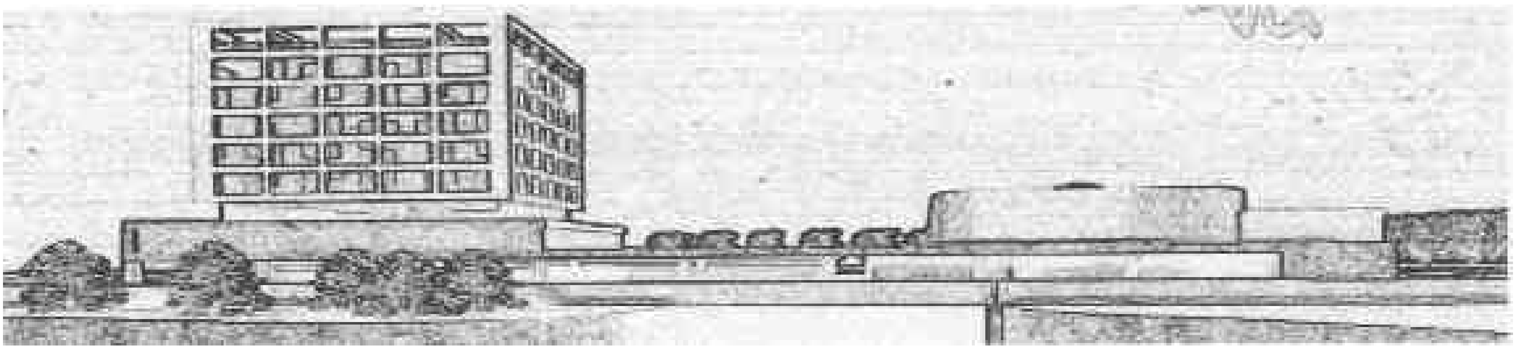
VOLUME IX, NUMBER 5



REPORTS ON SYSTEMS AND COMMUNICATIONS

GSyC

Algorithmic Mechanisms for Reliable Internet-based Computing under Collusion

Antonio Fernández Anta, Chryssis Georgiou and Miguel A. Mosteiro

Móstoles (Madrid), November 2009
Depósito Legal: M-50653-2004
ISSN: 1698-7489

Table of Contents

Algorithmic Mechanisms for Reliable Internet-based Computing under Collusion*

Antonio Fernández Anta, Chryssis Georgiou, and Miguel A. Mosteiro

LADyR, GSyC, Univ. Rey Juan Carlos, Spain.
(anto@gsyc.es,miguel.mosteiro@urjc.es).
Dept. of Computer Science, Univ. of Cyprus, Cyprus.
(chryssis@cs.ucy.ac.cy).
Dept. of Computer Science, Rutgers University, USA.
(mosteiro@cs.rutgers.edu).

Abstract. In this work, using a game-theoretic approach, cost-sensitive mechanisms that lead to reliable Internet-based computing are designed. In particular, we consider Internet-based master-worker computations, where a master processor assigns, across the Internet, a computational task to a set of potentially untrusted worker processors and collects their responses. Workers may collude in order to increase their benefit.

Several game-theoretic models that capture the nature of the problem are analyzed, and algorithmic mechanisms that, for each given set of cost and system parameters, achieve high reliability are designed. Additionally, two specific realistic system scenarios are studied. These scenarios are a system of volunteering computing like SETI, and a company that buys computing cycles from Internet computers and sells them to its customers in the form of a task-computation service. Notably, under certain conditions, non redundant allocation yields the best trade-off between cost and reliability.

Keywords: Internet-based computing, Mechanism design, Game theory, Task execution, Fault-tolerance, Rational players, Collusion.

1 Introduction

Motivation. As traditional one-processor machines have limited computational resources, and powerful parallel machines are very expensive to obtain and maintain, the Internet is emerging as the computational platform of choice for processing complex computational jobs. Several Internet-oriented systems and protocols have been designed to operate on top of this global computation infrastructure; examples include Grid systems [7, 31] and the "@home" projects [2], such as SETI [19] (a classical example

* This research was supported in part by Comunidad de Madrid grant S-0505/TIC/0285; Spanish MEC grant TIN2005-09198-C02-01; EU IST #15964 (AEOLUS); EU Marie Curie European Reintegration Grant IRG 210021; NSF grant CCF 0632838; and the University of Cyprus. A preliminary version of this work appears in the Proceedings of the 7th IEEE International Symposium on Network Computing and Applications (NCA 2008), pages 315–324, Cambridge, MA, 2008.

of *volunteering computing*). Although the potential is great, the use of Internet-based computing (also referred as P2P computing–P2PC [10, 32]) is limited by the untrustworthiness nature of the platform's components [2,12]. Let us take SETI as an example. In SETI, data is distributed for processing to millions of voluntary machines around the world. At a conceptual level, in SETI there is a machine, call it the *master*, that sends jobs, across the Internet, to these computers, call them the *workers*. These workers execute and report back the result of the task computation. However, these workers are not trustworthy, and hence might report incorrect results. Usually, the master attempts to minimize the impact of these bogus results by assigning the same task to several workers and comparing their outcomes (that is, *redundant* task allocation is employed [2]).

In this paper, Internet-based master-worker computations are studied from a game-theoretic point of view. Specifically, these computations are modeled as games where each worker chooses whether to be *honest* (that is, compute and return the correct task result) or a *cheater* (that is, fabricate a bogus result and return it to the master). Additionally, cost-sensitive mechanisms (algorithms) that provide the necessary incentive for the workers to truthfully compute and report the correct result are designed. The objective is to maximize the probability of the master of obtaining the correct result while minimizing its cost (or alternatively, increasing its benefit). In particular, we identify and propose mechanisms for two paradigmatic applications. Namely, a volunteering computing system as the aforementioned SETI where computing processors are altruistic, and a second scenario where a company distributes computing tasks among contractor processors that get an economic reward in exchange.

Background and Prior/Related Work. Prior examples of game theory in distributed computing include work on Internet routing [20, 21, 28], resource/facility location and sharing [11, 14], containment of viruses spreading [22], secret sharing [1, 16], and task computations [32]. For more discussion on the connection between game theory and computing we refer the reader to the survey by Halpern [15] and the book by Nisan et al. [25].

In traditional distributed computing, the behavior of the system components (i.e., processors) is characterized a priori as either good or bad, depending on whether they follow the prescribed protocol or not. In game theory, processors are assumed to act on their own *self-interest* and they do not have an a priori established behavior. Such processors are usually referred as *rational* [1,12]. In other words, the processors decide on how to act in an attempt to increase their own benefit, or alternatively to lower their own cost.

In *algorithmic mechanisms design* [1, 8, 24, 26], games are designed to provide the necessary incentives so that processors' interests are best served by acting "correctly." The usual practice is to provide some reward (resp. penalty) should the processors (resp. do not) behave as desired. The design objective is to force a desired unique *Nash equilibrium* (NE) [23], i.e., a strategy choice by each game participant such that none of them has incentive to change it.

In [9, 18] reliable master-worker computations have been considered by redundant task-allocation. In these works probabilistic guarantees of obtaining the correct result while minimizing the cost (number of workers chosen to perform the task) are also shown. However, a traditional distributed computing approach is used, in which the behavior of each worker is predefined. In this paper, much richer payoff parameters are studied and the behavior of each worker is not predefined, introducing new challenges that naturally drive to a game-theoretic approach.

Two other related works [4, 30] where the worker behavior is predefined consider collusion in desktop grid computing. In both proposals, the goal is to identify colluders by means of an statistical analysis that requires the processors to compute multiple times. In the present paper, we study the more challenging problem of dealing with collusion when each processor computes only once.

Master-worker computations in a game-theoretic model have been studied before [32]. In that paper, the master can audit the results returned by rational workers with a tunable probability. Bounds for that audit probability are computed to guarantee that workers have incentives to be honest in three scenarios: redundant allocation with and without collusion[1], and single-worker allocation. They conclude that, in their model, single-worker allocation is a cost-effective mechanism specially in presence of collusion. In our work, similar conclusions are extracted under certain system parameters even in the presence of weaker types of collusion. Additionally, our work complements that work in various ways, such as studying more algorithms and games, including a richer payoff model, or considering probabilistic cheating. Finally, useful trade-offs between the benefit of the master and the probability of accepting a wrong result are shown for the one-round protocols proposed.

Distributed computation in presence of selfishness was also studied within the scope of *Combinatorial Agencies* in Economics [3]. The computation is carried out as a game of complete information among rational players. The goal in that work is to study how the utility of the master is affected if the equilibria space is limited to pure strategies. To that extent, the computation of a few Boolean functions is evaluated. If the parameters of the problem yield multiple mixed equilibrium points, it is assumed that workers accept one "suggested" by the master.

A somewhat related work is [5] in which they face the problem of bootstrapping a P2P computing system, in the presence of rational peers. The goal is to incentive peers to join the system, for which they propose a scheme that mixes lottery psychology and multilevel marketing. In our setting, the master could use their scheme to recruit workers. We assume in this paper that enough workers are willing to participate in the computation.

Framework. We consider a distributed system consisting of a master processor that assigns a computational task to a set of workers to compute and return the task result[2]. It is assumed that the master has the possibility of verifying whether the value returned by a worker is the correct result of the task. It is also assumed that verifying an answer is more efficient than computing the task [13] (e.g., NP-complete problems if $P \neq NP$), but the correct result of the computation is not obtained if the verification fails. Therefore, by verifying, the master does not necessarily obtain the correct answer (e.g., when

[1] Cooperation among various workers concealed from the master.

[2] The tasks considered in this work are assumed to have a unique solution.

all workers cheat)[3]. As in [5, 32], workers are assumed to be rational and seek to maximize their benefit, i.e., they are not destructively malicious. We note that this assumption can conceptually be justified by the work of Shneidman and Parks [29] where they reason on the connection of rational players–of algorithmic mechanism designs–and workers in realistic P2P systems. Furthermore, we do not consider non-intentional errors produced by hardware or software problems.

The general protocol used by master and workers is the following. The master process assigns the task to n workers. Each worker processor i cheats with probability $p_{\mathcal{C}}^{(i)}$ and the master processor verifies the answers with some probability $p_{\mathcal{V}}$. If the master processor verifies, it rewards the honest workers and penalizes the cheaters. If the master does not verify, it accepts the answer returned by the majority of workers. However, it does not penalize any worker given that the majority can be actually cheating. Instead, the master rewards workers according to one of the three following models. Either the master rewards the majority only (*Reward Model* $\mathcal{R}_{\mathrm{m}}$), or the master rewards all workers independently of the returned value (*Reward Model* $\mathcal{R}_{\mathrm{a}}$), or the master does not reward at all (*Reward Model* $\mathcal{R}_{\emptyset}$).

The model used in this paper comprises the following form of collusion (that covers realistic types of collusions such as Sybil attacks [6]). Workers form colluding groups. Within the same group workers act homogeneously, i.e., either all choose to cheat, or all choose to be honest, perhaps randomizing their decision by tossing a unique coin. In the case that, within the group, all workers choose to be honest, then only one of them computes the task, and all of them return that result to the master (in this way they avoid the cost of all of them executing the task). In the case that all workers choose to cheat, then they simply agree on a bogus result and send that to the master. In addition, we assume that all "cheating groups" return the same incorrect answer. Since the master accepts the majority, this behavior maximizes the chances of cheating the master. Being this the worst case, it subsumes models where cheaters do not necessarily return the same answer. Note that this behavior can be viewed also as a form of collusion. We also assume that if a worker does not perform the task, then it is (almost) impossible to guess the correct answer (i.e., the probability is negligible). The master, of course, is not aware of the collusions.

Given the protocol above, the game is defined by a set of parameters that include rewards to the workers that return the correct value and punishments to the workers that cheated (that is, returned the incorrect result and "got caught"). Hence, the game is played between the master and the workers, where the first wants to obtain the correct result with a desired probability, while obtaining a desired utility value (in expectation), and the workers decide whether to be honest or cheaters, depending on their expected utility gain or loss. In this paper, we design several games and study the conditions under which unique Nash equilibria (NE) are achieved. Each NE results in a different benefit for the master and a different probability of accepting an incorrect result. Thus, the master can choose some game conditions so that a unique NE that best fits its goals is achieved.

[3] Alternatively, one might assume that the master verifies by simply performing the task and checking the answers of the workers. Our analysis can easily be modified to accommodate this different model.

Contribution. The main contributions of this paper are:

1. The identification of a collection of realistic payoff parameters that allow to model Internet-based master-worker computational environments in game theoretic terms. These parameters can either be fixed exogenously (they are system parameters) or be chosen by the master.

2. The definition of four different games that the master can force to be played: (a) A game between the master and a single worker, (b) a game between the master and a worker, played n times (with different workers), (c) a game with a master and n workers, and (d) a game of n workers in which the master participates indirectly. Games (c) and (d) consider collusions, game (a) considers no collusions as there is only one worker, and game (b) only considers singleton groups, where all cheaters return the same value. Together with the three reward models defined above, we have overall defined twelve games among which the master can choose the most convenient to use in each specific context.

3. The analyses of all the games under general payoff models, and the characterization of conditions under which a unique Nash Equilibrium point is reached for each game and each payoff-model. These analyses lead to mechanisms that the master can run to trade cost and reliability.

4. The design of mechanisms for two specific realistic scenarios, to demonstrate the utility of the analysis. These scenarios reflect, in their fundamental elements, (a) a system of volunteering computing like SETI, and (b) a company that buys computing cycles from Internet computers and sells them to its customers in the form of a task-computation service. Our results show that for (a) the best choice is non-redundant allocation, *even with only singleton colluding groups*. Furthermore, in this case we show that to obtain always the correct answer it is enough to verify with arbitrarily small probability. As an example of the results obtained in (b), if the master only chooses the number of workers n, we show that, again *even with only singleton colluding groups* the best choice is non-redundant allocation. However, in order to achieve correctness always, the required probability of verifying can now be large.

