Section 06: Discrete Mathematics and Computer Science | Poster number 365

Linear broadcast encryption schemes

Ignacio Gracia, Matemàtica Aplicada i Telemàtica, UPC.
Sebastià Martín*, Matemàtica Aplicada 2, UPC.
Paz Morillo, Matemàtica Aplicada i Telemàtica, UPC.
Carles Padró, Matemàtica Aplicada i Telemàtica, UPC.

ABSTRACT

The scenario in broadcast encryption consists of a trusted authority (TA) and a set of users in a broadcast network, in which any one connected to the network can access all the information that flows through it. A *broadcast encrytpion scheme* must enable the TA to send a secret message through the network in such a way that only the users in a certain privileged subset, which is not fixed in advance, can obtain it. We are interested in *unconditionally secure* schemes, that is, schemes whose security do not depend on any computational assumption. Broadcast encryption has a wide range of applications: multiparty conferences, on-line games, pay TV, etc.

A *broadcast encryption scheme* consists of two phases. The first one is the *key predistribution phase*, which has to be done off-band, that is, by using secure channels outside the broadcast network. In this phase, every user privately receives a personal key from the TA. The *message broadcast phase* begins once a privileged subset of users is determined. In this phase, the TA sends through the network an encrypted message. Every user in the privileged subset can decrypt the message by using its personal key and certain coalitions of users outside the privileged subset can not obtain any information about the message.

A simple solution is to give every user its own key and transmit an individually encrypted message to every member of the privileged subset. This requires a very long transmission. Another simple solution is to provide every possible privileged subset of users with a key. This requires every user to store a huge number of keys. Some non-trivial broadcast encryption schemes have been proposed in order to obtain a trade-off between the length of the broadcast message and the amount of secret information stored by the users.

We present in this poster a new model, based on Linear Algebra techniques, for the design of unconditionally secure broadcast encryption schemes that unifies and includes all previous proposals. This new model provides a common mathematical formulation and a better understanding of such schemes. Moreover, new families of broadcast encryption schemes can be constructed by using this model.

Keywords: *Cryptology, key distribution, broadcast encryption*

Mathematics Subject Classification: *94A60*

Contact Address: `smartin@ma2.upc.es`