Summary: Ma et al. [Int. J. Theor. Phys. (2021): 1328-1338] proposed a multi-party quantum key distribution (MQKD) protocol using Bell states, in which multiple participants can distribute a group key efficiently. However, this study indicates that Ma et al.’s protocol has two security loopholes. First, an attacker can obtain the pre-shared key $K_s$ using an eavesdropping attack. Second, the attacker uses an intercept-and-resend attack to steal the group key shared among the participants without being detected. An improved MQKD protocol is proposed to overcome these loopholes.

MSC:
- 81Pxx Foundations, quantum information and its processing, quantum axioms, and philosophy
- 68Pxx Theory of data
- 94A60 Cryptography

Keywords:
- quantum key distribution protocol
- eavesdropping attack
- intercept-and-resend attack

Full Text: DOI


[19] Hong, CH; Heo, JO; Khym, GL; Lim, J.; Hong, S-K; Yang, HJ, N quantum channels are sufficient for multi-user quantum key distribution protocol between n users, Opt. Commun., 283, 12, 2644-2646 (2010) - doi:10.1016/j.optcom.2010.02.037


This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.