# Appendix

## EC.1. Cryptographic Protocols for On-Chain Implementation

Ideally, to design a credible blockchain TFM, we seek to discourage all kinds of dishonest behavior by either *systematically* preventing them from being conducted, or *economically* discouraging them by making them non-profitable.

Fortunately, the transparency property of a blockchain (Bertino, Kundu, and Sura, 2019) and its implementation of many cryptographic protocols (Luntovskyy and Guetter, 2018) have already helped prevent several types of dishonest behaviors. For example, since the blockchain is public, it is not possible for the miner to behave in a Byzantine manner via commuting different bidding vectors to different users (see the discussion in (Ferreira and Weinberg, 2020)), and the slashing rule in the Ethereum blockchain also discourage the miner from conducting certain classes of dishonest behavior via monetary penalties (Cassez, Fuller, and Asgaonkar, 2022).

Also, Ferreira and Weinberg (2020) propose to adopt a secure commitment scheme, which uses cryptographic protocols to guarantee that a bid cannot be modified after proposal. This scheme has the following advantages:

1. It restricts the strategy space of the miner to merely adding fake transactions and concealing transactions, ruling out strategies for the miner to collude with users and change existing bids.
2. It implements a sealed-bidding auction format that not only makes the Bayesian game modeling valid but also guarantees fairness among users' information sets, restricting users' strategy space and preventing the MEV issue in which the miners strategically manipulate transaction orders to increase their utility.

REMARK EC.1. while we only need to prevent individual user deviations in the interim setting, for $c$-SCP and MIC properties we want a stronger ex-post version.

Particularly, we can implement the *commitment scheme* in the way as follows:

1. Users submit the (salted) *hash values* of their transactions.
2. The miner packs and broadcasts all the hash values of the transactions that compete for the block, following by a hash value of the all packed hash values.
3. The users reveal their transactions and the miner uploads them. If the uploaded transactions deviates from the hash values too much ($\Delta \geq \epsilon_3 n$ for a pre-set $\epsilon_3 \in (0,1)$, with $\Delta$ defined in Section 7.1), the miner is penalized.
4. The system processes the TFM.

For the miner-only deviation, the miner may behave dishonestly in Steps 1-3, and the number of deviations can be restricted in the way as follows:

1. The miner may submit fake transactions in Step 1, without seeing the honest transactions (interim M−FT). The system can restrict the number of transactions proposed by an identity in any block, and require any identity to have a deposit before proposing any transaction, so that the miner cannot create a large number of identities to submit too many fake transactions. We assume that the miner would not afford to inject more than $\epsilon_1 n$ transactions.
2. The miner may ignore some hashes in Step 2, without seeing their bids (interim M−TD). In this way, the system effectively runs with a smaller $n$. But if we set the parameter $h$ in the way described in Section 7.1, reducing $n$ cannot benefit the miner's revenue. Besides, the users who have their hashes ignored can also report this behavior and get the miner penalized. We assume that the miner will be caught if she ignores more than $\epsilon_2 n$ hashes.
3. The miner may insert or ignore transactions after she sees the bids in Step 3 (ex-post M−FT and M−TD), but this type of behavior will be detected. If the number of deviations goes beyond an acceptable level, the miner will be penalized. On the other hand, an acceptable level $\epsilon_3 > 0$ is necessary because a missing transaction might also be simply due to the unstable connection from the user.

Hence, our protocol can restrict the miner individual deviation into a low level compared to $n$, and from the argument in Section 7.1, the relative advantage in miner revenue from $\{\texttt{M−FT}, \texttt{M−TD}\}$ is bounded below $O\left(\left(\frac{\epsilon_1+\epsilon_3}{1-\epsilon_2}\right)^{4/3}\right)$. However, the miner-user collusion cannot be effectively prevented in this way, as they may conduct the collusion off-chain before Step 1.

Therefore, we can remark that:

REMARK EC.2. Existing cryptographic protocols can effectively prevent miner individual deviations, but can only prevent part of miner-user collusions.

On the other hand, one may feel that the individual user's deviation is a "least destructive" honest behavior, because it happens in users' minds and does not seemingly disrupt the blockchain system. Hence, it also cannot be detected or prevented on the system level at all. However, we still argue that a desirable TFM should satisfy *truthfulness*, i.e., no individual user's deviation should be profitable. One key reason to design truthful mechanisms is the Revelation Principle (Myerson, 1981; Myerson, 1979): informally, for any non-truthful mechanism, we can construct an "equivalent" direct truthful mechanism that incorporates agents' optimal strategies into the mechanism itself, so that agents would maximize their utilities by reporting their true types (bidding their valuations). It renders untruthfulness unable to gain more advantage revenue.[4] Additionally, by the argument of the Revelation Principle, we also only need to consider single-round mechanisms. Hence, we remark that:

REMARK EC.3. The optimal revenue for any single-round truthful TFM is optimal even considering the class of non-truthful and multi-round mechanisms.

Furthermore, due to the anonymity of the blockchains (Khalilov and Levi, 2018), it is difficult for users to collude with each other, as argued by Chung and Shi (2023). Thus, user-user collusion is not a critical issue in the design of blockchain transaction fee mechanisms. Therefore, the remaining challenge to resolve is the prevention of user individual deviation and miner-user collusion, but as we have discussed, such dishonest behavior cannot be effectively prevented at the systematic level, so we have to discourage them in an economic way. In conclusion, we can remark that:

REMARK EC.4. To design a desirable blockchain transaction fee mechanism, the most critical challenge is to **discourage individual user's deviation and miner-user collusion via economic methods**.

## EC.2. Impossibility Result on Deterministic TFM

In this section, we propose an impossibility result that under certain conditions, any deterministic TFM which is U-BNIC and 1-SCP cannot have positive miner revenue. Here we additionally introduce several notions. Although this impossibility does not fully rule out deterministic mechanisms, it does motivate us to introduce randomness into our main mechanism.

**Deterministic.** When bids are distinct, the outcome of the auction is deterministic, i.e., $a_i \in \{0, 1\}$.

**Symmetric.** When we swap the bids of two users, their allocations and payments are exactly swapped.

**Continuous.** $\mathbf{p}$ and $r$ are continuous functions of $\mathbf{b}$, and $V$ has bounded, strictly positive PDF on a simply connected support $\text{dom}(V)$.

**Strongly Monotone.** If we raise the bid of bidder $i$ while leave other bids unchanged, $a_i, p_i$ do not decrease and $a_j (\forall j \neq i)$ does not increase.

THEOREM EC.1. *For all deterministic, symmetric, continuous, strongly monotone, user-individually-rational and budget-feasible TFMs, if* $\mathbf{0} \in V$*, then U-BNIC and 1-SCP implies non-positive miner revenue.*

### EC.2.1. Proof of Theorem EC.1

**Proof sketch.** To prove the non-positive-miner-revenue property of all satisfying mechanisms, we first show that all satisfying mechanisms must obey certain restrictive conditions, as the payment (Sec. EC.2.1.1) and revenue (Sec. EC.2.1.2) rules both must follow corresponding closed-form formulas; then we show that this type of mechanisms have non-positive miner revenue.

In this section, we introduce the $\delta$-function with

$$\int_{-\epsilon}^{\epsilon} \delta(t)dt = 1, \qquad \forall \epsilon > 0. \tag{EC.1}$$

We assume there exists a transaction fee mechanism $M_0(\mathbf{a}, \mathbf{p}, r)$ that satisfies all conditions.

**EC.2.1.1. Pinning down the payment rule** From definition we know that if $M_0$ is BNIC, then

$$\left.\frac{\partial E_{\mathbf{v}_{-i}\sim V_{-i}}\left[u_i(b_i,v_i,\mathbf{v}_{-i})\right]}{\partial b_i}\right|_{b_i=v_i}=0, \qquad \forall v_i \tag{EC.2}$$

i.e.,

$$\int_{\mathbf{v}_{-i}}\Bigg((v_i-p_i(v_i,\mathbf{v}_{-i}))\frac{\partial a_i(v_i,\mathbf{v}_{-i})}{\partial v_i} -a_i(v_i,\mathbf{v}_{-i})\frac{\partial p_i(v_i,\mathbf{v}_{-i})}{\partial v_i}\Bigg)\rho_{-i}(\mathbf{v}_{-i})d\mathbf{v}_{-i}=0, \tag{EC.3}$$

in which $\rho_{-i}(\cdot)$ is the pdf of $V_{-i}$.

For fixed $\mathbf{v}_{-i}$, since the mechanism is deterministic, we have that $a_i(\cdot,\mathbf{v}_{-i})\in\{0,1\}$ almost everywhere. Additionally because $a_i(\cdot,\mathbf{v}_{-i})$ is monotonic increasing, we have

$$a_i(v_i,\mathbf{v}_{-i})=\begin{cases}0,\ v_i<\theta(\mathbf{v}_{-i})\\ 1,\ v_i>\theta(\mathbf{v}_{-i}),\end{cases} \tag{EC.4}$$

in which $\theta(\mathbf{v}_{-i})$ is a constant for fixed $\mathbf{v}_{-i}$. Therefore,

$$\frac{\partial a_i(v_i,\mathbf{v}_{-i})}{\partial v_i}=\delta(v_i-\theta(\mathbf{v}_{-i})). \tag{EC.5}$$

Now we have a lemma:

LEMMA EC.1. *For* $\forall\mathbf{v}_{-i}$,

$$p_i(\theta(\mathbf{v}_{-i}),\mathbf{v}_{-i})=\theta(\mathbf{v}_{-i}). \tag{EC.6}$$

*Proof.* If $p_i(\theta(\mathbf{v}_{-i}),\mathbf{v}_{-i})>\theta(\mathbf{v}_{-i})$, let $t=p_i(\theta(\mathbf{v}_{-i}),\mathbf{v}_{-i})-\theta(\mathbf{v}_{-i})$. Then by continuity, there exists a small $\epsilon>0$ s.t. $p_i(\theta(\mathbf{v}_{-i})+\epsilon,\mathbf{v}_{-i})>\theta(\mathbf{v}_{-i})+\frac{t}{2}$ and $a_i(\theta(\mathbf{v}_{-i})+\epsilon,\mathbf{v}_{-i})=1$, and the user $i$ would have negative utility. In this scenario, the miner would want to collude with user $i$ and ask him to change his bid to $\theta(\mathbf{v}_{-i})-\epsilon$, so that user $i$ would now have 0 utility.

But by continuity, the change of the miner's revenue is arbitrarily small, increasing their total utility. So the 1-SCP property is violated.

If $p_i(\theta(\mathbf{v}_{-i}),\mathbf{v}_{-i})<\theta(\mathbf{v}_{-i})$, similarly there exists a scenario where user $i$ has valuation $\theta(\mathbf{v}_{-i})-\epsilon$ but the miner would want to let her bid $\theta(\mathbf{v}_{-i})+\epsilon$ instead, also violating 1-SCP.

Therefore, it must hold that $p_i(\theta(\mathbf{v}_{-i}), \mathbf{v}_{-i}) = \theta(\mathbf{v}_{-i})$.

□

From Lemma EC.1 we have

$$\int_{\mathbf{v}_{-i}} \left( (v_i - p_i(v_i, \mathbf{v}_{-i})) \frac{\partial a_i(v_i, \mathbf{v}_{-i})}{\partial v_i} \right) \rho_{-i}(\mathbf{v}_{-i}) d\mathbf{v}_{-i} = 0, \tag{EC.7}$$

so

$$\int_{\mathbf{v}_{-i}} \left( a_i(v_i, \mathbf{v}_{-i}) \frac{\partial p_i(v_i, \mathbf{v}_{-i})}{\partial v_i} \right) \rho_{-i}(\mathbf{v}_{-i}) d\mathbf{v}_{-i} = 0. \tag{EC.8}$$

Since monotonicity implies $\frac{\partial p_i(v_i, \mathbf{v}_{-i})}{\partial v_i} \geq 0$, we know that $\forall v_i > \theta(\mathbf{v}_{-i}), \frac{\partial p_i(v_i, \mathbf{v}_{-i})}{\partial v_i} = 0$. Therefore,

$$\forall b_i > \theta(\mathbf{v}_{-i}), \epsilon > 0, \quad p_i(b_i, \mathbf{v}_{-i}) = p_i\left(\theta(\mathbf{v}_{-i}) + \epsilon, \mathbf{v}_{-i}\right). \tag{EC.9}$$

Combined with Lemma EC.1, from continuity we get

$$\forall b_i \geq \theta(\mathbf{v}_{-i}), \quad p_i(b_i, \mathbf{v}_{-i}) = \theta(\mathbf{v}_{-i}). \tag{EC.10}$$

**EC.2.1.2. Pinning down the miner revenue rule** In this part, we mainly use the 1-SCP property to prove that the miner revenue is a constant with regard to any user. To show this, we prove a lemma:

LEMMA EC.2. *If $v_i \neq \theta(\mathbf{v}_{-i})$, then $\frac{\partial r(v_i, \mathbf{v}_{-i})}{\partial v_i} = 0$.*

*Proof.* We recall that the total utility of the miner and user $i$ is

$$C_i(b_i, v_i, \mathbf{v}_{-i}) = a_i(b_i, \mathbf{v}_{-i})(v_i - p_i(b_i, \mathbf{v}_{-i})) + r(b_i, \mathbf{v}_{-i}). \tag{EC.11}$$

