International Journal of Innovative Computing, Information and Control
Volume **4**, Number **5**, May **2008**

ICIC International ©2008 ISSN 1349-4198
pp. **1043–1053**

AN ENHANCEMENT OF QUANTUM KEY DISTRIBUTION PROTOCOL WITH NOISE PROBLEM

Feng-Tse Lin

Department of Applied Mathematics
Chinese Culture University
Yangminshan, Taipei, Taiwan
ftlin@faculty.pccu.edu.tw

Received February 2007; revised August 2007

Abstract. *An enhanced version of the quantum key distribution (QKD) protocol in quantum cryptography is proposed. We consider that realistic detectors and imperfect devices may introduce noise into the transmission thereby causing a high error rate. The proposed scheme is based on an error rate analysis and a random sampling procedure in statistics to produce a probabilistic bound on the error estimation. Confidence intervals are used to interpret the error estimate with a specified confidence level. Based on the information obtained, Alice and Bob judge what caused the errors and establish confidence levels for the error rate of the remaining untested bits. Hence, they can determine the maximum number of times reconciliation needs to be performed to remove all errors from what remains of a raw key to produce an error-free secret key. As a result, the tedious reconciliation process can be reduced and a neglectful probability of not detecting the existence of remaining errors can be avoided as well. The privacy amplification is then applied: (1) to extract a secret key from a partially secret key, and (2) to enlarge the length of the secret key into the final key. The proposed scheme can work when dealing with errors caused by random noise and eavesdropping.*

Keywords: Quantum key distribution, Quantum cryptography, Confidence intervals, Random sampling, Reconciliation, Privacy amplification

1. **Introduction.** Cryptography has a long history of military and diplomatic applications dating back 2000 years ago when Julius Caesar used a simple substitution cipher, known as the Caesar cipher [4]. The purpose of cryptography is to transmit messages in such a way that access is restricted entirely to the intended recipient. Today, cryptography is becoming increasingly important in commercial and business applications. It is generally assumed that Alice (the sender) has some plaintext she wishes to send to Bob (the receiver), and Eve (an eavesdropper) always tries to gain access to the plaintext. All modern cryptosystems can be divided into two major groups, symmetrical and asymmetrical algorithms. Symmetrical algorithms, also known as secret-key or single-key cryptosystems, in which both Alice and Bob share a piece of information (a key), that is supposedly unknown to Eve. The key is applied each time for encryption and decryption. In contrast, asymmetrical algorithms, also called public-key or two-key cryptosystems, use a pair of keys. One of them is called the public key, which is used for encryption, and the other, called the private key, is used for message decryption [4,5].

A major problem in the practical use of symmetrical cryptosystems is the key distribution problem. This problem occurs because both Alice and Bob must hold a copy of the key, and must also prevent Eve from gaining a copy of the key. Consider a system with 1000 users, all of whom wish to communicate in secret with each other. In this case, each individual must hold a key for every individual except himself. That is, 999 keys for