What Can Cryptography Do For Decentralized Mechanism Design?

Elaine Shi, Hao Chung, and Ke Wu*

Carnegie Mellon University
{runting@cs, haochung@andrew, kew2@andrew}.cmu.edu

Abstract

Recent works of Roughgarden (EC'21) and Chung and Shi (Highlights Beyond EC'22) initiate the study of a new decentralized mechanism design problem called transaction fee mechanism design (TFM). Unlike the classical mechanism design literature, in the decentralized environment, even the auctioneer (i.e., the miner) can be a strategic player, and it can even collude with a subset of the users facilitated by binding side contracts. Chung and Shi showed two main impossibility results that rule out the existence of a *dream* TFM. First, any TFM that provides incentive compatibility for individual users and miner-user coalitions must always have zero miner revenue, no matter whether the block size is finite or infinite. Second, assuming finite block size, no non-trivial TFM can simultaenously provide incentive compatibility for any individual user, and for any miner-user coalition.

In this work, we explore what new models and meaningful relaxations can allow us to circumvent the impossibility results of Chung and Shi. Besides today's model that does not employ cryptography, we introduce a new MPC-assisted model where the TFM is implemented by a joint multi-party computation (MPC) protocol among the miners. We prove several feasibility and infeasibility results for achieving *strict* and *approximate* incentive compatibility, respectively, in the plain model as well as the MPC-assisted model. We show that while cryptography is not a panacea, it indeed allows us to overcome some impossibility results pertaining to the plain model, leading to non-trivial mechanisms with useful guarantees that are otherwise impossible in the plain model. Our work is also the first to characterize the mathematical landscape of transaction fee mechanism design under approximate incentive compatibility, as well as in a cryptography-assisted model.

*Author order is randomized.

Contents

1 Introduction

The widespread adoption of blockchains and cryptocurrencies spurred a new class of *decentralized* mechanism design problems. The recent works of Roughgarden [Rou20, Rou21] as well as Chung and Shi [CS21] considered a particularly important decentralized mechanism design problem, that is, *transaction fee mechanism* (TFM) design. In a transaction fee mechanism (TFM), we are auctioning space in the block to users who want their transactions included and confirmed in the block. If the block can contain up to k transactions, one can equivalently think of selling k identical products to the bidders.

Prior works [LSZ19, Yao, BEOS19, BCD+, Rou20, Rou21, FMPS21] observed that transaction fee mechanism design departs significantly from classical mechanism design [NRTV07]. The vast majority of classical auctions assume that the auctioneer honestly implements the prescribed mechanism. In comparison, in a blockchain environment, the auctioneer (i.e., the miner of the block), can be a strategic player in itself: it can deviate from the prescribed mechanism if it increases its expected gain; or it can collude with a subset of the users, and play strategically to improve the coalition's joint utility. As earlier works pointed out [LSZ19, Yao, BEOS19, BCD+, Rou20, Rou21], the existence of decentralized smart contracts in blockchain environments make it easy for the miner and users to rendezvous and engage in *binding* side contracts. Such side contracts allow the coalition to split their gains off the table in a binding fashion.

Observing the new challenges that arise in a decentralized environment, earlier works [LSZ19, Yao, BEOS19, BCD+, Rou20, Rou21] formulated a set of desiderata for a "dream" TFM:

- *User incentive compatibility (UIC)*: a user's best strategy is to bid truthfully, even when the user has observed others' bids.
- *Miner incentive compatibility (MIC)*: the miner's best strategy is to implement the honest mechanism, even when the miner has observed all users' bids.
- *c-side-contract-proofness (c-SCP)*: playing honestly maximizes the joint utility of a a coalition consisting of the miner and at most c users, even after having observed all others' bids.

A line of works explored how to get a dream TFM. However, assuming that the block size is *finite*, i.e., there can be more bids than the block size, all known works fall short of achieving all three properties at the same time. The closest we have come to in terms of achieving a dream TFM is in fact Etherem's EIP-1559. At a very high-level, when there is congestion, EIP-1559 behaves like a first-price auction which is not UIC. When the block size is infinite (i.e., no congestion), EIP-1559 approximates the following "burning posted price" auction: there is a fixed reserve price r, every bid that is at least r gets included and confirmed, and pays the price of r. All users' payment is burnt and the miner gets nothing[1]. Roughgarden [Rou20, Rou21] proved that when the block size is *infinite*, indeed, the burning posted price auction achieves all three properties at the same time!

Subsequently, Chung and Shi [CS21] further explored the landscape of TFM. They proved two interesting impossibility results:

1. *Zero miner revenue.* Any (possibly randomized) TFM that satisfies both UIC and SCP must always have 0 miner revenue, even when the miner colludes with at most one user, and no matter whether the block size is finite or infinite. This shows that the total burning in EIP-1559 is no accident: it is necessary to achieve all three properties under infinite block size.

[1] In practice, the miner gets a fixed block reward that is irrelevant to our game-theoretic analysis, so we ignore the fixed block reward in our modeling.

2. *Finite-block impossibility.* Suppose that block size is finite, then no non-trivial (possibly randomized) TFM can achieve UIC and SCP at the same time, even when the miner colludes with at most one user. This shows that it is no accident that all prior works fail to achieve the dream TFM for finite block sizes — indeed, there is a mathematical impossibility!

Given the status quo of our understanding, we ask the following natural question:

Are there meaningful new models or relaxations that allow us to circumvent the impossibility results of Chung and Shi?

Chung and Shi [CS21] made an initial exploration along this line. They show a relaxation that allows us to circumvent the impossibilities and achieve positive miner revenue under finite block size. In particular, their relaxation requires the additional assumption that offending bids (e.g., overbid or fake transactions) that have been posted to the public cannot be retracted in the future, and thus the offender may have to pay a cost when the offending transaction is confirmed in the future. While this assumption holds for some cryptocurrencies such as Bitcoin, it may not be universally true for all cryptocurrencies. Therefore, an important question is what other models or relaxations allow us to circumvent the impossibilities.

In this paper, we explore two new directions, aiming to understand whether they allow us to circumvent the impossibilities of Chung and Shi [CS21]: *i)* using an approximate notion of incentive compatibility that allows an ϵ additive slack; and *ii)* having the miners jointly run a multi-party computation (MPC) protocol to realize the TFM. Throughout the paper, we refer to the today's model, which does employ cryptography, as the *plain model*, and we refer to the case where the TFM is realized with MPC as the *MPC-assisted model*.

1.1 Our Results and Contributions

Our paper makes novel contributions at both *conceptual* and *technical* levels. From a technical perspective, prior to our work, we lacked techniques for characterizing the solution space of approximate incentive compatibility — in particular, classical tools like Myerson's Lemma [Mye81] breaks down when we allow ϵ slack in the incentive compatibility, and thus our classical insights often fail. One of our main technical contributions is to develop new techniques for mathematically reasoning about approximate incentive compatibility. On the conceptual front, while an elegant line of work has shown ways in which cryptography and game theory can help each other [HT04, KN08, ADGH06, OPRV09, AL11, ACH11, GKM+13, GKTZ15, GTZ15, Kat08, DR07, GLR10, CGL+18, WAS22, CCWS21, PS17, KMSW22, FW20, EFW22] (see Section 1.2 for more discussions), our work is of a different nature. Our results reveal exciting new connections between cryptography and mechanism design, motivated by a practical problem. The popularity of blockchains and decentralized applications poses many exciting new challenges for decentralized mechanism design, and cryptography-meets-game-theory is a natural and promising paradigm. We thus hope that our new conceptual contributions can provide fodder and inspire new works in this exciting and much explored space.

We give a summary of our main results below.

1.1.1 Characterizing Miner Revenue under Approximate Incentive Compatibility

We first focus on the plain model that was studied in earlier works [LSZ19, Yao, BEOS19, Rou20, Rou21, FMPS21, CS21]. Recall that assuming infinite block size, it is possible to achieve a dream TFM (e.g., the burning posted price auction), but the miner revenue has to be zero. We ask the following question: *suppose we are willing to relax the incentive compatibility notion and allow an*

ϵ additive slack, can we circumvent the zero miner revenue lower bound? If so, exactly how much miner revenue can we hope for?

More specifically, ϵ-incentive-compatibility requires that any deviation cannot increase the strategic individual or coalition's utility by more than ϵ. We show that under ϵ-incentive-compatibility, we can achieve linear (in the number of users) miner revenue assuming infinite block size. Moreover, we give matching upper- and lower-bounds that tightly characterize exactly how much miner revenue can be attained.

Infinite block size. Consider the simple posted price auction with reserve price $r \leq \frac{\epsilon}{c}$ where c is the maximum number of users controlled by the strategic coalition: all bids that bid at least r are confirmed. Each confirmed bid pays r. All payment goes to the miner. It is not hard to show that the above auction satisfies strict UIC, strict MIC (for an arbitrarily sized miner-coalition), and ϵ-SCP against c-sized coalitions. Further, the expected total miner revenue is $\Theta(n \cdot \frac{\epsilon}{c})$ when the users' true values are not too small.

Although the above posted price achieves linear in n revenue. the drawback is that the miner revenue is unscalable: even as the users' bids scale up (e.g., by some multiplicative factor), the miner revenue does not grow proportionally. We therefore ask if randomization can help achieve scalability in miner revenue. We show that indeed the following randomized TFM achieves scalability in miner revenue:

Proportional auction // Let r be a fixed reserve price.

- Every bid $b \geq r$ is confirmed with probability 1 and every candidate bid $b < r$ is confirmed with probability b/r. Each confirmed bid b pays $p = \min\{\frac{b}{2}, \frac{r}{2}\}$.
- For each confirmed bid, miner gets a pre-determined threshold $r' = \sqrt{\frac{2r\epsilon}{9c}}$ if $p \geq r'$.

For example, suppose all users' bids are sampled independently from some distribution $\mathcal{D}$, and let m be the median of the distribution such that $\Pr_{x\sim\mathcal{D}}[x \geq m] \geq 1/2$ (or any other constant). Then, if we set $r = m$, the expected miner revenue (taken over the randomness of users' bids as well as of the TFM itself) is $\Omega(n \cdot \min(m, \sqrt{\frac{m\epsilon}{c}}))$.

Combining the posted price auction and the proportional auction, we have the following theorem:

Theorem 1.1. *Consider the hybrid auction which, given some bid distribution $\mathcal{D}$ with median m, runs either the posted posted price auction with reserve price $r = \min(\frac{\epsilon}{c}, m)$ or the proportional auction with the reserve price $r = m$, depending on which one has higher expected revenue. The hybrid auction is strict UIC, strict MIC (for an arbitrarily sized miner coalition), and ϵ-SCP against any miner-user coalition with at most c users. Further, it achieves $\Omega\left(n \cdot (\min(\frac{\epsilon}{c} + \sqrt{\frac{m\epsilon}{c}}, m))\right)$ expected total miner revenue.*

Next, we prove a matching bound that shows the limitation on how much miner revenue can be attained under approximate incentive compatibility, as stated in the following theorem — this bound holds no matter whether the block size is finite or infinite.

Theorem 1.2 (Limit on miner revenue for infinite block size)**.** *For any possibly randomized TFM (in the plain model) that satisfies ϵ-UIC, ϵ-MIC, and ϵ-SCP for miner-user coalitions with 1 user, the expected total miner revenue over a random bid vector sampled from $\mathcal{D}^n$ must be upper bounded by*

$$[\mu(\mathbf{b})] \leq 6n \cdot (\epsilon + \sqrt{\epsilon} \cdot \mathbf{E}_{x\sim\mathcal{D}}[\sqrt{x}]),$$

where $\mu(\mathbf{b})$ denotes the total miner revenue under the bid vector $\mathbf{b}$, n is the number of users, $\mathcal{D}_i$ denotes the true value distribution of user $i \in [n]$.

Finite block size. Another natural question is: *can we circumvent the finite-block impossibility under approximate incentive compatibility?* Unfortunately, although it is indeed possible to overcome the finite-block impossibility with approximate incentive compatibility, we prove a new impossibility result that rules out the existence of "useful" mechanisms whose social welfare (i.e., the sum of everyone's utilities) scales up proportionally w.r.t. the bid distribution:

Theorem 1.3 (Scalability barrier for approximate incentive compatibility in the plain model)**.** *Fix any $\epsilon > 0$, and suppose that the block size is k. Any (possibly random) TFM in the plain model that simultaneously satisfies ϵ-UIC, ϵ-MIC, and ϵ-SCP (even when the miner colludes with at most one user) has at most $\widetilde{O}(k^3\epsilon)$ social welfare where k is the block size and $\widetilde{O}(\cdot)$ hides logarithmic factors.*

1.1.2 Can We Circumvent the Finite-Block Impossibility with Cryptography?

Due to the negative result of Theorem 1.3, we want to seek other avenues that allow us to circumvent the finite-block impossibility. Since cryptography is widely deployed in today's blockchains, it is natural to ask whether we can bring cryptography to the design of transaction fee mechanisms, to help us achieve what is otherwise impossible.

New model: MPC-assisted TFM. Consider a scenario henceforth called the MPC-assisted model, where a set of miners jointly run a multi-party computation (MPC) protocol to implement the TFM. Although in practice, lighter-weight cryptography would be desirable, as an initial theoretical exploration of the feasibility/infeasibility landscape, it makes sense to start with a generic abstraction like MPC. One may think of the MPC protocol as providing the following ideal functionality $\mathcal{F}_{\text{TFM}}$:

- Each player (either user or miner) may act as any number of identities (including 0), and on behalf of each identity, submit a bid to $\mathcal{F}_{\text{TFM}}$.
- The ideal functionality $\mathcal{F}_{\text{TFM}}$ executes the prescribed *allocation rule* of the TFM to decide which transactions to include and confirm in the block; it executes the *payment rule* and *miner revenue rule* of the TFM to decide how much each confirmed bid pays and the total miner revenue. $\mathcal{F}_{\text{TFM}}$ then sends to all players the set of bids that are confirmed, what price each confirmed bid pays, and the total miner revenue.

We require that the total miner revenue does not exceed the total payment, and that the total miner revenue is split among the miners proportional to their mining power. We also assume that the majority of the miners are honest and that the MPC provides guaranteed output (i.e., the strategic miners cannot cause the MPC protocol to abort without producing outcome).

Intuitively, an MPC-assisted TFM restricts the strategy space for players in comparison with the plain model:

R1 A strategic individual or coalition must decide its strategy without having seen honest users' bids (*c.f.* in the plain model, a strategic individual or coalition can decide their strategy after seeing other players' bids).

R2 Once the set of bids are committed to, the allocation rule must be implemented honestly (*c.f.* in the plain model, the winning miner or block proposer can strategically choose which transactions to include in the block).

Exactly because of the MPC-assisted model imposes the above restrictions on the strategy space, we are hopeful that it may allow us to circumvent impossibilities. Before we explain our results, we first discuss how to define incentive compatibility in the MPC-assisted model.

Ex post vs. Bayesian notions of incentive compatibility. In the plain model, because a strategic individual or coalition can decide their bids after seeing others' bids, prior works [Rou21, CS21] considered an *ex post* notion of incentive compatibility. In the new MPC-assisted model, since players must submit their bids to $\mathcal{F}_{\text{TFM}}$ without seeing others' bids, it also makes sense to consider a *Bayesian* notion of equilibrium.

Informally, we say that an MPC-assisted TFM satisfies *Bayesian Nash Equilibrium (BNE)* for a strategic coalition (or individual) $\mathcal{C}$, following the honest strategy allows $\mathcal{C}$ to maximize its expected gain, assuming that the bids of users not in $\mathcal{C}$ are drawn independently from some known distribution. If the coalition $\mathcal{C}$ consists of an individual user, we say that the scheme satisfies *Bayesian UIC*. When $\mathcal{C}$ consists of at most ρ fraction of the miners, we say that the scheme satisfies *Bayesian MIC* against a ρ-sized miner-coalition, Finally, when the coalition $\mathcal{C}$ consists of at most ρ fraction of miners as well as at least 1 and at most c users, we say that the scheme satisfies *Bayesian SCP* against a (ρ, c)-sized coalition.

Jumping ahead, for the MPC-assisted model, all our mechanism designs achieve incentive compatibility even in the *ex post* setting — in other words, the incentive compatibility guarantees hold even if $\mathcal{F}_{\text{TFM}}$ leaks other players' bids to the strategic players before they decide their own strategy. On the other hand, all of our impossibilities hold even for the Bayesian setting. This makes both our upper- and lower-bounds stronger.

MPC-assisted TFM under strict incentive compatibility. Unfortunately, as shown in Appendix C, the MPC-assisted model does not help us circumvent the zero miner revenue lower bound, even for Bayesian notions of equilibrium. Instead, the main question we care about here is *whether the MPC-assisted model allows us to circumvent the finite-block impossibility.* It turns out that the answer is not a simple binary one.

First, we show that absent user-user collusion, we can indeed circumvent the strong finite-block impossibility of Chung and Shi [CS21]. Specifically, we can indeed construct a TFM that simultaneously achieves UIC, MIC, and $(\rho, c = 1)$-SCP for any ρ. In particular, consider the following *finite-block posted price auction* — recall that to specify an MPC-assisted TFM, we only need to specify the allocation rule, the payment and miner revenue rules.

MPC-assisted, finite-block posted price auction

Let r be a fixed reserve price. Any bid that is at least r is considered as a candidate. Randomly choose up to block size k candidates to confirm. Any confirmed bid pays r. All payment is burnt and the miner revenue is 0.

Theorem 1.4 (MPC-assisted, finite-block posted price auction)**.** *The above MPC-assisted, finite-block posted price auction satisfies UIC, MIC, and* $(\rho, 1)$*-SCP in the ex post setting for an arbitrary* $\rho \in [0, 1]$.

Since Theorem 1.4 holds even in the ex post setting, another interpretation is that the enforcement of the allocation rule (i.e., restriction R2, and not R1) is what allows us to circumvent the finite-block impossibility when $c = 1$.

Table 1: Mathematical landscape of TFM. Results in blue background are shown in this paper. ✗ means impossible and ✓ means possible. $\Theta(\cdot)$ means that we show matching upper and lower bounds — here m is a term that depends on the scale of the bid distribution, and we ignore terms related to c for simplicity. Unless otherwise noted, the impossibilities hold even for $c = 1$.

		plain model	MPC-assisted model
Infinite block	strict	0 miner rev [CS21]	0 miner rev
	approximate	$\Theta(n \cdot (\epsilon + \sqrt{m\epsilon}))$ miner rev	$\Theta(n \cdot (\epsilon + \sqrt{m\epsilon}))$ miner rev
Finite block	strict	✗ [CS21]	✓: $c = 1$, ✗: $c \geq 2$
	approximate	scalability ✗ (ignoring log terms)	scalability ✓

The above finite-block posted price auction works for $c = 1$, i.e. no user-user collusion; however, it fails when the coalition may contain $c \geq 2$ users. Imagine that the number of users $n = k+1$, and suppose that there are two users (and any fraction of mining power) in the coalition. Now, suppose one of the colluding users has true value $v \gg r$, and the other has true value $v' = r$. In this case, the user with true value $v' = r$ should simply drop out and not submit a bid. This guarantees that the friend with large true value will be confirmed, and thus the coalition's joint utility increases.

It turns out that this is no accident. We prove that for $c \geq 2$, no MPC-assisted TFM can achieve UIC, MIC, and SCP for (ρ, c)-sized coalitions at the same time for any choice of ρ. Further, the impossibility holds even assuming Bayesian notions of incentive compatibility.

Theorem 1.5 (Finite-block impossibility in the MPC-assisted model for $c \geq 2$)**.** *Let $c \geq 2$ and let $\rho \in [0, 1]$. No (possibly randomized) MPC-assisted TFM with non-trivial utility can simultaneously achieve Bayesian UIC, Bayesian MIC, and Bayesian SCP for (ρ, c)-sized coalitions, assuming finite block size.*

MPC-assisted TFM under approximate incentive compatibility. Recall that in the plain model, even with approximate incentive compatibility, we cannot have scalable TFMs whose social welfare scales w.r.t. the bid distribution (Theorem 1.3). We show that if we consider approximate incentive compatibility in the MPC-assisted model, we can overcome this scalability barrier. Specifically, we construct an MPC-assisted TFM called the "diluted posted price auction" that can achieve up to $\Theta(M \cdot k)$ social welfare when many people's bids are large enough, where M is an upper bound on users' bid.

MPC-assisted, diluted posted price auction

- Let r be a fixed reserve price, let M be the maximum possible value of the bid, and let k be the block size.
- Remove all bids that are less than r, and suppose that there are ℓ bids left — these bids form the candidate pool.
- Let $N = \max\{c \cdot \sqrt{\frac{kM}{2\epsilon}}, k\}$. If $\ell < N$, pad the candidate pool with fake 0 bids such that its size is N.

- Choose k bids at random from the candidate pool. All real bids chosen are confirmed and pay the reserve price r.
- The miner gets $\frac{2\epsilon}{c}$ for each confirmed bid.

In the above mechanism, suppose we set the reserve price $r \leq M/2$, and further, imagine that $n \gg k$ people bid M. In this case, we will achieve $\Theta(M \cdot k)$ social welfare with high probability.

Theorem 1.6 (MPC-assisted, diluted posted price auction)**.** *The above MPC-assisted, diluted posted price auction satisfies strict UIC, strict MIC, and ϵ-SCP for (ρ, c)-sized coalitions in the ex post setting, for any choice of ρ and c. Further, the mechanism is scalable, i.e., it can achieve $\Theta(M \cdot k)$ expected social welfare under some bid configurations.*

Summary of landscape. Summarizing our understanding so far, we present the mathematical landscape of TFM in Table 1. Our results show that cryptography can help us circumvent fundamental impossibilities of the plain model under finite block size. First, for strict incentive compatibility, cryptography allows us to overcome the finite-block impossibility for $c = 1$ (Theorem 1.4). Second, with approximate incentive compatibility, cryptography allows us to overcome the scalability barrier for finite block size in the plain model.

On the other hand, cryptography is also not a panacea. For example, it does not fundamentally help us improve miner revenue in the infinite block size setting.

1.2 Additional Related Work

We review some additional related works besides the most closely related works on transaction mechanism design [LSZ19, Yao, BEOS19, BCD+, Rou20, Rou21, FMPS21, CS21] mentioned earlier.

Earlier, an elegant line of work [HT04, KN08, ADGH06, OPRV09, AL11, ACH11, GKM+13, GKTZ15, GTZ15, Kat08, DR07, GLR10, CGL+18, WAS22, CCWS21, PS17, KMSW22, FW20, EFW22] revealed ways in which cryptography and game theory can help each other. Among them, some works [DR07] showed how to rely on cryptography to remove the trusted mediator assumption in certain game theoretic notions such as correlated equilibrium. Some [HT04, ADGH06, IML05, OPRV09, CGL+18, WAS22] showed that adopting game theoretic notions of fairness rather than the more stringent cryptographic notions of fairness can allow us to circumvent well-known lower bounds. Recently, Ferreira et al. [FW20] and Essaidi et al. [EFW22] showed that using cryptographic commitments can help us circumvent lower bounds pertaining to credible auctions. As Chung and Shi [CS21] explained, credible auction is of a different nature from transaction fee mechanism design. Transaction fee mechanism is a new type of decentralized mechanism design problem, and the new connections between cryptography and mechanism design revealed in our paper differ in nature from the settings in prior works.

2 Model and Definitions

Notation. We use bold letters to denote vectors. For a vector $\mathbf{b} = (b_1, \ldots, b_N)$, we use b_i to represent the i-th entry of vector $\mathbf{b}$. The notation $\mathbf{b}_{-i} = (b_1, b_2, \ldots, b_{i-1}, b_{i+1}, \ldots, b_N)$ represents all except the i-th entry. We often use $(\mathbf{b}_{-i}, b_i)$ and $\mathbf{b}$ interchangeably. Throughout the paper, we use n to denote the number of users, and N to denote the number of bids. N is equal to n if everyone behaves truthfully. However, strategic users may post zero or multiple bids — in this case N may not be equal to n. Given a distribution $\mathcal{D}$, we use the notation $\mathrm{Supp}(D)$ to denote its support. We use $\mathbb{R}^{\geq 0}$ to denote non-negative real numbers.