Paper Structure. In Section 2 we provide basic definitions to be used throughout the paper. In Section 3 we present and analyze the games proposed. In Section 4 the mechanisms for the two realistic scenarios are designed. Finally, Section 5 presents conclusions and future lines of work.

2 Definitions

Game Definition. Game participants are referred as workers and master. In order to define the game played in each case, we follow the customary notation used in game theory. Given that this notation is repeatedly used throughout the paper, we summarize it in Table 1 for clarity. We assume that the master always chooses an odd number of workers n. In order to model collusion among workers, we view the set of workers as a set of non-empty subsets $W = \{W_1, \ldots, W_\ell\}$ such that $\sum_{i=1}^{\ell} |W_i| = n$ and $W_i \cap W_j = \emptyset$ for all $i \neq j$, $1 \leq i, j \leq \ell$. We refer to each of these subsets as a *group of workers* or a *group* for short. We also refer to groups and the master as *players*. Workers in the same group act homogeneously, i.e., either all choose to cheat, or all choose to be honest, perhaps randomizing their decision by tossing a unique coin. Workers acting individually are modeled as a group of size one. It is assumed that the size or composition of each group is known only to the members of the group, but all cheating groups return the same incorrect answer.

A strategy profile is defined as a mapping from players to pure strategies, denoted as s. For succinctness, we express a strategy profile as a collection of individual strategy choices together with collective strategy choices. For instance, $s_i = \mathcal{C}, s_M = \mathcal{V}, R_{-iM}, F_{-iM}, T_{-iM}$ stands for a strategy profile s where group W_i chooses strategy $\mathcal{C}$ (to cheat), the master chooses strategy $\mathcal{V}$ (to verify), a set R_{-iM} of groups (where group W_i and the master are not included) randomize their strategy choice with probability $p_{\mathcal{C}} \in (0,1)$, a set F_{-iM} of groups deterministically choose strategy $\mathcal{C}$, and a set T_{-iM} of groups deterministically choose strategy $\overline{\mathcal{C}}$ (to be honest). For games with one worker and the master, the strategy profile is composed only by their choices. For example, $m_{\mathcal{C}\mathcal{V}}$ stands for the master's payoff in the case that the worker cheated and the master verified. We require that, for each group W_i, $p_{\mathcal{C}}^{(i)} = 1 - p_{\overline{\mathcal{C}}}^{(i)}$ and, for the master, $p_{\mathcal{V}} = 1 - p_{\overline{\mathcal{V}}}$. For games where we only have one group or all groups use the same probability, we will express $p_{\mathcal{C}}^{(i)}$ (resp. $p_{\overline{\mathcal{C}}}^{(i)}$) simply by $p_{\mathcal{C}}$ (resp. $p_{\overline{\mathcal{C}}}$). Whenever the strategy is clear from the context, we will refer to the expected utility of group W_i as U_i, and for the master as U_M. In the games studied the master and the workers have complete information on the algorithm and the parameters involved, except on the number and the composition of the colluding groups.

Equilibrium Definition. We define now precisely the conditions for the equilibrium. In this context, the probability distributions are not independent among members of a group. Furthermore, the formulation of equilibrium conditions among individual workers would violate the very definition of equilibrium since the choice of a worker does change the choices of other workers. Instead, equilibrium conditions are formulated among groups. Of course, the computation of an equilibrium might not be possible since the size of the groups is unknown. But, finding appropriate conditions so that the unique equilibrium is the same independently of that size, the problem can be solved. An important point to be made is that the majority is evaluated in terms of number of single answers. Nevertheless, this fact has an impact on the payoffs of each player, which in this case is a whole group, but not in the correctness of the equilibrium formulation.

Recall from [27] that for any finite game, a mixed strategy profile σ^* is a *mixed-strategy Nash equilibrium* (MSNE) if, and only if, for each player π (either a worker group or the master),

$$U_\pi(s_\pi, \sigma^*_{-\pi}) = U_\pi(s'_\pi, \sigma^*_{-\pi}), \forall s_\pi, s'_\pi \in supp(\sigma^*_\pi), \quad (1)$$

$$U_\pi(s_\pi, \sigma^*_{-\pi}) \geq U_\pi(s'_\pi, \sigma^*_{-\pi}),$$
$$\forall s_\pi, s'_\pi : s_\pi \in supp(\sigma^*_\pi), s'_\pi \notin supp(\sigma^*_\pi). \quad (2)$$

In words, given a MSNE with mixed-strategy profile σ^*, for each player π, the expected utility, assuming that all other players do not change their choice, is the same for each pure strategy that the player can choose with positive probability in σ^*, and it is not less than the expected utility of any pure strategy with probability zero of being chosen in σ^*. A *fully* MSNE is an equilibrium with mixed strategy profile σ where, for each player π, $supp(\sigma_\pi) = \mathcal{S}_\pi$.

Payoffs Definition. We detail in Table 2 the payoff definitions that will be used throughout the paper. All the parameters in this table are non-negative. Notice that we split the reward to a worker into $WB_\mathcal{A}$ and $MC_\mathcal{A}$, to model the fact that the cost of the master might be different than the benefit of a worker. In fact, in some models they may be completely unrelated. Among the parameters involved, we assume that the master has the freedom of choosing the cheater penalty $WP_\mathcal{C}$ and the worker reward for computing $MC_\mathcal{A}$. By tuning these parameters and choosing n, the master achieves the desired trade-off between correctness and cost. Given that the master does not know the composition of groups (if there is any), benefits and punishments are applied individually to each worker, except for the cost for computing the task $WC_\mathcal{T}$ which is shared among all workers belonging to the same group (as it was explained in the Introduction).

3 Equilibria Analysis

In the following sections, different games are studied according to the participants involved. In order to identify the parameter conditions for which there is an NE, Equations (1) and (2) of the MSNE definition are instantiated in each particular game, without making any assumptions on the payoffs. We call this ***the general payoffs model***. From these instantiations, we obtain conditions on the parameters (payoffs and probabilities) that would make such equilibrium unique. Finally, we introduce the reward models described before on those conditions, so that we can compare among all games and models in Section 4.

3.1 Game 1:1: One Master - One Worker

We start the analysis by considering the game between the master and only one worker. Hence, collusions can not occur and we refer to the group just as "the worker."

General Payoffs Model. In order to evaluate all possible equilibria, all the different mixes have to be considered. In other words, according with the range of values that $p_\mathcal{C}$ and $p_\mathcal{V}$ can take, we can have fully MSNE, partially MSNE, or pure-strategies NE. More specifically, both $p_\mathcal{C}$ and $p_\mathcal{V}$ can take values either 0, 1, or in the open interval $(0, 1)$. Depending on these values, the different conditions in Equations (1) and (2) have to be achieved in order to have an equilibrium. Hence, conditions on $p_\mathcal{C}$ and $p_\mathcal{V}$ for each equilibrium can be obtained from these equations as detailed below.

– Case $p_\mathcal{C} \in (0, 1), p_\mathcal{V} \in (0, 1)$: From Equation (1), there is a fully MSNE if $U_M(\mathcal{V}, p_\mathcal{C}) = U_M(\overline{\mathcal{V}}, p_\mathcal{C})$ and $U_W(\mathcal{C}, p_\mathcal{V}) = U_W(\overline{\mathcal{C}}, p_\mathcal{V})$ simultaneously. These equations determine the value of $p_\mathcal{C}$ and $p_\mathcal{V}$ in the MSNE as follows.

$$p_\mathcal{C} m_{\mathcal{C}\mathcal{V}} + (1 - p_\mathcal{C}) m_{\overline{\mathcal{C}}\mathcal{V}} = p_\mathcal{C} m_{\mathcal{C}\overline{\mathcal{V}}} + (1 - p_\mathcal{C}) m_{\overline{\mathcal{C}\mathcal{V}}}$$
$$p_\mathcal{C} = \frac{m_{\overline{\mathcal{C}\mathcal{V}}} - m_{\overline{\mathcal{C}}\mathcal{V}}}{m_{\mathcal{C}\mathcal{V}} - m_{\overline{\mathcal{C}}\mathcal{V}} - m_{\mathcal{C}\overline{\mathcal{V}}} + m_{\overline{\mathcal{C}\mathcal{V}}}}.$$

$$p_{\mathcal{V}} w_{\mathcal{C}\mathcal{V}} + (1-p_{\mathcal{V}}) w_{\mathcal{C}\overline{\mathcal{V}}} = p_{\mathcal{V}} w_{\overline{\mathcal{C}}\mathcal{V}} + (1-p_{\mathcal{V}}) w_{\overline{\mathcal{C}\mathcal{V}}}$$
$$p_{\mathcal{V}} = \frac{w_{\overline{\mathcal{C}\mathcal{V}}} - w_{\mathcal{C}\overline{\mathcal{V}}}}{w_{\mathcal{C}\mathcal{V}} - w_{\mathcal{C}\overline{\mathcal{V}}} - w_{\overline{\mathcal{C}}\mathcal{V}} + w_{\overline{\mathcal{C}\mathcal{V}}}}.$$

– Case $p_{\mathcal{C}} = 0, p_{\mathcal{V}} \in (0,1)$: For the worker, Equation (1) trivially holds. From Equation (2), $U_W(\overline{\mathcal{C}}, p_{\mathcal{V}}) \geq U_W(\mathcal{C}, p_{\mathcal{V}})$ must hold, i.e.,

$$p_{\mathcal{V}} w_{\overline{\mathcal{C}}\mathcal{V}} + (1-p_{\mathcal{V}}) w_{\overline{\mathcal{C}\mathcal{V}}} \geq p_{\mathcal{V}} w_{\mathcal{C}\mathcal{V}} + (1-p_{\mathcal{V}}) w_{\mathcal{C}\overline{\mathcal{V}}}.$$

Then, if $w_{\mathcal{C}\overline{\mathcal{V}}} + w_{\overline{\mathcal{C}}\mathcal{V}} - w_{\overline{\mathcal{C}\mathcal{V}}} - w_{\mathcal{C}\mathcal{V}} > 0$,

$$p_{\mathcal{V}} \geq \frac{w_{\mathcal{C}\overline{\mathcal{V}}} - w_{\overline{\mathcal{C}\mathcal{V}}}}{w_{\mathcal{C}\overline{\mathcal{V}}} + w_{\overline{\mathcal{C}}\mathcal{V}} - w_{\overline{\mathcal{C}\mathcal{V}}} - w_{\mathcal{C}\mathcal{V}}}.$$

Else, if $w_{\mathcal{C}\overline{\mathcal{V}}} + w_{\overline{\mathcal{C}}\mathcal{V}} - w_{\overline{\mathcal{C}\mathcal{V}}} - w_{\mathcal{C}\mathcal{V}} < 0$,

$$p_{\mathcal{V}} \leq \frac{w_{\mathcal{C}\overline{\mathcal{V}}} - w_{\overline{\mathcal{C}\mathcal{V}}}}{w_{\mathcal{C}\overline{\mathcal{V}}} + w_{\overline{\mathcal{C}}\mathcal{V}} - w_{\overline{\mathcal{C}\mathcal{V}}} - w_{\mathcal{C}\mathcal{V}}}.$$

For the master, from Equation (1), $U_M(\mathcal{V}, p_{\mathcal{C}}) = U_M(\overline{\mathcal{V}}, p_{\mathcal{C}})$ must hold, which implies

$$p_{\mathcal{C}} m_{\mathcal{C}\mathcal{V}} + (1-p_{\mathcal{C}}) m_{\overline{\mathcal{C}}\mathcal{V}} = p_{\mathcal{C}} m_{\mathcal{C}\overline{\mathcal{V}}} + (1-p_{\mathcal{C}}) m_{\overline{\mathcal{C}\mathcal{V}}}$$
$$m_{\overline{\mathcal{C}}\mathcal{V}} = m_{\overline{\mathcal{C}\mathcal{V}}},$$

since $p_{\mathcal{C}} = 0$. So, under these conditions, there is an MSNE.

