URN etd-0407109-183716-1313
Author Tyng-Kwei Chang
Author's Email Address No Public.
Statistics This thesis had been viewed 36 times. Download 14 times.
Department
Year 2004
Semester 2
Degree Master
Type of Document Master's Thesis
Language zh-TW.Big5 Chinese
Title Researches of Quantum Key Distribution and Quantum Oblivious Transfer Protocols
Date of Defense 0000-00-00
Page Count 49
Keyword
No Any Keyword Information.

Abstract
Due to the rapid development of information technology, data communication is more frequent in the network. When two parties need to communicate in secret, they have to share a secret key in advance. The sender encrypts data, and then delivers it to the receiver. The receiver decrypts it using the same secret key. They can share the secret key by public key cryptography.
In order to against breaking, the length of the secret key has to be increased. However, even the length of the secret key is long, they still cannot against the attacks of quantum computers. Fortunately, Bennett and Brassard in 1984 proposed a BB84 quantum key distribution protocol, which is secure from the attack of quantum
computers.
Since BB84 protocol, the communication security has stepped forward to a new milestone. However, the key sharing efficiency is only 50% in BB84 protocol. Therefore, this master thesis will propose two new protocols: The first one is Bases Probability Adjustment (BPA); The second one is Preset Bases Quantum Key Distribution Protocol. These two protocols can improve the key sharing efficiency without affecting the security of BB84.
Another research topic of this master thesis is quantum oblivious transfer. It will introduce CrU+E9peau’s 1-out-of-2 quantum oblivious transfer protocol in 1994, and show how to use quantum bit commitment mechanism to prevent the storage attack. This thesis also proposes 1-out-of-2, 1-out-of-n, and m-out-of-n quantum oblivious transfer protocols.
Advisory Committee - advisor

Files etd-0407109-183716-1313-001.pdf

indicate access worldwide
Date of Submission 2005-07-20