Unconditionally Secure First-Price Auction Protocols Using a Multicomponent Commitment Scheme

Mehrdad Nojoumian * and Douglas R. Stinson **

David R. Cheriton School of Computer Science
University of Waterloo, Waterloo, ON, N2L 3G1, Canada
{mnojoumi, dstinson}@uwaterloo.ca

Abstract. Due to the rapid growth of e-commerce technology, secure auction protocols have attracted much attention among researchers. The main reason for constructing sealed-bid auction protocols is the fact that losing bids can be used in future auctions and negotiations if they are not kept private. Our motivation is to develop a new commitment scheme to construct first-price auction protocols similar to proposed solutions in [18, 17, 19]. Our constructions are auctioneer-free and unconditionally secure whereas those protocols rely on computational assumptions and use auctioneers. As our contribution, we first propose a *multicomponent commitment scheme*, that is, a construction with multiple committers and verifiers. Consequently, three secure first-price auction protocols are proposed, each of which has its own properties. We also provide the security proof and the complexity analysis of proposed constructions.

1 Introduction

The growth of e-commerce technology has created a remarkable opportunity for electronic auctions in which various bidders compete to buy a product online. As a result, the privacy of the proposed bids is a significant problem to be resolved.

The main motivation for privacy is the fact that bidders' valuations can be used in future auctions and negotiations by different parties, say auctioneers to maximize their revenues or competitors to win the auction. As an example, suppose a bidder proposes his bid on a specific product, if this valuation is released and the bidder loses the auction, other parties can use this information in the future auctions or negotiations for the same kind of the product.

In an auction mechanism, the winner is a bidder who submitted the highest bid. To define the selling price, there exists two major approaches: *first-price auction* and *second-price auction*. In the former, the winner pays the amount that he has proposed, i.e., the highest bid. In the latter, the winner pays the amount of the second-highest bid.

* Research supported by NSERC Canada Graduate Scholarship
** Research supported by NSERC Discovery Grant 203114-06

Sealed-bid auction models have many fundamental properties. *Correctness*: determining the winner and the selling price correctly. *Privacy*: preventing the propagation of private bids, that is, losing bids. *Verifiability*: verifying auction outcomes by players. *Non-Repudiation*: preventing bidders to deny their bids once they have submitted them. Traits of private auctions are presented in [15].

1.1 Motivation

The stated problem can be resolved by creating privacy-preserving protocols for computing auction outcomes, that is, the winner as well as the selling price. Unfortunately, most of current secure auction protocols are not unconditionally secure, i.e., they rely on computational assumptions such as hardness of factoring or discrete logarithm.

Our motivation therefore is to focus on the construction of first-price secure auction protocols in which bidders' valuations are kept private while defining auction outcomes. We would like to apply a new commitment scheme in an unconditionally secure setting. Our intention is to enforce the verifiability in the sense that all parties have confidence in correctness of protocols.

In our protocols, bidders first commit to their bids before the auction starts. They then apply a decreasing price mechanism in order to define the winner and the selling price, that is, each protocol starts with the highest price and decreases the price step by step until the auction outcomes are defined. This is similar to the approach in [18, 17, 19].

The authors in the first reference use undeniable signature schemes, in the second one they apply public-key encryption schemes, and in the last one they use collision intractable random hash functions. To show how our constructions differ from these solutions, we can refer to the following improvements. First, these solutions are only computationally secure whereas our protocols are unconditionally secure. Second, they all use an auctioneer to define auction outcomes whereas our protocols only use a trusted initializer.

The main difference between all the stated constructions and the *Dutch-style auction* is the early commitments where bidders decide on their bids ahead of time and independent of whatever information they may gain during the auction. Moreover, bidders cannot change their minds while the auction is running. Finally, we can better deal with a rush condition and its potential attacks. For instance, in a Dutch-style auction, a malicious bidder or a group of colluders can wait and bid immediately after the bid of an honest player.

1.2 Literature Review

In the first design of the sealed-bid auction [6], the authors apply cryptographic techniques in a computationally secure setting to construct a secure protocol. Subsequently, various types of secure auctions were proposed in the literature.

The authors in [11] (which is modified in [12]) demonstrate *multi-round sealed-bid auction* protocols in which winners from an auction round take part in

a consequent tie-breaking second auction round. This first-price auction protocol is computationally secure in a passive adversary model and applies the addition operation of the *secure multiparty computation*. Later, some shortcomings were identified in this scheme, and then they were fixed in [14].

We can refer to other first-price secure auction protocols with computational security. In [9], the authors apply *secure function evaluation* via ciphertexts and present a Mix-and-Max auction protocol. In [13], the authors apply *homomorphic secret sharing* and prevent attacks to existing secret-sharing-based protocols. In [3], the authors use *homomorphic encryption* such as the ElGamal cryptosystem to construct cryptographic auction protocols.

We can also refer to other kinds of sealed-bid auction protocols. The *second-price auction* protocol proposed in [8], where bids are compared digit by digit by applying secret sharing techniques. The $(M+1)^{st}$*-price auction* protocol proposed in [10], where the highest M bidders win the auction and pay a uniform price. The *combinatorial auction* protocol proposed in [20], where multiple items with interdependent values are sold simultaneously while players can bid on any combination of items. All these constructions are also computationally secure.

To conclude, the authors in [4, 5] investigate the possibility of unconditional full privacy in auctions. They demonstrate that the first-price secure auction can be emulated by such a full privacy, however, the protocol's round complexity is exponential in the bid size. On the other hand, they prove the impossibility of the full privacy for the second-price secure auction for more than two bidders.

1.3 Contribution

As our main contribution, we initially construct a *multicomponent commitment scheme* where multiple committers and verifiers act on many secrets. After that, several unconditionally secure first-price auction protocols are constructed based on this new commitment scheme. Each of these protocols consists of a trusted initializer and n bidders. They also work under the honest majority assumption.

