Cryptology ePrint Archive: Report 2011/605

Efficient and Secure Delegation of Linear Algebra

Payman Mohassel

Abstract: We consider secure delegation of linear algebra computation, wherein a client, \emph{privately} and \emph {verifiably}, outsources tasks such as matrix multiplication, matrix inversion, computing the rank and determinant, and solving a linear system to a remote worker.

When operating on $n \times n$ matrices, we design non-interactive, and secure protocols for delegating matrix multiplication, based on a number of encryption schemes with limited homomorphic properties where the client only needs to perform $O (n^2)$ work. The main component of these delegation protocols is a mechanism for efficiently verifying the \emph {homomorphic matrix multiplication} performed by the worker. We introduce a general method for performing this verification, for any homomorphic encryption scheme that satisfies two special properties. We then show that most existing homomorphic encryption schemes satisfy these properties and hence can utilize our general verification method. In case of the BGN-style encryption of [Gentry et al., EUROCRYPT 2010], we also show a simpler and more efficient verification method that does not follow our general approach.

Finally, we show constant round and efficient constructions for secure delegation of other linear algebra tasks based on our delegation protocol for matrix multiplication. In all of these constructions, the client's work is at most $O(n^2\log n)$. Our constructions can also be efficiently transformed to \emph{server-aided protocols} for secure two-party computation of linear algebra with similar efficiency.

Category / Keywords: cryptographic protocols /

Date: received 8 Nov 2011

Contact author: pmohasse at cpsc ucalgary ca