

# Cryptography with Quantum 'Public' File

E. Biham\*, B. Huttner† and T. Mor‡

## Abstract

Quantum cryptography provides security which relies solely on the laws of quantum mechanics. Public key cryptography provides security which relies on computational complexity assumptions. 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 then communicate with that user, without sharing any data with him in advance. In this paper we define new notions of public files, which are used to combine these advantages of public key cryptography and quantum cryptography. We suggest a particular quantum cryptosystem, in which correlations between quantum states are created upon request. As a result, *any* two users who have quantum keys in the same center can communicate securely.

## 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 XORed 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. Public Key Cryptography (PKC) [13] (and the RSA cryptosystem [20]) suggest a partial solution to these problems. In PKC Bob chooses a pair of mutually inverse transformations:  $E$  for encryption and  $D$  decryption. He publishes the encryption transformation  $E$  in a *public file* so that Alice, and actually any user, can use it (by calculating  $C = E(M)$ ) to send messages to Bob. The decryption algorithm  $D$  remains secret, and Bob is the only one who can execute it and read the message  $M = D(C)$ .

Unfortunately, PKC (and any public key cryptosystem (PKCS)) relies on *computational* complexity assumptions, and they can be broken if the inverse function  $D$  is found. However, if the complexity assumptions at the basis of some PKCS are correct, the computation time required to break it is too long to pose a real threat. In particular, PKCS could be broken by technological progress (new types of computers) and by mathematical

---

\*Computer Sciences Department, Technion, Haifa 32000, Israel

†NTT Basic Research Laboratories, 3-1 Morinosato Wakamya, Atsugi, Kanagawa 243-01, Japan

‡Department of Physics, Technion, Haifa 32000, Israel