Cryptology ePrint Archive: Report 2011/456

Delegation of Computation without Rejection Problem from Designated Verifier CS-Proofs

Shafi Goldwasser, Huijia Lin, Aviad Rubinstein

Abstract: We present a designated verifier CS proof system for polynomial time computations. The proof system can only be verified by a designated verifier: one who has published a public-key for which it knows a matching secret key unknown to the prover. Whereas Micali's CS proofs require the existence of random oracles, we can base soundness on computational assumptions: the existence of leveled fully homomorphic encryption (FHE) schemes, the DDH assumption and a new knowledge of exponent assumption. Using our designated verifier CS proof system, we construct two schemes for delegating (polynomial-time) computation. In such schemes, a delegator outsources the computation of a function F on input x to a polynomial time worker, who computes the output $y=F(x)$ and proves to the delegator the correctness of the output.

Let T be the complexity of computing F on inputs of length $n=\abs x $ and let k be a security parameter. Our first scheme calls for an one-time off-line stage where the delegator sends a message to the worker, and a non-interactive on-line stage where the worker sends the output together with a certificate of correctness to the prover per input x. The total computational complexity of the delegator during off-line and on-line stages is $ \poly(k, n, \log T)$. Compared with previous constructions by Gennaro-Gentry-Parno and Chung-Kalai-Vadhan~\cite{GGP10, CKV10} based on FHE, their on-line stage consists of two messages and their off-line stage has (delegator's) complexity of $\poly(k,n, T)$. Thus, they achieve delegator complexity $\poly (k, n, \log T)$ only in an amortized sense. Compared with the construction of \cite{GKR08} based on poly-log PIR, our first construction can handle any polynomial-time computable F rather than being restricted to $\NC$ computable F. Our second scheme requires no off-line stage and has a two-message ``on-line'' stage with complexity of $\poly(k, n, \log T)$. Most importantly, it achieves {\em robust soundness} that guarantees that it is infeasible for a cheating worker to convince the delegator of an invalid output even if the worker learns whether the delegator accepts or rejects previous outputs and proofs. Previously the only two-round protocol that achieves robust soundness under a computational assumption appeared in \cite{GKR08} and is restricted to only $\NC$ computations.

Category / Keywords: Extractable Collision Resistant Hash Function, Designated Verifier CS Proofs, Delegation, Knowledge of Exponent Assumption

Date: received 18 Aug 2011, last revised 18 Aug 2011

Contact author: huijia at cs cornell edu, aviadrub@mail tau ac il, shafi@theory csail mit edu