2.1 Transaction Fee Mechanism in the Plain Model

We first define transaction fee mechanism (TFM) in the plain model. Henceforth, we use $\mathcal{C}$ to denote a coalition of strategic players (or a strategic individual). In particular, $\mathcal{C}$ can be a user, the miner of the present block, or a coalition of the miner and one or more users.

Plain model. In the plain model, a transaction fee mechanism (TFM) describes the following game:

1. Users not in $\mathcal{C}$ submit their bids where each bid is represented by a single real value — let $\mathbf{b}_{-\mathcal{C}}$ denote the resulting bid vector.
2. The coalition $\mathcal{C}$ sees $\mathbf{b}_{-\mathcal{C}}$, and then users in $\mathcal{C}$ submit their bids.
3. The miner of the present block, possibly a member of $\mathcal{C}$, chooses up to k bids to include in the block, where k denotes the maximum block size.
4. Among the at most k bids included in the block, the trusted blockchain decides 1) which of them are confirmed, 2) how much each confirmed bid pays, and 3) how much revenue is paid to the miner.

Therefore, to specify a transaction fee mechanism (TFM) in the plain model, it suffices to specify the following rules which are *possibly randomized* functions:

- *Inclusion rule*: given a bid vector $\mathbf{b}$, the inclusion rule chooses up to k bids to include in the block;
- *Confirmation and payment rules*: Given the at most k bids included in the block, the confirmation rule decides which ones to confirm, and the payment rule decides how much each confirmed user pays.
- *Miner revenue rule*: Given the at most k bids included in the block, the miner revenue rule decides how much the miner earns.

In particular, the inclusion rule is implemented by the miner, and if the miner is strategic, it may not follow the prescribed inclusion rule but instead choose an arbitrary set of bids to include. By contrast, the confirmation, payment, and miner revenue rules are implemented by the blockchain, and honest implementation is guaranteed.

We assume that the (honest) TFM is *symmetric* in the following sense: if we apply any permutation π to an input bid vector $\mathbf{b} = (b_1, \ldots, b_N)$, it does not change the distribution of the *random variable* represented by the *set* $\{(b_i, x_i, p_i)\}_{i \in [N]}$ where x_i and p_i are random variables denoting the probability that bid i is confirmed, and its payment, respectively. An equivalent, more operational view of the above condition is the following. We may assume that the honest mechanism can always be equivalently described in the following manner: given a bid vector $\mathbf{b}$ where each bid may carry some extra information such as identity or timestamp, the honest mechanism always sorts the vector $\mathbf{b}$ by the bid amount first. During this step, if multiple bids have the same amount, then arbitrary tie-breaking rules may be applied, and the tie-breaking can depend on the extra information such as timestamp or identity. At this point, the inclusion rule and the confirmation rules should depend *only* on the amount of the bids and their relative position in the sorted bid vector. Note that our symmetry requirement is natural and quite general — it captures all the mechanisms we know so far [LSZ19, Yao, BEOS19, BCD+, Rou20, Rou21, FMPS21]. In particular, due to possible tie-breaking in the sorting step, our symmetry condition does *not* require two bids of the same amount to receive the same treatment, i.e., the distribution of their outcomes can be different.

$\mathcal{F}_{\text{TFM}}$: **Ideal Functionality**

// The functionality is parametrized with the allocation, payment, and miner revenue rules.

1. Receive a single bid b_i from each identity. Let $\mathbf{b}$ be the resulting bid vector.
2. Run the allocation rule, the payment rule, and the miner revenue rule with the bid vector $\mathbf{b}$. The outputs include a bit vector indicating whether each bid in $\mathbf{b}$ is confirmed or not, a payment vector where all unconfirmed bids must pay 0, and the total miner revenue. Send the outputs to everyone.

Figure 1: Ideal functionality realized by the MPC protocol.

Strategy space. A user's truthful behavior is submit a single bid representing its true value. However, strategic users may choose to submit zero to multiple bids, and the bids need not reflect their true value.

An honest miner does not submit any bids and honestly implements the prescribed inclusion rule. A strategic miner, on the other hand, may not honestly implement the prescribed inclusion rule — it can pick an arbitrary set of up to k bids of its choice to include. A strategic miner can also post fake bids. A coalition $\mathcal{C}$'s strategy space is defined in the most natural manner, i.e., it includes any strategic behavior of its members.

Notably, any strategic player in $\mathcal{C}$ can decide its actions *after* having observed the bids of the remaining users not in $\mathcal{C}$.

2.2 Transaction Fee Mechanism in the MPC-Assisted Model

Imagine that all miners jointly run an multi-party computation (MPC) protocol that implements the TFM. Figure 1 depicts the natural ideal functionality (denoted $\mathcal{F}_{\text{TFM}}$) realized by the MPC protocol. Further, the MPC protocol can achieve full security with guaranteed output as long as the majority of the miners are honest. Therefore, following the modular composition [Can00] paradigm in the standard cryptography literature, we can simply assume that a trusted party $\mathcal{F}_{\text{TFM}}$ exists — this is often to as the $\mathcal{F}_{\text{TFM}}$-hybrid model. We defer how to securely realize $\mathcal{F}_{\text{TFM}}$ to Appendix C.

MPC-assisted model. A transaction fee mechanism (TFM) in the MPC-assisted model describes the following game:

1. Every player (i.e., user or user) can take on *zero to multiple* identities, and every identity submits a bid represented by a single real value to $\mathcal{F}_{\text{TFM}}$ defined in Figure 1.
2. $\mathcal{F}_{\text{TFM}}$ decides which bids to confirm, how much each confirmed bid pays, and the total miner revenue. The total miner revenue is then divided among the miners proportional to their respective mining power.

Therefore, to specify a TFM in the MPC-assisted model, we need to specify the allocation rule, the payment rule, and the miner revenue rule — we assume that these rules are *possibly randomized*, polynomial-time algorithms, and the syntax of the rules are evident from $\mathcal{F}_{\text{TFM}}$ in Figure 1. In comparison with the plain model, here the *inclusion* rule and the *confirmation* rule are combined into a single *allocation* rule, since both inclusion and confirmation decisions are made by $\mathcal{F}_{\text{TFM}}$. Just like in the plain model, we assume that the (honest) TFM is symmetric.

Strategy space. A user's honest behavior is to take on a *single* identity, submit a single bid which reflects its true value. However, as mentioned above, any strategic user can take on zero or multiple identities, submit zero or multiple bids that need not be its true value.

An honest miner does not take on any identities or submit any bids. However, a strategic miner can take on one or more identities and submit fake bids. Unlike the plain model, here, a strategic miner can no longer choose which bids to include in the block — the allocation rule (i.e., the counterpart of the inclusion + confirmation rules of the plain model) is enforced by $\mathcal{F}_{\text{TFM}}$.

One technicality is whether the distribution of users' identities matter, and whether choosing identities strategically should be part of the strategy space. Jumping ahead, all of our mechanisms are proven to be incentive compatible even when the strategic individual or coalition can arbitrarily choose their identities as long as they cannot impersonate honest users' identities. On the other hand, all of our impossibility results hold even when the strategic individual or coalition is forced to choose their identities from some a-priori known distribution. This makes both our feasibility and infeasbility results stronger.

2.3 Defining Incentive Compatibility

Utility. Every user $i \in [n]$ has a true value $v_i \in \mathbb{R}^{\geq 0}$ if its transaction is confirmed. If user i's transaction is confirmed and the user pays p_i, then its utility is defined as $v_i - p_i$. A miner's utility is simply its revenue.

The utility of any strategic coalition $\mathcal{C}$ is the sum of the utilities of all members of $\mathcal{C}$. Considering the joint utility of the coalition is appropriate since we assume that the coalition has a *binding* mechanism (e.g., decentralized smart contracts) to split off their gains off the table.

Ex post incentive compatibility. We first define ex post incentive compatibility for both the plain model and the MPC-assisted model. Roughly speaking, ex post incentive compatibility requires that a strategic player or coalition's best response is always to behave honestly, even after observing the remaining users' bids. Similary, ex post ϵ-incentive compatibility requires that no strategy can increase a strategic player or coalition's expected utility by more than ϵ in comparison with the honest strategy, and this should hold even if the coalition can decide its strategy *after* having observed the remaining users' bids.

Below in our formal definitions, we define the *approximate* case that allows ϵ slack. When $\epsilon = 0$, we get *strict* incentive compatibiity — in this case, we can omit writing the ϵ.

Definition 2.1 (Ex post incentive compatibility)**.** We say that a mechanism satisfies *ex post* ϵ-incentive compatibility for a set of players $\mathcal{C}$ (possibly an individual), iff for any bid vector $\mathbf{b}_{-\mathcal{C}}$ posted by users not in $\mathcal{C}$, for any vector of true values $\mathbf{v}_{\mathcal{C}}$ of users in $\mathcal{C}$, no strategy can increase $\mathcal{C}$'s expected utility by more than ϵ in comparison with honest behavior. Specifically,

- *UIC.* We say that a TFM (in either the plain or MPC-assisted model) satisfies *ex post ϵ-user incentive compatibility (UIC)*, iff for any n, for any $i \in [n]$, for any bid vector $\mathbf{b}_{-i}$ of all users other than i, for any true value v_i of user i, no strategy can increase i's expected utility by more than ϵ in comparison with truthful bidding.

- *MIC.* In the plain model, we focus on the miner of the present block when defining miner incentive compatibility. We say a TFM in the plain model satisfies *ex post ϵ-miner incentive compatibility MIC*, iff for any bid vector $\mathbf{b}$, no strategy can increase the miner's expected utility by more than ϵ in comparison with honest behavior. Recall that that here, the miner's honest behavior is to honestly implement the inclusion rule and not inject any fake bids.

In the MPC-assisted model, we want MIC to hold for any miner wielding at most ρ fraction of the mining power. Therefore, we say that an MPC-assisted TFM satisfies *ex post ϵ-MIC* against ρ-sized coalitions, iff for any miner wielding at most ρ fraction of the mining power, for any bid vector $\mathbf{b}$, no strategy can increase the miner's expected utility by more than ϵ in comparison with honest behavior. In the $\mathcal{F}_{\text{TFM}}$-hybrid world, the miner's honest behavior is simply not to take on any identities and inject any fake bids.

- *SCP.* In the plain model, we want side-contract-proofness to hold for any miner-user coalition that involves the miner of the present block, and up to c users. We say that a TFM in the plain model satisfies ex post ϵ-side-contract-proofness (SCP) for c-sized coalitions, iff for any miner-user coalition consisting of the miner and up to c users, for any bid vector $\mathbf{b}_{-\mathcal{C}}$ posted by users not in $\mathcal{C}$, no strategy can increase $\mathcal{C}$'s expected utility by more than ϵ in comparison with honest behavior.

  In the MPC-assisted model, we want SCP to hold for any miner-user coalition that involves up to ρ fraction of mining power and up to c users. We say that an MPC-assisted TFM satisfies *ex post ϵ-SCP* for (ρ, c)-sized coalitions, iff for any miner-user coalition[2] consisting of at most ρ fraction of the mining power and up to c users, for any bid vector $\mathbf{b}_{-\mathcal{C}}$ posted by users not in $\mathcal{C}$, no strategy can increase the coalition's utility by more than ϵ in comparison with honest behavior.

Bayesian incentive compatibility. For the MPC-assisted model, it also makes sense to consider a Bayesian notion of incentive compatibility. In particular, the MPC-assisted model requires that the strategic player or coalition decide its strategy without having seen the remaining users' bids. We may assume that the strategic player or coalition has some a-prior belief of each honest user's true value distribution. We assume that all honest users' true values are independently and identically distributed (i.i.d.) and sampled from some distribution $\mathcal{D}$. In Bayesian incentive compatibility, we imagine that a strategic individual or coalition cares about maximizing its expected utility where the expectation is taken over not just the random coins of the mechanism, but also the remaining honest users' bids.

Henceforth, given a set $\mathcal{S}$ of players, we use the notation $\mathcal{D}_{\mathcal{S}}$ to denote $\mathcal{D}^u$ where u is the number of users in $\mathcal{S}$. Similarly, $\mathcal{D}_{-i} := \mathcal{D}^{n-1}$. Again, we define ϵ-incentive compatibility for the Bayesian setting below, where the corresponding strict incentive compatibility notions can be obtained by setting $\epsilon = 0$.

Definition 2.2 (Bayesian incentive compatibility)**.** We say that an MPC-assisted TFM satisfies Bayesian ϵ-incentive compatibility for a coalition or individual $\mathcal{C}$, iff for any $\mathbf{v}_{\mathcal{C}}$ denoting the true values of users in $\mathcal{C}$, sample $\mathbf{b}_{-\mathcal{C}} \sim \mathcal{D}_{-\mathcal{C}}$, then, no strategy can increase $\mathcal{C}$'s expected utility by more than ϵ in comparison with honest bevavior, where the expectation is taken over randomness of the honest users bids $\mathbf{b}_{-\mathcal{C}}$, as well as random coins consumed by the TFM. Specifically,

- *UIC.* We say that an MPC-assisted TFM satisfies Bayesian ϵ-UIC, iff for any n, for any user $i \in [n]$, for any true value $v_i \in \mathbb{R}^{\geq 0}$ of user i, for any strategic bid vector $\mathbf{b}_i$ from user i which could be empty or consist of multiple bids,

$$\mathop{\mathbf{E}}_{\mathbf{b}_{-i} \sim \mathcal{D}_{-i}} \left[\mathsf{util}^i(\mathbf{b}_{-i}, v_i) \right] \geq \mathop{\mathbf{E}}_{\mathbf{b}_{-i} \sim \mathcal{D}_{-i}} \left[\mathsf{util}^i(\mathbf{b}_{-i}, \mathbf{b}_i) \right] - \epsilon$$

[2] We require the miner-user coalition to consist of a non-zero fraction mining power and at least one user — otherwise the definition would degenerate to UIC or MIC.

where $\mathsf{util}^i(\mathbf{b})$ denotes the expected utility (taken over the random coins of the TFM) of user i when the bid vector is $\mathbf{b}$.

- *MIC.* We say that an MPC-assisted TFM satisfies Bayesian ϵ-MIC for ρ-sized coalitions, iff for any miner coalition $\mathcal{C}$ controlling at most ρ fraction of the mining power, for any strategic bid vector $\mathbf{b}'$ injected by the miner,

$$\mathop{\mathbf{E}}_{\mathbf{b}_{-\mathcal{C}} \sim \mathcal{D}_{-\mathcal{C}}} \left[\mathsf{util}^{\mathcal{C}}(\mathbf{b}_{-\mathcal{C}})\right] \geq \mathop{\mathbf{E}}_{\mathbf{b}_{-\mathcal{C}} \sim \mathcal{D}_{-\mathcal{C}}} \left[\mathsf{util}^{\mathcal{C}}(\mathbf{b}_{-\mathcal{C}}, \mathbf{b}')\right] - \epsilon$$

  where $\mathsf{util}^{\mathcal{C}}(\mathbf{b})$ denotes the expected utility (taken over the random coins of the TFM) of the coalition $\mathcal{C}$ when the input bid vector is $\mathbf{b}$.

- *SCP.* We say that an MPC-assisted TFM satisfies Bayesian ϵ-SCP for (ρ, c)-sized coalitions, iff for any miner-user coalition consisting of at most ρ fraction of mining power and at most c users, for any true value vector $\mathbf{v}_{\mathcal{C}}$ of users in $\mathcal{C}$, for any strategic bid vector $\mathbf{b}_{\mathcal{C}}$ of the coalition (whose length may not be equal to the number of users in $\mathcal{C}$),

$$\mathop{\mathbf{E}}_{\mathbf{b}_{-\mathcal{C}} \sim \mathcal{D}_{-\mathcal{C}}} \left[\mathsf{util}^{\mathcal{C}}(\mathbf{b}_{-\mathcal{C}}, \mathbf{v}_{\mathcal{C}})\right] \geq \mathop{\mathbf{E}}_{\mathbf{b}_{-\mathcal{C}} \sim \mathcal{D}^{-\mathcal{C}}} \left[\mathsf{util}^{\mathcal{C}}(\mathbf{b}_{-\mathcal{C}}, \mathbf{b}_{\mathcal{C}})\right] - \epsilon$$

Note that the Bayesian notions of incentive compatibility do not make sense in the plain model, since in the plain model, the strategic individual or coalition can decide its move *after* having observed the remaining honest users' bids. This is why we adopt only the ex post notion in the plain model. Formally, it is easy to show that any mechanism that satisfies Bayesian incentive compatibility in the plain model also satisfies ex post incentive compatibility.

In the MPC-assisted model, both notions make sense, and the ex post notions are strictly stronger than the Bayesian counterparts. Jumping ahead, all of our impossibility results for the MPC-assisted model work even for the Bayesian notions, and all of our mechanism designs in the MPC-assisted model work even for the ex post notions. This makes both our lower- and upper-bounds stronger.

3 Approximate Incentive Compatibility for Infinite Block Size

In the plain model, no UIC and SCP mechanism (even for $c = 1$ and infinite block size) can achieve positive miner revenue [CS21]. In Appendix B.1, we show that the same zero miner revenue lower bound holds even in the MPC-assisted model. Therefore, we consider how to get meaningful miner revenue using the relaxed notion of approximate incentive compatibility. In this section, we give a tight characterization of approximate incentive compatibility for infinite block size. This tight characterization applies to both the MPC-assisted model and the plain model.

3.1 Bounds on Miner Revenue

We first prove a limit on miner revenue in the MPC-assisted model, which holds even for in the Bayesian setting. The same limit applies to the plain model for the ex post setting — to see this, observe that the strategy space is strictly larger in the plain model, and moreover, for the plain model, we only care about $\rho = 1$.

We now show an MPC-assisted mechanism simultaneously satisfies ϵ-UIC, ϵ-MIC and ϵ-SCP even for the Bayesian setting and even for $c = 1$ and an arbitray choice $\rho \in (0, 1]$, then the miner

can gain at most $O(n \cdot (\epsilon + \cdot\sqrt{m^* \cdot \epsilon}))$-miner revenue, where n is the number of users, and m^* is a term that depends on the "scale" of the bid distribution.

To prove the limit on the miner revenue, we care only about the probability of each bid being confirmed, the expected payment of each bid, and the miner revenue. Therefore, we introduce the following notations to denote the outputs of the allocation, payment, and miner revenue rules — we assume that each user's true value is drawn i.i.d. from some distribution $\mathcal{D}$ since we are considering the Bayesian setting:

- **Allocation rule**: given a bid vector $\mathbf{b} = (b_1, \ldots, b_N)$, the allocation rule outputs a vector $\mathbf{x}(\mathbf{b}) := (x_1, \ldots, x_N) \in [0,1]^N$, where each x_i denotes the probability of b_i being confirmed.
- **Payment rule**: given a bid vector $\mathbf{b} = (b_1, \ldots, b_N)$, the payment rule outputs a vector $\mathbf{p}(\mathbf{b}) := (p_1, \ldots, p_N) \in \mathbb{R}^N$, where each p_i denotes the expected payment of b_i.
- **Miner revenue rule**: given a bid vector $\mathbf{b} = (b_1, \ldots, b_N)$, the miner revenue rule outputs $\mu(\mathbf{b}) \in \mathbb{R}$, denoting the amount paid to the miner.

We also define $\mathcal{D}_{-i} := \mathcal{D}^{N-1}$, and for the i-th user, we define

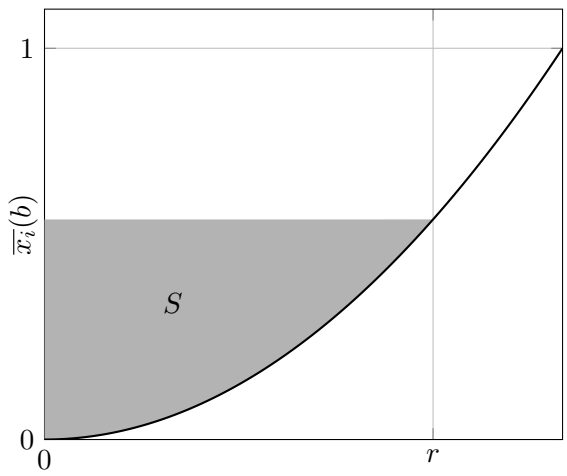
$$\overline{x_i}(\cdot) = \mathop{\mathbf{E}}_{\mathbf{b}_{-i} \sim \mathcal{D}_{-i}}[\mathbf{x}_i(\mathbf{b}_{-i}, \cdot)], \quad \overline{p_i}(\cdot) = \mathop{\mathbf{E}}_{\mathbf{b}_{-i} \sim \mathcal{D}_{-i}}[\mathbf{p}_i(\mathbf{b}_{-i}, \cdot)], \quad \overline{\mu_i}(\cdot) = \mathop{\mathbf{E}}_{\mathbf{b}_{-i} \sim \mathcal{D}_{-i}}[\mu(\mathbf{b}_{-i}, \cdot)].$$

Henceforth, we often use $(\mathbf{x}, \mathbf{p}, \mu)$ to denote a TFM in the MPC-assisted model. The crux of our proof is to characterize how miner revenue changes when we lower one user's bid to 0 (Lemma 3.3). We then apply this argument n times, and lower each user's bid one by one to 0 to get the desired bound. To make the second step work, we need to use approximate MIC to remove a user's bid from consideration once we have lowered it to zero — this ensures that in any step of our inductive argument, the non-strategic users' bids are always i.i.d. sampled from $\mathcal{D}$.

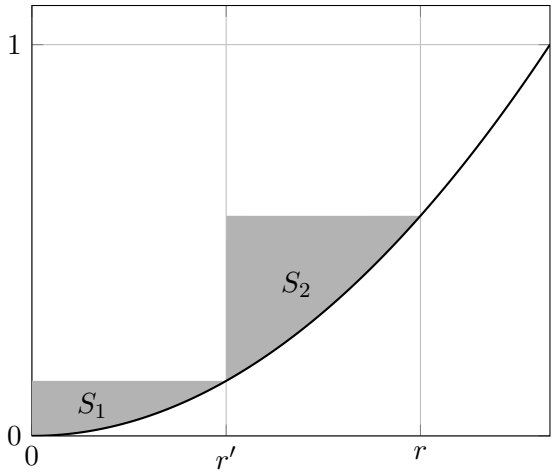
Warmup. To understand how much the miner revenue changes when one user lowers its bid to 0, we start from a simplified case where a TFM $(\mathbf{x}, \mathbf{p}, \mu)$ is Bayesian *strict*-UIC and Bayesian ϵ-SCP for $c = 1$ and some $\rho \in (0, 1]$. By Myerson's Lemma [Mye81], strict-UIC implies that, for any user i, the allocation rule $x_i(\cdot)$ must be non-decreasing. Moreover, the expected payment when bidding b is specified as

$$\overline{p_i}(b) = b \cdot \overline{x_i}(b) - \int_0^b \overline{x_i}(t)dt.$$

We care about how much the miner revenue can increase when user i bids r instead of 0. One trivial upper bound can be obtained as follows. Imagine that user i's true value is 0, but it bids r instead. In this case, the user's loss in utility (in comparison with truthful bidding) is represented by the area of the gray triangle S in Figure 2a. Due to ϵ-SCP, the miner revenue increase when user i bids r instead of 0 must be upper bounded by $S + \epsilon$. This bound, however, is not tight. To make it tighter, we consider bounding it in two steps by introducing a mid-point $r' \in (0, r)$. If user i's true value is 0, but it bids r' instead, its utility loss is the area S_1 of Figure 2b. By ϵ-SCP, we conclude that $\overline{\mu_i}(r') - \overline{\mu_i}(0) \geq S_1 + \epsilon$. Now, imagine user i's true value is r' but it bids r instead. Using a similar argument, we conclude that $\overline{\mu_i}(r) - \overline{\mu_i}(r') \geq S_2 + \epsilon$ (see Figure 2b). Summarizing the above, we have that $\overline{\mu_i}(r) - \overline{\mu_i}(0) \geq S_1 + S_2 + 2\epsilon$.



(a) When user i changes its bid from 0 to r, it loses utility S. Therefore, miner revenue changes by no more than $S + \epsilon$.



(b) When user i changes its bid from 0 to r', it loses utility S_1. Then when it changes its bid from r' to r, it loses utility S_2.

