WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Sharing Secret with Multi Party Using Efficient Verifiable Threshold Algorithm

Dr. Renuka K[1], Miriam Phinehas. R[2]

[1]MSc., M.Phil., Ph. D, Assistant Professor, Department of computer science, Kovaipudur, Coimbatore, Tamil nadu, India
[2]Department of computer science, Sri Krishna Adithya college of arts and science, Kovaipudur, Coimbatore, Tamil nadu, India
miriamphinehas@gmail.com

ABSTRACT_

Secret sharing schemes are highly versatile cryptographic primitives and, as a result, have been employed in a vast range of different applications including protection of cryptographic keys, access control, key recovery mechanisms, electronic voting, distributed certificate authorities, online auctions and secure multiparty computation. They are also objects of inherent mathematical interest and have also been researched as such.

The access structure of a secret sharing scheme normally partitions the set of all subsets of participants into authorized sets who are able to recover the secret and unauthorized sets who cannot. (Some schemes feature a third class of subsets who are neither authorized or unauthorized.) The two fundamental properties of a secret sharing scheme are thus:

1. Privacy: Unauthorized subsets of participants should be prevented from learning the secret.

2. Recoverability: Authorized subsets of participants should be able to recover the secret by pooling their shares.

Secret sharing schemes also involve two functionalities that are, in many cases, carried out by a dedicated entity. The dealer is normally responsible for generating system parameters, generating the secret, creating initial shares and sending initial shares to participants. The combiner is responsible for pooling shares and reconstructing the secret. The dealer is normally a fully trusted third party, while the combiner is often left unspecified (but can be a third party or even one of the participants).In real life, it is dangerous to keep some sensitive and important information, such as passwords of opening bank safes or launching missiles, by a single person, because the information is easy to be damaged, lost or tampered. Therefore, it is urgent to establish novel key dispersion schemes. In the custody system, a secret sharing system is established, and it is an important method to protect information security and data security. Secret sharing has very important applications in modern cryptography, such as key distribution, access control, secure multi-party computing, e-commerce, and even the control of missile launches.

Existing system

The earliest secret sharing scheme is the threshold-based secret sharing scheme, which was proposed by Biakley and Shamir, respectively. In general, the system of secret sharing assumes that both dealer and participants are honest, but this is unrealistic in real life. Therefore, these systems cannot effectively stop the dealer from cheating the participants (the dealer distributes fake shares to some participants) and stop the participants from deceiving the other participants (some participants distribute false shares when reconstructing to the secret).

In order to solve these problems, several verifiable secret sharing schemes have been proposed. In these schemes, verification algorithm is added and participants can test whether the dealer distributes the false shares to restore the secret and moreover each participant can test whether other participants have provided a valid share. In several effective multi-secret sharing schemes have been proposed based on Shamir threshold scheme.

Drawbacks

- The shares are selected by the dealer and distributed to the participants through a secure channel.
- Since a secure channel needs to be established between the participant and the dealer, the scheme has relatively high requirements of the system.
- In a secret sharing scheme, dishonest participants and the dealer are likely to cheat the other participants during execution.

Proposed system

To alleviate these concerns, we improve our scheme with verifiability properties, such as variable and publicly verifiable secret sharing. Verifiability stops the dealer from sharing wrong shares and hence public verifiability forces participants to submit their sub-shares correctly.

In the dynamic secret sharing schemes, the main concern is the updates of secret and share, as well as the addition of new individuals or the deletion of the participant, which does not involve changes of the threshold value t. In the multi-secret sharing scheme, we propose a multi-stage secret sharing scheme, in which each secret corresponds to an independent threshold. When reconstructing multiple secrets with different threshold values, the secret holder needs to disclose part of the information in order to keep the number of shares saved by the participants as less as possible.

In our proposed scheme, the participants' share is generated independently and randomly which has nothing to do with a single secret. All the secrets are also generated independently and randomly. For each secret, the secret holder publishes its own independent public information in advance, and the corresponding threshold value of each secret is determined by its public information.

Features

- Our protocol provides a 2FA security
- Our protocol supports fine-grained attribute-based access which provides a great flexibility for the system to set different access policies according to different scenarios. At the same time, the privacy of the user is also preserved.

System specification

SOFTWARE SPECIFICATION

Operating System : Windows XP/8/10

Programming Language : Java

IDE : My Eclipse 6.0

HARDWARE SPECIFICATION

Processor : i5

RAM : 5GB

HDD : 1TB

Conclusion

This project will explore a new verifiable threshold algorithm multi-secret sharing scheme and outsource the process of the secret reconstruction to the cloud service provider. Our proposed scheme enjoys four advantages such as the multiple secret sharing, the privacy of the shared secrets, the efficient secret reconstruction, and the efficient verification of the share and the returned result. The last two properties are thanking to the outsourcing computation of the secret reconstruction and the share verification. Furthermore, our proposed system supports the participants to recover the desired return as well as to identify the hacker.

Scope of future enchancement

We can also expect further developments in the formalization of models for such schemes, as only robust secret sharing schemes have been set in a framework compatible with much of the recent theoretical formalization of other types of cryptographic primitive. There would thus seem to remain some room in this area for further application of interesting mathematical techniques to provide secret sharing schemes with the capability of coping with sophisticated adversarial behavior.