SEAL: Sealed-Bid Auction Without Auctioneers

Samiran Bag, Feng Hao, Siamak F. Shahandashti, and Indranil Ghosh Ray

***Abstract*— We propose the first auctioneer-free sealed-bid auction protocol with a linear computation and communication complexity $O(c)$, c being the bit length of the bid price. Our protocol, called Self-Enforcing Auction Lot (SEAL), operates in a decentralized setting, where bidders jointly compute the maximum bid while preserving the privacy of losing bids. In our protocol, we do not require any secret channels between participants. All operations are publicly verifiable; everyone including third-party observers is able to verify the integrity of the auction outcome. Upon learning the highest bid, the winner comes forward with a proof to prove that she is the real winner. Based on the proof, everyone is able to check if there is only one winner or there is a tie. While our main protocol works with the first-price sealed-bid, it can be easily extended to support the second-price sealed-bid (also known as the Vickrey auction), revealing only the winner and the second highest bid, while keeping the highest bid and all other bids secret. To the best of our knowledge, this work establishes to date the best computation and communication complexity for sealed-bid auction schemes without involving any auctioneer.**

***Index Terms*— E-auction, Vickrey auction, cryptographic protocol, multi-party computation (MPC).**

I. Introduction

Auction is a method of allocating scarce resources based on competition. Goods or services are sold by offering them to bidding, and the winner is the bidder who has the highest bid. From the allocation of bandwidth spectrum to the sales of antiques, painting and rare collectibles, auction has become a prevailing practice in our society. It is also commonly used by governments, e.g., long-term securities are sold in weekly auctions conducted by the U.S. Treasury to finance the borrowing needs of the government [1].

In general, there are two types of auctions: open cry and sealed bid. In an open-cry auction, the price may be ascending from a reserve price until there is only one bidder left, or descending from a high price until the first bidder comes forward willing to pay at that price. The former is often known as “English auction” while the later “Dutch auction”. In a sealed-bid auction, each bidder hands over a sealed envelope containing their secret bid to an auctioneer. The auctioneer opens all envelopes and declares the highest bidder as the winner, while keeping losing bids secret. In the first-price sealed-bid, the winner pays for the highest bid, but in the second-price sealed-bid, the winner only needs to pay the second highest bid. The second-price sealed-bid is also called the Vickrey auction (named after William Vickrey).

There has been extensive research in auction theory to show the inherent relations between various auction schemes [1]. In particular, the Dutch auction is shown to be strategically equivalent to the first-price sealed-bid auction based on game theory. The English auction is equivalent to the Vickrey auction under the assumption that bidders evaluate the value of the item in private. The Vickrey auction is extremely important in auction theory, as it is *strategy-proof*. In other words, when the evaluated values are all private, the best strategy for bidders is to bid their true evaluation. William Vickrey first developed the theory for this auction scheme and received a Nobel prize in 1996. The scheme is thereafter named after him in recognition of his ground-breaking contributions.

Unfortunately, the Vickrey auction is rarely used in practice [2]. This is largely due to two reasons, both of which are related to the distrust on the auctioneer. First, a dishonest auctioneer might surreptitiously substitute the second highest price to one slightly below the top price to increase the revenue. Second, a dishonest auctioneer might disclose the losing bids to other parties, since the true evaluation of the auction item is considered a commercial secret.

Since the early work in this field by Franklin and Reiter in 1996 [3], many sealed-bid e-auction schemes have been proposed [2], [4]–[10]. However, the past schemes generally assume the role of an auctioneer (as in traditional sealed-bid auctions). To mitigate the trust problem about the auctioneer, researchers propose to apply threshold cryptography or multi-party computation (MPC) techniques [10], [11] to distribute the trust from a single auctioneer to two or several. However, one can never rule out the possibility that the auctioneers may collude all together to compromise the privacy of the bids [7].

In this article, we propose to address the trust issue about the auctioneer by removing the need for any auctioneer completely from an auction system. We consider a totally decentralized setting with public verifiability. In this setting, the auction is run by the bidders themselves without involving any auctioneer, and all operations are publicly verifiable without any secret channels. Clearly, generic MPC techniques [12] that require pairwise secret channels are unsuitable for our purpose. Our setting is similar to the “bidder-resolved auction” proposed by Brandt [2], [7], [13], and Brandt and Sandholm [14]), but Brandt’s schemes also involve a seller, who actively takes part

Manuscript received March 18, 2019; revised July 4, 2019 and October 10, 2019; accepted November 14, 2019. Date of publication November 25, 2019; date of current version January 30, 2020. This work was supported in part by the European Research Council (ERC) Starting under Grant 306994 and in part by the Royal Society under Grant ICA/R1/180226. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Julien Bringer. *(Corresponding author: Feng Hao.)*

S. Bag, F. Hao, and I. G. Ray are with the Department of Computer Science, University of Warwick, Coventry CV4 7AL, U.K. (e-mail: samiran.bag@warwick.ac.uk; feng.hao@warwick.ac.uk; indranil.ghosh-ray@warwick.ac.uk).

S. F. Shahandashti is with the Department of Computer Science, University of York, York YO10 5GH, U.K. (e-mail: siamak.shahandashti@york.ac.uk).

Digital Object Identifier 10.1109/TIFS.2019.2955793

in the protocol and is trusted not to collude with bidders. Furthermore, Brandt's schemes incur an exponential system complexity $O(2^c)$ for computation and bandwidth usage, c being the bit length of the bid price. No sealed-bid auction scheme in the past has achieved the linear system complexity $O(c)$ in a decentralized setting.

