Broadcast Encryption

Paz Morillo, Ignacio Gracia and Sebastià Martín,*
Dpt. de Matemàtica Aplicada y Telemàtica, E.T.S.E.T.B.
C3, Campus Nord, c/ Jordi Girona 1-3, 08034 Barcelona
Tel 401 60 08, Fax 401 59 81, e–mail: paz@mat.upc.es
** Dpt. de Matemàtica Aplicada II, E.T.S.E.I.T.*
c/ Colom 11, 08122 Terrassa, Barcelona
Tel 739 81 64, e–mail: smartin@ma2.upc.es

We consider scenarios where there is a center and a set of users. At some moment, the center wishes to send a message (e.g. a key to decipher a TV programme) to a privileged subset of the users, through an open channel, in such a way that non-members of the privileged class cannot learn the message. Of course, the message must be encypted.

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 subset of users with a key. This requires every user to store a huge number of keys.

Since there exists a trade-off between transmission length and keys storage, two parameters are considered to measure the efficiency of a broadcast encryption scheme: he amount of secret information stored by each user as compared to the information content, and the size of the broadcast as compared to its information content.

Broadcast encryption has a wide range of applications: video multi-party conferences, on-line games, pay TV, etc.

In this talk, we provide a survey of the main broadcast encryption schemes designed so far. In 1993, Fiat and Naor [1] proposed one of the first schemes which focuses on avoiding that a coalition of at most k non-authorized users have access to the information being broadcast. Blundo, Frota and Stinson [2]

provide new techniques to design broadcast encryption schemes, resilient to predetermined subsets of users. In [3], Stinson gives a broadcast encryption scheme, using secret sharing schemes, efficient in some cases. Another aspect studied in the literature about he subject, and important in database access systems, is traitor tracing. Chor, Fiat and Naor [4] gave a scheme that allows tracing the source of leaks when a non-authorized decoder has been captured. In many settings, the set of users is dynamic; therefore efficient key redistribution schemes are required. Canetti, Malkin and Nissim [5] design such a scheme based on binary balanced trees.

References

[1] A. Fiat, M. Naor. Broadcast encryption. Proceedings of Crypto'93.

[2] C. Blundo, L.A. Frota, D.R. Stinson. Trade-offs between communication and storage in unconditionally secure schemes for broadcast encryption and interactive key distribution. Proceedings of Crypto'96.

[3] D.R. Stinson. On some methods for unconditionally secure key distribution and broadcast encryption. Designs, codes and cryptography (1997).

[4] B. Chor, A. Fiat, M. Naor. Tracing traitors. Proceedings of Crypto'96.

[5] R. Canetti, T. Malkin, K. Nissim. Efficient communication-storage tradeoffs for multicast encryption. Proceedings of Eurocrypt'99.