Available online at www.sciencedirect.com

ScienceDirect

Computers & Security 00 (2019) 1–18

Computers & Security

www.elsevier.com/locate/procedia

Comprehensive Survey on Privacy-Preserving Protocols for Sealed-Bid Auctions

Ramiro Alvarez[1], Mehrdad Nojoumian[1]

Florida Atlantic University
Department of Computer & Electrical Engineering and Computer Science
777 Glades Road, Boca Raton, FL 33431

Abstract

The internet is a ubiquitous technology that has changed conventional human interactions. In our present time, it is not unusual for financial transactions to take place virtually with nothing more than a computer and a credit card; many times without ever having to engage face-to-face with another person. Part of these electronic transactions taking place day-to-day are not simple economic mechanisms, instead they are constructed in the form of auctions in which a key aspect is the protection of bidders. Ideally, electronic auction mechanisms should provide the following fundamental properties: privacy of the losing bids, robustness, verifiability, and non-repudiation. This can only be accomplished by proper sealed-bid auction protocols. Indeed, the main motivation for constructing sealed-bid auction protocols is the fact that auctioneers and/or sellers may use the past losing bids to maximize their revenues in future auctions and negotiations. In addition, private valuations can be used to disclose personal preferences and private information about the bidders. This paper therefore surveys existing cryptographic solutions that are used for electronic sealed-bid auction protocols, and provides the challenges that currently exist in this field. Overall, various technical approaches will be covered and the state-of-the-art will be reviewed thoroughly.

Keywords: Electronic Auctions, Seal-Bid Auctions, Privacy-Preserving Protocols.

1. Introduction

An auction is a mechanism for trading commodities among two groups, sellers and bidders. Most auctions also include an auctioneer who is responsible for arranging the auction, accepting the bids, and declaring a winner on behalf of the seller. To properly execute an auction, there must be methods for registering participants, accepting bids, and opening bids. The method employed for bidding defines the type of the auction. For instance, if an auction requires participants to bid in an increasing fashion, it is said to fall under the category of the *English auction*. On the other hand, if the opposite approach is taken, the mechanism is labeled as the *Dutch auction*, i.e., the price repeatedly decreases until someone is willing to pay the current price. This is commonly seen in perishable markets. In another type of auction, the buyers bid on a subset of items. This is known as *combinatorial auction*. General speaking, in an auction mechanism, the winner is a bidder who has submitted the highest bid. To define the selling price, there are

Email addresses: ramiroalvare2015@fau.edu (Ramiro Alvarez), mnojoumian@fau.edu@fau.edu (Mehrdad Nojoumian)

two methods: *first-price auction* and *second-price auction*. In the former, the winner pays the amount that he has proposed, i.e., highest bid. In the latter, the winner pays the amount of the second-highest bid. It is worth mentioning that the *(M+1)-price auction* is the generalization of the 2nd-price auction where $M = 1$.

In privacy-preserving auction protocols, also known as *sealed-bid auctions*, the bidders seal their bids using cryptographic technique. After the execution of the auction, only the auction outcomes, i.e., the winner and the selling price, are revealed. As a result, the losing bids are kept private. The main motivation for constructing sealed-bid auction protocols is the fact that the auctioneers and/or sellers may use the past losing bids to maximize their revenues in future auctions and negotiations. In addition, private valuations can be used to disclose personal preferences and private information about the bidders.

For instance, a subset of the highest losing bids or the average of the losing bids can motivate the sellers/auctioneers to increase the starting price or the minimum value of the bid in future auctions of similar items. Furthermore, a losing bid reveals how much a buyer is willing to pay, how interested a buyer is, or a minimum threshold of a buyer's cash, and so on. These are critical information specifically in high-end auctions for expensive items or antiques when there exists a serious competition among the bidders. Another example is the commercial websites for travel-related purchases such as airline tickets and hotel. Rumors state that, if a bidder loses in the first bidding effort, these websites store the initial losing bid on their servers or in the bidder's browser cache and never provide any offer to the bidder below that threshold in near-future. In other words, the bidder cannot go below his initial losing bid if he decides to bid again. This is not unlikely although verifying companies' secrets is hard. Therefore, if an auction protocol is executed in a way that the winner and the selling price are determined correctly without revealing the losing bids, none of the aforementioned issues will arise. Note that the 2nd-price sealed-bid auctions are also referred to as *Vickrey auctions*, named after Dr. William Vickrey. Figure 1 shows the classification of auctions.

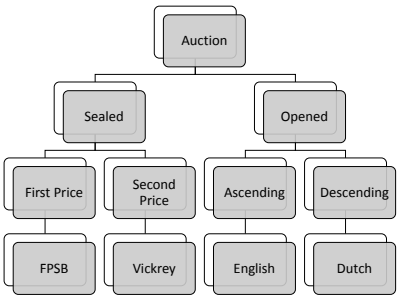

Fig. 1. Auction Classification.

1.1. Desired Properties and Trust Models

In online auctions, we face a number of challenges that do not exist in auctions taking place physically. One of the advantages of an auction taking place in person is that we can associate a bid to a bidder, which means no one can deny his participation. However, there are disadvantages such as number of people who can participate in the auction due to location or available space. With online auctions, we can overcome these kinds of problems, however we entrust the participants to follow the auction protocol honestly. A collection of unwanted features are described in [1, 2, 3, 4]. Ideally, electronic auction mechanisms should provide the following fundamental properties: privacy of the losing bids, robustness, verifiability, and non-repudiation. In addition, they may provide secrecy of the bidders' identities and anonymity, and also, guarantee fairness. These properties [5, 6] are explained in Figure 2.

Auctions consist of self-interested parties who can form strategies to achieve their personal goals. Therefore, design of a system with strategic players brings another layer of complexity to auction protocols. For instance, an auctioneer may collude with a seller to maximize the profit. This can occur in several ways, but a common method seen in the second-price auctions is to submit an artificial bid as close as possible to the winning bid for the purpose of increasing the selling price. Note that corrupted activities may occur by the sellers, bidders, or auctioneers. These challenges are out of the scope of this article and we refer the readers to the literature to learn about other complications of auctions and corresponding counter measures.

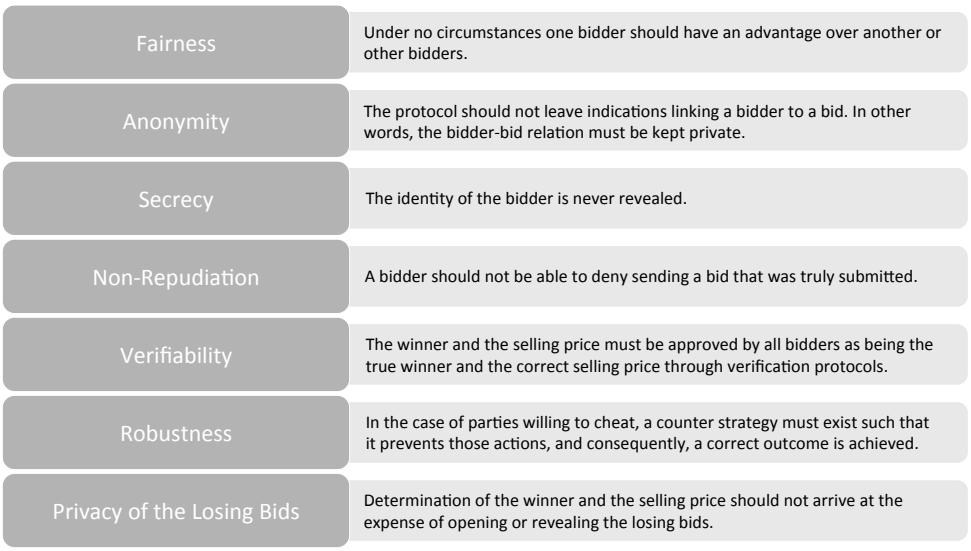

Fig. 2. Auction Properties.

Overall, an auctioneer delineating from the rules is a major concern, which is central to some of the papers in the literature. These papers consider the ideas of auctioneer trust, trusted third parties (TTP), threshold trust, distributed-bidder trust, and two-server trust. However, not all protocols are constructed with a corrupted auctioneer in mind due to computational and communication complexities as well as security challenges. Below is a summary of the trust models across the entire literature of the sealed-bid auctions.

