Abstract

Multi secret sharing is an extension of secret sharing technique where several secrets are shared between the participants, each according to a specified access structure. The secrets can be reconstructed according to the access structure by participants using their private shares. Each participant has to hold a single share, additional information are made available in a public bulletin board. The scheme is computationally efficient and also each participant can verify the shares of the other participants and also the reconstructed secret. The scheme doesn’t need any secure channel also.

References

- Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation. In Proceedings of the twentieth
University of Science and Technology, 2009.

Index Terms

Computer Science

Security

Keywords

access structure dynamic participants cheating detection