Generalized Secret Sharing Schemes using N-mu-MDS Codes

Dr. Vishal Saraswat

Robert Bosch India Limited

Secret sharing schemes are one of the essential mechanisms for safeguarding secret information and have found many applications in modern cryptographic protocols such as distributed computing, secure multiparty computations, threshold cryptography, attribute-based encryption, access control, generalized oblivious transfer and Byzantine agreement.

We propose an N-mu-MDS codes based efficient generalized secret sharing scheme which is ideal and perfect and has the desirable security features of cheating detection and cheater identification.