Cryptology ePrint Archive: Report 2011/587

Publicly Verifiable Delegation of Computation

Charalampos Papamanthou, Elaine Shi, and Roberto Tamassia

Abstract: We initiate the study of \textit{publicly verifiable computation}, which generalizes authenticated data structures, and verifiable computation in the secret-key setting. In publicly verifiable computation, a trusted source outsources an application (algorithm) to an untrusted server. Any client can ask the server to run the application over some given inputs, and the server can produce a witness vouching for the correctness of the outcome. We propose publicly verifiable computation schemes supporting expressive manipulations over multivariate polynomials, such as polynomial evaluation and differentiation. Our scheme allows the client to verify the outcome in time proportional to the size of the input, and not depending on the degree and the description of the polynomial, i.e., in asymptotically less time than performing the computation locally. Moreover, our scheme allows the source to efficiently update the polynomial coefficients without performing expensive recomputations proportional to the size of the polynomial.

Category / Keywords: public-key cryptography / verifiable computation

Date: received 29 Oct 2011, last revised 2 Nov 2011

Contact author: cpap at cs berkeley edu