Game-Theoretic Framework for Integrity Verification in Computation Outsourcing

Qiang Tang and Balázs Pejó

University of Luxembourg
6, rue Richard Coudenhove-Kalergi, L-1359 Luxembourg
{qiang.tang, balazs.pejo}@uni.lu

Abstract. Nowadays, in order to avoid computational burdens, many organizations tend to outsource their computations to third-party cloud servers [2]. In order to protect service quality, the integrity of computation results need to be guaranteed. We define a game, where the client wants to outsource some computation to the server and verify the results. We provide a strategy for the client to minimize its own cost and force a rational server to execute the computation task honestly, e.g. *not-cheat* is a dominant strategy for the server. The details of our work appear in the full paper [1]. We give a sketch below.

The Settings. In our model we have two entity: the client, who wants to outsource some computation and the server, who will actually perform the computation. Both of them have they own strategies: the server sets ρ percent of the results to be random numbers while the client chooses σ percent of the outputs to verify by recomputing them. Based on these values, a detection rate P_d can be defined. However, ρ is unknown to the client, it is infeasible to calculate $P_d(\sigma, \rho)$. To tackle this, we define a threshold cheating toleration rate θ. Now, if the server sets ρ above this threshold then it will be caught at least with probability $P_d(\sigma, \theta)$.

The Game. We define a two-player Stackelberg game, where the client makes an offer W (e.g. how much it willing to pay for the computation) to the server. If the server rejects this, the game terminates. If the offer is accepted, then the server carries out the computation with some level of cheating (ρ). Then the client verifies the results and in case of detected cheating it refuses to pay.

Results. Our analysis showed, that the only condition that must be satisfied to make the *not-cheat* a dominant strategy for the server is the following: $W^{-1} < P_d(\sigma, \theta)$. In other words, the inverse of the payment is the lower limit for the detection rate. Furthermore, this rate corresponds to a verification cost V_d which is the other part of the client's cost (besides the payment W). So for each possible payment there is a corresponding verification cost. By searching exhaustively amongst these pairs ($W + V_d$), the client is able to determine the one with the lowest sum, which is the game's Nash Equilibrium.

Use Cases. We apply our model to two recommender algorithm (Weighted Slope One and Stochastic Gradient Descent Matrix Factorization) with two real world dataset (Movilens 1M and Netflix). We show that the payment in the equilibrium is only slightly bigger than the cost of the calculation.

References

1. Qiang Tang and Balázs Pejó. Game-Theoretic Framework for Integrity Veri cation in Computation Outsourcing. http://eprint.iacr.org/2016/639.
2. Jaideep Vaidya, Ibrahim Yakut, and Anirban Basu. Efficient integrity verification for outsourced collaborative filtering. In *IEEE International Conference on Data Mining*, pages 560–569. IEEE, 2014.