

We remain with the problem of secure distribution of the key to both users. In the old days, the only possibilities were personal meetings and trusted couriers, which made the techniques rather expensive, and not practical for many applications. Currently there are only two known solutions to this problem: quantum cryptography and public key cryptography. Quantum cryptography allows any two users to distribute keys but in networks of many users it has several disadvantages: (i) The keys should be transmitted *online*, or else, all the ( $O(N^2)$ ) pairs of users should transmit the keys in advance. (ii) The network should assure authenticity of the users (since all quantum protocols assume

---

\*Computer Science Department, Technion, Haifa 32000, Israel.

†Department of Physics, Technion, Haifa 32000, Israel.