From 1-SCP we know that

$$0 = \left. \frac{\partial C_i(b_i, v_i, \mathbf{v}_{-i})}{\partial b_i} \right|_{b_i = v_i} \tag{EC.12}$$

$$= \left( (v_i - p_i(v_i, \mathbf{v}_{-i})) \frac{\partial a_i(v_i, \mathbf{v}_{-i})}{\partial v_i} - a_i(v_i, \mathbf{v}_{-i}) \frac{\partial p(v_i, \mathbf{v}_{-i})}{\partial v_i} \right) + \frac{\partial r(v_i, \mathbf{v}_{-i})}{\partial v_i}. \tag{EC.13}$$

From Eq. (EC.10) we know $a_i(v_i, \mathbf{v}_{-i}) \frac{\partial p(v_i, \mathbf{v}_{-i})}{\partial v_i} \equiv 0$, and from Eq. (EC.5) we know $v_i \neq \theta(\mathbf{v}_{-i}) \Rightarrow \frac{\partial a_i(v_i, \mathbf{v}_{-i})}{\partial v_i} = 0$. So we deduce

$$v_i \neq \theta(\mathbf{v}_{-i}) \Rightarrow \frac{\partial r(v_i, \mathbf{v}_{-i})}{\partial v_i} = 0. \tag{EC.14}$$

□

Because the continuity condition guarantees $r(\mathbf{b})$ is a continuous function of $\mathbf{b}$, from Lemma EC.2 we know that for fixed $\mathbf{v}_{-i}$, $r(\cdot, \mathbf{v}_{-i})$ is a constant, hence

$$r(v_i, \mathbf{v}_{-i}) = r(0, \mathbf{v}_{-i}). \tag{EC.15}$$

By iteratively apply Eq. (EC.15) to all components of $\mathbf{v}$, we get

$$r(\mathbf{v}) = r(\mathbf{0}). \tag{EC.16}$$

We notice that from UIR,

$$\begin{aligned} r(\mathbf{0}) &\leq \sum_{i=1}^{n} a_i(\mathbf{0}) p_i(\mathbf{0}) && \text{(EC.17)} \\ &\leq \sum_{i=1}^{n} a_i(\mathbf{0}) \cdot 0 && \text{(EC.18)} \\ &= 0. && \text{(EC.19)} \end{aligned}$$

Therefore, we have

$$r(\mathbf{v}) \leq 0, \qquad \forall \mathbf{v}. \tag{EC.20}$$

Here we prove Theorem EC.1.

## EC.3. Additional Perspectives of Auxiliary Mechanism Method

### EC.3.1. A Failed Example: the First-Price Auction

In this part, we use a simple example to help readers understand the constraints for an admissible variation term. In particular, we will demonstrate a $\boldsymbol{\theta}$ function that cannot be coupled with any $\tilde{r}$ to form an admissible variation term. The $\boldsymbol{\theta}$ function is constructed based on the natural first-price auction. As an interesting by-product, this example also shows that, although the first-price auction mechanism can be adapted to satisfy U-BNIC, it cannot be combined with a miner payment rule $\tilde{r}$ to further enjoy the 1-SCP property.

We now define $\boldsymbol{\theta}$ based on the first-price auction. For simplicity, we consider only $n = 2$ users and the block size $k = 1$. The first-price auction for the single block entry defines the following allocation rule $\mathbf{a}$

(both first-price and second-price auctions confirm the highest-bid user, also note that $b_{-i}$ is a scalar since there are only 2 users):

$$a_i(b_i, b_{-i}) = \begin{cases} 1, \, b_i > b_{-i} \\ \frac{1}{2}, \, b_i = b_{-i} \\ 0, \, b_i < b_{-i} \end{cases}. \tag{EC.21}$$

We then consider the payment rules that will help us to finally define $\boldsymbol{\theta}$. The first payment rule $\mathbf{p}$ is the dominant association of $\mathbf{a}$. We calculate $\mathbf{p}$ via Eq. (7) as follows.

$$p_i(b_i, b_{-i}) = \begin{cases} b_{-i}, & b_i \geq b_{-i} \\ 0, & b_i < b_{-i} \end{cases}. \tag{EC.22}$$

Indeed, $\mathbf{a}$ and $\mathbf{p}$ form the second-price auction which is DSIC.

We now turn to the second payment rule $\tilde{\mathbf{p}}$ which is adapted from the payment rule of the first-price auction. It is well-known that the first-price auction is not truthful (DSIC) (Roughgarden, 2021): users would prefer to bid lower than their valuations, which is necessary for them to get any surplus even if they get the item. Nevertheless, there exist Bayesian Nash equilibria for specific settings when distributions of valuations are known. For example, when there are $n$ users with *i.i.d.* uniformly random valuations over $[0, 1]$, it is a Bayesian Nash equilibrium for each bidder to bid $\frac{n-1}{n} v_i$. By the Revelation Principle (Myerson, 1981; Myerson, 1979), we can derive a payment rule $\tilde{p}$ to make the confirmed user pay $\frac{n-1}{n}$ times her bid. For $n = 2$, we derive $\tilde{p}$ as follows.

$$\tilde{p}_i(b_i, b_{-i}) = \begin{cases} \frac{1}{2} b_i & b_i \geq b_{-i} \\ 0 & b_i < b_{-i} \end{cases}. \tag{EC.23}$$

Finally, we define $\boldsymbol{\theta}$ according to Eq. (8) and get that

$$\theta_i(b_i, b_{-i}) = \begin{cases} \frac{1}{2} b_i - b_{-i} & b_i > b_{-i} \\ -\frac{1}{4} b_i & b_i = b_{-i} \\ 0 & b_i < b_{-i} \end{cases}. \tag{EC.24}$$

When the user valuation is uniformly random over $[0, 1]$, we have that $\mathbb{E}_{b_{-i} \sim U[0,1]}[\theta_i(0, b_{-i})] = 0$ for $i \in \{1, 2\}$, indicating that $\boldsymbol{\theta}$ satisfies the second condition (Eq. (11)) of the admissibility property. Suppose that we could find a miner revenue function $\tilde{r}$ such that $T = (\boldsymbol{\theta}, \tilde{r})$ is admissible. Let $M = (\mathbf{a}, \mathbf{p}, 0)$. According to Theorem 2 and by the definition of $\boldsymbol{\theta}$, we have that the composed TFM

$$\tilde{M} = M + T = (\mathbf{a}, \mathbf{p}, 0) + (\boldsymbol{\theta}, \tilde{r}) = (\mathbf{a}, \tilde{\mathbf{p}}, \tilde{r})$$

is U-BNIC and 1-SCP. Then we could get the TFM $\tilde{M}$ which is a natural adaptation of the first-price auction (since its payment rule $\tilde{\mathbf{p}}$ is adapted from the first-price payment rule).

On the other hand, however, we show that this is impossible – there exists no $\tilde{r}$ such that $(\boldsymbol{\theta}, \tilde{r})$ is admissible. We prove this by contradiction. Suppose there exists such an $\tilde{r}$, we compute $\tilde{r}(1,1)$ in two different ways. By the first condition of admissibility (Eq. (10)), we have that

$$\begin{aligned}\tilde{r}(1,1) &= \tilde{r}(0,0) + (\tilde{r}(1,0) - \tilde{r}(0,0)) + (\tilde{r}(1,1) - \tilde{r}(1,0)) \\ &= \tilde{r}(0,0) + \theta_1(1,0) + \theta_2(1,1) \\ &= \tilde{r}(0,0) + 0.5 - 0.25 \\ &= \tilde{r}(0,0) + 0.25.\end{aligned}$$

We can also invoke Eq. (10) and compute $\tilde{r}(1,1)$ via a different path:

$$\begin{aligned}&\tilde{r}(1,1) \\ &= \tilde{r}(0,0) + (\tilde{r}(0.5,0) - \tilde{r}(0,0)) + (\tilde{r}(0.5,1) - \tilde{r}(0.5,0)) \\ &\qquad + (\tilde{r}(1,1) - \tilde{r}(0,1)) - (\tilde{r}(0.5,1) - \tilde{r}(0,1)) \\ &= \tilde{r}(0,0) + \theta_1(0.5,0) + \theta_2(0.5,1) + \theta_1(1,1) - \theta_1(0.5,1) \\ &= \tilde{r}(0,0) + 0.25 + 0 - 0.25 - 0 \\ &= \tilde{r}(0,0) + 0.\end{aligned}$$

Now we reach the contradiction. This example shows that using our auxiliary mechanism method, we are not able to extend the natural first-price auction to a U-BNIC and 1-SCP TFM.[5] We will need to carefully design a different $\boldsymbol{\theta}$ to satisfy the admissibility conditions.

### EC.3.2. A Conservative-field Perspective of the Payment Difference Function $\{\theta_i\}$

In this part, we distill our experience in the trial in Appendix EC.3.1 and provide an additional perspective for the design of $\boldsymbol{\theta}$. From the example, we see that if we sum up the differences of $\boldsymbol{\theta}$ along any path that consists of axis-aligned arcs, the summation should only depend on the two terminals of the path. This suggests the path-independence property of the $\boldsymbol{\theta}$ function. In particular, for any $\boldsymbol{\theta}$ in an admissible variation term $(\boldsymbol{\theta}, \tilde{r})$, if we define the vector field

$$\mathbf{D}_{\boldsymbol{\theta}}(\mathbf{b}) = \left( \frac{\partial}{\partial b_1} \theta_1(b_1, \mathbf{b}_{-1}), \cdots, \frac{\partial}{\partial b_n} \theta_n(b_n, \mathbf{b}_{-n}) \right), \tag{EC.25}$$

then $\mathbf{D}_{\boldsymbol{\theta}}$ should be a conservative field (Connell and Drost, 1983). In other words, for any closed curve $C$ (with parametrization $\mathbf{z}$), we have the following equality for the integration

$$\oint_C \mathbf{D}_{\boldsymbol{\theta}} \cdot d\mathbf{z} = 0. \tag{EC.26}$$

According to Eq. (10), $\tilde{r}$ is actually the potential of $\mathbf{D}_{\boldsymbol{\theta}}$. From this conservative-field perspective, we see that in order to successfully construct an admissible variation term, we may consider first constructing a $\tilde{r}$ (as the *potential* that determines the field), while guaranteeing the $\boldsymbol{\theta}$ functions satisfies Eq. (11). This intuition helps our design of the admissible variation term. Nevertheless, it is still quite challenging to construct a good variation term. Thanks to the almost-modular property of the auxiliary mechanism and the variation term, we can re-use an admissible variation term in different settings, as we do in Sections 5-6.

### EC.3.3. Intuition of Variation Term Construction in Section 5.2

From the admissibility condition Eq. (10), i.e., $\theta_i(b_i, \mathbf{b}_{-i}) = \tilde{r}(b_i, \mathbf{b}_{-i}) - \tilde{r}(0, \mathbf{b}_{-i})$, we get

$$\tilde{r}(b_i, \mathbf{b}_{-i}) = \tilde{r}(b_i, \mathbf{0}) + \theta(b_i, \mathbf{b}_{-i}) \tag{EC.27}$$

From another admissibility condition of Eq. (11), i.e., $\mathbb{E}_{\mathbf{b}_{-i}}[\theta_i(b_i, \mathbf{b}_{-i})] = 0$, for convenience we decouple $b_i$ and $\mathbf{b}_{-i}$ and construct $\theta_i$ in the following form

$$\theta_i(b_i, \mathbf{b}_{-i}) = h \cdot \alpha(b_i) \cdot \beta(\mathbf{b}_{-i}), \tag{EC.28}$$

in which $\beta(\mathbf{b}_{-i})$ is a symmetric expression on $\mathbf{b}_{-i}$ and

$$\mathbb{E}_{\mathbf{b}_{-i}}[\beta(\mathbf{b}_{-i})] = 0. \tag{EC.29}$$

Now we consider the case of $\mathbf{b}_{-i} = \mathbf{0}$ and $m$ is large, i.e., the situation is close to a second-price auction in which all other users bid zero, and the user $i$'s payment in the auxiliary mechanism is close to zero.

However, as long as $b_i > 0$, by intuition user $i$ is capable of paying more. From the allocation rule, for any fixed $m$ we can actually find a $K > 0$ in which $a_i(b_i, \mathbf{0}) \geq K b_i$, and hence user $i$ is able to pay at least $a_i(b_i, \mathbf{0}) \cdot b_i \geq K b_i^2$. On the other hand, from Myerson's Lemma (Lemma 1), in the auxiliary mechanism we also have $a_i(b_i, \mathbf{0}) p_i(b_i, \mathbf{0}) = \Theta(b_i^2)$ when $b_i \to 0$, but quickly "saturating" when $b_i > \Theta(\frac{1}{m})$ and $a_i(b_i, \mathbf{0})$ become close to 1. Hence, to uniformly exploit payment from user $i$ for different values of $b_i$, we would like to construct[6]

$$\alpha(b_i) = \frac{1}{2} b_i^2. \tag{EC.30}$$

On the other hand, since the expression of $\theta_i(\cdot)$ will appear in the expression of $\tilde{r}(\cdot)$, and $\tilde{r}(\cdot)$ is a symmetric expression. In order to ensure symmetry, we construct

$$\beta(\mathbf{b}_{-i}) = 1 - \mu \sum_{j: j \neq i} b_j^2. \tag{EC.31}$$

Even if it indicated less payment when $\mathbf{b}_{-i}$ are large on the users' side, the negative fourth order terms in the expression of $\tilde{r}(\mathbf{b})$ are "halved" compared to the sum of $\{\theta_i(b_i, \mathbf{b}_{-i})\}$, yielding a positive expected miner revenue.

