A Secret Sharing Scheme Without Third-Party Dealers

Kim, Minwoo (School: Korea Science Academy of KAIST)
Lee, Taehyun (School: Korea Science Academy of KAIST)
Jeon, Gunwook (School: Korea Science Academy of KAIST)

Secret sharing refers to a class of protocols for splitting a given secret into several shares and distributing them to a group of participants, who can later reconstruct the secret. All the existing secret sharing schemes rely extensively on third-party dealers. Since the third-party dealer has full control over the secret, information leakage from a malicious dealer is a risk. Therefore, it is unrealistic to assume that all participants can trust a third-party dealer. This research proposes an improved secret sharing scheme that does not rely on third-party dealers. Our scheme is designed to have the effect of replacing potentially dishonest dealers with internal participants. As the internal participants play the role that external dealers originally carry out, our scheme prevents third-party members from accessing the secret. We also rigorously prove the information-theoretic security of our scheme, which implies that not even a single bit of information about the secret is leaked under our scheme. Additionally, we extend our scheme to be verifiable, allowing participants in hostile relationships to carry out the protocol without losing mutual trust. Secret sharing schemes proposed so far have not been actively used in situations where the leakage of secrets is fatal due to the potential risk caused by third-party dealers. Our technique, which eliminates this problem, can be used even in critical situations. Specifically, the proposed scheme can be directly applied to the security protocol for CCTV in medical operating rooms, which can settle down a serious controversy over mandatory CCTV installation.