How to Force Mechanisms to Commit

MATHEUS V. X. FERREIRA, Princeton University
S. MATTHEW WEINBERG, Princeton University

We consider the mechanism design problem of a single item auction with multiple bidders where the auctioneer is sequentially rational and unable to commit to the rules of the auction. Bidders do not share any information and can only communicate privately with the auctioneer, who is free to manipulate the auction as long as deviations are undetectable by bidders. In this setting, strategy-proof direct revelation mechanisms are not credible since the auctioneer can easily mischaracterize the history of the game to obtain higher revenue. We introduce the Deferred Revelation Auction (DRA), a two-round mechanism that is strategy-proof not only for bidders but also for the auctioneer under distributional and computational hardness assumptions circumventing a known impossibility result due to Akbarpour and Li [1].

Additional Key Words and Phrases: Credible Mechanisms; Cryptographic Auctions; Optimal Auction Design; Mechanism Design and Approximation; Mechanism Design with Imperfect Commitment; E-commerce.

1 INTRODUCTION

We consider the problem of an auctioneer that wants to auction a single item to multiple bidders. Bidders can only communicate privately with the auctioneer and there is no previous setup between bidders – e.g., bidders do not share any private information and do not know each other's identity. We assume bidders have independent private values (IPV) drawn from a distribution known by the auctioneer.

In this setting, the question of how to design strategy-proof auctions – in which following the protocol is an equilibrium for bidders – is central question to mechanism design. More than a half-century ago, when first introducing second-price auctions[1] to the academic world, Vickrey [2] argued that the strategy-proof second-price auction incurs low mental effort from bidders to participate. This potentially attracts more participants to the auction, improving the allocation of resources and the seller's revenue. Unfortunately, unlike first-price auctions, second-price auctions are not self-policing and require bidders to trust that the auctioneer will commit to the "rules of the game".

To address this lack of transparency, Vickrey [2] envisioned the existence of a trusted third-party that handles the bids, revealing the second-highest bid to the winner. In practice, to abstract away the incentives behind the auctioneer, the research community has traditionally assumed the mechanism and the auctioneer, the agent responsible for implementing the rules of the game, are one indivisible entity which commits to the mechanism [3, 4].

In the internet age, online auctions are ubiquitous and contribute to multi-billion dollar markets in advertising [5, 6], wireless spectrum [7], and commodities [8, 9] to name a few. However, consumers increasingly require more transparency and trust from online services [10]; notwithstanding, there is a real fear by bidders of the auctioneer cheating in a second-price auction [11]. This lack of self-regulation embedded in the rules of the second-price auction allowed ad-exchanges to introduce complex dynamics on how the mechanism is implemented, generating mistrust from buyers and leading major ad-exchanges to move away from second-price auctions to first-price auctions [12].

As our main contribution, we introduce an efficient two-round[2] cryptographic auction that is strategy-proof for the auctioneer and bidders under standard computational hardness assumptions

[1] On the contrary of the first-price auction where the winner is the highest bidder who pays his bid, in a second-price auction, the winner is still the highest bidder who pays only the second-highest bid. In a second-price auction, assuming truthful bidding by other bidders, a bidder has no incentive to not bid his true value.

[2] We define round complexity of a game as the maximum number of times a player is invited to play.

(i.e., existence of cryptographic commitments [13]) and distributional assumptions on a bidder's prior (i.e., α-Strongly Regularity [14], and/or Monotone Hazard Rate [15]) without the need of any trusted third-party (e.g., Auditors), service (e.g., Public-Key Infrastructure [16], Blockchain [17]), or setup (e.g., Public Randomness [18]). In a formal sense, under such general model, the auctioneer can still deviate; however, the auctioneer commits to follow the rules of the game because any deviation is either detectable or not profitable in expectation.

1.1 Related Work

1.1.1 Optimal Credible Auctions. The mechanism designer wishes to design an ex-ante mechanism that maximizes expected revenue subject to incentive compatibility constraints – that is, it is in bidders best interest to act according to their true preferences. Myerson [4] gave a complete characterization of the optimal auction for the single item, multiple bidders case. When bidders are symmetric (i.e., have the same prior), the optimal auction is known to be the second-price auction with an optimal reserve price (i.e., the minimum price the auctioneer will accept to sell the item). Throughout the paper, we will often refer to mechanisms that implement the second-price auction allocation, but our results extend to optimal auctions in the non-symmetric case as well.

By introducing incentive compatibility to the auctioneer, Akbarpou and Li [1] formally defined a mechanism as *credible* if there are no safe deviations[3] from the mechanism's rules that are profitable. Credibility is seen as one property responsible for the success or failure of auctions in practice [19]. Although a desirable property, Akbarpou and Li showed a trade-off between strategy-proofness and credibility. One can design efficient single-round auctions that are credible or strategy-proof: the first and second-price auctions respectively; however, there is a unique optimal auction format that is strategy-proof and credible and such auction requires an unbounded number of rounds in the worst-case: the ascending auction with optimal reserve.

Their result draws an interesting observation: although the optimal ascending auction implements the same outcome as the optimal second-price auction, how information is revealed to the auctioneer plays a central role in the incentives for the auctioneer to honestly implement the auction format. Inspired by their work, we show that their impossibility result can be overcome by introducing computational (i.e., the auctioneer is computationally bounded and the existence of cryptographic commitments) and Bayesian assumptions (i.e., bidders are drawn from a commonly assumed family of distributions).

1.1.2 Mechanism Design with Imperfect Commitment. The literature in mechanism design with imperfect commitment considers the ex-post mechanism design problem where the auctioneer aggregates information learned during the game in the choice of the outcome [20, 21]. Bester and Strausz [22] consider the mechanism design problem when the mechanism designer cannot commit to an allocation function and show that for more than one agent, direct revelation mechanisms are sub-optimal. Liu et al. [23] consider the mechanism design problem when the auctioneer cannot commit to not re-auction the item, at a lower reserve, if all bidders are below the reserve. Most related to our work is the work of Akbarpour and Li [1] where the auction game is modeled as an extensive-form game where the auctioneer is sequentially rational and the auction is one-shot – that is, the auctioneer cannot re-auction the item if it is not allocated.

1.1.3 Secure Computation. In secure computation, agents have private inputs and wish to compute a functionality privately without the need of a trusted third-party. Introduced in Yao's millionaire problem [24] – two millionaires want to compute who has more money without revealing their

[3] A deviation is safe if no bidder can ever detect with certainty a deviation from the mechanism's rules.

wealth –, secure multi-party computation has been a central problem in cryptography (See chapter 7 of [25] for a survey on the topic).

Given the success and the advancements in secure computation, it is natural to ask if we could borrow those techniques to construct credible auctions. In particular, we could envision a scenario where bidders privately compute the outcome of the auction without the need for an auctioneer. Unfortunately, known impossibility results limit the use of general multi-party secure computation to the auction setting when bidders cannot be forced to participate and the lack of a trusted third-party to authenticate bidders and the lack of a trusted setup between bidders forces the auction to be permissionless[4].

It is known that general secure multi-party computation is possible under a strict majority of honest parties and access to broadcast channels [27–29]. By having multiple auctioneers and assuming at least a third of the auctioneers are honest, Franklin and Reiter [30] have proposed a distributed auction that is guaranteed not to have price inflation. When a majority is not guaranteed, general multi-party computation is impossible if parties are allowed to abort [31]. By allowing parties to abort, we cannot have fairness – once a party learns the output, that party can abort the protocol and refuse to share the output with other parties. Assuming no collusion, Bradford et al. [32] analyzed protocols for secure computation of an auction and consider the incentives of bidders to not abort once they learn the outcome.

Bentov and Kumaresan [33] have proposed a protocol for secure computation that penalizes parties through security deposits in Bitcoin [26]: parties have their deposit withheld if a deviation is detected. Security deposits are a common paradigm in the domain of rational adversaries where it is often assumed there is a large enough penalty that incentivizes parties to behave honestly; however, for the domain of credible auction design, we show that no penalty suffices if bidders have unbounded support distribution, Theorem 4.1 and Theorem 5.2.

The known impossibility results for general multi-party computation reveal the challenge of designing credible auctions in a general setting: an honest majority is not possible since the auctioneer can perform a Sybil attack [34] (i.e., forge the identity of multiple bidders), and bidders can abort from the auction at any point of the game.

1.1.4 Cryptographic Auctions. Cryptographic Vickrey Auctions have been proposed to handle the privacy of bids [35, 36] and the fear of a cheating auctioneer [37–39]. In addition to standard cryptographic assumptions, previous work has introduced many different assumptions to deal with a cheating auctioneer. Assuming bidders do not abort, and the existence of a public-key authority to authenticate bidder's identities, Nurmi [37] proposed an auction where bidders first post encrypted bids, and then reveal their private decryption key. Unfortunately, public-key encryption and digital signatures are only secure if there is a previous setup between bidders and/or assuming a trusted authority to authenticate bidders. If bidders require the auctioneer to share bidder's identities and/or setup a key-agreement protocol, the auctioneer can act as an active adversary that intercepts every communication between bidders [40].

Focusing on the privacy of bids, assuming a public-key authority, Brandt [38] proposed a cryptographic auction where bidders encrypt for all possible bids a bit indicating if they are willing to pay for that bid. Their protocol allows the auctioneer to recover the second-highest bid without learning too much information about other bids. [39] removes the need of the auctioneer by using

[4]In a permissionless protocol, any agent is free to enter and participate without previous permission and authentication. Permissionless is an important component behind the success of the internet and blockchain technologies [26]. Although desirable, permissionless protocols are vulnerable to a Sybil attack where one party can forge multiple identities. In a permissionless auction, we are particularly concerned about the auctioneer impersonating multiple bidder identities turning any protocol requiring honest majority vulnerable.

a variant of a secret sharing scheme. Brandt [38, 39] punish through fines bidders that deviate from the protocol and refuse to participate. As a limitation, [38] and [39] requires bandwidth linear to the bidding space (i.e., exponential in the bit representation of bids) and did not explicitly define the punishment scheme. In the present work, we raise a subtle point about protocols that require punishing cheating agents. If fines are paid to the auctioneer and the auctioneer can perform a Sybil attack, then fines incurred by agents controlled by the auctioneer are irrelevant and will never impact the auctioneer's utility. In our work, we propose a simple but effective change of paradigm by requiring penalties to be paid to the highest bidder; therefore, a Sybil (i.e., fake bidder) that is detected deviating indirectly affects the auctioneer's utility.

Stubblebine et al. [41] propose a fair online auction but require trusted notaries and public-key authorities. Parkes et al. [42] propose an auditable auction with the use of trusted notaries and a trusted Time-Lapse Cryptography Service (TLC), a service that releases a decryption key after a specified time. TLC provides benefits to cryptographic commitment schemes since a bidder cannot refuse to reveal their bid; however, it requires a trusted service and the extra latency can be impracticable for many applications.

1.2 Cryptographic Credible Mechanisms

As our main result, we propose a simple modification to any ex-ante direct revelation mechanism – that is, a mechanism that commits to an allocation function and then requests bidders to submit their bids. In this section, we will first describe a strawman mechanism that implements the second-price auction with a reserve price and describe safe deviations that are profitable for the auctioneer to later informally motivate the final construction. In Section 3, we formally give the construction for every ex-ante direct revelation mechanism including the case of optimal auctions for non-symmetric bidders.

Definition 1.1 (Strawman Auction).
1^{st} *Round:*

- *The auctioneer requests bidders to submit cryptographic commitments*[5] *of their bids.*
- *The auctioneer makes bid commitments public to everyone.*

2^{nd} *Round:*

- *The auctioneer request bidders to open their bid commitments.*
- *The auctioneer opens all bid commitments to everyone.*
- *The item is allocated to the highest bidder, who pays the second-highest bid or the reserve (whichever is higher).*

The auctioneer cannot inflate the second-highest bid by introducing new bids after a bidder reveals his bid; however, the auctioneer can forge the identity of multiple fake bidders before the end of 1^{st} round. By doing so, each fake bid works as a "reserve price". If the auctioneer always reveals all fake bids, there is no point for the auctioneer to submit more than one fake bid since the non-highest fake bids will never influence the outcome of the auction. Moreover, if the reserve price is optimal, in hindsight, there is no reason for the auctioneer to submit any fake bid. However, if the reserve was not optimal, in hindsight, the auctioneer can submit a fake bid equal to the optimal reserve which results in a profitable deviation. An identical phenomenon happens in the ascending

[5]A criptographic commitment scheme is a 2-ary function $Commit(v, r)$ where v is the value being committed and r is a random string of size λ, the security parameter. A sender commits to a value v by sending $c = Commit(v, r)$ to the receiver. The sender opens the commitment by making (v, r) public. The commitment is successfully opened if upon receiving strings (v', r'), the receiver confirms that $c = Commit(v', r')$. Informally, a commitment is secure if it is hiding (e.g., by observing only c, the receiver learns nothing about v) and binding (e.g., the sender cannot find inputs (v, r) and (v', r') where $Commit(v, r) = Commit(v', r')$).

auction where Akbarpou and Li [23] pointed out that the ascending auction with optimal reserve is only credible because it is an ex-ante optimal auction.

