Vector Space Secret Sharing Scheme and Efficient Secret Share Computing

Mustafa Atici, Western Kentucky University

The threshold scheme, the monotone circuit construction, and the vector space construction are some of the well-known secret sharing schemes in cryptography. The threshold and monotone circuit secret sharing schemes are fairly easy to construct for any given access structure Γ. The construction of a secret sharing scheme realizing a given access structure Γ with Vector Space Construction requires the existence of a function ϕ from a set of participants into a vector space, that is, $\phi : \mathcal{P} \longrightarrow (\mathcal{Z}_p)^d$. This function ϕ must satisfy certain conditions. There is no known algorithm to construct such a function ϕ in general. Constructions are mainly done by trial and error. In this paper, we develop polynomial algorithms to construct ϕ functions for vector space secret sharing scheme realizing certain types of access structures. Some examples are given to illustrate the algorithms.