The first construction is *a verifiable protocol without the non-repudiation property*. This protocol has a low computation cost. The second construction is *a verifiable protocol with the non-repudiation property*. The computation cost of this protocol has an extra multiplication factor. The last construction is *an efficient verifiable protocol with the non-repudiation property and partial privacy*. This protocol preserves the privacy of losing bids by a security relaxation with a lower computation cost.

2 Preliminaries

2.1 Commitment Schemes

Commitment schemes were introduced by Blum [1] in order to solve the coin flipping problem. In a commitment scheme, the first party initially commits to a value while keeping it hidden, i.e., *commitment phase*. Subsequently, he reveals the committed value to the second party in order to be checked, i.e., *reveal phase*.

R. Rivest [16] proposed an unconditionally secure commitment scheme in which the sender and receiver are both computationally unbounded. He assumes the existence of a trusted initializer, Ted, and a private channel between each pair of parties. The protocol is as follows:

1. **Initialize:** Ted randomly selects a and b which define a line, and securely sends these values to Alice. He then selects a point (x_1, y_1) on this line and sends it to Bob privately: $y = ax + b, y_1 = ax_1 + b$ where $a \in \mathbb{Z}_q^*$ and $b \in \mathbb{Z}_q$.
2. **Commit:** at this phase, Alice computes $y_0 = ax_0 + b$ as a committed value and sends it to Bob, where x_0 is her secret.
3. **Reveal:** Alice discloses the pair (a, b) as well as x_0 to Bob. Finally, Bob checks that the pairs (x_0, y_0) and (x_1, y_1) are on the line $y = ax + b$. If so, Bob accepts x_0, otherwise, he rejects it.

There exists a minor problem with this scheme. In a scenario where $y_0 = y_1$ (e.g., the committed value y_0 is equal to the second value that Bob receives from Ted), Bob learns x_0 before the reveal phase, that is, if $y_0 = y_1$ then $x_0 = x_1$ because $y = ax + b$ is a one-to-one function. This problem is fixed in [2] by replacing $y_0 = ax_0 + b$ with $y_0 = x_0 + a$ in the commitment phase. We further provide the security proof of this scheme in order to show the way it works.

Theorem 1. *The presented scheme is unconditionally secure, that is, parties are computationally unbounded and the scheme satisfies binding and hiding properties with $1/q$ probability of cheating.*

Proof. **Binding**: If Alice changes her mind and decides to cheat by revealing a fake secret x_0', she needs to provide a fake line (a', b') such that $y_1 = a'x_1 + b'$ and $y_0 = a'x_0' + b'$ (since she has already committed to y_0). Suppose the actual line is $\mathcal{L}$ and the fake line is $\mathcal{L}'$. These two lines either are parallel or intersect at one point. In the former case, since $(x_1, y_1) \in \mathcal{L}$ and $\mathcal{L} \parallel \mathcal{L}'$, therefore, $(x_1, y_1) \notin \mathcal{L}'$, which means Bob does not accept (a', b') and consequently x_0'. In the latter case, Alice can cheat only if two lines intersect at (x_1, y_1), which means Alice needs to guess Bob's point (x_1, y_1) in order to be able to cheat. The probability of guessing this point is $1/q$ since all elements in $\mathbb{Z}_q$ have an equal chance of occurrence. **Hiding**: even by having an unlimited computation power, Bob can only learn the pair (x_1, y_1) and the committed value y_0 in the first two phases. Considering the modified version in [2], there is no chance for Bob to infer x_0 from (x_1, y_1) and y_0. □

2.2 Evaluation and Interpolation Costs

Now, we review computation costs of polynomial evaluation and interpolation. Using a naive approach to evaluate $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1}$ at a single point α, we need $3n - 4$ operations in the finite field. First we require $n-2$ multiplications to compute $\alpha^2 = \alpha \times \alpha, \alpha^3 = \alpha \times \alpha^2, \ldots, \alpha^{n-1} = \alpha \times \alpha^{n-2}$. Then, computing terms a_ix^i requires a further $n - 1$ multiplications. Finally, adding all terms together takes $n - 1$ additions. This approach can be improved

slightly by the Horner's evaluation. Therefore, the total cost of the evaluation for a polynomial of degree at most $n-1$ at a single point α is $O(n)$, consequently, the evaluation at n points takes $O(n^2)$. To interpolate n points and construct a polynomial of degree at most $n-1$, we need $O(n^2)$ operations using the Lagrange/Newton interpolation [7].

These techniques can be improved by using the fast multipoint evaluations (n points) and the fast interpolation of a polynomial of degree at most $n-1$. These methods take $O(\mathcal{C}(n)\log n)$, where $\mathcal{C}(n)$ is the cost of multiplying two polynomials of degree at most $n-1$. Therefore, the multipoint evaluation and the fast interpolation take $O(n\log^2 n)$ arithmetic operations using fast fourier transform, which requires the existence of a primitive root of unity in the field.

$$\mathcal{C}(n): \begin{cases} O(n^2) \text{ classical method} \\ O(n^{1.59}) \text{ Karatsuba' s method} \\ O(n\log n) \text{ Fast Fourier Transform} \end{cases}$$

3 Multicomponent Commitment Scheme ($\mathcal{MCS}$)

We first provide the formal definition of a *multicomponent commitment scheme* ($\mathcal{MCS}$), i.e., a construction with multiple committed values and verifiers.

Definition 1. *A multicomponent commitment scheme is a construction with multiple committers and several verifiers, and is said to be unconditionally secure if the following conditions are hold:*

1. ***Hiding**: each receiver is computationally unbounded and cannot learn anything regarding secret values before the reveal phase except with a negligible probability $Pr[\epsilon_1]$.*
2. ***Binding**: each sender is computationally unbounded and cannot cheat with the help of colluders in the reveal phase by sending a fake secret except with a negligible probability $Pr[\epsilon_2]$.*
3. ***Validating**: assuming the sender is honest, other honest players should be able to correctly validate each secret during the reveal phase in the presence of colluders.*

In the following constructions, we have n players $P_1, P_2, \ldots, P_n$ and a trusted initializer $\mathcal{T}$ who leaves the scheme before starting protocols. We consider the existence of a private channel between each pair of parties, and an authenticated public broadcast channel. We also assume the majority of players are honest. For the sake of simplicity, first a scheme with one committer, say P_i, and several verifiers $P_1, \ldots, P_{i-1}, P_{i+1}, \ldots, P_n$ is presented.