Even if the reserve price is optimal, it is not realistic to assume that all bidders will continue to participate of the auction once they have learned of the other bidder's bids – that is, it is reasonable and realistic to assume that bidders can abort from the protocol at any time. Participation incentives in games have been vastly studied in the literature of rational secret sharing and multi-party computation [43–45]. In rational secret sharing, players favor to learn the secret above all else but prefer to learn the secret alone. In that context, Halpern and Teague [43] showed that Shamir's secret sharing protocol has a unique equilibrium where no party shares their share; moreover, that property is shared by every finite protocol due to a backward induction argument.

In the strawman auction, if we assume bidders can abort from the protocol at any point, the auctioneer can abort fake bidders that bid above the highest real bidder. For the real bidder, it is not possible to distinguish from the context what caused a bidder to no reveal his commitment. As an alternative, we could modify the mechanism to require the auction to restart once a bidder aborts; however, this gives power for the auctioneer to force the auction to abort and restart once the auctioneer learns the value of the real bidders. As an alternative solution, we can simply ignore bidders that abort and design a punishment scheme for such bidders. By ignoring bidders that abort, Theorem 4.1 shows that such deviations can be extremely profitable for the auctioneer even when we introduce a punishment scheme. In Section 5, by introducing assumptions in the bidders prior, we can overcome the impossibility result of Theorem 4.1.

Next, we modify the strawman auction to include a punishment scheme for bidders that abort.

Definition 1.2 (Strawman Auction with Punishment).
1^{st} *Round:*

- *The auctionner requests bidders to submit cryptographic commitments of their bids.*
- *Bidders send their bid commitment together with a pre-agreed commitment fee deposit.*
- *The auctioneer makes bid commitments public to everyone.*

2^{nd} *Round:*

- *The auctioneer request bidders to open their bid commitments.*
- *The auctioneer opens all bid commitments to everyone.*
- *The auctioneer refunds the commitment fee of a bidder if the bidder successfully opens his bid commitment.*
- *The item is allocated to the highest bidder, who pays the second-highest bid or the reserve (whichever is higher).*
- *If a bidder aborts or fails to open his commitment, their commitment fee is given to the winning bidder.*

The main modification of the mechanism is to introduce a commitment fee (e.g., entry fee) to the auction. The goal of the fee is two-fold: we want to disincentivize bidders from aborting during the game and we want to penalize the auctioneer for impersonating fake bidders. Auctions with entry fee have been studied in the context of optimal entry of bidders – that is, the number of bidders is not fixed but depends on the equilibrium induce by the entry fee – in first-price auctions [46] and in more general auction formats [47].

By introducing bid commitments and commitment fees to the second-price auction, the mechanism "appears to become self-policing" because the winning bidder only accepts the outcome of the auction if the auctioneer can prove no bidder bid higher; therefore, by introducing fake bids, the auctioneer risks overbidding the highest bidder. It is still possible for the auctioneer to deviate and hide fake bids that are above the highest bidder but that incurs the payment of a penalty to the

winning bidder. We emphasize the mechanism simply appears to become self-policy. Because the auctioneer is aware of the prior distribution of bidders, without restricting the class of distributions bidders are drawn, we show that the auctioneer can profitably deviate for any penalty policy, Theorem 4.1.

Although previous work in cryptographic auctions focused mostly in the privacy of bids, and audibility of the auctioneer's actions, our cryptographic auction gives no expectation of privacy. We focus in designing optimal strategy-proof credible auctions with as few rounds as possible; however, we point out that the auctioneer could use a Zero-Knowledge Interactive Proof (ZKIP) for every language in NP[6] to prove that the allocation is consistent without revealing the bids. By using Feige and Shamir's protocol [48] privacy can be preserved with two extra rounds, which can be removed in the common reference string model [49] (i.e., access to public randomness) or in the random oracle model [50].

1.3 Organization and Summary

In Section 3, for every ex-ante direct revelation auction, we define cryptographic auction, a Deferred Revelation Auction (DRA), that computes the same allocation and payment of the direct revelation counterpart. We define Deferred Revelation Second-Price Auction (DRSPA) as the DRA that implements the second-price auction. A natural question is how big if any, should the commitment fee be so that the mechanism becomes credible. For that, we show a connection between the tail of bidder's prior-value distribution and credibility.

In Section 4, we analyze the case where bidders have a regular distribution and show that regularity is not sufficient for DRSPA with optimal reserve to be credible. In Theorem 4.1, we construct an auction instance with a single bidder drawn from a regular distribution where for every commitment fee – even if fees are allowed to depends on the current state of the game –, DRSPA is not credible. Moreover, Theorem 4.1 shows that the auctioneer can obtain revenue with an infinite gap from the revenue of the optimal truthful mechanism.

In Section 5, we relax regularity and consider the class of α-strongly regular distributions [14, 51] and Monotone Hazard Rate distributions (MHR) [15]. We show that as long as bidders have MHR distribution and the commitment fee of each bidder is at least their optimal reserve price, DRA with optimal reserve is credible, Corollary 5.1. For α-strongly regular distributions, we show that for a single bidder, if the commitment fee is $O(r)$ (r is the optimal reserve), DRSPA is credible, Theorem 5.1. For two or more bidders, for all commitment fees – even if fees are allowed to depends on the current state of the game –, there is a safe deviation for the auctioneer that gets strictly more revenue than the optimal truthful auction; however, for a commitment fee of $poly(1/\epsilon, n, r)$, DRSPA is ϵ-credible – that is, the auctioneer cannot get more than the revenue of the optimal truthful auction plus ϵ additive bonus.

2 PRELIMINARIES

Distribution. For random variable X, let F_X and $f_X(x)$ be the cumulative density and probability density functions of X respectively. Let $u^X_{min} := \sup\{x|F(x) = 0\}$ and $u^X_{max} := \inf\{x|F(x) = 1\}$ which defines the interval where X is supported.

Auction. There is an auctioneer with a single indivisible item and a set $[n] = \{1, 2, ..., n\}$ of bidders. In the end of the auction, the auctioneer allocates the item and request payments. We assume bidders have independent private values where bidder $i \in [n]$ has value v_i drawn from

[6]Formally a language $L \in NP$ if there is a polynomial-time verifier V such that for all $x \in L$, there is a witness w where the verifier accepts w as a witness for the membership of x in L. On the other hand, if $x \notin L$, then for all w, the verifier rejects w as a witness for the membership of x in L.

distribution $D_i \in \mathcal{D}$ with finite support X_i where $\mathcal{D}$ is a finite collection of distributions. The auctioneer knows D_i but not v_i. Bidders know their value and their distribution but do not share any private information. We denote $D = \times_{i=1}^{n} D_i$ as the product distribution where the value profile $v = (v_1, v_2, .., , v_n)$ is drawn. We denote v_{-i} as the value of all bidders but bidder i. For distribution D_i, $F_i(x) = Pr_{v \leftarrow D_i}[v \leq x]$ denotes the cumulative density function and $f_i(x) = Pr_{v \leftarrow D_i}[v = x]$ denotes the probability density function.

Communication Model. The auctioneer has access to a private communication channel with each bidder. The game starts with the auctioneer active. Once active, the auctioneer can abort a bidder or activate a bidder by submitting a request. Once activated with a request, a bidder aborts or submits a reply. Once a bidder aborts or replies, the auctioneer is activated. The game ends when all bidders abort or the auctioneer halts.

Game. A game G is a sequence of requests by the auctioneer and replies by bidders. A game is represented by a game tree where each node is owned by the agent responsible for the next move. Given an auctioneer strategy $s_0 \in \mathcal{S}_0$, we denote G^{s_0} as the game implemented by strategy s_0. Similarly, each bidder i has a corresponding strategy $s_i \in \mathcal{S}_i$ when playing game G^{s_0}.

Computational Assumptions. We assume all agents (i.e., the auctioneer and bidders) are computationally bounded. That is, a strategy s of a computationally bounded agent is valid if there is a probabilistic Turing Machine (TM) that can simulate s in polynomial-time with respect to the number of bidders n and the **security parameter**[7] λ.

Mechanism. A mechanism is a tuple (G, s) where $s = (s_1, s_2, ..., s_n)$ is the strategy profile of all bidders. Given values $v = (v_1, v_2, ..., v_n)$ and strategies s, the game G results in an outcome $O(G, s, v)$. Let $O_i(G, s, v)$ be part of the outcome observed by bidder i such that $O(G, s, v) = \cup_{i \in [n]} O_i(G, s, v)$. The outcome results in an allocation $\pi : \times_{i \in [n]} \mathcal{S}_i \times X \rightarrow [0, 1]^n$ and payment $p : \times_{i \in [n]} \mathcal{S}_i \times X \rightarrow \mathbb{R}^n$ where $\pi_i(s, v)$ denotes the probability bidder i receives the item and $p_i(s, v)$ denotes bidder's i payment. An allocation is feasible if $\sum_{i=1}^{n} \pi_i(s, v) \leq 1$. A mechanism is deterministic if $\pi_i(s, v) \in \{0, 1\}$ for all $i \in [n]$. Bidders have quasi-linear utility, where bidder i has utility $u_i^G(s, v) = (v_i - p_i(s, v)) \cdot \pi_i(s, v)$. We denote $u_0(s_0, s, v) = \sum_{i=1}^{n} p_i(s, v)$ as the revenue for the auctioneer.

A mechanism (G, s) is Bayes Incentive-Compatible (BIC), if for all bidders $i \in [n]$ is in their best interest to follow strategy s_i in expectation over s_{-i}.

Definition 2.1 (Bayes Incentive-Compatible (BIC) Mechanism). *A mechanism (G, s) is BIC if $\forall i \in [n], \forall v_i \in X_i, \forall s_i' \in \mathcal{S}_i$:*

$$E_{v_{-i} \leftarrow D_{-i}}[u_i^G(s_i, s_{-i}, v)] \geq E_{v_{-i} \leftarrow D_{-i}}[u_i^G(s_i', s_{-i}, v)]$$

Direct Revelation Mechanism. A mechanism is direct revelation if bidders are restrict to strategies that map values to bids – that is, $s_i : X_i \rightarrow X_i$. We say the auctioneer public commits to an ex-ante mechanism (π, p) if for all bid profiles $b \in X$, the auctioneer is guaranteed to allocate the item according to $\pi(b)$ and collect payments according to $p(b)$ where π and p are public n-ary functions. For a direct revelation mechanism represented by (π, p), when bidders bid according to strategy s and have value profile v, we write $\pi(b)$ instead of $\pi(s(v))$ and $p(b)$ instead of $p(s(v))$ where $b = s(v)$ is the bid profile of all bidders. If direct revelation mechanism (G, s) is BIC, then bidders bid their value – that is, $s(v) = v$.

If the auctioneer can commit to a mechanism, by the **Revelation Principle** (Theorem 2 of [52]), it is without loss of generality to consider only direct revelation mechanisms when maximizing revenue over BIC mechanisms – that is, for every BIC mechanism, there is always a direct revelation mechanism that gives the same utility for the auctioneer and bidders.

[7]The security parameter measures how hard it is for an adversary to break a cryptographic scheme.

Virtual Values. For a one dimensional distribution F, we define for all $x \geq 0$, $\phi^F(x) := x - \frac{1-F(x)}{f(x)}$ as the virtual value function of F. We drop the superscript F if F is clear from context. We call $h^F(x) := \frac{f(x)}{1-F(x)}$ the **Hazard Rate** of F.