Figure 2: User's utility change

To get a tight bound, the key is how to choose the optimal number of steps L we use in the above argument. Taking more steps makes the total area of the gray triangles smaller; however, every step incurs an extra ϵ. Given the number of steps L, the sum of the L triangles is upper bounded by r/L, and since each step incurs an additive ϵ term, our goal is to minimize the expression $r/L + \epsilon L$. Picking $L = \sqrt{\frac{r}{\epsilon}}$ minimizes the expression and thus we have that $\overline{\mu_i}(r) - \overline{\mu_i}(0) \leq 2\sqrt{r\epsilon}$.

Full proof. The above warmup argument works for strict-UIC and ϵ-SCP. We want to prove a limitation on miner revenue for Bayesian ϵ-UIC and ϵ-SCP. The challenge is that for ϵ-UIC, Myerson's lemma no longer holds — in particular, the allocation rule may not even be monotone any more. The key idea our proof is to give a generalization of Myerson's lemma to account for the ϵ slack in incentive compatibility. We first prove a generalization of Myerson's *payment difference sandwich* for ϵ-UIC.

Lemma 3.1. *Given any (possibly randomized) MPC-assisted TFM that is Bayesian ϵ-UIC, it must be that for any user i, for any $y \leq z$,*

$$z \cdot [\overline{x_i}(z) - \overline{x_i}(y)] + \epsilon \geq \overline{p_i}(z) - \overline{p_i}(y) \geq y \cdot [\overline{x_i}(z) - \overline{x_i}(y)] - \epsilon. \tag{1}$$

Proof. The proof is similar to the proof of Myerson's Lemma. Note that user i's expected utility is $v \cdot \overline{x_i}(b) - \overline{p_i}(b)$ if its true value is v and its bid is b. By the definition of Bayesian ϵ-UIC, it must be that

$$z \cdot \overline{x_i}(z) - \overline{p_i}(z) + \epsilon \geq z \cdot \overline{x_i}(y) - \overline{p_i}(y).$$

Otherwise if user i's true value is z, bidding y can bring it strictly more than ϵ utility compared to bidding truthfully, which contradicts Bayesian ϵ-UIC. By the same reasoning, we have

$$y \cdot \overline{x_i}(y) - \overline{p_i}(y) + \epsilon \geq y \cdot \overline{x_i}(z) - \overline{p_i}(z).$$

The lemma thus follows by combining these two inequalities.

□

Based on this payment difference sandwich, we have the following result about the expected miner's revenue for approximate incentive compatibility.

Lemma 3.2. *Fix any $\rho \in (0, 1]$. For any (possibly randomized) MPC-assisted TFM that is Bayesian ϵ_u-UIC and Bayesian ϵ_s-SCP against a $(\rho, 1)$-sized coalition, it must be that for any user i, for any $y \le z$,*

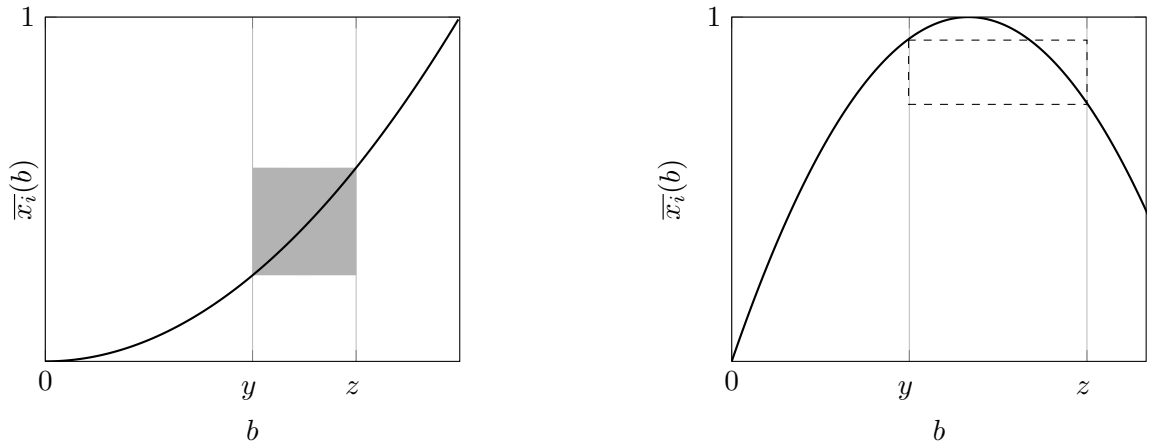
$$\overline{\mu_i}(z) - \overline{\mu_i}(y) \le \frac{1}{\rho}(\epsilon_u + \epsilon_s + S(y, z)), \tag{2}$$

where $S(y, z) = (z - y)[\overline{x_i}(z) - \overline{x_i}(y)]$.

Proof. The utility of user i is $v \cdot \overline{x_i}(b) - \overline{p_i}(b)$ if its true value is v and it bids b. Imagine that the user i's true value is y. If user i overbids $z > y$ instead of its true value y, then its expected utility decreases by

$$\begin{aligned}
\Delta &= y \cdot \overline{x_i}(y) - \overline{p_i}(y) - [y \cdot \overline{x_i}(z) - \overline{p_i}(z)] \\
&= -y \cdot [\overline{x_i}(z) - \overline{x_i}(y)] + (\overline{p_i}(z) - \overline{p_i}(y)) \\
&\le -y \cdot [\overline{x_i}(z) - \overline{x_i}(y)] + z \cdot [\overline{x_i}(z) - \overline{x_i}(y)] + \epsilon_u \qquad \text{By Bayesian } \epsilon_u\text{-UIC and (1)} \\
&= (z - y) \cdot [\overline{x_i}(z) - \overline{x_i}(y)] + \epsilon_u = S(y, z) + \epsilon_u.
\end{aligned}$$

A graphical description of $S(y, z)$ is shown in Figure 3 — note that $S(y, z)$ can be *negative* since the allocation rule $\overline{x_i}(\cdot)$ may not be monotone under approximate UIC.



(a) An illustrative example of $S(y, z)$ in increasing function. The size of the gray area in the figure is exactly $S(y, z)$.

(b) When the function decreases, $S(y, z)$ can be negative. $S(y, z)$ is the negative of the dashed rectangle area.

Figure 3: User's utility change

By Bayesian ϵ_s-SCP, it must be that $\rho\overline{\mu_i}(z) - \rho\overline{\mu_i}(y) \le \Delta + \epsilon_s$; otherwise, a miner with ρ fraction of mining power can collude with user i, and ask user i to bid z instead of its true value y. This increases the coalition's utility by strictly more than ϵ_s compared to the honest strategy, which contradicts Bayesian ϵ_s-SCP. □

Lemma 3.3. *Fix any $\rho \in (0, 1]$. Let $(\mathbf{x}, \mathbf{p}, \mu)$ be any (possibly randomized) MPC-assisted TFM that is Bayesian ϵ_u-UIC and Bayesian ϵ_s-SCP against a $(\rho, 1)$-sized coalition. Then, for any user*

i, for any value r, it must be that

$$\overline{\mu_i}(r) - \overline{\mu_i}(0) \leq \begin{cases} \frac{2}{\rho}(\epsilon_s + \epsilon_u), & \text{if } r \leq \epsilon_s + \epsilon_u \\ \frac{2}{\rho}(\sqrt{r(\epsilon_s + \epsilon_u)}), & \text{if } r > \epsilon_s + \epsilon_u. \end{cases} \tag{3}$$

Proof. Let $\epsilon' = \epsilon_s + \epsilon_u$. To prove this Lemma, we consider the following two cases.

Case 1: If $r \leq \epsilon'$. In this case, by Lemma 3.2, we have that

$$\overline{\mu_i}(r) - \overline{\mu_i}(0) \leq \frac{1}{\rho}\left(\epsilon_u + \epsilon_s + S(0, r)\right) \leq \frac{1}{\rho}\left(\epsilon_u + \epsilon_s + r\right) \leq \frac{2\epsilon'}{\rho}.$$

Case 2: If $r > \epsilon'$. We choose a sequence of points that partitions the interval $[0, r]$ as follows. Let $L = \lfloor \sqrt{\frac{r}{\epsilon'}} \rfloor$. Set $r_0 = 0$ and $r_{L+1} = r$. For $l = 1, \ldots, L$, we set $r_l = l \cdot \sqrt{r\epsilon'}$. Each segment except the last one is of length $\sqrt{r\epsilon'}$, while the last one has length no more than $\sqrt{r\epsilon'}$.

Now we proceed to bound $\overline{\mu_i}(r) - \overline{\mu_i}(0)$. Note that

$$\begin{aligned}
\overline{\mu_i}(r) - \overline{\mu_i}(0) &= \sum_{l=0}^{L} [\overline{\mu_i}(r_{l+1}) - \overline{\mu_i}(r_l)] \\
&\leq \sum_{l=0}^{L} \frac{1}{\rho}[\epsilon' + S(r_l, r_{l+1})] && \text{By Lemma 3.2} \\
&= \frac{L\epsilon'}{\rho} + \frac{1}{\rho}\sum_{l=0}^{L} (r_{l+1} - r_l) \cdot [\overline{x_i}(r_{l+1}) - \overline{x_i}(r_l)] \\
&\leq \frac{L\epsilon'}{\rho} + \frac{1}{\rho}\sqrt{r\epsilon'}\sum_{l=0}^{L} [\overline{x_i}(r_{l+1}) - \overline{x_i}(r_l)] && \text{By the choice of } r_l \\
&\leq \frac{L\epsilon'}{\rho} + \frac{1}{\rho}\sqrt{r\epsilon'} && \text{By } \overline{x_i}(r) \leq 1
\end{aligned}$$

Since $L = \lfloor \sqrt{\frac{r}{\epsilon'}} \rfloor \leq \sqrt{\frac{r}{\epsilon'}}$, we have that

$$\overline{\mu_i}(r) - \overline{\mu_i}(0) \leq \frac{2\sqrt{r\epsilon'}}{\rho}.$$

□

Now, we want to bound the miner revenue by lowering each user's bid to 0 one by one, and apply Lemma 3.3 in each step. To make this argument work, one key insight is to rely on approximate MIC to remove a user's bid from consideration after lowering it to zero — see Equation (5) in the proof of Theorem 3.4 below. This ensures that in any step of the induction, any honest user's bid is sampled from $\mathcal{D}$.

Theorem 3.4 (Limit on miner revenue for approximate incentive compatibility)**.** *Suppose that there are n users, whose true values are drawn i.i.d. from some distribution $\mathcal{D}$. Given any (possibly randomized) MPC-assisted TFM that is Bayesian ϵ_u-UIC, Bayesian ϵ_m-MIC against a ρ-sized miner coalition and Bayesian ϵ_s-SCP against a $(\rho, 1)$-sized coalition, it must be that*

$$\mathop{\mathbf{E}}_{\mathbf{b} \sim \mathcal{D}^n}[\mu(\mathbf{b})] \leq \frac{2n}{\rho}\left(\epsilon + C_{\mathcal{D}}\sqrt{\epsilon}\right), \tag{4}$$

where $\epsilon = \epsilon_s + \epsilon_u + \epsilon_m$, *and* $\mathcal{C}_{\mathcal{D}} = \mathbf{E}_{X\sim\mathcal{D}}[\sqrt{X}]$ *is a term that depends on the "scale" of the distribution* $\mathcal{D}$.

Proof. Since the TFM is Bayesian ϵ_m-MIC, it must be that for any ℓ,

$$\mathop{\mathbf{E}}_{\mathbf{b}\sim\mathcal{D}^\ell}[\rho\mu(\mathbf{b},0)] \le \mathop{\mathbf{E}}_{\mathbf{b}\sim\mathcal{D}^\ell}[\rho\mu(\mathbf{b})] + \epsilon_m. \tag{5}$$

Otherwise, the strategic miner can inject a bid 0 and increase its miner revenue by strictly more than ϵ_m, while it does not need pay anything for injecting this 0-bid. This violates Bayesian ϵ_m-MIC.

Let $f(\cdot)$ be the p.d.f. of distribution $\mathcal{D}$. By the law of total expectation,

$$\mathop{\mathbf{E}}_{\mathbf{b}\sim\mathcal{D}^n}[\mu(\mathbf{b})] = \int_0^\infty \mathop{\mathbf{E}}_{\mathbf{b}'\sim\mathcal{D}^{n-1}}[\mu(\mathbf{b}',r)]f(r)dr.$$

Let $\epsilon' = \epsilon_s + \epsilon_u$. Since the mechanism is Bayesian ϵ_u-UIC and Bayesian ϵ_s-SCP against $(\rho,1)$-sized coalition, by Lemma 3.3, it must be that

$$\int_0^{\epsilon'} \mathop{\mathbf{E}}_{\mathbf{b}'\sim\mathcal{D}^{n-1}}[\mu(\mathbf{b}',r)]f(r)dr \le \int_0^{\epsilon'} \left[\mathop{\mathbf{E}}_{\mathbf{b}'\sim\mathcal{D}^{n-1}}[\mu(\mathbf{b}',0)] + \frac{2\epsilon'}{\rho}\right] f(r)dr;$$
$$\int_{\epsilon'}^\infty \mathop{\mathbf{E}}_{\mathbf{b}'\sim\mathcal{D}^{n-1}}[\mu(\mathbf{b}',r)]f(r)dr \le \int_{\epsilon'}^\infty \left[\mathop{\mathbf{E}}_{\mathbf{b}'\sim\mathcal{D}^{n-1}}[\mu(\mathbf{b}',0)] + \frac{2\sqrt{r\epsilon'}}{\rho}\right] f(r)dr.$$

Summing up the two inequalities above, we can bound the expected miner revenue with

$$\begin{aligned}
&\mathop{\mathbf{E}}_{\mathbf{b}\sim\mathcal{D}^n}[\mu(\mathbf{b})] \\
&= \int_0^{\epsilon'} \mathop{\mathbf{E}}_{\mathbf{b}'\sim\mathcal{D}^{n-1}}[\mu(\mathbf{b}',r)]f(r)dr + \int_{\epsilon'}^\infty \mathop{\mathbf{E}}_{\mathbf{b}'\sim\mathcal{D}^{n-1}}[\mu(\mathbf{b}',r)]f(r)dr \\
&\le \int_0^{\epsilon'} \left[\mathop{\mathbf{E}}_{\mathbf{b}'\sim\mathcal{D}^{n-1}}[\mu(\mathbf{b}',0)] + \frac{2\epsilon'}{\rho}\right] f(r)dr + \int_{\epsilon'}^\infty \left[\mathop{\mathbf{E}}_{\mathbf{b}'\sim\mathcal{D}^{n-1}}[\mu(\mathbf{b}',0)] + \frac{2\sqrt{r\epsilon'}}{\rho}\right] f(r)dr \\
&\le \mathop{\mathbf{E}}_{\mathbf{b}'\sim\mathcal{D}^{n-1}}[\mu(\mathbf{b}',0)] + \frac{2\epsilon'}{\rho}\int_0^{\epsilon'} f(r)dr + \frac{2\sqrt{\epsilon'}}{\rho}\int_{\epsilon'}^\infty \sqrt{r}f(r)dr
\end{aligned}$$

By (5), we have that $\mathop{\mathbf{E}}_{\mathbf{b}'\sim\mathcal{D}^{n-1}}[\mu(\mathbf{b}',0)] \le \mathop{\mathbf{E}}_{\mathbf{b}'\sim\mathcal{D}^{n-1}}[\mu(\mathbf{b}')] + \frac{\epsilon_m}{\rho}$. Therefore,

$$\begin{aligned}
&\mathop{\mathbf{E}}_{\mathbf{b}\sim\mathcal{D}^n}[\mu(\mathbf{b})] \\
&\le \mathop{\mathbf{E}}_{\mathbf{b}'\sim\mathcal{D}^{n-1}}[\mu(\mathbf{b}',0)] + \frac{2\epsilon'}{\rho}\int_0^{\epsilon'} f(r)dr + \frac{2\sqrt{\epsilon'}}{\rho}\int_{\epsilon'}^\infty \sqrt{r}f(r)dr \\
&\le \mathop{\mathbf{E}}_{\mathbf{b}'\sim\mathcal{D}^{n-1}}[\mu(\mathbf{b}')] + \frac{\epsilon_m}{\rho} + \frac{2\epsilon'}{\rho} + \frac{2\sqrt{\epsilon'}}{\rho}\mathbf{E}_{X\sim\mathcal{D}}[\sqrt{X}] \\
&\le \mathop{\mathbf{E}}_{\mathbf{b}'\sim\mathcal{D}^{n-1}}[\mu(\mathbf{b}')] + \frac{2\epsilon}{\rho} + \frac{2C_{\mathcal{D}}\sqrt{\epsilon}}{\rho},
\end{aligned}$$

where the last step comes from the fact that $\epsilon = \epsilon_s + \epsilon_u + \epsilon_m$. The theorem follows by induction on n, where in each induction step we repeat the argument above. □

It is easy to see that the same miner revenue limit of Theorem 3.4 also holds in the plain model, as stated in the following corollary.

Corollary 3.5. *Suppose that there are n users, whose true values are drawn i.i.d. from some distribution $\mathcal{D}$. Given any (possibly randomized) TFM in the plain model that is ϵ_u-UIC, ϵ_m-MIC, and ϵ_s-SCP even for $c = 1$, it must be that*

$$\mathop{\mathbf{E}}_{\mathbf{b}\sim\mathcal{D}^n}[\mu(\mathbf{b})] \le 2n\left(\epsilon + C_{\mathcal{D}}\sqrt{\epsilon}\right), \tag{6}$$

where $\epsilon = \epsilon_s+\epsilon_u+\epsilon_m$, and $C_{\mathcal{D}} = \mathbf{E}_{X\sim\mathcal{D}}[\sqrt{X}]$ is a term that depends on the "scale" of the distribution $\mathcal{D}$.

Proof. Follows directly from Theorem 3.4 which holds in particular for $\rho = 1$, and the fact that the strategy space in the plain model is strictly larger than in the MPC-assisted model. □

3.2 Achieving Optimal Revenue: Proportional Auction

We now show that the limit on miner revenue in Theorem 3.4 is asymptotically tight, i.e., we can indeed design a TFM, even in the plain model, whose miner revenue asymptotically matches Equation (4) for some natural bid distribution.

Proportional Auction (plain model)

Parameters: the slack ϵ, the reserved price r where $r \ge 2\epsilon$.

Input: a bid vector $\mathbf{b} = (b_1, \ldots, b_N)$.

Mechanism:

- *Inclusion rule.* Include all bids in $\mathbf{b}$.
- *Confirmation rule.* For each bid b, if $b < r$, it is confirmed with the probability b/r; otherwise, if $b \ge r$, it is confirmed with probability 1.
- *Payment rule.* For each confirmed bid b, if $b < r$, it pays $b/2$; otherwise, it pays $r/2$.
- *Miner revenue rule.* For each confirmed bid b, if $b \ge \sqrt{2r\epsilon}$[a], then miner is paid $\frac{\sqrt{2r\epsilon}}{2}$.

[a] This guarantees that the miner revenue does not exceed the total payment.

The above mechanism is called the proportional mechanism since the user's confirmation probability is proportional to the bid in the region $[0, r]$, and any bid that is at least r is confirmed with probability 1.

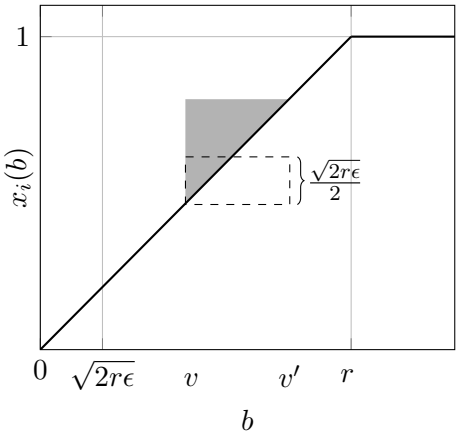
Theorem 3.6. *The above proportional auction in the plain model is UIC, MIC and $\frac{5}{4}c\epsilon$-SCP against c-sized coalitions for arbitrary $c \ge 1$.*

Proof intuition. We provide the proof intuition and defer the full proof to Appendix A. First, UIC and MIC are easy to prove. Observe that the allocation rule (i.e., the union of the inclusion and confirmation rules) is monotone, and by design, the payment rule is the unique one that satisfies Myerson's Lemma. Therefore, the mechanism satisfies UIC. It is easy to see that injecting a bid does not help the miner, since each bid's contribution to the miner revenue is independent and limited by the payment amount.

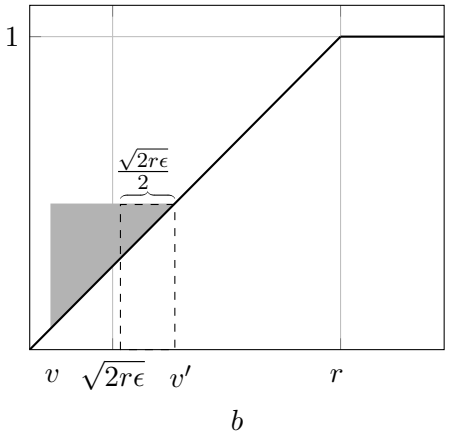
Proving that the mechanism satisfies $\frac{5}{4}c\epsilon$-SCP is more technical. Here we give an illustrative explanation to show that the joint utility of each user and the miner can increase by at most $\frac{5}{4}\epsilon$. Since underbidding does not increase the user's utility or the miner's revenue, we focus on overbidding. Note that overbidding does not increase the joint utility for a user whose true value is $v \ge r$. Therefore, we focus in the case where the colluding user has true value $v < r$ and overbids.

If $v \geq \sqrt{2r\epsilon}$, the user's utility loss when overbidding to v' is represented by the gray triangle in Figure 4a. Meanwhile, the miner's expected revenue increases by $\frac{\sqrt{2r\epsilon}}{2}(\frac{v'}{r} - \frac{v}{r})$, which is the area of the dashed rectangle in Figure 4a. Therefore, when the user overbids by $v' - v = \frac{\sqrt{2r\epsilon}}{2}$, the coalition's utility increase is maximized and equals to $\frac{\epsilon}{4}$.

If $v < \sqrt{2r\epsilon}$ and the colluding user overbids to $v' \geq \sqrt{2r\epsilon}$, then the user's utility loss when overbidding to v' is represented by the area of the gray triangle in Figure 4b. The miner's revenue now increases by $\frac{v'}{r} \cdot \frac{\sqrt{2r\epsilon}}{2}$, because the user's utility would be 0 if the user behaves honestly. The increase in the miner's revenue is represented by the dashed rectangle in Figure 4b. The increase in the joint utility of the coalition is maximized when v is arbitrarily close to $\sqrt{2r\epsilon}$ and the user overbids by $v' - v = \frac{\sqrt{2r\epsilon}}{2}$. In this case, the joint utility of the coalition increases by $\frac{5}{4}\epsilon$.



(a) An illustrative example of the coalition's joint utility change when the user's true value $v \geq \sqrt{2r\epsilon}$.



(b) An illustrative example of the coalition's joint utility change when the user's true value $v < \sqrt{2r\epsilon}$.

Figure 4: Coalition's joint utility change when the miner colluding with one user

4 Characterization of Finite Block Size in the Plain Model

In real-world blockchains, we do not have an infinite block size. Chung and Shi [CS21] showed that no non-trivial plain-model TFM can achieve strict UIC and strict SCP (even when $c = 1$) for finite block size. In this section, we show that although approximate incentive compatibility can help us overcome this impossibility, nonetheless we cannot get useful mechanisms whose social welfare scales with the bid distribution (ignoring logarithmic terms).

Theorem 4.1. *Suppose the block size is upper bounded by k. Fix any $\epsilon > 0$. Given any TFM in the plain model that satisfies ϵ-UIC, ϵ-MIC and ϵ-SCP when the miner can collude with at most $c = 1$ user, and given any bid vector $\mathbf{b}$, let $M = \max(\mathbf{b})$ be the maximum bid of any user, it must be that*

- *the miner's expected revenue is upper bounded by $12k^2\epsilon \log\left(\frac{M}{\epsilon} + 1\right) + 2k\epsilon$;*
- *every user's expected utility is upper bounded by $12k^2\epsilon \log\left(\frac{M}{\epsilon} + 1\right) + (2k+1)\epsilon$ conditioned on the bid being included in the block, and assuming the bid reflects its true value;*
- *the expected social welfare is upper bounded by $O\left(k^3\epsilon \log\left(\frac{M}{\epsilon} + 1\right) + k^2\epsilon\right)$.*

The rest of Section 4 is dedicated to proving Theorem 4.1.