1. *Auctioneer Trust:* A naive approach for relying on the auctioneer to follow the protocol as an honest agent of the process.
2. *Trusted Third Parties:* The auctioneers and bidders have a third party, with no personal gain from the auction, which is trusted by both. This TTP can ensure that the protocol is executed correctly.
3. *Threshold Trust:* Consist of having more than one auctioneer. The auctioneers can only collude if a number of them are working together to disrupt the protocol. This number is the threshold and as long as the number of corrupted auctioneers is less than this threshold, the auction is executed properly.
4. *Distributed-Bidder Trust:* Bidder divide the trust among themselves, there is no auctioneer involved.
5. *Two-Server Trust:* This method splits the trust between two entities. The auctioneers and the bidders each own one of the servers. Correctness is then achieved as long as two entities do not collude.

1.2. Our Motivation and Contribution

Market economies are driven by supply-and-demand. Hence, a significant number of goods do not have established prices. Auctions are a mechanism that can be utilized to determine the value of products that would otherwise be hard to estimate. They are frequently used in government contracts, markets of natural resources, and real estate. Although the revenue-equivalence theorem predicts that revenue is independent of the bidding rules, empirical data suggests that different commodities sell with higher revenues depending on the type of the auction that is used. In addition, to provide a mechanism for setting the price, sealed-bid auctions offer several benefits over the open counterpart. For instance, open auctions are prone to collusion among bidders since the face-to-face interaction provides enough information to form strategies and to learn about the opponent's behavior. Secondly, open auctions favor richer bidders, that is, the bidders with more purchasing power can learn the maximum valuation of the opponents and just bid to win the opponent rather than to place a true valuation [7]. As we stated earlier in detail, open auctions also provide an advantage for the auctioneers/sellers interested in learning about the strategies and private valuations of the bidders in order to maximize their revenues in future auctions. These factors motivated us to start preparing this comprehensive survey on privacy-preserving protocols for sealed-bid auctions.

In short, the motivation of this article is to study and scrutinize theoretical constructions of sealed-bid auction protocols that are a key element of market economies with such important advantages, i.e., a tool that shifts allocation towards the bidders, provides an equal opportunity, and generates revenue without loss of competitiveness [8]. To the best of our knowledge this is the first survey article on the sealed-bid auctions. Our contribution is to elucidate the significance, the trajectory, and the current state-of-the-art. To sum up, our contribution is to provide a comprehensive collection of pioneering and contemporary research works that is still simple-to-follow for further research and development in this domain.

1.3. Organization of the Article

Section 2 explains the necessary preliminary materials. Section 3 reviews the literature of the sealed-bid auction protocols thoroughly by the following classification: first-price sealed-bid auctions, second-price sealed-bid/Vickrey auctions, (M+1)-price sealed-bid auctions, rule-flexible sealed-bid auctions, and combinatorial sealed-bid auctions. Note that overlaps exist among different types of sealed-bid auction protocols. Section 4 provides technical discussions. Finally, Section 5 concludes with final remarks.

2. Preliminary Materials

The following section provides a basic review of the most commonly used cryptographic techniques in sealed-bid auctions. It is worth mentioning that there exist many sealed-bid auction protocols both in *passive* and *active* adversary models. In the former, the parties follow the protocols correctly but are curious to learn the losing bids. In the latter, the parties may also deviate from the protocols. Besides, the security model of a privacy-preserving protocol might be *computational* or *unconditional*. In the former, the intended properties are achieved by relying on hard mathematical problems such as *integer factoring* or *discrete logarithm* problem. In the latter, they are accomplished without relying on those problems and even if parties have an unlimited computational power. The integer factoring problem states that, it is computationally infeasible to reduce a sufficiently large integer to its prime factors. On the other hand, the discrete logarithm problem states that, given a prime number p, a generator g of finite field Z_p, and a random number x, it is easy to compute $y = g^x mod p$. However, given y, g and p, it is computationally infeasible to compute x.

2.1. Private-Key, Public-Key, and Homomorphic Encryptions

Private-key encryption, a.k.a., symmetric-key encryption, consists of fast and secure algorithms for exchanging information between two parties over insecure channels. The same key is used for encryption and decryption, making the key management a concern. Mathematically, an encryption function $E(k, m)$ uses k as a key of an encryption scheme on message m to produce cipher text c. The decryption function $D(k, c)$ then utilizes the same key k to recover the original message m such that $m = D(k, E(k, m))$.

On the other hand, *public-key encryption*, a.k.a., asymmetric-key encryption, uses different keys for encryption and decryption. At the beginning, two keys are generated. One of them is revealed publicly and the other one is kept private by the entity that is supposed to receive secret messages. Anyone wishing to send a secret message to the receiver will utilize the public-key to perform encryption. The receiver will then use the private-key to do decryption. Mathematically, $c = E(k_{pub}, m)$ is the cipher text generated by the public-key, whereas the plaintext is recovered using the private-key as follows $m = D(k_{priv}, c)$. Two commonly known public-key cryptosystems are RSA [9] and ElGamal [10]. The RSA security relies on the hardness of integer factoring, while the ElGamal relies on the hardness of the discrete logarithm problem.

Homomorphic encryption is a form of encryption that allows to process data in the encrypted format. The result of the processing remains encrypted and does not provide any access to the plaintext. Once decryption is performed, the operations that were performed over the ciphertext are reflected in the plaintext as if they had been done directly to the plaintext.

2.2. Cryptographic Hash Functions

A cryptographic hash function [11] is a function that takes as its input a message m of any size and then returns a fixed-length string, named *hash value*. Cryptographic hashes are one-way functions, i.e., once computed, it is computationally infeasible to invert the hash value and get the original message. Common hash functions are MD-5 and the SHA family such as SHA-1, SHA-2 and SHA-3.

2.3. Digital Signature Scheme

A *digital signature scheme* [12] confirms that a sender of a message is the intended source of the message and that message is also the original intended message. In other words, digital signatures can be used for properties such as authenticity and integrity. One way to construct a digital signature scheme is to use a public-key cryptosystem along with a hash function. The digital signature is then generated by taking the original message, hashing it, and encrypting the hash value with the private-key rather than the public-key. The signature and the message are then sent to the receiving party. Using the public-key, the receiver can decrypt the signature to recover the hash of the original message. If the received hash value, which is protected, is the same as the hash value that was recovered from the decryption of the signature, the receiver accepts the message as an authenticated and unchanged message.

2.4. Secret Sharing and Secure Multiparty Computation

Secret Sharing is a method for distributing a secret among a group of parties such that a subset of the players can then recover the secret when it's required. Shamir's secret sharing scheme [13], a.k.a., threshold secret sharing, consists of n players with threshold t where $t \leq n$. In this scheme, initially a random polynomial $f(x)$ of degree $t-1$ is generated by a dealer where the constant term of the polynomial is secret $f(0) = \alpha$. The dealer then sends one random point of the polynomial to each player during the sharing phase, i.e., n points or shares. We know that a polynomial of degree $t-1$ requires t distinct points to be interpolated using the Lagrange interpolation method. Thus, if t players come together during the reconstruction phase, they can recover secret sharing polynomial $f(x)$, and consequently, reconstruct $f(0) = \alpha$.

A secure multiparty computation (MPC) protocol [14] allows the participating parties to compute a function value based on their private inputs. That is, at the end of the execution, function value $f(\alpha_1, \alpha_2, \cdots, \alpha_n)$ is revealed to all players while private values $\alpha_1, \alpha_2, \cdots, \alpha_n$ are kept private. For example, suppose that Alice, Bob, and Charlie intend to enter into a voting scheme where "yes" is equivalent to choosing 1 and "no" is equivalent to selecting 0. Since we have three parties, it is clear that a sum greater than or equal to 2 indicates that the majority of the parties voted "yes," whereas 1 or 0 indicates that the majority voted "no." In this scenario, the main purpose is to learn the voting result through the summation function while keeping the individual votes private. There are two fundamental techniques to build secure MPC circuits for different functions, i.e., arithmetic versus boolean circuits. In the former, the circuit consists of secure addition and multiplication gates. In the latter, it is built based on secure boolean operations.

3. Survey on Sealed-Bid Auction Protocols

In this section, a comprehensive overview of the state-of-the-are related to sealed-bid auction protocols is provided. For the sake of readability, the section is split into the following categories: first-price, second-price/Vickrey, (M+1)-price, rule-flexible, and combinatorial selaed-bid auctions.