The celebrated Myerson's lemma characterize the revenue of a ex-ante BIC direct revelation mechanism in terms of the expected virtual welfare of the mechanism:

Lemma 2.1 (Myerson's lemma[4]). *For an ex-ante BIC mechanism with allocation rule π, and payment rule p, we have*

$$E_{v\leftarrow D}\left[\sum_{i=1}^{n} p_i(v)\right] = E_{v\leftarrow D}\left[\sum_{i=1}^{n} \pi_i(v)\phi_i(v_i)\right] \tag{1}$$

where $\phi_i(v)$ is the virtual value function of bidder i. The allocation $\pi(v)$ uniquely determines the payment rule $p(v)$:

$$p_i(v) = \pi_i(v)v_i - \int_0^{v_i} \pi_i(x_i, v_{-i})dx_i \tag{2}$$

A Safe Deviation. Given game G^{s_0}, we assume the auctioneer can deviate to any strategy s_0' that is safe – that is, deviations that are undetectable by bidders. A deviation is undetectable – and therefore, safe – if it has an **Innocent Explanation** [1]. Due to the fact the auctioneer is computationally bounded, all safe deviations must run in probabilistic polynomial-time. An outcome $O(G^{s_0'}, s, v)$ has an innocent explanation, if for every bidder i, there is a sequence of actions for the other bidders that would have resulted in the same outcome: $\forall i \in [n]$, $\exists v'_{-i} \in X_{-i}$, $\exists s'_{-i} \in \mathcal{S}_{-i}$ such that $O_i(G^{s_0}, s_i, s'_{-i}, v_i, v'_{-i}) = O_i(G^{s_0'}, s_i, s_{-i}, v_i, v_{-i})$.

Example 2.1 (Safe deviations in the Sealed-Bid Second-Price Auction). *Assume bidder 1 bids $v_1 = 5$ and bidder 2 bids $v_2 = 10$. The rules of the mechanism says that the auctioneer must allocate the item to bidder 2 and request a payment of 5; however, because bidder 2 cannot observe what the auctioneer communicates with bidder 1, the auctioneer can request a payment of 9 instead which has an innocent explanation – bidder 1 could have bid 9.*

Credible Mechanism. A mechanism (G, s) is ϵ-credible if for all safe deviations s_0' from s_0^G,

$$E_{v\leftarrow D}[u_0(s_0^G, s, v)] \geq E_{v\leftarrow D}[u_0(s_0', s, v)] - \epsilon$$

Initially defined by Akbarpour and Li [1], a mechanism is credible if it is 0-credible.

2.1 Commitment Schemes

Ideal Commitment Scheme. is a protocol between a sender and receiver divided in two phases. In the commitment phase, the sender commits to a value x. In the opening phase, the sender opens the commitment and the receiver learns x. Informally, an ideal commitment scheme is:

- **Hiding**: the receiver learns nothing – information theoretically – about x before the sender opens the commitment in the opening phase.
- **Binding**: once the sender commits to x, the sender can only open the commitment to x. In other words, it is impossible for the sender to convince the receiver that they committed to $x' \neq x$.

An ideal commitment scheme can be trivially implemented with a trusted third-party $\mathcal{F}_{COM}$ and a private communication channel between $\mathcal{F}_{COM}$ and the players [53]. In the first round, the sender commits to value x by sending x to $\mathcal{F}_{COM}$ which stores x in memory. In the second, round the sender sends an open request to $\mathcal{F}_{COM}$ which sends x to the receiver.

Cryptographic Commitment Scheme. To remove the requirement for a trusted third-party, we turn to cryptographic commitment schemes which require us to assume either the sender or the receiver are computationally bounded. In the commitment phase, the sender with input x computes $c = Commit(x, r) : \{0,1\}^\ell \times \{0,1\}^\lambda \to \{0,1\}^m$ and sends c to the receiver. $Commit(x, r)$ is a commitment for the value $x \in \{0,1\}^\ell$ using random string $r \in \{0,1\}^\lambda$ where λ is the security parameter. In the opening phase, the sender sends (x', r') and the receiver checks if c equals to $Commit(x', r')$.

Unfortunately, no such scheme can be secure (e.g. hiding and binding) if both sender and receiver are computationally unbounded. If the receiver is unbounded, for all strings $c \in \{0,1\}^m$ there must exist two distinct inputs $x \neq x'$ and random strings r and r' such that $Commit(x, r) = Commit(x', r')$; otherwise, the receiver can compute the inverse of $Commit(\cdot, \cdot)$ and learn x. However, if the sender commits to x using random string r, a computationally unbounded sender can open the commitment to $x' \neq x$ using the random string r'. Due to this impossibility, we will assume the existence of a computationally binding and perfectly hiding commitment scheme which can be implemented with Pedersen's commitment scheme [13] under the discrete logarithm assumption. Next, we give the formal security definition.

Perfectly Hiding. A commitment scheme $Commit(\cdot, \cdot)$ is perfectly hiding if for all $x \neq x'$, $Commit(x, r)$ and $Commit(x', r)$ are identically distributed where r is a uniformly-random string from $\{0,1\}^\lambda$. Information theoretically, this definition is identical to the hiding property of ideal commitments.

Computationally Binding. A commitment scheme $Commit(\cdot, \cdot)$ is computationally binding if for all Probabilistic Polynomial Time (PPT) algorithms $\mathcal{A}$ outputting inputs $x' \neq x$ and random strings r, r', the probability that $Commit(x, r) = Commit(x', r')$ is negligible.

$$Pr[Commit(x, r) = Commit(x', r') : (x, r, x', r') \leftarrow \mathcal{A}(n, \lambda)] < \mu(\lambda)$$

where the probability is taken over the randomness of $\mathcal{A}$ and $\mu(\lambda)$ is a **negligible function**. A function is negligible if for every positive polynomial $poly(\cdot)$, there is $N > 0$ such that for every $x > N$,

$$|\mu(x)| < \frac{1}{poly(x)}$$

We say a property holds **Asymptotically Almost Surely** (a.a.s.) if over a sequence of sets, the probability converges to 1. As example, for all PPT algorithm $\mathcal{A}(n, \lambda)$ let $f(\lambda)$ be the indicator random variable which take value 1 if $\mathcal{A}$ does not violate the computationally binding property. We say the commitment scheme is computationally binding if a.s.s. $\{f(\lambda)\}_{\lambda \in \mathbb{Z}^+}$ converges to the universe.

3 DEFERRED REVELATION AUCTION

In this section, we describe the Deferred Revelation Auction (DRA). The rules and the input of the mechanism are pre-agreed between the auctioneer and all bidders and are public to everyone. On the other hand, some parameters are instance-specific and are only available when the auction starts (e.g., the number of bidders and their distributions). Instance-specific parameters are private input to the auctioneer and are unknown to bidders and can be corrupted by the auctioneer.

3.1 Auction Construction

The input to the mechanism consists of a *security parameter* $\lambda \in \mathbb{Z}^+$; a collection of distributions $\mathcal{D}$; and a ensemble of ex-ante BIC allocation and payment rules $\{(\pi^{n,D}(v), p^{n,D}(v))\}_{n \in \mathbb{Z}, D \in \mathcal{D}^n}$ indexed by the number of bidders n and their distributions where we drop the superscript when explicit from the context. For each distribution $D_i \in \mathcal{D}$, the mechanism has a policy to compute a *commitment*

fee k_i. The commitment fee is allowed to depend on all messages exchanged so far between the auctioneer and bidders – i.e., the commitment fee k_i for a bidder drawn from distribution D_i could depend on the number of bidders n and in the bidders' distribution D.

In the setup phase, the auctioneer observes privately the number n of bidders and their class – i.e., the distribution D_i of bidder $i \in [n]$. For each bidder, the auctioneer announces the number of bidders $n \in \mathbb{Z}^+$ and their classes. A bidder knows his value v_i and his class D_i. Initialize $A = \emptyset$. The game proceeds as follows:

Commitment Phase

- For all $i \in [n]$, the auctioneer activates bidder i and request bidder i to reply with a commitment for his bid. When bidder i is active:
  - Bidder i draws a uniformly-random string $r_i \leftarrow \{0,1\}^\lambda$.
  - Bidder i replies $c_i = \mathit{Commit}(v_i, r_i)$ and deposit the commitment fee k_i.
- For all $i \in [n]$, the auctioneer sends c_{-i} to bidder i.

Revelation Phase

- For all $i \in [n]$, the auctioneer activates bidder i and request bidder i to open commitment c_i. When bidder i is active:
  - Bidder i replies (v_i, r_i).
  - Upon receiving (v_i', r_i') from bidder i, the auctioneer checks $c_i \stackrel{?}{=} \mathit{Commit}(v_i', r_i')$. If $c_i = \mathit{Commit}(v_i', r_i')$, update $A = A \cup \{i\}$ and returns the commitment fee to bidder i; otherwise, the auctioneer aborts bidder i. If bidder i aborts, set $v_i' = 0$.

Allocation Phase

- The auctioneer allocates the item according to $\pi^n(v')$ requests payment according to $p_i^n(v')$. If the item is allocated, let i^* be the bidder that receives the item.

Verification Phase

- **Proof of allocation and payment.** The auctioneer opens the commitments $\{c_j\}_{j \in A}$ to bidder i by sending $\{(v_j, r_j)\}_{j \in A/\{i\}}$.
- **Payment of penalties.** The auctioneer gives bidder i^* the commitment fee of bidders that committed and aborted before opening their commitment – that is, the commitment fee of all bidders $i \notin A$.

3.2 Optimal Deferred Revelation Auctions

Let $(\pi^{n,D}, p^{n,D})_{n \in \mathbb{Z}, D \in \mathcal{D}^n}$ be an optimal ex-ante BIC mechanism where bidders have monotone increasing virtual values[8]. By Myerson's Lemma, the optimal DRA instantiated with allocation and payment $(\pi^{n,D}, p^{n,D})_{n \in \mathbb{Z}, D \in \mathcal{D}^n}$ allocates the item to the bidder i with highest non-negative virtual value and request payment $p_i(v) = \max\{r_i, \phi_i^{-1}(\max_{j \neq i} \phi_j(v_j))\}$ where $r_i = \phi_i^{-1}(0)$ is bidder's i reserve price[9]. We can this auction **Virtual Deferred Revelation Auction** (VDRA).

When bidders are symmetric – that is, have the same distribution –, the optimal auction allocates the item to the highest bidder i if $v_i \geq r_i$ and charges the second-highest bid or the reserve price (whichever is higher). We call the DRA implementing the second-price auction the **Deferred Revelation Second-Price Auction** (DRSPA).

[8] A virtual value function is monotone increasing if the distribution is regular. If the distribution is not regular, virtual values can be replaced by monotone increasing ironed virtual values [4].

[9] A surprising corollary of Myerson's Lemma is that the optimal reserve does depend in the number of bidders. Instead, the optimal reserve varies from bidder to bidder and depends on the bidders prior distribution.

3.3 Discussion

At first glance, it appears that bid commitments improve credibility since by opening the commitments, bidders can verify the consistency of the allocation and payment announced by the auctioneer – recall from Myerson's Lemma that the allocation uniquely determines payments of a BIC mechanism. Also, if the auctioneer submits fake bids and aborts those bids in the revelation phase, the auctioneer must pay a penalty for the winner so it is plausible to conjecture that for large enough fees the auctioneer would not have enough incentive to submit fake bids.

The problem with our false conjecture is that it does not take into consideration the prior distribution of the bidders. In Section 4, we show that by taking into consideration the bidder's prior, there is a distribution where the auctioneer can carefully craft m fake bids and obtain revenue $\Omega(m)$ no matter how big the commitment fees while by being honest, the auctioneer could obtain revenue at most 1. In Section 5, we show that by introducing usual assumptions in the bidder's prior, DRA can be made credible or ϵ-credible asymptotically almost surely for sufficiently large commitment fees.

The next Lemma implies that asymptotically almost surely if the auctioneer sends a commitment to value v, the commitment can only be opened to v. The proof is straightforward and uses the fact that an adversary for the commitment scheme can record all calls to $Commit(\cdot,\cdot)$ and violates the binding property if the auctioneer can open the commitment to more than one value.

