CORR 2000-18

dynamic Multi-Threshold Metering Schemes

Carlo Blundo*, Annalisa De Bonis*, Barbara Masucci* &
Douglas R. Stinson

Abstract A *metering scheme* is a method by which an audit agency is able to measure the interaction between clients and servers on the web during a certain number of time frames. Naor and Pinkas [7] considered metering schemes in which any server is able to construct a proof to be sent to the audit agency if and only if it has been visited by at least a number, say h, of clients in a given time frame. In their schemes the parameter h is fixed and is the same for any server and any time frame. This is acceptable whenever there is a long-term relationship between the audit agency and the servers.

In order to measure any number of visits in any granularity we introduce *dynamic multi-threshold metering schemes*, which are metering schemes in which there is a threshold h_j^t associated to any server S_j for any time frame t. We mainly focus on the efficiency of dynamic multi-threshold metering schemes, providing lower bounds on the size of the information distributed to clients and servers (this is important otherwise the task of receiving and sending information would burden the clients, that are not interested in the metering process).

Keywords Metering Schemes, Security, Cryptography, Entropy.