3.1. First-Price Sealed-Bid Auctions

In a first-price sealed-bid auction, the participants simultaneously submit their bids in a sealed format. No bidder will learn anything about the content of another bid except his/her own bid. Some of the early works on the topic include the papers of [15, 16, 17, 18, 19]. A brief description follows below. Based on a foundation of secure MPC, Kikuchi, Hakavy and Tygar [15] proposed a first-price sealed-bid auction protocol. This protocol follows a model similar to what Franklin and Reiter [20] provided, i.e., there exist one seller, multiple bidders, and multiple auctioneers. Figure 3 demonstrates the architecture of these types of common constructions. A set of prices k are published during the initialization phase. The bidders can have the option of assigning ID or zero to each price k depending on their valuations of the good. Once a bidder has prepared a sequence of bids for each k, each sequence becomes the input to a secure multiparty computation protocol. The addition operation of MPC determines the winner. For a price k, if only a single winner exists, the MPC reveals his ID; otherwise, it reveals the sum of their IDs. When no winner is found at a given price k, the result is zero. If a tie occurs, which is likely for lower discrete k values, the subsequent rounds with different bid values are constructed with the winners from the previous round.

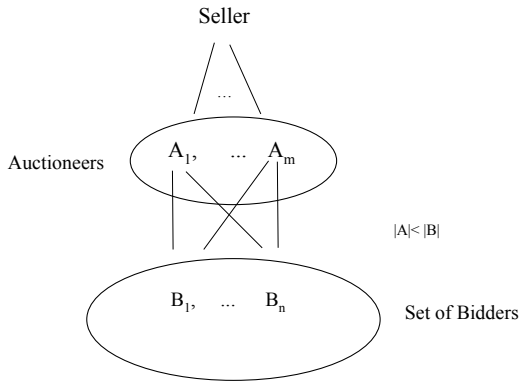

Fig. 3. Auction Model

The privacy of the protocol is then improved with extra computational cost in [21]. As suggested by [22], this protocol can be further improved to provide fairness, anonymity, and robustness. Finally, the authors of [23] created an alternative solution for better efficiency using a deniable signature scheme. This protocol offers a higher round complexity but an improved efficiency and bandwidth.

Another general scheme applicable to the first-price auction presented by [16]. Bid privacy is achieved with homomorphic encryption and MPC. The protocol does not depend on circuit evaluation, however, it requires the use of two servers in which the users only communicate with one of the servers. Homomorphic public-key encryption is used to seal the bids. Through a multiparty computation protocol, the semi-trusted third party compares the bids of two different bidders, and then, determines the highest of two values by comparing the encrypted bits starting from the most significant bit position. A result can be retrieved by the properties of the ϕ-hiding assumption. At the end of the protocol, only the highest bid is found but it can be simply extended to find the second highest bid as well. One of the disadvantages of the protocol is that, it can only function as intended with a pairwise comparison at each step.

The authors of [17] proposed a sealed-bid auction mechanism using undeniable signature schemes. The bidders use undeniable signatures to send their encrypted bids. To determine the winner, the auctioneer starts from the highest possible price. If a bidder meets the current price from the list, he must then prove it with the undeniable signature scheme. Subsequently, the auctioneer opens the bid in order to publicly verify the result. If no one meets the current price, the auctioneer moves to the next highest price until a winner is found, i.e., the Dutch-Style auction strategy. The authors of [18] utilized a public-key cryptosystem such as ElGamal or RSA to construct a similar protocol. Essentially, a set of bid values is selected from a set of possible prices. During the bidding phase, the bidders encode a message of their valuations and send them to the auctioneers. The auctioneers then begin from the highest bid value and use the associated key to decrypt each received message. When a key opens a message, it follows that the message corresponds to the current highest value. The main goal of the approach is to hide losing bids with a protocol that guarantees a bid cannot be successfully decrypted unless it is the highest bid. More specifically, it is based on a probabilistic encryption of a submitted bid that cannot be decrypted unless the bid is the highest valuation. However, the only problem is that, the auctioneers hold the key and can decide to open every received message. To circumvent this scenario, the authors suggest sharing the key among the auctioneers using secret sharing. Unlike the previous two protocols, the approach taken by [19] utilized only hash functions for a sealed-bid auction protocol. More precisely, the protocol uses an intractable hash function such as SHA-1. First, the bidders compute a hash chain on their bids with the use of a randomly selected seed. Each bid is sent to auctioneers along with a signature for the non-repudiation purpose. During the opening phase, the auctioneers perform an equality test on a given price. If no one satisfies the test of equality, the auctioneers decrease the price by one. The procedure is performed repeatedly until a price is found for which the test result is valid. As an alternative solution, the paper proposed to avoid the bidders communicating with the auctioneers during the opening phase.

Another approach utilized an off-line trusted third patry (TTP) in a Dutch-style auction using the key chaining technique [24]. In this protocol, the bidders choose a random list of integers s_{ij} and compute a list of α_{ij} where $\alpha_{ij} = g^{s_{ij}} mod p$ and $VE(s_{ij})$ can only be decrypted by the TTP if the verification is required. The list of integers is used as the input of the verifiable encryption $VE(s_{ij})$ and the output is send along with α_{ij} as tuple. The auctioneer receives the tuple in addition to a signature on that tuple. If the auctioneer can verify the received information, a certificate is sent to a particular bidder. In the final step of the registration, the auctioneer publishes the tuples as well as the ecryption key corresponding to the bidding prices on a bulletin board. Entering the bidding phase, the parties send a concatenated result that includes information such as the bidder choice on a specific price. The bidders have shares of the public-key that decrypt the bid. The possible set of prices are opened from the highest value in a decreasing order. Due to the property of the universal verifiability, the highest bid is guaranteed to be the winner of the auction. Upon finding a winner, the auctioneer can open this bid, but cannot open the losing bids. In the case of a dispute or bidders trying to disturb the protocol, the TTP can be brought to determine if a bidder is cheating or not; otherwise, he remains offline reducing the round complexity. In this paper, the method of key chaining does not yield a strong bid privacy for losing bids since the assumption is that the auctioneer and TTP will not collude. With the modification presented in [25], this problem is resolved. Essentially the key chaining is modified such that finding the highest bid completely breaks the key chain and losing bids can no longer be revealed.

In another approach [26], a new construction proposed by the use of binding group signatures. In this protocol, each bidder must be awarded a certificate that permits him to participate in the auction. Then using the private membership, a particular bidder can place a bid and sign it with a group signature scheme. A group signature on a bid is distributed using a group signature sharing scheme. During the opening phase, the auctioneers retrieve the highest bid using secure multiparty computation. They can find the identity associated with the wining bid by the revocation procedure of the group signature scheme.

In [27], the authors used homomorphic secret sharing scheme. The new idea presented in this paper is to use a form of verifiable secret sharing (VSS), namely Pedersen's secret sharing scheme [28], to prevent the sealed-bid auction from attacks that typically occurs through auctioneer-bidder collusion (ABC), bidder-bidder collusion (BBC), and a dispute strategy. The construction involves two rounds of communication. First, the bidders commit on their bids. Subsequently, they help the auctioneers to determine the winner. In short, the protocol is as follows. Each auctioneer establishes corresponding Paillier's encryption function [29] and decryption key while publishing the public encryption key and encryption function on a bulletin board. Each bidder generates a bidding vector by choosing an integer for each possible price. A non-zero random integer indicates selection of that price, whereas a zero value indicates not wanting to buy at that certain price. Using system parameter established by the group of auctioneers, the bidders commit to the bid vectors. Finally, binary search along with homomorphic secret recovery determine the winning bid. A similar scheme proposed in [30] without using any auctioneers. To remove the auctioneers from the protocol, computations are done by the bidders. Each bidder again generates a bid vector as explained above. He slices and shares his vector with the other bidders keeping only a part secret. Each bidder adds the received shares to his own vector. Assuming that no bidder shares the same highest value, the protocol can recover the winner by adding and subtracting bid vectors until the index of the highest price is found. Finally, the commitments are tested to find a matching bid. The authors in [31] proposed another similar solution based on the homomorphic encryption. Each auctioneer chooses a private-key and shares the key among the other auctioneers using threshold secret sharing. The bidders create bit-wise bid vectors with "0" indicating opting out and "1" indicating interest in a specific price. The bid vector of each bidder is encrypted with ElGammal public-key encryption scheme. Similar to other homomorphic bid opening schemes, a binary search is executed until the winning price is found. Finally, all bidders with a non-zero value for the winning price in their bid vectors are selected as winners. In a more recent work [32], the authors proposed a sealed-bid auction protocol using two managers and a zero-knowledge proof technique for the winner determination of the auction. The protocol reduces the transfer cost by using a bulletin board. The privacy and manipulation of bids are prevented using a secret database and a read-only bulletin board.

