# CORR 2000-21

## Metering Schemes for General Access Structures

**Barbara Masucci* & Douglas R. Stinson**

**Abstract** A *metering scheme* is a method by which an audit agency is able to measure the interaction between servers and clients during a certain number of time frames. Naor and Pinkas [7] considered schemes in which any server is able to construct a cryptographically secure *proof* if and only if it has been visited by at least a number, say $h$, of clients in a given time frame.

In this paper we construct metering schemes for more general access structures, which include *multilevel* and *compartmented* access structures. Metering schemes realizing these access structures have useful practical applications: for example, they can be used to measure the interaction of a web site with a specific audience which is of special interest. We also prove lower bounds on the communication complexity of metering schemes realizing general access structures.

**Keywords** Distributed Audit, Metering, Security, Cryptography, Entropy.