From Eq.(EC.29), we have

$$\mu = \frac{1}{\mathbb{E}_{b_{-i}}[\sum_{j:j\neq i} b_j^2]} \tag{EC.32}$$

$$= \frac{1}{c_\rho(n-1)}. \tag{EC.33}$$

From Eqs. (EC.28,EC.30,EC.31,EC.33) we get the construction of the variation term as Eqs. (19,20).

## EC.4. Omitted Proofs

### EC.4.1. Proof of Theorem 2

First, we observe a sufficient condition for a TFM to be U-BNIC.

OBSERVATION 1. $\tilde{M}$ is U-BNIC if

$$\mathbb{E}_{\mathbf{b}_{-i}\sim V_{-i}}[\theta_i(b_i, \mathbf{b}_{-i})] = 0. \tag{EC.34}$$

*Proof.* Because user $i$'s expected utility $\tilde{u}(b_i, \mathbf{b}_{-i}; v_i) = u(b_i, \mathbf{b}_{-i}; v_i) - \theta(b_i, \mathbf{b}_{-i})$, if $\mathbb{E}_{\mathbf{b}_{-i}\sim V_{-i}}[\theta_i(b_i, \mathbf{b}_{-i})] = 0$, then for any bidding vector $\mathbf{b}$ and $i$'s valuation $v_i$, mechanisms $M$ and $\tilde{M}$ have the same expected utility

$$\mathbb{E}_{b_{-i}\sim V_{-i}}[u(b_i, \mathbf{b}_{-i}; v_i)] = \mathbb{E}_{b_{-i}\sim V_{-i}}[\tilde{u}(b_i, \mathbf{b}_{-i}; v_i)]. \tag{EC.35}$$

As mechanism $M$ is U-BNIC, it holds that $\tilde{M}$ is also U-BNIC.

□

As we have characterized a sufficient condition for U-BNIC, now we consider the condition for 1-SCP. We first introduce a lemma as a sufficient and necessary condition for a TFM to be 1-SCP:

LEMMA EC.3. *The mechanism $M = (\mathbf{a}, \mathbf{p}, r)$ is 1-SCP if and only if the following conditions are satisfied:*

- *Monotone allocation: $a_i(\cdot, \mathbf{b}_{-i})$ is monotonic non-decreasing,*
- *Constrained payment function:*

$$\begin{aligned} &a_i(b_i, \mathbf{b}_{-i})p_i(b_i, \mathbf{b}_{-i}) - r(b_i, \mathbf{b}_{-i}) \\ &= \int_0^{b_i} t\frac{\partial a_i(t, \mathbf{b}_{-i})}{\partial t}dt + a_i(0, \mathbf{b}_{-i})p_i(0, \mathbf{b}_{-i}) - r(0, \mathbf{b}_{-i}). \end{aligned} \tag{EC.36}$$

*Proof.* Consider another mechanism $M' = (\mathbf{a}, \mathbf{p} - \frac{r}{\mathbf{a}}, 0)$. Since $M'$ has zero miner revenue, it is 1-SCP if and only if it is U-DSIC.

From Lemma 1, $M'$ is U-DSIC if and only if the given conditions hold. So $M'$ is 1-SCP if and only if the conditions hold.

Notice that for the same bidding vector $\mathbf{b}$, the miner and user $i$ have the same total utilities in mechanisms $M$ and $M'$. So $M$ is 1-SCP if and only if the conditions hold.

□

From Lemma EC.3 we know that for an 1-SCP mechanism $(\mathbf{a}, \tilde{\mathbf{p}}, \tilde{\mathbf{r}})$, if we fix $\mathbf{b}_{-i}$, the difference of $a_i(\cdot, \mathbf{b}_{-i})\tilde{p}_i(\cdot, \mathbf{b}_{-i})$ and $\tilde{r}_i(\cdot, \mathbf{b}_{-i})$ is a constant. Furthermore, since $a(\cdot, \mathbf{b}_{-i})$ is monotonic increasing, if we want $\tilde{M}$ to be 1-SCP, from Lemma EC.3 we need and only need:

$$\begin{aligned} &a_i(b_i, \mathbf{b}_{-i})\tilde{p}_i(b_i, \mathbf{b}_{-i}) - \tilde{r}(b_i, \mathbf{b}_{-i}) \\ &= \int_0^{b_i} t \frac{\partial a_i(t, \mathbf{b}_{-i})}{\partial t} dt + a_i(0, \mathbf{b}_{-i})\tilde{p}_i(0, \mathbf{b}_{-i}) - \tilde{r}(0, \mathbf{b}_{-i}). \end{aligned} \tag{EC.37}$$

From the construction of $\mathbf{p}$ we have

$$a_i(b_i, \mathbf{b}_{-i})p_i(b_i, \mathbf{b}_{-i}) = \int_0^{b_i} t \frac{\partial a_i(t, \mathbf{b}_{-i})}{\partial t} dt. \tag{EC.38}$$

Since we set the boundary condition $\tilde{p}_i(0, \mathbf{b}_{-i}) = 0$, and the definition of $\{\theta_i\}$ as $\theta_i(b_i, \mathbf{b}_{-i}) = a_i(b_i, \mathbf{b}_{-i})(\tilde{p}_i(b_i, \mathbf{b}_{-i}) - p_i(b_i, \mathbf{b}_{-i}))$, we get a sufficient condition of 1-SCP as:

$$\theta_i(b_i, \mathbf{b}_{-i}) = \tilde{r}(b_i, \mathbf{b}_{-i}) - \tilde{r}(0, \mathbf{b}_{-i}), \quad \forall i. \tag{EC.39}$$

So $\tilde{M}$ is indeed U-BNIC and 1-SCP if $M$ is U-DSIC and 1-SCP and $T$ is admissible.

### EC.4.2. Proof of Lemma 2

We have

$$\tilde{r}(b_i, \mathbf{b}_{-i}) - \tilde{r}(0, \mathbf{b}_{-i}) = \frac{1}{2}h\left(b_i^2 - \frac{\sum_{j \neq i} b_i^2 b_j^2}{c_\rho(n-1)}\right) \tag{EC.40}$$

$$= \frac{1}{2}hb_i^2\left(1 - \frac{\sum_{j \neq i} b_j^2}{c_\rho(n-1)}\right) \tag{EC.41}$$

$$= \theta_i(b_i, \mathbf{b}_{-i}) \tag{EC.42}$$

and

$$\begin{aligned}
&\mathbb{E}_{\mathbf{b}_{-i}\sim V_{-i}}\theta_i(b_i,\mathbf{b}_{-i})\\
&=\mathbb{E}_{\mathbf{b}_{-i}\sim V_{-i}}\left[-\frac{1}{2}hb_i^2\left(\frac{\sum_{j\neq i}b_j^2}{c_\rho(n-1)}-1\right)\right] &\text{(EC.43)}\\
&=-\frac{1}{2}hb_i^2\left(\frac{\sum_{j\neq i}\mathbb{E}_{\mathbf{b}_{-i}\sim V_{-i}}[b_j^2]}{c_\rho(n-1)}-1\right) &\text{(EC.44)}\\
&=-\frac{1}{2}hb_i^2\left(\frac{\sum_{j\neq i}c_\rho}{c_\rho(n-1)}-1\right) &\text{(EC.45)}\\
&=0. &\text{(EC.46)}
\end{aligned}$$

Therefore, the variation term $T$ is admissible.

### EC.4.3. Proof of Theorem 3

From the auxiliary mechanism method, the mechanism $\tilde{M}=(\mathbf{a},\tilde{\mathbf{p}},r)$ is U-BNIC and 1-SCP from Theorem 2. Now we prove the UIR, BF and U-SP properties.

**EC.4.3.1. Proof of UIR and BF** From Eq. (16) we know $p_i(0,\mathbf{b}_{-i})=0$. Then for $n\to\infty$, from Lemma 1 and $b_i\in[0,1]$ we get:

$$\begin{aligned}
a_i(b_i,\mathbf{b}_{-i})p_i(b_i,\mathbf{b}_{-i})&=\int_0^{b_i}t\frac{\partial a_i(t,\mathbf{b}_{-i})}{\partial t}dt &\text{(EC.47)}\\
&=\int_0^{b_i}t\cdot\frac{e^t\sum_{j\neq i}e^{b_j}}{\left(e^t+\sum_{j\neq i}e^{b_j}\right)^2}dt. &\text{(EC.48)}
\end{aligned}$$

Since $t\in[0,1]$, it holds that

$$\begin{aligned}
\frac{e^t\sum_{j\neq i}e^{b_j}}{e^t+\sum_{j\neq i}e^{b_j}}&=\left(\frac{1}{e^t}+\frac{1}{\sum_{j\neq i}e^{b_j}}\right)^{-1} &\text{(EC.49)}\\
&\geq\left(\frac{1}{1}+\frac{1}{n-1}\right)^{-1} &\text{(EC.50)}\\
&=\frac{n-1}{n}. &\text{(EC.51)}
\end{aligned}$$

Combined with $e^t+\sum_{j\neq i}e^{b_j}\leq en$, we have

$$\frac{e^t\sum_{j\neq i}e^{b_j}}{\left(e^t+\sum_{j\neq i}e^{b_j}\right)^2}\geq\frac{n-1}{en^2}. \tag{EC.52}$$

Hence,

$$a_i(b_i, \mathbf{b}_{-i}) p_i(b_i, \mathbf{b}_{-i}) \geq \int_0^{b_i} t \frac{n-1}{en^2} dt \tag{EC.53}$$

$$= \frac{n-1}{2en^2} \cdot b_i^2. \tag{EC.54}$$

Therefore, the difference of the total collected fee and miner revenue in $\tilde{M}$ is

$$\sum_{i=1}^n a_i(b_i, \mathbf{b}_{-i}) \tilde{p}_i(b_i, \mathbf{b}_{-i}) - \tilde{r}(\mathbf{b})$$

$$= \sum_{i=1}^n a_i(b_i, \mathbf{b}_{-i}) p_i(b_i, \mathbf{b}_{-i}) + \sum_{i=1}^n \theta_i(b_i, \mathbf{b}_{-i}) - \tilde{r}(\mathbf{b}) \tag{EC.55}$$

$$\geq \frac{n-1}{2en^2} \cdot \sum_{i=1}^n b_i^2 - \left( h \frac{\sum_{1 \leq i < j \leq n} b_i^2 b_j^2}{c_\rho(n-1)} - \frac{h}{2} \sum_{i=1}^n b_i^2 \right)$$
$$- \frac{1}{2} h \left( \sum_{i=1}^n b_i^2 - \frac{\sum_{1 \leq i < j \leq n} b_i^2 b_j^2}{c_\rho(n-1)} \right) \tag{EC.56}$$

$$= \frac{n-1}{2en^2} \cdot \sum_{i=1}^n b_i^2 - \frac{h}{2c_\rho(n-1)} \sum_{1 \leq i < j \leq n} b_i^2 b_j^2 \tag{EC.57}$$

$$\geq \frac{n-1}{2en^2} \cdot \sum_{i=1}^n b_i^2 - \sum_{i=1}^n b_i^2 \left( \frac{h}{4c_\rho(n-1)} \sum_{i=1}^n b_i^2 \right) \tag{EC.58}$$

$$\geq \frac{n-1}{2en^2} \cdot \sum_{i=1}^n b_i^2 - \sum_{i=1}^n b_i^2 \left( \frac{h}{4c_\rho(n-1)} \cdot n \right) \tag{EC.59}$$

$$= \sum_{i=1}^n b_i^2 \cdot \left( \frac{n-1}{2en^2} - \frac{hn}{4c_\rho(n-1)} \right). \tag{EC.60}$$

So $\tilde{M}$ is budget feasible as long as $h \leq \frac{2c_\rho(n-1)^2}{en^3} = \Theta(c_\rho/n)$.