Finally, the proposed solutions in [33, 34] describes a multicomponent commitment scheme that consists of a trusted initializer and n bidders. During the initialization phase, the trusted initializer selects n polynomials of degree $n-1$, sends $g_i(x)$ to bidder B_i and also $n-1$ distinct points on each $g_i(x)$ to other bidders.

Each bidder B_i computes $y_i = g_i(\beta_i)$ as a committed value to his bid and broadcasts y_i to other bidders. The Dutch-style strategy is used to run the auction. In the reveal phase, the winner claims he is the winner at a particular price and then proves his claim by revealing his commitments. The losers also prove that their bids have been less than the winning price. To approve the winner's claim, the bidders first investigate the validity of $y_i = g_i(\beta_i)$. They then check to see if all $n - 1$ points that they have are on $g_i(x)$.

Table 1. Summary of the First-Price Sealed-Bid Auction Protocols.

Reference	Cryptographic Method	Adversary Model	Security Model
[15]	Relies on MPC, more specifically on addition property	Passive	Unconditional
[16]	Homomorphic Encryption and MPC	Active	Computational
[17]	A bid is an Undeniable Signature	Passive	Computational
[18]	ElGammal or RSA. A bid is a key pair.	Passive	Computational
[19]	Hash functions and digital signatures	Passive	Computational
[33]	Multicomponent Commitment Scheme	Passive/Active	Unconditional

3.2. Second-Price Sealed-Bid/Vickrey Auctions

In a second-price sealed-bid auction, the bidders submit to a bid taker a sealed value presumably of ones true valuation. The bidders can submit as long as the closing time is not reached. Once the allowed time of submission is passed, new bids are not accepted. Entering the opening phase, the winner is defined as the entity with the highest bid, and as the rule dictates, the winner pays the second highest valid bid.

In one of the earliest publications [35], the authors proposed the idea of constructing a second-price sealed-bid auction using cryptographic protocols. During the opening phase, the losing bids are kept private. Once a winner is determined, only the first and second largest bids are revealed in order to define the winner and the selling price. The authors suggested a series of steps to be followed in their protocol. The protocol is described for the case with only two bidders A and B along with an auctioneer C. Each bidder can represent a bid by a value in the interval $[1, 100]$. Both bidders proceed to submit encrypted messages using the auctioneer's public-key plus their own public-key. One of the bidders calculates the difference between the encrypted numbers, labeled k, and the ordinal value, labeled j. The receiver calculates a sequence based on the equation $y_u = dA(k - j + u)$ where u is all possible values of $[1, 100]$. He also computes $z_u = y_u(modq)$ where q is an arbitrary prime number. The sequence is then sent back from which the other bidder can determine if his value is strictly larger or perhaps smaller of the other valuation.

One of the earliest work in this domain is [20]. This protocols utilized the verifiable signature sharing scheme of [36] in addition to (t, n)-threshold secret sharing scheme and a digital cash. The service is constructed using more than one auction server and it allows less than a third of the auctioneers to collude in order to preserve the privacy of the losing bids. Essentially, the bidders submit bids to the corresponding server by splitting a digital coin in the form of $(v\$, Obank(v\$), ws)$ using (t, n)-threshold secret sharing, except for the middle item that utilizes a verifiable signature sharing primitive. When the bidding period is ended, the auctioneers reconstruct the bid values using one of the suggested group multicast primitive, and then declare a winner after comparing the results. Finally, the auction can collect the money easily since the verifiable signature scheme gives such a right of ownership.

[37] provided a sealed-bid auction protocol without any threshold trust. The protocol requires the use of an oblivious third party, labeled as the auction issuer who is particularly in charge of constructing the

circuit to be used by the auctioneers. The protocol behaves with a property of fairness mainly by avoiding leakage of information even if the auction issuer and the auctioneers collude. The bidders must communicate directly with two servers. The bids are encrypted before sending to the circuit. Using a boolean circuit MPC, decryption keys are shared among a few of the auctioneers. The auctioneers publish the result to be publicly verifiable.The protocol efficiency is improved by [38] using a homomorphic encryption scheme. The limitations of one of the servers cheating is the topic of [39], where a possible solution to this problem is to split each bid into two shares.

Another construction [40] proposed a protocol that resolves one of the major issues of the Vickrey auctions, more specifically, the problem that arises when the auctioneer lies about the actual value of the selling price. The proposed protocol is built with two major phases. In the first phase, each bidder encrypts a binary bid list. Encryption occurs over every bid with a different unique personal key. Encrypted bids are published on a bulletin board as a bid matrix. By publishing each bid anonymously, the auctioneer cannot insert fake bids. In the next step, decryption over the bids by the public keys determines the winner. In order to efficiently find the winner and to not reveal any unnecessary information, three methods are offered by the authors. The three search methods include: downward search, upward search, and binary search. Once a winner is found, the winning key is published. Since this is unique, only the winner can prove to be the winner of the auction. Finally, the protocol enforces a fine on bidders who attempted a key denial attack.

In a later research work [41], a new protocol without using any auctioneers was proposed. In this construction, the bidders once again create binary entries for choice of a valuation. There is "yes" or "no" choice for the price. The bidders submit shares of their bids and must jointly compute a function on all shares received for each discrete price. A personal key is associated with each bidder and price. All calculations are performed in a finite Abelian Group. For instance, computing keys is performed by using the ring transfer, which is also used to determine the winning key. One important aspect is that, the bidders can only jointly learn the winning key and nothing else is revealed. Once the winning key is published, the bidder holding the same key can be determined as the winner.

The authors of [42] constructed a protocol with verifiable discriminant of p_0-th root that requires no anonymous channel. The protocol requires two auction managers who are in charge of different tasks. AM1 handles the registration and AM2 manages the bidding phase. During the process of bidding, both managers can verify the validity of the bids, while during opening phase, any one can verify validity. The protocol is constructed with signatures based on proof of knowledge, public-key encryption, and verifiable decryption mix. AM1 chooses values $t^0_{i,k}$ and $t^1_{i,k}$ that have the $p_0 - th$ root. the bidders have the liberty to see all possible prices from the AM2's database. After selection choice, the bidders send a public-key with signature which depends on values $t^0_{i,k}$ and $t^1_{i,k}$ chosen by AM1. Validity over the bids is checked by using decryption mix and it is a matter of showing the bids have the $p_0 - th$ root. During the opening phase, computation of $M(X_k)$ and $M(Y_k)$ informs the auction managers if a bid was higher than k. For example, if $M(X_k)$ and $M(Y_k)$ return $(1, 0)$ for the point k, no one submitted higher than this point. If $M(X_k)$ and $M(Y_k)$ return $(0, 1)$, at least one of the bidders has placed a bid at that price. The last possible scenario is that $M(X_k)$ and $M(Y_k)$ return $(0, 0)$ meaning that multiple bidders have placed a bid at this value or higher than this value. The problem is that cases $(0, 1)$ and $(1, 0)$ are indistinguishable. Once a winning bid is determined, a winner is found by AM1 and AM2 working together.

The protocol in [43] consists of R number of rounds each being a second-price sealed-bid auction. However, the essence of the protocol is a mechanism created with parameters ϵ and m that create a trade-off and allow for flexibility between important desired properties such as resource-effectiveness, cognitive cost, security and privacy. The bidders must obtain commitment keys, encryption keys, and signature keys. A monotonic bijective function from the possible valuations to the actual valuations is used by the bidders to create their bids at each round, that is, $b^r_i = \phi(B_i(e^r_i))$. Pre-computed values are allowed at each round of the protocol to reduce the round complexity and computational cost. Each bidder submits an encryption of b^r_i and argues that $\phi(\frac{1}{1-\epsilon}\phi^{-1}(b^1_i)) \geqslant b^r_i$ using a zero-knowledge proof. The auction is said to finish once the winning price of the current round and its corresponding bidder are the same from the previous round. If a tie occurs, the ultimate winner is chosen by an equal probability rule.

The authors of [44] constructed two second-price sealed-bid auction protocols using masking techniques and verifiable secret sharing [45]. As stated in the paper, the protocol can also be constructed with the more

complicated VSS of [46]. In the first implementation, the bidders hide their bids by masking it using + operation of two shared secrets. In the second construction, the bidders hide their bids using both the + and x operations of two shared secrets. These protocols provide unconditional security in both passive and active adversarial models.

Table 2. Summary of the Second-Price Sealed-Bid/Vickrey Auction Protocols.