1. **Initialize:** $\mathcal{T}$ randomly selects a polynomial $g(x) \in \mathbb{Z}_q[x]$ of degree $n-1$, and privately sends $g(x)$ to committer P_i. He then selects $n-1$ distinct points (x_j, y_j) uniformly at random on this polynomial, and sends (x_j, y_j) to P_j for $1 \le j \le n$ and $j \ne i$ through the private channels.

$$y_1 = g(x_1) \quad y_2 = g(x_2) \quad \ldots \quad y_n = g(x_n)$$

2. **Commit:** Player P_i first selects the secret x_i and computes $y_i = g(x_i)$ as a committed value. He then broadcasts y_i to other players.
3. **Reveal:** P_i discloses the polynomial $g(x)$ and his secret x_i to other parties through the public broadcast channel. First, other players investigate the validity of $y_i = g(x_i)$, where y_i is the value that P_i has already committed to. After that, each P_j checks to see if his point is on $g(x)$, i.e., $y_j = g(x_j)$ for $1 \leq j \leq n$ and $j \neq i$. If $y_i = g(x_i)$ and the majority of players confirm the validity of $g(x)$ (or an equal number of confirmations and rejections is received), x_i is accepted as the secret of P_i, otherwise, it is rejected.

Now, we extend our approach to a construction with multiple committers and several verifiers, that is, n independent instances of the previous scheme.

1. **Initialize:** $\mathcal{T}$ randomly selects n polynomials $g_1(x), g_2(x), \ldots, g_n(x) \in \mathbb{Z}_q[x]$ of degree $n-1$, and privately sends $g_i(x)$ to P_i for $1 \leq i \leq n$. He then selects $n-1$ distinct points (x_{ij}, y_{ij}) uniformly at random on each polynomial $g_i(x)$, and sends (x_{ij}, y_{ij}) to P_j for $1 \leq j \leq n$ and $j \neq i$ through private channels. The following matrix shows the information that each player P_j receives, i.e., all entries in j^{th} row:

$$\mathcal{E}_{n\times n} = \begin{pmatrix} g_1(x) & y_{21} = g_2(x_{21}) & \cdots & y_{n1} = g_n(x_{n1}) \\ y_{12} = g_1(x_{12}) & g_2(x) & \cdots & y_{n2} = g_n(x_{n2}) \\ \vdots & \vdots & \ddots & \vdots \\ y_{1n} = g_1(x_{1n}) & y_{2n} = g_2(x_{2n}) & \cdots & g_n(x) \end{pmatrix}$$

2. **Commit:** each player P_i computes $y_i = g_i(x_i)$ as a committed value and broadcasts y_i to other players, where x_i is the secret of P_i, i.e., $y_1, y_2, \ldots, y_n$ are committed values and $x_1, x_2, \ldots, x_n$ are secrets of players accordingly.
3. **Reveal:** each player P_i discloses $g_i(x)$ and his secret x_i to other parties through the public broadcast channel. First, other players investigate the validity of $y_i = g_i(x_i)$, where y_i is the value that P_i has already committed to. In addition, they check to see if all those $n-1$ points corresponding to $g_i(x)$ are in fact on this polynomial (i.e., the validity of $g_i(x)$: $y_{ij} = g_i(x_{ij})$ for $1 \leq j \leq n$ and $j \neq i$). If $y_i = g_i(x_i)$ and the majority of players confirm the validity of $g_i(x)$ (or an equal number of confirmations and rejections is received), x_i is accepted as a secret, otherwise, it is rejected.

Theorem 2. *The proposed multicomponent commitment scheme $\mathcal{MCS}$ is an unconditionally secure construction under the honest majority assumption in an active adversary setting, that is, it satisfies the hiding, binding, and validating properties of Definition 1.*

Proof. Malicious participants might be able to provide fake polynomials and consequently incorrect secrets, or disrupt the voting result.
Hiding: when a player P_i commits to a value, each player P_j for $1 \leq j \leq n$ and $j \neq i$ only knows his pair (x_{ij}, y_{ij}) and the committed value y_i in the first two phases even by having an unlimited computation power. In the worst case

scenario, even if $\frac{n-1}{2}$ players P_j collude, they are not able to construct $g_i(x)$ of degree $n-1$ to reveal x_i. In the case where the committed value y_i of P_i is equal to y_{ij} of a player P_j, P_j might be able to infer some information about the secret x_i. This occurs with the following probability:

$$\mathbf{Pr}[y_i = y_{ij}] \leq \frac{n-1}{q} \quad \textit{for some } j \in [1,n] \textit{ and } j \neq i \tag{1}$$

Although a polynomial is not a one-to-one function (that is, two points on the polynomial with an equal y-coordinate may or may not have the same x-coordinate), a polynomial of degree $n-1$ has at most $n-1$ roots, meaning that, given (x_i, y_i) and $(x_{ij}, y_{ij}) \in g_i(x)$:

$$\textit{if} \quad \exists j \textit{ s.t. } y_i = y_{ij} \quad \textit{then} \quad \frac{1}{n-1} \leq \mathbf{Pr}[x_i = x_{ij}] \leq 1 \tag{2}$$