For user individual rationality,

$$b_i - \tilde{p}_i(b_i, \mathbf{b}_{-i})$$

$$= b_i - p_i(b_i, \mathbf{b}_{-i}) - \frac{\theta_i(b_i, \mathbf{b}_{-i})}{a_i(b_i, \mathbf{b}_{-i})} \tag{EC.61}$$

$$= \frac{1}{a_i(b_i, \mathbf{b}_{-i})} \Big[ b_i \left( a_i(0, \mathbf{b}_{-i}) + \int_0^{b_i} \frac{\partial a_i(t, \mathbf{b}_{-i})}{\partial t} dt \right)$$
$$- \int_0^{b_i} t \frac{\partial a_i(t, \mathbf{b}_{-i})}{\partial t} \Big] \tag{EC.62}$$

$$= \frac{1}{a_i(b_i, \mathbf{b}_{-i})} \Big[ b_i a_i(0, \mathbf{b}_{-i}) + \int_0^{b_i} (b_i - t) \frac{\partial a_i(t, \mathbf{b}_{-i})}{\partial t} dt$$
$$+ \frac{1}{2} h b_i^2 \left( \frac{\sum_{j \neq i} b_j^2}{c_\rho(n-1)} - 1 \right) \Big]. \tag{EC.63}$$

From Eq.(EC.52), we also have

$$\begin{aligned}
&\int_0^{b_i}(b_i-t)\frac{\partial a_i(t,\mathbf{b}_{-i})}{\partial t}dt \\
&=\int_0^{b_i}(b_i-t)\cdot\frac{e^t\sum_{j\neq i}e^{b_j}}{\left(e^t+\sum_{j\neq i}e^{b_j}\right)^2}dt && \text{(EC.64)}\\
&\geq\int_0^{b_i}(b_i-t)\cdot\frac{n-1}{en^2}dt && \text{(EC.65)}\\
&=\frac{n-1}{2en^2}\cdot b_i^2. && \text{(EC.66)}
\end{aligned}$$

Therefore, when $h=\frac{2c_\rho(n-1)^2}{en^3}$, since $c_\rho\leq 1$, we have

$$\begin{aligned}
&\tilde{u}_i(b_i,\mathbf{b}_{-i};b_i)\\
&=b_ia_i(0,\mathbf{b}_{-i})+\int_0^{b_i}(b_i-t)\frac{\partial a_i(t,\mathbf{b}_{-i})}{\partial t}dt\\
&\quad+\frac{1}{2}hb_i^2\left(\frac{\sum_{j\neq i}b_j^2}{c_\rho(n-1)}-1\right) && \text{(EC.67)}\\
&\geq\frac{b_i}{en}+\int_0^{b_i}(b_i-t)\frac{\partial a_i(t,\mathbf{b}_{-i})}{\partial t}dt\\
&\quad+\frac{1}{2}hb_i^2\left(\frac{\sum_{j\neq i}b_j^2}{c_\rho(n-1)}-1\right) && \text{(EC.68)}\\
&\geq b_i^2\left(\frac{1}{en}+\frac{n-1}{2en^2}-\frac{h}{2}\right) && \text{(EC.69)}\\
&=b_i^2\left(\frac{1}{en}+\frac{n-1}{2en^2}-\frac{c_\rho(n-1)^2}{en^3}\right) && \text{(EC.70)}\\
&\geq b_i^2\left(\frac{1}{en}+\frac{n-1}{2en^2}-\frac{1}{en}\right) && \text{(EC.71)}\\
&\geq 0. && \text{(EC.72)}
\end{aligned}$$

So the UIR also holds for $h=\frac{2c_\rho(n-1)^2}{en^3}$.

Therefore, we have shown $h_*(n,c_\rho)\geq\frac{2c_\rho(n-1)^2}{en^3}=\Omega(c_\rho/n)$.

### EC.4.3.2. Proof of U-SP

We firstly consider the auxiliary mechanism $(\mathbf{a},\mathbf{p},r)$. Denote $w_{-i}=\sum_{j\neq i}e^{mb_j}$, then we have

$$\begin{aligned}
a_i(b_i,\mathbf{b}_{-i})&=\frac{e^{mb_i}}{e^{mb_i}+w_{-i}} && \text{(EC.73)}\\
p_i(b_i,\mathbf{b}_{-i})&=b_i-\frac{e^{mb_i}+w_{-i}}{me^{mb_i}}\ln\frac{e^{mb_i}+w_{-i}}{1+w_{-i}}. && \text{(EC.74)}
\end{aligned}$$

The utility of identity $i$ is $u_i(b_i, \mathbf{b}_{-i}; v_i) = a_i(b_i, \mathbf{b}_{-i})(v_i - p_i(b_i, \mathbf{b}_{-i}))$. We can also regard as it as a function of $(b_i, w_{-i}, v_i)$, then we have

$$\left.\frac{\partial u_i}{\partial w_{-i}}\right|_{b_i=v_i} = \frac{-\frac{1}{1+w_{-i}} + \frac{1}{e^m+w_{-i}}}{m} \leq 0. \tag{EC.75}$$

As injecting fake bids is equivalent to increasing $w_{-i}$ for identity $i$ in the auxiliary mechanism, it cannot increase identity $i$'s utility in the auxiliary mechanism.

However, the injected fake bids can influence user $i$'s utility in two more aspects, as:

- The variation term.
- The utilities of fake identities.

We denote $h$ as the scaling parameter for total user number $n+l$, hence, we have

$$h \leq \frac{2c_\rho(n+l-1)^2}{e(n+l)^3}. \tag{EC.76}$$

Without fake identities, the expectation of $\theta_i(b_i, \mathbf{b}_{-i})$ is zero. Therefore, denote $\Omega = \{i\} \cup \{n+1, \cdots, n+l\}$, then $\Omega$ is the set of all identities that the user has access to, and we only need to show that

$$\mathbb{E}_{\mathbf{b}_{-i}\sim V_{-i}}\left[\sum_{j=n+1}^{n+l} a_j(b_j, \mathbf{b}_{-j}^+)p_j(b_j, \mathbf{b}_{-j}^+) + \sum_{j\in\Omega}\theta(b_j, \mathbf{b}_{-j}^+)\right] \geq 0. \tag{EC.77}$$

For a refined analysis of constants, we denote the Sybil attacker has real identity $i$, and submits fake bids with identities $n+1, \cdots, n+l$. We denote that:

$$\sigma = \sum_{j\leq n, j\neq i} b_j^2,$$
$$\sigma_\# = \sum_{j=n+1}^{n+l} b_j^2,$$

Then $\sigma$ is a random variable independent to any $b_j$ for $j \in \Omega$, and it holds that

$$\mathbb{E}_{\mathbf{b}_{-i}\sim V_{-i}}[\sigma] = c_\rho(n-1).$$

From Eq. (EC.54) , we have

$$\sum_{j=n+1}^{n+l} a_j(b_j, \mathbf{b}_{-j}^+)p_j(b_j, \mathbf{b}_{-j}^+) \geq \frac{n+l-1}{2e(n+l)^2}\sum_{j=n+1}^{n+l} b_j^2 \tag{EC.78}$$

$$\geq \frac{1}{2e(n+l+2)} \cdot \sigma_\#. \tag{EC.79}$$

For $j \in \Omega$, we have

$$\theta(b_j, \mathbf{b}^+_{-j}) = -\frac{1}{2} h b_j^2 \left( \frac{\sum_{t \le n+l, t \ne j} b_t^2}{c_\rho (n+l-1)} - 1 \right) \tag{EC.80}$$

$$= -\frac{1}{2} h b_j^2 \left( \frac{\sigma + \sigma_\# + b_i^2 - b_j^2}{c_\rho (n+l-1)} - 1 \right). \tag{EC.81}$$

Here, $\sigma$ is the only random variable in the expression, and

$$\mathbb{E}_{\mathbf{b}_{-i} \sim V_{-i}} \left[ \sum_{j \in \Omega} \theta(b_j, \mathbf{b}^+_{-j}) \right]$$

$$= \mathbb{E}_{\mathbf{b}_{-i} \sim V_{-i}} \left[ -\sum_{j \in \Omega} \frac{1}{2} h b_j^2 \left( \frac{\sigma + \sigma_\# + b_i^2 - b_j^2}{c_\rho (n+l-1)} - 1 \right) \right] \tag{EC.82}$$

$$= -\frac{h}{2} \sum_{j \in \Omega} b_j^2 \cdot \left( \frac{\mathbb{E}_{\mathbf{b}_{-i} \sim V_{-i}} [\sigma] + \sigma_\# + b_i^2}{c_\rho (n+l-1)} - 1 \right) + \frac{h}{2} \sum_{j \in \Omega} \frac{b_j^4}{c_\rho (n+l-1)} \tag{EC.83}$$

$$= -\frac{h}{2} (\sigma_\# + b_i^2) \cdot \frac{\sigma_\# + b_i^2 - c_\rho l}{c_\rho (n+l-1)} + \frac{h}{2} \cdot \frac{\sum_{j \in \Omega} b_j^4}{c_\rho (n+l-1)} \tag{EC.84}$$

$$= \frac{h}{2 c_\rho (n+l-1)} \Bigg( -\sigma_\#^2 - 2 b_i^2 \sigma_\# - b_i^4 + c_\rho l (\sigma_\# + b_i^2) + b_i^4 + \sum_{j=n+1}^{n+l} b_j^4 \Bigg) \tag{EC.85}$$

$$\ge \frac{h}{2 c_\rho (n+l-1)} \left( -\sigma_\#^2 - 2 b_i^2 \sigma_\# \right) \tag{EC.86}$$

$$\ge \frac{n+l-1}{e (n+l)^3} \left( -\sigma_\#^2 - 2 \sigma_\# \right). \tag{EC.87}$$

From Eqs. (EC.79,EC.87), Eq. (EC.77) is implied by

$$\frac{1}{2e(n+l+2)} \sigma_\# \ge \frac{n+l-1}{e(n+l)^3} (\sigma_\#^2 + 2\sigma_\#). \tag{EC.88}$$

Noticing that $\forall b_i \le 1$, so $\sigma_\# \le l$. We only need

$$(n+l)^3 \ge 2(n+l+2)(n+l-1)(l+2). \tag{EC.89}$$

Now for any $C \in [0,1)$, we assume $n \ge \frac{6C+5}{1-C^2}$, then denote $\varphi = \frac{l}{n} \le C$, and we have

$$(1+\varphi)^3 n^3 - 2((1+\varphi)n+2)((1+\varphi)n-1)(\varphi n+2) \tag{EC.90}$$

$$= (1+\varphi)((1-\varphi^2)n-(6\varphi+4))n-4)n+8. \tag{EC.91}$$

Since $n \geq \frac{6C+5}{1-C^2}$, we see that $n \geq 5$, and $(1-\varphi^2)n-(6\varphi+4) \geq (1-C^2)n-(6C+4) \geq 1$. Hence,

$$(1+\varphi)((1-\varphi^2)n-(6\varphi+4))n-4)n+8 \tag{EC.92}$$

$$\geq 1 \cdot (1 \cdot n-4)n+8 \tag{EC.93}$$

$$\geq 13 \tag{EC.94}$$

$$> 0. \tag{EC.95}$$

Now we prove that the mechanism is $(C, \frac{6C+5}{1-C^2})$-U-SP for any $C \in [0,1)$.

### EC.4.4. Proof of Theorem 4

From the auxiliary mechanism method, we have the U-BNIC and 1-SCP properties as long as the allocation rule is monotone. Hence, our proof for Theorem consists of 3 parts:

- Proof of monotonicity of allocation rule.
- Proof of UIR and BF.
- Proof of U-SP.

**EC.4.4.1. Proof of Monotonicity of Allocation Rule.** For monontonicity, we just need to show that for any $\mathbf{b}_{-i}$, $a_i(b_i, \mathbf{b}_{-i}) \geq a_i(b_i', \mathbf{b}_{-i})$ if $b_i \geq b_i'$.

If $1 \leq n \leq k$, we have $a_i(b_i, \mathbf{b}_{-i}) = a_i(b_i', \mathbf{b}_{-i}) = 1$, so the monotonicity holds. Now we consider $n > k$.

For convenience denote $w_i = e^{mb_i}$ and without loss of generality we assume $i = n$. Now For any map $X : \mathbb{N}_+ \to [0,1)$, vector $\mathbf{t}$ s.t. $0 = t_0 < t_1 < t_2 < \cdots < t_{n-1} < t_n = 1$, $B_0 \subseteq [0,1)$ and $k \leq n-1$, define an algorithm as Algorithm 1:

Now we denote $W_i = \frac{w_i}{\sum_{i=1}^n w_i}$ for $1 \leq i \leq n$, and

$$W_i' = \begin{cases} W_i, & i \leq n-1 \\ \frac{e^{mb_n'}}{\sum_{i=1}^n w_i}, & i = n. \end{cases}$$

Then, we define $\mathbf{t}, \mathbf{t}'$ as

$$t_i = \sum_{j=1}^{i} W_j, \quad 0 \leq i \leq n$$

$$t_i' = \begin{cases} \sum_{j=1}^{i} W_j', & 0 \leq i \leq n \\ 1, & i = n+1. \end{cases}$$

**Algorithm 1** $Draw(X, \mathbf{t}, B_0, k)$

Input $X, \mathbf{t}, B_0, k$;
$B \leftarrow B_0$; $S \leftarrow \emptyset$;
$u \leftarrow 1$; $v \leftarrow 1$;
**while** $v \leq k$ **do**
    $x \leftarrow X(u)$;
    **if** $x \notin B$ **then**
        Find $i$ s.t. $x \in [t_{i-1}, t_i)$;
        $S \leftarrow S \cup i$;
        $v \leftarrow v + 1$;
    **end if**
    $B \leftarrow B \cup [t_{x-1}, t_x)$;
    $u \leftarrow u + 1$;
**end while**
Output $S$;

Then when $X$ is a *i.i.d.* uniform random sequence in $[0, 1)$, we can see that

- $Draw(X, \mathbf{t}, \emptyset, k)$ randomly samples $k$ items among $\{1, \cdots, n\}$ with weights $\{W_i\}$ without replacement.
- $Draw(X, \mathbf{t}', [t'_n, 1), k)$ randomly samples $k$ items among $\{1, \cdots, n\}$ with (relative) weights $\{W'_i\}_{i \in [n]}$ without replacement.

