A Practical Protocol for Three-party Authenticated Quantum Key Distribution

Dah-Jyh Guan, Yuan-Jiun Wang, and E. S. Zhuang

Department of Computer Science

National Sun Yat-sen University
Kaohsiung, Taiwan, R.O.C.

Abstracts:

Recently, Hwang et al. proposed two three-party authenticated quantum key distribution protocols for two communicating parties to establish a session key via a trusted center. They also showed their protocols were secure by using random oracle model. However, their protocols were designed to run in an ideal world. In this paper we present a more practical protocol by considering some issues which have not been addressed in their protocols. These issues include (1) session key consistence, (2) online guessing attack, and (3) noise in quantum channels. To deal with these issues, we use error correction code and key evolution. We also give a formal proof for the security of our protocols by using standard reduction, instead of the random oracle model.