Reference	Cryptographic Method	Adversary Model	Security Model
[35]	Uses public key encryption, compares two bidder at a time	Passive	Computational
[20]	First to bring Verifiable Signature Sharing	Passive	Computational
[37]	MPC is used to share Public/Private keys	Active	Computational
[38]	Homomorphic Encryption	Active	Computational
[40]	Uses public key cryptography, and three possible ways of searching: downward, upward, and binary	Passive	Computational
[41]	Differential Bid Vector. Shifting down of vector along with user input retrieves the highest price.	Active	Computational
[44]	Verifiable Secret Sharing and masking using + and x operations	Active	Computational
[42]	Zero knowledge proof signatures, and ElGamal cryptosystem.	Active	Computational

3.3. (M+1)-Price Sealed-Bid Auctions

The $(M + 1)$-price auction is a form of auction in which the M highest bidders win and the $(M + 1)$-st valuation defines the selling price. As stated earlier, when $M = 1$, the protocol resembles a Vickrey auction in which the second highest price is paid. Papers such as [47, 48, 49, 50, 51] contain details on how to construct the $(M + 1)$-price sealed bid auction protocols.

[47] used a secure multiparty computation scheme for its construction. Instead of hiding each bid in the sum and product of the free variables, the protocol hides each bid in the degree of a polynomial. The main idea is to compute the summation of polynomials in a way that the resulting polynomial returns the number of bidders willing to pay at a specific price. The auctioneers determine the winner by polling until the highest price is found. After identifying a winner, he must prove to be a true recipient of the prize. In order to realize the $(M + 1)$-price sealed-bid auction, the auctioneers remove the winners from the set and reiterate the process to find the next set of winners.

The approach presented in [48] consists of the bidders, auctioneers, and a trusted third party. The trusted party generates the public-key and private-key in preparation for ElGammal public-key encryption. The bidders use their available keys to generate a publicly encrypted bid vector. They also compute the differential of the bid vector. The auctioneers take the integral to recover the information along with a mix-and-match procedure to test if a bid is lower or higher than a predetermined value. The search for the winner is performed via a homomorphic binary search.

Felix Brandt proposed two fully private protocols for the $(M + 1)$-price sealed bid auction, i.e., no auctioneers or TTP are used to solve the auction. citebrandt2002verifiable improves some of the issues in [41] related to leaking information when bids are equal or the lack of verifiability. Similar to other protocols

stated earlier, there is an ordered set of k possible prices $p_1, p_2, \cdots, p_k$. Each bidder sets a differential bid vector and distributes it to other bidders. Finding the highest price requires shifting down the components of the bid vector. Each bidder b_i contributes a final computation, which is multiplication on the shares. If the multiplication changes value 0 to 1, that bidder b_i producing 1 is the winner. Public verification is achieved inherently as a result of using VSS in the protocol. Another protocol was proposed by the same authors in [50] using ElGammal encryption scheme. The bidders jointly compute the results of the auction protocol in constant rounds, usually 3, regardless of the number of bidders and combination of binds.

The focus in [51] shifted from the price being the unique strategy dimension to the quality offered by an item or the attributes of a deal. In this context, the auctioneers are buyers and the bidders are sellers, that is, there is a single buyer (government) and a set of sellers $N = \{1, 2, ...n\}$. Each item has a cost and associated quality $c(\theta, q)$. The gross quality of a buyer is $V(q)$ and the payment to the i^{th} seller is p_i. Therefore the utility of a seller is $p_i - c(\theta, q)$ and that of the buyer is $V(q) - p_i$. In the first step, the bidders send (q_i, b_i) in an encrypted format applying homomorphic encryption. A second prize winner is found using the same technique as of [48]. After the second prize winner is found, a decryption of quality $D(E(q_i))$ and calculation of $V(q_i) - b_{2nd}$ define the final payment.

Table 3. Summary of the (M+1)-Price Sealed-Bid Auction Protocols.

Reference	Cryptographic Method	Adversary Model	Security Model
[47]	MPC. Bid value is in the degree of polynomial	Active	Unconditional
[48]	A TTP generates key pairs that are used in a mix and match approach	Passive	Computational
[49]	Bidders create a differential bid vector. Bidders share with other bidders. A bidder computed number determines the winner..	Active	Unconditional
[50]	A sealed bid auction built around ElGamal	Active	Computational
[51]	Auctioneers are buyers, and bidders are sellers. Bid are encrypted using homomorphic encryption	Passive	Computational

3.4. Rule-Flexible Sealed-Bid Auctions

Previously, it was established that an auction in which the winner pays his own price is regarded as the first-price auction while paying the second-highest bid is referred to as the second-price auction. Some of the protocols mentioned above have been designed for a specific setting, namely, first or second price auctions. The next protocols are simply concerned with providing a method for sealed-biding in the more general sense with a flexibility to the rules of the game. The next reviewed works are [52, 53, 54, 55, 56, 57].

In one of the first papers on the topic [53], a protocol designed to utilize the idea of distributed computation based on [14]. More generally, the authors describe a protocol that could resolve ties and would never reveal bids to any party even after the auction is completed. This protocol distributes information among the auctioneers by means of polynomials providing t-privacy and t-resilience. From the two operations, multiplication and addition, the most significant operation used throughout the protocol is the addition of polynomials. During the bid submission phase, the bidders encode their bid that is a value from a price list. Each of the digits of the bid is encoded by a secret sharing polynomial. The bidders proceed to distribute their shares among the auctioneers. Later, the auctioneers perform multi-round computation (one for each digit) on the encoded information to find the largest or second largest bid. As a final stage, the bidders' bids

are summed by the auctioneers working together to find the ID of the winner. If a tie occurs, no one will be able to claim the winning ID. In the situation of a tie, a second round with a new price list takes place for the participants that tied. The process continues repeatedly until the protocol can distinguish a single winner. Moreover, the protocol can be improved by [21] providing an improvement on privacy at double the cost of computation. Lastly, the proposed protocol can be improved as suggested by [22] to provide fairness, anonymity, and robustness.

In the category of auction design with public-key cryptosystem, the authors of [52] designed a multi-step protocol. The protocol relies on private and public key encryption schemes as well as a broadcast channel. The protocol had several deficiencies on efficiency and data manipulation by malware or malicious users. In order to improve the protocol, [58] introduced the notion of time-stamp into the protocol. However, while the time-stamp provides an extra challenge for a malicious user, it did not completely prevent data from falsification. By introducing a one-time registration stage, [59] improved the protocol. One of the drawbacks left unresolved in this construction was a third party conspiracy with a bidder, which was remedy by [60].

The authors of [54] innovated a protocol that uses mix networks as a main tool. The set of players generate one-way collision resistant hash functions on some inputs $c_i = H(b_i v_i)$. Applying either decryption chaining [61] or re-encryption [62], all c_i are shuffled, and later in another round, (b_i,v_i) are shuffled in the mix network. Proceeding shuffling, the permutations and commitments are posted on a bulletin board by a set of servers. During the opening phase, decryption among all bids occurs. In order to determine a winner, a bidder must prove his commitment matches that of the winning bid.

The authors of [55] created a homomorphic protocol using boolean AND and OR gates. In the initial step of the protocol, the participating parties must publish their public-keys. Each of the participants encrypts the price of choice under all other public-keys including his own. A boolean circuit is introduced in the protocol as a part of function that determines the highest or second highest bidder. If the protocol requires protection against malicious adversary, a similar protocol is deployed but using Paillier's encryption scheme.

Normally, MPC with verifiable secret sharing for robustness requires the bidders to submit ciphertexts and zero-knowledge proofs, which results in a larger overhead. However, one approach to improve MPC and avoid VSS altogether is to create a private decryption key that is shared among the servers. This idea is describe in [63, 64]. Both forms of efficient MPC, that is mix-and-match method and additive homomorphic cryptosystem, are extended in the work of [56] to create an efficient sealed-bid auction protocol where a bidder submits only one ciphertext and experiences only a few multi-exponentiations.

In a homomorphic scheme, the authors of [57] constructed a protocol based on a modified version of Goldwasser-Micali encryption scheme[65]. In the set-up phase, a broadcast communication channel is used by m auctioneers $A_1, A_2, \cdots, A_m$ to provide a different GM encryption scheme and public key. The bidders have to select from a discrete set of prices and represent their valuations as a bid vector with "-1" indicating participation at a specific price and "1" indicating opting out. The auctioneers perform a binary search to find the winning price. During the binary search, if a decryption returns positive, the search head upwards; otherwise, it takes a downward direction. Once a winner is found, in order to publicly verify and proof correctness, a zero-knowledge proof is implemented. For ciphertext returning "-1", a proof of knowledge of square root of ciphertext suffices. The zero-knowledge proof is based on the earlier work of [66].