Consequently, with the probability $\mathbf{Pr}[\epsilon_1] = \mathbf{Pr}[y_i = y_{ij} \wedge x_i = x_{ij}]$, player P_j may know the secret x_i before the reveal phase:

$$\mathbf{Pr}[\epsilon_1] \leq \frac{n-1}{q} \quad \text{by (1) and (2)}$$

Binding: if a player P_i changes his mind and decides to cheat by revealing a fake secret x_i', he needs to provide a fake polynomial $g_i'(x)$ of degree $n-1$ such that **(a)** $y_i = g_i'(x_i')$, since he has already committed to y_i, and **(b)** $y_{ij} = g_i'(x_{ij})$ for $1 \leq j \leq n$ and $j \neq i$, meaning that $g_i(x)$ and $g_i'(x)$ must pass through $n-1$ common points, that is, P_i needs to guess all points of other players. The alternative solution for P_i is to collude with malicious players and change the voting result such that a sufficient number of players accept the fake secret x_i'. It is clear that two distinct polynomials $g_i(x)$ and $g_i'(x)$ of degree $n-1$ agree at most on $n-1$ points, therefore, for a randomly selected point (x_{ij}, y_{ij}) we have:

$$\mathbf{Pr}[y_{ij} = g_i(x_{ij}) \wedge y_{ij} = g_i'(x_{ij})] \leq \frac{n-1}{q} \tag{3}$$

Therefore, suppose we have the maximum number of colluders to support P_i and assume $n-1$ is an even number. To hold the honest majority assumption, there are always two more honest voters, i.e, $\left(\frac{n-1}{2}+1\right) - \left(\frac{n-1}{2}-1\right) = 2$. Since the committer P_i is dishonest, he can only change the voting result if he guesses at least one point of honest players, which leads to an equal number of confirmations and rejections. As a consequence, the probability of cheating with respect to the binding property is as follows:

$$\mathbf{Pr}[\epsilon_2] \leq \left(\frac{n-1}{2}+1\right) \times \left(\frac{n-1}{q}\right) = O\left(\frac{n^2}{q}\right) \quad \text{by (3)}$$

Validating: suppose the committer P_i is honest and $n-1$ is an even number, to hold the honest majority assumption, there is an equal number of honest and dishonest voters P_j for $1 \leq j \leq n$ and $j \neq i$, that is, players who are validating $g_i(x)$ belonging to P_i. Therefore, $g_i(x)$ and consequently x_i are accepted since an equal number of confirmations and rejections is achieved. □

Theorem 3. *The multicomponent commitment scheme $\mathcal{MCS}$ takes 3 rounds of communications and $O(n^2 \log^2 n)$ computation cost.*

Proof. It can be seen that every stage takes only one round of communications which comes to 3 rounds in total. To achieve a better performance, suppose we use a primitive element ω in the field to evaluate polynomials, i.e., $y_{ij} = g_i(\omega^{x_{ij}})$. As a consequence, in the first two stages, each $g_i(x)$ of degree $n-1$ is evaluated at n points with $O(n \log^2 n)$ computation cost. This procedure is repeated for n polynomials, consequently, the total cost is $O(n^2 \log^2 n)$. In the third stage, everything is repeated with the same computation cost of the first two steps, therefore, the total computation cost is $O(2n^2 \log^2 n) = O(n^2 \log^2 n)$. □

4 Sealed-Bid First-Price Auction Protocols

Now, three first-price sealed-bid auction protocols based on the multicomponent commitment scheme are presented. Our constructions are auctioneer-free in an unconditionally secure setting, i.e., bidders define auction outcomes themselves.

Our protocols consist of a trusted initializer $\mathcal{T}$ and n bidders $B_1, \ldots, B_n$ where bidders valuations $\beta_i \in [\eta, \kappa]$. Let $\theta = \kappa - \eta + 1$ denotes our price range. In cryptography constructions, an *initializer* leaves the scheme before running protocols while a *trusted authority* may stay in the scheme until the end of protocols. We consider existence of private channels between the initializer and each bidder as well as each pair of bidders. There exists an authenticated public broadcast channel on which information is transmitted instantly and accurately to all parties. Let $\mathbb{Z}_q$ be a finite field and let ω be a primitive element in this field; all computations are performed in the field $\mathbb{Z}_q$. We need n^2/q to be very small due to our commitment scheme $\mathcal{MCS}$. Therefore, q must be large enough to satisfy this requirement.

4.1 Verifiable Protocol with Repudiation Problem ($\mathcal{VR}$)

We assume majority of bidders are honest, and at most $n/2$ of bidders may collude to disrupt auction outcomes or learn losing bids.

1. **Initialize:** $\mathcal{T}$ randomly selects n polynomials $g_1(x), g_2(x), \ldots, g_n(x) \in \mathbb{Z}_q[x]$ of degree $n-1$, and privately sends $g_i(x)$ to B_i for $1 \leq i \leq n$. He then selects $n-1$ distinct points $(\omega^{x_{ij}}, y_{ij})$ uniformly at random on each polynomial $g_i(x)$, and sends $(\omega^{x_{ij}}, y_{ij})$ to B_j for $1 \leq j \leq n$ and $i \neq j$ through the private channels. Subsequently, $\mathcal{T}$ leaves the scheme.
2. **Start:** when the auction starts, each B_i commits to β_i by $\alpha_i = g_i(\omega^{\beta_i})$ and broadcasts α_i to other bidders, where β_i is the bidder's valuation. There is a specific time interval in which bidders are allowed to commit to their bids.
3. **Close:** after the closing time, bidders set the initial price γ to be the highest possible price, i.e., $\gamma = \kappa$, and then define winners as follows:

(a) The bidder B_k who has committed to γ claims that he is the winner. Consequently, he must prove $\beta_k = \gamma$. Ties among multiple winners can be simply handled by assigning priority to bidders or by a random selection after providing valid proofs by different winners.
(b) B_k also reveals $g_k(x)$ so that other bidders are able to investigate the validity of $\alpha_k = g_k(\omega^{\beta_k})$. They then check to see if all those $n-1$ points are on $g_k(x)$. If these conditions are hold based on the $\mathcal{MCS}$ protocol, B_k is accepted as the winner, otherwise, his claim is rejected.
(c) If no one claims as a winner or the bidder who claimed as a potential winner could not prove his plea, then bidders decrease the selling price by one, i.e., $\gamma = \kappa - 1$, and the procedure is repeated from stage (a).