In fact, Algorithm 1 performs random drawing without replacement in the following way. Every round an item in $\{1, \cdots, n\}$ is drawn, and in the second scenario the total weights is less than 1 so that a "placeholder" item $n+1$ with weight $1 - t'_n$ is added. If the item is already drawn or is the "placeholder", we draw again; other wise, we finalize it and add it to $S$.

In the rest of the proof, we prove that

$$\begin{aligned}&\Pr[n \in Draw(X, \mathbf{t}, \emptyset, k)]\\ &\quad \geq \Pr[n \in Draw(X, \mathbf{t}', [t'_n, 1), k)]\end{aligned}$$

by actually showing

$$n \in Draw(X, \mathbf{t}', [t'_n, 1), k) \Rightarrow n \in Draw(X, \mathbf{t}, \emptyset, k).$$

In fact, assume $n \in Draw(X, \mathbf{t}', [t'_n, 1), k)$. By the time the drawing process $Draw(X, \mathbf{t}', [t'_n, 1), k)$ stops, if no value $X(u) \in [t'_n, 1)$ is obtained, then $Draw(X, \mathbf{t}, \emptyset, k)$ has exactly the same outcome, so it also contains $n$.

If in some round $X(u) \in [t'_n, 1)$ is obtained in $Draw(X, \mathbf{t}', [t'_n, 1), k$, we consider the first round that happens.

Before that round, $Draw(X, \mathbf{t}, \emptyset, k)$ have the same outcome, so it is not stopped either. In that round, $Draw(X, \mathbf{t}, \emptyset, k)$ adds $n$ to $S$, so $n \in Draw(X, \mathbf{t}, \emptyset, k)$.

So we have shown that $n \in Draw(X, \mathbf{t}', [t'_n, 1), k) \Rightarrow n \in Draw(X, \mathbf{t}, \emptyset, k)$, implying the monotonicity of the allocation rule.

**EC.4.4.2. Proof of UIR and BF.** From Lemma 1, similar to the case of block size 1, we essentially need to derive a lower bound on $\frac{\partial a_i(t, \mathbf{b}_{-i})}{\partial t}$, in order to lower bound the total payment. Therefore, we only need to analyze the partial derivative of $\delta_t(i; j)$ on $w_i$.

When we fix $j$ and $\mathbf{b}_{-i}$ (i.e., $\mathbf{w}_{-i}$), we can regard $\delta_t(i; j)$ as a function of $w_i$. Here we make a notation of $X_s$ for $0 \le s \le k-1$ as

$$X_s = W - w_i - \sum_{z=1}^{s} w_{j_z}, \tag{EC.96}$$

then $X_s$ is a constant.

From Eq. (24) we get (note that $W - \sum_{z=1}^{s} w_{j_s} = X_s + w_i$)

$$\frac{\partial \delta_t(i; j)}{\partial w_i} = \left( \prod_{s=1}^{t-1} w_{j_s} \right) \cdot \frac{\partial}{\partial w_i} \frac{w_i}{\prod_{s=0}^{t-1} (X_s + w_i)}, \tag{EC.97}$$

and

$$\begin{aligned}
&\frac{\partial}{\partial w_i} \frac{w_i}{\prod_{s=0}^{t-1} (X_s + w_i)} \\
&= \frac{\partial}{\partial w_i} \left( w_i \cdot \prod_{s=0}^{t-1} \frac{1}{X_s + w_i} \right) && \text{(EC.98)} \\
&= \prod_{s=0}^{t-1} \frac{1}{X_s + w_i} + w_i \cdot \frac{\partial}{\partial w_i} \prod_{s=0}^{t-1} \frac{1}{X_s + w_i} && \text{(EC.99)} \\
&= \prod_{s=0}^{t-1} \frac{1}{X_s + w_i} - w_i \cdot \left( \sum_{s=0}^{t-1} \frac{1}{X_s + w_i} \right) \cdot \left( \prod_{s=0}^{t-1} \frac{1}{X_s + w_i} \right) && \text{(EC.100)} \\
&= \left( \prod_{s=0}^{t-1} \frac{1}{X_s + w_i} \right) \cdot \left( 1 - w_i \sum_{s=0}^{t-1} \frac{1}{X_s + w_i} \right) && \text{(EC.101)}
\end{aligned}$$

Notice that $X_s + w_i$ is a sum of $(n - s)$ weights, each one no less than 1, so $\frac{1}{X_s + w_i} \le \frac{1}{n-s} \le \ln \frac{n-s}{n-s-1}$, and $w_i = e^{m b_i} \le e^m$. Therefore,

$$1 - w_i \sum_{s=0}^{t-1} \frac{1}{X_s + w_i} \geq 1 - e^m \sum_{s=0}^{t-1} \ln \frac{n-s}{n-s-1} \tag{EC.102}$$

$$= 1 - e^m \ln \frac{n}{n-t}. \tag{EC.103}$$

Denote

$$D(m, \lambda) = 1 - e^m \ln \frac{\lambda}{\lambda - 1}, \tag{EC.104}$$

then $\forall \frac{n}{k} < \frac{e}{e-1}$, $\exists m > 0$ s.t. $D\left(m, \frac{n}{k}\right) > 0$.

Therefore, from Eq. (EC.97) we have

$$\frac{\partial \delta_t(i;j)}{\partial w_i} \geq D\left(m, \frac{n}{k}\right) \left(\prod_{s=1}^{t-1} w_{j_s}\right) \left(\prod_{s=0}^{t-1} \frac{1}{X_s + w_i}\right) \tag{EC.105}$$

$$= D\left(m, \frac{n}{k}\right) \cdot \frac{w_{j_1}}{X_0 + w_i} \cdot \frac{w_{j_2}}{X_1 + w_i} \cdot \cdots \cdot \frac{1}{X_{t-1} + w_i}. \tag{EC.106}$$

We notice that $\frac{w_{j_1}}{X_0+w_i} \cdot \frac{w_{j_2}}{X_1+w_i} \cdot \cdots \cdot \frac{w_{j_{t-1}}}{X_{t-2}+w_i}$ is just the probability that the sampling outcome of the first $t-1$ rounds are $(j_1, j_2, \cdots, j_{t-1})$, denoted as $P(j_{[t-1]})$. Furthermore, from $X_{t-1} + w_i \leq e^m \cdot n$, we have

$$\frac{\partial \delta_t(i;j)}{\partial w_i} \geq \frac{D\left(m, \frac{n}{k}\right)}{e^m n} P(j_{[t-1]}). \tag{EC.107}$$

Therefore from Eq. (23):

$$\frac{\partial \delta_t(i)}{\partial w_i} = \sum_{j \in J_t(i)} \frac{\partial \delta_t(i;j)}{\partial w_i} \tag{EC.108}$$

$$\geq \frac{D\left(m, \frac{n}{k}\right)}{e^m n} \sum_{j \in J_t(i)} P(j_{[t-1]}). \tag{EC.109}$$

For $j \in J_t(i)$, we observe that $j_{[t-1]}$ iterates through all $(t-1)$-permutations of $[n]$ that does not contain element $i$. Therefore, $\sum_{j \in J_t(i)} P(j_{[t-1]})$ is the probability that $i$ is not chosen in the first $(t-1)$ rounds.

To compute the probability that $i$ is not chosen in the first $(t-1)$ rounds, we consider each round. In each round, there are at least $(n-k)$ users each with weight at least 1, and user $i$ has weight at most $e^m$, so $i$ is chosen with probability at most $\frac{e^m}{n-k}$. Therefore for $t$ rounds, the probability that $i$ is not ever chosen is at most $\left(1 - \frac{e^m}{n-k}\right)^t \geq \left(1 - \frac{e^m}{n-k}\right)^k = (1 - o(1))e^{-\frac{e^m k}{n-k}}$. That implies:

$$\frac{\partial \delta_t(i)}{\partial w_i} \geq (1-o(1))\frac{D\left(m,\frac{n}{k}\right)}{e^m n}e^{-\frac{e^m k}{n-k}}, \tag{EC.110}$$

so

$$\frac{\partial a_i(b_i,\mathbf{b}_{-i})}{\partial b_i} = \frac{\partial w_i}{\partial b_i}\cdot\frac{\partial a_i(b_i,\mathbf{b}_{-i})}{\partial w_i} \tag{EC.111}$$

$$= me^{mb_i}\cdot\sum_{t=1}^{k}\frac{\partial \delta_t(i)}{\partial w_i} \tag{EC.112}$$

$$\geq me^{mb_i}\cdot\sum_{t=1}^{k}\left((1-o(1))\frac{D\left(m,\frac{n}{k}\right)}{e^m n}e^{-\frac{e^m k}{n-k}}\right) \tag{EC.113}$$

$$= \frac{k}{n}\left((1-o(1))me^{mb_i}\frac{D\left(m,\frac{n}{k}\right)}{e^m}e^{-\frac{e^m k}{n-k}}\right) \tag{EC.114}$$

For any fixed $\lambda_0 > \frac{e}{e-1}$, let $\lambda = \frac{n}{k}$. If $\lambda \geq \lambda_0$, let

$$m = m_{\#}(\lambda_0) = \min\left\{\frac{1}{2}\ln\frac{1}{\ln\frac{\lambda_0}{\lambda_0-1}}, 1\right\} \tag{EC.115}$$

be a constant. Then we have:

$$D(m,\lambda) = \max\left\{1-\sqrt{\ln\frac{\lambda}{\lambda-1}}, 1-e\ln\frac{\lambda}{\lambda-1}\right\}. \tag{EC.116}$$

Because $m_{\#}(\cdot)$ and $D(m,\cdot)$ are non-decreasing, we have

$$\frac{\partial a_i(b_i,\mathbf{b}_{-i})}{\partial t} \geq \frac{k}{n}\left((1-o(1))me^{mb_i}\frac{D\left(m,\frac{n}{k}\right)}{e^m}e^{-\frac{e^m k}{n-k}}\right) \tag{EC.117}$$

$$\geq \frac{k}{n}\left((1-o(1))m\frac{D\left(m,\lambda_0\right)}{e}e^{-\frac{e^m}{\lambda_0-1}}\right). \tag{EC.118}$$

Because $m, \lambda_0, D(m,\lambda_0)$ are all positive constants, we get

$$\frac{\partial a_i(b_i,\mathbf{b}_{-i})}{\partial t} \geq \frac{k}{n}f(\lambda_0)(1-o(1)). \tag{EC.119}$$

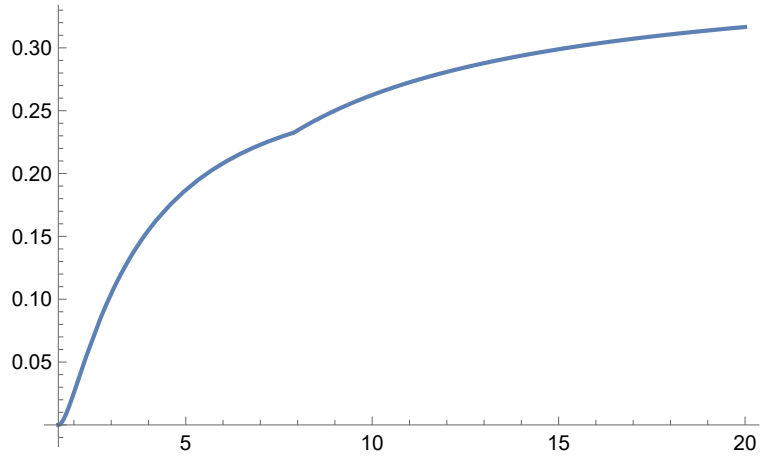


**Figure EC.1** The plot of $f(\cdot)$.

Therefore, from Lemma 1 and $p_i(0,\mathbf{b}_{-i})=0$, we get

$$a_i(b_i,\mathbf{b}_{-i})p_i(b_i,\mathbf{b}_{-i}) = \int_0^{b_i} t\frac{\partial a_i(t,\mathbf{b}_{-i})}{\partial t}dt \tag{EC.120}$$

$$\geq \int_0^{b_i} t\frac{k}{n}f(\lambda_0)(1-o(1))dt \tag{EC.121}$$

$$= f(\lambda_0)\Theta\left(\frac{k}{n}b_i^2\right). \tag{EC.122}$$

Here, the expression of $f(\cdot)$ is given by

$$f(\lambda) = \frac{m_{\#}(\lambda)D(m_{\#}(\lambda),\lambda)}{e^{m_{\#}(\lambda)}} \tag{EC.123}$$

and can be plotted as in Figure EC.1. It can be noticed that $f(\cdot)$ is monotonic increasing and

$$\lim_{\lambda\to+\infty} f(\lambda) = \frac{1}{e}. \tag{EC.124}$$

Then, when we let $\tilde{p}_i(b_i,\mathbf{b}_{-i}) = p_i(b_i,\mathbf{b}_{-i}) + \frac{\theta_i(b_i,\mathbf{b}_{-i})}{a_i(b_i,\mathbf{b}_{-i})}$ while using the variation term of Eqs. (19-20), similar to the argument of Eqs. (EC.55-EC.63), we can get the UIR and BF properties.

