URN etd-0407109-183715-1171
Author Jung Chic Chen
Author's Email Address No Public.
Statistics This thesis had been viewed 31 times. Download 11 times.
Department
Year 2004
Semester 2
Degree Master
Type of Document Master's Thesis
Language zh-TW.Big5 Chinese
Title Cryptographic systems based on symmetric balanced incomplete block design
Date of Defense 0000-00-00
Page Count 51
Keyword
Cryptography
Security
Conference key
Multi-proxy signature
Symmetric balanced incomplete block design

Abstract
Since internet is an open environment, everyone can access or communicate by network in everywhere. So, when internet becomes popular, everyone will concern about the questions of information security. This thesis will study and analyze two group-oriented cryptographic systems: conference key distribution system and multi-proxy signature scheme, respectively.
In 2002, Chung, Choi, Kim and Lee proposed an efficient conference key distribution system, which is generated by employing symmetric balanced incomplete block design. In Chung et al. protocol, the symmetric balanced incomplete block design can reduce the message overhead to in the case of , but it requires two rounds of message exchange. In 2004, Lee and Hwang further proposed an improved conference key distribution system. They also showed that Chung et al. protocol suffered several security problems, and proposed an improved protocol. Unfortunately, both Chung et al. protocol and Lee-Hwang protocol are insecure. This thesis will show that both Chung et al. protocol and Lee-Hwang protocol are vulnerable to the malicious participant conspiracy attack, and then propose an improved protocol.
For multi-proxy signature scheme, Lin-Wu-Hwang proposed a multi-proxy signature scheme for partial delegation with cheater identification in 2002. This thesis finds that Lin-Wu-Hwang scheme requires message overhead (where is the number of proxy signer) and one round of message exchange. Thus, this thesis will propose a multi-proxy signature scheme employing symmetric balanced incomplete block design, and reduces the message overhead to in the case of . During the multi-proxy signature generation phase, it only requires two rounds of message exchange.
The performance is very important for group-orientated cryptographic systems. Thus, this thesis reduces the message overhead employing symmetric balanced incomplete block design. Two improved protocol are more efficient than Chung et al. protocol and Lin-Wu-Hwang improved protocol.
Advisory Committee Narn Yih Lee - advisor

Files etd-0407109-183715-1171-001.pdf

indicate access worldwide
Date of Submission 2005-07-19