This new protocol has many useful properties. First of all, it is a verifiable scheme in which bidders are able to investigate the correctness of auction outcomes while preserving privacy of losing bids. Second, it is a simple construction with a low computation cost. Finally, bidders are able to define auction outcomes without any auctioneers in an unconditionally secure setting. However, it has a shortcoming in the sense that a malicious player (or a group of colluders) may refuse to claim as the winner when his bid is equal to the current price γ, that is, the *repudiation problem*.

Theorem 4. *Excluding the repudiation problem, the first-price auction protocol $\mathcal{VR}$ determines auction outcomes correctly with a negligible probability of error and protects losing bids.*

Proof. Under the honest majority assumption and the proof in Theorem 2, the scheme protects all losing bids with a negligible probability of error and only reveals the highest bid. Moreover, bidders are able to verify the claim of the winner and consequently define the selling price with a negligible probability of cheating. It is worth mentioning that the protocol has definitely a winner since more than half of players are honest. In other words, in the case of the repudiation problem, the first honest bidder who has proposed the highest bid or the first malicious player who claims as the winner and has the highest bid is the winner. □

Theorem 5. *The first-price auction protocol $\mathcal{VR}$ takes at most $O(\theta)$ rounds of communications and $O(n^2 \log^2 n)$ computation cost.*

Proof. There exist two rounds of communication for the first two stages. In addition, the third phase takes at most θ rounds, which comes to $O(\theta)$ in total. To compute the computation cost, each $g_i(x)$ of degree $n-1$ is evaluated at n points in the first two steps with $O(n \log^2 n)$ computation cost, i.e, $n-1$ evaluations in the first step and one evaluation in the second step. This procedure is repeated for n bidders, as a consequence, the total cost is $O(n^2 \log^2 n)$. In the third stage, a constant number of polynomials equivalent to the number of winners are evaluated, therefore, the total computation cost for the entire protocol is $O(n^2 \log^2 n)$. Even if all players propose a unique value and we have n winners, the computation cost is the same. □

4.2 Verifiable Protocol with Non-Repudiation ($\mathcal{VNR}$)

Similar to the previous approach, we assume majority of bidders are honest and at most $n/2$ of bidders may collude to disrupt auction outcomes or learn losing bids. To handle the repudiation problem, we modify our earlier construction such that all losers prove that their bids are less than the winning price at the end of the protocol.

1. **Initialize:** The trusted initializer $\mathcal{T}$ first provides some private data through pair-wise channels and then leaves the scheme.
   (a) He randomly selects θ polynomials $g_{i1}(x), g_{i2}(x), \ldots, g_{i\theta}(x) \in \mathbb{Z}_q[x]$ of degree $n-1$ for each bidder B_i, and privately sends these polynomials to B_i for $1 \leq i \leq n$.
   (b) He then selects $n-1$ distinct points $(\omega^{x^k_{ij}}, y^k_{ij})$ for $1 \leq k \leq n$ and $k \neq i$ uniformly at random on each polynomial $g_{ij}(x)$, where $1 \leq j \leq \theta$. He finally sends these points to B_k. The following matrix shows the information that each B_k receives, i.e., all entries in k^{th} row:

$$\mathcal{E}_{n\times\theta n} = \begin{pmatrix} g_{11}(x) & \ldots & g_{1\theta}(x) & \ldots & (\omega^{x^1_{n1}}, y^1_{n1}) \ldots (\omega^{x^1_{n\theta}}, y^1_{n\theta}) \\ (\omega^{x^2_{11}}, y^2_{11}) \ldots & (\omega^{x^2_{1\theta}}, y^2_{1\theta}) & \ldots & (\omega^{x^2_{n1}}, y^2_{n1}) \ldots & (\omega^{x^2_{n\theta}}, y^2_{n\theta}) \\ \vdots & \ddots & \vdots & \ddots & \vdots \quad \ddots \quad \vdots \\ (\omega^{x^n_{11}}, y^n_{11}) \ldots & (\omega^{x^n_{1\theta}}, y^n_{1\theta}) & \ldots & g_{n1}(x) & \ldots \quad g_{n\theta}(x) \end{pmatrix}$$

2. **Start:** when the auction starts, there is a specific time interval in which bidders are allowed to commit to their bids.
   (a) Each B_i first defines his bid β_i as shown below. In fact, b_{ij}'s are elements of the vector $\mathcal{B}_i = [b_{i1}, b_{i2}, \ldots, b_{i\theta}]$. By having a constant number of 1's, elements of each $\mathcal{B}_i$ can have different permutations in this vector.

$$\beta_i = \kappa - \sum_{j=1}^{\theta} b_{ij} \text{ where } b_{ij} \in \{0, 1\}$$

   (b) Each B_i then applies a random mapping $\mathcal{M}_i(x) : \{0,1\} \rightarrow \mathbb{Z}_q$ to convert $\mathcal{B}_i$ to a new vector $\mathcal{B}'_i$ so that its elements $b'_{ij} \in \mathbb{Z}_q$. $\mathcal{M}_i(x) \in [0, q/2)$ if $x = 0$, otherwise, $\mathcal{M}_i(x) \in [q/2, q)$.
   (c) Finally, each bidder B_i for $1 \leq i \leq n$ commits to b'_{ij} by $\alpha_{ij} = g_{ij}(\omega^{b'_{ij}})$ for $1 \leq j \leq \theta$ and broadcasts all α_{ij} to other bidders.

3. **Close:** after the closing time, bidders set the initial price γ to be the highest possible price, i.e., $\gamma = \kappa$, and then define winners as follows:
   (a) B_k who has committed to γ claims he is the winner. Consequently, he must prove $\beta_k = \gamma$. Therefore, he reveals $g_{kj}(x)$ and b'_{kj} for $1 \leq j \leq \theta$. By using the inverse mappings $[0, q/2) \rightarrow 0$ and $[q/2, q) \rightarrow 1$, b_{kj} for $1 \leq j \leq \theta$ are recovered and $\beta_k = \kappa - \sum_{j=\eta}^{\kappa} b_{kj}$ is computed.