– Case $p_{\mathcal{C}} = 1, p_{\mathcal{V}} \in (0,1)$: For the worker, Equation (1) trivially holds. From Equation (2), it must be true that $U_W(\mathcal{C}, p_{\mathcal{V}}) \geq U_W(\overline{\mathcal{C}}, p_{\mathcal{V}})$. So,

$$p_{\mathcal{V}} w_{\mathcal{C}\mathcal{V}} + (1-p_{\mathcal{V}}) w_{\mathcal{C}\overline{\mathcal{V}}} \geq p_{\mathcal{V}} w_{\overline{\mathcal{C}}\mathcal{V}} + (1-p_{\mathcal{V}}) w_{\overline{\mathcal{C}\mathcal{V}}}.$$

Then, if $w_{\mathcal{C}\mathcal{V}} + w_{\overline{\mathcal{C}\mathcal{V}}} - w_{\mathcal{C}\overline{\mathcal{V}}} - w_{\overline{\mathcal{C}}\mathcal{V}} > 0$,

$$p_{\mathcal{V}} \geq \frac{w_{\overline{\mathcal{C}\mathcal{V}}} - w_{\mathcal{C}\overline{\mathcal{V}}}}{w_{\mathcal{C}\mathcal{V}} + w_{\overline{\mathcal{C}\mathcal{V}}} - w_{\mathcal{C}\overline{\mathcal{V}}} - w_{\overline{\mathcal{C}}\mathcal{V}}}.$$

Else, if $w_{\mathcal{C}\mathcal{V}} + w_{\overline{\mathcal{C}\mathcal{V}}} - w_{\mathcal{C}\overline{\mathcal{V}}} - w_{\overline{\mathcal{C}}\mathcal{V}} < 0$,

$$p_{\mathcal{V}} \leq \frac{w_{\overline{\mathcal{C}\mathcal{V}}} - w_{\mathcal{C}\overline{\mathcal{V}}}}{w_{\mathcal{C}\mathcal{V}} + w_{\overline{\mathcal{C}\mathcal{V}}} - w_{\mathcal{C}\overline{\mathcal{V}}} - w_{\overline{\mathcal{C}}\mathcal{V}}}.$$

For the master, from Equation (1), $U_M(\mathcal{V}, p_{\mathcal{C}}) = U_M(\overline{\mathcal{V}}, p_{\mathcal{C}})$, and since $p_{\mathcal{C}} = 1$,

$$p_{\mathcal{C}} m_{\mathcal{C}\mathcal{V}} + (1-p_{\mathcal{C}}) m_{\overline{\mathcal{C}}\mathcal{V}} = p_{\mathcal{C}} m_{\mathcal{C}\overline{\mathcal{V}}} + (1-p_{\mathcal{C}}) m_{\overline{\mathcal{C}\mathcal{V}}}$$
$$m_{\mathcal{C}\mathcal{V}} = m_{\mathcal{C}\overline{\mathcal{V}}}.$$

So, under these conditions, there is an MSNE.

– Case $p_{\mathcal{C}} \in (0,1), p_{\mathcal{V}} = 0$: For the master, Equation (1) trivially holds. From Equation (2), it must hold that $U_M(\overline{\mathcal{V}}, p_{\mathcal{C}}) \geq U_M(\mathcal{V}, p_{\mathcal{C}})$. Then,

$$p_{\mathcal{C}} m_{\mathcal{C}\overline{\mathcal{V}}} + (1-p_{\mathcal{C}}) m_{\overline{\mathcal{C}\mathcal{V}}} \geq p_{\mathcal{C}} m_{\mathcal{C}\mathcal{V}} + (1-p_{\mathcal{C}}) m_{\overline{\mathcal{C}}\mathcal{V}}.$$

Then, if $m_{\overline{\mathcal{C}}\mathcal{V}} + m_{\mathcal{C}\overline{\mathcal{V}}} - m_{\overline{\mathcal{C}\mathcal{V}}} - m_{\mathcal{C}\mathcal{V}} > 0$,

$$p_{\mathcal{C}} \geq \frac{m_{\overline{\mathcal{C}}\mathcal{V}} - m_{\overline{\mathcal{C}\mathcal{V}}}}{m_{\overline{\mathcal{C}}\mathcal{V}} + m_{\mathcal{C}\overline{\mathcal{V}}} - m_{\overline{\mathcal{C}\mathcal{V}}} - m_{\mathcal{C}\mathcal{V}}}.$$

Else, if $m_{\overline{\mathcal{C}}\mathcal{V}} + m_{\mathcal{C}\overline{\mathcal{V}}} - m_{\overline{\mathcal{C}\mathcal{V}}} - m_{\mathcal{C}\mathcal{V}} < 0$,

$$p_{\mathcal{C}} \leq \frac{m_{\overline{\mathcal{C}}\mathcal{V}} - m_{\overline{\mathcal{C}\mathcal{V}}}}{m_{\overline{\mathcal{C}}\mathcal{V}} + m_{\mathcal{C}\overline{\mathcal{V}}} - m_{\overline{\mathcal{C}\mathcal{V}}} - m_{\mathcal{C}\mathcal{V}}}.$$

For the worker, from Equation (1), $U_W(\mathcal{C}, p_{\mathcal{V}}) = U_W(\overline{\mathcal{C}}, p_{\mathcal{V}})$, and given that $p_{\mathcal{V}} = 0$ we have that

$$p_{\mathcal{V}} w_{\mathcal{C}\mathcal{V}} + (1-p_{\mathcal{V}}) w_{\mathcal{C}\overline{\mathcal{V}}} = p_{\mathcal{V}} w_{\overline{\mathcal{C}}\mathcal{V}} + (1-p_{\mathcal{V}}) w_{\overline{\mathcal{C}\mathcal{V}}}$$
$$w_{\mathcal{C}\overline{\mathcal{V}}} = w_{\overline{\mathcal{C}\mathcal{V}}}.$$

So, under these conditions, there is an MSNE.

– Case $p_{\mathcal{C}} \in (0,1), p_{\mathcal{V}} = 1$: For the master, Equation (1) trivially holds. From Equation (2), $U_M(\mathcal{V}, p_{\mathcal{C}}) \geq U_M(\overline{\mathcal{V}}, p_{\mathcal{C}})$ and

$$p_{\mathcal{C}} m_{\mathcal{C}\mathcal{V}} + (1-p_{\mathcal{C}}) m_{\overline{\mathcal{C}}\mathcal{V}} \geq p_{\mathcal{C}} m_{\mathcal{C}\overline{\mathcal{V}}} + (1-p_{\mathcal{C}}) m_{\overline{\mathcal{C}\mathcal{V}}}.$$

Then, if $m_{\mathcal{C}\mathcal{V}} - m_{\overline{\mathcal{C}}\mathcal{V}} - m_{\mathcal{C}\overline{\mathcal{V}}} + m_{\overline{\mathcal{C}\mathcal{V}}} > 0$,

$$p_{\mathcal{C}} \geq \frac{m_{\overline{\mathcal{C}\mathcal{V}}} - m_{\overline{\mathcal{C}}\mathcal{V}}}{m_{\mathcal{C}\mathcal{V}} - m_{\overline{\mathcal{C}}\mathcal{V}} - m_{\mathcal{C}\overline{\mathcal{V}}} + m_{\overline{\mathcal{C}\mathcal{V}}}}.$$

Else, if $m_{\mathcal{C}\mathcal{V}} - m_{\overline{\mathcal{C}}\mathcal{V}} - m_{\mathcal{C}\overline{\mathcal{V}}} + m_{\overline{\mathcal{C}\mathcal{V}}} < 0$,

$$p_{\mathcal{C}} \leq \frac{m_{\overline{\mathcal{C}\mathcal{V}}} - m_{\overline{\mathcal{C}}\mathcal{V}}}{m_{\mathcal{C}\mathcal{V}} - m_{\overline{\mathcal{C}}\mathcal{V}} - m_{\mathcal{C}\overline{\mathcal{V}}} + m_{\overline{\mathcal{C}\mathcal{V}}}}.$$

For the worker, from Equation (1), $U_W(\mathcal{C}, p_{\mathcal{V}}) = U_W(\overline{\mathcal{C}}, p_{\mathcal{V}})$ and since $p_{\mathcal{V}} = 1$,

$$p_{\mathcal{V}} w_{\mathcal{C}\mathcal{V}} + (1-p_{\mathcal{V}}) w_{\mathcal{C}\overline{\mathcal{V}}} = p_{\mathcal{V}} w_{\overline{\mathcal{C}}\mathcal{V}} + (1-p_{\mathcal{V}}) w_{\overline{\mathcal{C}\mathcal{V}}}$$
$$w_{\mathcal{C}\mathcal{V}} = w_{\overline{\mathcal{C}}\mathcal{V}}.$$

So, under these conditions, there is an MSNE.

Finally, the following are conditions to have a pure-strategies NE with profile s.

– Case $s = \{\mathcal{C}, \mathcal{V}\}$: $m_{\mathcal{C}\mathcal{V}} \geq m_{\mathcal{C}\overline{\mathcal{V}}}$ and $w_{\mathcal{C}\mathcal{V}} \geq w_{\overline{\mathcal{C}}\mathcal{V}}$.
– Case $s = \{\overline{\mathcal{C}}, \mathcal{V}\}$: $m_{\overline{\mathcal{C}}\mathcal{V}} \geq m_{\overline{\mathcal{C}\mathcal{V}}}$ and $w_{\overline{\mathcal{C}}\mathcal{V}} \geq w_{\mathcal{C}\mathcal{V}}$.
– Case $s = \{\mathcal{C}, \overline{\mathcal{V}}\}$: $m_{\mathcal{C}\overline{\mathcal{V}}} \geq m_{\mathcal{C}\mathcal{V}}$ and $w_{\mathcal{C}\overline{\mathcal{V}}} \geq w_{\overline{\mathcal{C}\mathcal{V}}}$.

– Case $s = \{\overline{\mathcal{C}}, \overline{\mathcal{V}}\}$: $m_{\overline{\mathcal{C}}\overline{\mathcal{V}}} \geq m_{\overline{\mathcal{C}}\mathcal{V}}$ and $w_{\overline{\mathcal{C}}\overline{\mathcal{V}}} \geq w_{\mathcal{C}\overline{\mathcal{V}}}$.

On the other hand, the expected utility of the master and the worker in any equilibrium are $U_M = p_\mathcal{C} p_\mathcal{V} m_{\mathcal{C}\mathcal{V}} + (1-p_\mathcal{C}) p_\mathcal{V} m_{\overline{\mathcal{C}}\mathcal{V}} + p_\mathcal{C}(1-p_\mathcal{V}) m_{\mathcal{C}\overline{\mathcal{V}}} + (1-p_\mathcal{C})(1-p_\mathcal{V}) m_{\overline{\mathcal{C}}\overline{\mathcal{V}}}$ and $U_W = p_\mathcal{C} p_\mathcal{V} w_{\mathcal{C}\mathcal{V}} + p_\mathcal{C}(1-p_\mathcal{V}) w_{\mathcal{C}\overline{\mathcal{V}}} + (1-p_\mathcal{C}) p_\mathcal{V} w_{\overline{\mathcal{C}}\mathcal{V}} + (1-p_\mathcal{C})(1-p_\mathcal{V}) w_{\overline{\mathcal{C}}\overline{\mathcal{V}}}$ respectively, and the probability of accepting the wrong answer is $\mathbf{P}_{wrong} = (1-p_\mathcal{V}) p_\mathcal{C}$.
Reward Model $\mathcal{R}_\mathrm{m}$. Recall that in this model we assume that when the master does not verify, it rewards only the majority. Given that there is only one worker, in this case the master rewards always. Under the payoff model detailed in Table 2, the payoffs are

$$
\begin{aligned}
m_{\mathcal{C}\mathcal{V}} &= -MC_\mathcal{V} & w_{\mathcal{C}\mathcal{V}} &= -WP_\mathcal{C} \\
m_{\overline{\mathcal{C}}\mathcal{V}} &= MB_\mathcal{R} - MC_\mathcal{V} - MC_\mathcal{A} & w_{\overline{\mathcal{C}}\mathcal{V}} &= WB_\mathcal{A} - WC_\mathcal{T} \\
m_{\mathcal{C}\overline{\mathcal{V}}} &= -MP_\mathcal{W} - MC_\mathcal{A} & w_{\mathcal{C}\overline{\mathcal{V}}} &= WB_\mathcal{A} \\
m_{\overline{\mathcal{C}}\overline{\mathcal{V}}} &= MB_\mathcal{R} - MC_\mathcal{A} & w_{\overline{\mathcal{C}}\overline{\mathcal{V}}} &= WB_\mathcal{A} - WC_\mathcal{T}
\end{aligned}
$$

Replacing appropriately, we obtain the conditions for equilibrium, probability of accepting the wrong answer, and utilities for each case.

Reward Model $\mathcal{R}_\mathrm{a}$. In this model we assume that if the master does not verify, it rewards all workers independently of the answer. Hence, the analysis is identical to the previous case.

Reward Model $\mathcal{R}_\emptyset$. Recall that in this model we assume that if the master does not verify, it does not reward the worker. Hence, under the payoff model detailed in Table 2, the payoffs are

$$
\begin{aligned}
m_{\mathcal{C}\mathcal{V}} &= -MC_\mathcal{V} & w_{\mathcal{C}\mathcal{V}} &= -WP_\mathcal{C} \\
m_{\overline{\mathcal{C}}\mathcal{V}} &= MB_\mathcal{R} - MC_\mathcal{V} - MC_\mathcal{A} & w_{\overline{\mathcal{C}}\mathcal{V}} &= WB_\mathcal{A} - WC_\mathcal{T} \\
m_{\mathcal{C}\overline{\mathcal{V}}} &= -MP_\mathcal{W} & w_{\mathcal{C}\overline{\mathcal{V}}} &= 0 \\
m_{\overline{\mathcal{C}}\overline{\mathcal{V}}} &= MB_\mathcal{R} & w_{\overline{\mathcal{C}}\overline{\mathcal{V}}} &= -WC_\mathcal{T}
\end{aligned}
$$

Replacing appropriately, we obtain the conditions for equilibrium, probability of accepting the wrong answer, and utilities for each case, as we will see in the next section. The probability of accepting the wrong result, the master utility for each case, the conditions for equilibrium, and the workers utility for the reward models $\mathcal{R}_\mathrm{m}$ and $\mathcal{R}_\emptyset$ can be obtained from Tables 3 and 4 by replacing $n = 1$.

3.2 Game 1:1^n: n Games One to One

In this section it is considered the case where the master runs n instances of the one to one game analyzed in the previous section. Workers are assumed to compute the equilibrium as if they were playing alone against the master. Hence, given the assumption that the players are rational and compute the equilibrium to decide what to do, the consideration of collusion is meaningless for this game. Hence, all groups are assumed to have exactly one member; we do assume however that cheaters return the same incorrect value (to obtain worst case analysis). Games where workers know about the existence of other workers and they can collude to fool the master are studied later. Given the equilibria computed in Section 3.1, the master runs n instances of that game, one with each of the n workers, choosing to verify or not with probability $p_{\mathcal{V}}$ only once. Additionally, when paying while not verifying, the master rewards all or none according with the one-to-one game.

