Section 06: Discrete Mathematics and Computer Science | Poster number 578

General key predistribution scheme

Germán Sáez, Univ. Politècnica de Catalunya.

ABSTRACT

One of the major problems in communication and network security is key distribution. From the point of view of security, most network can be thought of as broadcast networks, in that anyone connected to the network will have access to all the information that flows through it. This leads to many problems related to the confidentiality and authenticity that is transmitted through the network. This paper is related to one problem: key predistribution schemes. The usual scenario in a *key predistribution scheme* is the following: a center wishes to broadcast some secret key (e.g. a key to decipher some TV program in a pay-per-view television broadcast) to a privileged subset of users in such a way that a family of forbidden subsets of users can not obtain any information of the value of the key. This must be done for every privileged subset (and family of forbidden sets of users) with protocols that provide unconditional security (i.e. they are not based on any computational assumption). The key predistribution schemes are based in a predistribution of information among the users.

Because every user in a privileged subset should be able to compute individually the secret key, the obvious solution is to give every user its own secret key (one for each privileged subset in which the user belongs to). It is easy to imagine that the amount of information that every user must keep secret can be too big. A better key predistribution scheme was presented in [3] by A. Fiat and M. Naor for any subset P of privileged users with forbidden subsets the collection of disjoint subsets with P of cardinality at most t. The Fiat-Naor key predistribution scheme distributes information in an optimal way (see [1] for more details). Some other key predistribution schemes have been presented (see [6] for more schemes).

We present in this poster a key predistribution scheme for a general family of privileged subsets and general family of forbidden subsets of users. We use in this key predistribution scheme some tools of *secret sharing schemes* (see [4, 5] for a comprehensive introduction), mainly the *vector space secret sharing scheme* due to Brickell [2]. The Fiat-Naor key predistribution scheme is produced as a particular case of this construction. We give some bounds on the amount of information that must be kept secret by the users.

References

[1] C. Blundo and A. Cresti. Space Requirements for Broadcast Encryption. *Advances in Cryptology EUROCRYPT'94. Lecture Notes in Computer Science*, **950** (1995) 287–298.

[2] E.F. Brickell. Some ideal secret sharing schemes. *J. Combin. Math. and Combin. Comput.*, **9** (1989) 105–113.

[3] A. Fiat and M. Naor. Broadcast Encryption. *Advances in Cryptology CRYPTO'93. Lecture Notes in Computer Science*, **773** (1994) 480–491.

[4] D.R. Stinson. An explication of secret sharing schemes. *Designs, Codes and Cryptography* **2** (1992) 357–390.

[5] D.R. Stinson. *Cryptography: Theory and Practice*. CRC Press Inc., Boca Raton (1995).

[6] D.R. Stinson. On Some Methods for Unconditionally Secure Key Distribution and Broadcast Encryption. *Designs, Codes and Cryptography*, **12** (1997) 215–243.

Keywords: *key predistribution scheme, cryptography, Fiat-Naor key predistribution scheme, secret sharing schemes*

Mathematics Subject Classification: *94A60, 68P25, 11T71, 11Y16, 11Y40*

Contact Address: `german@mat.upc.es`