Lemma 3.1. *Assume $Commit(\cdot,\cdot)$ is computationally binding, the auctioneer's strategy runs in probabilistic polynomial time and bidders commit to follow the mechanism rules. If the auctioneer send commitment c to a bid v, then with probability at least $1-\mu(\lambda)$ the auctioneer can only open c by revealing v.*

Proof. Let s_0 be the auctioneer's strategy and let $s = (s_1, s_2, ..., s_n)$ be the bidder's strategy. Without loss of generality, let c be the commitment to some value v and note that v might be known or unknown by the auctioneer – that is, c could have been generated by a bidder that forwarded c to the auctioneer. If c was generated by a bidder, then that bidder invoked $Commit(v, r)$ with some random string r. If c was generated by the auctioneer, then it is possible that c was generated without invoking $Commit(\cdot,\cdot)$. In that case, if the auctioneer can open c, then the auctioneer can compute the inverse $(v, r) = Commit^{-1}(c)$. In that case, we will assume the auctioneer computes (v, r) and invoke $Commit(v, r)$ – for bookkeeping – before sending c to the bidder. Note that the definition of computational binding commitments does not limit an adversary from inverting commitments as long as the adversary cannot open c to two different values.

At this point, after the bidder receives c, either another bidder or the auctioneer invoked $Commit(v, r)$. Assume for contradiction, the auctioneer opens the commitment to $v' \neq v$ using random string r' with probability at least $\mu(\lambda)$. Construct an adversary $\mathcal{A}$ that simulates the auction game with an auctioneer following strategy s_0 and bidders following strategy $s = (s_1, s_2, ..., s_n)$ and record all calls to $Commit(\cdot,\cdot)$. If two calls evaluate to the same commitment string under different inputs $(v, r) \neq (v', r')$ output (v, r, v', r'); otherwise, output $\perp$. To analyze the run-time of $\mathcal{A}$, observe each simulated bidder following strategy s_i, $i \in [n]$, makes at most one call to $Commit(\cdot,\cdot)$ and the auctioneer's strategy s_0 makes polynomial many calls to the $Commit(\cdot,\cdot)$ since the auctioneer runs in polynomial time. In addition, $\mathcal{A}$ outputs (v, r) and (v', r') such that $Commit(v, r) = Commit(v', r')$ with probability at least $\mu(\lambda)$, contradicting $Commit(\cdot,\cdot)$ is computationally binding. □

If the auctioneer uses a polynomial time randomized strategy, then the auctioneer randomizes over polynomial time deterministic strategies[10]. Differently from the case where the auctioneer

[10]A randomized strategy is simply a strategy with a random input used to decide random choices. By fixing the random input, a randomized strategy becomes deterministic.

is computationally unbounded, it is not without loss of generality to consider only deterministic strategies. That is, since the auctioneer can violate computational binding security with non-zero probability, there are deterministic strategies that are profitable – i.g., the hardness assumption simply state that it is hard for a computationally bounded auctioneer to find such deviations. However, if we condition a polynomial time randomized strategy on not violating computational binding security, then the revenue is bounded by the revenue of the optimal deterministic strategy that never violates computational binding security, Lemma 3.2.

Lemma 3.2. *Asymptotically almost surely the revenue of a safe deviation is at most the revenue of a deterministic safe deviation that does not violate computational binding security.*

Proof. Let s_r be an optimal polynomial time randomized safe deviation for the auctioneer. By Lemma 3.1, with probability $1-\mu(\lambda)$, s_r does not violate computational binding security. Conditioned on not violating computational binding security, s_r randomize over deterministic safe deviations that do not violate computational binding security. It follows with probability $1-\mu(\lambda)$, the revenue of s_r is at most the revenue of the optimal deterministic safe deviation that does not violate computational binding security. □

If we assume the auctioneer plays a deterministic safe deviation, another source of randomness in the game is the commitments received from bidders; however, because the commitments are perfectly hiding, it is without loss of generality to assume the actions taken by the auctioneer does not depend on the commitments received, Lemma 3.3. That is, after a bidder sends a commitment, all next subgames are identical.

Lemma 3.3. *If s_0' is an optimal safe deviation, then there is an optimal safe deviation whereupon receiving commitment c_i the future actions taken by the auctioneer does not depend on c_i.*

Proof. At game $G^{s_0'}$ implemented by s_0', suppose there is a node q where bidder i is invited to submit a bid commitment and upon receiving commitment c the next node in the game is q_c. If s_0' is optimal, then for all $c \neq c'$, the expected revenue in subgame rooted at q_c is equals to the expected revenue in subgame rooted at $q_{c'}$. If the expected revenue differs, then the commitments either reveal information about the bids (even though $Commit(\cdot,\cdot)$ is perfectly hiding) or s_0' is not optimal, both leading to a contradiction. Since both subgames rooted in q_c and $q_{c'}$ respectively have the same expected revenue, we can modify $G^{s_0'}$ so that the actions taken by the auctioneer does not depend on the commitment received at node q. □

4 REGULARITY AND CREDIBILITY

In this section, we will consider the case where bidders are drawn from regular distributions and show in Theorem 4.1 that regularity is not sufficient for the optimal Deferred Revelation Second-Price Auction (DRSPA) to even be approximate credibility – that is, the revenue gap between the optimal strategy-proof auction and a safe deviation from the optimal strategy-proof auction is unbounded.

In the proof, we consider a bidder drawn from a heavy-tail regular distributions with infinite expected value. We show the auctioneer can carefully craft a safe deviation that extracts almost all the welfare of the bidder. Surprisingly, not all distributions with infinite expected value share the same pathology. In Theorem 4.2, we consider a bidder drawn from a distribution with infinite expected value where DRSPA is approximately credible for large enough commitment fee.

Definition 4.1 (Regular Distribution). *A one dimensional distribution F is regular if $\phi^F(x)$ is monotone increasing.*

Theorem 4.1. *There exists a regular distribution D, such that for every commitment fee, for every $L > 0$, the optimal Deferred Revelation Second-Price Auction is not L-credible.*

Proof. The auctioneers and bidders agree in participating in the DRA with optimal second-price auction allocation – that is, each bidder class has a public optimal reserve price. Consider the case where there is a single real bidder and the input distribution D is the equal revenue[11] $F(v) = 1 - \frac{1}{v}$. Given D, the optimal reserve price is $p = 1$ ($p = \arg\max pPr_{v \leftarrow D}[v \geq p]$). Suppose for contradiction there is a commitment fee where the second price auction with commitments is L-credible.

Commitment schemes can only be used to commit to finite set of inputs; therefore, a bidder drawn from D must round his bid. To avoid unnecessary distractions, we will assume the bidding space is finite but sufficiently dense so that any computational errors resulting from rounding are negligible.

Next, we define a safe deviation s' from DRSPA. In the commitment phase, for some integer $m = O(L)$, the auctioneer announces $m + 1$ participants to the real bidder. At this point, the auctioneer computes the commitment fee k using some arbitrary policy pre-agreed with the bidders. Next, the auctioneer simulates m bidders with values $x_1, ..., x_m$ where $x_1 = e^{(k+1)m^3}$, $x_i = e^{x_{i-1}}$ for $i = 2, ..., m$.

In the revelation phase, let v denote the bid of the real bidder. If $v \in [x_i, x_{i+1})$, the auctioneer revel commitments for $x_1, ..., x_{i-1}$ and abort bids $x_{i+1}, ..., x_m$. If $v < x_1$ or $v > x_m$, the auctioneer revel all commitments. An important observation about the auctioneer's strategy is that the event where $v < x_1$ which happens with high probability is also the event where the auctioneer does not deviate and pays no penalty. By doing so, the auctioneer only deviates when penalties are guaranteed to be negligible compared to the revenue the auctioneer can obtain. We will show this strategy gets revenue proportional to m while a honest auctioneer would get revenue $rev(D) = p(1 - F(p)) = 1$ for all prices $p \geq 1$.

In the view of the real bidder, the transcript of the game looks exactly as if it was participating in the deferred revelation second price auction with m real bidders; therefore, the deviation is safe. Below, let $Pr[v \geq x_{m+1}] = \lim_{y \to \infty} Pr[v \geq y] = 0$. The expected revenue is given by:

$$E[u_0(s', s, v)] = \sum_{i=1}^{m} (x_i - k(m-i)) Pr[v \in [x_i, x_{i+1})]$$

Rewriting $Pr[v \in [x_i, x_{i+1})] = Pr[v \geq x_i] - Pr[v \geq x_{i+1}]$, the revenue is:

$$\begin{aligned} E[u_0(s', s, v)] &= x_1 Pr[v \geq x_1] + \sum_{i=2}^{m} x_i Pr[v \geq x_i] \\ &\quad - \sum_{i=2}^{m} x_{i-1} Pr[v \geq x_i] - k \sum_{i=1}^{m} (m-i)(Pr[v \geq x_i] - Pr[v \geq x_{i+1}]) \\ &= 1 + \sum_{i=2}^{m} (x_i - x_{i-1}) Pr[v \geq x_i] - k \sum_{i=1}^{m} (m-i)(Pr[v \geq x_i] - Pr[v \geq x_{i+1}]) \end{aligned}$$

[11] $Pr[v \leq x] = 1 - \frac{1}{x}$ is known as equal revenue because if there is a single bidder drawn from F, then for all prices $p \geq 1$, the probability of sale is $Pr[v \geq p]$, and the expected revenue is $pPr[v \geq p] = 1$

Using the fact $Pr[v \geq x_i] \leq Pr[v \geq x_1]$,

$$\begin{aligned}
E[u_0(s', s, v)] &\geq 1 + (m-1) - \sum_{i=2}^{m} \frac{x_{i-1}}{e^{x_{i-1}}} - km^2 Pr[v \geq x_1] \\
&\geq m - \sum_{i=2}^{m} \frac{x_{i-1}}{e^{x_{i-1}}} - \frac{km^2}{e^{km^3}} \quad \text{(By definition } x_1 \geq e^{km^3}\text{)} \\
&\geq m - \sum_{i=1}^{m-1} \frac{x_i}{x_i^2/2} - \frac{km^2}{km^3} \quad \text{(By Taylor's Theorem, } e^x \geq 1 + x + \frac{x^2}{2}\text{)} \\
&\geq m - \frac{2m}{e^{m^3}} - \frac{1}{m} \quad \text{(By definition } x_i \geq x_1 \geq e^{m^3}\text{)}
\end{aligned}$$

The statement follows by setting $m = cL + d$ for sufficiently large constants c and d. □

Theorem 4.2. *There is a distribution D with infinite expected value where Deferred Revelation Second-Price Auction is $O(1)$-credible.*

5 STRONG REGULARITY AND CREDIBILITY

In this section, we consider the case where bidders are drawn from α-Strongly Regular distributions, an interpolation between regular and MHR distributions introduced by Roughgarden and Cole [14]. We show that α-strong regularity together with a large enough commitment fee is sufficient for the Deferred Revelation Auction (DRA) to be credible when there is a single bidder, Theorem 5.1.

For more than one bidder, for any commitment fee, the auctioneer can use an adaptive strategy to probe the values of all bidders except one and implement a profitable safe deviation with the last bidder, Theorem 5.2. Intuitively, the probes allow the auctioneer to only deviate when it is guaranteed the highest bid is sufficiently larger than the penalties for deviating. Although strictly more profitable than being honest, we show that such deviations cannot yield much more revenue than honestly implementing the auction – that is, for every $\epsilon > 0$, DRA is ϵ-credible for large enough commitment fee.

Definition 5.1 (α-Strongly Regular Distribution). *A one dimensional distribution F is α-strongly regular if for all $v' \geq v$,*

$$\phi(v') - \phi(v) \geq \alpha(v' - v) \tag{3}$$

It follows regular distributions are 0-strongly regular.

Theorem 5.1. *If there is a single bidder drawn from an α-strongly regular distribution and the commitment fee is $k = O(r)$, then asymptotically almost surely the optimal DRA is credible.*

Theorem 5.2. *Assume there is at least two bidders. For every $\alpha \in (0, 1)$, there is an α-strongly regular distribution F^α such that for every commitment fee $k \geq 0$, the optimal DRA is not credible if bidders are i.i.d. with distribution F^α.*

We further consider the class of Monotone Hazard Rate (MHR) distributions, distributions that are 1-Strongly Regular, where the optimal Deferred Revelation Auction is credible as long as the commitment fees of each bidder is at least their optimal reserve price.

Definition 5.2 (Monotone Hazard Rate (MHR)). *A one dimensional distribution F has monotone hazard rate if the hazard rate $h(x)$ is monotone decreasing for $x \in [u^F_{min}, u^F_{max}]$. We call such an F a Monotone Hazard Rate, or MHR distribution.*

In the second-price auction, an ideal safe deviation for the auctioneer is to force the highest bidder to pay for his bid instead of the second-highest bid – obviously no deviation is safe if a bidder is asked to pay higher than his bid. The next Lemma states a property of α-strongly regular distributions by showing that the expectation of random variable v is not too far from the expectation of the virtual value $\phi(v)$ when we condition on $v \geq r$ where r is the optimal reserve of the distribution.