General Payoffs Model. Since this game is just a multiple-instance version of the previous game, under the payoff model detailed in Table 2, the conditions for equilibria and the utility of a worker are the same as in Section 3.1. However, the expected utility of the master and the probability of accepting the wrong result change. In order to give those expressions, we define the following notation. Let $\mathcal{W}$ be the set of partitions in two subsets (F, T) of W, i.e., $\mathcal{W} = \{(F, T) | F \cap T = \emptyset, F \cup T = W\}$. F is the set of workers that cheat and T the set of honest workers. We also define master payoff functions $m_s : \{0, 1, \ldots, n\} \to \mathbb{R}$, that still depend on the number of workers that cheat or not, but are not necessarily just n times the individual payoff of a 1:1 game (reflecting the fact that the cost may include some fixed amount for unique verification or unique cost of being wrong). For the sake of clarity, we will denote the probability that the majority cheats as $\mathbf{P}_{\mathcal{C}}$. Then, the probability that the majority cheats, the probability of being wrong, and the master's utility are

$$
\begin{aligned}
\mathbf{P}_{\mathcal{C}} &= \sum_{\substack{(F,T)\in\mathcal{W}\\ |F|>|T|}} \prod_{f\in F} p_{\mathcal{C}}^{(f)} \prod_{t\in T}(1 - p_{\mathcal{C}}^{(t)}), \\
\mathbf{P}_{wrong} &= (1 - p_{\mathcal{V}})\mathbf{P}_{\mathcal{C}}, \\
U_M &= p_{\mathcal{V}} \sum_{(F,T)\in\mathcal{W}} \prod_{f\in F} p_{\mathcal{C}}^{(f)} \prod_{t\in T}(1 - p_{\mathcal{C}}^{(t)}) m_{\mathcal{V}} + \\
&\quad (1 - p_{\mathcal{V}}) \sum_{(F,T)\in\mathcal{W}} \prod_{f\in F} p_{\mathcal{C}}^{(f)} \prod_{t\in T}(1 - p_{\mathcal{C}}^{(t)}) m_{\overline{\mathcal{V}}}.
\end{aligned}
$$

Respectively, where $m_{\mathcal{V}} = m_{\mathcal{CV}}(|F|) + m_{\overline{\mathcal{C}}\mathcal{V}}(|T|)$ and $m_{\overline{\mathcal{V}}} = m_{\mathcal{C}\overline{\mathcal{V}}}(|F|) + m_{\overline{\mathcal{CV}}}(|T|)$.

Reward Models. In this game, we assume that the cost of verification $MC_{\mathcal{V}}$ is independent of the number of workers (since all cheating workers return the same value) and that, as long as some worker is honest, upon verification the master obtains the correct result. It is important to note that, under this assumption, the probability of obtaining the correct result is not $1 - \mathbf{P}_{wrong}$, given that if the master verifies but all workers cheat, the master does not obtain the correct result. Recall that the master plays n instances of a one-to-one game, thus, depending on the model, it must reward every worker if not verifying independently of majorities. We summarize the probability of accepting the wrong result, the master utility for each case, the conditions for equilibrium, and the workers utility for the reward models $\mathcal{R}_{\mathrm{m}}$ and $\mathcal{R}_{\emptyset}$ in Tables 3 and 4 respectively (Tables 3 and 4 give also these values for Game 1:1 replacing appropriately $n = 1$).

3.3 Game 0:n: No Master in the Game

Another natural generalization of the game of Section 3.1 is to consider a game in which the master assigns the task to n workers that play the game among them. Intuitively, it can be seen that, in case of not verifying, workers will compete to be in the majority (to persuade the master). Given that workers know the existence of the other workers, including collusions in the analysis is in order. The question of how the participation of the master in the game would affect the results obtained in this section is addressed in Section 3.4.

General Payoffs Model. In order to analyze this game, it is convenient to partition the set of groups. More precisely, consider disjoint sets F, T and R, such that $F \cup T \cup R = W$, as follows. F is the set of groups that choose to cheat as a pure strategy, i.e., $F = \{W_i | W_i \in W \wedge p_{\mathcal{C}}^{(i)} = 1\}$. T is the set of groups that choose not to cheat as a pure strategy, i.e., $T = \{W_i | W_i \in W \wedge p_{\mathcal{C}}^{(i)} = 0\}$. R is the set of groups that randomize their choice, i.e., $R = \{W_i | W_i \in W \wedge p_{\mathcal{C}}^{(i)} \in (0,1)\}$. Let $F_{-i} = F \setminus \{W_i\}$, $T_{-i} = T \setminus \{W_i\}$, and $R_{-i} = R \setminus \{W_i\}$. Let $\mathcal{R}_{-i}$ be the set of partitions in two subsets (R_F, R_T) of R_{-i}, i.e., $\mathcal{R}_{-i} = \{(R_F, R_T) | R_F \cap R_T = \emptyset \wedge R_F \cup R_T = R_{-i}\}$. Let $\mathbf{E}[w_s^{(i)}]$ be the expected payoff of group W_i for the strategy profile s, taking the expectation over the choice of the master of verifying or not. Then, for each group $W_i \in W$ and for each strategy profile $s_{-i} = R_{-i}, F_{-i}, T_{-i}$, we have

$$\begin{aligned} &U_i(s_{-i}, s_i = \mathcal{C}) = \\ &\quad \sum_{(R_F,R_T)\in\mathcal{R}_{-i}} \prod_{W_f \in R_F} p_{\mathcal{C}}^{(f)} \prod_{W_t \in R_T} (1 - p_{\mathcal{C}}^{(t)}) \mathbf{E}[w^{(i)}_{\substack{F_{-i}\cup R_F, \\ T_{-i}\cup R_T, \\ s_i = \mathcal{C}}}], \\ &U_i(s_{-i}, s_i = \overline{\mathcal{C}}) = \\ &\quad \sum_{(R_F,R_T)\in\mathcal{R}_{-i}} \prod_{W_f \in R_F} p_{\mathcal{C}}^{(f)} \prod_{W_t \in R_T} (1 - p_{\mathcal{C}}^{(t)}) \mathbf{E}[w^{(i)}_{\substack{F_{-i}\cup R_F, \\ T_{-i}\cup R_T, \\ s_i = \overline{\mathcal{C}}}}]. \end{aligned}$$

In order to find conditions for a desired equilibrium, we study

$$\Delta U_i(s) = U_i(s_{-i}, s_i = \mathcal{C}) - U_i(s_{-i}, s_i = \overline{\mathcal{C}}).$$

For clarity, define $N_{F-i} = \sum_{S \in F_{-i} \cup R_F} |S|$, $N_{T-i} = \sum_{S \in T_{-i} \cup R_T} |S|$, and, for each partition $(R_F, R_T) \in \mathcal{R}_i$, let $\Delta w_{\mathcal{C}}^{(i)} = \mathbf{E}[w_{s_i=\mathcal{C}}^{(i)}] - \mathbf{E}[w_{s_i=\overline{\mathcal{C}}}^{(i)}]$, when $N_{F-i} - N_{T-i} > |W_i|$, $\Delta w_{\overline{\mathcal{C}}}^{(i)} = \mathbf{E}[w_{s_i=\mathcal{C}}^{(i)}] - \mathbf{E}[w_{s_i=\overline{\mathcal{C}}}^{(i)}]$, when $N_{T-i} - N_{F-i} > |W_i|$, and $\Delta w_X^{(i)} = \mathbf{E}[w_{s_i=\mathcal{C}}^{(i)}] - \mathbf{E}[w_{s_i=\overline{\mathcal{C}}}^{(i)}]$, when $|N_{F-i} - N_{T-i}| < |W_i|$. Given that the payoff depends only on the outcome majority, we have

$$\Delta U_i(s) =$$
$$\Delta w_{\mathcal{C}}^{(i)} \sum_{\substack{(R_F,R_T)\in\mathcal{R}_{-i} \\ N_{F-i}-N_{T-i}>|W_i|}} \prod_{W_f\in R_F} p_{\mathcal{C}}^{(f)} \prod_{W_t\in R_T} (1-p_{\mathcal{C}}^{(t)})+$$
$$\Delta w_{X}^{(i)} \sum_{\substack{(R_F,R_T)\in\mathcal{R}_{-i} \\ |N_{F-i}-N_{T-i}|<|W_i|}} \prod_{W_f\in R_F} p_{\mathcal{C}}^{(f)} \prod_{W_t\in R_T} (1-p_{\mathcal{C}}^{(t)})+$$
$$\Delta w_{\overline{\mathcal{C}}}^{(i)} \sum_{\substack{(R_F,R_T)\in\mathcal{R}_{-i} \\ N_{T-i}-N_{F-i}>|W_i|}} \prod_{W_f\in R_F} p_{\mathcal{C}}^{(f)} \prod_{W_t\in R_T} (1-p_{\mathcal{C}}^{(t)}). \tag{3}$$

Restating the equilibrium conditions of Equations (1) or (2) in terms of Equation (3), for each group $i \in R$ that does not choose a pure strategy, the equilibrium condition is $\Delta U_i(s) = 0$; for each group $i \in F$ (i.e., that chooses to cheat as a pure strategy) the condition is $\Delta U_i(s) \geq 0$; and for each group $i \in T$, it must hold that $\Delta U_i(s) \leq 0$.

Lemma 1. *Given a game as defined, if $\Delta w_{\mathcal{C}}^{(i)} \geq \Delta w_{X}^{(i)} \geq \Delta w_{\overline{\mathcal{C}}}^{(i)}$ for every group $W_i \in W$, then there is no unique equilibrium where $R \neq \emptyset$ (i.e, all groups decide deterministically).*

Proof. For the sake of contradiction, assume there is a unique equilibrium σ for which $R \neq \emptyset$ and $\Delta w_{\mathcal{C}}^{(i)} \geq \Delta w_{X}^{(i)} \geq \Delta w_{\overline{\mathcal{C}}}^{(i)}$ for every group $W_i \in W$. Then, for every group $W_i \in R$, $\Delta U_i(s) = 0$ must be solvable. If $\Delta w_{\mathcal{C}}^{(i)} \geq 0$, for all $W_i \in R$, there would be also an equilibrium where all groups in R choose to cheat and σ would not be unique, which is a contradiction. Consider now the case where there exists some $W_i \in R$ such that $\Delta w_{\mathcal{C}}^{(i)} < 0$. Then, it must hold that $|R| > 1$, otherwise $\Delta U_i = 0$ is false for W_i. Given that $|R| > 1$, the probabilities given by the summations in Equation (3) for W_i are all strictly bigger than zero. Therefore, given that $\Delta U_i = 0$ must be solvable, at least one of $\Delta w_{X}^{(i)} > 0$ and $\Delta w_{\overline{\mathcal{C}}}^{(i)} > 0$ must hold, which is also a contradiction with the assumption that $\Delta w_{\mathcal{C}}^{(i)} \geq \Delta w_{X}^{(i)} \geq \Delta w_{\overline{\mathcal{C}}}^{(i)}$.

In the following sections, conditions to obtain unique equilibria under different payoff models are studied. In all these models it holds that $\Delta w_{\mathcal{C}}^{(i)} \geq \Delta w_{X}^{(i)} \geq \Delta w_{\overline{\mathcal{C}}}^{(i)}$ for all $W_i \in W$. Then, by Lemma 1, there is no unique equilibrium where $R \neq \emptyset$. Regarding equilibria where $R = \emptyset$, unless the task assigned has a binary output (the answer can be negated), a unique equilibrium where all groups choose to cheat is not useful. Then, we make $\Delta w_{\mathcal{C}}^{(i)} < 0$, $\Delta w_{X}^{(i)} < 0$ and $\Delta w_{\overline{\mathcal{C}}}^{(i)} < 0$ for all $W_i \in W$ so that $\Delta U_i \geq 0$ has no solution and no group can choose to cheat as a pure strategy. Thus, the only equilibrium is for all the groups to choose to be honest, which solves $\Delta U_i \leq 0$. Therefore, $p_{\mathcal{C}}^{(i)} = 0$, $\forall W_i \in W$, and hence $\mathbf{P}_{wrong} = 0$.

