A Novel Threshold Changeable Secret Sharing Scheme

Lein HARN, Chingfang HSU, Zhe XIA

Frontiers of Computer Science, DOI: 10.1007/s11704-020-0300-x

Problems & Ideas

- Problems: Recently, a new secret sharing scheme based on a bivariate polynomial is proposed in which shares generated initially by a dealer can be used not only to reconstruct the secret but also to protect the secrecy of shares when the secret reconstruction is performed over a network. This scheme is not a threshold changeable secret sharing (TCSS).
- Ideas: We further extend this scheme to enable it to be a TCSS without any modification. Our proposed TCSS is dealer-free and non-interactive. Shares generated by a dealer in our scheme can serve for three purposes, (a) to reconstruct a secret; (b) to protect the secrecy of shares if secret reconstruction is performed over a network; and (c) to enable the threshold changeable property.

Main Contributions

- **It is the first secret sharing scheme which can support both secret reconstruction over a network and TCSS simultaneously.**
- **The proposed secret sharing scheme is almost the same as the original Shamir's secret sharing scheme except that an asymmetric bivariate polynomial is used to replace a univariate polynomial.**
- **The TCSS is a dealer-free and non-interactive. So, it requires low overheads on computation and communication.**
- **We believe that the same design principle can be generalized to other secret sharing scheme based on bivariate polynomials such as based on a symmetric bivariate polynomial, to enable TCSS.**