Lemma 5.1. *For α-strongly regular D, let r be the optimal reserve price of D. For random variable X with distribution D, let E be some event that implies $X \geq r$, then*

$$E_{X\leftarrow D}[X|E] \leq E_{X\leftarrow D}[\phi(X)|E] + \frac{1-\alpha}{\alpha} E_{X\leftarrow D}[\phi(X)|E] + r$$

Theorem 5.3. *Assume bidders have independent private values and bidder i has α_i-strongly regular distribution D_i. If DRA is an optimal auction and the commitment fee for each bidder is at least their reserve price, then asymptotically almost surely, the auctioneer's revenue under any safe deviation is at most*

$$E_{v\leftarrow D}\left[\sum_{i=1}^{n} \pi_i(v)\phi_i(v_i)\right] + E_{v\leftarrow D}\left[\sum_{i=1}^{n} \frac{1-\alpha_i}{\alpha_i}\pi_i(v)\phi_i(v_i)\cdot \mathbb{I}[v_i \geq k_i]\right]$$

where $\pi(v)$ is the allocation induced by the safe deviation when bidders play truthfully and have valuation v.

Proof. If DRA is an optimal auction, by Myerson's Lemma, each bidder has a reserve price $r_i = \phi_i^{-1}(0)$ and the item is allocated to bidder i with highest non-negative virtual value which pays $\phi_i^{-1}(\phi_j(v_j))$ or the reserve (whichever is higher) where bidder j is the bidder with second-highest virtual value. Let s_0 be the auctioneer's strategy that implements the optimal DRA with reserve r_i for all bidders $i \in [n]$. Let $s = (s_1, s_2, ..., s_n)$ be the strategy profile of all bidders specified by DRA – that is, given value v_i, a bidder playing s_i must commit to v_i with random string r_i. Let s_r be an optimal randomized safe deviation. By Lemma 3.2, asymptotically almost surely, the revenue of s_r is at most the revenue of the optimal deterministic safe deviation s_0' that does not violates computational binding security. Next, we bound the revenue of s_0' which directly implies a bound in the revenue of s_r.

In the view of bidder i, the auctioneer announces n_i bidders and their respective classes – that is, the j-th bidder in the view of i is declared as being sampled from $D_j^i \in \mathcal{D}$ which allows bidder i to compute virtual values $\phi_j^i(\cdot)$. Next, bidder i observes bid commitments $c^i = (c_1^i, c_2^i, ..., c_{n_i}^i)$. For commitment c_j^i, let x_j^i be the value that c_j^i commits to and define $x^i = (x_1^i, x_2^i, ..., x_{n_i}^i)$. Without loss of generality, let $x_1^i < x_2^i < ... < x_{n_i}^i$. In the view of bidder i, define the virtual value of j-th bidder as $\eta_j^i := \phi_j^i(x_j^i)$.

Because s_0' is deterministic and by Lemma 3.3, c_i does not affect the auctioneer's actions, given v, we have that x^i is deterministic – we write $x^i(b)$ to denote the bids sent to bidder i when bidders report bid profile b. We further claim that without loss of generality $x^i(v_i, v_{-i}) = x^i(v_i', v_{-i})$ for all $v_i' \in X_i$. Consider a game G where bidder i commits to $c_i = Commit(v_i, r_i)$ and another game identical to G except that bidder i commits to $c_i' = Commit(v_i', r_i)$. By Lemma 3.3, the auctioneer's actions are identical regardless of receiving commitment c_i or c_i' which implies $x^i(v_i, v_{-i}) = x^i(v_i', v_{-i})$.

The next claim bounds the revenue for the case where there is a bidder $i \in [n]$ where $\phi_i(v_i) > \eta_{n_i}^i$:

Claim 5.1. *Assuming a safe deviation s_0' does not violate the commitment security, we have*

$$E_{v\leftarrow D}[u_0(s_0', s, v)\cdot \mathbb{I}[\exists i \in [n], \phi_i(v_i) > \eta_{n_i}^i(v)]] = \sum_{i=1}^{n} E_{v\leftarrow D}[\phi_i(v_i)\pi_i(v)\cdot \mathbb{I}[\phi_i(v_i) > \eta_{n_i}^i(v)]]$$

Proof. If $\phi_i(v_i) > \eta^i_{n_i}(v)$, the item must be allocated to bidder i since there is no commitments the auctioneer can open to bidder i to proof that bidder i is not the winner. This implies for all $j \neq i$, events $\{\phi_i(v_i) > \eta^i_{n_i}(v)\}$ and $\{\phi_j(v_j) > \eta^j_{n_j}(v)\}$ are disjoint:

$$\forall i \neq j, Pr_{v\leftarrow D}[\phi_i(v_i) > \eta^i_{n_i}(v) \wedge \phi_j(v_j) > \eta^j_{n_j}(v)] = 0$$

Otherwise, strategy s'_0 is not safe and the auctioneer risks having to allocate the item to two distinct bidders. It follows, if $\phi_i(v_i) > \eta^i_{n_i}(v)$, the auctioneer must open all commitments and allocate the item to bidder i and get $p_i(v) := \phi_i^{-1}(\eta^i_{n_i}(v))$ as payment by Myerson's payment rule. It follows, the revenue is given by

$$\begin{aligned} E_{v\leftarrow D}[u_0(s'_0, s, v) \cdot \mathbb{I}[\exists i \in [n], \phi_i(v_i) > \eta^i_{n_i}(v)]] &= \sum_{i=1}^{n} E_{v\leftarrow D}[u_0(s'_0, s, v) \cdot \mathbb{I}[\phi_i(v_i) > \eta^i_{n_i}(v)]] \\ &= \sum_{i=1}^{n} E_{v\leftarrow D}[p_i(v) \cdot \mathbb{I}[\phi_i(v_i) > \eta^i_{n_i}(v)]] \end{aligned}$$

To bound the revenue in terms of virtual values, we observe that there is an ex-ante mechanism that gets the same allocation and payment:

- Request a bid from all bidders.
- Allocate the item to bidder i at price $p_i(v)$ if $\phi_i(v_i) > \eta^i_{n_i}(v)$. If $\phi_i(v_i) \leq \eta^i_{n_i}(v)$ for all $i \in [n]$, don't allocate the item.

First observe, the mechanism computes a valid allocation because events $\{\phi_i(v_i) > \eta^i_{n_i}(v)\}$ and $\{\phi_j(v_j) > \eta^j_{n_j}(v)\}$ are disjoint for $i \neq j$ when v is drawn from D.

Next, we claim the mechanism is Dominant-Strategy Incentive-Compatible (DSIC).

Definition 5.3 (Dominant-Strategy Incentive-Compatible (DSIC) Mechanism). *A mechanism (G, s) is DSIC if $\forall v \in X, \forall i \in [n], \forall s'_i \in \mathcal{S}_i$:*

$$u_i^G(s_i, s_{-i}, v) \geq u_i^G(s'_i, s_{-i}, v)$$

It follows directly from the definition that a DSIC mechanism is also BIC.

A bidder i that wins the item has no incentive to bid $b_i \neq v_i$ since $p_i(v_i, v_{-i}) = p_i(b_i, v_{-i})$ by Myerson's payment rule. For bidder i that looses the item, bidder i can bid $b_i \neq v_i$, but we have showed that $x^i(b_i, v_{-i}) = x^i(v_i, v_{-i})$ which implies bidder i can only change the allocation if $\phi_i(b_i) > \eta^i_{n_i}(v)$ requiring bidder i to pay $\phi_i^{-1}(\eta^i_{n_i}) > v_i$ getting negative utility.

Because the mechanism is feasible and BIC, we invoke Myerson's Lemma to conclude

$$\sum_{i=1}^{n} E_{v\leftarrow D}[p_i(v) \cdot \mathbb{I}[\phi_i(v_i) > \eta^i_{n_i}(v)]] = \sum_{i=1}^{n} E_{v\leftarrow D}[\phi_i(v_i) \cdot \mathbb{I}[\phi_i(v_i) > \eta^i_{n_i}(v)]]$$

□

Asymptotically almost surely, we have that $\forall i \in [n], \phi_i(v_i) \neq \eta^i_{n_i}$. The next claim bounds the revenue for the case where for all bidders $i \in [n]$, $\phi_i(v_i) < \eta^i_{n_i}$.

Claim 5.2. *For all safe deviations s'_0,*

$$E[u_0(s'_0, s, v) \cdot \mathbb{I}[\forall i \in [n], \phi_i(v_i) < \eta^i_{n_i}(v)]] \leq \sum_{i=1}^{n} E[\phi_i(v_i)\pi_i(v) \cdot \mathbb{I}[\forall i \in [n], \phi_i(v_i) < \eta^i_{n_i}(v)]] + \sum_{i=1}^{n} \frac{1-\alpha_i}{\alpha_i} E[\phi_i(v_i)\pi_i(v) \cdot \mathbb{I}[\forall i \in [n], \phi_i(v_i) < \eta^i_{n_i}(v)]]$$

Proof. For all bidders $i \in [n]$, even though $\phi_i(v_i) < \eta^i_{n_i}(v)$, the auctioneer can allocate the item to bidder i by revealing $\eta^i_\ell(v)$ if $\eta^i_\ell < \phi_i(v_i)$ and hiding $\eta^i_\ell(v)$ if $\eta^i_\ell(v) > \phi_i(v_i)$. For bidder $j \neq i$, the auctioneer reveals everything proving to bidder j that he is not the winner. Let $q_i(v)$ be the profit the auctioneer can obtain by allocating the item to bidder i. We must have $q_i(v) \leq v_i - k_i$ since the payment can be at most v_i and the penalties are at least k_i since the auctioneer must hide at least $x^i_{n_i}$ from bidder i. It follows:

$$E[u_0(s'_0, s, v) \cdot \mathbb{I}[\forall i \in [n], \phi_i(v_i) < \eta^i_{n_i}(v)]] \leq \sum_{i=1}^{n} E[(v_i - k_i)\pi_i(v) \cdot \mathbb{I}[\forall i \in [n], \phi_i(v_i) < \eta^i_{n_i}(v)]]$$

If the item is allocated to bidder i ($\pi_i(v) = 1$), then $v_i \geq k_i$; otherwise, the auctioneer gets negative profit. Because $k_i \geq r_i$, we can invoke Lemma 5.1 to conclude:

$$E[(v_i - k_i)\pi_i(v) \cdot \mathbb{I}[\forall i \in [n], \phi_i(v_i) < \eta^i_{n_i}(v)]] \leq E[\phi_i(v_i)\pi_i(v) \cdot \mathbb{I}[\forall i \in [n], \phi_i(v_i) < \eta^i_{n_i}(v)]] + \frac{1-\alpha_i}{\alpha_i} E[\phi_i(v_i)\pi_i(v) \cdot \mathbb{I}[\forall i \in [n], \phi_i(v_i) < \eta^i_{n_i}(v)]]$$

The statement follows by adding over all $i \in [n]$. □

The theorem statement follows directly from Claim 5.1 and Claim 5.2 and observing $v_i \geq k_i$ when $\pi_i(v) = 1$ and $\phi_i(v_i) < \eta^i_{n_i}(v)$. □

Corollary 5.1. *Assume bidders have independent private values and bidder i has MHR distribution D_i. If DRA is an optimal auction and the commitment fee for each bidder is at least their optimal reserve price, then asymptotically almost surely DRA is credible.*

Proof. If the prior distribution is MHR, then $\alpha_i = 1$ for all $i \in [n]$. By Theorem 5.3, the revenue is at most $\sum_{i=1}^{n} E_{v \leftarrow D}[\phi_i(v_i)\pi_i(v)]$. This revenue can be obtained by a truthful mechanism by always allocating the item to the bidder with highest non-negative virtual value and using Myerson's payment rule. □

Theorem 5.4. *Assume bidders have independent private values and bidder i has α_i-strongly regular distribution D_i. For every $\epsilon > 0$, there is a commitment fee $k = poly(1/\epsilon, n, max_{i \in [n]} r_i)$ and allocation where asymptotically almost surely DRA is an optimal strategy-proof ϵ-credible mechanism.*

REFERENCES

[1] Mohammad Akbarpour and Shengwu Li. Credible mechanisms. *Available at SSRN 3033208*, 2019.