Reward Model $\mathcal{R}_{\mathrm{m}}$. Replacing appropriately the payoffs detailed in Table 2, we obtain for any group $W_i \in W$

$$\begin{aligned}
\Delta w_{\mathcal{C}}^{(i)} &= -p_{\mathcal{V}}|W_i|(WP_{\mathcal{C}} + 2\,WB_{\mathcal{A}}) + |W_i|\,WB_{\mathcal{A}} + WC_{\mathcal{T}},\\
\Delta w_{X}^{(i)} &= -p_{\mathcal{V}}|W_i|(WP_{\mathcal{C}} + WB_{\mathcal{A}}) + WC_{\mathcal{T}},\\
\Delta w_{\overline{\mathcal{C}}}^{(i)} &= -p_{\mathcal{V}}|W_i|\,WP_{\mathcal{C}} - |W_i|\,WB_{\mathcal{A}} + WC_{\mathcal{T}}.
\end{aligned}$$

To make $\Delta w_{\mathcal{C}}^{(i)} < 0$ we want

$$p_{\mathcal{V}} > \frac{|W_i|\,WB_{\mathcal{A}} + WC_{\mathcal{T}}}{|W_i|(WP_{\mathcal{C}} + 2\,WB_{\mathcal{A}})}, \forall W_i \in W.$$

And the expected utilities are then

$$\begin{aligned}
U_M &= MB_{\mathcal{R}} - p_{\mathcal{V}}MC_{\mathcal{V}} - nMC_{\mathcal{A}}\\
U_{W_i} &= |W_i|\,WB_{\mathcal{A}} - WC_{\mathcal{T}},\ \text{for each } W_i \in W.
\end{aligned}$$

Reward Model $\mathcal{R}_{\mathrm{a}}$. Similarly, for any group $W_i \in W$,

$$\begin{aligned}
\Delta w_{\mathcal{C}}^{(i)} &= -p_{\mathcal{V}}|W_i|(WP_{\mathcal{C}} + WB_{\mathcal{A}}) + WC_{\mathcal{T}},\\
\Delta w_{X}^{(i)} &= -p_{\mathcal{V}}|W_i|(WP_{\mathcal{C}} + WB_{\mathcal{A}}) + WC_{\mathcal{T}},\\
\Delta w_{\overline{\mathcal{C}}}^{(i)} &= -p_{\mathcal{V}}|W_i|(WP_{\mathcal{C}} + WB_{\mathcal{A}}) + WC_{\mathcal{T}}.
\end{aligned}$$

Then, the condition to obtain the desired unique equilibrium and the expected utilities are

$$\begin{aligned}
p_{\mathcal{V}} &> \frac{WC_{\mathcal{T}}}{|W_i|(WP_{\mathcal{C}} + WB_{\mathcal{A}})}, \forall W_i \in W,\\
U_M &= MB_{\mathcal{R}} - p_{\mathcal{V}}MC_{\mathcal{V}} - nMC_{\mathcal{A}},\\
U_{W_i} &= |W_i|\,WB_{\mathcal{A}} - WC_{\mathcal{T}},\ \text{for each } W_i \in W.
\end{aligned}$$

Reward Model $\mathcal{R}_{\emptyset}$. Again, for any group $W_i \in W$,

$$\begin{aligned}
\Delta w_{\mathcal{C}}^{(i)} &= -p_{\mathcal{V}}|W_i|(WP_{\mathcal{C}} + WB_{\mathcal{A}}) + WC_{\mathcal{T}},\\
\Delta w_{X}^{(i)} &= -p_{\mathcal{V}}|W_i|(WP_{\mathcal{C}} + WB_{\mathcal{A}}) + WC_{\mathcal{T}},\\
\Delta w_{\overline{\mathcal{C}}}^{(i)} &= -p_{\mathcal{V}}|W_i|(WP_{\mathcal{C}} + WB_{\mathcal{A}}) + WC_{\mathcal{T}}.
\end{aligned}$$

And the condition to obtain the unique equilibrium and the expected utilities are

$$\begin{aligned}
p_{\mathcal{V}} &> \frac{WC_{\mathcal{T}}}{|W_i|(WP_{\mathcal{C}} + WB_{\mathcal{A}})}, \forall W_i \in W,\\
U_M &= MB_{\mathcal{R}} - p_{\mathcal{V}}(MC_{\mathcal{V}} + nMC_{\mathcal{A}}),\\
U_{W_i} &= p_{\mathcal{V}}|W_i|\,WB_{\mathcal{A}} - WC_{\mathcal{T}},\ \text{for each } W_i \in W.
\end{aligned}$$

In order to maximize the master utility we would like to design games where $p_\mathcal{V}$ is small. Therefore, we look for a lower bound on $p_\mathcal{V}$. It is easy to see that, in all of the three payoff models, the worst case lower bound is given by the group of minimum size. Although at a first glance this fact seems counterintuitive, it is not surprising due to the following two reasons. On one hand, colluders are likely to be in the majority, but the unique equilibrium occurs when all workers are honest. On the other hand, the extra benefit that workers obtain by colluding is not against the master interest since it is just a saving in computation costs.

3.4 Game 1:n: One Master - n Workers

We now observe how the conditions obtained in the previous game are modified if the master also participates as a player. The equilibria analysis regarding groups follows the same lines as in Section 3.3. However, now Equations (1) and (2) have to be applied to the master, as follows.

General Payoffs Model. Recall that R is the set of groups that randomize their choice. Let $\mathcal{R}$ be the set of partitions in two subsets (R_F, R_T) of R, i.e., $\mathcal{R} = \{(R_F, R_T) | R_F \cap R_T = \emptyset \wedge R_F \cup R_T = R\}$. Then, for the master,

$$U_M(R, F, T, s_M = \mathcal{V}) = \sum_{(R_F,R_T)\in\mathcal{R}} \prod_{f\in R_F} p_\mathcal{C}^{(f)} \prod_{t\in R_T} (1 - p_\mathcal{C}^{(t)}) m_{\substack{F\cup R_F,\\ T\cup R_T,\\ s_M=\mathcal{V}}}$$

$$U_M(R, F, T, s_M = \overline{\mathcal{V}}) = \sum_{(R_F,R_T)\in\mathcal{R}} \prod_{f\in R_F} p_\mathcal{C}^{(f)} \prod_{t\in R_T} (1 - p_\mathcal{C}^{(t)}) m_{\substack{F\cup R_F,\\ T\cup R_T,\\ s_M=\overline{\mathcal{V}}}}.$$

From Equation (1), if $p_\mathcal{V} \in (0, 1)$, the MSNE condition is $U_M(R, F, T, s_M = \mathcal{V}) = U_M(R, F, T, s_M = \overline{\mathcal{V}})$. From Equation (2), if $p_\mathcal{V} = 0$ the condition is $U_M(R, F, T, s_M = \mathcal{V}) \leq U_M(R, F, T, s_M = \overline{\mathcal{V}})$, and if $p_\mathcal{V} = 1$ the condition is $U_M(R, F, T, s_M = \mathcal{V}) \geq U_M(R, F, T, s_M = \overline{\mathcal{V}})$.

The MSNE conditions for groups are the same as in Section 3.3. Hence, the conditions obtained for each of the reward models are the same. However, additional conditions are obtained from the master-utility conditions as follows. As in Section 3.3, the desired unique MSNE occurs when $p_\mathcal{C} = 0$. Using that, in the master-utility conditions we get for the reward model $\mathcal{R}_\mathrm{m}$ that if $p_\mathcal{V} < 1$, $MB_\mathcal{R} - MC_\mathcal{V} - nMC_\mathcal{A} = MB_\mathcal{R} - nMC_\mathcal{A}$, and if $p_\mathcal{V} = 1$, $MB_\mathcal{R} - MC_\mathcal{V} - nMC_\mathcal{A} \geq MB_\mathcal{R} - nMC_\mathcal{A}$. Therefore, in any case it must hold $MC_\mathcal{V} = 0$. For the reward model $\mathcal{R}_\mathrm{a}$, the master-utility conditions give, if $p_\mathcal{V} < 1$, $MB_\mathcal{R} - MC_\mathcal{V} - nMC_\mathcal{A} = MB_\mathcal{R} - nMC_\mathcal{A}$ and if $p_\mathcal{V} = 1$, $MB_\mathcal{R} - MC_\mathcal{V} - nMC_\mathcal{A} \geq MB_\mathcal{R} - nMC_\mathcal{A}$. Therefore, again, $MC_\mathcal{V} = 0$. Finally, for the reward model $\mathcal{R}_\emptyset$, the master-utility conditions give if $p_\mathcal{V} < 1$, $MB_\mathcal{R} - MC_\mathcal{V} - nMC_\mathcal{A} = MB_\mathcal{R}$ and if $p_\mathcal{V} = 1$, $MB_\mathcal{R} - MC_\mathcal{V} - nMC_\mathcal{A} \geq MB_\mathcal{R}$. Therefore, $MC_\mathcal{V} = MC_\mathcal{A} = 0$. Hence, to achieve the goal of forcing the groups to be honest, *in this game, verifying must be free for the master.*

4 Algorithmic Mechanisms

In this section two realistic scenarios in which the master-worker model considered could be naturally applicable are proposed. For these scenarios, we determine appropriate games and parameters to be used by the master to maximize its benefit.

The basic protocol (mechanism) used by the master to accept the correct task result while maximizing its benefit is as follows: Given the payoffs parameters (these can either be fixed exogenously or be chosen by the master), the master sends the task (to be computed), the game to be played, the probability of verification $p_{\mathcal{V}}$, the payoff model to be used, and a certificate to the workers. After receiving the replies from all workers, and independently of the distribution of the answers, the master processor chooses to verify the answers with the probability $p_{\mathcal{V}}$. If the answers were not verified it accepts the result of the majority. Then, it applies the corresponding reward model. The protocol is detailed in Algorithm 1.

Algorithm 1: Master algorithm

```
send (task, game, p_V, payoff model R, certificate) to all workers
upon receiving all answers do
    verify the answers with probability p_V
    if the answers were not verified then
        accept the majority
    end
    apply the reward model
endupon
```

Hence, the master, given the payoff parameters, can determine the game and parameters (including the value of $p_{\mathcal{V}}$) to force the workers into a unique NE, that would result to the correct task result (with high probability) while maximizing the master's benefit. Examples of specific parameters (including the value of $p_{\mathcal{V}}$) and games such that the master can achieve this are analyzed in the following subsections.

For computational reasons, the master also sends a certificate to the workers. The certificate includes the strategy that if the workers play will lead them to the unique NE, together with the appropriate data to demonstrate this fact. More details for the use of the certificate are given in Section 4.3.

4.1 SETI-like Scenario

The first scenario considered is a volunteering computing system such as SETI@home, where users accept to donate part of their processors idle time to collaborate in the computation of large tasks. In this case, we assume that workers incur in no cost to perform the task, but they obtain a benefit by being recognized as having performed it (possibly in the form of prestige, e.g, by being included on SETI's top contributors list). Hence, we assume that $WB_{\mathcal{A}} > WC_{\mathcal{T}} = 0$. The master incurs in a (possibly small) cost $MC_{\mathcal{A}}$ when rewarding a worker (e.g., by advertising its participation in the project). As assumed in the general model, in this model the master may verify the values returned by the workers, at a cost $MC_{\mathcal{V}} > 0$. We also assume that the master obtains a benefit $MB_{\mathcal{R}} > MC_{\mathcal{A}}$ if it accepts the correct result of the task, and suffers a cost $MP_{\mathcal{W}} > MC_{\mathcal{V}}$ if it accepts an incorrect value.

Under these constraints, the equilibria for games 1:1 and $1{:}1^n$ collapse to one single equilibrium point. Also, since game $1{:}n$ requires free verification ($MC_{\mathcal{V}} = 0$) for the equilibrium to be unique, it cannot be used in this scenario. The different applicable cases are summarized in Table 5. In this table it can be observed that in games 1:1 and $1{:}1^n$ the equilibrium is achieved with any value of $p_{\mathcal{C}}$ in an interval. The master has no way to force the specific value of $p_{\mathcal{C}}$ that a worker uses within the interval. And, in particular, it cannot force $p_{\mathcal{C}} = 0$ (i.e., $\mathbf{P}_{wrong} = 0$). Additionally, looking at the master utility, all games have $U_M < MB_{\mathcal{R}}$. However, in game ($0{:}n$,$\mathcal{R}_\emptyset$) the master can make U_M arbitrarily close to $MB_{\mathcal{R}}$ by setting $p_{\mathcal{V}}$ arbitrarily small. (Notice that the utility of a worker will be arbitrarily small likewise, but given that workers are volunteering this is not a problem.) *In conclusion, the game ($0{:}n$,$\mathcal{R}_\emptyset$) with $n = 1$ ($|W| = |W_i| = 1$) and very small $p_{\mathcal{V}}$ is the best choice in this scenario, since it satisfies $\mathbf{P}_{wrong} = 0$ and $U_M \approx MB_{\mathcal{R}}$.*

4.2 Contractor Scenario

The second scenario considered is a company that buys computational power from Internet users and sells it to computation-hungry costumers. In this case the company pays the users an amount $S = WB_{\mathcal{A}} = MC_{\mathcal{A}}$ for using their computing capabilities, and charges the consumers another amount $MB_{\mathcal{R}} > MC_{\mathcal{A}}$ for the provided service. Since the users are not altruistic in this scenario, we assume that computing a task is not free for them (i.e., $WC_{\mathcal{T}} > 0$), and they must have incentives to participate (i.e., $U_{W_i} > 0, \forall W_i \in W$). As in the previous case, we assume that the master verifies and has a cost for accepting a wrong value, such that $MP_{\mathcal{W}} > MC_{\mathcal{V}} > 0$. Again, under these assumptions, the equilibria for games 1:1 and $1{:}1^n$ collapse to unique equilibria and game $1{:}n$ can not be used. The different cases are summarized in Table 6. Observe that there are cases in this table in which the group has negative expected utility U_{W_i}. Given that in this scenario workers are not altruistic, they will not accept to participate in such a game. This fact immediately rules out games (1:1,$\mathcal{R}_\emptyset$) and ($1{:}1^n$,$\mathcal{R}_\emptyset$). Similarly, this restriction forces the master to use a value of $p_{\mathcal{V}} > WC_{\mathcal{T}}/|W_i|\, WB_{\mathcal{A}}, \forall W_i \in W$ in game ($0{:}n$,$\mathcal{R}_\emptyset$). Finally, comparing games ($0{:}n$,$\mathcal{R}_{\mathrm{m}}$) and ($0{:}n$,$\mathcal{R}_{\mathrm{a}}$), it can be seen that the master would never choose the former, because the lower bound of $p_{\mathcal{V}}$ is smaller in the latter while the rest of expressions are the same, which leads to a larger master utility.

In this scenario, beyond choosing the game and number of workers as in the previous one, we assume that the master can also choose the reward $WB_{\mathcal{A}}$ to the workers for correctly computing the task, and the punishment $WP_{\mathcal{C}}$ if they are caught returning an incorrect value. All possible combined variations of these parameters yield a huge number of cases to be considered. In this work, we assume that the master only can choose one of these parameters, while the rest are predefined. A study of richer combinations is left for future work.