In a special kind of work focused on multi-attribute auctions (auction not only concern on price, but other quantitative and qualitative properties), [67] proposed an auction to determine the winner or the bidder with the highest score using the Paillier encryption scheme in a homomorphic setting. Finally, in a recent work, an auction focused on mobile users [68] proposed a scheme that protects the confidentiality of the bids only during the bidding phase. The protocol relies on cryptographic primitives such as public-key encryption and hash functions. It is conducted using the technique of crowd-sensing. The winner is determined by not only the price but the kind of data that it provides to the crowd-sensing system.

3.5. Combinatorial Sealed-Bid Auctions

In contrast to the above mentioned auctions, combinatorial auctions allow the bidders to bid on any number of combination of items, called bundle or set. Combinatorial auctions can be multi-unit (multiple units of the same item), linear-good, and general auction (a set of different items). Linear-good auctions

Table 4. Summary of the Rule-Flexible Sealed-Bid Auction Protocols.

Reference	Cryptographic Method	Adversary Model	Security Model
[52]	Encode each digit of bid by a polynomial. MPC over every digit produces the winner.	Passive	Computational
[53]	Uses public key encryption as well as a broadcast channel	Passive	Unconditional
[25]	An auction with mix networks	Passive	Computational
[55]	Homomorphic encryption is to encrypt bids. Boolean circuit determines highest bidder.	Passive	Computational
[57]	Create a private decryption key that is shared among servers, to avoid VSS. Uses homomorphic encryption to avoid communication complexity of MPC.	Passive	Computational
[56]	An auction based on Goldwasser-Micali Encryption	Passive	Computational

consist of a set of sequentially ordered goods, and the bidders tend to bid such that they obtain a sequence of goods [69]. Cases where combinatorial auctions are in use include the sale of furnitures, spectrum auctions held by the Federal Communication Commission [70], and the sale of airport time slots.

An inherent challenge of combinatorial auctions, referred to as combinatorial auction problem or winner determination problem, is the computation of an optimal solution, i.e., the set of disjoint goods such that the sum of the goods is maximized. Papers such as [71, 72, 73, 74] have provided possible solutions to the winner determination problem. Most of the time, for sealed-bid auctions, the solution is solved with a dynamic programming approach since it is a strong tool for solving the longest or shortest path problem on a directed graph. In general, the idea behind combinatorial auctions is to make a profit from selling desirable complementary items, while finding the winning party is a matter of solving a hard combinatorial optimization problem, usually implemented with a dynamic algorithm. An in depth coverage of combinatorial auctions is presented in [75]. Sealed-bid protocols for combinatorial auctions are presented in [76, 77, 78].

Taking an approach of dynamic programming and using Shamir's secret sharing in a similar manner as of [47], the authors of [76] constructed a sealed-bid combinatorial auction protocol for the general case and effective against the passive adversary model. The method consists of using secret sharing to share bids among the publisher and evaluators. The evaluators come together to solve the optimal value using secure dynamic programming. In a final step, the evaluators trace back the links to obtain the optimal solution or the longest path. Due to its nature, this type of construction generates a protocol with unconditional security.

The next protocol [77] utilized homomorphic public-key encryption of ElGammal to realize secure dynamic programming. The bidders are represented by weight publishers. Part of the auction servers are represented by the evaluators. Each evaluator only knows his own valuation. At the start of the protocol, the weights are encrypted with public-key encryption. Because ElGammal provides indistinguishable, homomorphic and randomizable scheme, the wights are each encrypted with different random value r and a random constant f is added. During the winner determination phase, the optimal value is found by decrypting the $j-th$ element from the component-wise product and checking if the value is equal to "1." When the value is not equal to "1," it can be concluded that a maximum has been found.

As mentioned, the research work in [78] provided another solution to combinatorial auctions. The approach taken by the authors is to use Paillers'e encryption as a cryptographic primitive. At the start of the

auction, the auctioneer provides a public time-lapse cryptographic key N [79]. The auctioneer proceeds to publish the price vector followed by the bidders encrypting and submitting their bids. During the winner determination phase, a branch-and-bound algorithm is used to solve the optimization problem in the plaintext of bids. The plaintext is used for reducing the time complexity, however, even though the bids are revealed, the auctioneer cannot modify or change the outcome of the auction.

Finally, [44] constructed two protocols for combinatorial selaed-bid auctions. These protocols use a trusted initializer, the + operation of MPC and *max* function in order to execute the protocol. Furthermore, the auction model is represented as a case of multiple traveling salesman problem and is solved using dynamic programming techniques in one implementation and the inter-agent negotiation in the second implementation.

Table 5. Summary of the Cobinatorial Sealed-Bid Auction Protocols.

Reference	Cryptographic Method	Adversary Model	Security Model
[76]	Combines secret sharing and dynamic programming.	Passive	Unconditional
[77]	Homomorphic encryption based on ElGamal to realize a secure dynamic programming solution	Passive	Computational
[78]	Uses Paillers's encryptions, and time-lapse cryptographic key. A branch and bound algorithm is used for optimization.	Passive	Computational

4. Technical Discussion

Most of the protocols are computationally secure and treat the adversary as passive. In some cases, the protocols are not efficient enough for deployment in real-world scenarios or there exist technical flaws.

To begin with, [17] proposed a sealed-bid auction protocol that iterates through rounds of computation on an undeniable signature scheme. This protocol is expensive in terms of computation because of the number and size of the exponentiation. The protocol is also expensive in terms of communication rounds since it must go through many iterations of elimination before determining the winner. [15] has a deficiency around ties. The only way to resolve a tie is to have additional rounds. One problem is that, the protocol cannot determine the exact number of ties and where these ties coming from. [18] created a protocol with each bid having a pair of encryption and decryption keys. The bidders have access to all the encryption keys and can choose an encrypting key depending on the bid value. The main problem with this protocol is that, the auctioneers are assumed to be honest. Another protocol [19] used hash chaining to improve efficiency, however, it also fails to maintain bid privacy entirely since the scheme cannot keep any bids secret from the center. The proposed scheme based on group signature [26] can leak bid information if the group manager breaks the anonymity. [80] attempted to decouple the group managers by having two managers, namely a registration manager and an auction manager. One issue with this construction is the winner determination since the identity of the winner could not be published at the end. Later, the winner determination problem of this protocol was resolved by [81] making use of a bulletin board and by [82] making use of hash functions.

In [49], the auctioneers can frame the bidders as they are responsible for bidders ID and for the process of signing a received bid. At the time of bidding, anyone can insert a fake bid, especially using a pseudonym, as there is no protocol for authentication. The protocol is susceptible to malicious activity of a player who can insert a random bid value not present on the list of possible values that bidders are expected to choose. As a result, the protocol may never define a winner. In [16], values of the bids are not protected from the

auctioneers since it is required to perform decryption over all bids for winner determination. In addition, there is no mechanism to prevent the auctioneers from colluding with another party. Furthermore, it is stated explicitly that the protocol has a problems when the players supply no or false keys, called the key denial problem. In some auction protocols, for example [47, 22, 21, 15] efficiency is improved by using homomorphic bid opening during the winner determination phase. An attack producing invalid bids can have detrimental impacts as shown in [83]. Specifically, an attack of invalid bids can affect quality of correctness and fairness. A possible solution is to impose a verification mechanism, which then affects the efficiency provided by the homomorphic techniques. In general, a trade-off exists between the level of privacy that a protocol can provide and its efficiency.

5. Concluding Remarks

In this article, we thoroughly reviewed different types of sealed-bid auction protocols and illustrated challenges that exist when designing a privacy-preserving auction protocol. As stated earlier, sealed-bid auctions are mechanisms that treat the losing bids as private information that must be protected. Ideally, in a sealed-bid auction protocol, the only information to be revealed should be the winner and the selling price. Although, many cryptographic constructions focus on (M+1)-price and combinatorial sealed-bid auctions, in general, first-price and second-price (Vickrey) sealed-bid auctions are more common. Thus, a vast majority of the literature is dedicated towards these types of auctions. One paper in particular [84] leads us to believe that there is no unconditional full-privacy in the first-price and second-price sealed-bid auctions if we consider the protocols that do not rely on any trusted third party.

