URN etd-0407109-183722-1783
Author Rih-Chen Liao
Author's Email Address No Public.
Statistics This thesis had been viewed 47 times. Download 0 times.
Department
Year 2006
Semester 1
Degree Master
Type of Document Master's Thesis
Language zh-TW.Big5 Chinese
Title 1 out of n Conditional Oblivious Cast Protocol
Date of Defense 0000-00-00
Page Count 70

Keyword
oblivious transfertransfer
conditional oblivious transfer
conditional oblivious transfer
homomorphic encryption
cryptography

Abstract
Oblivious transfer protocol is an important basic technology in cryptography. It includes two parties: Sender and Receiver, where sender wants to convey secret values to receiver, and receiver can choose the secret value he wanted. But the sender cannot know which secret value the receiver chose. Moreover, the receiver cannot get any secret values that he did not choose. According to the amount of information that the sender holds and the amount of information that the receiver can choose, oblivious transfer protocols canbe classified as original oblivious transfer plotocol, 1 out of 2 oblivious transfer protocol, 1 out of n oblivious transfer protocol and t out of n oblivious transfer protocol. Conditional oblivious transfer protocol is that a public predicate is used to evaluate the sender’s and receiver’s inputs, and Construction of conditional oblivious cast protocol is another varicnt of the COT. Those protocols are proposed in the types of 1 out of 2 conditional oblivious transfer protocol and 1 out of 2 conditional oblivious cast protocol. This thesis will propose a 1 out of n conditional oblivious transfer protocol and a 1 out of n conditional oblivious cast protocol by using additive homomorphic encryption and multiplicative homomorphic encryption technologies. Thes protocols can be used to enhance the efficiency and extend the applied enuironanent of oblivious transfer.
Advisory Committee Narn-Yih Lee - advisor

Files No Any Full Text File.
Date of Submission 2007-08-15