The following notation is used for clarity. Whenever a parameter may be different among different games being compared, a super-index indicates the game to which the parameter belongs. For instance, $U_M^{(i,j)}$ is the utility of the master for game (i,j). $MC_{\mathcal{A}}$ and $WB_{\mathcal{A}}$ are referred to as simply S $(= MC_{\mathcal{A}} = WB_{\mathcal{A}})$.

A simple observation of games $(0{:}n,\mathcal{R}_{\rm a})$ and $(0{:}n,\mathcal{R}_{\emptyset})$ leads to find that in both cases it is convenient for the master to choose the smallest possible value of $p_{\mathcal{V}}$. For this reason, in the following we assume in these games values $p_{\mathcal{V}}^{(0:n,\mathcal{R}_{\rm a})} = \frac{WC_{\mathcal{T}}}{WP_{\mathcal{C}}+S} + \gamma^{(0:n,\mathcal{R}_{\rm a})}$ and $p_{\mathcal{V}}^{(0:n,\mathcal{R}_{\emptyset})} = \frac{WC_{\mathcal{T}}}{S} + \gamma^{(0:n,\mathcal{R}_{\emptyset})}$, for arbitrarily small $\gamma^{(0:n,\mathcal{R}_{\rm a})} > 0$ and $\gamma^{(0:n,\mathcal{R}_{\emptyset})} > 0$ [4].

Tunable n: Regarding games $(1{:}1,\mathcal{R}_{\rm m})$ and $(1{:}1^n,\mathcal{R}_{\rm m})$, in this case the master has no control over $p_{\mathcal{C}}$ or $p_{\mathcal{V}}$, since they are completely defined by the application parameters. Hence, the probability of accepting a wrong answer might be arbitrarily close to 1, even for game $(1{:}1^n,\mathcal{R}_{\rm m})$, because $\mathbf{P}_{\mathcal{C}}$ grows with n if $p_{\mathcal{C}} > 1/2$ as shown in Claim 4.2. Given that we want to design a mechanism that can be applied to any setting, we rule out these games for this case. In the case that n is tunable, the benefit of the master in games $(0{:}n,\mathcal{R}_{\rm a})$ and $(0{:}n,\mathcal{R}_{\emptyset})$ decreases as n increases. Hence for these games the master chooses $n = 1$. (So, $|W| = |W_i| = 1$.) Additionally, these games provide $\mathbf{P}_{wrong} = 0$. *Out of these games, $(0{:}n,\mathcal{R}_{\rm a})$ is better iff $WC_{\mathcal{T}} + WC_{\mathcal{T}}MC_{\mathcal{V}}/S > S + WC_{\mathcal{T}}MC_{\mathcal{V}}/(WP_{\mathcal{C}}+S)$.*

Tunable $WP_{\mathcal{C}}$: Comparing games $(0{:}n,\mathcal{R}_{\rm a})$ and $(0{:}n,\mathcal{R}_{\emptyset})$, $U_M^{(0:n,\mathcal{R}_{\rm a})} = MB_{\mathcal{R}} - p_{\mathcal{V}}^{(0:n,\mathcal{R}_{\rm a})}MC_{\mathcal{V}} - nS = MB_{\mathcal{R}} - WC_{\mathcal{T}}MC_{\mathcal{V}}/(S + WP_{\mathcal{C}}{}^{(0:n,\mathcal{R}_{\rm a})}) - nS - \gamma^{(0:n,\mathcal{R}_{\rm a})}MC_{\mathcal{V}}$ and $U_M^{(0:n,\mathcal{R}_{\emptyset})} = MB_{\mathcal{R}} - p_{\mathcal{V}}^{(0:n,\mathcal{R}_{\emptyset})}MC_{\mathcal{V}} - p_{\mathcal{V}}^{(0:n,\mathcal{R}_{\emptyset})}nS = MB_{\mathcal{R}} - WC_{\mathcal{T}}MC_{\mathcal{V}}/S - n\,WC_{\mathcal{T}} - \gamma^{(0:n,\mathcal{R}_{\emptyset})}MC_{\mathcal{V}} - \gamma^{(0:n,\mathcal{R}_{\emptyset})}nS$. *Thus, game $(0{:}n,\mathcal{R}_{\emptyset})$ is better iff $n > WC_{\mathcal{T}}MC_{\mathcal{V}}/S(S - WC_{\mathcal{T}})$ for small enough $\gamma^{(0:n,\mathcal{R}_{\emptyset})}$. Otherwise, $(0{:}n,\mathcal{R}_{\rm a})$ is better for small enough $\gamma^{(0:n,\mathcal{R}_{\rm a})}$ and large enough $WP_{\mathcal{C}}{}^{(0:n,\mathcal{R}_{\rm a})}$.* As argued in the previous case, in this case the master has no control over $p_{\mathcal{C}}$. Although the master can reduce $WP_{\mathcal{C}}$ to increase $p_{\mathcal{V}}$, it can not make $p_{\mathcal{V}}$ arbitrarily close to 1 to reduce $\mathbf{P}_{wrong}$ in case $p_{\mathcal{C}}$ is big (and consequently $\mathbf{P}_{\mathcal{C}}$). Then, some cases might lead to a big probability of accepting the wrong answer. Thus, games $(1{:}1,\mathcal{R}_{\rm m})$ and $(1{:}1^n,\mathcal{R}_{\rm m})$ are ruled out from consideration.

Tunable $S \in (WC_{\mathcal{T}}, MB_{\mathcal{R}})$: In this case n is fixed, and given that we do not make any assumptions about its magnitude, we evaluate game $1{:}1$ while evaluating game $1{:}1^n$ for an arbitrary n. Using calculus, the utility of the master for game $(0{:}n,\mathcal{R}_{\rm a})$ is maximum when $S_{\max}^{(0:n,\mathcal{R}_{\rm a})} = \pm\sqrt{MC_{\mathcal{V}}\,WC_{\mathcal{T}}/n} - WP_{\mathcal{C}}$. Due to the aforementioned constraints, only values in the interval $(WC_{\mathcal{T}}, MB_{\mathcal{R}})$ are valid for S. Assuming then that $WC_{\mathcal{T}} < S_{\max}^{(0:n,\mathcal{R}_{\rm a})} < MB_{\mathcal{R}}$, the utilities are $U_M^{(0:n,\mathcal{R}_{\rm a})}(S = S_{\max}^{(0:n,\mathcal{R}_{\rm a})}) = MB_{\mathcal{R}} - 2\sqrt{nMC_{\mathcal{V}}\,WC_{\mathcal{T}}} + n\,WP_{\mathcal{C}}$ and $U_M^{(0:n,\mathcal{R}_{\emptyset})} = MB_{\mathcal{R}} - WC_{\mathcal{T}}MC_{\mathcal{V}}/S^{(0:n,\mathcal{R}_{\emptyset})} - n\,WC_{\mathcal{T}} - \gamma^{(0:n,\mathcal{R}_{\emptyset})}(MC_{\mathcal{V}} + nS^{(0:n,\mathcal{R}_{\emptyset})})$. *Since $U_M^{(1:1^n,\mathcal{R}_{\rm m})} \leq MB_{\mathcal{R}}$, game $(0{:}n,\mathcal{R}_{\rm a})$ is better than game $(1{:}1^n,\mathcal{R}_{\rm m})$ whenever $n > 4MC_{\mathcal{V}}\,WC_{\mathcal{T}}/\,WP_{\mathcal{C}}{}^2$. On the other hand, game $(0{:}n,\mathcal{R}_{\emptyset})$ is better than game $(0{:}n,\mathcal{R}_{\rm a})$ if $MB_{\mathcal{R}} > WC_{\mathcal{T}}MC_{\mathcal{V}}/(2\sqrt{nMC_{\mathcal{V}}\,WC_{\mathcal{T}}} -$*

[4] We assume here the worst case scenario where $\min_{W_i \in W}\{|W_i|\} = 1$. If a better lower bound can be guaranteed, a similar analysis taking it into account follows.

$n(WP_{\mathcal{C}} + WC_{\mathcal{T}}))$, *for small enough* $\gamma^{(0:n,\mathcal{R}_\emptyset)}$ *and* $S^{(0:n,\mathcal{R}_\emptyset)}$ *arbitrarily close to* $MB_{\mathcal{R}}$. In order to show a scenario where game $(1:1^n.\mathcal{R}_{\rm m})$ is better, we assume now that $MP_{\mathcal{W}} \geq 2MC_{\mathcal{V}}$. Then, under this assumption, $p_{\mathcal{C}} \leq 1/2$. The following claim that makes use of this fact will be useful.

Claim. For game $1:1^n$, let $\mathbf{P}_{\mathcal{C}}(n)$ denote the probability that the majority out of n workers cheat. If the probability that a worker cheats is $p_{\mathcal{C}} \leq \frac{1}{2}$, then $\mathbf{P}_{\mathcal{C}}(n+2) \leq \mathbf{P}_{\mathcal{C}}(n)$.

Proof. Let $\mathbf{P}_{\mathcal{C}}(n, > 1)$ be the probability that, out of n workers, the number of cheaters exceed the number of honest workers by more than one (i.e., at least 3 given that we consider only odd number of workers), $\mathbf{P}_{\mathcal{C}}(n, = 1)$ by exactly one, and $\mathbf{P}_{\overline{\mathcal{C}}}(n, = 1)$ be the probability that the number of honest workers exceed the number of cheaters by exactly one. Then, $\mathbf{P}_{\mathcal{C}}(n+2) = \mathbf{P}_{\mathcal{C}}(n, > 1)(p_{\mathcal{C}}^2 + (1-p_{\mathcal{C}})^2) + \mathbf{P}_{\mathcal{C}}(n, = 1)(p_{\mathcal{C}}^2 + 2p_{\mathcal{C}}(1-p_{\mathcal{C}})) + \mathbf{P}_{\overline{\mathcal{C}}}(n, = 1)p_{\mathcal{C}}^2$. Bounding $p_{\mathcal{C}}$ the claim follows.

From the previous claim, given that $\mathbf{P}_{\mathcal{C}} = 1/2$ for $p_{\mathcal{C}} = 1/2$, we conclude that $\mathbf{P}_{\mathcal{C}} \leq 1/2$. Using that $p_{\mathcal{C}} \leq 1/2$, $\mathbf{P}_{\mathcal{C}} \leq 1/2$, and $MP_{\mathcal{W}} > 2MC_{\mathcal{V}}$, the utility of the master for game $(1{:}1^n,\mathcal{R}_{\rm m})$ is

$$\begin{aligned}
U_M^{(1:1^n,\mathcal{R}_{\rm m})} \geq & \frac{1}{2}MB_{\mathcal{R}} - p_{\mathcal{V}}^{(1:1^n,\mathcal{R}_{\rm m})}MC_{\mathcal{V}} \\
& - \frac{1}{2}(1 - p_{\mathcal{V}}^{(1:1^n,\mathcal{R}_{\rm m})})MP_{\mathcal{W}} - nS^{(1:1^n,\mathcal{R}_{\rm m})} \\
= & \frac{1}{2}MB_{\mathcal{R}} - p_{\mathcal{V}}^{(1:1^n,\mathcal{R}_{\rm m})}MC_{\mathcal{V}} - \frac{1}{2}MP_{\mathcal{W}} \\
& + \frac{1}{2}p_{\mathcal{V}}^{(1:1^n,\mathcal{R}_{\rm m})}MP_{\mathcal{W}} - nS^{(1:1^n,\mathcal{R}_{\rm m})} \\
\geq & \frac{1}{2}(MB_{\mathcal{R}} - MP_{\mathcal{W}}) - nS^{(1:1^n,\mathcal{R}_{\rm m})}.
\end{aligned}$$

As shown before, game ($0:n$,$\mathcal{R}_{\rm a}$*) is better than game (*$0:n$,$\mathcal{R}_\emptyset$*) when* $MB_{\mathcal{R}} < WC_{\mathcal{T}}MC_{\mathcal{V}}/(2\sqrt{nMC_{\mathcal{V}}WC_{\mathcal{T}}} - n(WP_{\mathcal{C}} + WC_{\mathcal{T}}))$. Comparing games $(1:1^n,\mathcal{R}_{\rm m})$ and $(0:n,\mathcal{R}_{\rm a})$ when $WC_{\mathcal{T}} < \sqrt{MC_{\mathcal{V}}WC_{\mathcal{T}}/n} - WP_{\mathcal{C}} < MB_{\mathcal{R}}$, we have $(MB_{\mathcal{R}} - MP_{\mathcal{W}})/2 - nS^{(1:1^n,\mathcal{R}_{\rm m})} \geq MB_{\mathcal{R}} - 2\sqrt{nMC_{\mathcal{V}}WC_{\mathcal{T}}} + nWP_{\mathcal{C}}$. *Therefore, game (*$1{:}1^n$,$\mathcal{R}_{\rm m}$*) is better whenever*

$$\begin{aligned}
WC_{\mathcal{T}} \leq S^{(1:1^n,\mathcal{R}_{\rm m})} \leq & 2\sqrt{\frac{MC_{\mathcal{V}}WC_{\mathcal{T}}}{n}} \\
& - \frac{1}{2n}(MB_{\mathcal{R}} + MP_{\mathcal{W}}) - WP_{\mathcal{C}} \qquad (4)
\end{aligned}$$

All three conditions are feasible simultaneously for big enough $MC_{\mathcal{V}}$, therefore there exists a scenario for which game $(1{:}1^n,\mathcal{R}_{\rm m})$ is better. Notice that under the aforementioned condition, for game $(0{:}n,\mathcal{R}_{\rm a})$ to be better, i.e., $n > 4MC_{\mathcal{V}}WC_{\mathcal{T}}/WP_{\mathcal{C}}{}^2$, it must be true that $WP_{\mathcal{C}} > 2\sqrt{MC_{\mathcal{V}}WC_{\mathcal{T}}/n}$ and the inequality (4) does not hold.