**Detailed constant analysis.**

From the assumption that $n\geq 30$ and $n > \frac{e}{e-1}k$, we have $n-k\geq 3 > e \geq e^m$. Since

$$(1-\alpha)^k = (1+\frac{\alpha}{1-\alpha})^{-k} \geq e^{-\frac{k\alpha}{1-\alpha}},\ \ \alpha\in[0,1)$$

we have

$$\left(1-\frac{e^m}{n-k}\right)^k \geq e^{-\frac{e^m k}{n-k-e^m}}. \tag{EC.125}$$

Then we get that

$$\frac{\partial \delta_t(i)}{\partial w_i} \geq \frac{D\left(m,\frac{n}{k}\right)}{e^m n} e^{-\frac{e^m k}{n-k-e^m}}, \tag{EC.126}$$

Since $n \geq 30$, we have

$$\begin{aligned}
\frac{\partial a_i(b_i,\mathbf{b}_{-i})}{\partial t} &\geq \frac{k}{n}\left(me^{mb_i}\frac{D\left(m,\frac{n}{k}\right)}{e^m}e^{-\frac{e^m k}{n-k-e^m}}\right) && \text{(EC.127)}\\
&> \frac{k}{n}\left(me^{mb_i}\frac{D\left(m,\frac{n}{k}\right)}{e^m}e^{-\frac{e^m k}{(n-3)-k}}\right) && \text{(EC.128)}\\
&\geq \frac{k}{n}\left(me^{mb_i}\frac{D\left(m,\frac{n}{k}\right)}{e^m}e^{-\frac{e^m k}{0.9n-k}}\right) && \text{(EC.129)}\\
&\geq \frac{k}{n}\left(m\frac{D\left(m,\lambda_0\right)}{e^m}e^{-\frac{e}{0.9\lambda_0-1}}\right) && \text{(EC.130)}\\
&= \frac{k}{n}\left(f(\lambda_0)e^{-\frac{e}{0.9\lambda_0-1}}\right). && \text{(EC.131)}
\end{aligned}$$

Here, we can let

$$g(\lambda) = ef(\lambda)e^{-\frac{e}{0.9\lambda-1}}, \tag{EC.132}$$

then $g$ is increasing and

$$\lim_{\lambda\to\infty} g(\lambda) = 1. \tag{EC.133}$$

It holds that

$$\begin{aligned}
a_i(b_i,\mathbf{b}_{-i})p_i(b_i,\mathbf{b}_{-i}) &= \int_0^{b_i} t\frac{\partial a_i(t,\mathbf{b}_{-i})}{\partial t}dt && \text{(EC.134)}\\
&\geq \frac{g(\lambda)}{2e}\cdot\frac{k}{n}b_i^2. && \text{(EC.135)}
\end{aligned}$$

Similar to the argument of Eqs. (EC.55-EC.63), the UIR and BF hold when

$$h_* = g(\lambda_0)\cdot\frac{2kc_\rho(n-1)}{en^2}. \tag{EC.136}$$

**EC.4.4.3. Proof of U-SP.** Since the variation term of the mechanism for block size $k$ has the same form as block size 1, we can show that the effects of the variation term do not influence the U-SP property in the same way as Appendix EC.4.3.2. Furthermore, because fake transactions have zero valuation and non-negative payment, we only need to prove the following proposition:

PROPOSITION EC.1. *For any user $i$, adding a fake bid will not benefit her utility in the Auxiliary Mechanism $M$ for block size $k$.*

Actually when $p_i(0, \mathbf{b}_{-i}) = 0$, the payment function in Myerson's Lemma has an equivalent form (Chung and Shi, 2023):

$$a_i(b_i, \mathbf{b}_{-i}) p_i(b_i, \mathbf{b}_{-i}) = a_i(b_i, \mathbf{b}_{-i}) b_i - \int_0^{b_i} a_i(t, \mathbf{b}_{-i}) dt. \tag{EC.137}$$

Therefore, the utility of user $i$ when truthfully bidding in the auxiliary mechanism is:

$$u_i(b_i, \mathbf{b}_{-i}; b_i) = \int_0^{b_i} a_i(t, \mathbf{b}_{-i}) dt. \tag{EC.138}$$

Now we only need to show that when we inject a fake transaction, the probability that a user (bidding arbitrary $t$) is confirmed would not increase, as the following lemma:

LEMMA EC.4. *In a weighted random sampling without replacement, if we add a new item, the probability that any already existing item is chosen does not increase.*

*Proof.* Consider the Algorithm 1. Now we assume there are $n$ items $1, \cdots, n$ with weights $w_1, \cdots, w_n$ and without loss of generality we assume $\sum_{i=1}^{n} = 1$, and define $t_j = \sum_{i=1}^{j} w_i$, then when $X$ is a *i.i.d.* uniform random sequence in $[0, 1)$, we can see that

- $Draw(X, \mathbf{t}, \emptyset, k)$ randomly samples $k$ items among $\{1, \cdots, n\}$ without replacement.
- $Draw(X, \mathbf{t}, [t_{n-1}, 1), k)$ randomly samples $k$ items among $\{1, \cdots, n-1\}$ without replacement.

We recall that Algorithm 1 performs random drawing without replacement in the following way. Every round an item in $\{1, \cdots, n\}$ is drawn. If the item is already drawn or does not exist, we draw again; otherwise, we finalize it and add it to $S$.

In the rest of the proof, we prove that $\forall i \in \{1, \cdots, n-1\}$,

$$\begin{aligned} &\Pr[i \in Draw(X, \mathbf{t}, [t_{n-1}, 1), k)] \\ &\quad \geq \Pr[i \in Draw(X, \mathbf{t}, \emptyset, k)] \end{aligned}$$

by actually showing

$$i \in Draw(X, \mathbf{t}, \emptyset, k) \Rightarrow i \in Draw(X, \mathbf{t}, [t_{n-1}, 1), k).$$

In fact, for fixed $X$, because

$$P \subseteq Q \quad \Rightarrow \quad P \cup R \subseteq Q \cup R,$$

after each round of drawing, the $B$ in $Draw(X, \mathbf{t}, \emptyset, k)$ is always a subset of the $B$ in $Draw(X, \mathbf{t}, [t_{n-1}, 1), k)$. Therefore, $Draw(X, \mathbf{t}, [t_{n-1}, 1), k)$ would draw no less rounds than $Draw(X, \mathbf{t}, \emptyset, k)$.

Besides, we see that when $i \neq n$, $i$ is drawn if and only if a $x \in [t_{i-1}, t_i)$ appears by the time the drawing completes, so if $i \in Draw(X, \mathbf{t}, \emptyset, k)$, we indeed have $i \in Draw(X, \mathbf{t}, [t_{n-1}, 1), k)$.

Hence we have shown that $\Pr[i \in Draw(X, \mathbf{t}, [t_{n-1}, 1), k)] \geq \Pr[i \in Draw(X, \mathbf{t}, \emptyset, k)]$.

□

From Lemma EC.4 we prove that our TFM for block size $k$ is U-SP.

For the corresponding constants, we note that in the mechanism of block size 1, the expected payment of a user bidding $b_i$ is lower bounded by $\sim \frac{b_i^2}{2en}$ and $h \lesssim \frac{2c_\rho}{en}$, and it is $\left(C, O(\frac{1}{1-C})\right)$-U-SP for any $C < 1$. In the mechanism of block size $k$, the expected payment of user $i$ is lower bounded by $g(\lambda_0)k \cdot \frac{b_i^2}{2en}$, and $h \lesssim g(\lambda_0)k \cdot \frac{2c_\rho}{en}$. Hence, it can be shown in a similar way that Mechanism 3 is also $\left(C, O(\frac{1}{1-C})\right)$-U-SP for any $C < 1$.

### EC.4.5. Proof of Theorem 5

Without loss of generality, we can assume the miner will conduct the deviation in this way: in Stage 1 the miner deletes transactions one by one, and then in Stage 2 inject fake transactions one by one. Then we introduce two lemmas before proving the theorem: firstly analyze the robustness of the miner revenue function $\tilde{r}$, then upper bound the advantage the miner may gain in each stage.

**EC.4.5.1. Robustness analysis of the miner revenue function.** Firstly, we assume that the mean of $b_i^2$ is close to $c_\rho = \Theta(1)$, which holds with high probability with large $n$ and $\Delta = o(n)$. Here we define $H = Lc_\rho$, then we prove the following lemma, showing that as long as the average of $\{b_i^2\}$ is close to $c_\rho$, adding or deleting a transaction would not have a significant impact on the miner revenue:

LEMMA EC.5. *If* $\left|\frac{\sum_{i=1}^n b_i^2}{n} - c_\rho\right| < \delta$*, and recall that*

$$\tilde{r}(\mathbf{b}) = \frac{Hk}{2n}\left(\sum_{i=1}^n b_i^2 - \frac{\sum_{1 \leq i < j \leq n} b_i^2 b_j^2}{c_\rho(n-1)}\right), \tag{EC.139}$$

*then for* $n \geq 3$*, there exists a constant* $C_{LEC.5}$ *s.t.* $\forall j \in [n]$*,*

$$|\tilde{r}(\mathbf{b}_{-j}) - \tilde{r}(\mathbf{b})| \leq C_{LEC.5}\delta \cdot \frac{Hk}{c_\rho n}. \tag{EC.140}$$

*Proof.* Without loss of generality we assume $j = n$. Then, we compute that

$$\begin{aligned}
&\frac{\tilde{r}(\mathbf{b}_{-n}) - \tilde{r}(\mathbf{b})}{\frac{1}{2}Hk} \\
&= \frac{\sum_{i=1}^{n-1} b_i^2}{n-1} - \frac{\sum_{1\le i<j\le n-1} b_i^2 b_j^2}{c_\rho(n-2)(n-1)} \\
&\qquad - \frac{\sum_{i=1}^{n} b_i^2}{n} + \frac{\sum_{1\le i<j\le n} b_i^2 b_j^2}{c_\rho(n-1)n} && \text{(EC.141)} \\
&= \frac{1}{n(n-1)} \sum_{i=1}^{n-1} b_i^2 - \frac{b_n^2}{n} \\
&\qquad - \frac{2\sum_{1\le i<j\le n-1} b_i^2 b_j^2}{c_\rho n(n-1)(n-2)} + \frac{b_n^2 \sum_{i=1}^{n-1} b_i^2}{c_\rho n(n-1)} && \text{(EC.142)} \\
&= \frac{1}{n(n-1)} \left( \sum_{i=1}^{n-1} b_i^2 - \frac{2\sum_{1\le i<j\le n-1} b_i^2 b_j^2}{c_\rho(n-2)} \right) \\
&\qquad + \frac{b_n^2}{n} \left( \frac{\sum_{i=1}^{n-1} b_i^2}{c_\rho(n-1)} - 1 \right) && \text{(EC.143)}
\end{aligned}$$

From the assumption we see that $\left| \frac{\sum_{i=1}^{n-1} b_i^2}{c_\rho(n-1)} - 1 \right| = O(\delta/c_\rho)$ and $b_n^2 \le 1$, we have

$$\left| \frac{b_n^2}{n} \left( \frac{\sum_{i=1}^{n-1} b_i^2}{c_\rho(n-1)} - 1 \right) \right| = O(\delta/c_\rho n). \tag{EC.144}$$

Now we only need to prove that $\left| \sum_{i=1}^{n-1} b_i^2 - \frac{2\sum_{1\le i<j\le n-1} b_i^2 b_j^2}{c_\rho(n-2)} \right| = O(\delta n/c_\rho)$.

In fact, we notice that

$$2 \sum_{1\le i<j\le n-1} b_i^2 b_j^2 = \left( \sum_{i=1}^{n-1} b_i^2 \right)^2 - \sum_{i=1}^{n-1} b_i^4. \tag{EC.145}$$

Hence,

$$\begin{aligned}
&\left| \sum_{i=1}^{n-1} b_i^2 - \frac{2\sum_{1\le i<j\le n-1} b_i^2 b_j^2}{c_\rho(n-2)} \right| \\
&= \left| \sum_{i=1}^{n-1} b_i^2 - \frac{\left(\sum_{i=1}^{n-1} b_i^2\right)^2 - \sum_{i=1}^{n-1} b_i^4}{c_\rho(n-2)} \right| && \text{(EC.146)} \\
&= \left| \sum_{i=1}^{n-1} b_i^2 \cdot \left( 1 - \frac{\sum_{i=1}^{n-1} b_i^2}{c_\rho(n-2)} \right) - \frac{\sum_{i=1}^{n-1} b_i^4}{c_\rho(n-2)} \right| && \text{(EC.147)} \\
&\le \sum_{i=1}^{n-1} b_i^2 \cdot \left| \left( 1 - \frac{\sum_{i=1}^{n-1} b_i^2}{c_\rho(n-2)} \right) \right| + \left| \frac{\sum_{i=1}^{n-1} b_i^4}{c_\rho(n-2)} \right| && \text{(EC.148)} \\
&= O(n) \cdot O(\delta/c_\rho) + O(1) && \text{(EC.149)} \\
&= O(\delta n/c_\rho). && \text{(EC.150)}
\end{aligned}$$

□

**EC.4.5.2. Advantage analysis of** M−TD**.** Now we analyze the advantage in revenue the miner can get after conducting all the transaction deletions. Intuitively, we first show that for large $n$ and $\delta = \omega(\Delta/n)$, the condition $\left|\frac{\sum_{i=1}^n b_i^2}{n} - c_\rho\right| < \delta$ holds with high probability at each step in the $\Delta = o(n)$ deletions. Then we use Lemma EC.5 to bound the advantage.

First, we deduce the following concentration lemma.

