URN etd-0407109-183713-1085
Author Chi-Hsuan Lin
Author's Email Address No Public.
Statistics This thesis had been viewed 39 times. Download 0 times.
Department
Year 2005
Semester 2
Degree Master
Type of Document Master's Thesis
Language zh-TW.Big5 Chinese
Title Reusable Oblivious Transfer Protocol
Date of Defense 0000-00-00
Page Count 62

Keyword
Oblivious transfer
Cryptography
Un-chosen message replay attack
Man in the middle attack
User authentication

Abstract
Oblivious transfer is an important and basic technique in the field of cryptography. Basically, an oblivious transfer protocol includes two parties, Sender and Receiver. Sender has many secrets, and Receiver can freely choose one from those secrets. However, Receiver's choice is a secret to Sender; Receiver learns nothing from the other secrets. Oblivious transfer protocols can be applied to private information retrieval, exchange secret, fair electronic contract signing, and Internet auction.
Oblivious transfer protocols often need to be reused in many applications. After the initial phase of oblivious transfer protocols is completed and the initial parameters can be used repeatedly, the computation cost and transmission cost will be reduced. However, some security problems could be appeared because of reuse. In 2005, Huang and Chang proposed an efficient t-out-of-n oblivious transfer protocol, but this protocol suffers from the un-chosen message replay attack. This thesis will propose a reusable oblivious transfer protocol, which can resist the un-chosen message replay attack.
Besides, Wu, Zhang, and Wang in 2003 proposed another t-out-of-n oblivious transfer protocol, which mentioned it cannot efficiently prevent the man-in-the-middle attack in an insecure channel. Hence, this study proposes two authenticated oblivious transfer protocols. One is an oblivious transfer protocol with explicated user authentication, and the other is an oblivious transfer protocol with implicated user authentication. Both protocols can efficiently avoid man-in-the-middle attack.
Advisory Committee Narn-Yih Lee - advisor

Files No Any Full Text File.
Date of Submission 2006-06-24