URN etd-0407109-183710-731
Author Ming-Kung Sun
Author's Email Address No Public.
Statistics This thesis had been viewed 49 times. Download 29 times.
Department
Year 2002
Semester 2
Degree Master
Type of Document Master's Thesis
Language zh-TW.Big5 Chinese
Title The Study of Threshold Partially Blind Signature
Date of Defense 0000-00-00
Page Count 43

Keyword
cryptography
discrete logarithm problem
restrictive
partially blind signature
threshold signature
public key
fair blind signature

Abstract
In this paper, we propose a threshold restrictive partially blind signature scheme based on the discrete logarithm problem. The original structure includes the following two concepts: one is the Harn's threshold signature scheme without the assistance of mutually trusted party which enables any or more out of signers to cooperate to generate a group-oriented signature, another is the Maitland-Boyd's restrictive partially blind signature which can reduce the size of e-cash database and it can make sure that common information is restricted in the blinding manipulations and avoid the double spending. The proposed scheme combines both above properties. It satisfies the demand for e-cash application and the security is based on Abe-Okamoto's scheme. The verification operation for signatures is simplified by the group public key.

In addition, we describe the Stadler et al.'s fair blind signature. Then, we will demonstrate that Hwang et al.'s claim is incorrect. So that the Stadler et al.'s first scheme still holds the untraceability property of the blind signature.
Advisory Committee Narn-Yih Lee - advisor

Files etd-0407109-183710-731-001.pdf

indicate access worldwide
Date of Submission 2003-07-11