LEMMA EC.6. *For any* i.i.d. *random variable* $\{b_i\}$ *in* $[0,1]$ *satisfying* $\mathbb{E}[b_i^2] = c_\rho$ *and given* $\delta > 0$*, we have*

$$\Pr\left[\left|\frac{\sum_{i=1}^n b_i^2}{n} - c_\rho\right| \geq \frac{\delta}{2}\right] \leq 2\exp\left(-\frac{\delta^2 n}{2}\right). \tag{EC.151}$$

*Proof.* Hoeffding's inequality (Hoeffding, 1963) states that when $\{x_i\}$ are independent random variables with $l_i \leq x_i \leq r_i$, and denoting $s_n = \sum_{i=1}^n x_i$, it holds that

$$\Pr[|s_n - \mathbb{E}[s_n]| \geq t] \leq 2\exp\left(-\frac{2t^2}{\sum_{i=1}^n (r_i - l_i)^2}\right). \tag{EC.152}$$

Let $x_i = b_i^2, l_i = 0, r_i = 1, t = \frac{\delta n}{2}$, then $\mathbb{E}[s_n] = c_\rho n$ and we get:

$$\Pr\left[\left|\sum_{i=1}^n b_i^2 - c_\rho n\right| \geq \frac{\delta n}{2}\right] \leq 2\exp\left(-\frac{\frac{1}{2}\delta^2 n^2}{n}\right), \tag{EC.153}$$

i.e.,

$$\Pr\left[\left|\frac{\sum_{i=1}^n b_i^2}{n} - c_\rho\right| \geq \frac{\delta}{2}\right] \leq 2\exp\left(-\frac{\delta^2 n}{2}\right). \tag{EC.154}$$

□

Then we upper bound the impact of transaction deletion on the average of $\{b_i^2\}$. Without loss of generality, we assume the miner deletes $b_n, b_{n-1}, \cdots, b_{n-t+1}$ sequentially[7] for $t \leq \Delta = o(n)$, and we want that $\left|\frac{\sum_{i=1}^n b_i^2}{n} - \frac{\sum_{i=1}^{n-t+1} b_i^2}{n-t+1}\right| \leq \frac{\delta}{2}$.

In fact, we have $\mathbf{b}_i \in [0,1]$, so

$$\frac{\sum_{i=1}^n b_i^2}{n-t+1} \leq \frac{\sum_{i=1}^{n-t+1} b_i^2}{n-t+1} \leq \frac{(\sum_{i=1}^n b_i^2) - t}{n-t+1} \tag{EC.155}$$

Therefore, for $t \le \Delta$, There exists constant $C_{MIC1}$ s.t. for $n \ge C_{MIC1}\frac{\Delta}{\delta}$ and $n-t+1 \ge 3$, we indeed have

$$\left| \frac{\sum_{i=1}^{n} b_i^2}{n} - \frac{\sum_{i=1}^{n-t+1} b_i^2}{n-t+1} \right| \le \frac{\delta}{2}. \tag{EC.156}$$

Combined with Lemma EC.5, we deduce that when $n \ge C_{MIC1}\frac{\Delta}{\delta}$, with probability at least $1 - 2\exp(\delta^2 n/2)$, the advantage of M−TD with $t$ deletions is at most $O(\delta)\cdot\frac{Hkt}{c_\rho n}$. We also see that when we require $\delta \in (0,1]$, then because $\Delta \ge 1$, $n-t+1 \ge 3$ is guaranteed. Formally:

THEOREM EC.2 **(Our mechanism is almost-{M−TD}-proof).** *Denote $B_\Delta^-(\mathbf{b})$ as the family of all bidding vectors generated via deleting at most $\Delta$ bids from $\mathbf{b}$. Then for universal constant $C_{MIC1} > 0$ and $\delta \in (0,1], n \ge C_{MIC1}\frac{\Delta}{\delta}$, we have*

$$\begin{aligned} &\Pr_{\mathbf{b}}\left[\sup_{\mathbf{b}'\in B_\Delta^-(\mathbf{b})} (\tilde{r}(\mathbf{b}') - \tilde{r}(\mathbf{b})) > O(\delta)\frac{Hk\Delta}{c_\rho n}\right] \\ &\le 2\exp\left(-\frac{\delta^2 n}{2}\right). \end{aligned} \tag{EC.157}$$

**EC.4.5.3. Advantage analysis of M−FT.** Finally we analyze the miner advantage of the miner's injection of fake transactions. The advantage a miner can get consists of two parts: increase of the miner revenue $\tilde{r}(\cdot)$, and the utility of fake identities. We notice that the robustness analysis of $\tilde{r}(\cdot)$ not only holds for transaction deletion, but also injection. So we can upper bound the miner advantage in the immediate revenue via very similar arguments. Formally, we have (proof omitted):

COROLLARY EC.1. *Denote $B_\Delta(\mathbf{b})$ as the family of all bidding vectors generated via injecting and deleting a total of at most $\Delta$ bids to/from $\mathbf{b}$. Then for universal constants $C_{M0}, C_{M0'}, C_{MIC2}, C_{MIC3} > 0$ and $\delta \in (0,1], n \ge C_{MIC2}\frac{\Delta}{\delta}$,*

$$\begin{aligned} &\Pr_{\mathbf{b}}\left[\sup_{\mathbf{b}'\in B_\Delta(\mathbf{b})} (\tilde{r}(\mathbf{b}') - \tilde{r}(\mathbf{b})) > C_{M0}\delta\frac{Hk\Delta}{c_\rho n}\right] \\ &\le C_{M0'}\exp\left(-C_{MIC3}\delta^2 n\right). \end{aligned} \tag{EC.158}$$

Hence, we only need to further upper bound the advantage from the utility of fake identities. We notice that the fake transactions do not have intrinsic values, so the valuations of fake transactions are zero.

Now we consider the total utility of fake identities. Because the valuations are zero, their total utility are just the opposite of their payment. So for $b'_j \in \mathbf{b}' \backslash \mathbf{b}$, the utility of identity $j'$ is

$$\begin{aligned}
&\tilde{u}_j(b'_j, \mathbf{b}'_{-j}; 0) \\
&= -a_j(b'_j, \mathbf{b}'_{-j})\tilde{p}_j(b'_j, \mathbf{b}'_{-j}) && \text{(EC.159)} \\
&= -a_j(b'_j, \mathbf{b}'_{-j})p_j(b'_j, \mathbf{b}'_{-j}) - \theta_j(b'_j, \mathbf{b}'_{-j}). && \text{(EC.160)}
\end{aligned}$$

From Eq. (EC.122)[8], and denote that the number of bids in $\mathbf{b}'$ is $n' \in [n-\Delta, n+\Delta]$, we get:

$$a_j(b'_j, \mathbf{b}'_{-j})p_j(b'_j, \mathbf{b}'_{-j}) = \Theta\left(\frac{k{b'_j}^2}{n}\right). \tag{EC.161}$$

From $h = \frac{Hk}{n'}$ we get:

$$\theta_j(b'_j, \mathbf{b}'_{-j}) = -\frac{Hk}{2n}{b'_j}^2\left(\frac{\sum_{i\neq j} {b'_i}^2}{c_\rho(n'-1)} - 1\right) \tag{EC.162}$$

Similar to the argument in Appendix EC.4.5.2, as long as $c_\rho = \Theta(1)$ and $\left|\frac{\sum_{i=1}^n b_i^2}{n} - c_\rho\right| < O(\delta)$, we have $\left|\frac{\sum_{i\neq j} {b'_i}^2}{c_\rho(n'-1)} - 1\right| \leq O(\delta/c_\rho)$ for any $(\mathbf{b}' \in B_\Delta(b), j \in \mathbf{b}' \backslash \mathbf{b})$, which happens with probability at least $1 - \exp(-\Theta(\delta^2 n))$.

In this case, we have:

$$\left|\theta_j(b'_j, \mathbf{b}'_{-j})\right| \leq O(\delta) \cdot \frac{Hk}{c_\rho n}. \tag{EC.163}$$

Therefore, with probability at least $1 - \exp(-\Theta(\delta^2 n))$, for any $\mathbf{b}' \in B_\Delta(b)$

$$\begin{aligned}
&\sum_{b'_j \in \mathbf{b}' \backslash \mathbf{b}} \tilde{u}_j(b'_j, \mathbf{b}'_{-j}; 0) \\
&= \sum_{b'_j \in \mathbf{b}' \backslash \mathbf{b}} -a_j(b'_j, \mathbf{b}'_{-j})p_j(b'_j, \mathbf{b}'_{-j}) - \theta_j(b'_j, \mathbf{b}'_{-j}) && \text{(EC.164)} \\
&= \sum_{b'_j \in \mathbf{b}' \backslash \mathbf{b}} \left(-\Theta\left(\frac{k{b'_j}^2}{n}\right) + O(\delta) \cdot \frac{Hk}{c_\rho n}\right) && \text{(EC.165)} \\
&\leq \sum_{b'_j \in \mathbf{b}' \backslash \mathbf{b}} O(\delta) \cdot \frac{Hk}{c_\rho n} && \text{(EC.166)} \\
&\leq O(\delta) \cdot \frac{Hk\Delta}{c_\rho n}. && \text{(EC.167)}
\end{aligned}$$

Combined with Corollary EC.1, we deduce that for universal constants $C_{M0}, C_{MIC2}, C_{MIC3} > 0$, $C_{M0'} > 1$ and $\delta \in (0,1], n \geq C_{MIC2}\frac{\Delta}{\delta}$,

$$\Pr_{\mathbf{b}}\left[\sup_{\mathbf{b}'\in B_\Delta(\mathbf{b})}\left(\tilde{r}(\mathbf{b}')-\tilde{r}(\mathbf{b})+\sum_{b'_j\in\mathbf{b}'\setminus\mathbf{b}}\tilde{u}_j(b'_j,\mathbf{b}'_{-j};0)\right) > C_{M0}\delta\cdot\frac{Hk\Delta}{c_\rho n}\right] < C_{M0'}\exp(-C_{MIC3}\delta^2 n). \tag{EC.168}$$

Particularly, we can let $\delta = (\Delta/n)^{1/3}$, then for $n \geq C_{MIC2}^{3/2}\Delta$,

$$\Pr_{\mathbf{b}}\left[\sup_{\mathbf{b}'\in B_\Delta(\mathbf{b})}\left(\tilde{r}(\mathbf{b}')-\tilde{r}(\mathbf{b})+\sum_{b'_j\in\mathbf{b}'\setminus\mathbf{b}}\tilde{u}_j(b'_j,\mathbf{b}'_{-j};0)\right) > C_{M0}\frac{Hk\Delta^{4/3}}{c_\rho n^{4/3}}\right] < C_{M0'}\exp(-C_{MIC3}\Delta^{2/3}n^{1/3}). \tag{EC.169}$$

Therefore, because $\Delta \geq 1$, for any $\epsilon > 0$ when $n \geq \max\{C_{MIC2}^{3/2}\Delta, C_{MIC3}^{-3}\log^3\frac{C_{M0'}}{\epsilon}\}$, we have

$$\Pr_{\mathbf{b}}\left[\sup_{\mathbf{b}'\in B_\Delta(\mathbf{b})}\left(\tilde{r}(\mathbf{b}')-\tilde{r}(\mathbf{b})+\sum_{b'_j\in\mathbf{b}'\setminus\mathbf{b}}\tilde{u}_j(b'_j,\mathbf{b}'_{-j};0)\right) > C_{M0}\frac{Hk\Delta^{4/3}}{c_\rho n^{4/3}}\right] < \epsilon. \tag{EC.170}$$

For $\epsilon \in (0, 1/2)$, we have

$$\begin{aligned}\log\frac{C_{M0'}}{\epsilon} &= \log C_{M0'} + \log\frac{1}{\epsilon}\\ &= \log\frac{1}{\epsilon}\left(1+\frac{\log C_{M0'}}{\log\frac{1}{\epsilon}}\right)\\ &< \log\frac{1}{\epsilon}\left(1+\frac{\log C_{M0'}}{\log 2}\right).\end{aligned}$$

Just let $C_{M1} = C_{MIC2}^{3/2}$, $C_{M2} = C_{MIC3}^{-3}\left(1+\frac{\log C_{M0'}}{\log 2}\right)^3$, and from $H = Lc_\rho$, we have proven Theorem 5.