[2] William Vickrey. Counterspeculation, auctions, and competitive sealed tenders. *The Journal of finance*, 16(1):8–37, 1961.

[3] William Vickrey. Optimal auctions. *The American Economic Review*, 71(3):381–392, 1981.

[4] Roger B Myerson. Optimal auction design. *Mathematics of operations research*, 6(1):58–73, 1981.

[5] Hal R Varian. Position auctions. *international Journal of industrial Organization*, 25(6):1163–1178, 2007.

[6] Benjamin Edelman, Michael Ostrovsky, and Michael Schwarz. Internet advertising and the generalized second-price auction: Selling billions of dollars worth of keywords. *American economic review*, 97(1):242–259, 2007.

[7] Peter Cramton et al. Spectrum auctions. *Handbook of telecommunications economics*, 1:605–639, 2002.

[8] Dan Ariely and Itamar Simonson. Buying, bidding, playing, or competing? value assessment and decision dynamics in online auctions. *Journal of Consumer psychology*, 13(1-2):113–123, 2003.

[9] Patrick Bajari and Ali Hortaçsu. The winner's curse, reserve prices, and endogenous entry: Empirical insights from ebay auctions. *RAND Journal of Economics*, pages 329–355, 2003.

[10] Ye Diana Wang and Henry H Emurian. An overview of online trust: Concepts, elements, and implications. *Computers in human behavior*, 21(1):105–125, 2005.

[11] David Lucking-Reiley. Vickrey auctions in practice: From nineteenth-century philately to twenty-first-century e-commerce. *Journal of economic perspectives*, 14(3):183–192, 2000.

[12] Sarah Sluis. Google switches to first-price auction, Mar 2019.

[13] Torben Pryds Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. In *Annual International Cryptology Conference*, pages 129–140. Springer, 1991.

[14] Richard Cole and Tim Roughgarden. The sample complexity of revenue maximization. In *Proceedings of the forty-sixth annual ACM symposium on Theory of computing*, pages 243–252. ACM, 2014.

[15] Richard E Barlow, Albert W Marshall, Frank Proschan, et al. Properties of probability distributions with monotone hazard rate. *The Annals of Mathematical Statistics*, 34(2):375–389, 1963.

[16] Ueli Maurer. Modelling a public-key infrastructure. In *European Symposium on Research in Computer Security*, pages 325–350. Springer, 1996.

[17] Melanie Swan. *Blockchain: Blueprint for a new economy.* " O'Reilly Media, Inc.", 2015.

[18] Ran Canetti, Yevgeniy Dodis, Rafael Pass, and Shabsi Walfish. Universally composable security with global setup. In *Theory of Cryptography Conference*, pages 61–85. Springer, 2007.

[19] Paul Klemperer. What really matters in auction design. *Journal of economic perspectives*, 16(1):169–189, 2002.

[20] Laura Doval and Vasiliki Skreta. Mechanism design with limited commitment. *arXiv preprint arXiv:1811.03579*, 2018.

[21] David McAdams and Michael Schwarz. Credible sales mechanisms and intermediaries. *American Economic Review*, 97(1):260–276, 2007.

[22] Helmut Bester and Roland Strausz. Imperfect commitment and the revelation principle: the multi-agent case. *Economics Letters*, 69(2):165–171, 2000.

[23] Qingmin Liu, Konrad Mierendorff, Xianwen Shi, and Weijie Zhong. Auctions with limited commitment. *American Economic Review*, 109(3):876–910, 2019.

[24] Andrew Chi-Chih Yao. Protocols for secure computations. In *FOCS*, volume 82, pages 160–164, 1982.

[25] Oded Goldreich. *Foundations of cryptography: volume 2, basic applications*. Cambridge university press, 2009.

[26] Satoshi Nakamoto et al. Bitcoin: A peer-to-peer electronic cash system. 2008.

[27] Andrew Chi-Chih Yao. How to generate and exchange secrets. In *27th Annual Symposium on Foundations of Computer Science (sfcs 1986)*, pages 162–167. IEEE, 1986.

[28] Oded Goldreich, Silvio Micali, and Avi Wigderson. How to play any mental game. In *Proceedings of the nineteenth annual ACM symposium on Theory of computing*, pages 218–229. ACM, 1987.

[29] David Chaum, Claude Crépeau, and Ivan Damgard. Multiparty unconditionally secure protocols. In *Proceedings of the twentieth annual ACM symposium on Theory of computing*, pages 11–19. ACM, 1988.

[30] Matthew K Franklin and Michael K Reiter. The design and implementation of a secure auction service. *IEEE Transactions on Software Engineering*, 22(5):302–312, 1996.

[31] Richard Cleve. Limits on the security of coin flips when half the processors are faulty. In *Proceedings of the eighteenth annual ACM symposium on Theory of computing*, pages 364–369. ACM, 1986.

[32] Phillip G Bradford, Sunju Park, Michael H Rothkopf, and Heejin Park. Protocol completion incentive problems in cryptographic vickrey auctions. *Electronic Commerce Research*, 8(1-2):57–77, 2008.

[33] Iddo Bentov and Ranjit Kumaresan. How to use bitcoin to design fair protocols. In *Annual Cryptology Conference*, pages 421–439. Springer, 2014.

[34] John R Douceur. The sybil attack. In *International workshop on peer-to-peer systems*, pages 251–260. Springer, 2002.

[35] Felix Brandt. How to obtain full privacy in auctions. *International Journal of Information Security*, 5(4):201–216, 2006.

[36] Michael O Rabin, Rocco A Servedio, and Christopher Thorpe. Highly efficient secrecy-preserving proofs of correctness of computations and applications. In *22nd Annual IEEE Symposium on Logic in Computer Science (LICS 2007)*, pages 63–76. IEEE, 2007.

[37] Hannu Nurmi and Arto Salomaa. Cryptographic protocols for vickrey auctions. *Group Decision and Negotiation*, 2(4):363–373, 1993.

[38] Felix Brandt. Cryptographic protocols for secure second-price auctions. In *International Workshop on Cooperative Information Agents*, pages 154–165. Springer, 2001.

[39] Felix Brandt. Secure and private auctions without auctioneers. *Technical Report FKI-245–02. Institut fur Informatick, Technishce Universitat Munchen*, 2002.

[40] Danny Dolev and Andrew Yao. On the security of public key protocols. *IEEE Transactions on information theory*, 29(2):198–208, 1983.
[41] Stuart Gerhard Stubblebine and Paul F Syverson. Fair on-line auctions without special trusted parties. In *International Conference on Financial Cryptography*, pages 230–240. Springer, 1999.
[42] David C Parkes, Michael O Rabin, Stuart M Shieber, and Christopher Thorpe. Practical secrecy-preserving, verifiably correct and trustworthy auctions. *Electronic Commerce Research and Applications*, 7(3):294–312, 2008.
[43] Joseph Halpern and Vanessa Teague. Rational secret sharing and multiparty computation. In *Proceedings of the thirty-sixth annual ACM symposium on Theory of computing*, pages 623–632. ACM, 2004.
[44] S Dov Gordon and Jonathan Katz. Rational secret sharing, revisited. In *International Conference on Security and Cryptography for Networks*, pages 229–241. Springer, 2006.
[45] Gillat Kol and Moni Naor. Cryptography and game theory: Designing protocols for exchanging information. In *Theory of Cryptography Conference*, pages 320–339. Springer, 2008.
[46] R Preston McAfee and John McMillan. Auctions with entry. *Economics Letters*, 23(4):343–347, 1987.
[47] Dan Levin and James L Smith. Equilibrium in auctions with entry. *The American Economic Review*, pages 585–599, 1994.
[48] Uriel Feige and Adi Shamir. Zero knowledge proofs of knowledge in two rounds. In *Conference on the Theory and Application of Cryptology*, pages 526–544. Springer, 1989.
[49] Manuel Blum, Paul Feldman, and Silvio Micali. Non-interactive zero-knowledge and its applications. In *Proceedings of the twentieth annual ACM symposium on Theory of computing*, pages 103–112. ACM, 1988.
[50] Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. In *Conference on the Theory and Application of Cryptographic Techniques*, pages 186–194. Springer, 1986.
[51] Richard Cole and Shravas Rao. Applications of α-strongly regular distributions to bayesian auctions. *ACM Transactions on Economics and Computation (TEAC)*, 5(4):18, 2017.
[52] Roger B Myerson. Incentive compatibility and the bargaining problem. *Econometrica: journal of the Econometric Society*, pages 61–73, 1979.
[53] Ran Canetti and Marc Fischlin. Universally composable commitments. In *Annual International Cryptology Conference*, pages 19–40. Springer, 2001.
[54] MH Hooshmand. Ultra power and ultra exponential functions. *Integral Transforms and Special Functions*, 17(8):549–558, 2006.

A OMITTED PROOFS OF SECTION 4

Proof of Theorem 4.2. We will consider an auction with single bidder drawn from a continuous distribution D with infinite expected value. We will first define D such that even though it has infinite expected value, the tail of D is not too heavy so that with a finite commitment fee we can limit the revenue the auctioneer can obtain. Similarly to the proof of Theorem 4.1, we will assume the bidding space X is finite but sufficiently dense such that any computational errors from bid rounding is negligible.

Let's first define an extension of tetration for positive real numbers.

$$h(x) := \begin{cases} 1 + x & \text{, for } x \leq 0 \\ e^{h(x-1)} & \text{, for } x > 0 \end{cases}$$

This function is continuous and differentiable ([54] for a detailed analysis of ultra exponential functions). Differentiating with respect to x,

$$h'(x) = \begin{cases} 1 & \text{, for } x \leq 0 \\ h(x)h'(x-1) & \text{, for } x > 0 \end{cases}$$

Define the natural super-logarithm $\ln^*(\cdot)$ to be the inverse of $h(\cdot)$. More formally, $\ln^*(x) = y$ if and only if $h(y) = x$ which implies the following property for every $x \in \mathbb{R}$,

$$\ln^*(e^x) = 1 + \ln^*(x)$$

In addition, we have $\ln^*(1) = 0$. Informally, one can interpret $\ln^*(x)$ as counting how many times one must take the natural-logarithm of x to get 1. We define the distribution D supported on $[1, \infty)$

in terms of the probability measure $Pr_{X\leftarrow D}[X \geq x] := 1 - F(x)$ where

$$1 - F(x) := \begin{cases} 1 & \text{, for } x \leq 1 \\ \frac{d}{dx} \ln^*(x) & \text{, for } x > 1 \end{cases}$$

By the chain rule $1-F(x) = \frac{1}{h'(\ln^*(x))}$. To see this is a valid distribution, observe $1-F(x)$ is monotone decreasing, $1 - F(1) = 1$, and $\lim_{n\to\infty} 1 - F(n) = 0$. Next, we show D satisfy the assumption of having infinity expected value.

Claim A.1. $E_{X\leftarrow D}[X] = \infty$

Proof. For a positive continuous random variable X, it is known that $E_{X\leftarrow D}[X] = \int_0^\infty Pr_{X\leftarrow D}[X \geq x]dx$, then

$$\begin{aligned} E_{X\leftarrow D}[X] &= 1 + \int_1^\infty Pr_{X\leftarrow D}[X \geq x]dx \\ &= 1 + \lim_{n\to\infty} \ln^* n - \ln^* 1 = \infty \end{aligned}$$

□

For every safe deviation from the auctioneer, a bidder drawn from D observes $n \geq 0$ commitments in the commitment phase and the auctioneer reveals a subset of those commitments in the allocation phase. If $n = 0$, the auctioneer's revenue is maximized by selecting the optimal reserve price. In the next claim, we show that for every price $p \geq 0$, $rev(p) := pPr_{X\leftarrow D}[X \geq p] \leq 1$.

Claim A.2. *For all $x \in \mathbb{R}^+$, $rev(x) \leq 1$.*

Proof. If $x(1 - F(x)) > 1$, we must have $x > 1$. If $x > 1$, $\ln^* x > 0$ and by the recursive definition of $h'(x)$, we can expand $h'(\ln^* x)$:

$$\begin{aligned} 1 - F(x) = \frac{1}{h'(\ln^* x)} &= \frac{1}{h(\ln^* x)h'(\ln^*(x-1))} \\ &= \frac{1}{xh'(\ln^* x - 1)} \\ &\leq \frac{1}{x} \end{aligned}$$

where the last inequality follows from $h'(x) \geq 1$ for all $x \in (1, \infty)$. This implies, $rev(x) = x(1 - F(x)) \leq 1$. □

Suppose for contradiction, the auctioneer can extract infinite revenue from a bidder drawn from D when the commitment fee $k = h(2) = e^e$. This implies for all $L > 0$, there is a $n > 0$ where the auctioneer submit commitments for $x \in R^n_+$ (without loss assume $x_1 < x_2 < \ldots < x_n$) and the auctioneer gets revenue at least L.