4.1 Proof Roadmap

We first explain the blueprint. To prove that the total social welfare is small, we first show that the miner revenue must be $\widetilde{O}(k^2\epsilon)$ for any bid configuration. If we can show this, then given that the block size is finite, we can show that every user i's utility conditioned on being included is small, which then allows us to bound the total social welfare. Suppose this is not the case, i.e., suppose that under some bid configuration $\mathbf{b} := (b_1, \ldots, b_N)$, there is a user i with expected utility (conditioned on being included) significantly larger than the maximum possible expected miner revenue (which is upper bounded by $\widetilde{O}(k^2\epsilon)$). Then, imagine a world consisting of $\mathbf{b}$ and additionally (infinitely) many users whose true value is the same as b_i. In this case, there must be one such user j whose expected utility is almost 0. Thus, if j is the miner's colluding friend, the miner would be willing to sacrifice all of its revenue, pretend that the world consists of $\mathbf{b}$ where the i-th coordinate is replaced with j's bid, and run the honest mechanism subject to j being included. In this case, the coalition can increase its expected joint utility since user j would be doing much better than the honest case.

The crux of our proof, therefore, is to show that the expected miner revenue must be bounded for any bid vector. To show this, we take two main steps. First, we show that if the world consists of only bids of value M, the expected miner revenue must be small (see Lemma 4.4). Using the above as base case, we then go through an inductive argument to show that in fact, for any bid vector where users do not necessarily bid M, the miner revenue must be small too (see Lemma 4.5). Note that showing the first step itself relies on another inductive argument that inducts on the length of the bid vector.

4.2 Detailed Proof

4.2.1 Individual User's Influence on Miner Revenue is Bounded

Before proving Theorem 4.1, we introduce some useful lemmas. The following lemma states that if, given some bid configuration, a user's expected utility is not too large, then, the miner's expected revenue should not drop too much when we lower that user's bid to 0.

Lemma 4.2. *Given any (possibly randomized) TFM in the plain model that satisfies ϵ-UIC, ϵ-MIC and ϵ-SCP against 1-sized coalition, for any $\mathbf{b}_{-i}$ and v, we have the following where $\mathsf{util}^i(\mathbf{b})$ denotes user i's expected utility and $\mu(\mathbf{b})$ is the expected miner revenue when the bid vector is $\mathbf{b}$:*

$$\mu(\mathbf{b}_{-i}, v) - \mu(\mathbf{b}_{-i}, 0) \leq \begin{cases} 4\epsilon, & v \leq 2\epsilon \\ \mathsf{util}^i(\mathbf{b}_{-i}, v) + 3\epsilon \log \frac{v}{\epsilon} + 4\epsilon, & v > 2\epsilon. \end{cases}$$

Proof. Henceforth, we use $\mathbf{x}(\mathbf{b})$ to denote the vector of probabilities that each bid in $\mathbf{b}$ is included and confirmed, and let $\mathbf{p}(\mathbf{b})$ denote the vector of expected payments for every user when the bid vector is $\mathbf{b}$.

First, observe that Lemma 3.1 and Equation (7) still hold in the plain model where the terms $\overline{x}_i(\cdot)$, $\overline{p}_i(\cdot)$, and $\overline{\mu}(\cdot)$ are now replaced with $x_i(\mathbf{b}_{-i}, \cdot)$ $p_i(\mathbf{b}_{-i}, \cdot)$, and $\mu(\mathbf{b}_i, \cdot)$ respectively, i.e., we now fix an arbitrary fixed $\mathbf{b}_{-i}$ rather than taking expectation over the random choice $\mathbf{b}_{-i}$.

Specifically, Lemma 3.1 implies that for any $\mathbf{b}_{-i}$, for any $b \leq b'$,

$$b' \cdot [x_i(\mathbf{b}_{-i}, b') - x_i(\mathbf{b}_{-i}, b)] + \epsilon \geq p_i(\mathbf{b}_{-i}, b') - p_i(\mathbf{b}_{-i}, b) \geq b \cdot [x_i(\mathbf{b}_{-i}, b') - x_i(\mathbf{b}_{-i}, b)] - \epsilon. \quad (7)$$

Lemma 3.2 implies that for any $\mathbf{b}_{-i}$, for any $b \leq b'$,

$$\mu(\mathbf{b}_{-i}, b') - \mu(\mathbf{b}_{-i}, b) \leq 2\epsilon + (b' - b) \cdot [x_i(\mathbf{b}_{-i}, b') - x_i(\mathbf{b}_{-i}, b)]. \quad (8)$$

Henceforth in this proof, we always fix an arbitrary $\mathbf{b}_{-i}$. For simplicity, in this proof, we omit $\mathbf{b}_{-i}$ and use the short-hand notations $x_i(v) := x_i(\mathbf{b}_{-i}, v)$, $p_i(v) := p_i(\mathbf{b}_{-i}, v)$, and $\mu(v) := \mu(\mathbf{b}_{-i}, v)$.

For $v \le 2\epsilon$, the lemma directly follows from (8). In the rest of the proof, we focus on the case where $v > 2\epsilon$. Define a function $u_i(b)$ such that $\int_0^b u_i(t)dt = b \cdot x_i(b) - p_i(b)$. For any $b \le b'$, the payment when bidding b is

$$p_i(b) = b \cdot x_i(b) - \int_0^b u_i(t)dt.$$

Since we do not have the guarantee that the utility increases with the bids, it can be that $u_i(b) \le 0$ for some b. However, we have that guarantee that at any point, $\int_0^b u_i(t)dt$ is non-negative.

By Equation (7), we know that for any $b \le b'$, we have $p_i(b') - p_i(b) \le b'[x_i(b') - x_i(b)] + \epsilon$, i.e.,

$$\left[b' \cdot x_i(b') - \int_0^{b'} u_i(t)dt\right] - \left[b \cdot x_i(b) - \int_0^b u_i(t)dt\right] \le b' \cdot [x_i(b') - x_i(b)] + \epsilon,$$

which is equivalent to

$$\xi(b, b') := (b' - b) \cdot x_i(b) - \int_b^{b'} u_i(t)dt \le \epsilon. \tag{9}$$

Intuitively, the meaning of $\xi(b, b')$ is how much we are over-estimating if we use a rectangle of width $b' - b$ and height $x_i(b)$ to approximate the area-under-curve[3] for u_i, between b and b'. For example, the blue area in Figure 5a represents $\xi(b, b')$, whereas the red area *minus* the gray area is $\xi(b'', v)$.

Now consider the following sequence: $b_l = v - \frac{v}{2^l}$ for $l = 0, \ldots, L$ where $L = \lceil \log \frac{v}{2\epsilon} \rceil$. By (8), the miner revenue

$$\mu(b_l) - \mu(b_{l-1}) \le 2\epsilon + S(b_{l-1}, b_l),$$

where $S(b_{l-1}, b_l) := (b_l - b_{l-1}) \cdot [x_i(b_l) - x_i(b_{l-1})]$. Summing up the miner revenue difference together, we have

$$\begin{aligned}
&\mu(v) - \mu(0) = \mu(v) - \mu(b_L) + \sum_{l=1}^{L} \mu(b_l) - \mu(b_{l-1}) \\
\le& 2\epsilon + (v - b_L) \cdot [x_i(v) - x_i(b_L)] + \sum_{l=1}^{L} (S(b_{l-1}, b_l) + 2\epsilon) && \text{By (8)} \\
\le& 4\epsilon + 2L\epsilon + \sum_{l=1}^{L} S(b_{l-1}, b_l). && \text{By } v - b_L \le 2\epsilon
\end{aligned}$$

Now we proceed to bound the sum $\sum_{l=1}^{L} S(b_{l-1}, b_l)$. For each $l = 1, \ldots, L$, by the choice of the sequence, we have

$$b_l - b_{l-1} = \frac{v}{2^l} = v - b_l, \quad \text{and} \quad S(b_{l-1}, b_l) = (v - b_l) \cdot [x_i(b_l) - x_i(b_{l-1})]$$

[3] We may assume that any area under 0 contributes negatively to the area-under-curve.

For simplicity, let $b_{L+1} := v$. We have the following:

$$\begin{aligned}
&\sum_{l=1}^{L} S(b_{l-1}, b_l) = \sum_{l=1}^{L} (v - b_l) \cdot [x_i(b_l) - x_i(b_{l-1})] \\
=&(v - b_L) \cdot x_i(b_L) + \sum_{l=1}^{L-1} (b_{l+1} - b_l) \cdot x_i(b_l) \\
=&\sum_{l=1}^{L} (b_{l+1} - b_l) \cdot x_i(b_l). && \text{By } v = b_{L+1}
\end{aligned}$$

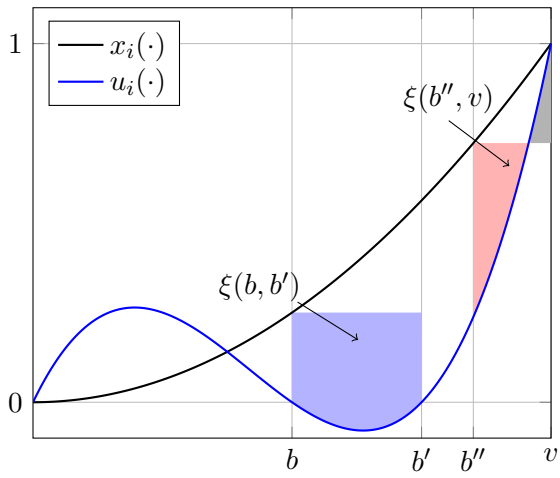
In other words, the sum $\sum_{l=1}^{L} S(b_{l-1}, b_l)$ is equal to the total area of the dashed rectangles in Figure 5b. We want to show that the sum $\sum_{l=1}^{L} S(b_{l-1}, b_l)$ is not significantly greater than $\mathsf{util}^i(v)$, i.e., the area under the u_i-curve. The follow calculation says that this difference is upper bounded by $\sum_{l=1}^{L} \xi(b_l, b_{l+1})$. Formally,

$$\begin{aligned}
&\sum_{l=1}^{L} S(b_{l-1}, b_l) - \int_0^v u_i(t)dt = \sum_{l=1}^{L} (b_{l+1} - b_l) x_i(b_l) - \int_0^v u_i(t)dt \\
\leq&\sum_{l=1}^{L} \left\{ (b_{l+1} - b_l) \cdot x_i(b_l) - \int_{b_l}^{b_{l+1}} u_i(t)dt \right\} && \text{By } \int_0^{b_1} u_i(t) \geq 0 \\
=&\sum_{l=1}^{L} \xi(b_l, b_l + 1) \leq \sum_{l=1}^{L} \epsilon = L\epsilon. && \text{By (9)}
\end{aligned}$$

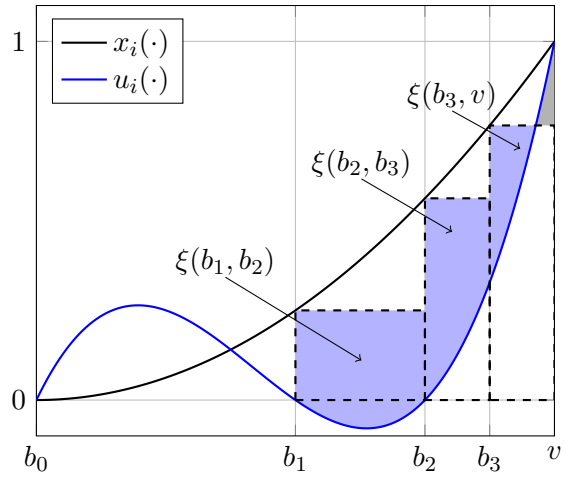
Putting it together, the change in miner revenue $\mu(v) - \mu(0)$ is upper bounded by

$$\begin{aligned}
&\mu(v) - \mu(0) \leq 4\epsilon + 2L\epsilon + \sum_{l=1}^{L} S(b_{l-1}, b_l) \\
\leq&4\epsilon + 2L\epsilon + L\epsilon + \int_0^v u_i(t)dt \leq \mathsf{util}^i(\mathbf{b}_{-i}, v) + 3\epsilon \log \frac{v}{\epsilon} + 4\epsilon,
\end{aligned}$$

where the last step comes from the fact that $L \leq \log \frac{v}{\epsilon}$ by our choice of L. □



(a) The blue area denotes $\xi(b, b')$, and the red area minus the gray area denotes $\xi(b'', v)$.



(b) The sum of the dashed rectangles is equal to $\sum_{l=1}^{L} S(b_l, b_{l+1})$. The difference between $\sum_{l=1}^{L} S(b_l, b_{l+1})$ and the area under the $u_i(\cdot)$ curve is upper bounded by $\sum_{l=1}^{L} \xi(b_l, b_{l+1})$, represented by the sum of the blue areas minus the gray area.

Figure 5: Graphical explanation of the proof to Lemma 4.2

Because the miner can inject a bid 0 for free, Lemma 4.2 implies the following corollary, which says that if we remove a bid, the miner revenue should not be affected by too much.

Corollary 4.3. *Let $(\mathbf{x}, \mathbf{p}, \mu)$ denote any (possibly randomized) TFM in the plain model that satisfies ϵ-UIC, ϵ-MIC and ϵ-SCP against 1-sized coalition. For any $\mathbf{b}_{-i}$ and v,*

$$\mu(\mathbf{b}_{-i}, v) - \mu(\mathbf{b}_{-i}) = \begin{cases} 5\epsilon, & v \le 2\epsilon \\ \mathsf{util}^i(\mathbf{b}_{-i}, v) + 3\epsilon \log \frac{v}{\epsilon} + 5\epsilon, & v > 2\epsilon. \end{cases}$$

Proof. Because the miner can inject a bid 0 for free, by ϵ-MIC, it must be

$$\mu(\mathbf{b}_{-i}, 0) - \mu(\mathbf{b}_{-i}) \le \epsilon. \tag{10}$$

The corollary is now directly implied by Equation (10) and Lemma 4.2. □

4.2.2 Bounds on Miner Revenue

We now prove bounds for the miner's revenue. To do this, we first prove a bound on miner revenue when everyone bids the same value M (see Lemma 4.4). Then, we generalize to the case when everyone's bids need not be the same (see Lemma 4.5).

Notation. Henceforth, for $t \in \mathbb{N} \cup \{0\}$, we define $\mathbf{m}_t := (M, \ldots, M)$ where $|\mathbf{m}_t| = t$; that is, $\mathbf{m}_t$ consists of t copies of M. Recall that $\mu(\mathbf{b})$ denote the expected miner revenue given that the world consists of the bid vector $\mathbf{b}$ (assuming the mechanism is honestly implemented). We define $\widetilde{\mu}(\mathbf{b}')$ to be the expected miner revenue given that *the block configuration* is $\mathbf{b}'$.

Lemma 4.4. *Suppose that the block size is upper bounded by k. Fix an arbitrary any $\epsilon > 0$ and $M > 2\epsilon$ and let $\mathbf{m}_t := (M, M, \ldots, M)$ be a vector containing t repetitions of M. Then, for any*

(possibly randomized) TFM in the plain model that satisfies ϵ-UIC, ϵ-MIC and ϵ-SCP even when the miner colludes with at most $c = 1$ user, it holds that $\widetilde{\mu}(\mathbf{m}_t) \le 12k^2\epsilon \log \frac{M}{\epsilon}$ for all $t \le k$.

Proof. Imagine the world consists of the bid vector $\mathbf{m}_K$ where $K > \frac{Mk}{\epsilon}$ is sufficiently large. Let $\mathbf{m}_{t^*}$ be the block configuration that gives the miner optimal revenue; that is $t^* = \arg\max_{t \le k} \widetilde{\mu}(\mathbf{m}_t)$. Clearly, it must be $\widetilde{\mu}(\mathbf{m}_{t^*}) \ge \mu(\mathbf{m}_K)$. Because of ϵ-MIC, we have $\mu(\mathbf{m}_{t^*}) \ge \widetilde{\mu}(\mathbf{m}_{t^*}) - \epsilon$. Otherwise, if $\mu(\mathbf{m}_{t^*}) < \widetilde{\mu}(\mathbf{m}_{t^*}) - \epsilon$, when the world is $\mathbf{m}_{t^*}$, the miner could simply choose $\mathbf{m}_{t^*}$ as the block configuration so that the revenue becomes $\widetilde{\mu}(\mathbf{m}_{t^*})$, which is more than ϵ higher than its honest utility $\mu(\mathbf{m}_{t^*})$. Combining the two inequalities, we have $\mu(\mathbf{m}_{t^*}) \ge \mu(\mathbf{m}_K) - \epsilon$.

Recall that $\mathsf{util}^i(\mathbf{b})$ denotes user i's expected utility when the bid vector is $\mathbf{b}$. Next, we will show that for any $t \le K$ and any user $i \in [t]$, it must be

$$\mu(\mathbf{m}_t) + \mathsf{util}^i(\mathbf{m}_t) \le \mu(\mathbf{m}_K) + 2\epsilon. \tag{11}$$

For the sake of reaching a contradiction, suppose there is an integer t and user i such that $\mu(\mathbf{m}_t) + \mathsf{util}^i(\mathbf{m}_t) > \mu(\mathbf{m}_K) + 2\epsilon$. Imagine that the world is $\mathbf{m}_K$, where $K > \frac{Mk}{\epsilon}$. There must exist a user j whose confirmation probability is at most $x_j(\mathbf{m}_K) \le \frac{k}{K} < \frac{\epsilon}{M}$, as at most k bids can be included in a block. Therefore, user j's utility is at most $\mathsf{util}^j(\mathbf{m}_K) \le x_j(\mathbf{m}_K) \cdot M < \epsilon$. Imagine that the miner now colludes with user j. The miner implements the inclusion rule as if the world consists of the bid vector $\mathbf{m}_t$ where the i-th position is occupied by user j's bid. Since the TFM is symmetric, and both users bid M, user j's expected utility is now $\mathsf{util}^i(\mathbf{m}_t)$. The joint utility of the coalition now is $\mu(\mathbf{m}_t) + \mathsf{util}^i(\mathbf{m}_t) > \mu(\mathbf{m}_K) + 2\epsilon > \mu(\mathbf{m}_K) + \mathsf{util}^j(\mathbf{m}_K) + \epsilon$, which contradicts ϵ-SCP. Consequently, Equation (11) must hold for any $t \le K$ and any user $i \in [t]$.

According to Equation (11), we have $\mu(\mathbf{m}_{t^*}) + \mathsf{util}^i(\mathbf{m}_{t^*}) \le \mu(\mathbf{m}_K) + 2\epsilon$ for any user i. As we have shown, it must be $\mu(\mathbf{m}_{t^*}) \ge \mu(\mathbf{m}_K) - \epsilon$. Combining these two inequalities, we have

$$\mathsf{util}^i(\mathbf{m}_{t^*}) \le \mu(\mathbf{m}_K) + 2\epsilon - \mu(\mathbf{m}_{t^*}) \le \mu(\mathbf{m}_K) + 2\epsilon - \mu(\mathbf{m}_K) + \epsilon = 3\epsilon.$$

Since the utility of user i is bounded, by applying Corollary 4.3, it must be

$$\mu(\mathbf{m}_{t^*}) - \mu(\mathbf{m}_{t^*-1}) \le \mathsf{util}^i(\mathbf{m}_{t^*}) + 3\epsilon \log \frac{M}{\epsilon} + 5\epsilon \le 8\epsilon + 3\epsilon \log \frac{M}{\epsilon}. \tag{12}$$

Consequently, we have

$$\begin{aligned}
&\mathsf{util}^i(\mathbf{m}_{t^*-1}) \le \mu(\mathbf{m}_K) + 2\epsilon - \mu(\mathbf{m}_{t^*-1}) && \text{By (11)}\\
\le&\mu(\mathbf{m}_K) + 2\epsilon - \mu(\mathbf{m}_{t^*}) + 8\epsilon + 3\epsilon \log \frac{M}{\epsilon} && \text{By (12)}\\
\le&\mu(\mathbf{m}_K) + 2\epsilon - \mu(\mathbf{m}_K) + \epsilon + 8\epsilon + 3\epsilon \log \frac{M}{\epsilon} && \text{By } \mu(\mathbf{m}_{t^*}) \ge \mu(\mathbf{m}_K) - \epsilon\\
=&11\epsilon + 3\epsilon \log \frac{M}{\epsilon}.
\end{aligned}$$

Then, we can apply Corollary 4.3 again, and we have

$$\mu(\mathbf{m}_{t^*-1}) - \mu(\mathbf{m}_{t^*-2}) \le \mathsf{util}_i(\mathbf{m}_{t^*-1}) + 3\epsilon \log \frac{M}{\epsilon} + 5\epsilon \le 16\epsilon + 6\epsilon \log \frac{M}{\epsilon}.$$

By the same reason, for any $r \le t^*$, we have

$$\mu(\mathbf{m}_{t^*-r}) - \mu(\mathbf{m}_{t^*-r-1}) \le (8r + 8)\epsilon + (3r + 3) \cdot \epsilon \log \frac{M}{\epsilon}. \tag{13}$$

Since $M \geq 2\epsilon$, we have $\epsilon \log \frac{M}{\epsilon} \geq \epsilon$. By Eq.(13), we have

$$\begin{aligned}
&\mu(\mathbf{m}_{t^*}) - \mu(\mathbf{m}_0) = \sum_{r=0}^{t^*-1} \mu(\mathbf{m}_{t^*-r}) - \mu(\mathbf{m}_{t^*-r-1}) \\
\leq &(8t^* + 4(t^*-1)t^*)\,\epsilon + \left(3t^* + \frac{3(t^*-1)t^*}{2}\right) \cdot \epsilon \log \frac{M}{\epsilon} \\
\leq &11(t^*)^2 \epsilon \log \frac{M}{\epsilon}. && \text{By } \epsilon \log \frac{M}{\epsilon} \geq \epsilon \text{ and } t^* \geq 1
\end{aligned}$$

Notice that $\mu(\mathbf{m}_0) = 0$, so we have

$$\mu(\mathbf{m}_{t^*}) \leq 11(t^*)^2 \epsilon \log \frac{M}{\epsilon}.$$

Recall that we define $t^* = \arg\max_{t \leq k} \widetilde{\mu}(\mathbf{m}_t)$. By definition, $\widetilde{\mu}(\mathbf{m}_t) \leq \widetilde{\mu}(\mathbf{m}_{t^*})$ for all $t \leq k$. As we have shown at the beginning, it must be $\mu(\mathbf{m}_{t^*}) \geq \widetilde{\mu}(\mathbf{m}_{t^*}) - \epsilon$. Thus, we have $\widetilde{\mu}(\mathbf{m}_t) \leq \widetilde{\mu}(\mathbf{m}_{t^*}) \leq \mu(\mathbf{m}_{t^*}) + \epsilon$ for all $t \leq k$. Combine the arguments above, we have $\widetilde{\mu}(\mathbf{m}_t) \leq 11k^2\epsilon \log \frac{M}{\epsilon} + \epsilon \leq 12k^2\epsilon \log \frac{M}{\epsilon}$ for all $t \leq k$.

□

Lemma 4.5. *Suppose the block size is upper bounded by k. Fix any $\epsilon > 0$. For any (possibly randomized) TFM in the plain model that satisfies ϵ-UIC, ϵ-MIC and ϵ-SCP (even when the miner only colludes with one user), for any block configuration $\mathbf{b}$, the following must hold where M is the maximum bid amount in the bid vector $\mathbf{b}$:*

$$\widetilde{\mu}(\mathbf{b}) \leq \begin{cases} 2k\epsilon, & \text{if } M < 2\epsilon, \\ 12k^2\epsilon \log \frac{M}{\epsilon} + 2k\epsilon, & \text{if } M \geq 2\epsilon. \end{cases}$$

Proof. Given any block configuration $\mathbf{b}$, the miner revenue must be upper bounded by the sum of the bids in $\mathbf{b}$. Thus, if $M < 2\epsilon$, the miner revenue is upper bounded by $2k\epsilon$.