(b) If $\beta_k = \gamma$, other bidders then investigate the validity of $\alpha_{kj} = g_{kj}(\omega^{b'_{kj}})$ for $1 \leq j \leq \theta$. They also check to see if each set of $n-1$ points $(\omega^{x^i_{kj}}, y^i_{kj})$ for $1 \leq i \leq n$ and $i \neq k$ are on $g_{kj}(x)$'s. If these conditions are hold, B_k is accepted as the winner, otherwise, his claim is rejected.

(c) Each loser B_l must prove $\beta_l < \beta_k$. Therefore, each B_l reveals any subset of his commitments b'_{lj} for some $j \in \{1, \ldots, \theta\}$ such that the following condition is hold:

$$\sum_{j \in \{1,\ldots,\theta\}} b_{lj} = \kappa - \beta_k + 1$$

where b_{lj} is the inverse mapping of b'_{lj}. Obviously, B_l needs to provide valid proofs for b'_{lj}'s.

(d) If no one claims as a winner or the bidder who claimed as a potential winner could not prove his plea, then bidders decrease the selling price by one, i.e., $\gamma = \kappa - 1$, and the procedure is repeated from stage (a).

By a simple modification in this protocol, it is feasible to catch malicious bidders before determining the winner. As we decrease the price one by one, each bidder B_i must reveal one $b'_{ij} \in [q/2, q)$ (i.e, $b_{ij} = 1$) at each round, otherwise, he is removed from the scheme as a malicious bidder.

Example 1. Suppose each $\beta_i \in [0, 7]$ and all computations are performed in the field $\mathbb{Z}_{13}$. Assume $\beta_i = 7 - 5 = 2$ and the winning price is $\beta_k = 5$ or $\beta_k = 3$ in two different scenarios. $\mathcal{M}_i(x) \in [0, 7)$ if $x = 0$, otherwise, $\mathcal{M}_i(x) \in [7, 13)$. Therefore, we have the following vectors:

$$\mathcal{B}_i = \{1, 0, 1, 1, 0, 0, 1, 1\} \text{ and } \mathcal{B'}_i = \{12, 6, 10, 7, 5, 3, 11, 9\}$$

When $\beta_k = 5$, the loser B_i reveals $7-5+1 = 3$ values larger than $q/2$ in order to prove he has at least three 1's in $\mathcal{B}_i$, which shows his bid is less than the winning price. When $\beta_k = 3$, B_i reveals $7 - 3 + 1 = 5$ values larger than $q/2$ to prove his bid is less than the winning price.

Theorem 6. *The proposed first-price auction protocol $\mathcal{VNR}$ determines auction outcomes correctly with a negligible probability of error and protects losing bids. It also satisfies the non-repudiation property.*

Proof. We need to follow the same proof in Theorem 2 for the verifiability and privacy. Moreover, it is required to show that losers do not reveal any information in part (c) of stage 3. As shown in the protocol $\mathcal{VNR}$, each bidder B_i commits to θ values such that the protocol can handle the repudiation problem. Suppose the bidder B_k wins the auction.

$$\beta_k = \kappa - \sum_{j=1}^{\theta} b_{kj} \text{ where } b_{kj} \in \{0, 1\}$$

$$\beta_k = \kappa - \sum_{j \in \{1,\ldots,\theta\}} b_{kj} \text{ where each } b_{kj} = 1 \text{ by excluding all } b_{kj} = 0$$

$$\beta_k > \kappa - \sum_{j \in \{1,\ldots,\theta\}} b_{kj} - 1 = \kappa - (\sum_{j \in \{1,\ldots,\theta\}} b_{kj} + 1)$$

This illustrates that the bid of each loser B_l is exactly less than β_k if he reveals only an extra 1 compared to the winner, that is, $b_{lj} = 1$ and its corresponding commitment $b'_{lj} \in [q/2, q)$. Therefore, losers do not reveal any extra information regarding their bids. □

Theorem 7. *The protocol $\mathcal{VNR}$ takes at most $O(\theta)$ rounds of communications and $O(\theta n^2 \log^2 n)$ computation cost where θ denotes the price range.*

Proof. The analysis is similar to the computation cost of the protocol $\mathcal{VR}$ except that here we have θn polynomials $g_{ij}(x)$ of degree $n-1$ to be evaluated at n points for n bidders. □

4.3 Efficient Verifiable Protocol with Non-Repudiation ($\mathcal{EVNR}$)

We modify our previous approach in order to construct a more efficient protocol with partial privacy of bids. Let $\lambda = \lceil \log_2 \theta \rceil$ where θ denotes our price range.

1. **Initialize:** The trusted initializer $\mathcal{T}$ first provides some private data through pair-wise channels and then leaves the scheme.
   (a) He randomly selects λ polynomials $g_{i1}(x), g_{i2}(x), \ldots, g_{i\lambda}(x) \in \mathbb{Z}_q[x]$ of degree $n-1$ for each bidder B_i, and privately sends these polynomials to B_i for $1 \leq i \leq n$.
   (b) He then selects $n-1$ distinct points $(\omega^{x^k_{ij}}, y^k_{ij})$ for $1 \leq k \leq n$ and $k \neq i$ uniformly at random on each polynomial $g_{ij}(x)$, where $1 \leq j \leq \lambda$. He finally sends these points to B_k. The following matrix shows the information that each B_k receives, i.e., all entries in k^{th} row:

$$\mathcal{E}_{n\times\lambda n} = \begin{pmatrix} g_{11}(x) & \ldots & g_{1\lambda}(x) & \ldots & (\omega^{x^1_{n1}}, y^1_{n1}) \ldots (\omega^{x^1_{n\lambda}}, y^1_{n\lambda}) \\ (\omega^{x^2_{11}}, y^2_{11}) \ldots & (\omega^{x^2_{1\lambda}}, y^2_{1\lambda}) & \ldots & (\omega^{x^2_{n1}}, y^2_{n1}) \ldots & (\omega^{x^2_{n\lambda}}, y^2_{n\lambda}) \\ \vdots & \ddots & \vdots & \ddots & \vdots \quad \ddots \quad \vdots \\ (\omega^{x^n_{11}}, y^n_{11}) \ldots & (\omega^{x^n_{1\lambda}}, y^n_{1\lambda}) & \ldots & g_{n1}(x) \quad \ldots & g_{n\lambda}(x) \end{pmatrix}$$

