Cryptology ePrint Archive: Report 2011/518

Two 1-Round Protocols for Delegation of Computation

Ran Canetti and Ben Riva and Guy N. Rothblum

Abstract: Consider a weak client that wishes to delegate computation to an untrusted server and be able to succinctly verify the correctness of the result, all within one round of interaction. We provide solutions for two relaxed variants of this problem. Specifically:

\begin{itemize}

\item We consider a model where the client delegates the computation to {\em two or more} servers, and is guaranteed to output the correct answer as long as even a {\em single} server is honest. We call this model \emph{Refereed Delegation of Computation (RDoC)}. In this model, we show a 1-round {\sf unconditionally statistically sound} protocol for any log-space uniform $\mathcal{NC}$ circuit. In contrast, all known one-round delegation protocols with a single server are only computationally sound.

\item We consider a model with a non-succinct offline stage and {\sf pubic verifiability.} (Previously, this model was considered only with private verifiability, namely the client has to maintain some secret local information pertaining to the offline stage [Gennaro et al., CRYPTO 2010]). Public verifiability does away with the secret state, and so allows delegating the offline stage to a ``semi-trusted" external third party that is potentially used by many clients, even mutually suspicious ones. It also allows for a stronger, more adaptive notion of soundness. In this model we show a 1-round computationally-sound protocol for any circuit C, {\em even a non-uniform one}. The client runs in time $poly(log(size(C)), depth(C))$, and soundness is guaranteed assuming the existence of collisions resistant hashing and poly-logarithmic PIR. Previously, publicly verifiable one round delegation protocols were known only for functions in log-space uniform $\mathcal {NC}$.

\end{itemize}

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

Date: received 20 Sep 2011, last revised 20 Sep 2011

Contact author: benriva at post tau ac il