Henceforth, we focus on the case $M \geq 2\epsilon$. Throughout the proof, we say that a bid b is a *low bid* if $b < M$. Then, any block configuration, up to reordering, can be represented by $(\mathbf{m}_t, \mathbf{L})$ for some $t \geq 1$, where $\mathbf{m}_t$ consists of t repetitions of M, $\mathbf{L}$ which is possibly of length 0, contains only low bids. We prove the following claim by induction on the length of $\mathbf{L}$:

> *For any $\mathbf{L}$ consisting of only low bids, for any t such that $t + |\mathbf{L}| \leq k$, the miner revenue $\widetilde{\mu}(\mathbf{m}_t, \mathbf{L}) \leq \tau + 2|\mathbf{L}|\epsilon$, where we set $\tau := 12k^2\epsilon \log \frac{M}{\epsilon}$.*

For the base case where $|\mathbf{L}| = 0$, i.e. the block does not contain any low bid, it is proven by Lemma 4.4.

Now, suppose we have proven that for any $\mathbf{L}'$ of length R, for any t, the miner revenue $\widetilde{\mu}(\mathbf{m}_t, \mathbf{L}') \leq \tau + 2R\epsilon$. We are going to show that for any $\mathbf{L}$ of length $R+1$, for any t, the miner revenue $\widetilde{\mu}(\mathbf{m}_t, \mathbf{L}) \leq \tau + 2(R+1)\epsilon$.

For the sake of contradiction, suppose there exists a bid $\mathbf{L}$ of length $R+1$ and there exists a t, such that for the block configuration $(\mathbf{m}_t, \mathbf{L}) = (\mathbf{m}_t, d_1, \ldots, d_R, d_{R+1})$, the miner's revenue is $\tau + 2(R+1)\epsilon + \delta$ for some $\delta > 0$. Now, imagine that the world consists of $(\mathbf{m}_K, d_1, \ldots, d_R)$, where $K > \frac{kM}{\epsilon}$. In this case, the block configuration output by the honest inclusion rule must be of the form $(\mathbf{m}_{t^*}, \mathbf{d})$ for some $t^* \leq k - |\mathbf{d}|$ and $\mathbf{d} \subseteq \{d_1, \ldots, d_R\}$ consists of only low bids. Since $(\mathbf{m}_{t^*}, \mathbf{d})$ only contains at most R low bids, the miner revenue $\widetilde{\mu}(\mathbf{m}_{t^*}, \mathbf{d}) \leq \tau + 2R\epsilon$ by induction hypothesis.

By our choice of K, there must exist a user i with true value M, whose confirmation probability $x_i(\mathbf{m}_K, d_1, \ldots, d_R) \leq \frac{k}{K} < \frac{\epsilon}{M}$ when the miner is honest. Thus, user i's utility is at most $M \cdot x_i(\mathbf{m}_K, d_1, \ldots, d_R) < \epsilon$. Now the miner can collude with user i, ask user i to bid d_{R+1} instead of its true value M and include $(\mathbf{m}_t, d_1, \ldots, d_R, d_{R+1})$ in the block. Since $d_{R+1} < M$ and the payment never exceeds the bid, user i's utility is at least zero. This implies that the decrease of the utility of user i is strictly less than ϵ. Now the miner revenue is $\tau + 2(R+1)\epsilon + \delta$ by our assumption, whereas the miner revenue in the honest case is at most $\tau + 2R\epsilon$. Thus, the miner revenue increases by more than 2ϵ compared to the honest case. Thus, the joint utility of the coalition increases by more than ϵ, which contradicts ϵ-SCP. Therefore, by induction, we have that $\mu(\mathbf{m}_t, \mathbf{L}) \leq \tau + 2|\mathbf{L}|\epsilon$ for any $\mathbf{L}$ and any t where $|\mathbf{L}| + t \leq k$. Finally, since $|\mathbf{L}| \leq k$, we conclude that $\widetilde{\mu}(\mathbf{b}) \leq 12k^2\epsilon \log \frac{M}{\epsilon} + 2k\epsilon$. □

4.2.3 Completing the Proof of Theorem 4.1

We now complete the proof of Theorem 4.1. To do so, we prove that each user's utility conditioned on being included must be bounded given that the miner revenue is bounded (see Lemma 4.6), which then leads to our conclusion that the total social welfare must be small.

Lemma 4.6. *Suppose that the block size is upper bounded by k. Fix any $\epsilon > 0$. For any (possibly randomized) TFM in the plain model satisfies ϵ-UIC and ϵ-SCP (even when the miner colludes with only one user), for any bid vector $\mathbf{b}$ where $M := \max(\mathbf{b})$, for and any user i, conditioned on user i being included in the block, user i's utility must be upper bounded by $U + \epsilon$ where $U = \max_{|\mathbf{b}'| \leq k, \max(\mathbf{b}') \leq M} \widetilde{\mu}(\mathbf{b}')$, i.e., U is the maximum possible revenue the miner can get among all possible block configurations where all bids are at most M.*

Proof. For the sake of contradiction, suppose that under some bid vector $\mathbf{b}'$ where all bids are at most M, some user j's expected utility conditioned on being included in the block is strictly more than $U + \epsilon$. This implies that there must exist a block configuration $\mathbf{b} = (b_1, \ldots, b_{|\mathbf{b}|})$ where all bids are at most M, and some $i \leq |\mathbf{b}|$, such that under conditioned on the block configuration being $\mathbf{b}$, the i-th bid b_i in the block has expected utility at least $U + \epsilon + \delta$ for some positive δ. Let $T = \lceil \frac{b_i k}{\delta} \rceil + 1$. Imagine that the world consists of the bid vector $\mathbf{b}'$ of length $T + |\mathbf{b}|$ where

$$\mathbf{b}' = (\mathbf{b}, \underbrace{b_i, b_i, \ldots, b_i}_{T}).$$

Because the block size is upper bounded by k, there must exist a user j whose bid is b_i while its confirmation probability is at most $\frac{k}{T}$. Therefore, if user j bids truthfully, its utility is at most $b_i \cdot \frac{k}{T} < \delta$. By our assumption, the miner revenue is at most U under any block configuration where bids are upper bounded by M. Thus, when behaving honestly, the miner and user j have joint utility strictly less than $U + \delta$. However, the miner can collude with user j and prepare the block where the block configuration is $\mathbf{b}$ and the i-th position is replaced with user j's bid instead. In this case, user j's utility is $U + \epsilon + \delta$. Because the coalition does not inject any fake bid, the miner's utility is at least zero. Thus, by deviating from the mechanism, the joint utility of the coalition becomes at least $U + \epsilon + \delta$, which exceeds the honest case by more than ϵ. This contradicts ϵ-SCP. □

Proof of Theorem 4.1. Suppose the world consists of an arbitrary bid vector $\mathbf{b}$. Let $M = \max(\mathbf{b})$. If $M < 2\epsilon$, the miner can have at most $2k\epsilon$-miner revenue by Lemma 4.5. For any user i who is bidding truthfully, its true value must be upper bounded by M since $M = \max(\mathbf{b})$.

Moreover, each confirmed user's utility is at most its true value, which is upper bounded by $M < 2\epsilon$. Since there are at most k number of confirmed user, the expected social welfare is $\sum_i \mathsf{util}^i(\mathbf{b})$ plus the miner's expected utility, which is upper bounded by $4k\epsilon$.

In the rest of the proof, we assume $M \geq 2\epsilon$ and we define $\widehat{\mathsf{util}}^i(\mathbf{b})$ to be the utility of user i conditioned on being confirmed when the world consists of the bid vector $\mathbf{b}$. By Lemma 4.5, the miner can have at most $\left(12k^2\epsilon \log \frac{M}{\epsilon} + 2k\epsilon\right)$-miner revenue. By Lemma 4.6, for any i, $\widehat{\mathsf{util}}^i(\mathbf{b}) \leq 12k^2\epsilon \log \frac{M}{\epsilon} + (2k+1)\epsilon$. Let γ_i be the probability that user i is included in the block given the bid vector $\mathbf{b}$. Observe that $\sum_i \gamma_i \leq k$ for any $\mathbf{b}$. Therefore, the expected total utility of all users is upper bounded by

$$\sum_i \mathsf{util}^i(\mathbf{b}) = \sum_i \widehat{\mathsf{util}}^i(\mathbf{b}) \cdot \gamma_i \leq \left(12k^2\epsilon \log \frac{M}{\epsilon} + (2k+1)\epsilon\right) \cdot \sum_i \gamma_i = O\left(k^3\epsilon \log \frac{M}{\epsilon}\right).$$

The expected social welfare is $\sum_i \mathsf{util}^i(\mathbf{b})$ plus the miner's expected utility. Clearly, it is also upper bounded by $O\left(k^3\epsilon \log \frac{M}{\epsilon}\right)$.

Combine the argument above, because $\log\left(\frac{M}{\epsilon} + 1\right)$ is always non-negative, the theorem follows.

5 Characterization for Finite Block Size in the MPC-Assisted Model

5.1 Characterization for Strict Incentive Compatibility

In this section, we give a characterization of strict incentive compatibility in the MPC-assisted model for finite block size. We show that cryptography helps us overcome the finite-block impossibility [CS21] for $c = 1$, but for $c \geq 2$, the impossibility still holds.

5.1.1 Feasibility for $c = 1$

In the MPC-assisted model, we indeed can have a mechanism that achieves UIC, MIC, and $(\rho, 1)$-SCP against a coalition with an arbitrary $\rho \in (0, 1]$ mining power and $c = 1$ user.

MPC-assisted, finite-block posted price auction

Parameters: the reserved price r, and a block size k.
Input: a bid vector $\mathbf{b} = (b_1, \ldots, b_N)$.
Mechanism:

- *Allocation rule.* Any bid that is at least r is considered as a candidate. Randomly select k bids from the candidates to confirm.
- *Payment rule.* Each confirmed bid pays r.
- *Miner revenue rule.* Miner gets 0 revenue.

In the above mechanism, the miner gains zero revenue. This is inevitable as shown in Theorem B.5 of Appendix B.1. Even in the MPC-assisted model, the miner must have zero revenue if we insist on strict incentive compatibility (even under Bayesian notions of equilibrium).

Theorem 5.1. *Assuming a finite block size k. The above MPC-assisted, finite-block posted price auction in the MPC-assisted model satisfies UIC, MIC, and $(\rho, 1)$-SCP (in the ex post setting) for arbitrary $\rho \in (0, 1]$.*

Proof. We will prove the three incentive compatibility properties separately.

UIC. Let v_i denote the true value of user i. First, refusing to bid cannot increase its utility. Moreover, injecting bids does not help either. To see this, assume that user i bids its true value v_i and injects a bid b'. If $b' < r$, then it does not influence user i's utility. If $b' \geq r$, it either decreases the probability of user i being confirmed if $v_i \geq r$, or it brings user i negative expected utility if $v_i < r$.

Thus, we only need to argue that overbidding or underbidding does not increase the user's utility. If user i's true value $v_i < r$, then its utility when overbidding $b \geq r$ is $q \cdot (v_i - r) < 0$, where q is the probability of b being confirmed. If user i's true value $v_i \geq r$, then underbidding $b < r$ brings it 0-utility, whereas the honest utility $q(v_i - r)$ is positive. Therefore, no matter how user i deviates from the protocol, its utility does not increase.

MIC. Since the total miner revenue is always 0, injecting fake bids does not increase the colluding miner's utility. The miner cannot increase its utility by deviating from the protocol.

SCP. No matter how the coalition deviates, the colluding miner's revenue is always 0. Therefore, the joint utility of the coalition is at most the utility of the colluding user. By strict UIC, the joint utility does not increase. □

Note that the above mechanism does not work for $c = 2$. Imagine that the miner colludes with two users i and j, where user i has true value exactly r and user j has a sufficiently large true value. User i may choose not to bid to increase the probability of user j being confirmed. This brings the coalition strictly more utility than behaving honestly.

5.1.2 Impossibility for $c \geq 2$

Unfortunately, even in the MPC-assisted model, no mechanism with non-trivial utility can achieve UIC, MIC, and $(\rho, 2)$-SCP, even for Bayesian notions of incentive compatibility. To see this, observe that under the strict incentive compatible notion, (ρ, c)-SCP implies that any coalition of $\leq c$ users cannot benefit from any deviation[4], since the miner revenue has to be 0 by Theorem B.5 of Appendix B.1. Similar to the proof in Goldberg and Hartline [GH05], we show that any mechanism that is Bayesian UIC and Bayesian SCP against a $(\rho, 2)$-sized coalition (for an arbitrary $\rho \in (0, 1]$ must satisfy the following condition: no matter how a user j changes its bid, user i's utility should not change. Formally,

Lemma 5.2. *Given any (possibly random) mechanism in the MPC-assisted model that is Bayesian UIC and Bayesian SCP against $(\rho, 2)$-sized coalition for some $\rho \in (0, 1]$, and suppose each user's true value is drawn i.i.d. from a distribution $\mathcal{D}$. Then, for any user i and user j, for any bid b_j and b'_j, any value v, it must be that for any ℓ,*

$$\mathop{\mathbf{E}}_{\mathbf{b}_{-i,j} \sim \mathcal{D}^\ell}[\mathsf{util}^i(v, b_j, \mathbf{b}_{-i,j})] = \mathop{\mathbf{E}}_{\mathbf{b}_{-i,j} \sim \mathcal{D}^\ell}[\mathsf{util}^i(v, b'_j, \mathbf{b}_{-i,j})],$$

where $\mathbf{b}_{-i,j}$ represents all except user i and user j's bids.

The proof of this lemma is deferred to Appendix B.2. This lemma implies that no matter how user j changes its bid, the utility of user i when bidding its true value should not change. Consequently, we have the following result stating that user i's utility should remain the same when bidding its true value, regardless of how many users are there.

[4] We credit Bahrani, Garimidi, Roughgarden, Shi, and Weinberg for making this observation.

Lemma 5.3. *Given any (possibly randomized) mechanism in the MPC-assisted model that achieves Bayesian UIC and Bayesian SCP against $(\rho, 2)$-sized coalition for some $\rho \in (0, 1]$, it holds that for any user i and user j, any value v_i and b_j, for any ℓ,*

$$\mathop{\mathbf{E}}_{\mathbf{b}_{-i,j} \sim \mathcal{D}^\ell}[\mathsf{util}^i(v_i, b_j, \mathbf{b}_{-i,j})] \leq \mathop{\mathbf{E}}_{\mathbf{b}_{-i,j} \sim \mathcal{D}^\ell}[\mathsf{util}^i(v_i, \mathbf{b}_{-i,j})],$$

where v_{id} (b_{id}) denotes a bid v (b) coming from identity id.

Proof roadmap for Lemma 5.3. By Lemma 5.2, $\mathop{\mathbf{E}}_{\mathbf{b}_{-i,j} \sim \mathcal{D}^\ell}[\mathsf{util}^i(v_i, b_j, \mathbf{b}_{-i,j})] = \mathop{\mathbf{E}}_{\mathbf{b}_{-i,j} \sim \mathcal{D}^\ell}[\mathsf{util}^i(v_i, 0_j, \mathbf{b}_{-i,j})]$. Therefore, to prove Lemma 5.3, it suffices to prove that

$$\mathop{\mathbf{E}}_{\mathbf{b}_{-i,j} \sim \mathcal{D}^\ell}[\mathsf{util}^i(v_i, 0_j, \mathbf{b}_{-i,j})] \leq \mathop{\mathbf{E}}_{\mathbf{b}_{-i,j} \sim \mathcal{D}^\ell}[\mathsf{util}^i(v_i, \mathbf{b}_{-i,j})].$$

This claim is relatively easy to prove if we are willing to assume a *strong* symmetry assumption explained below. With a technically more involved proof, we can eventually get rid of this *strong* symmetry assumption and prove it under our current (much weaker) symmetry assumption defined in Section 2.1.

> *Strong symmetry assumption.* On top of our current symmetric assumption defined in Section 2.1, we additionally assume that for any bid vector $\mathbf{b} := (b_1, \ldots, b_N)$, if for $i \neq j$, $b_i = b_j$, then the random variables (x_i, p_i) and (x_j, p_j) are identically distributed, where (x_i, p_i) are random variables denoting i's confirmation probability and i's payment, respectively, and (x_j, p_j) are similarly defined.

In other words, the strong symmetry assumption additionally assumes that two bids of the same amount receive the same treatment, on top of our existing symmetry assumption — note that this is a very strong assumption, and this is why we want to get rid of it eventually. If the above strong symmetry assumption holds, then we have that for any identity i' that injects a 0 bid,

$$\mathop{\mathbf{E}}_{\mathbf{b}_{-i,j} \sim \mathcal{D}^\ell}[\mathsf{util}^i(v_i, 0_j, \mathbf{b}_{-i,j})] = \mathop{\mathbf{E}}_{\mathbf{b}_{-i,j} \sim \mathcal{D}^\ell}[\mathsf{util}^i(v_i, 0_{i'}, \mathbf{b}_{-i,j})],$$

This is because under the strong symmetry assumption, anyone who bids the same amount as i has the same expected utility, and moreover, this utility is not affected by whether the 0 bid is posted by j or i'. Finally, we have

$$\mathop{\mathbf{E}}_{\mathbf{b}_{-i,j} \sim \mathcal{D}^\ell}[\mathsf{util}^i(v_i, 0_{i'}, \mathbf{b}_{-i,j})] \leq \mathop{\mathbf{E}}_{\mathbf{b}_{-i,j} \sim \mathcal{D}^\ell}[\mathsf{util}^i(v_i, \mathbf{b}_{-i,j})].$$

Otherwise, user i can inject a 0-bid using an arbitrary identity i', which strictly increases its utility. This contradicts Bayesian UIC. We refer the reader to Appendix B.3 for a full proof of Lemma 5.3 without relying on the strong symmetry assumption.

Lemma 5.4. *Given any (possibly randomized) mechanism in the MPC-assisted model that achieves Bayesian UIC and Bayesian SCP against $(\rho, 2)$-sized coalitions for some $\rho \in (0, 1]$, it holds that for any user i, any value v_i, for any $\ell \geq 0$,*

$$\mathop{\mathbf{E}}_{\mathbf{b}_{-i} \sim \mathcal{D}^\ell}[\mathsf{util}^i(v_i, \mathbf{b}_{-i})] = \mathsf{util}^i(v_i).$$

Proof. We first show that for any j, user i's utility should not change if user j refuses to bid. Formally, for any b_j,

$$\mathop{\mathbf{E}}_{\mathbf{b}_{-i,j}\sim\mathcal{D}^\ell}[\mathsf{util}^i(v_i, b_j, \mathbf{b}_{-i,j})] = \mathop{\mathbf{E}}_{\mathbf{b}_{-i,j}\sim\mathcal{D}^\ell}[\mathsf{util}^i(v_i, \mathbf{b}_{-i,j})]. \tag{14}$$

To see this, by Lemma 5.3, we have

$$\mathop{\mathbf{E}}_{\mathbf{b}_{-i,j}\sim\mathcal{D}^\ell}[\mathsf{util}^i(v_i, b_j, \mathbf{b}_{-i,j})] \leq \mathop{\mathbf{E}}_{\mathbf{b}_{-i,j}\sim\mathcal{D}^\ell}[\mathsf{util}^i(v_i, \mathbf{b}_{-i,j})].$$

Moreover, by Lemma 5.2, we have

$$\mathop{\mathbf{E}}_{\mathbf{b}_{-i,j}\sim\mathcal{D}^\ell}[\mathsf{util}^i(v_i, b_j, \mathbf{b}_{-i,j})] = \mathop{\mathbf{E}}_{\mathbf{b}_{-i,j}\sim\mathcal{D}^\ell}[\mathsf{util}^i(v_i, 0_j, \mathbf{b}_{-i,j})] \geq \mathop{\mathbf{E}}_{\mathbf{b}_{-i,j}\sim\mathcal{D}^\ell}[\mathsf{util}^i(v_i, \mathbf{b}_{-i,j})].$$

Otherwise the miner can collude with user i and user j with true value 0, and ask user j not to bid. This strictly increase user i's utility while user j's and miner's utility remain unchanged. This contradicts Bayesian SCP against $(\rho, 2)$-sized coalition. Equation (14) thus follows.

Let $f(\cdot)$ denote the p.d.f. of $\mathcal{D}$. By definition of expectation,

$$\begin{aligned}
&\mathop{\mathbf{E}}_{\mathbf{b}_{-i}\sim\mathcal{D}^\ell}[\mathsf{util}^i(v_i, \mathbf{b}_{-i})] = \int_0^\infty \mathop{\mathbf{E}}_{\mathbf{b}_{-i,1}\sim\mathcal{D}^{\ell-1}}[\mathsf{util}^i(v_i, z_1, \mathbf{b}_{-i,1})] f(z_1) dz_1 \\
&= \int_0^\infty \mathop{\mathbf{E}}_{\mathbf{b}_{-i,1}\sim\mathcal{D}^{\ell-1}}[\mathsf{util}^i(v_i, \mathbf{b}_{-i,1})] f(z_1) dz_1 && \text{By Equation (14)} \\
&= \mathop{\mathbf{E}}_{\mathbf{b}_{-i,1}\sim\mathcal{D}^{\ell-1}}[\mathsf{util}^i(v_i, \mathbf{b}_{-i,1})].
\end{aligned}$$

The lemma follows by repeating the above argument. □

Now we are ready to prove the theorem stating that there is no mechanism that gives non-zero utility to either users or miners and yet satisfies Bayesian UIC, MIC and SCP against $(\rho, 2)$-sized coalitions.

Theorem 5.5. *Suppose the block size is k. No MPC-assisted mechanism with non-trivial utility simultaneously achieves Bayesian UIC, Bayesian MIC and Bayesian SCP against $(\rho, 2)$-sized coalitions.*

Proof. By Theorem B.5, the miner-revenue has to be 0. Therefore, it suffices to prove that every user must have 0-utility. Suppose there are n users, whose true values are drawn i.i.d. from a distribution $\mathcal{D}$. For the sake of contradiction suppose that there exists an MPC-assisted mechanism with non-trivial utility that is UIC, MIC and SCP against $(\rho, 2)$-sized coalitions. Then there must exist a bid vector $\mathbf{b}_{-j^*} \in \mathrm{Supp}\left(\mathcal{D}^{n-1}\right)$ and a value v such that when user j^* bids its true value v, it gets utility $\mathsf{util}^{j^*}(v_{j^*}, \mathbf{b}_{-j^*}) > 0$. Therefore,

$$\mathop{\mathbf{E}}_{\mathbf{b}_{-j^*}\sim\mathcal{D}^{n-1}}[\mathsf{util}^{j^*}(v_{j^*}, \mathbf{b}_{-j^*})] = u^* > 0.$$

Let $f(\cdot)$ denote the p.d.f. of $\mathcal{D}$. In the rest of the proof, we will omit the identity who bids v, since the identity is implied by the rest of the world $\mathbf{b}_{-i}$. Note that for any ℓ, any user i,

by Lemma 5.4,

$$\begin{aligned}
&\mathsf{util}^i(v) = \mathop{\mathbf{E}}_{\mathbf{b}_{-i}\sim\mathcal{D}^{\ell-1}}[\mathsf{util}^i(v,\mathbf{b}_{-i})] \\
&= \int_0^\infty \mathop{\mathbf{E}}_{\mathbf{b}_{-i,1}\sim\mathcal{D}^{\ell-2}}[\mathsf{util}^i(v,z_1,\mathbf{b}_{-i,1})]f(z_1)dz_1 \\
&= \int_0^\infty \mathop{\mathbf{E}}_{\mathbf{b}_{-i,1}\sim\mathcal{D}^{\ell-2}}[\mathsf{util}^i(v,v,\mathbf{b}_{-i,1})]f(z_1)dz_1 && \text{By Lemma 5.2} \\
&= \mathop{\mathbf{E}}_{\mathbf{b}_{-i,1}\sim\mathcal{D}^{\ell-2}}[\mathsf{util}^i(v,v,\mathbf{b}_{-i,1})] \\
&= \cdots = \mathsf{util}^i\underbrace{(v,v,\ldots,v)}_{\ell}.
\end{aligned}$$

We also have that for any user i, $\mathsf{util}^i(v,\ldots,v) = \mathsf{util}^i(v) = \mathsf{util}^{j^*}(v) = \mathop{\mathbf{E}}_{\mathbf{b}_{-j^*}\sim\mathcal{D}^{n-1}}[\mathsf{util}^{j^*}(v_{j^*},\mathbf{b}_{-j^*})] = u^* > 0$, where the second equality follows from the symmetry of the mechanism, and the third equality comes from Lemma 5.4.