2. **Start:** when the auction starts, there is a specific time interval in which bidders are allowed to commit to their bids.
   (a) Each bidder B_i first defines his bid β_i as shown below. The second term $(b_{i\lambda} \ \ldots \ b_{i2} \ b_{i1})_2$ is the binary representation of a positive integer in $\mathbb{Z}_q$.

$$\beta_i = \kappa - (b_{i\lambda} \ \ldots \ b_{i2} \ b_{i1})_2 \text{ where } b_{ij} \in \{0, 1\}$$

   (b) Each bidder B_i then applies a random mapping $\mathcal{M}_i(x) : \{0,1\} \rightarrow \mathbb{Z}_q$ to convert set $\{b_{i\lambda}, \ \ldots, \ b_{i2}, \ b_{i1}\}$ to a new set $\{b'_{i\lambda}, \ \ldots, \ b'_{i2}, \ b'_{i1}\}$ so that each $b'_{ij} \in \mathbb{Z}_q$. $\mathcal{M}_i(x) \in [0, q/2)$ if $x = 0$, otherwise, $\mathcal{M}_i(x) \in [q/2, q)$.
   (c) Finally, each bidder B_i for $1 \leq i \leq n$ commits to b'_{ij} by $\alpha_{ij} = g_{ij}(\omega^{b'_{ij}})$ for $1 \leq j \leq \lambda$ and broadcasts all α_{ij} to other bidders.

3. **Close:** after the closing time, bidders set the initial price γ to be the highest possible price, i.e., $\gamma = \kappa$, and then define winners as follows:
   (a) B_k who has committed to γ claims he is the winner. Consequently, he must prove $\beta_k = \gamma$. Therefore, he reveals $g_{kj}(x)$ and b'_{kj} for $1 \leq j \leq \lambda$. By using the inverse mappings $[0, q/2) \rightarrow 0$ and $[q/2, q) \rightarrow 1$, b_{kj} for $1 \leq j \leq \lambda$ are recovered and $\beta_i = \kappa - (b_{i\lambda} \ \ldots \ b_{i2} \ b_{i1})_2$ is computed.
   (b) If $\beta_k = \gamma$, other bidders then investigate the validity of $\alpha_{kj} = g_{kj}(\omega^{b'_{kj}})$ for $1 \leq j \leq \lambda$. They also check to see if each set of $n-1$ points $(\omega^{x^i_{kj}}, y^i_{kj})$ for $1 \leq i \leq n$ and $i \neq k$ are on $g_{kj}(x)$'s. If these conditions are hold, B_k is accepted as the winner, otherwise, his claim is rejected.
   (c) Each loser B_l must prove $\beta_l < \beta_k$. Therefore, each B_l reveals a minimum subset of his commitments b'_{lj} for some $j \in \{1, \ldots, \lambda\}$ such that the following condition is hold:
   $$\sum_{j \in \{1,\ldots,\lambda\}} (b_{lj} \times 2^{j-1}) > \kappa - \beta_k$$
   where b_{lj} is the inverse mapping of b'_{lj}. Obviously, B_l needs to provide valid proofs for b'_{lj}'s.
   (d) If no one claims as a winner or the bidder who claimed as a potential winner could not prove his plea, then bidders decrease the selling price by one, i.e., $\gamma = \kappa - 1$, and the procedure is repeated from stage (a).

Example 2. Suppose each $\beta_i \in [0, 7]$ and all computations are performed in the field $\mathbb{Z}_{13}$. Assume $\beta_i = 7 - (101)_2 = 7 - 5 = 2$ and the winning price is $\beta_k = 5$ or $\beta_k = 3$ in two different scenarios. $\mathcal{M}_i(x) \in [0, 7)$ if $x = 0$, otherwise, $\mathcal{M}_i(x) \in [7, 13)$. Therefore, we have the binary representation $\{1, 0, 1\}$ and its corresponding mapping $\{11, 5, 9\}$. When $\beta_k = 5$, B_i reveals his 3^{rd} commitment to prove $(1 \times 2^2) > 7 - 5$. This shows his bid is at most 3 which is less than the winning price. When $\beta_k = 3$, B_i reveals his 3^{rd} and 1^{st} commitments to prove $(1 \times 2^2 + 1 \times 2^0) > 7 - 3$. This shows his bid is at most 2 which is less than the winning price.

Theorem 8. *The first-price auction protocol $\mathcal{EVNR}$ defines auction outcomes correctly with a negligible probability of error. This protocol partially protects losing bids and satisfies the non-repudiation property.*

Proof. Similar to the previous theorem, we only analyze part (c) of stage 3 to show the partial information leakage. Suppose the bidder B_k wins the auction, each loser B_l must reveal a subset of his commitments such that $\sum_{j \in \{1,\ldots,\lambda\}} (b_{lj} \times 2^{j-1}) > \kappa - \beta_k$. We also know:

$$\beta_l = \kappa - (b_{l\lambda} \ \ldots \ b_{l2} \ b_{l1})_2$$
$$\beta_l = \kappa - \sum_{j=1}^{\lambda} (b_{lj} \times 2^{j-1})$$
$$\beta_l \leq \kappa - \sum_{j \in \{1,\ldots,\lambda\}} (b_{lj} \times 2^{j-1})$$

This illustrates that by revealing a subset of commitments, an upper bound of the losing bid is also revealed, that is, the losing bid is at most $\kappa - \sum_{j\in\{1,\ldots,\lambda\}}(b_{lj} \times 2^{j-1})$. Therefore, depending on the winning bid β_k, losers may reveal some extra information regarding their bids. □

Theorem 9. *The first-price auction protocol $\mathcal{EVNR}$ takes at most $O(\theta)$ rounds of communications and $O(\lambda n^2 \log^2 n) = O(\log_2 \theta \times n^2 \log^2 n)$ computation cost where θ denotes the price range.*

Proof. The analysis is similar to the computation cost of the protocol $\mathcal{VNR}$ except that here we have λn polynomials $g_{ij}(x)$ of degree $n-1$ where $\lambda = \lceil \log_2 \theta \rceil$. □

5 Conclusion

We initially illustrated the lack of unconditional security in sealed-bid auction protocols, and then proposed three unconditionally secure constructions. We constructed a multicomponent commitment scheme $\mathcal{MCS}$ and proposed three secure first-price auction protocols base on that construction. Table 1 represents outlines of our contributions.

