URN etd-0407109-183723-1870
Author Wei-Liang Tsai
Author's Email Address No Public.
Statistics This thesis had been viewed 45 times. Download 21 times.
Department
Year 2001
Semester 2
Degree Master
Type of Document Master's Thesis
Language zh-TW.Big5 Chinese
Title Dynamic Conference Key Agreement Protocol with Fault Tolerance
Date of Defense 0000-00-00
Page Count 59

Keyword
Cryptography
Digital signature
Fault tolerance
Conference-key agreement

Abstract
In order to hold a secure conference, the participators of the conference can use conference key distribution system to generate a common secret key and then exchange secret information.

At PKC 2000, Tzeng announced a new conference-key agreement protocol. This protocol can detect and exclude malicious users

from the conference.

Based on the Tzeng"s scheme, this master thesis will adopt group-oriented cryptographic systems to provide dynamic joining

and leaving on Tzeng"s scheme. It is more officient than the original Tzeng"s scheme.
Advisory Committee Narn-Yih Lee - advisor

Files etd-0407109-183723-1870-001.pdf

indicate access worldwide
Date of Submission 2002-07-01