URN etd-0407109-183724-1973
Author Chien-Chih Wang
Author's Email Address No Public.
Statistics This thesis had been viewed 36 times. Download 24 times.
Department
Year 2004
Semester 2
Degree Master
Type of Document Master's Thesis
Language zh-TW.Big5 Chinese
Title Study on verifiable oblivious transfer
Date of Defense 0000-00-00
Page Count 46

Keyword
Information security
Cryptography
Oblivious transfer
Verifiable
Same message attack

Abstract
With the development of network, more and more trade and data transmitting are taking place in the internet. So that how to ensure the safety of data transmitting is an important subject. The design of the cryptography has offered a method to secretly transmit information in the public network. A safe, practical cryptography can help us to transmit information in the public network effectively and safey. Oblivious transfer protocol is a quite important tool that is used for designing a cryptographic protocol. It has already applied to a lot of relevant cryptosystems. So, it is quite important to study a safe and efficient oblivious transfer protocol.
Since the first oblivious transfer protocol proposed by Rabin in 1981, it has already become a very important cryptographic technology. A lot of oblivious transfer protocols have been developed, e.g.1 out of 2 oblivious transfer, non-interactive 1 out of 2 oblivious transfer, and 1 out of n oblivious transfer,etc. Oblivious transfer protocols must keep two important characteristics: sender’s privacy and receiver’s privacy. In receiver’s privacy: the receiver learns some information about the input from the sender and it does not allow the sender to figure out what the receiver has learned. Moreover, in the receiver’s privacy: the receiver cannot get other messages that he/she did not choose. On the basis of these two important characteristics, this thesis finds some 1out of n oblivious transfer protocols cannot against the same message attack. The reason that the same message attack can work is that the receiver cannot verify the messages sent by the sender. So that this thesis will show the secure flaw in these oblivious transfer protocols and improve them to against the same message attack.
In addition, Kurosawa and Duong proposed a new idea in 2004: how to design multiple-use 1-out-of-n oblivious transfer. This thesis also try to propose a verifiable oblivious transfer, which can be extended to be multiple-use 1-out-of-n oblivious transfer protocol.
Advisory Committee Lee Narn-Yih - advisor

Files etd-0407109-183724-1973-001.pdf

indicate access worldwide
Date of Submission 2005-07-14