Abstract

The idea of secret sharing is to start with a secret, divide it into pieces called shares, which are then distributed amongst participants by the dealer. Only certain authorized subsets of participants can reconstruct the original secret. Applications for secret sharing schemes seem to be getting more important nowadays. For many circumstances, secret sharing has to provide more flexibility and functionality as per the need of an application. Secret Sharing has been an active research field for many years. Various secret sharing techniques have been developed to secure data, but there is a need to implement a secret sharing scheme with all augmented capabilities like general access structure, robustness against cheating shareholders, verifiability of the shares, proactive redistribution of shares etc. The intent of this paper is to explain the extended capabilities of secret sharing schemes and analyze the relation in application semantics and multifarious secret sharing schemes.

References

- Benaloh, J., and J. Leichter, Generalized secret sharing and monotone functions, CRYPTO &apos;88, Springer Verlag, pp. 27-35.
- Sai-zhi Ye, Guo-xiang Yao, Quan-long Guan, "A multiple secret sharing scheme with general access structure," International Symposium on Intelligent Ubiquitous Computing and Education, 2009 IEEE.
Index Terms

Computer Science  Security

Keywords

Security  Secret Sharing  Multi Functionality  Extended Capabilities  Cryptography