Cryptology ePrint Archive: Report 2011/132

Verifiable Delegation of Computation over Large Datasets

Siavosh Benabbas and Rosario Gennaro and Yevgeniy Vahlis

Abstract: We study the problem of computing on large datasets that are stored on an untrusted server. We follow the approach of \emph{amortized verifiable computation} introduced by Gennaro, Gentry, and Parno in CRYPTO 2010. We present the first practical verifiable computation scheme for high degree polynomial functions. Such functions can be used, for example, to make predictions based on polynomials fitted to a large number of sample points in an experiment. In addition to the many non-cryptographic applications of delegating high degree polynomials, we use our verifiable computation scheme to obtain new solutions for verifiable keyword search, and proofs of retrievability. Our constructions are based on the DDH assumption and its variants, and achieve adaptive security, which was left as an open problem by Gennaro \etal (albeit for general functionalities).

Our second result is a primitive which we call a \emph{verifiable database} (VDB). Here, a weak client outsources a large table to an untrusted server, and makes retrieval and update queries. For each query, the server provides a response and a proof that the response was computed correctly. The goal is to minimize the resources required by the client. This is made particularly challenging if the number of update queries is unbounded. We present a VDB scheme based on the hardness of the subgroup membership problem in composite order bilinear groups.

Category / Keywords: cryptographic protocols / verifiable computation, diffie-hellman, bilinear maps

Publication Info: An extended abstract of this paper will be published in the proceedings of Crypto'11

Date: received 15 Mar 2011, last revised 11 Jul 2011

Contact author: evahlis at cs columbia edu