4.3 Computational Issues

In previous sections, a mechanism for the master to choose games, payoff models, and appropriate values of $p_{\mathcal{V}}$ for different scenarios was designed (based on Algorithm 1). A natural question is what is the computational cost of using such mechanism. In addition to simple arithmetical calculations, there are two kinds of relevant computations required: binomial probabilities and verification of conditions for Nash equilibria. Both computations are n-th degree polynomial evaluations and can be carried out using any of the well-known numerical tools [17] with polynomial asymptotic cost. These numerical methods yield only approximations, but all these calculations are performed either to decide in which case the parameters fit in, or to assign a value to $p_{\mathcal{V}}$, or to compare utilities. Given that these evaluations and assignments were obtained in the design as inequalities or restricted only to lower bounds, it is enough to choose the appropriate side of the approximation in each case. Regarding the computational resources that the workers require to carry out these calculations, notice that the choice of $p_{\mathcal{V}}$ in the mechanism only yields a unique NE. Then, in order to make the computation feasible to the workers, the master sends together with the task a certificate proving such equilibrium. Such a certificate is the value of $p_{\mathcal{V}}$, payoff values, game, and payoff model, which is enough to verify uniqueness.

5 Conclusions

In this paper we consider computational systems in which a master processor assigns tasks for execution to rational workers. We have defined the general model and cost-parameters, and we have proposed and analyzed several games that the master can choose to play in order to achieve high reliability at low cost. Based on our game analysis, we have designed appropriate algorithmic mechanisms for two realistic scenarios of these kinds of systems.

For future work we plan to design more complex mechanisms where more than one parameter at a time is tunable by the master, and consider other realistic scenarios where our work can be applied. It would also be interesting to consider the case where the workers and/or the master do not have complete information of all the system parameters. Another interesting research direction is to study trade-offs between reliability and cost in distributed systems with both selfish and destructively malicious workers.

References

1. I. Abraham, D. Dolev, R. Goden, and J.Y. Halpern. Distributed computing meets game theory: Robust mechanisms for rational secret sharing and multiparty computation. In *proc. of PODC 2006*, pp. 53–62, 2006.
2. D. Anderson. BOINC: A system for public-resource computing and storage. In *proc. of GRID 2004*, pp. 4–10, 2004.
3. M. Babaioff, M. Feldman, and N. Nisan. Mixed Strategies in Combinatorial Agency. In *proc. of WINE 2006*, pp. 353–364, 2006.

4. G. Cosmin Silaghi, F. Araujo, L. Moura Silva, P. Domingues, and A. E. Arenas. Defeating Colluding Nodes in Desktop Grid Computing Platforms *Journal of Grid Computing*, August 19, 2009, `http://www.springerlink.com/content/ d37g118k06413712/`.

5. J. R. Douceur and T. Moscibroda. Lottery trees: motivational deployment of networked systems In *proc. of SIGCOMM 2007*, pp. 121–132, 2007.

6. J. R. Douceur. The Sybil attack. In *proc. of IPTPS 2002*, pp. 251–260, 2002.

7. "Enabling Grids for E-sciencE", `http://www.eu-egee.org`.

8. J. Feigenbaum, Ch. Papadimitriou, R. Sami, and S. Shenker. A BGP-based mechanism for lowest-cost routing. *Distributed Computing*, 18(1):61–72, 2005.

9. A. Fernández, C. Georgiou, L. Lopez, and A. Santos. Reliably executing tasks in the presence of untrusted processors. In *proc. of SRDS 2006*, pp. 39–50, 2006.

10. I.T. Foster and A. Iamnitchi. On death, taxes, and the convergence of P2P and grid computing. In *proc. of IPTPS 2003*, pp. 118–128, 2003.

11. D. Fotakis. Memoryless facility location in one pass. In *proc. of STACS 2006*, pp. 608–620, 2006.

12. P. Golle and I. Mironov. Uncheatable distributed computations. In *proc. of CT-RSA 2001*, pp. 425–440, 2001.

13. P. Golle and S. Stubblebine. Secure distributed computing in a commercial environment. In *proc. of Financial Cryptography*, 2001.

14. M. Halldorsson, J.Y. Halpern, L. Li, and V. Mirrokni. On spectrum sharing games. In *proc. of PODC 2004*, pp. 107—114, 2004.

15. J.Y. Halpern. Computer science and game theory: A brief survey. *Palgrave Dictionary of Economics*, to appear.

16. J.Y. Halpern and V. Teague. Rational secret sharing and multiparty computation. In *proc. of STOC 2004*, pp. 623–632, 2004.

17. W. G. Horner. A new method of solving numerical equations of all orders by continuous approximation. *Philos. Trans. Roy. Soc. London* 109:308–335, 1819.

18. K.M. Konwar, S. Rajasekaran, and A.A. Shvartsman. Robust network supercomputing with malicious processes. In *proc. of DISC 2006*, pp. 474–488, 2006.

19. E. Korpela, D. Werthimer, D. Anderson, J. Cobb, and M. Lebofsky. SETI@home: Massively distributed computing for SETI. *Computing in Science and Engineering*, 3(1):78–83, 2001.

20. E. Koutsoupias and Ch. Papadimitriou. Worst-case equilibria. In *proc. of STACS 1999*, pp. 404–413, 1999.

21. M. Mavronicolas and P. Spirakis. The price of selfish routing. *Algorithmica*, 48(1):91–126, 2007.

22. T. Moscibroda, S. Schmid, and R. Wattenhofer. When selfish meets evil: byzantine players in a virus inoculation game. In *proc. of PODC 2006*, pp. 35–44, 2006.

23. J.F. Nash. Equilibrium points in n-person games. *National Academy of Sciences*, 36(1):48–49, 1950.

24. N. Nisan and A. Ronen. Algorithmic mechanism design. *Games and Economic Behavior*, 35:166–196, 2001.

25. N. Nisan, T. Roughgarden, E. Tardos, and V.V. Vazirani, editors. *Algorithmic Game Theory*. Cambridge University Press, 2007.

26. A. Lopez-Ortiz. Algorithmic foundations of the Internet. ACM SIGACT News Distributed Computing Column 18, 2005.

27. M.J. Osborne. *An Introduction to Game Theory.* Oxford University Press, 2003.

28. T. Roughgarden and E. Tardos. How bad is selfish routing? *Journal of ACM*, 49(2):236–259, 2002.

29. J. Shneidman and D.C. Parkes. Rationality and self-interest in P2P networks. In *proc. of IPTPS 2003*, pp. 139–148, 2003.

30. E. Staab and T. Engel. Collusion Detection for Grid Computing. In *proc. of CCGRID 2009*, pp 412–419, 2009.

31. “TeraGrid”, `http://www.teragrid.org`.

32. M. Yurkewych, B.N. Levine, and A.L. Rosenberg. On the cost-ineffectiveness of redundancy in commercial P2P computing. In *proc. of CCS 2005*, pp. 280–288, 2005.

$W = \{W_1, \ldots, W_\ell\}$	set of worker groups
M	master processor
$\mathcal{S}_i = \{\mathcal{C}, \overline{\mathcal{C}}\}$	set of pure strategies available to group W_i
$\mathcal{S}_M = \{\mathcal{V}, \overline{\mathcal{V}}\}$	set of pure strategies of the master
s	strategy profile (a mapping from players to pure strategies)
s_i	strategy used by group W_i in the strategy profile s
s_M	strategy used by the master in the strategy profile s
s_{-i}	strategy used by each player but W_i in the strategy profile s
s_{-M}	strategy used by each player but the master in the strategy profile s
$w_s^{(i)}$	payoff of group W_i for the strategy profile s
m_s	payoff of the master for the strategy profile s
$p_{s_i}^{(i)}$	probability that group W_i uses strategy s_i
p_{s_M}	probability that the master uses strategy s_M
σ	mixed strategy profile (a mapping from players to prob. distrib. over pure strategies)
σ_i	probability distribution over pure strategies used by group W_i in σ
σ_M	probability distribution over pure strategies used by the master in σ
σ_{-i}	probability distribution over pure strategies used by each player but W_i in σ
σ_{-M}	probability distribution over pure strategies used by each player but the master in σ
$U_i(s_i, \sigma_{-i})$	expected utility of group W_i with mixed strategy profile σ
$U_M(s_M, \sigma_{-M})$	expected utility of master with mixed strategy profile σ
$supp(\sigma_i)$	set of strategies of group W_i with probability > 0 in σ
$supp(\sigma_M)$	set of strategies of the master with probability > 0 in σ

Table 1. Game notation

$WP_{\mathcal{C}}$	worker's punishment for being caught cheating
$WC_{\mathcal{T}}$	group's cost for computing the task
$WB_{\mathcal{A}}$	worker's benefit from master's acceptance
$MP_{\mathcal{W}}$	master's punishment for accepting a wrong answer
$MC_{\mathcal{A}}$	master's cost for accepting the worker's answer
$MC_{\mathcal{V}}$	master's cost for verifying worker's answers
$MB_{\mathcal{R}}$	master's benefit from accepting the right answer

Table 2. Payoffs

Equilibrium $p_{\mathcal{C}}, p_{\mathcal{V}}$	Conditions	$\mathbf{P}_{wrong}$	U_M	U_{W_i}
$\frac{MC_{\mathcal{V}}}{MC_{\mathcal{A}}+MP_{\mathcal{W}}}, \frac{WC_{\mathcal{T}}}{WB_{\mathcal{A}}+WP_{\mathcal{C}}}$		$(1-p_{\mathcal{V}})\mathbf{P}_{\mathcal{C}}$	$p_{\mathcal{V}}((1-p_{\mathcal{C}}^n)MB_{\mathcal{R}}-$ $MC_{\mathcal{V}}-(1-p_{\mathcal{C}})nMC_{\mathcal{A}})+$ $(1-p_{\mathcal{V}})(MB_{\mathcal{R}}(1-\mathbf{P}_{\mathcal{C}})-$ $MP_{\mathcal{W}}\mathbf{P}_{\mathcal{C}}-nMC_{\mathcal{A}})$	$WB_{\mathcal{A}}-WC_{\mathcal{T}}$
$0, \frac{WC_{\mathcal{T}}}{WB_{\mathcal{A}}+WP_{\mathcal{C}}} \leq p_{\mathcal{V}} < 1$ $0 < p_{\mathcal{V}}$	$MC_{\mathcal{V}}=0$	0	$MB_{\mathcal{R}}-nMC_{\mathcal{A}}$	$WB_{\mathcal{A}}-WC_{\mathcal{T}}$
$1, 0 < p_{\mathcal{V}} \leq \frac{WC_{\mathcal{T}}}{WB_{\mathcal{A}}+WP_{\mathcal{C}}}$ $p_{\mathcal{V}} < 1$	$MC_{\mathcal{V}}=MP_{\mathcal{W}}+MC_{\mathcal{A}}$	$1-p_{\mathcal{V}}$	$-p_{\mathcal{V}}MC_{\mathcal{V}}-(1-p_{\mathcal{V}})(MP_{\mathcal{W}}+nMC_{\mathcal{A}})$	$(1-p_{\mathcal{V}})WB_{\mathcal{A}}-$ $p_{\mathcal{V}}WP_{\mathcal{C}}$
$0 \leq p_{\mathcal{C}} \leq \frac{MC_{\mathcal{V}}}{MC_{\mathcal{A}}+MP_{\mathcal{W}}}, 0$ $p_{\mathcal{C}} < 1$	$WC_{\mathcal{T}}=0$	$\mathbf{P}_{\mathcal{C}}$	$MB_{\mathcal{R}}(1-\mathbf{P}_{\mathcal{C}})-MP_{\mathcal{W}}\mathbf{P}_{\mathcal{C}}-nMC_{\mathcal{A}}$	$WB_{\mathcal{A}}$
$\frac{MC_{\mathcal{V}}}{MC_{\mathcal{A}}+MP_{\mathcal{W}}} \leq p_{\mathcal{C}} < 1, 1$ $0 < p_{\mathcal{C}}$	$WC_{\mathcal{T}}=WB_{\mathcal{A}}+WP_{\mathcal{C}}$	0	$(1-\prod_{j\in W}p_{\mathcal{C}}^{(j)})MB_{\mathcal{R}}-MC_{\mathcal{V}}-$ $\sum_{(W_F,W_T)\in\mathcal{W}}\prod_{j\in W_F}p_{\mathcal{C}}^{(j)}\cdot$ $\prod_{k\in W_T}(1-p_{\mathcal{C}}^{(k)})\lvert W_T\rvert MC_{\mathcal{A}}$	$-WP_{\mathcal{C}}$
1, 1	$MC_{\mathcal{V}} \leq MP_{\mathcal{W}}+MC_{\mathcal{A}}$ $WC_{\mathcal{T}} \geq WB_{\mathcal{A}}+WP_{\mathcal{C}}$	0	$-MC_{\mathcal{V}}$	$-WP_{\mathcal{C}}$
0, 1	$MC_{\mathcal{V}}=0$ $WC_{\mathcal{T}} \leq WB_{\mathcal{A}}+WP_{\mathcal{C}}$	0	$MB_{\mathcal{R}}-nMC_{\mathcal{A}}$	$WB_{\mathcal{A}}-WC_{\mathcal{T}}$
1, 0	$MC_{\mathcal{V}} \geq MP_{\mathcal{W}}+MC_{\mathcal{A}}$	1	$-MP_{\mathcal{W}}-nMC_{\mathcal{A}}$	$WB_{\mathcal{A}}$