### EC.4.6. Proof of Theorem 6

For convenience we let $t = |\mathbf{b}| - 1$. Denote $M(\mathbf{a}, \mathbf{p}, r)$ and $T(\theta, \tilde{r})$ is the auxiliary-variation decomposition of an 1-SCP mechanism $\tilde{M}$, then from Lemma 1 and Lemma EC.3 we know that

$$\theta_i(b_i, \mathbf{b}_{-i}) - \theta_i(0, \mathbf{b}_{-i}) = \tilde{r}(b_i, \mathbf{b}_{-i}) - \tilde{r}(0, \mathbf{b}_{-i}). \tag{EC.171}$$

User $i$'s utility in $\tilde{M}$ is

$$\begin{aligned}
&\tilde{u}(b_i, \mathbf{b}_{-i}; v_i) \\
&= a_i(b_i, \mathbf{b}_{-i})(v_i - p_i(b_i, \mathbf{b}_{-i})) - \theta_i(b_i, \mathbf{b}_{-i}) && \text{(EC.172)} \\
&= u(b_i, \mathbf{b}_{-i}; v_i) - \theta_i(b_i, \mathbf{b}_{-i}). && \text{(EC.173)}
\end{aligned}$$

From U-BNIC of $\tilde{M}$ we know that $\mathbb{E}_{\mathbf{b}_{-i}}[\tilde{u}(b_i+\delta, \mathbf{b}_{-i}; b_i)] \le \mathbb{E}_{\mathbf{b}_{-i}}[\tilde{u}(b_i, \mathbf{b}_{-i}; b_i)]$ and $\mathbb{E}_{\mathbf{b}_{-i}}[\tilde{u}(b_i, \mathbf{b}_{-i}; b_i+\delta)] \le \mathbb{E}_{\mathbf{b}_{-i}}[\tilde{u}(b_i+\delta, \mathbf{b}_{-i}; b_i+\delta)]$, i.e.,

$$\begin{aligned}
&\mathbb{E}_{\mathbf{b}_{-i}}[u(b_i, \mathbf{b}_{-i}; b_i) - \theta_i(b_i, \mathbf{b}_{-i})] \\
&\ge \mathbb{E}_{\mathbf{b}_{-i}}[u(b_i+\delta, \mathbf{b}_{-i}; b_i) - \theta_i(b_i+\delta, \mathbf{b}_{-i})] && \text{(EC.174)} \\
&\mathbb{E}_{\mathbf{b}_{-i}}[u(b_i, \mathbf{b}_{-i}; b_i+\delta) - \theta_i(b_i, \mathbf{b}_{-i})] \\
&\le \mathbb{E}_{\mathbf{b}_{-i}}[u(b_i+\delta, \mathbf{b}_{-i}; b_i+\delta) - \theta_i(b_i+\delta, \mathbf{b}_{-i})]. && \text{(EC.175)}
\end{aligned}$$

From U-BNIC (implied by U-DSIC) of $M$ we get:

$$\begin{aligned}
\mathbb{E}_{\mathbf{b}_{-i}}[u(b_i, \mathbf{b}_{-i}; b_i)] &\ge \mathbb{E}_{\mathbf{b}_{-i}}[u(b_i+\delta, \mathbf{b}_{-i}; b_i)] && \text{(EC.176)} \\
\mathbb{E}_{\mathbf{b}_{-i}}[u(b_i, \mathbf{b}_{-i}; b_i+\delta)] &\le \mathbb{E}_{\mathbf{b}_{-i}}[u(b_i+\delta, \mathbf{b}_{-i}; b_i+\delta)]. && \text{(EC.177)}
\end{aligned}$$

By integration on $b_i$ for fixed $\mathbf{b}_{-i}$, we know that

$$\mathbb{E}_{\mathbf{b}_{-i}}[\theta_i(b_i, \mathbf{b}_{-i})] - \mathbb{E}_{\mathbf{b}_{-i}}[\theta_i(0, \mathbf{b}_{-i})] = 0. \quad \text{(EC.178)}$$

From NFL we know that $\theta_i(0, \mathbf{b}_{-i}) = 0$, so

$$\mathbb{E}_{\mathbf{b}_{-i}}[\theta_i(b_i, \mathbf{b}_{-i})] = 0. \quad \text{(EC.179)}$$

Combined with Eq. (EC.171), we know that

$$\begin{aligned}
&\mathbb{E}_{\mathbf{b}_{-i}}[\tilde{r}(b_i, \mathbf{b}_{-i}) - \tilde{r}(0, \mathbf{b}_{-i})] && \text{(EC.180)} \\
&= \mathbb{E}_{\mathbf{b}_{-i}}[\theta_i(b_i, \mathbf{b}_{-i}) - \theta_i(0, \mathbf{b}_{-i})] && \text{(EC.181)} \\
&= \mathbb{E}_{\mathbf{b}_{-i}}[\theta_i(b_i, \mathbf{b}_{-i})] = 0. && \text{(EC.182)}
\end{aligned}$$

From assumption we know that $\mathbb{E}_{\mathbf{b}_{-i}}[r(0,\mathbf{b}_{-i})] \le \mathbb{E}_{\mathbf{b}_{-i}}[r(\mathbf{b}_{-i})]$, so we have

$$\mathbb{E}_{\mathbf{b}}[\tilde{r}(b_i,\mathbf{b}_{-i})] = \mathbb{E}_{b_i}[\mathbb{E}_{\mathbf{b}_{-i}}[\tilde{r}(b_i,\mathbf{b}_{-i})]] \tag{EC.183}$$

$$= \mathbb{E}_{b_i}[\mathbb{E}_{\mathbf{b}_{-i}}[\tilde{r}(0,\mathbf{b}_{-i})]] \le \mathbb{E}_{b_i}[\mathbb{E}_{\mathbf{b}_{-i}}[\tilde{r}(\mathbf{b}_{-i})]] \tag{EC.184}$$

$$= \mathbb{E}_{\mathbf{b}_{-i}}[\tilde{r}(\mathbf{b}_{-i})]. \tag{EC.185}$$

Hence the expected revenue for $t+1$ users is at most the expected revenue for $t$ users. We notice that when there is zero user the expected revenue is non-positive, so by induction, the expected revenue for arbitrary $n$ users is non-positive.

## EC.4.7. Proof of Theorem 7

**Necessity.** Let $\forall b_i = 1$, then it has already been shown that $\tilde{r}(\mathbf{b}) = \Theta(k)\left(1-\frac{1}{2c_\rho}\right)$. If $c_\rho < \frac{1}{2}$, then in this case $\tilde{r}(\mathbf{b}) < 0$, violating MIR.

**Sufficiency.** Because $\forall b_i \in [0,1]$, we have $b_i^2 \ge b_i^4$. Therefore,

$$\tilde{r}(\mathbf{b}) = \Theta\left(\frac{k}{n}\right)\cdot\left(\sum_{i=1}^n b_i^2 - \frac{\sum_{1\le i<j\le n} b_i^2 b_j^2}{c_\rho(n-1)}\right) \tag{EC.186}$$

$$\ge \Theta\left(\frac{k}{n}\right)\cdot\left(\sum_{i=1}^n b_i^4 - \frac{\sum_{1\le i<j\le n} b_i^2 b_j^2}{c_\rho(n-1)}\right) \tag{EC.187}$$

$$= \Theta\left(\frac{k}{n}\right)\cdot\left(\left(1-\frac{1}{2c_\rho}\right)\sum_{i=1}^n b_i^4 + \frac{1}{4c_\rho(n-1)}\sum_{i=1}^n \left(b_i^2-b_j^2\right)^2\right). \tag{EC.188}$$

If $c_\rho \ge \frac{1}{2}$, then $1-\frac{1}{2c_\rho} \ge 0$, so $\tilde{r}(\mathbf{b})$ is lower bounded by a sum of squares. Therefore, $\tilde{r}(\mathbf{b})$ is non-negative for any $\mathbf{b}\in[0,1]^n$, proving the MIR property of the mechanism.

## EC.4.8. Proof of Theorem 8

We have that

$$\tilde{r}(\mathbf{b}) = \frac{h}{2}\cdot\left(\sum_{i=1}^n b_i^2 - \frac{\sum_{1\le i<j\le n} b_i^2 b_j^2}{c_\rho(n-1)}\right) \tag{EC.189}$$

$$= \frac{h}{2}\cdot\left(\sum_{i=1}^n b_i^2 - \frac{1}{2c_\rho(n-1)}\left(\left(\sum_{i=1}^n b_i^2\right)^2 - \sum_{i=1}^n b_i^4\right)\right). \tag{EC.190}$$

By the Cauchy–Schwarz inequality, we have $(\sum_{i=1}^n b_i^4)\cdot(\sum_{i=1}^n 1) \ge (\sum_{i=1}^n b_i^2)^2$, i.e.,

$$\sum_{i=1}^n b_i^4 \ge \frac{1}{n}\left(\sum_{i=1}^n b_i^2\right)^2. \tag{EC.191}$$

Therefore,

$$\tilde{r}(\mathbf{b}) \geq \frac{h}{2}\left(\sum_{i=1}^{n} b_i^2 - \frac{1}{2c_\rho n}\left(\sum_{i=1}^{n} b_i^2\right)^2\right) \tag{EC.192}$$

$$= \frac{h}{2}\sum_{i=1}^{n} b_i^2\left(1 - \frac{1}{2c_\rho n}\sum_{i=1}^{n} b_i^2\right) \tag{EC.193}$$

$$= \frac{hc_\rho n}{4}\left(1 - \frac{1}{c_\rho^2 n^2}\left(\sum_{i=1}^{n} b_i^2 - c_\rho n\right)^2\right). \tag{EC.194}$$

We know that $\mathbb{E}[\tilde{r}(\mathbf{b})] = \frac{hc_\rho n}{4}$, so

$$\frac{\tilde{r}(\mathbf{b})}{\mathbb{E}[\tilde{r}(\mathbf{b})]} \geq 1 - \frac{1}{c_\rho^2 n^2}\left(\sum_{i=1}^{n} b_i^2 - c_\rho n\right)^2. \tag{EC.195}$$

Hoeffding's inequality (Hoeffding, 1963) states that when $\{x_i\}$ are independent random variables with $l_i \leq x_i \leq r_i$, and denoting $s_n = \sum_{i=1}^{n} x_i$, it holds that

$$\Pr[|s_n - \mathbb{E}[s_n]| \geq t] \leq 2\exp\left(-\frac{2t^2}{\sum_{i=1}^{n}(r_i - l_i)^2}\right). \tag{EC.196}$$

We let $x_i = b_i^2, l_i = 0, r_i = 1, t = \sqrt{\frac{\lambda n}{2}}$, and get:

$$\Pr\left[\left|\sum_{i=1}^{n} b_i^2 - c_\rho n\right| \geq \sqrt{\frac{\lambda n}{2}}\right] \leq 2\exp(-\lambda). \tag{EC.197}$$

Combined with Eq. (EC.195), we get:

$$\Pr\left[\frac{\tilde{r}(\mathbf{b})}{\mathbb{E}[\tilde{r}(\mathbf{b})]} \leq 1 - \frac{\lambda}{c_\rho^2 n}\right] \leq 2\exp(-\lambda). \tag{EC.198}$$

## Endnotes

4. As long as there exists a mechanism whose outcome can achieve certain desired properties, we can indeed construct the equivalent truthful mechanism that both prevents agents from strategic behavior, and simplify the analysis as we can assume rational agents who seek to maximize their individual utilities will indeed follow the mechanism as we expect.

5. It is possible to prove a stronger statement: there exists no $\tilde{r}$ such that the TFM $(\mathbf{a}, \tilde{\mathbf{p}}, \tilde{r})$ is 1-SCP (where $\mathbf{a}$ and $\tilde{\mathbf{p}}$ are defined based on the first-price auction as in Section EC.3.1). Therefore, the does not exist a U-BNIC and 1-SCP TFM extension based on the first-price auction. We omit the detailed proof of this statement since it is not directly related to the construction and the analysis of our TFM.

6. We introduced a coefficient $\frac{1}{2}$ because we initially constructed the variation term via partial derivatives.
7. Notice that the argument holds for any subset and order of deletion, via re-permutations of $\{b_i\}$.
8. let $\lambda_0 = 1.582$ and compute $f(\lambda_0), m$ accordingly.

## References


Bertino, Elisa, Ahish Kundu, and Zehra Sura (2019). "Data transparency with blockchain and AI ethics". In: *Journal of Data and Information Quality (JDIQ)* 11.4, pp. 1–8.

Cassez, Franck, Joanne Fuller, and Aditya Asgaonkar (2022). "Formal Verification of the Ethereum 2.0 Beacon Chain". In: *International Conference on Tools and Algorithms for the Construction and Analysis of Systems*. Springer, pp. 167–182.

Chung, Hao and Elaine Shi (2023). "Foundations of transaction fee mechanism design". In: *Proceedings of the 2023 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*. SIAM, pp. 3856–3899.

Connell, E and J Drost (1983). "Conservative and divergence free algebraic vector fields". In: *Proceedings of the American Mathematical Society* 87.4, pp. 607–612.

Ferreira, Matheus V. X. and S. Matthew Weinberg (July 2020). "Credible, Truthful, and Two-Round (Optimal) Auctions via Cryptographic Commitments". In: *Proceedings of the 21st ACM Conference on Economics and Computation*. ACM. DOI: 10.1145/3391403.3399495. URL: https://doi.org/10.1145%2F3391403.3399495.

Hoeffding, Wassily (1963). "Probability Inequalities for Sums of Bounded Random Variables". In: *Journal of the American Statistical Association* 58.301, pp. 13–30.

Khalilov, Merve Can Kus and Albert Levi (2018). "A survey on anonymity and privacy in bitcoin-like digital cash systems". In: *IEEE Communications Surveys & Tutorials* 20.3, pp. 2543–2585.

Luntovskyy, Andriy and Dietbert Guetter (2018). "Cryptographic technology blockchain and its applications". In: *The International Conference on Information and Telecommunication Technologies and Radio Electronics*. Springer, pp. 14–33.

Myerson, Roger B (1979). "Incentive compatibility and the bargaining problem". In: *Econometrica: journal of the Econometric Society*, pp. 61–73.

— (1981). "Optimal auction design". In: *Mathematics of operations research* 6.1, pp. 58–73.

Roughgarden, Tim (2021). "Transaction fee mechanism design". In: *ACM SIGecom Exchanges* 19.1, pp. 52–55.