URN etd-0407109-183713-1081
Author Huai Yi Huang
Author's Email Address No Public.
Statistics This thesis had been viewed 56 times. Download 29 times.
Department
Year 2004
Semester 2
Degree Master
Type of Document Master's Thesis
Language zh-TW.Big5 Chinese
Title Study on Chameleon Signatures and Its Application
Date of Defense 0000-00-00
Page Count 50
Keyword
Action attack
Passive attack
Digital signature
Chameleon signature
Chameleon hash
Threshold signature

Abstract
In the recently, because the Internet is developed very rapidly, and Asymmetric Digital Subscriber Line (ADSL) is cheaper, the Internet becomes a necessary service for families, users and enterprises, etc. However, people may lose their privacy because the malicious attackers' active attacks or passive attacks. Therefore, it is important to prove the validity of the digital documents. For this reason, digital signature technologies have been developed gradually. It denotes that the signer generates digital signatures by using his private key, and the receiver needs to use the signer's public key to verify the validity of the signature.
In 2000, Krawczyk and Rabin brought out a chameleon signature idea. It is a variant of undeniable signature scheme. The rightful receiver can prove the validity of signature. It can prevent falsely incriminate for signer. In verification phase, the receiver can prove the validity of signature, he/she does not need any interaction with the signer. Because of this characteristic, this technology can save communication and computation cost. The receiver cannot prove the validity of signature to third party, so it can provide the property of the non-transferability.
In 1984, Shamir introduced an Id-based signature idea, the technology is different from other public key systems. Its public key is user's identity, not like other public key systems. This thesis will propose an Id-based chameleon signature scheme, which are mainly based on the digital signature scheme proposed by Shamir in 1984 and the chameleon hash function.
Then, this thesis will propose two threshold chameleon signature schemes, which are mainly based on the digital signature scheme proposed by Krawczyk and Rabin in 2000. It can extend personal digital signature to threshold signatures. It also makes chameleon signatures more flexible.
Advisory Committee Narn Yih Lee - advisor

Files etd-0407109-183713-1081-001.pdf

indicate access worldwide
Date of Submission 2005-07-19