Cryptology ePrint Archive: Report 2013/156

Incentivizing Outsourced Computation

Mira Belenkiy and Melissa Chase and C. Chris Erway and John Jannotti and Alptekin Küpçü and Anna Lysyanskaya

Abstract: We describe different strategies a central authority, the boss, can use to distribute computation to untrusted contractors. Our problem is inspired by volunteer distributed computing projects such as SETI@home, which outsource computation to large numbers of participants. For many tasks, verifying a task's output requires as much work as computing it again; additionally, some tasks may produce certain outputs with greater probability than others. A selfish contractor may try to exploit these factors, by submitting potentially incorrect results and claiming a reward. Further, malicious contractors may respond incorrectly, to cause direct harm or to create additional overhead for result-checking.

We consider the scenario where there is a credit system whereby users can be rewarded for good work and fined for cheating. We show how to set rewards and fines that incentivize proper behavior from rational contractors, and mitigate the damage caused by malicious contractors. We analyze two strategies: random double-checking by the boss, and hiring multiple contractors to perform the same job.

We also present a bounty mechanism when multiple contractors are employed; the key insight is to give a reward to a contractor who catches another worker cheating. Furthermore, if we can assume that at least a small fraction h of the contractors are honest (1% − 10%), then we can provide graceful degradation for the accuracy of the system and the work the boss has to perform. This is much better than the Byzantine approach, which typically assumes $h > 60\%$.

Available formats: [PDF](#) | [BibTeX Citation](#)

Version: 20130319:183934 ([All versions of this report](#))

Discussion forum: [Show discussion](#) | [Start new discussion](#)