One major problem with all forms of sealed-bid auctions is the possibility of collusion. Under one scenario, the bidders can coordinate to insert artificial bids such that a member pertaining to the group can obtain the reward at a favorable price. Another possibility is the collusion of bidder(s) and auctioneer(s) that can arise in many forms, e.g., in the form of bribery. Furthermore, auctioneer(s) can collude to gain a higher revenue for themselves and for the sellers of the good. Even with cryptographic protocols, most of the aforementioned papers suffer from a trust in auctioneer(s), or a trust in the bidders. Improvements on existing protocols require adding additional time complexity and round complexity to ensure the privacy of the losing bids are preserved.

To conclude, the expansion of computers and the Internet means that e-commerce is an unavoidable piece of our society. In order to face the issues related to fair trading, and allowing an auction mechanism to establish a fair price for goods, we must construct concrete privacy-preserving protocols. While the literature is rich in terms of novel ideas, there is still room for improvements in the area of computational efficiency [85, 86], privacy under the active adversary model, and unconditional security.

6. Acknowledgment

We would like to thank the anonymous reviewers for their constructive feedback and inspiring comments. The reviewers invaluable comments significantly improved this survey paper.

References

[1] F. Brandt, G. Weiß, Antisocial agents and vickrey auctions, in: International Workshop on Agent Theories, Architectures, and Languages, Springer, 2001, pp. 335–347.
[2] F. Brandt, G. Wei, Vicious strategies for vickrey auctions, in: Proceedings of the fifth international conference on Autonomous agents, ACM, 2001, pp. 71–72.
[3] T. W. Sandholm, Limitations of the vickrey auction in computational multiagent systems, in: Proceedings of the Second International Conference on Multiagent Systems (ICMAS-96), 1996, pp. 299–306.
[4] F. Brandt, T. Sandholm, Y. Shoham, Spiteful bidding in sealed-bid auctions., in: IJCAI, Vol. 7, 2007, pp. 1207–1214.
[5] K. Peng, C. Boyd, E. Dawson, K. Viswanathan, Five sealed-bid auction models, in: Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003-Volume 21, Australian Computer Society, Inc., 2003, pp. 77–86.
[6] J. Dreier, P. Lafourcade, Y. Lakhnech, Formal verification of e-auction protocols, in: International Conference on Principles of Security and Trust, Springer, 2013, pp. 247–266.
[7] E. Maskin, J. Riley, Asymmetric auctions, The Review of Economic Studies 67 (3) (2000) 413–438.

[8] S. Athey, J. Levin, E. Seira, Comparing open and sealed bid auctions: Evidence from timber auctions, The Quarterly Journal of Economics 126 (1) (2011) 207–257.
[9] R. L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM 21 (2) (1978) 120–126.
[10] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, In Advances in Cryptology - CRYPTO' 84, vol. 196 of LNCS, pp. 10-18. Springer-Verlag.
[11] D. R. Stinson, Cryptography: theory and practice, CRC press, 2005.
[12] W. Diffie, M. Hellman, New directions in cryptography, IEEE transactions on Information Theory 22 (6) (1976) 644–654.
[13] A. Shamir, How to share a secret, Communications of the ACM 22 (11) (1979) 612–613.
[14] M. Ben-Or, S. Goldwasser, A. Wigderson, Completeness theorems for non-cryptographic fault-tolerant distributed computation, in: Proceedings of the twentieth annual ACM symposium on Theory of computing, ACM, 1988, pp. 1–10.
[15] H. Kikuchi, M. Hakavy, D. Tygar, Multi-round anonymous auction protocols, IEICE Transactions on Information and Systems 82 (4) (1999) 769–777.
[16] C. Cachin, Efficient private bidding and auctions with an oblivious third party, in: Proceedings of the 6th ACM conference on Computer and communications security, ACM, 1999, pp. 120–127.
[17] K. Sakurai, S. Miyazaki, A bulletin-board based digital auction scheme with bidding down strategy-towards anonymous electronic bidding without anonymous channels nor trusted centers, in: Proc. International Workshop on Cryptographic Techniques and E-Commerce, 1999, pp. 180–187.
[18] K. Sako, An auction protocol which hides bids of losers, in: International Workshop on Public Key Cryptography, Springer, 2000, pp. 422–432.
[19] K. Suzuki, K. Kobayashi, H. Morita, Efficient sealed-bid auction using hash chain, in: International Conference on Information Security and Cryptology, Springer, 2000, pp. 183–191.
[20] M. K. Franklin, M. K. Reiter, The design and implementation of a secure auction service, IEEE Transactions on Software Engineering 22 (5) (1996) 302–312.
[21] H. Kikuchi, S. Hotta, K. Abe, S. Nakanishi, Distributed auction servers resolving winner and winning bid without revealing privacy of bids, in: Parallel and Distributed Systems: Workshops, Seventh International Conference on, 2000, IEEE, 2000, pp. 307–312.
[22] K. Peng, C. Boyd, E. Dawson, K. Viswanathan, Robust, privacy protecting and publicly verifiable sealed-bid auction, in: International Conference on Information and Communications Security, Springer, 2002, pp. 147–159.
[23] C.-C. Chang, Y.-F. Chang, Efficient anonymous auction protocols with freewheeling bids, Computers & Security 22 (8) (2003) 728–734.
[24] Y. Watanabe, H. Imai, Reducing the round complexity of a sealed-bid auction protocol with an off-line ttp, in: Proceedings of the 7th ACM conference on Computer and communications security, ACM, 2000, pp. 80–86.
[25] K. Peng, C. Boyd, E. Dawson, K. Viswanathan, Non-interactive auction scheme with strong privacy, in: International Conference on Information Security and Cryptology, Springer, 2002, pp. 407–420.
[26] K. Q. Nguyen, J. Traoré, An online public auction protocol protecting bidder privacy, in: Australasian Conference on Information Security and Privacy, Springer, 2000, pp. 427–442.
[27] K. Peng, C. Boyd, E. Dawson, Optimization of electronic first-bid sealed-bid auction based on homomorphic secret sharing, in: International Conference on Cryptology in Malaysia, Springer, 2005, pp. 84–98.
[28] T. P. Pedersen, Distributed provers with applications to undeniable signatures, in: Workshop on the Theory and Application of of Cryptographic Techniques, Springer, 1991, pp. 221–242.
[29] P. Paillier, Public-key cryptosystems based on composite degree residuosity classes, in: International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 1999, pp. 223–238.
[30] S. Zheng, L. McAven, Y. Mu, First price sealed bid auction without auctioneers, in: Proceedings of the 2007 international conference on Wireless communications and mobile computing, ACM, 2007, pp. 127–131.
[31] K. Peng, E. Dawson, Efficient bid validity check in elgamal-based sealed-bid e-auction, in: International Conference on Information Security Practice and Experience, Springer, 2007, pp. 209–224.
[32] M.-J. Li, J. S.-T. Juan, J. H.-C. Tsai, Practical electronic auction scheme with strong anonymity and bidding privacy, Information Sciences 181 (12) (2011) 2576–2586.
[33] M. Nojoumian, D. R. Stinson, Unconditionally secure first-price auction protocols using a multicomponent commitment scheme, in: 12th International Conference on Information and Communications Security (ICICS), Vol. 6476 of LNCS, Springer, 2010, pp. 266–280.
[34] M. Nojoumian, Novel secret sharing and commitment schemes for cryptographic applications, Ph.D. thesis, Department of Computer Science, University of Waterloo, Canada (2012).
[35] H. Nurmi, A. Salomaa, Cryptographic protocols for vickrey auctions, Group Decision and Negotiation 2 (4) (1993) 363–373.
[36] M. K. Franklin, M. K. Reiter, Verifiable signature sharing, in: International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 1995, pp. 50–63.
[37] M. Naor, B. Pinkas, R. Sumner, Privacy preserving auctions and mechanism design, in: Proceedings of the 1st ACM conference on Electronic commerce, ACM, 1999, pp. 129–139.
[38] H. Lipmaa, N. Asokan, V. Niemi, Secure vickrey auctions without threshold trust, in: International Conference on Financial Cryptography, Springer, 2002, pp. 87–101.
[39] A. Juels, M. Szydlo, A two-server, sealed-bid auction protocol, in: International Conference on Financial Cryptography, Springer, 2002, pp. 72–86.
[40] F. Brandt, Cryptographic protocols for secure second-price auctions, in: International Workshop on Cooperative Information Agents, Springer, 2001, pp. 154–165.