The optimal strategy for the auctioneer consists on observing the value v of the bidder, then hiding x_i if $x_i > v$ and revealing x_i if $x_i \leq v$ and $x_i > k(n - i)$. It follows, the optimal revenue for the auctioneer is given by:

$$\sum_{i=1}^{n} \max\{0, x_i - k(n-i)\} Pr[v \in [x_i, x_{i+1})]$$

where we can write $Pr[v \in [x_i, x_{i+1})] = F(x_{i+1}) - F(x_i)$ and define $1-F(x_{n+1}) = \lim_{y\to\infty}(1-F(y)) = 0$.

Next, we argue the auctioneer must submit at least $m+1$ commitments bids to obtain revenue $L > m$. By Claim A.2, the auctioneer can obtain at most revenue m when it submits m commitments:

$$\begin{aligned}\sum_{i=1}^{m}(x_i - k(m-i))Pr[v \in [x_i, x_{i+1})] &\leq \sum_{i=1}^{m} x_i Pr[v \geq x_i] \\ &\leq m\end{aligned}$$

When $L > 2$, we must have $n > 2$ which implies $x_1 \geq k(n-1) > k$; otherwise, to get x_1 as payment by hiding $x_2, ..., x_n$, the auctioneer pays a penalty of $k(n-1) > x_1$ and the auctioneer could get at least the same revenue by not committing to x_1.

Now let m be the index where for all $1 \leq i \leq m$, $x_i < e^n$ and for all $m < i \leq n$, $x_i \geq e^n$. We will first bound the contribution of fake bids $x_{m+1}, ..., x_n$ to the revenue:

$$\begin{aligned}\sum_{i=m+1}^{n}(x_i - k(n-i))Pr[v \in [x_i, x_{i+1})] &\leq \sum_{i=m+1}^{n} x_i Pr[v \geq x_i] \\ &= \sum_{i=m+1}^{n} \frac{x_i}{x_i \ln x_i h'(\ln^* x_i - 2)} \quad \text{(By the fact } x_i \geq k = h(2)\text{)} \\ &\leq \sum_{i=m+1}^{n} \frac{1}{nh'(\ln^* x_i - 2)} \quad \text{(By the fact } x_i \geq e^n\text{)} \\ &\leq \frac{n}{nh'(0)} \quad \text{(Because } x_i \geq e^e \text{ and } h'(\cdot) \text{ is monotone increasing)} \\ &\leq 1\end{aligned}$$

Next, we bound the contribution of fake bids $x_1, ..., x_m$ to the revenue:

$$\begin{aligned}\sum_{i=1}^{m}(x_i - k(n-i))Pr[v \in [x_i, x_{i+1})] &\leq \sum_{i=1}^{m} x_i[(1-F(x_i)) - (1-F(x_{i+1}))] \\ &= \sum_{i=2}^{m} x_i(1-F(x_i)) + x_1(1-F(x_1)) - \sum_{i=2}^{m} x_{i-1}(1-F(x_i))\end{aligned}$$

By Claim A.2, we have $x_1(1-F(x_1)) \leq 1$, then

$$\begin{aligned}\sum_{i=2}^{m} x_i(1-F(x_i)) + x_1(1-F(x_1)) - \sum_{i=2}^{m} x_{i-1}(1-F(x_i)) &\leq \sum_{i=2}^{m}(x_i - x_{i-1})(1-F(x_i)) + 1 \\ &= \sum_{i=2}^{m}\int_{x_{i-1}}^{x_i}(1-F(x_i))dx + 1\end{aligned}$$

Because $1-F(x)$ is monotone decreasing,

$$\begin{aligned}\sum_{i=2}^{m}\int_{x_{i-1}}^{x_i}(1-F(x_i))dx + 1 &\leq \sum_{i=2}^{m}\int_{x_{i-1}}^{x_i}(1-F(x))dx + 1 \\ &= \int_{x_1}^{x_m}(1-F(x))dx + 1\end{aligned}$$

Bellow, in the first inequality, we use the fact $x_1 \geq n-1$, $x_m \leq e^n$, $1-F(x) \geq 0$. In the first equality, we use the definition $1-F(x) = \frac{d}{dx}\ln^*(x)$ for $x \geq 1$,

$$\begin{aligned}\int_{x_1}^{x_m}(1-F(x))dx + 1 &\leq \int_{n-1}^{e^n}(1-F(x))dx + 1\\ &= \ln^*(e^n) - \ln^*(n-1) + 1\\ &= 1 + \ln^*(n) - \ln^*(n-1) + 1\\ &\leq 3\end{aligned}$$

Combining the individual contributions to the revenue of fake bids $x_1, ..., x_m$ and $x_{m+1}, ..., x_n$, the revenue the auctioneer can obtain is at most 4 when the commitment fee is $k = e^e$ which completes the proof.

□

B OMITTED PROOFS OF SECTION 5

Proof of Theorem 5.1. Let $rev(p) := pPr_{v\leftarrow D}[v \geq p]$, $k = r + \frac{r}{1-\alpha}\left(\left(\frac{2}{\alpha}\right)^{\frac{1-\alpha}{\alpha}} - 1\right)$. If there is a single bidder, the only possible strategy for the auctioneer consists in submitting fake bids $x_1, ..., x_m \in \mathbb{R}^m$ for some $m \geq 0$. When $m = 0$, the auctioneer behaves honestly. If $m = 1$, the auctioneer cannot get more revenue than posting an optimal reserve price. To see, observe the auctioneer never hides x_1 to get the the reserve as payment since $(r-k) \leq 0$. This implies the revenue is $x_1 Pr[v \geq x_1] \leq rPr[v \geq r]$. Assuming $m > 1$, we must have $x_1 > k$; otherwise, $(x_1 - k) \leq 0$ which implies the auctioneer gets no revenue by submitting x_1 as a fake bid. Without loss of generality, let $k < x_1 < x_2 < ... < x_m$. For the optimal strategy, the auctioneer reveals x_i if $x_i \leq v$ and hides x_i if $x_i > v$. Define $F(x_{m+1}) = \lim_{y\to\infty} F(y) = 1$, then the revenue is:

$$\begin{aligned}\sum_{i=1}^{m}(x_i - k(m-i))Pr[v \in [x_i, x_{i+1})] &\leq \sum_{i=1}^{m} x_i(F(x_{i+1}) - F(x_i))\\ &= x_1(1-F(x_1)) + \sum_{i=2}^{m} x_i(1-F(x_i)) - \sum_{i=2}^{m+1} x_{i-1}(1-F(x_i))\\ &= \sum_{i=2}^{m}(x_i - x_{i-1})(1-F(x_i)) + x_1(1-F(x_1))\\ &= \sum_{i=2}^{m}\int_{x_{i-1}}^{x_i} 1-F(x_i)dx + x_1(1-F(x_1))\\ &\leq \sum_{i=2}^{m}\int_{x_{i-1}}^{x_i} 1-F(x)dx + x_1(1-F(x_1))\\ &\leq \int_{x_1}^{\infty} 1-F(x)dx + x_1(1-F(x_1))\end{aligned}$$

To bound the integral, we first use Lemma C.2 and observe $x_1 > k \geq r + \frac{r}{1-\alpha}\left(\left(\frac{2}{\alpha}\right)^{\frac{1-\alpha}{\alpha}} - 1\right)$:

$$\begin{aligned}
\int_{x_1}^{\infty} 1 - F(x)dx &\leq (1 - F(r)) \int_{x_1}^{\infty} \left(\frac{r}{\alpha r + (1-\alpha)x}\right)^{\frac{1}{1-\alpha}} dx \\
&= (1 - F(r))\left[\frac{-(1-\alpha)}{\alpha}\left(\frac{r}{\alpha r + (1-\alpha)x}\right)^{\frac{\alpha}{1-\alpha}} \frac{r}{1-\alpha}\right]_{x=x_1}^{x=\infty} \\
&= (1 - F(r))\frac{r}{\alpha}\left(\frac{r}{\alpha r + (1-\alpha)x_1}\right)^{\frac{\alpha}{1-\alpha}} \\
&\leq rev(r)\frac{1}{\alpha}\left(\frac{\alpha}{2}\right) = \frac{rev(r)}{2}
\end{aligned}$$

To bound $x_1(1 - F(x_1))$, we first invoke Lemma C.2, then we use the fact $x_1 > k$:

$$\begin{aligned}
x_1(1 - F(x_1)) &\leq r(1 - F(r))\frac{x_1}{r}\left(\frac{r}{\alpha r + (1-\alpha)x_1}\right)^{\frac{1}{1-\alpha}} \\
&\leq rev(r)\frac{1}{1-\alpha}\left(\left(\frac{2}{\alpha}\right)^{\frac{1-\alpha}{\alpha}} - \alpha\right)\left(\frac{2}{\alpha}\right)^{-\frac{1}{\alpha}} \\
&= rev(r)\frac{1}{2}\frac{\alpha}{1-\alpha}(1 - \alpha^{\frac{1}{\alpha}}) \\
&\leq \frac{rev(r)}{2}
\end{aligned}$$

where in the last inequality we use the fact $\frac{\alpha}{1-\alpha}(1-\alpha^{\frac{1}{\alpha}}) \leq 1$ for $\alpha \in (0, 1)$. Combining the inequalities, we have that the revenue is at most $rev(r) = rPr[v \geq r]$ which concludes the proof. □

Proof of Theorem 5.2. For the proof, we will construct an adaptive strategy for every commitment fee k. Informally, the auctioneer will behave honestly with all bidders except the last one and induce those bidders to reveal their bids. Given what was observed, the auctioneer decide based on how big the highest bid is so far to submit or not a fake bid to the last bidder. The observation is that even if the last bidder is not the highest bidder, the auctioneer loses nothing by shill bidding since the item can safely be allocated to one of the first $n - 1$ bidders. When the last bidder is the highest bidder and the auctioneer submit a fake bid, v_n will be sufficiently large such that even when the auctioneer has to hide a fake bid, the penalty k is negligible when compared with the payments.

Define the distribution density functions:

$$F^{\alpha}(v) = \begin{cases} 0 & , v < 1 \\ 1 - \left(\frac{1}{v}\right)^{\frac{1}{1-\alpha}} & , v \geq 1 \end{cases} \qquad f^{\alpha}(v) = \begin{cases} 0 & , v < 1 \\ \frac{1}{1-\alpha}\left(\frac{1}{v}\right)^{\frac{2-\alpha}{1-\alpha}} & , v \geq 1 \end{cases}$$

The hazard rate of F^{α} is $h^{F^{\alpha}}(v) = \frac{1}{(1-\alpha)v}$ for $v \geq 1$ and the virtual value function of F^{α} is $\phi^{F^{\alpha}}(v) = v - \frac{1}{h^{F^{\alpha}}(v)} = \alpha v$.

Define the threshold $T = \frac{k+1}{(1-\alpha)(1-(3/4)^{1-\alpha})}$. Consider the auctioneer's strategy s_0' that first request commitment c_i from bidder $i = 1, \ldots, n$. Forward c_{-i} to bidder $i = 1, \ldots, n-1$ learning $v_1, \ldots, v_{n-1}$. Let $i^* = \arg\max_{i \in \{1,\ldots,n-1\}} v_i$. If $v_{i^*} < T$, continue the execution of the auction honestly. If $v_{i^*} \geq T$, submit commitments to bids $v_1, \ldots, v_{n-1}, v_{i^*} + k$ to bidder n and request bidder n to reveal v_n. If $v_n \leq v_{i^*}$, allocate the item to bidder i^* and charge the second highest bid. If $v_n \in (v_{i^*}, v_{i^*} + k)$,

allocate the item to bidder n by revealing $v_1, ..., v_{n-1}$ and hiding $v_{i^*} + k$. If $v_n \geq v_{i^*} + k$, reveal everything and allocate the item to bidder n.