However, consider a world with $K = \lceil\frac{v(k+1)}{u^*}\rceil$ bids all equal to v. There must exist a user j whose utility is no more than $v\cdot\frac{k}{K} < u^*$ by the choice of K, i.e., $\mathsf{util}^j\underbrace{(v,v,\ldots,v)}_{K} < u^*$. This contradicts the conclusion that $\mathsf{util}^j\underbrace{(v,v,\ldots,v)}_{K} = \mathsf{util}^j(v) = u^*$. □

Remark 5.6. *If we are willing to assume an a-priori known upper bound M on the users' true values, we can actually design a mechanism that is UIC, MIC and SCP for arbitrary $\rho\in(0,1]$ and $c\geq 1$ with 0 user and miner utility. We simply run posted price auction with the reserved price M and the miners get nothing. However, this mechanism is utility-equivalent to a trivial mechanism where no one is confirmed.*

5.2 Feasibility of Approximate Incentive Compatibility

Although strict (even Bayesian) incentive compatibility is impossible to achieve for $c\geq 2$ in the MPC-assisted model, we have meaningful feasibility results if we allow ϵ additive slack. Still, we use k to denote the finite block size and M to denote the upper bound of the true values. Specifically, we can achieve $\Theta(kM)$ social welfare as long as many people place high enough bids, which is asymptotically the best possible social welfare one can hope for.

MPC-assisted, Diluted Posted Price Auction

Parameters: the block size k, an upper bound c of the number of users colluding with the miner, an upper bound M of users' true values, a slack $\epsilon\geq 0$, and a posted-price r such that $r\geq\frac{\epsilon}{2c}$.

Input: a bid vector $\mathbf{b} = (b_1,\ldots,b_N)$.

Mechanism:

1. *Allocation rule.*

   - Given a bid vector $\mathbf{b} = (b_1,\ldots,b_N)$, remove all bids which are smaller than r. Let $\widetilde{\mathbf{b}} = (\widetilde{b}_1,\ldots,\widetilde{b}_\ell)$ denote the resulting vector.

- Let $T = \max\left(2c\sqrt{\frac{kM}{\epsilon}}, k\right)$. If $\ell \geq T$, let $\mathbf{d} = \widetilde{\mathbf{b}}$. Else, let $\mathbf{d} = (\widetilde{b}_1, \ldots, \widetilde{b}_\ell, 0, \ldots, 0)$ such that $|\mathbf{d}| = T$. In other words, $\mathbf{d}$ is $\widetilde{\mathbf{b}}$ appended with $T - \ell$ zeros.
- Randomly choose a set S of size k from $\mathbf{d}$, and every non-zero bid in S is confirmed.

2. *Payment rule.* For each confirmed bid b, it pays r.

3. *Miner revenue rule.* For each confirmed bid b, the miner is paid $\frac{\epsilon}{2c}$.

Theorem 5.7. *Suppose there exists an upper bound M on users' true values. The above MPC-assisted, diluted posted price auction satisfies UIC, MIC, and ϵ-SCP (in the ex post setting) against (ρ, c)-sized coalitions for arbitrary $\rho \in (0, 1]$ and $c \geq 1$.*

Proof. We will prove the three incentive compatibility properties separately. Note that in this mechanism, refusing to bid is equivalent to underbidding some value less than r. So we mainly focus on the strategy space of bidding untruthfully and injecting bids. When we say the expected utility of a user, the randomness is taken over the randomness in the mechanism.

UIC. Fix any user i, and let v denote the true value of user i. In the mechanism, any confirmed bid pays r and any bid less than r must be unconfirmed. Thus, if $v \leq r$, bidding untruthfully cannot give a postive utility, so bidding truthfully and getting 0-utility is optimal.

Below we focus on the case when $v > r$. In this case, the bid has a non-negative probability of being confirmed and it pays r. So following the honest strategy leads to positive utility. Bidding less than r will cause the bid to be unconfirmed and will not help the user. Therefore, we may assume that the user bids at least r and may inject some fake bids. Observe that any bid that is at least r is treated the same by the mechanism. Moreover, injecting fake bids either make no difference (when $\ell \leq T$ after injecting), or it reduces the probability of bid v being elected into the set S (when $\ell > T$ after injecting). Therefore, bidding untruthfully and/or injecting fake bids does not help the user.

MIC. By injecting fake bids, the strategic miner cannot increase the expected number of real bids in the vector $\mathbf{d}$. Thus, injecting fake bids cannot increase other bids' contribution towards the miner's revenue. Therefore, the expected gain in miner revenue must be upper bounded by the fake bids' contribution towards miner revenue minus the expected payments of the fake bids. For each confirmed bid, the miner revenue is fixed to $\frac{\epsilon}{2c}$, which is no more than the payment of the bid. Thus, the expected miner revenue cannot increase through injecting fake bids, i.e., the mechanism is MIC.

ϵ-SCP. First, we argue that injecting bids does not help the coalition. Specifically, using a similar proof as UIC, injecting bids does not help improve the utility of any user in the coalition. Using a similar argument as MIC, injecting bids does not improve the miner's revenue minus the payment of the injected bids. Therefore, injecting bids will not increase the coalition's joint utility.

Now it suffices to argue that underbidding or overbidding does not increase the coalition's joint utility by more than ϵ. Suppose when bidding honestly, the number of bids in $\widetilde{\mathbf{b}}$ is ℓ. Each bid in $\widetilde{\mathbf{b}}$ is confirmed with probability $\frac{k}{\max\{T,\ell\}}$. Assume that by bidding untruthfully, the coalition changes the length of $\widetilde{\mathbf{b}}$ to ℓ'. Now each bid in $\widetilde{\mathbf{b}}$ is confirmed with probability $\frac{k}{\max\{T,\ell'\}}$.

We partition the players in the coalition into the following groups:

- Those whose true values are less than r and bid less than r. Their expected utility does not change.
- Those whose true values are less than r and bid higher than or equal to r. Their expected utility does not increase.
- Those whose true values are at least r and bid less than r. Their expected utility does not increase.
- Those whose true values are at least r and bid at least r. For each of these users, its expected utility increases by at most

$$(v-r)\frac{k}{\max\{T,\ell'\}} - (v-r)\frac{k}{\max\{T,\ell\}}. \tag{15}$$

Note that for $\ell' \geq \ell$, then (15) ≤ 0. Therefore, we only need to consider the case where $\ell' < \ell$. If $\ell \leq T$, then (15) is 0. If $\ell > T$, then (15) is upper bounded by

$$\begin{aligned}(15) &\leq (v-r)\left[\frac{k}{\ell'} - \frac{k}{\ell}\right] \\ &\leq (v-r)\left[\frac{k}{\ell-c} - \frac{k}{\ell}\right] \leq (v-r)\frac{ck}{\ell(\ell-c)} \\ &\leq M \cdot \frac{ck}{T(T-c)}.\end{aligned}$$

By the choice of T, we have that $T(T-c) \geq \frac{1}{2}T^2$. Thus,

$$(15) \leq M \cdot \frac{ck}{T(T-c)} \leq \frac{2Mck}{T^2} \leq \frac{\epsilon}{2c}.$$

This implies that each user's utility can increase by at most $\frac{\epsilon}{2c}$. Meanwhile, for each user in the coalition, it can increase the miner's revenue by no more than $\frac{\epsilon}{2c}$ via bidding untruthfully. Since there are at most c users in the coalition, the coalition can gain at most ϵ more utility in total, no matter how they deviate.

□

References

[ACH11] Gilad Asharov, Ran Canetti, and Carmit Hazay. Towards a game theoretic view of secure computation. In *Eurocrypt*, 2011.

[ADGH06] Ittai Abraham, Danny Dolev, Rica Gonen, and Joseph Halpern. Distributed computing meets game theory: Robust mechanisms for rational secret sharing and multiparty computation. In *PODC*, 2006.

[AL11] Gilad Asharov and Yehuda Lindell. Utility dependence in correct and fair rational secret sharing. *Journal of Cryptology*, 24(1), 2011.

[BCD+] Vitalik Buterin, Eric Conner, Rick Dudley, Matthew Slipper, and Ian Norden. Ethereum improvement proposal 1559: Fee market change for eth 1.0 chain. https://github.com/ethereum/EIPs/blob/master/EIPS/eip-1559.md.

[BEOS19] Soumya Basu, David A. Easley, Maureen O'Hara, and Emin Gün Sirer. Towards a functional fee market for cryptocurrencies. *CoRR*, abs/1901.06830, 2019.

[Can00] Ran Canetti. Security and composition of multiparty cryptographic protocols. *Journal of Cryptology*, 2000.

[CCWS21] Kai-Min Chung, T-H. Hubert Chan, Ting Wen, and Elaine Shi. Game-theoretic fairness meets multi-party protocols: The case of leader election. In *CRYPTO*. Springer-Verlag, 2021.

[CGL+18] Kai-Min Chung, Yue Guo, Wei-Kai Lin, Rafael Pass, and Elaine Shi. Game theoretic notions of fairness in multi-party coin toss. In *TCC*, volume 11239, pages 563–596, 2018.

[CS21] Hao Chung and Elaine Shi. Foundations of transaction fee mechanism design. *arXiv preprint arXiv:2111.03151*, 2021.

[DR07] Yevgeniy Dodis and Tal Rabin. Cryptography and game theory. In *AGT*, 2007.

[EFW22] Meryem Essaidi, Matheus V. X. Ferreira, and S. Matthew Weinberg. Credible, strategyproof, optimal, and bounded expected-round single-item auctions for all distributions. In Mark Braverman, editor, *13th Innovations in Theoretical Computer Science Conference, ITCS 2022, January 31 - February 3, 2022, Berkeley, CA, USA*, volume 215 of *LIPIcs*, pages 66:1–66:19, 2022.

[FMPS21] Matheus V. X. Ferreira, Daniel J. Moroz, David C. Parkes, and Mitchell Stern. Dynamic posted-price mechanisms for the blockchain transaction-fee market. *CoRR*, abs/2103.14144, 2021.

[FW20] Matheus V. X. Ferreira and S. Matthew Weinberg. Credible, truthful, and two-round (optimal) auctions via cryptographic commitments. In Péter Biró, Jason D. Hartline, Michael Ostrovsky, and Ariel D. Procaccia, editors, *EC '20: The 21st ACM Conference on Economics and Computation, Virtual Event, Hungary, July 13-17, 2020*, pages 683–712. ACM, 2020.

[GH05] Andrew V. Goldberg and Jason D. Hartline. Collusion-resistant mechanisms for single-parameter agents. In *SODA 2005*, pages 620–629, 2005.

[GKM+13] Juan A. Garay, Jonathan Katz, Ueli Maurer, Björn Tackmann, and Vassilis Zikas. Rational protocol design: Cryptography against incentive-driven adversaries. In *FOCS*, 2013.

[GKTZ15] Juan Garay, Jonathan Katz, Björn Tackmann, and Vassilis Zikas. How fair is your protocol? a utility-based approach to protocol optimality. In *PODC*, 2015.

[GLR10] Ronen Gradwohl, Noam Livne, and Alon Rosen. Sequential rationality in cryptographic protocols. In *FOCS*, 2010.

[GTZ15] Juan A. Garay, Björn Tackmann, and Vassilis Zikas. Fair distributed computation of reactive functions. In *DISC*, volume 9363, pages 497–512, 2015.

[Har] Jason Hartline. Lectures on optimal mechanism design. http://users.eecs.northwestern.edu/~hartline/omd.pdf.

[HT04] Joseph Halpern and Vanessa Teague. Rational secret sharing and multiparty computation. In *STOC*, 2004.

[IML05] Sergei Izmalkov, Silvio Micali, and Matt Lepinski. Rational secure computation and ideal mechanism design. In *FOCS*, 2005.

[Kat08] Jonathan Katz. Bridging game theory and cryptography: Recent results and future directions. In *TCC*, 2008.

[KMSW22] Ilan Komargodski, Shinichiro Matsuo, Elaine Shi, and Ke Wu. log*-round game-theoretically-fair leader election. In *CRYPTO*, 2022.

[KN08] Gillat Kol and Moni Naor. Cryptography and game theory: Designing protocols for exchanging information. In *TCC*, 2008.

[LSZ19] Ron Lavi, Or Sattath, and Aviv Zohar. Redesigning bitcoin's fee market. In *The World Wide Web Conference, WWW 2019*, pages 2950–2956, 2019.

[Mye81] Roger B. Myerson. Optimal auction design. *Math. Oper. Res.*, 6(1), 1981.

[NRTV07] Noam Nisan, Tim Roughgarden, Eva Tardos, and Vijay V. Vazirani. *Algorithmic Game Theory*. Cambridge University Press, USA, 2007.

[OPRV09] Shien Jin Ong, David C. Parkes, Alon Rosen, and Salil P. Vadhan. Fairness with an honest minority and a rational majority. In *TCC*, 2009.

[Pas04] Rafael Pass. Bounded-concurrent secure multi-party computation with a dishonest majority. In *Proceedings of the thirty-sixth annual ACM symposium on Theory of computing*, pages 232–241, 2004.

[PS17] Rafael Pass and Elaine Shi. Fruitchains: A fair blockchain. In *PODC*, 2017.

[Rou20] Tim Roughgarden. Transaction fee mechanism design for the Ethereum blockchain: An economic analysis of EIP-1559. Manuscript, https://timroughgarden.org/papers/eip1559.pdf, 2020.

[Rou21] Tim Roughgarden. Transaction fee mechanism design. In *EC*, 2021.

[WAS22] Ke Wu, Gilad Asharov, and Elaine Shi. A complete characterization of game-theoretically fair, multi-party coin toss. In *Eurocrypt*, 2022.

[Yao] Andrew Chi-Chih Yao. An Incentive Analysis of Some Bitcoin Fee Designs (Invited Talk). In *ICALP 2020*.

A Full Proof of Theorem 3.6

We now prove Theorem 3.6 of Section 3.2, i.e., the propotional auction in the plain model satisfies UIC, MIC, and $\frac{5}{4}c\epsilon$-SCP against any miner-user coalition with an arbitrary $c \geq$ number of users.

Proof of Theorem 3.6. We prove the three properties individually.

UIC. Because the confirmation and the payment of each bid are independent of other bids, injecting fake bids does not help to increase any user's utility. Next, suppose user i's true value is v_i. If user i bids b_i, its expected utility is

$$\begin{cases} \left(v_i - \frac{b_i}{2}\right)\frac{b_i}{r}, & \text{if } b_i < r, \\ v_i - \frac{r}{2}, & \text{if } b_i \geq r. \end{cases}$$

By direct calculation, the expected utility is maximized when $b_i = v_i$. Thus, proportional auction is strict UIC.

MIC. Since the block size is infinite, the miner's best strategy is to include all bids to maximize its revenue. Notice that the confirmation of each bid and the miner revenue of each bid are independent of other bids. Thus, injecting fake bids does not change the miner revenue from "other bids." Moreover, for each confirmed bid, the miner revenue is upper bounded by the payment of that bid. Thus, the increment of the miner revenue never exceeds the cost of the injected fake bids. Thus, the miner revenue cannot increase by injecting fake bids, so the mechanism is strict MIC.

$\frac{5}{4}c\epsilon$-SCP. As we have shown in the argument for strict UIC and strict MIC, injecting fake bids does not change the colluding miner's revenue. Because the confirmation and the payment of each bid are independent of other bids, injecting fake bids does not help to increase any user's utility. Thus, in the rest of the proof, we assume the only deviation of the coalition is to change the bids from colluding users' true values to other values. Let user i be a colluding user. We will show that the joint utility increases at most by $\frac{5}{4}\epsilon$ if user i changes its bid from its true value to other values, no matter what other bids are. Because there are at most c colluding users, the mechanism is $\frac{5}{4}c\epsilon$-SCP for all c.

Let user i be a colluding user with true value v_i, and let b_i be user i's bid. We now proceed to analyze the utility of coalition based on how users in the coalition bid untruthfully.

1. Underbidding. Suppose $b_i < v_i$. Notice that the miner can get the payment from b_i only when b_i is confirmed, and the miner is paid $\frac{\sqrt{2r\epsilon}}{2}$ if $b_i \geq \sqrt{2r\epsilon}$. When user i underbids, the miner's revenue can not increase. Because the mechanism is strict UIC, underbidding does not increase user i's utility either. Thus, the joint utility does not increase if $b_i < v_i$.

2. Overbidding. Suppose $b_i > v_i$. We first consider the following cases based on whether the true value v_i is less than r.

- **If $v_i \geq \sqrt{2r\epsilon}$.** If $v_i \geq r$, bidding truthfully already guarantees user i's bid to be confirmed, and the miner is paid $\sqrt{\frac{r\epsilon}{2}}$. Thus, when $v_i \geq r$, overbidding does not increase the joint utility.

In the following, we assume $v_i < r$. Let $\Delta = \min(b_i - v_i, r - v_i) > 0$. If user i bids truthfully, its bid is confirmed with the probability $\frac{v_i}{r}$, so its expected utility is

$$\left(v_i - \frac{v_i}{2}\right)\frac{v_i}{r}.$$

Next, suppose user i bids $b_i > v_i$. Then, b_i is confirmed with the probability $\frac{v_i+\Delta}{r}$, and the payment is $\frac{v_i+\Delta}{2}$ if b_i is confirmed. Thus, user i's expected utility is

$$\left(v_i - \frac{v_i+\Delta}{2}\right)\frac{v_i+\Delta}{r}.$$

Hence, compared to bidding truthfully, user i's expected utility decreases by

$$\left(v_i - \frac{v_i}{2}\right)\frac{v_i}{r} - \left(v_i - \frac{v_i+\Delta}{2}\right)\frac{v_i+\Delta}{r} = \frac{\Delta^2}{2r} > 0.$$

On the other hand, if user i bids truthfully, the miner's expected revenue is $\frac{v_i}{r}\sqrt{\frac{r\epsilon}{2}}$. If user i bids $b_i > v_i$, the miner's expected revenue is $\frac{v_i+\Delta}{r}\sqrt{\frac{r\epsilon}{2}}$. Thus, compared to bidding truthfully, the miner's expected utility increases by

$$\frac{v_i+\Delta}{r}\sqrt{\frac{r\epsilon}{2}} - \frac{v_i}{r}\sqrt{\frac{r\epsilon}{2}} = \frac{\Delta}{r}\sqrt{\frac{r\epsilon}{2}}.$$

Combine the argument above, the joint utility increases by

$$\frac{\Delta}{r}\sqrt{\frac{r\epsilon}{2}} - \frac{\Delta^2}{2r}. \tag{16}$$

The maximum of Eq.(16) is $\frac{\epsilon}{4}$, so overbidding b_i can only increase the joint utility by $\frac{\epsilon}{4}$.

- **If $v_i < \sqrt{2r\epsilon}$.** Because the mechanism is strict-UIC, overbidding does not increase user i's utility. If $b_i < \sqrt{2r\epsilon}$, the miner revenue is still zero. Thus, we assume $b_i \geq \sqrt{2r\epsilon}$. From the argument in the previous case, we know that compared to bidding truthfully, user i's expected utility decreases by $\frac{\Delta^2}{2r}$. However, if user i bids truthfully, the miner's revenue is zero. If user i bids $b_i > v_i$, the miner's expected revenue is $\frac{v_i+\Delta}{r}\sqrt{\frac{r\epsilon}{2}}$. Thus, compared to bidding truthfully, the miner's expected revenue increases by $\frac{v_i+\Delta}{r}\sqrt{\frac{r\epsilon}{2}}$. Consequently, the joint utility increases by

$$\frac{v_i}{r}\sqrt{\frac{r\epsilon}{2}} + \frac{\Delta}{r}\sqrt{\frac{r\epsilon}{2}} - \frac{\Delta^2}{2r}. \tag{17}$$

Because the maximum of Eq.(16) is $\frac{\epsilon}{4}$, the maximum of Eq.(17) when $v_i < \sqrt{2r\epsilon}$ is at most $\frac{5\epsilon}{4}$. Thus, overbidding b_i can only increase the joint utility by $\frac{5\epsilon}{4}$.

To sum up, among all cases, overbidding b_i can only increase the joint utility by at most $\frac{5}{4}\epsilon$. The theorem thus follows.

Proportional auction for the MPC-assisted model. In the MPC-assisted model, we want to ensure incentive compatibility for any miner-user coalition with at most ρ fraction of mining power and at most c users — recall that the total miner revenue is divided among the miners proportional to their mining power. By contrst, in the plain model, effectively ρ is always equal to 1 since we always focus on the miner of the present block. Therefore, to make the proportional auction work in the MPC-assisted model, we make a small modification to the scheme and proof. For the scheme, the only modification is that we now allow the miner revenue to scale up w.r.t. $\frac{1}{\rho}$ (up to the total user payment), such that the miner revenue can be larger if we only want to be resilient against coalitions with little mining power — see the formal description below.

Proportional Auction for the MPC-assisted Model

Parameters: the approximate factor ϵ, upper bound ρ on the colluding miners' mining power and the reserved price r such that $r \geq 2\epsilon$.

Input: a bid vector $\mathbf{b} = (b_1, \ldots, b_N)$.

Mechanism:

- *Allocation rule.* For each bid b, if $b < r$, it is confirmed with the probability b/r; otherwise, if $b \geq r$, it is confirmed with probability 1.
- *Payment rule.* For each confirmed bid b, if $b < r$, it pays $b/2$; otherwise, if $b \geq r$, it pays $r/2$.
- *Miner revenue rule.* For each confirmed bid b, let p be the payment of b, and the miner is paid $\min\left(p, \frac{\sqrt{2r\epsilon}}{2\rho}\right)$.[a]

[a] The minimum guarantees that the miner revenue never exceed the payment.

It is not hard to see that our proof of Theorem 3.6 can be easily modified to work for the MPC-assisted model. The only difference is that when the colluding user's true value v_i is smaller than the threshold $\frac{\sqrt{2r\epsilon}}{\rho}$, overbidding to $v_i + \Delta < \frac{\sqrt{2r\epsilon}}{\rho}$ also increases the joint utility. There are two cases:

- When a user with true value v_i overbids to $v_i + \Delta < \frac{\sqrt{2r\epsilon}}{\rho}$, the coalition of the miner and this colluding user can gain at most ϵ more utility if $\Delta = \sqrt{2r\epsilon}$.
- When a user with true value v_i overbids to $v_i + \Delta \geq \frac{\sqrt{2r\epsilon}}{\rho}$, the coalition of the miner and this colluding user can gain at most $\frac{9}{4}\epsilon$ more utility when $\Delta = \sqrt{2r\epsilon}$ and v_i is arbitrarily close to $\frac{\sqrt{2r\epsilon}}{\rho}$.

B Deferred Proofs of Section 5

B.1 Strict Incentive Compatibility in MPC-Assisted Model: Necessity of Zero Miner Revenue

Chung and Shi [CS21] showed that the posted-price auction with burning gives strict incentive compatibility in the plain model, assuming infinite block size. One may hope that with the Bayesian notion of incentive compatibility, we can achieve larger miner revenue. Unfortunately, in this section we show that zero-miner revenue is the best we can hope for strict incentive compatibility, even in the Bayesian setting.

Prelimary: Myerson's lemma for the Bayesian setting. We first review the Bayesian version of Myerson's lemma. Recall that $\mathbf{b}_{-i}$ denotes all but user i's bid, and $(\mathbf{b}_{-i}, b_i) = \mathbf{b}$. We also let $\mathcal{D}_{-i}$ to denote $\mathcal{D}_1 \times \cdots \times \mathcal{D}_{i-1} \times \mathcal{D}_{i+1} \times \cdots \times \mathcal{D}_n$, which denotes the distribution of other users' true values.