[41] F. Brandt, Secure and private auctions without auctioneers, Technical Report FKI-245–02. Institut fur Informatick, Technishce Universitat Munchen.
[42] K. Omote, A. Miyaji, A second-price sealed-bid auction with verifiable discriminant of p 0-th root, in: International Conference on Financial Cryptography, Springer, 2002, pp. 57–71.
[43] E. Elkind, H. Lipmaa, Interleaving cryptography and mechanism design, in: International Conference on Financial Cryptography, Springer, 2004, pp. 117–131.
[44] M. Nojoumian, D. R. Stinson, Efficient sealed-bid auction protocols using verifiable secret sharing, in: 10th International Conference on Information Security Practice and Experience (ISPEC), Vol. 8434 of LNCS, Springer, 2014, pp. 302–317.
[45] D. R. Stinson, R. Wei, Unconditionally secure proactive secret sharing scheme with combinatorial structures, in: International Workshop on Selected Areas in Cryptography, Springer, 1999, pp. 200–214.
[46] T. Rabin, M. Ben-Or, Verifiable secret sharing and multiparty protocols with honest majority, in: Proceedings of the twenty-first annual ACM symposium on Theory of computing, ACM, 1989, pp. 73–85.
[47] H. Kikuchi, (m+ 1) st-price auction protocol, IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences 85 (3) (2002) 676–683.
[48] M. Abe, K. Suzuki, M+ 1-st price auction using homomorphic encryption, in: International Workshop on Public Key Cryptography, Springer, 2002, pp. 115–124.
[49] F. Brandt, A verifiable, bidder-resolved auction protocol, in: Proceedings of the 5th International Workshop on Deception, Fraud and Trust in Agent Societies (Special Track on Privacy and Protection with Multi-Agent Systems), Citeseer, 2002, pp. 18–25.
[50] F. Brandt, Fully private auctions in a constant number of rounds, in: International Conference on Financial Cryptography, Springer, 2003, pp. 223–238.
[51] K. Suzuki, M. Yokoo, Secure multi-attribute procurement auction, in: International Workshop on Information Security Applications, Springer, 2005, pp. 306–317.
[52] S. Subramanian, Design and verification of a secure electronic auction protocol, in: Reliable Distributed Systems, 1998. Proceedings. Seventeenth IEEE Symposium on, IEEE, 1998, pp. 204–210.
[53] M. Harkavy, J. D. Tygar, H. Kikuchi, Electronic auctions with private bids., in: USENIX Workshop on Electronic Commerce, 1998.
[54] K. Peng, C. Boyd, E. Dawson, K. Viswanathan, Efficient implementation of relative bid privacy in sealed-bid auction, in: International Workshop on Information Security Applications, Springer, 2003, pp. 244–256.
[55] B. Olivier, S. Jacques, Non-interactive private auctions, Lecture Notes in Computer Science 2339 (2002) 0354–0354.
[56] T. Nakanishi, D. Yamamoto, Y. Sugiyama, Sealed-bid auctions with efficient bids, in: International Conference on Information Security and Cryptology, Springer, 2003, pp. 230–244.
[57] K. Peng, C. Boyd, E. Dawson, A multiplicative homomorphic sealed-bid auction based on goldwasser-micali encryption, in: International Conference on Information Security, Springer, 2005, pp. 374–388.
[58] M.-S. Hwang, E. J.-L. Lu, I.-C. Lin, Adding timestamps to the secure electronic auction protocol, Data & Knowledge Engineering 40 (2) (2002) 155–162.
[59] H.-T. Liaw, W.-S. Juang, C.-K. Lin, An electronic online bidding auction protocol with both security and efficiency, Applied mathematics and computation 174 (2) (2006) 1487–1497.
[60] C.-C. Wu, C.-C. Chang, I.-C. Lin, New sealed-bid electronic auction with fairness, security and efficiency, Journal of Computer Science and Technology 23 (2) (2008) 253–264.
[61] D. L. Chaum, Untraceable electronic mail, return addresses, and digital pseudonyms, Communications of the ACM 24 (2) (1981) 84–90.
[62] C. Park, K. Itoh, K. Kurosawa, Efficient anonymous channel and all/nothing election scheme, in: Workshop on the Theory and Application of of Cryptographic Techniques, Springer, 1993, pp. 248–259.
[63] R. Cramer, I. Damgård, J. B. Nielsen, Multiparty computation from threshold homomorphic encryption, in: International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2001, pp. 280–300.
[64] M. Jakobsson, A. Juels, Mix and match: Secure function evaluation via ciphertexts, in: International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2000, pp. 162–177.
[65] S. Goldwasser, S. Micali, Probabilistic encryption, Journal of computer and system sciences 28 (2) (1984) 270–299.
[66] L. C. Guillou, J.-J. Quisquater, A paradoxical identity-based signature scheme resulting from zero-knowledge, in: Proceedings on Advances in cryptology, Springer-Verlag New York, Inc., 1990, pp. 216–231.
[67] W. Shi, A sealed-bid multi-attribute auction protocol with strong bid privacy and bidder privacy, Security and Communication Networks 6 (10) (2013) 1281–1289.
[68] T. Dimitriou, I. Krontiris, Privacy-respecting auctions and rewarding mechanisms in mobile crowd-sensing applications, Journal of Network and Computer Applications 100 (2017) 24–34.
[69] M. Tennenholtz, Some tractable combinatorial auctions, in: AAAI/IAAI, 2000, pp. 98–103.
[70] J. McMillan, Selling spectrum rights, The Journal of Economic Perspectives 8 (3) (1994) 145–162.
[71] Y. Fujishima, K. Leyton-Brown, Y. Shoham, Taming the computational complexity of combinatorial auctions: Optimal and approximate approaches, in: IJCAI, Vol. 99, DTIC Document, 1999, pp. 548–553.
[72] M. H. Rothkopf, A. Pekeč, R. M. Harstad, Computationally manageable combinational auctions, Management science 44 (8) (1998) 1131–1147.
[73] Y. Sakurai, M. Yokoo, K. Kamei, An efficient approximate algorithm for winner determination in combinatorial auctions, in: Proceedings of the 2nd ACM conference on Electronic commerce, ACM, 2000, pp. 30–37.
[74] T. Sandholm, Algorithm for optimal winner determination in combinatorial auctions, Artificial intelligence 135 (1-2) (2002) 1–54.
[75] S. De Vries, R. V. Vohra, Combinatorial auctions: A survey, INFORMS Journal on computing 15 (3) (2003) 284–309.

[76] K. Suzuki, M. Yokoo, Secure combinatorial auctions by dynamic programming with polynomial secret sharing, in: International Conference on Financial Cryptography, Springer, 2002, pp. 44–56.
[77] M. Yokoo, K. Suzuki, Secure multi-agent dynamic programming based on homomorphic encryption and its application to combinatorial auctions, in: Proceedings of the first international joint conference on Autonomous agents and multiagent systems: part 1, ACM, 2002, pp. 112–119.
[78] D. C. Parkes, M. O. Rabin, C. Thorpe, Cryptographic combinatorial clock-proxy auctions, in: International Conference on Financial Cryptography and Data Security, Springer, 2009, pp. 305–324.
[79] M. O. Rabin, C. Thorpe, Time-lapse cryptography.
[80] K. Omote, A. Miyaji, An anonymous auction protocol with a single non-trusted center using binary trees, in: International Workshop on Information Security, Springer, 2000, pp. 108–120.
[81] K. Omote, A. Miyaji, A practical english auction with simple revocation, IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences 85 (5) (2002) 1054–1061.
[82] B. Lee, K. Kim, J. Ma, Efficient public auction with one-time registration and public verifiability, in: International Conference on Cryptology in India, Springer, 2001, pp. 162–174.
[83] K. Peng, C. Boyd, E. Dawson, Batch verification of validity of bids in homomorphic e-auction, Computer Communications 29 (15) (2006) 2798–2805.
[84] F. Brandt, T. Sandholm, On the existence of unconditionally privacy-preserving auction protocols, ACM Transactions on Information and System Security (TISSEC) 11 (2) (2008) 6.
[85] S. Krishnamachari, M. Nojoumian, K. Akkaya, Implementation and analysis of dutch-style sealed-bid auctions: Computational vs unconditional security, in: 1st International Conference on Information Systems Security and Privacy (ICISSP), 2015, pp. 106–113.
[86] R. Alvarez, M. Nojoumian, Efficient implementation and computational analysis of sealed-bid auctions, in: Under Review, 2019.