“Certified Information Access”
C. Blundo

Abstract:
Certified Information Access (CIA) primitives allow a User to obtain answers to database queries in a way that she can verify the correctness of the received information. The database answers to a query by providing the information matching the query along with a proof that such information are consistent with the actual content of the database. Current solutions to this problem require a computationally intensive setup phase. We describe an implementation of a CIA service by means of a Web computing library. In our system, the setup phase is completely and securely outsourced to a web-cluster. A key issue to be considered is the need of guaranteeing on one hand the confidentiality of the database contents and, on the other hand, the correctness and soundness of the answers obtained by the users.

We argue that classical cryptographic primitives are not sufficient for our purposes. To this aim we introduce a new primitive the "Verifiable Deterministic Envelope" which may be of independent interest.