Protocol	**Assumption**	**Private**	**Verifiable**	**Non-Rep**	**Round**	**Cost**
$\mathcal{VR}$	honest majority	yes	yes	no	$O(\theta)$	$O(n^2 \log^2 n)$
$\mathcal{VNR}$	honest majority	yes	yes	yes	$O(\theta)$	$O(\theta n^2 \log^2 n)$
$\mathcal{EVNR}$	honest majority	partial	yes	yes	$O(\theta)$	$O(n^2 \log_2 \theta \log^2 n)$

Table 1. Unconditionally Secure First-Price Auction Protocols Using $\mathcal{MCS}$

Our constructions are unconditionally secure. They work under the honest majority assumption without using any auctioneers. It is quite challenging to construct protocols in this setting. In other words, if one relaxes any of these assumptions, he can subsequently decrease the computation and communication complexities. For instance, constructing the proposed schemes by relying on computational assumptions, or considering the simple passive adversary model, or using many auctioneers in the protocols.

References

1. Blum, M.: Coin flipping by telephone - a protocol for solving impossible problems. In: Proceedings of the 24th Computer Society International Conference. pp. 133–137. IEEE Computer Society (1982)
2. Blundo, C., Masucci, B., Stinson, D., Wei, R.: Constructions and bounds for unconditionally secure non-interactive commitment schemes. Designs, Codes and Cryptography 26(1), 97–110 (2002)

3. Brandt, F.: How to obtain full privacy in auctions. International Journal of Information Security 5(4), 201–216 (2006)
4. Brandt, F., Sandholm, T.: (im)possibility of unconditionally privacy-preserving auctions. In: Proceedings of the 3rd International Joint Conference on AAMAS. pp. 810–817. IEEE Computer Society (2004)
5. Brandt, F., Sandholm, T.: On the existence of unconditionally privacy-preserving auction protocols. ACM Transactions on Information and System Security 11(2), 1–21 (2008)
6. Franklin, M.K., Reiter, M.K.: The design and implementation of a secure auction service. IEEE Transactions on Software Engineering 22(5), 302–312 (1996)
7. Gathen, J.V.Z., Gerhard, J.: Modern Computer Algebra. Cambridge University Press, New York, NY, USA (2003)
8. Harkavy, M., Tygar, J.D., Kikuchi, H.: Electronic auctions with private bids. In: Proceedings of the 3rd Workshop on Electronic Commerce. pp. 61–74. USENIX Association (1998)
9. Jakobsson, M., Juels, A.: Mix and match: Secure function evaluation via ciphertexts. In: 6th Int. Con. on the Theory and Application of Cryptology and Information Security, ASIACRYPT. LNCS, vol. 1976, pp. 162–177. Springer (2000)
10. Kikuchi, H.: (m+1)st-price auction protocol. In: Proceedings of the 5th International Conference on Financial Cryptography, FC. pp. 351–363. Springer (2002)
11. Kikuchi, H., Harkavy, M., Tygar, J.D.: Multi-round anonymous auction protocols. In: Proceedings of the 1st IEEE Workshop on Dependable and Real-Time E-Commerce Systems. pp. 62–69. Springer (1999)
12. Kikuchi, H., Hotta, S., Abe, K., Nakanishi, S.: Distributed auction servers resolving winner and winning bid without revealing privacy of bids. In: Proceedings of the 7th Int. Conf. on Parallel and Distributed Systems. pp. 307–312. IEEE (2000)
13. Peng, K., Boyd, C., Dawson, E.: Optimization of electronic first-bid sealed-bid auction based on homomorphic secret sharing. In: 1st International Conference on Cryptology in Malaysia. LNCS, vol. 3715, pp. 84–98. Springer (2005)
14. Peng, K., Boyd, C., Dawson, E., Viswanathan, K.: Robust, privacy protecting and publicly verifiable sealed-bid auction. In: Proceedings of the 4th Int. Conf. on Information and Communications Security, ICICS. pp. 147–159. Springer (2002)
15. Peng, K., Boyd, C., Dawson, E., Viswanathan, K.: Five sealed-bid auction models. In: Proceedings of the Australasian Information Security Workshop Conference. pp. 77–86. Australian Computer Society (2003)
16. Rivest, R.L.: Unconditionally secure commitment and oblivious transfer schemes using private channels and a trusted initializer. Tech. rep., Massachusetts Institute of Technology (1999)
17. Sako, K.: An auction protocol which hides bids of losers. In: 3rd International Workshop on Practice and Theory in Public Key Cryptography, PKC. LNCS, vol. 1751, pp. 422–432. Springer (2000)
18. Sakurai, K., Miyazaki, S.: A bulletin-board based digital auction scheme with bidding down strategy. In: Proceedings of the CrypTEC. pp. 180–187. HongKong City University (1999)
19. Suzuki, K., Kobayashi, K., Morita, H.: Efficient sealed-bid auction using hash chain. In: 3rd Annual International Conference on Information Security and Cryptology, ICISC. LNCS, vol. 2015, pp. 183–191. Springer (2000)
20. Suzuki, K., Yokoo, M.: Secure combinatorial auctions by dynamic programming with polynomial secret sharing. In: Proceedings of the 6th International Conference on Financial Cryptography, FC. LNCS, vol. 2357, pp. 44–56. Springer (2002)