A secret sharing scheme based on the polynomial ring over a finite field.

H. Tapia-Recillas*, Dpto. de Matemáticas, Univ. Autónoma Metropolitana-I, México, D.F.

Secret sharing schemes (SSSchs), independently introduced by Shamir and Blakley have since been then focus of several researches due to applications (including data protection) and the underlying mathematics on which several schemes are based. For example, there are SSChs based on polynomial interpolation (Shamir), linear codes over a finite field, using boolean function with special properties (bent functions). The general framework of a SSSch can be stated as follows: a secret datum S has to be distributed among a set of participants $\mathcal{P} = \{P_0.P_1, ..., P_n\}$ and each participant P_i receives a piece of the secret (share) s_i such that from the shares of qualified subsets of participants the secret S can be recovered; however, the secret can not be recovered from a non-qualified subset of participants. In this talk, a SSSch is presented based on the ring of polynomials in one variable over a finite field. Its robustness is based on the fact that the number of polynomials is large particularly if the degree is large. An example is given to illustrate the main idea of the scheme.

Keywords: secret sharing scheme, polynomial ring, finite field.