Cryptology ePrint Archive: Report 2011/553

Non-Interactive Time-Stamping and Proofs of Work in the Random Oracle Model

Mohammad Mahmoody and Tal Moran and Salil Vadhan

Abstract: We construct a non-interactive scheme for proving computational work in the Random Oracle Model. Given a uniformly random ``puzzle" $P <- {0,1}^n$ (where $n$ is the security parameter), a corresponding ``solution" can be generated using N oracle queries (for any parameter $n < N < 2^{o(n)}$), and any adversarial strategy for generating valid solutions must make $\Omega(N)$ adaptive rounds of oracle queries after receiving P. Thus, valid solutions constitute a ``proof" that $\Omega(N)$ parallel time elapsed since $P$ was received. Solutions can be publicly and efficiently verified (in time $\poly(n)$). Applications of these ``time-lock puzzles" include non-interactive time-stamping of documents and universally verifiable CPU benchmarks.

Our construction makes a novel use of ``depth-robust" directed acyclic graphs --- ones whose depth remains large even after removing a constant fraction of vertices --- which were previously studied for the purpose of complexity lower-bounds. The construction bypasses a recent lower-bound of Mahmoody, Moran, and Vadhan (CRYPTO `11), which showed that it is impossible to have time-lock puzzles like ours in the random oracle model if the puzzle generator also computes a solution together with the puzzle.

Category / Keywords: cryptographic protocols /

Publication Info: combinatorial cryptography, hash functions, random oracles,

Date: received 6 Oct 2011

Contact author: mahmoody at gmail com

Available formats: PDF | BibTeX Citation

Version: 20111011:182316 (All versions of this report)