Table 3. Game 1:1^n, Models $\mathcal{R}_{\mathrm{m}}$ and $\mathcal{R}_{\mathrm{a}}$ (and Game 1:1 for $n=1$)

Equilibrium $p_{\mathcal{C}}, p_{\mathcal{V}}$	Conditions	$\mathbf{P}_{wrong}$	U_M	U_{W_i}
$\frac{MC_{\mathcal{V}}+MC_{\mathcal{A}}}{MC_{\mathcal{A}}+MP_{\mathcal{W}}}, \frac{WC_{\mathcal{T}}}{WB_{\mathcal{A}}+WP_{\mathcal{C}}}$		$(1-p_{\mathcal{V}})\mathbf{P}_{\mathcal{C}}$	$p_{\mathcal{V}}((1-p_{\mathcal{C}}^n)MB_{\mathcal{R}} - MC_{\mathcal{V}} - (1-p_{\mathcal{C}})nMC_{\mathcal{A}}) + (1-p_{\mathcal{V}})(MB_{\mathcal{R}}(1-\mathbf{P}_{\mathcal{C}}) - MP_{\mathcal{W}}\mathbf{P}_{\mathcal{C}})$	$-p_{\mathcal{V}}\, WP_{\mathcal{C}}$
$0, \frac{WC_{\mathcal{T}}}{WB_{\mathcal{A}}+WP_{\mathcal{C}}} \leq p_{\mathcal{V}} < 1$ $0 < p_{\mathcal{V}}$	$MC_{\mathcal{A}} = MC_{\mathcal{V}} = 0$	0	$MB_{\mathcal{R}}$	$p_{\mathcal{V}}\, WB_{\mathcal{A}} - WC_{\mathcal{T}}$
$1, 0 < p_{\mathcal{V}} \leq \frac{WC_{\mathcal{T}}}{WB_{\mathcal{A}}+WP_{\mathcal{C}}}$ $p_{\mathcal{V}} < 1$	$MC_{\mathcal{V}} = MP_{\mathcal{W}}$	$1-p_{\mathcal{V}}$	$-MC_{\mathcal{V}}$	$-p_{\mathcal{V}}\, WP_{\mathcal{C}}$
$0 \leq p_{\mathcal{C}} \leq \frac{MC_{\mathcal{V}}+MC_{\mathcal{A}}}{MC_{\mathcal{A}}+MP_{\mathcal{W}}}, 0$ $p_{\mathcal{C}} < 1$	$WC_{\mathcal{T}} = 0$	$\mathbf{P}_{\mathcal{C}}$	$MB_{\mathcal{R}}(1-\mathbf{P}_{\mathcal{C}}) - MP_{\mathcal{W}}\mathbf{P}_{\mathcal{C}}$	0
$\frac{MC_{\mathcal{V}}+MC_{\mathcal{A}}}{MC_{\mathcal{A}}+MP_{\mathcal{W}}} \leq p_{\mathcal{C}} < 1, 1$ $0 < p_{\mathcal{C}}$	$WC_{\mathcal{T}} = WB_{\mathcal{A}} + WP_{\mathcal{C}}$	0	$(1-\prod_{j\in W} p_{\mathcal{C}}^{(j)})MB_{\mathcal{R}} - MC_{\mathcal{V}} - \sum_{(W_F,W_T)\in\mathcal{W}} \prod_{j\in W_F} p_{\mathcal{C}}^{(j)} \cdot \prod_{k\in W_T}(1-p_{\mathcal{C}}^{(k)})\|W_T\|MC_{\mathcal{A}}$	$-WP_{\mathcal{C}}$
$1, 1$	$MC_{\mathcal{V}} \leq MP_{\mathcal{W}}$ $WC_{\mathcal{T}} \geq WB_{\mathcal{A}} + WP_{\mathcal{C}}$	0	$-MC_{\mathcal{V}}$	$-WP_{\mathcal{C}}$
$0, 1$	$MC_{\mathcal{V}} = MC_{\mathcal{A}} = 0$ $WC_{\mathcal{T}} \leq WB_{\mathcal{A}} + WP_{\mathcal{C}}$	0	$MB_{\mathcal{R}}$	$WB_{\mathcal{A}} - WC_{\mathcal{T}}$
$1, 0$	$MC_{\mathcal{V}} \geq MP_{\mathcal{W}}$	1	$-MP_{\mathcal{W}}$	0

Table 4. Game 1:1^n, Model $\mathcal{R}_\emptyset$ (and Game 1:1 for $n = 1$)

(Game,Model)	Equilibrium $p_{\mathcal{C}}, p_{\mathcal{V}}$	$\mathbf{P}_{wrong}$	U_M	U_{W_i}
(1:1,$\mathcal{R}_{\rm m}$), (1:1,$\mathcal{R}_{\rm a}$)	$0 \leq p_{\mathcal{C}} \leq \frac{MC_{\mathcal{V}}}{MC_{\mathcal{A}}+MP_{\mathcal{W}}}, p_{\mathcal{C}} < 1, p_{\mathcal{V}} = 0$	$p_{\mathcal{C}}$	$MB_{\mathcal{R}} - p_{\mathcal{C}}(MB_{\mathcal{R}} + MP_{\mathcal{W}}) - MC_{\mathcal{A}}$	$WB_{\mathcal{A}}$
(1:1,$\mathcal{R}_\emptyset$)	$0 \leq p_{\mathcal{C}} \leq \frac{MC_{\mathcal{V}}+MC_{\mathcal{A}}}{MC_{\mathcal{A}}+MP_{\mathcal{W}}}, p_{\mathcal{C}} < 1, p_{\mathcal{V}} = 0$	$p_{\mathcal{C}}$	$MB_{\mathcal{R}} - p_{\mathcal{C}}(MB_{\mathcal{R}} + MP_{\mathcal{W}})$	0
(1:1^n,$\mathcal{R}_{\rm m}$), (1:1^n,$\mathcal{R}_{\rm a}$)	$0 \leq p_{\mathcal{C}} \leq \frac{MC_{\mathcal{V}}}{MC_{\mathcal{A}}+MP_{\mathcal{W}}}, p_{\mathcal{C}} < 1, p_{\mathcal{V}} = 0$	$\mathbf{P}_{\mathcal{C}}$	$MB_{\mathcal{R}} - \mathbf{P}_{\mathcal{C}}(MB_{\mathcal{R}} + MP_{\mathcal{W}}) - nMC_{\mathcal{A}}$	$WB_{\mathcal{A}}$
(1:1^n,$\mathcal{R}_\emptyset$)	$0 \leq p_{\mathcal{C}} \leq \frac{MC_{\mathcal{V}}+MC_{\mathcal{A}}}{MC_{\mathcal{A}}+MP_{\mathcal{W}}}, p_{\mathcal{C}} < 1, p_{\mathcal{V}} = 0$	$\mathbf{P}_{\mathcal{C}}$	$MB_{\mathcal{R}} - \mathbf{P}_{\mathcal{C}}(MB_{\mathcal{R}} + MP_{\mathcal{W}})$	0
(0:n,$\mathcal{R}_{\rm m}$)	$p_{\mathcal{C}} = 0, \frac{WB_{\mathcal{A}}}{WP_{\mathcal{C}}+2WB_{\mathcal{A}}} < p_{\mathcal{V}} \leq 1$	0	$MB_{\mathcal{R}} - p_{\mathcal{V}}MC_{\mathcal{V}} - nMC_{\mathcal{A}}$	$\|W_i\|WB_{\mathcal{A}}$
(0:n,$\mathcal{R}_{\rm a}$)	$p_{\mathcal{C}} = 0, 0 < p_{\mathcal{V}} \leq 1$	0	$MB_{\mathcal{R}} - p_{\mathcal{V}}MC_{\mathcal{V}} - nMC_{\mathcal{A}}$	$\|W_i\|WB_{\mathcal{A}}$
(0:n,$\mathcal{R}_\emptyset$)	$p_{\mathcal{C}} = 0, 0 < p_{\mathcal{V}} \leq 1$	0	$MB_{\mathcal{R}} - p_{\mathcal{V}}(MC_{\mathcal{V}} + nMC_{\mathcal{A}})$	$p_{\mathcal{V}}\|W_i\|WB_{\mathcal{A}}$

Table 5. SETI-like Scenario

(Game,Model)	Equilibrium $p_{\mathcal{C}}, p_{\mathcal{V}}$	$\mathbf{P}_{wrong}$	U_M	U_{W_i}
(1:1,$\mathcal{R}_{\mathrm{m}}$), (1:1,$\mathcal{R}_{\mathrm{a}}$)	$\frac{MC_{\mathcal{V}}}{MC_{\mathcal{A}}+MP_{\mathcal{W}}}, \frac{WC_{\mathcal{T}}}{WB_{\mathcal{A}}+WP_{\mathcal{C}}}$	$(1-p_{\mathcal{V}})p_{\mathcal{C}}$	$MB_{\mathcal{R}} - p_{\mathcal{C}}(MB_{\mathcal{R}} + MP_{\mathcal{W}}) - MC_{\mathcal{A}}$	$WB_{\mathcal{A}} - WC_{\mathcal{T}}$
(1:1,$\mathcal{R}_{\emptyset}$)	$\frac{MC_{\mathcal{V}}+MC_{\mathcal{A}}}{MC_{\mathcal{A}}+MP_{\mathcal{W}}}, \frac{WC_{\mathcal{T}}}{WB_{\mathcal{A}}+WP_{\mathcal{C}}}$	$(1-p_{\mathcal{V}})p_{\mathcal{C}}$	$MB_{\mathcal{R}} - p_{\mathcal{C}}(MB_{\mathcal{R}} + MP_{\mathcal{W}})$	$-p_{\mathcal{V}} WP_{\mathcal{C}}$
(1:1^n,$\mathcal{R}_{\mathrm{m}}$), (1:1^n,$\mathcal{R}_{\mathrm{a}}$)	$\frac{MC_{\mathcal{V}}}{MC_{\mathcal{A}}+MP_{\mathcal{W}}}, \frac{WC_{\mathcal{T}}}{WB_{\mathcal{A}}+WP_{\mathcal{C}}}$	$(1-p_{\mathcal{V}})\mathbf{P}_{\mathcal{C}}$	$(p_{\mathcal{V}}(1-p_{\mathcal{C}}^n) + (1-p_{\mathcal{V}})(1-\mathbf{P}_{\mathcal{C}}))MB_{\mathcal{R}}$ $-p_{\mathcal{V}} MC_{\mathcal{V}} - (1-p_{\mathcal{V}})\mathbf{P}_{\mathcal{C}} MP_{\mathcal{W}}$ $-(1-p_{\mathcal{V}}p_{\mathcal{C}})nMC_{\mathcal{A}}$	$WB_{\mathcal{A}} - WC_{\mathcal{T}}$
(1:1^n,$\mathcal{R}_{\emptyset}$)	$\frac{MC_{\mathcal{V}}+MC_{\mathcal{A}}}{MC_{\mathcal{A}}+MP_{\mathcal{W}}}, \frac{WC_{\mathcal{T}}}{WB_{\mathcal{A}}+WP_{\mathcal{C}}}$	$(1-p_{\mathcal{V}})\mathbf{P}_{\mathcal{C}}$	$(p_{\mathcal{V}}(1-p_{\mathcal{C}}^n) + (1-p_{\mathcal{V}})(1-\mathbf{P}_{\mathcal{C}}))MB_{\mathcal{R}}$ $-p_{\mathcal{V}} MC_{\mathcal{V}} - (1-p_{\mathcal{V}})\mathbf{P}_{\mathcal{C}} MP_{\mathcal{W}}$ $-p_{\mathcal{V}}(1-p_{\mathcal{C}})nMC_{\mathcal{A}}$	$-p_{\mathcal{V}} WP_{\mathcal{C}}$
(0:n,$\mathcal{R}_{\mathrm{m}}$)	0, $\frac{\lvert W_i\rvert WB_{\mathcal{A}}+WC_{\mathcal{T}}}{\lvert W_i\rvert(WP_{\mathcal{C}}+2WB_{\mathcal{A}})} < p_{\mathcal{V}} \leq 1$	0	$MB_{\mathcal{R}} - p_{\mathcal{V}} MC_{\mathcal{V}} - nMC_{\mathcal{A}}$	$\lvert W_i\rvert WB_{\mathcal{A}} - WC_{\mathcal{T}}$
(0:n,$\mathcal{R}_{\mathrm{a}}$)	0, $\frac{WC_{\mathcal{T}}}{\lvert W_i\rvert(WP_{\mathcal{C}}+WB_{\mathcal{A}})} < p_{\mathcal{V}} \leq 1$	0	$MB_{\mathcal{R}} - p_{\mathcal{V}} MC_{\mathcal{V}} - nMC_{\mathcal{A}}$	$\lvert W_i\rvert WB_{\mathcal{A}} - WC_{\mathcal{T}}$
(0:n,$\mathcal{R}_{\emptyset}$)	0, $\frac{WC_{\mathcal{T}}}{\lvert W_i\rvert(WP_{\mathcal{C}}+WB_{\mathcal{A}})} < p_{\mathcal{V}} \leq 1$	0	$MB_{\mathcal{R}} - p_{\mathcal{V}}(MC_{\mathcal{V}} + nMC_{\mathcal{A}})$	$p_{\mathcal{V}}\lvert W_i\rvert WB_{\mathcal{A}} - WC_{\mathcal{T}}$

Table 6. Contractor Scenario