By inspection, strategy s_0' is a safe deviation from the second-price commitment auction. In addition, when compared to the second-price commitment auction, the payment received by the auctioneer only differ when $v_n > v_{i^*} \geq T$. This is due to the fact that when $v_n \leq v_{i^*}$, the auctioneer maximizes revenue by allocating the item to bidder i^* and charging the second highest bid as payment even if the auctioneer submit a fake bid to bidder n.

We first upper bound the probability that $v_n \in (x, x+k)$ given that $v_n \geq x$ for all $x \geq 1$,

$$\begin{aligned} Pr[v_n \in (x, x+k) | v_n \geq x] &= \int_x^{x+k} \frac{f^\alpha(v)}{1 - F^\alpha(x)} dv \\ &\leq \int_x^{x+k} \frac{f^\alpha(x)}{1 - F^\alpha(x)} dx \\ &= k h^{F^\alpha}(x) = \frac{k}{(1-\alpha)x} \end{aligned}$$

Next, we compute the expected revenue for the auctioneer conditioned on v_n being the highest bid, and the second highest bid being $x \geq 1 + k$. Recall that when $v_n \in (x, x+k)$, the auctioneer hide the fake bid $x + k$ and charge x from bidder n. When $v_n \geq x + k$, the auctioneer reveal all the bids and charge $x + k$ from bidder n.

$$\begin{aligned} E[u_0(s_0', s, v) | v_n > x] &= E[(x-k) \cdot \mathbb{I}[v_n \in (x, x+k)] | v_n > x] + E[(x+k) \cdot \mathbb{I}[v_n \geq x+k] | v_n > x] \\ &= x - k Pr[v_n \in (x, x+k) | v_n > x] + k Pr[v_n \geq x + k | v_n > x] \\ &\geq x - \frac{k^2}{(1-\alpha)x} + k \left(\frac{x}{x+k} \right)^{\frac{1}{1-\alpha}} \end{aligned}$$

Observe $\left(\frac{x}{x+k}\right)^{1/(1-\alpha)}$ is a monotone increasing with respect to x. Using the fact $x \geq \frac{k(3/4)^{1-\alpha}}{(1-\alpha)(1-(3/4)^{1-\alpha})}$, we have

$$\begin{aligned} E[u_0(s_0', s, v) | v_n > x] &\geq x - k \left(\frac{1}{(3/4)^{1-\alpha}} - 1 \right) + k \left(\frac{(3/4)^{1-\alpha}}{(3/4)^{1-\alpha} + (1-\alpha)(1-(3/4)^{1-\alpha})} \right)^{\frac{1}{1-\alpha}} \\ &\geq x - k \left(\frac{1}{(3/4)^{1-\alpha}} - 1 \right) + \frac{3}{4} k \\ &\geq x - \frac{1}{3} k + \frac{3}{4} k = x + \frac{5}{12} k \end{aligned}$$

Finally, observe the expected revenue for the auctioneer conditioned on v_n not being the highest bid or $v_1, ..., v_{n-1} < T$ is the same as the expected revenue of the auctioneer when honestly implementing the auction. When v_n is the highest bid and $v_{i^*} \geq T$, we showed the auctioneer get revenue strictly higher than x. Formally, we apply the tower rule by computing the conditional

expectation when $v_{i^*} = x$:

$$\begin{aligned}
E[u_0(s_0', s, v)] &= E[u_0(s_0', s, v) \cdot \mathbb{I}[v_n \le v_{i^*} \vee v_{i^*} < T]] + E[u_0(s_0', s, v) \cdot \mathbb{I}[v_n > v_{i^*}, v_{i^*} \ge T]] \\
&= E[u_0(s_0, s, v) \cdot \mathbb{I}[v_n \le v_{i^*} \vee v_{i^*} < T]] \\
&\quad + E_{v_{i^*}}[E[u_0(s_0', s, v)|v_n > x]|v_n > v_{i^*}, v_{i^*} \ge T]Pr[v_n > v_{i^*}, v_{i^*} \ge T] \\
&\ge E[u_0(s_0, s, v) \cdot \mathbb{I}[v_n \le v_{i^*} \vee v_{i^*} < T]] \\
&\quad + E_{v_{i^*}}[v_{i^*} + 5/12k|v_n > v_{i^*}, v_{i^*} \ge T]Pr[v_n > v_{i^*}, v_{i^*} \ge T] \\
&= E[u_0(s_0, s, v)] + \frac{5}{12}kPr[v_n > v_{i^*}, v_{i^*} \ge T]
\end{aligned}$$

We conclude $E[u_0(s_0', s, v)] > E[u_0(s_0, s, v)]$ which concludes the proof. □

Proof of Lemma 5.1. First, we will rewrite the expected value.

$$\begin{aligned}
E[X|E] &= E[X + \phi(X) - \phi(X)|E] \\
&= E[\phi(X)|E] + E\left[X - X + \frac{1 - F(X)}{f(X)}\middle|E\right] \quad \text{(by definition of virtual values)} \\
&= E[\phi(X)|E] + E[1/h(X)|E]
\end{aligned}$$

Event E implies $X \ge r$, then by setting $v' = X$ and $v = r$ in Lemma C.1, we have

$$\begin{aligned}
&E[X|E] \le E[\phi(X)|E] + E[(1 - \alpha)(X - r) + 1/h(r)|E] \\
\implies &E[X|E] \le \frac{E[\phi(X)|E]}{\alpha} + r \quad \text{(by the fact } h(r) = 1/r)
\end{aligned}$$

which implies the statement and concludes the proof. □

Proof of Theorem 5.4. From Theorem 5.3, it is sufficient to show that for $k = poly(n, 1/\epsilon)$,

$$\sum_{i=1}^{n} \frac{1 - \alpha_i}{\alpha_i} E[\phi_i(v_i)\pi_i(v) \cdot \mathbb{I}[v_i \ge k]] \le \epsilon$$

Let $i^* = \arg\sup_{i \in [n]} \frac{1-\alpha_i}{\alpha_i} E[\phi_i(v_i)\pi_i(v) \cdot \mathbb{I}[v_i \ge k]]$. Then, the the previous expression is bounded by:

$$n \frac{1 - \alpha_{i^*}}{\alpha_{i^*}} E_{v_{i^*} \leftarrow D_{i^*}}[\phi_{i^*}(v_{i^*}) \cdot \mathbb{I}[v_{i^*} \ge k]]$$

Let $\alpha = \alpha^{i^*}$, $r = r^{i^*}$. By the α-strong regularity property,

$$\begin{aligned}
E_{v_{i^*}\leftarrow D_{i^*}}[\phi_{i^*}(v_{i^*})|v_{i^*} \geq k] &\leq E_{v_{i^*}\leftarrow D_{i^*}}[v_{i^*}|v_{i^*} \geq k] \\
&= k + \int_k^\infty Pr_{v\leftarrow D_{i^*}}[v \geq x|v \geq k]dx \\
&\leq k + \int_k^\infty \left(\frac{\alpha r + (1-\alpha)k}{\alpha r + (1-\alpha)x}\right)^{\frac{1}{1-\alpha}} dx \quad \text{(By Lemma C.2)} \\
&= k - \left[\frac{1-\alpha}{\alpha}\left(\frac{\alpha r + (1-\alpha)x}{\alpha r + (1-\alpha)k}\right)^{-\frac{\alpha}{1-\alpha}} \frac{\alpha r + (1-\alpha)k}{1-\alpha}\right]_k^\infty \\
&= k + r + \frac{1-\alpha}{\alpha}k \\
&= \frac{k}{\alpha} + r
\end{aligned}$$

By Lemma C.2,

$$Pr_{v\leftarrow D_{i^*}}[v \geq k] \leq \left(\frac{r}{\alpha r + (1-\alpha)k}\right)^{\frac{1}{1-\alpha}}$$

Let $k = r + rx$ for some $x \geq 0$. It follows,

$$\begin{aligned}
n\frac{1-\alpha}{\alpha}E[\phi_{i^*}(v_{i^*}) \cdot \mathbb{I}[v_{i^*} \geq k]] &\leq n\frac{1-\alpha}{\alpha}\left(\frac{k}{\alpha} + r\right)\left(\frac{r}{\alpha r + (1-\alpha)k}\right)^{\frac{1}{1-\alpha}} \\
&\leq \frac{2n(1-\alpha)r(x+1)}{\alpha^2}\left(\frac{r}{\alpha r + (1-\alpha)k}\right)^{\frac{1}{1-\alpha}} \\
&\quad \text{(Using the fact } r \leq k/\alpha \text{ and } k = r(x+1)\text{)} \\
&\leq \frac{2n(1-\alpha)r(x+1)}{\alpha^2}\left(\frac{1}{1 + (1-\alpha)x}\right)^{\frac{1}{1-\alpha}} \\
&\quad \text{(Using the fact } k = r(x+1)\text{)}
\end{aligned}$$

setting $x = \frac{1}{1-\alpha}\left(\left(\frac{2nr}{\alpha^2\epsilon}\right)^{\frac{1-\alpha}{\alpha}} - 1\right)$, we have

$$\begin{aligned}
\sum_{i=1}^n \frac{1-\alpha_i}{\alpha_i}E[\phi_i(v_i)\pi_i(v) \cdot \mathbb{I}[v_i \geq k]] &\leq \frac{2n(1-\alpha)r}{\alpha^2}\frac{1}{1-\alpha}\left(\frac{2nr}{\alpha^2\epsilon}\right)^{\frac{1-\alpha}{\alpha}}\left(\frac{2nr}{\alpha^2\epsilon}\right)^{-\frac{1}{\alpha}} \\
&= \frac{2nr}{\alpha^2}\left(\frac{2nr}{\alpha^2}\right)^{-1}\epsilon \\
&= \epsilon
\end{aligned}$$

□

C STRUCTURAL LEMMAS FOR α-STRONGLY REGULAR DISTRIBUTIONS

The following lemma, follows directly from the definition of virtual values and α-strongly regular distributions [14].

Lemma C.1. *If F is an α-strongly regular distribution, then for all $v' \geq v$,*

$$h(v') \geq \frac{1}{(1-\alpha)(v'-v) + 1/h(v)} \tag{4}$$

Proof of Lemma C.1. For all $v' \geq v$, if $h(v)$ is the hazard rate of F, then $\phi(v') = 1 - 1/h(v)$. By definition of α-strongly regularity,

$$\begin{aligned} &\phi(v') - \phi(v) = v' - 1/h(v') - v + 1/h(v) \geq \alpha(v' - v) \\ \implies &1/h(v') \leq (1-\alpha)(v' - v) + 1/h(v) \end{aligned}$$

The later implies the statement. □

Lemma C.2. *Let D be an α-strongly regular distribution. For all $x \geq r$,*

$$Pr_{v \leftarrow D}[v \geq x] \leq Pr_{v \leftarrow D}[v \geq r]\left(\frac{r}{(1-\alpha)x + \alpha r}\right)^{\frac{1}{1-\alpha}}$$

Proof of Lemma C.2. Let $H(v) = \int_0^v h(x)dx$. We first claim $1 - F(v) = e^{-H(v)}$. Let $\frac{d}{dx}\ln(1 - F(x)) = -\frac{f(x)}{1-F(x)} = -h(x)$. By the fundamental theorem of calculus, $\int_0^v -h(x)dx = \ln(1 - F(v)) - \ln(1 - F(0)) = \ln(1 - F(v))$ which is equivalent to $1 - F(v) = e^{-\int_0^v h(x)dx}$.

By Lemma C.1, we have

$$\begin{aligned} H(v) &= \int_0^v h(x)dx = \int_0^r h(x)dx + \int_r^v h(x)dx \\ &\geq H(r) + \int_r^v \frac{1}{(1-\alpha)(x-r) + r}dx \\ &= H(r) + \frac{1}{1-\alpha}\Big[\ln((1-\alpha)(x-r) + r)\Big]_r^v \\ &= H(r) + \frac{1}{1-\alpha}\ln\left(\frac{(1-\alpha)v + \alpha r}{r}\right) \end{aligned}$$

It follows,

$$\begin{aligned} Pr_{v \leftarrow D}[v \geq x] &= e^{-H(x)} \\ &\leq e^{-H(r)} e^{\frac{1}{1-\alpha}\ln\frac{r}{\alpha r + (1-\alpha)x}} \\ &= Pr_{v \leftarrow D}[v \geq r]\left(\frac{r}{\alpha r + (1-\alpha)x}\right)^{\frac{1}{1-\alpha}} \end{aligned}$$

□