Linear key predistribution schemes

Carles Padró, Ignacio Gracia, Sebastià Martín*, Paz Morillo
Dept. Matemàtica Aplicada i Telemàtica
*Dept. Matemàtica Aplicada II
Universitat Politècnica de Catalunya (UPC)
Jordi Girona 1-3
08034 Barcelona
Spain
Tel. +34 93 4016041
Email: smartin@ma2.upc.es

27 April 2000

Keywords: cryptographic protocols, key predistribution schemes, broadcast encryption, information rates.

In a key predistribution scheme (KPS), some secret information is distributed among a set of users. This secret information must enable every user in some specified privileged groups to compute a common key associated to that group. Besides, this common key must remain unknown to some coalitions of users outside the privileged group. The information rate, that is, the ratio between the length of the key and the maximum length of the secret information given to the users, is the main parameter to measure the efficiency of a KPS.

We present in this poster a general model, based on Linear Algebra techniques, for the design of key predistribution schemes that unifies all previous proposals. This model provides a better understanding of KPS and can be a useful tool for future proposals. Concretely, our model makes easier the verification of the security requirements in a KPS, namely, that every authorised user can obtain the common key associated to a privileged set and no forbidden coalition of non-authorised users obtains any information about that key.

We present two methods to construct KPS, and two new families are given by using these methods. Some of the schemes in these families heve better information rates than the KPS in the previous proposals. Some KPS that are suitable for situations that were not previously considered are also found in those families.