Lemma B.1 (Myerson's Lemma [Mye81])**.** *Let $\mathcal{D} = \mathcal{D}_1 \times \cdots \times \mathcal{D}_n$ be the joint distribution of users' true values. Let $(\mathbf{x}, \mathbf{p}, \mu)$ be a single-parameter TFM that is Bayesian UIC. Then, it must be that*

1. *The allocation rule* $\mathbf{x}$ *is monotonically non-decreasing. Formally, for any user* i*, and any* $b_i' > b_i$*, it must be that* $\mathbf{E}_{\mathbf{b}_{-i}\sim\mathcal{D}_{-i}}[x_i(\mathbf{b}_{-i}, b_i')] \geq \mathbf{E}_{\mathbf{b}_{-i}\sim\mathcal{D}_{-i}}[x_i(\mathbf{b}_{-i}, b_i)]$.

2. *The payment rule* $\mathbf{p}$ *is defined as follows. For any user* i*, and bid* b_i *from user* i*, it must be*

$$\mathbf{E}_{\mathbf{b}_{-i}\sim\mathcal{D}_{-i}}[p_i(\mathbf{b}_{-i}, b_i)] = \mathbf{E}_{\mathbf{b}_{-i}\sim\mathcal{D}_{-i}}\left[b_i \cdot x_i(\mathbf{b}_{-i}, b_i) - \int_0^{b_i} x_i(\mathbf{b}_{-i}, t)dt\right]. \tag{18}$$

Lemma B.2 (Technical lemma implied by the proof of Myerson's Lemma [Mye81, Har])**.** *Let* $f(z)$ *be a non-decreasing function. Suppose that* $z \cdot (f(z') - f(z)) \leq g(z') - g(z) \leq z' \cdot (f(z') - f(z))$ *for any* $z' \geq z \geq 0$*, and moreover,* $g(0) = 0$*. Then, it must be that*

$$g(z) = z \cdot f(z) - \int_0^z f(t)dt.$$

Necessity of zero miner revenue. Henceforth we use the following simplified notation.

$$\overline{x_i}(\cdot) = \mathop{\mathbf{E}}_{\mathbf{b}_{-i}\sim\mathcal{D}_{-i}}[\mathbf{x}(\mathbf{b}_{-i}, \cdot)], \quad \overline{p_i}(\cdot) = \mathop{\mathbf{E}}_{\mathbf{b}_{-i}\sim\mathcal{D}_{-i}}[\mathbf{p}(\mathbf{b}_{-i}, \cdot)], \quad \overline{\mu_i}(\cdot) = \mathop{\mathbf{E}}_{\mathbf{b}_{-i\sim\mathcal{D}_{-i}}}[\mu(\mathbf{b}_{-i}, \cdot)].$$

The following technical lemma was given in [CS21].

Lemma B.3 (Lemma 4.8 in [CS21])**.** *Let* $(\mathbf{x}, \mathbf{p}, \mu)$ *be any (possibly randomized) TFM in the Bayesian setting. If* $(\mathbf{x}, \mathbf{p}, \mu)$ *is Bayesian SCP against a* $(\rho, 1)$*-sized coalition, then for any bid vector* $\mathbf{b}$*, user* i*, and* r, r' *such that* $r < r'$*, it must be*

$$r \cdot \left(\overline{x_i}(r') - \overline{x_i}(r)\right) \leq \pi(r') - \pi(r) \leq r' \cdot \left(\overline{x_i}(r') - \overline{x_i}(r)\right),$$

where $\pi(r) := \overline{p_i}(r) - \rho\overline{\mu_i}(r)$*.*

The following result shows that if we allow the strategic players to inject fake bids, then the miner's revenue can only be 0 if the mechanism is UIC, MIC, and 1-SCP. Actually, in the proof of the lower bound, we only need the deviation where the miners in the coalition injecting fake bids, and colluding users only bid untruthfully.

We first show that if a TFM is Bayesian UIC and Bayesian SCP against $(\rho, 1)$-sized coalition, then the miner revenue must be independent from each user's bid. Without loss of generality, we assume that 0 is the minimum value in the support of $\mathcal{D}_i$ for $i \in [n]$.

Lemma B.4. *Let* $\mathcal{D} = \mathcal{D}_1 \times \cdots \times \mathcal{D}_n$ *be the joint distribution of users' true values. Let* $(\mathbf{x}, \mathbf{p}, \mu)$ *be any (possibly randomized) TFM in the MPC model. If* $(\mathbf{x}, \mathbf{p}, \mu)$ *is Bayesian UIC and Bayesian SCP against a* $(\rho, 1)$*-sized miner-user coalition, then for any user* i*, any bid* b*, it must be*

$$\overline{\mu_i}(b) = \overline{\mu_i}(0). \tag{19}$$

In other words, the miner's revenue is a constant that is independent of user i*'s bid* b *when other bids* $\mathbf{b}_{-i}$ *are drawn from the distribution* $\mathcal{D}_{-i}$*.*

Proof. Define $\widetilde{\pi}(r)$ as

$$\widetilde{\pi}(r) = \overline{p_i}(r) - \rho\overline{\mu_i}(r) - (\overline{p_i}(0) - \rho\overline{\mu_i}(0)).$$

By Lemma B.3, and the fact that definition of $\widetilde{\pi}(r)$ and $\pi(r)$ differs by only a fixed constant, it must be that

$$r \cdot \left(\overline{x_i}(r') - \overline{x_i}(r)\right) \leq \widetilde{\pi}(r') - \widetilde{\pi}(r) \leq r' \cdot \left(\overline{x_i}(r') - \overline{x_i}(r)\right). \tag{20}$$

Therefore, we have the following two inequalities:

$$r \cdot [\overline{x_i}(r') - \overline{x_i}(r)] \leq \widetilde{\pi}(r') - \widetilde{\pi}(r)$$
$$r \cdot [\overline{x_i}(r') - \overline{x_i}(r)] \geq \widetilde{\pi}(r') - \widetilde{\pi}(r)$$

Now, observe that the above expression strictly agrees with the "payment sandwich" in the proof of Myerson's Lemma [Mye81, Har]. Furthermore, we have that $\widetilde{\pi}(0) = 0$ by definition; and $\mathbf{x}$ must be monotone because the TFM is UIC and satisfies Myerson's Lemma. Due to Lemma B.2, it must be that $\widetilde{\pi}(\cdot)$ obeys the unique payment rule specified by Myerson's Lemma; that is,

$$\widetilde{\pi}(r) = \left[b_i \cdot \overline{x_i}(b_i) - \int_0^{b_i} \overline{x_i}(t)dt\right].$$

On the other hand, since the TFM is UIC, its payment rule itself must also satisfy the same expression (Eq.(18)), that is,

$$\overline{p_i}(b_i) = b_i \cdot \overline{x_i}(b_i) - \int_0^{b_i} \overline{x_i}(t)dt.$$

We therefore have that

$$\widetilde{\pi}(r) = \overline{p_i}(b_i).$$

In other words, $\rho\overline{\mu_i}(r) = \rho\overline{\mu_i}(0) - \overline{p_i}(0)$. Because $\overline{p_i}(0) = 0$, we conclude $\overline{\mu_i}(r) = \overline{\mu_i}(0)$. □

Note that the result in Lemma B.4 holds even if users do not inject any fake bids. This provides a stronger impossibility result.

Now we show that, if in addition the mechanism $(\mathbf{x}, \mathbf{p}, \mu)$ is Bayesian MIC, then the total miner revenue can only be 0.

Theorem B.5. *Let $\{\mathcal{D}^{(n)}\}_n$ be a sequence of distributions where $\mathcal{D}^{(n)} = \mathcal{D}_1 \times \cdots \times \mathcal{D}_n$ is the joint distribution of n users' true values, where user i's true value is drawn from $\mathcal{D}_i$ independently. Let $(\mathbf{x}, \mathbf{p}, \mu)$ be any (possibly randomized) TFM in the MPC model. If $(\mathbf{x}, \mathbf{p}, \mu)$ is Bayesian UIC, Bayesian MIC against ρ-sized miner coalition and Bayesian SCP against $(\rho, 1)$-sized miner-user coalition, then*

$$\mathop{\mathbf{E}}_{\mathbf{b}\sim\mathcal{D}^{(n)}}[\mu(\mathbf{b})] = 0.$$

Proof. For any $n \geq 2$, we have the following claim:

Lemma B.6. *If $(\mathbf{x}, \mathbf{p}, \mu)$ is Bayesian MIC against $(\rho, 1)$-sized miner-user coalition, then* $\mathop{\mathbf{E}}_{\mathbf{b}\sim\mathcal{D}^{(n)}}[\mu(\mathbf{b})] \leq \mathop{\mathbf{E}}_{\mathbf{b}'\sim\mathcal{D}^{(n-1)}}[\mu(\mathbf{b}')]$.

For now assume Lemma B.6 holds and we explain why Theorem B.5 follows from it. The proof of Lemma B.6 appears right afterwards. By induction on n, we have that

$$\mathop{\mathbf{E}}_{\mathbf{b}\sim\mathcal{D}^{(n)}}[\mu(\mathbf{b})] \leq \mathop{\mathbf{E}}_{b\sim\mathcal{D}_1}[\mu(b)].$$

By Lemma B.4, for any $b \in \mathrm{Supp}(\mathcal{D}_1)$, it should be that $\mu(b) = \mu(0)$. Therefore,

$$\mathop{\mathbf{E}}_{b\sim\mathcal{D}_1}[\mu(b)] \le \mu(0) = 0,$$

where the last equality comes from the requirement that the miner's revenue cannot exceeds the payment of the single identity, who will pay at most what it bids. Theorem B.5 thus follows. □

Proof of Lemma B.6 Since $(\mathbf{x}, \mathbf{p}, \mu)$ is Bayesian-SCP against $(\rho, 1)$-sized coalition, it must be that for any user i,

$$\mathop{\mathbf{E}}_{\mathbf{b}\sim\mathcal{D}^{(n-1)}}[\rho\mu(\mathbf{b}, 0)] \le \mathop{\mathbf{E}}_{\mathbf{b}\sim\mathcal{D}^{(n-1)}}[\rho\mu(\mathbf{b})]. \tag{21}$$

Otherwise, the miners can collude with user i, ask user i to bid, and inject 0 and increase the coalition's miner revenue while it does not need to pay anything for injecting the 0-bid. This violates the MIC condition.

By the law of total expectation, we have that

$$\begin{aligned}
\mathop{\mathbf{E}}_{\mathbf{b}\sim\mathcal{D}^{(n)}}[\mu(\mathbf{b})] &= \int_0^{+\infty} \mathop{\mathbf{E}}_{\mathbf{b}'\sim\mathcal{D}^{(n-1)}}[\mu(\mathbf{b}', r)]f(r)dr \\
&= \int_0^{+\infty} \mathop{\mathbf{E}}_{\mathbf{b}'\sim\mathcal{D}^{(n-1)}}[\mu(\mathbf{b}', 0)]f(r)dr && \text{By Lemma B.4} \\
&= \mathop{\mathbf{E}}_{\mathbf{b}'\sim\mathcal{D}^{(n-1)}}[\mu(\mathbf{b}', 0)] \le \mathop{\mathbf{E}}_{\mathbf{b}'\sim\mathcal{D}^{(n-1)}}[\mu(\mathbf{b}')] && \text{By (21)}
\end{aligned}$$

Lemma B.6 thus follows.

B.2 Proof of Lemma 5.2

Lemma B.7 (Restatement of Lemma 5.2)**.** *Let $(\mathbf{x}, \mathbf{p}, \mu)$ be any (possibly random) mechanism that is Bayesian UIC and Bayesian SCP against $(\rho, 2)$-sized coalition for some $\rho \in (0, 1]$. Suppose each user's true value is drawn i.i.d. from a distribution $\mathcal{D}$. Then for any bid b_j and b'_j, any value v, it must be that for any ℓ*

$$\mathop{\mathbf{E}}_{\mathbf{b}\sim\mathcal{D}^{(\ell)}}[\mathsf{util}^i(v, b_j, \mathbf{b})] = \mathop{\mathbf{E}}_{\mathbf{b}\sim\mathcal{D}^{(\ell)}}[\mathsf{util}^i(v, b'_j, \mathbf{b})].$$

Proof. By Bayesian Myerson's Lemma, when bidding its true value v, user i's utility is

$$\mathop{\mathbf{E}}_{\mathbf{b}\sim\mathcal{D}^{(\ell)}}[\mathsf{util}^i(v, b_j, \mathbf{b})] = \mathop{\mathbf{E}}_{\mathbf{b}\sim\mathcal{D}^{(\ell)}} \int_0^v x_i(t, b_j, \mathbf{b})dt.$$

Now the expected gain of user i when user j changes its bid from b_j to b'_j (this "gain" might be negative) is

$$\text{i-gain}(b_j, b'_j) = \mathop{\mathbf{E}}_{\mathbf{b}\sim\mathcal{D}^{(\ell)}}\left[\int_0^v x_i(t, b'_j, \mathbf{b})dt\right] - \mathop{\mathbf{E}}_{\mathbf{b}\sim\mathcal{D}^{(\ell)}}\left[\int_0^v x_i(t, b_j, \mathbf{b})dt\right]. \tag{22}$$

Note that in Appendix B.1, we will show that the miner revenue have to be 0. Therefore, Bayesian *SCP* against $(\rho, 2)$-sized coalition implies that the two users i and j cannot gain benefit no matter how they deviate from the protocol. Henceforth, he utility gain of user i must be bounded by user j's loss:

$$\begin{aligned}
\text{i-gain}(b_j, b'_j) &\le \text{j-loss}(b_j, b'_j) \\
&\le (b'_j - b_j) \mathop{\mathbf{E}}_{\mathbf{b}\sim\mathcal{D}^{(\ell)}}\left[x_j(t, b'_j, \mathbf{b}) - x_j(t, b_j, \mathbf{b})\right]
\end{aligned} \tag{23}$$

In the above inequalities, j-loss(b_j, b'_j) intuitively represents the loss for user j would incur by non-truthfully bidding b'_j when its actual valuation is b_j. This quantity is always positive and is given by (23).

Without loss of generality we assume that $b'_j \geq b_j$. Note that (22) implies that i-gain$(b_j, b'_j) =$ i-gain(b_j, b''_j) + i-gain(b''_j, b'_j) for any b''_j. If we divide the interval between $[b_j, b'_j]$ into L equally sized segments $b_j^{(0)}, \ldots, b_j^{(L)}$, then the total gain for user i can be bounded by

$$\begin{aligned}
\text{i-gain}(b_j, b'_j) &= \sum_{l=0}^{L} \text{i-gain}(b_j^{(l)}, b_j^{(l+1)}) \\
&\leq \sum_{l=0}^{L} (b_j^{(l+1)} - b_j^{(l)}) \mathop{\mathbf{E}}_{\mathbf{b}\sim\mathcal{D}^{(\ell)}} \left[x_j(t, b_j^{(l+1)}, \mathbf{b}) - x_j(t, b_j^{(l)}, \mathbf{b}) \right] \\
&= \frac{b'_j - b_j}{L} \sum_{l=0}^{L} \mathop{\mathbf{E}}_{\mathbf{b}\sim\mathcal{D}^{(\ell)}} \left[x_j(t, b_j^{(l+1)}, \mathbf{b}) - x_j(t, b_j^{(l)}, \mathbf{b}) \right].
\end{aligned}$$

This holds for any L. Taking limit for L going to infinity, we have that

$$\text{i-gain}(b_j, b'_j) \leq 0.$$

Since i-gain$(b_j, b'_j) = -(\text{i-gain}(b'_j, b_j))$, we have that i-gain$(b_j, b'_j) = 0$, for arbitrary b_j and b'_j. The lemma thus follows. □

B.3 Full Proof of Lemma 5.3

In this section, we provide a full proof of Lemma 5.3 assuming the symmetry assumption in Section 2.1.

By Lemma 5.2, for any i, j, v_i, b_j, ℓ, we have

$$\mathop{\mathbf{E}}_{\mathbf{b}_{-i,j}\sim\mathcal{D}^{\ell}}[\mathsf{util}^i(v_i, b_j, \mathbf{b}_{-i,j})] = \mathop{\mathbf{E}}_{\mathbf{b}_{-i,j}\sim\mathcal{D}^{\ell}}[\mathsf{util}^i(v_i, 0_j, \mathbf{b}_{-i,j})].$$

Therefore, it suffices to prove that for any i, j, v_i, ℓ, $\mathop{\mathbf{E}}_{\mathbf{b}_{-i,j}\sim\mathcal{D}^{\ell}}[\mathsf{util}^i(v_i, 0_j, \mathbf{b}_{-i,j})] \leq \mathop{\mathbf{E}}_{\mathbf{b}_{-i,j}\sim\mathcal{D}^{\ell}}[\mathsf{util}^i(v_i, \mathbf{b}_{-i,j})]$.

Suppose for the sake of contradiction, the above statement is not true, that is, there exist some i, j, v_i, ℓ, such that $\mathop{\mathbf{E}}_{\mathbf{b}_{-i,j}\sim\mathcal{D}^{\ell}}[\mathsf{util}^i(v_i, 0_j, \mathbf{b}_{-i,j})] > \mathop{\mathbf{E}}_{\mathbf{b}_{-i,j}\sim\mathcal{D}^{\ell}}[\mathsf{util}^i(v_i, \mathbf{b}_{-i,j})]$.

Consider an arbitrary fake identity m registered by the miner. There are two possible cases.

Good identity m: $\mathop{\mathbf{E}}_{\mathbf{b}_{-i,j}\sim\mathcal{D}^{\ell}}[\mathsf{util}^i(v_i, 0_m, \mathbf{b}_{-i,j})] > \mathop{\mathbf{E}}_{\mathbf{b}_{-i,j}\sim\mathcal{D}^{\ell}}[\mathsf{util}^i(v_i, \mathbf{b}_{-i,j})]$.

Bad identity m: $\mathop{\mathbf{E}}_{\mathbf{b}_{-i,j}\sim\mathcal{D}^{\ell}}[\mathsf{util}^i(v_i, 0_m, \mathbf{b}_{-i,j})] \leq \mathop{\mathbf{E}}_{\mathbf{b}_{-i,j}\sim\mathcal{D}^{\ell}}[\mathsf{util}^i(v_i, \mathbf{b}_{-i,j})] < \mathop{\mathbf{E}}_{\mathbf{b}_{-i,j}\sim\mathcal{D}^{\ell}}[\mathsf{util}^i(v_i, 0_j, \mathbf{b}_{-i,j})]$.

Now, suppose the miner samples a fake identity m. Over the choice of m, either Pr(Good identity m) $\geq \frac{1}{2}$ or Pr(Bad identity m) $\geq \frac{1}{2}$. If Pr(Good identity m) $\geq \frac{1}{2}$, then suppose that the world consists of $\ell + 1$ users not including j, and the miner forms a coalition with user i whose true value is v_i. The miner can sample a random identity m, and if it is a good identity, the miner can inject a fake bid 0_m, and the coalition can strictly gain. This violates SCP when $c = 1$.

Henceforth, we focus on the case when $\Pr(\text{Bad identity } m) \geq \frac{1}{2}$. In this case, there are two possibilities, either with probability at least $1/4$ over the choice of the identity m, for all v_i',

$$\mathop{\mathbf{E}}_{\mathbf{b}_{-i,j}\sim\mathcal{D}^\ell}[\mathsf{util}^i(v_i', 0_m, \mathbf{b}_{-i,j})] \leq \mathop{\mathbf{E}}_{\mathbf{b}_{-i,j}\sim\mathcal{D}^\ell}[\mathsf{util}^i(v_i', 0_j, \mathbf{b}_{-i,j})], \tag{24}$$

or with probability at least $1/4$ over the choice of m, there exists some v_i' such that $\mathop{\mathbf{E}}_{\mathbf{b}_{-i,j}\sim\mathcal{D}^\ell}[\mathsf{util}^i(v_i', 0_m, \mathbf{b}_{-i,j})] > \mathop{\mathbf{E}}_{\mathbf{b}_{-i,j}\sim\mathcal{D}^\ell}[\mathsf{util}^i(v_i', 0_j, \mathbf{b}_{-i,j})]$. If it is the latter case, then, consider a scenario where the miner colludes with user i whose true value is v_i', and user j whose true value is 0, and the rest of the world is a random variable $\mathbf{b}_{-i,j}$. Now, the miner can sample a random fake identity m, and see if dropping 0_j and injecting 0_m can help its friend i. If so, it performs this strategic behavior. This strategy can strictly help the coalition which violates SCP for $c = 2$.

It suffices to rule out the former case, that is, with probability at least $1/4$ over the choice of the identity m, for all v_i', Equation (24) is satisfied. Recall also, for v_i specifically, we have strict inequality, that is, $\mathop{\mathbf{E}}_{\mathbf{b}_{-i,j}\sim\mathcal{D}^\ell}[\mathsf{util}^i(v_i, 0_m, \mathbf{b}_{-i,j})] < \mathop{\mathbf{E}}_{\mathbf{b}_{-i,j}\sim\mathcal{D}^\ell}[\mathsf{util}^i(v_i, 0_j, \mathbf{b}_{-i,j})]$. Thus, $\mathop{\mathbf{E}}_{\mathbf{b}_{-j}\sim\mathcal{D}^{\ell+1}}[\mathsf{util}^i(0_m, \mathbf{b}_{-j})] < \mathop{\mathbf{E}}_{\mathbf{b}_{-j}\sim\mathcal{D}^{\ell+1}}[\mathsf{util}^i(0_j, \mathbf{b}_{-j})]$.

For every bad identity m that additionally satisfies Equation (24), there must exist some $i' \neq i$ and $i \neq j$, and some $b_{i'} > 0$, such that

$$\mathop{\mathbf{E}}_{\mathbf{b}_{-j,i'}\sim\mathcal{D}^\ell}[\mathsf{util}^{i'}(0_m, b_{i'}, \mathbf{b}_{-j,i'})] > \mathop{\mathbf{E}}_{\mathbf{b}_{-j,i'}\sim\mathcal{D}^\ell}[\mathsf{util}^{i'}(0_j, b_{i'}, \mathbf{b}_{-j,i'})] \tag{25}$$

We can prove the above claim by contradiction. Suppose for the sake of contradiction that for all $i' \neq i$ and $i \neq j$, and for all $b_{i'}$, $\mathop{\mathbf{E}}_{\mathbf{b}_{j,i'}\sim\mathcal{D}^\ell}[\mathsf{util}^{i'}(0_m, b_{i'}, \mathbf{b}_{-j,i'})] \leq \mathop{\mathbf{E}}_{\mathbf{b}_{j,i'}\sim\mathcal{D}^\ell}[\mathsf{util}^{i'}(0_j, b_{i'}, \mathbf{b}_{-j,i'})]$. Therefore, it must be that for any $i' \neq i$ and $i \neq j$, $\mathop{\mathbf{E}}_{\mathbf{b}_{-j}\sim\mathcal{D}^{\ell+1}}[\mathsf{util}^{i'}(0_m, \mathbf{b}_{-j})] \leq \mathop{\mathbf{E}}_{\mathbf{b}_{-j}\sim\mathcal{D}^{\ell+1}}[\mathsf{util}^{i'}(0_j, \mathbf{b}_{-j})]$. Therefore, we have that

$$\mathop{\mathbf{E}}_{\mathbf{b}_{-j}\sim\mathcal{D}^{\ell+1}}[\mathsf{USW}(0_m, \mathbf{b}_{-j})] < \mathop{\mathbf{E}}_{\mathbf{b}_{-j}\sim\mathcal{D}^{\ell+1}}[\mathsf{USW}(0_j, \mathbf{b}_{-j})] \tag{26}$$

where $\mathsf{USW}(\mathbf{b})$ denotes the social welfare for all users (i.e., sum of all user utilities) when the bid vector is $\mathbf{b}$. However, by our symmetry assumption in Section 2.1, it must be that $\mathop{\mathbf{E}}_{\mathbf{b}_{-j}\sim\mathcal{D}^{\ell+1}}[\mathsf{USW}(0_m, \mathbf{b}_{-j})] = \mathop{\mathbf{E}}_{\mathbf{b}_{-j}\sim\mathcal{D}^{\ell+1}}[\mathsf{USW}(0_j, \mathbf{b}_{-j})]$, which contradicts Equation (26).

