On some methods for unconditionally secure key distribution and broadcast encryption

D. R. Stinson
Department of Computer Science and Engineering
and Center for Communication and Information Science
University of Nebraska-Lincoln
Lincoln NE 68588, USA

Abstract

In this talk, we discuss methods by which a trusted authority can distribute keys and/or broadcast a message over a network, so that each member of a specified privileged subset of users can compute a key or decrypt the broadcast message. Moreover, this is done in such a way that no forbidden coalition is able to recover any information on any a key (or broadcast message) they are not supposed to know.

These problems are studied in the setting of information theory, so the security provided is unconditional (i.e., it is not based on any computational assumption).

We give a brief survey of some of the more elegant key distribution schemes, such as the Blom scheme (and the generalization due to Blundo *et al*) and the Fiat-Naor scheme. As well, we describe a general method of constructing broadcast schemes by combining key distribution schemes with secret sharing schemes. The 1993 Fiat-Naor broadcast scheme can be viewed in this way, and new schemes can also be produced by this method. This approach also leads to the investigation of various combinatorial problems that seem to be of independent interest.