Cryptology ePrint Archive: Report 2012/726

Applications of Polynomial Properties to Verifiable Delegation of Computation and Electronic Voting

Marc Obrador and Paz Morillo and Sandra Guasch

Abstract: This paper presents some proposals of protocols for two types of schemes such as verifiable delegation of computation and remote electronic voting, based on polynomial properties. Our protocols for verifiable delegation of computation are aimed to the efficient evaluation of polynomials, working on schemes where the polynomial and/or the input are kept secret to the server. Our proposal for remote electronic voting allows the verification of vote well-formation upon reception at the voting server, with little overhead of computations for the voter.

Category / Keywords: cryptographic protocols / delegation of computation, verifiable, electronic voting

Date: received 28 Dec 2012, last revised 30 Dec 2012

Contact author: sandra guasch at scytl com

Available formats: PDF | BibTeX Citation

Note: Minor corrections for broken references.

Version: 20121230:143502 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]