Let i' be a user such that Equation (25) happens with probability at least $1/4(\ell+2)$ over the choice of m — clearly, such a user must exist since we are assuming that with probability at least $1/4$ over the choice of m, m is a bad identity satisfying Equation (24). Now, imagine that the world consists of $\ell+2$ users including both i and j, and the miner forms a coalition with users i' and j. The miner samples a random fake identity m, and if the identity helps i' in the sense that Equation (25) holds, then the coalition replaces j's bid 0_j with 0_m. This strategy strictly increases the coalition's joint utility, and this violates SCP when $c = 2$.

C Multi-Party Computation Model Implementing $\mathcal{F}_{\text{TFM}}$

In this section, we will show how to instantiate the ideal functionality $\mathcal{F}_{\text{TFM}}$ in the real world with cryptography. Formally, we assume that there are n identities, each will commit to a bid it

wishes to submit. Moreover, there are m miners who interact with each other through pairwise private channels and the blockchain, which we can think of as a public broadcast channel. We assume that each of the n identities has access to the blockchain, and a private channel with each of the miners. All communication channels are authenticated, i.e., messages carry the senders identity. Moreover, the network is synchronous and the protocol proceeds in rounds. The protocol execution is parametrized with a security parameter λ. We assume that the coalition performs a *rushing* attack: In the r-th round, it waits for all honest players (those not in the coalition) to send messages in round r and decide what messages the identities or miners in the coalition send in round r. At the end, the protocol outputs the output of the mechanism. i.e., $(\mathbf{x}, \mathbf{p}, \mu)$, based on each identity's bid.

C.1 Building Blocks

We first introduce some building blocks used in the protocol.

C.1.1 Commitment Scheme

A commitment scheme $(\mathsf{C}, \mathsf{R}, \mathsf{V})$ consists of a pair of interacting Turing machines, the committer C, the receiver R, and a deterministic verifier V. We assume that the protocol has two phases, a commitment phase and an opening phase. The verifier, upon receiving a transcript Γ of the commitment protocol, outputs either a bit $b \in \{0,1\}$ to accept or $\perp$ to reject. We use $\langle \mathsf{C}^*(z), \mathsf{R}^*(z') \rangle$ to denote an execution between C^* on input $z, 1^\lambda$, and R^* on input $z', 1^\lambda$, where λ is the security parameter.

Perfect Binding. Perfect binding guarantees that the commitment phase will determine only one bit that can be successfully opened. Formally, let $(\Gamma_c, \Gamma_o) \in \{0,1\}^{\ell(\lambda)}$ be the transcripts of the commitment phase and the opening phase, respectively, where $\ell(\lambda)$ is a fixed polynomial function denoting the maximum length of the transcripts. Then for any $\lambda \in \mathbb{N}$, any transcripts $\Gamma_c, \Gamma_o, \Gamma_o'$, if $\mathsf{V}(1^\lambda, \Gamma_c, \Gamma_o) = b$ and $\mathsf{V}(1^\lambda, \Gamma_c, \Gamma_o') = b'$, where $b, b' \in \{0,1\}$, it must be that $b = b'$.

Computationally Hiding. Computationally hiding guarantees that at the end of the commitment phase, the receiver learns only a negligible amount of information about the input that the committer commits to. Formally, let $p_\lambda(v)$ denote the probability that R^* outputs 1 at the end of the commitment phase in an execution $\langle \mathsf{C}^*(1^\lambda, v), \mathsf{R}^*(1^\lambda) \rangle$, then for any non-uniform p.p.t. R^*, there exists a negligible function $\mathsf{negl}(\cdot)$ such that for every $\lambda \in \mathbb{N}$ and every $v_1, v_2 \in \{0,1\}^\lambda$, it holds that $|p_\lambda(v_1) - p_\lambda(v_2)| \leq \mathsf{negl}(\lambda)$.

C.1.2 Secret Sharing

A t-out-of-n Secret sharing consists of two algorithms, share and $\mathsf{reconstruct}$.

- share takes as an input a secret s, and outputs n shares $(s_1, \ldots, s_n)$ of the secret.
- $\mathsf{reconstruct}$ takes as input a set I, and the corresponding shares $\{s_i\}_{i \in I}$, and outputs the corresponding shares if $|I| \geq t$. Otherwise, the algorithm returns $\perp$.

A t-out-of-n secret sharing satisfies the following two properties:

- **Correctness:** For any secret s and any set $I \subseteq [n]$ such that $|I| \geq t$, it must be that

$$\Pr[\mathsf{reconstruct}(I, \{s_i\}_{i \in I}) = s : (s_1, \ldots, s_n) \leftarrow \mathsf{share}(s)].$$

- **Security:** For any two secret s and s', and for all set $T \subseteq [n]$ such that $|I| \leq t-1$, it must be that

$$\{\{s_i\}_{i\in I} : (s_1, \ldots, s_n) \leftarrow \mathsf{share}(s)\} \equiv_c \{\{s_i\}_{i\in I} : (s_1, \ldots, s_n) \leftarrow \mathsf{share}(s')\}.$$

C.1.3 Public Verifiable Bounded-Concurrent Zero-Knowledge Proof

Basically, $\mathsf{IdealZK}$ either sends $\mathsf{success}$ to everyone indicating that the proof is correct, or the identity of the prover/verifier who leads to the failure of the proof. Formally,

Ideal Zero-knowledge Functionality $\mathsf{IdealZK}[x, L, i, j]$

The functionality involves n parties $1, \ldots, n$, and is parametrized with a statement x, the language L, the prover's identity i and the verifier's identity j.

1. If both the prover i and the verifier j are corrupted, receive a bit b from the prover i. If $b = 1$, send $(\mathsf{success}, i, j)$ to everyone.
2. Receive ok or $\perp$ from the verifier j.
3. If received $\perp$ from the verifier, send (fail, j) to everyone.
4. Receive w or $\perp$ from the prover.
5. If $\mathcal{R}(x, w) = 1$, send $(\mathsf{success}, i, j)$ to everyone. Otherwise send (fail, i) to everyone.

We stress the public verifiability of the zero-knowledge proof because in our final protocol, we need to guarantee that every miner agrees on the set of bids/identities to consider in the mechanism. In an n-party $\mathsf{IdealZK}$-hybrid protocol, the players can invoke the ideal zero-knowledge functionality $\mathsf{IdealZK}[x, L, i, j]$ between any prover i and any verifier j, and for arbitrary NP language L. Without loss of generality, in every round, there can be at most n^2 concurrent invocations of $\mathsf{IdealZK}$. Given an n-party $\mathsf{IdealZK}$-hybrid protocol, we can instantiate $\mathsf{IdealZK}$ with actual cryptography using the elegant techniques suggested by Pass [Pas04].

Theorem C.1. *(Constant-round, bounded concurrent secure computation [Pas04]). Assume the existence of enhanced trapdoor permutations and collision-resistant hash functions. Then, given an n-party $\mathsf{IdealZK}$-hybrid protocol Π^*, in which the number of concurrent calls of $\mathsf{IdealZK}$ is upper bounded by a priori known bound $m = \mathsf{poly}(\lambda)$, there exists a real-world protocol Π such that the following hold:*

- **Simulatability***: For every real-world non-uniform p.p.t. adversary $\mathcal{A}$ controlling an arbitrary subset of up to $n-1$ players in Π, there exists a non-uniform p.p.t. adversary $\mathcal{A}^*$ in the protocol Π^*, such that for any input $(x_1, \ldots, x_n)$, every auxiliary string $z \in \{0,1\}^*$,*

$$\mathsf{Exec}^{\Pi,\mathcal{A}}(1^\lambda, x_1, \ldots, x_n, z) \equiv_c \mathsf{Exec}^{\Pi^*,\mathcal{A}^*}(1^\lambda, x_1, \ldots, x_n, z).$$

  In the above, the notation $\mathsf{Exec}^{\Pi,\mathcal{A}}$ (or $\mathsf{Exec}^{\Pi^*,\mathcal{A}^*}$) outputs each honest players outputs as well as the corrupt players (arbitrary) outputs.

- **Round efficiency***: The round complexity of Π is at most a constant factor worse than that of Π^*.*

C.2 Protocol Description

Below we give the multi-party computation protocol. Without loss of generality, we assume that each identity's bid is drawn from a distribution $\mathcal{D}$, whose support is a subset of a finite field $\mathbb{F}$.

Protocol $\Pi_{(\mathbf{x},\mathbf{p},\mu)}$ instantiating $\mathcal{F}_{\text{TFM}}$ in the $\mathsf{IdealZK}$-hybrid world

Parameters: Let λ be the security parameter and $\mathcal{D}$ be an initially empty sets. Let $t = \lceil \frac{m}{2} \rceil$ be the upper bound of the number of colluding miners. Let Env be the variable encoding the blockchain status and blockchain validity rule.

Building blocks: A perfectly binding, computationally hiding commitment scheme comm.

Input: Each identity i has an input $b_i \in \mathbb{F}$ as its bid. Each miner has no input.

Sharing phase

1. Identity i splits b_i into t-out-of-m Shamir secret shares. Let $X_{i,j}$ denote the j-th share of b_i. Let $\widehat{X}_{i,j} = \mathsf{comm}(X_{i,j}, r_{i,j})$ where $r_{i,j}$ are fresh randomness. Broadcast the commitments of shares $\{\widehat{X}_{i,j}\}_{j\in[m]}$. If an identity i fails to broadcast the commitments, add i to the set $\mathcal{D}$.

2. For each $j \in [m]$, identity i invoke $\mathsf{IdealZK}[\mathsf{stmt}_i, i, j]$ for each miner j, with the statement $\mathsf{stmt}_i = \{\widehat{X}_{i,j}\}_{j\in[m]}$, and send the witness $w = (b_i, \{X_{i,j}, r_{i,j}\}_{j\in[m]})$ to prove that

   - For each $j \in [m]$, $(X_{i,j}, r_{i,j})$ is the correct opening of $\widehat{X}_{i,j}$;
   - $\{X_{i,j}\}_{j\in[m]}$ forms a valid t-out-of-m secret sharing of b_i.

   For each identity $i \in [n]$, if there exists a j that $\mathsf{IdealZK}[\mathsf{stmt}_i, i, j]$ outputs (fail, i), i.e., the identity fails to prove the statement to miner j, add i to the set $\mathcal{D}$.

3. For $j \in [m]$, identity i sends $(X_{i,j}, r_{i,j})$ to miner j.

4. Each miner j does the following: for every $i \in [n] \setminus \mathcal{D}$, if it receives a message $(X_{i,j}, r_{i,j})$ that is a correct opening with respect to $\widehat{X}_{i,j}$, record $(X_{i,j}, r_{i,j})$ and broadcast (ok, i, j). Otherwise, broadcast $(\mathsf{complain}, i, j)$ to complain about identity i.

5. Each identity i does the following: for all j such that there is a complain $(\mathsf{complain}, i, j)$ in Step 4, identity i broadcasts the corresponding opening $(i, j, X_{i,j}, r_{i,j})$.

6. Unless identity i broadcasts all correct openings for those miners who has sent $(\mathsf{complain}, i, j)$ to complain about identity i, add i to the set $\mathcal{D}$.

7. Miner j does the following: for $i \in [n] \setminus \mathcal{D}$, if miner j sent $(\mathsf{complain}, i, j)$ in Step 4, and that identity i broadcast a correct opening $(X_{i,j}, r_{i,j})$ in Step 5. then record the correct opening $(X_{i,j}, r_{i,j})$.

Computation Phase Miners invoke $\mathcal{F}_{\text{check}}$ parameterized with the commitments of shares $\{\widehat{X}_{i,j}\}_{i\in[n]\setminus\mathcal{D}, j\in[m]}$ and the environment variable Env described below.

Output Phase Each miner broadcasts the output of $\mathcal{F}_{\text{check}}$. The majority vote of the output of $\mathcal{F}_{\text{check}}$ will be the output for this protocol.

Ideal Functionality $\mathcal{F}_{\text{check}}$

Parameters Commitments of shares $\{\widehat{X}_{i,j}\}_{i\in[n]\setminus\mathcal{D},j\in[m]}$, and the environment variable Env, and the mechanism $(\mathbf{x},\mathbf{p},\mu)$.

Input Each miner j has input $\{(X_{i,j},r_{i,j})\}_{i\in[n]\setminus\mathcal{D}}$, where $(X_{i,j},r_{i,j})$ is a correct opening of $\widehat{X}_{i,j}$.

Functionality

1. Each miner sends its input $\{(X_{i,j},r_{i,j})\}_{i\in[n]\setminus\mathcal{D}}$ to $\mathcal{F}_{\text{check}}$.
2. For each $j\in[m]$, the functionality $\mathcal{F}_{\text{check}}$ checks if $(X_{i,j},r_{i,j})$ is an correct opening of $\widehat{X}_{i,j}$ for all $i\in[n]\setminus\mathcal{D}$. If not, the functionality put j into an initially empty set $\mathcal{D}'$.
3. For each $i\in[n]\setminus\mathcal{D}$, the functionality reconstruct b_i using $\{X_{i,j}\}_{j\in[m]\setminus\mathcal{D}'}$.
4. The functionality removes any bid that violates the blockchain validity rule encoded by Env.
5. Let $\mathbf{b}$ denote the remaining bids that reconstructed successfully. The functionality then computes $\mathbf{x}(\mathbf{b}),\mathbf{p}(\mathbf{b}),\mu(\mathbf{b})$, and send the output to every miner.

Lemma C.2. *If the commitment scheme* comm *is perfectly binding and computationally hiding, then* $\Pi_{(\mathbf{x},\mathbf{p},\mu)}$ *securely realizes* $\mathcal{F}_{\text{TFM}}$ *in the* $(\mathsf{IdealZK},\mathcal{F}_{\text{check}})$*-hybrid model as long as the number of colluding miners is less than* $\frac{m}{2}$.

Proof. We show that for any non-uniform p.p.t. adversary $\mathcal{A}$ controlling the coalition interacting with $\Pi_{(\mathbf{x},\mathbf{p},\mu)}$, there exists an adversary $\mathcal{S}$ interacting with $\mathcal{F}_{\text{TFM}}$, such that $\mathcal{A}$'s views in an execution with $\Pi_{(\mathbf{x},\mathbf{p},\mu)}$ is computationally indistinguishable from its view simulated by $\mathcal{S}$. Note that since $t<\frac{m}{2}$, for each $i\in[n]\setminus\mathcal{D}$, the bid b_i is guaranteed to be successfully reconstructed.

In the following, we use $\mathcal{H}_I$ and $\mathcal{H}_M$ to denote the set of honest identities and miners, respectively, and $\mathcal{K}_I$, $\mathcal{K}_M$ to denote the set of identities and the set of miners in the coalition, respectively. The simulator $\mathcal{S}$ behaves as follows.

Sharing Phase

1. Emulate honest identities $i\in\mathcal{H}_I$ as follows: For each corrupted miner $k\in\mathcal{K}_M$, let $X_{i,k}$ be uniformly random chosen. For honest miner $j\in\mathcal{H}_M$, let $X_{i,j}=0$.
2. Emulate honest identity $i\in\mathcal{H}_I$ as follows: commit to the shares $\widehat{X}_{i,j}=\mathsf{comm}(X_{i,j},r_{i,j})$ using fresh randomness $r_{i,j}$ for miner $j\in[m]$. Send the commitments $\{\widehat{X}_{i,j}\}_{j\in[m]}$ to $\mathcal{A}$.
3. Wait for corrupted identities to send their commitments $\{\widehat{X}_{k,j}\}_{j\in[m]}$ for $k\in\mathcal{K}_I$. If a corrupted player k fails to send the commitments, add k to $\mathcal{D}$.
4. Emulate the $\mathsf{IdealZK}$ ideal functionality $\mathsf{IdealZK}$ as follows:

- For honest identity (prover) i and honest miner (verifier) i', send $(\mathsf{success}, i, i')$ to $\mathcal{A}$.
- For honest identity (prover) $i \in \mathcal{H}_I$ and corrupted miner (verifier) $k \in \mathcal{K}_M$: If received $\perp$ from a corrupted verifier $k \in \mathcal{K}_M$, send (fail, k) to $\mathcal{A}$. Otherwise, send $(\mathsf{success}, i, k)$ to $\mathcal{A}$.
- For corrupted identity (prover) $k \in \mathcal{K}_I$ and honest miner (verifier), send ok to $\mathsf{IdealZK}$ for the honest verifier, and forward $\perp$ or witness w received from $\mathcal{A}$ to $\mathsf{IdealZK}$. Send the output of $\mathsf{IdealZK}$ to $\mathcal{A}$.
- For corrupt identity (prover) $k \in \mathcal{K}_I$ and corrupt miner (verifier) $k' \in \mathcal{K}_M$, receive a bit from $\mathcal{A}$, and send the output of $\mathsf{IdealZK}$ to $\mathcal{A}$.

5. For corrupt identity (prover) $k \in \mathcal{K}_I$, if there exists a miner $j \in [m]$ such that the output of $\mathsf{IdealZK}[\mathsf{stmt}_\mathsf{k}, k, j]$ is (fail, k), add k to $\mathcal{D}$.
6. Emulate the honest identities $i \in \mathcal{H}_I$ to send the shares for corrupted miners $\{(X_{i,k}, r_{i,k})\}_{k \in \mathcal{K}_M}$ to $\mathcal{A}$.
7. Receive the shares for honest miners $\{(X_{k,i}, r_{k,i})\}_{i \in \mathcal{H}_M}$ from corrupted identities $k \in \mathcal{K}_I$.
8. Emulate honest miner i as follows: it checks whether $(X_{k,i}, r_{k,i})$ it receives from corrupted identity $k \in \mathcal{K}_I$ is a correct opening of $\widehat{X}_{k,i}$. If yes, send (ok, i, k) to $\mathcal{A}$. Otherwise send $(\mathsf{complain}, i, k)$ to $\mathcal{A}$.
9. Emulate honest identity i as follows: If it receives $(\mathsf{complain}, k, i)$ from a corrupted miner k, send $(X_{i,k}, r_{i,k})$ to $\mathcal{A}$.
10. Receive opening $(X_{k,i}, r_{k,i})$ from corrupt identity $k \in \mathcal{K} \setminus \mathcal{D}$, if there exists a complain $(\mathsf{complain}, i, k)$ for k.
11. Check for all corrupted identities $k \in \mathcal{K}_I \setminus \mathcal{D}$: If k sent all correct openings $(X_{k,j}, r_{k,j})$ of commitment $\widehat{X}_{k,j}$ for those j who complained, record the correct openings. Otherwise, add k to the set $\mathcal{D}$.

Note that by this point, for those corrupted identities $k \in \mathcal{K}_I \setminus \mathcal{D}$, the simulator $\mathcal{S}$ has received the witness b_k, $\{X_{k,j}, r_{k,j}\}_{j \in [m]}$ for $\mathsf{IdealZK}$. The simulator thus sends b_k to $\mathcal{F}_{\mathrm{TFM}}$ for all $k \in \mathcal{K}_I \setminus \mathcal{D}$, and $\perp$ to $\mathcal{F}_{\mathrm{TFM}}$ for those identities in $\mathcal{D}$. After the simulator $\mathcal{S}$ receives $\mathbf{x}(\mathbf{b}), \mathbf{p}(\mathbf{b}), \mu(\mathbf{b})$ from $\mathcal{F}_{\mathrm{TFM}}$, it emulates the $\mathcal{F}_{\mathrm{check}}$ functionality and sends $\mathbf{x}(\mathbf{b}), \mathbf{p}(\mathbf{b}), \mu(\mathbf{b})$ to $\mathcal{A}$.

We now show that the joint distribution of the output of the honest parties and the view of the adversary in the ideal execution (denoted as $\mathsf{Exp}_{\mathcal{A}}^{\mathsf{Ideal}}$) is computationally indistinguishable to the output of the honest parties and the view of the adversary in the real execution (denoted as $\mathsf{Exp}_{\mathcal{A}}^{\mathsf{Real}}$). Consider the following hybrids.

- Hyb_0: denotes an execution of $\Pi_{(\mathbf{x},\mathbf{p},\mu)}$, in which the simulator acts on behalf of all honest players and interacts with the adversary. Moreover, the simulator emulates $\mathsf{IdealZK}$ and $\mathcal{F}_{\mathrm{check}}$ for the adversary.
- Hyb_1: The simulator behaves same as in Hyb_0 except that in the sharing phase, for honest identity $i \in \mathcal{H}_I$, it generates t-out-of-m sharing $\{X_{i,j}\}_{j \in [n]}$ of b_i; but the commitments are computed as follows: $\widehat{X}_{i,k} = \mathsf{comm}(X_{i,k}, r_{i,k})$ for $k \in \mathcal{K}_M$, and $\widehat{X}_{i,i'} = \mathsf{comm}(0, r_{i,i'})$ for $i' \in \mathcal{H}_M$.

  Then, the simulator emulates the $\mathsf{IdealZK}$ functionality and vouches for honest players' commitments as follows:

– For honest identity (prover) i and honest miner (verifier) i', send $(\mathsf{success}, i, i')$ to $\mathcal{A}$.
– For honest identity prover $i \in \mathcal{H}_I$ and corrupt miner (verifier) $k \in \mathcal{K}$: If received $\perp$ from a corrupted miner (verifier) $k \in \mathcal{K}_M$, send (fail, k) to $\mathcal{A}$. Otherwise, send $(\mathsf{success}, i, k)$ to $\mathcal{A}$.

During the sharing phase, the simulator acts on behalf of honest identity $i \in \mathcal{H}_I$ and sends the shares $X_{i,j}$ to miner j. However, the honest miners do not complain about another honest share from an honest identity.

When emulate the $\mathcal{F}_{\text{check}}$ functionality, the simulator use the true shares to reconstruct the bids $\mathbf{b}$ directly, without checking the commitments for $X_{i,j}$ for honest identifier i and honest miner j.

$\underline{\mathsf{Exp}_{\mathcal{A}}^{\mathsf{Real}} \equiv \mathsf{Hyb}_0}$: By definition.

$\underline{\mathsf{Hyb}_0 \equiv_c \mathsf{Hyb}_1}$: This is due to the computational hiding property of the commitment scheme comm. Consider a sequence of hybrids Hyb_0^i for $i \in \mathcal{H}_I$. Without loss of generality we just assume that $i \in [|\mathcal{H}_I|]$.

- Hyb_0^0 is same as Hyb_0.
- Hyb_0^i is same as Hyb_0^{i-1} except that the commitments $\widehat{X}_{i,j}$ for honest miner $j \in \mathcal{H}_M$ are replaced with commitment of 0.
- $\mathsf{Hyb}_0^{|\mathcal{H}_I|}$ is exactly Hyb_1.

By the computational hiding property of the commitment scheme comm, for any $i \in [|\mathcal{H}_I|]$, we have $\mathsf{Hyb}_0^i \equiv_c \mathsf{Hyb}_0^{i-1}$. Otherwise, if there exists a non-uniform p.p.t. adversary $\mathcal{A}'$ that can distinguish Hyb_0^i from Hyb_0^{i-1} with a non-negligible probability, then we can build a non-uniform p.p.t. adversary $\mathcal{A}''$ that can distinguish the commitments of 0 and the commitments of the sharing $\{X_{i,j}\}_{j \in \mathcal{H}_M}$ with the same advantage. This breaks the hiding property of comm. Consequently, by hybrids argument, we have that $\mathsf{Hyb}_0 \equiv \mathsf{Hyb}_1$.

$\underline{\mathsf{Hyb}_1 \equiv \mathsf{Exp}_{\mathcal{A}}^{\mathsf{Ideal}}}$: This is due to the property of secret sharing. In Hyb_1, the shares $\{X_{i,k}\}_{i \in \mathcal{H}_I, k \in \mathcal{K}_M}$ are generated from honest identity's secret b_i, whereas in $\mathsf{Exp}_{\mathcal{A}}^{\mathsf{Ideal}}$, they are generated uniformly at random. Since the number of corrupted miners is smaller than $\frac{m}{2}$, by the security of Shamir secret sharing.

Moreover, since for each $i \in [n] \setminus \mathcal{D}$, the bid b_i is guaranteed to be reconstructed successfully in $\mathcal{F}_{\text{check}}$. Therefore, in both experiments, the honest players' output are identical. □