URN etd-0407109-183710-734
Author Pei-Hsiu Ho
Author's Email Address No Public.
Statistics This thesis had been viewed 40 times. Download 0 times.
Department
Year 2002
Semester 2
Degree Master
Type of Document Master's Thesis
Language zh-TW.Big5 Chinese
Title The Study of Digital Signature with a Subliminal Channel
Date of Defense 0000-00-00
Page Count 53
Keyword
Cryptography
Covert communication
Digital signature
Undeniable signature
Subliminal channel
Convertible undeniable signature
Threshold system

Abstract
Simmons first proposed the concept of subliminal channel in 1983. Since then, many subliminal channels based on digital signatures are proposed. Up to now, only a fixed number of subliminal messages can be hidden in a digital signature and the content of the subliminal messages cannot be changed after the signature is generated. Moreover, the sender has to share a secret key with the subliminal receivers. Chaum and Antwerpen, in 1989, proposed the concept of the undeniable signature which cannot be verified without the signer’s cooperation. Later, Chaum also proposed a zero-knowledge undeniable signature scheme. A convertible undeniable signature is an undeniable signature and can be converted to a general digital signature. A (t,n) threshold scheme allows a secret to be shared among n users so that only t or more users can reconstruct the secret.

The aims of this Master thesis are as follows.

1. Integrate subliminal channels with an undeniable signature：A undeniable signature can be used to hide subliminal messages repeatedly. Moreover, the sender does not need to share any secret key with the subliminal receivers.

2. Combine subliminal channels with a convertible undeniable signature：We are going to propose a new scheme which can embed subliminal channels into a convertible undeniable signature scheme.

3. Combine subliminal channels with threshold system： We are going to propose the first threshold subliminal channel which can convey a subliminal message to a group of users. Deriving the subliminal message relies on the cooperation of t or more users in the group. Moreover, the validation of the subliminal message can be verified in the scheme.
Advisory Committee Narn-Yih Lee - advisor

Files No Any Full Text File.
Date of Submission 2003-06-30