Our contributions in this article are summarized below.

- We propose the first decentralized sealed-bid auction protocol with a linear computation and communication complexity $O(c)$, c being the bit length of the bid price. Our protocol is publicly verifiable without involving any auctioneer or requiring any secret channels between bidders.
- We present security proofs to prove the correctness, and privacy aspects of the protocol, as well as performing analysis on the system complexity.
- We show how our first-prize sealed-bid auction scheme can be extended to support second-prize sealed-bid auctions (Vickrey auction) while maintaining the linear system complexity.

II. Preliminaries

A. Communication Model

Sealed-bid auction can be considered a special instance of a secure multiparty computation (MPC) problem, in which participants jointly compute the highest bid without revealing losing bids. In a typical MPC setting, the communication model assumes that there exist pairwise secret and authenticated channels between participants, in addition to an authenticated public channel [8], [10], [15]. In the real-world example of applying MPC to the Danish sugar beets auction, three appointed auctioneers set up pairs of public and private key, which were used to establish secure point-to-point channels between the auctioneers [9]. The existence of secret channels is not considered a problem in [9], since by design all farmers are required to trust auctioneers – more specifically, trusting that at least 2 out of the 3 auctioneers are honest.

In a decentralized setting without any auctioneer, we consider it desirable to remove any secret channels, so all operations are publicly verifiable. This is especially important for third-party observers (e.g., the seller) who are not involved in the protocol, but still want to verify the integrity of the auction process. Therefore, in our model, we only assume an authenticated public channel available to all participants. Such a channel can be realized using physical means or a public bulletin board, as described in [6], [16], [17].

B. A Modified Anonymous Veto Protocol

A basic building block in our auction protocol is a primitive that securely computes the logical-OR of binary inputs without revealing each individual bit. We choose to modify Hao-Zieliński's Anonymous Veto network (AV-net) protocol [18] for our purpose. This protocol is chosen for its optimal efficiency in terms of the number of rounds, the computation and the communication bandwidth. However, we need to modify the original scheme to make it applicable to our system.

The modified AV-net protocol works as follows. Assume a group of n voters who wish to find out if there is one voter who would like to veto a motion. In other words, they wish to securely compute the logical-OR function of a number of input bits, each bit coming from a separate entity. Let G be a group of p elements in which the Decisional Diffie-Hellman problem is assumed to be intractable. Let g be a random generator of G. All computations in G are modular operations with respect to a prime modulus q, but we omit the $\bmod q$ notation for simplicity. Each voter V_i holds a secret bit $v_i \in \{0, 1\}$, and they compute the logical-OR $\bigvee_{i=1}^{n} v_i$ in two rounds. For any two integers a and b, where $a < b$, we denote by $[a, b]$, the set: $\{a, a+1, \ldots, b\}$.

Round I: Each voter $V_i : i \in [1, n]$ chooses two random elements $(x_i, r_i) \in \mathbb{Z}_p^2$ and computes $X_i = g^{x_i}, R_i = g^{r_i}$. V_i posts (X_i, R_i) on the public bulletin board, together with non-interactive zero-knowledge (NIZK) proofs [19], [20] to prove the knowledge of x_i and r_i, respectively, using Schnorr's signature [18].

Round II: Each voter $V_i : i \in [1, n]$ computes $Y_i = \prod_{j=1}^{i-1} X_j / \prod_{j=i+1}^{n} X_j$. V_i also computes an encrypted ballot b_i and posts it on the bulletin board together with a NIZK proof to show b_i is well-formed.

$$b_i = \begin{cases} Y_i^{x_i} & \text{if } v_i = 0 \\ R_i^{x_i} & \text{if } v_i = 1 \end{cases}$$

The NIZK proof in the second round is to prove the following statement: $(b_i = Y_i^{x_i}) \vee (b_i = R_i^{x_i})$. Note that the first term is equivalent to proving $\{X_i, Y_i, b_i = Y_i^{x_i}\}$ is a DDH tuple and the second term equivalent to proving $\{X_i, R_i, b_i = R_i^{x_i}\}$ is a DDH tuple. Thus, the NIZK proof on the well-formedness of b_i is a disjunctive proof of two sub-statements. More details on the zero-knowledge proofs used in this protocol can be found in [21].

After the second round, everyone can compute $B = \prod_{i=1}^{n} b_i$ after fetching the ballots $b_i : i \in [1, n]$ from the bulletin board. It is easy to see that if every input is 0, $B = 1$; otherwise, if at least one input is 1, $B \neq 1$ with overwhelming probability (i.e., B is a random element in G). Hence, the logical-OR of all input bits has been securely computed by all participants without revealing the value of each individual bit. The key element in this protocol is the fact that $\prod_i Y_i^{x_i} = 1$, i.e., the random factors x_i are all canceled out. For a proof of this fact, the reader is referred to [18].

Our modified veto protocol differs from Hao-Zieliński's AV-net protocol [18] in that we use two random variables, x_i and r_i, while AV-net only uses one. This requires more computation from each participant, but the (asymptotic) computation and communication complexity remains the same as AV-net. In AV-net, the '1' vote (or the 'veto' vote) is encoded by raising a pre-defined generator to the power of a random variable, while in the modified veto protocol, the '1' vote is encoded by raising a random generator to the power of a pre-defined exponent (namely, x_i). This modification allows us to effectively integrate the veto protocol into the e-auction

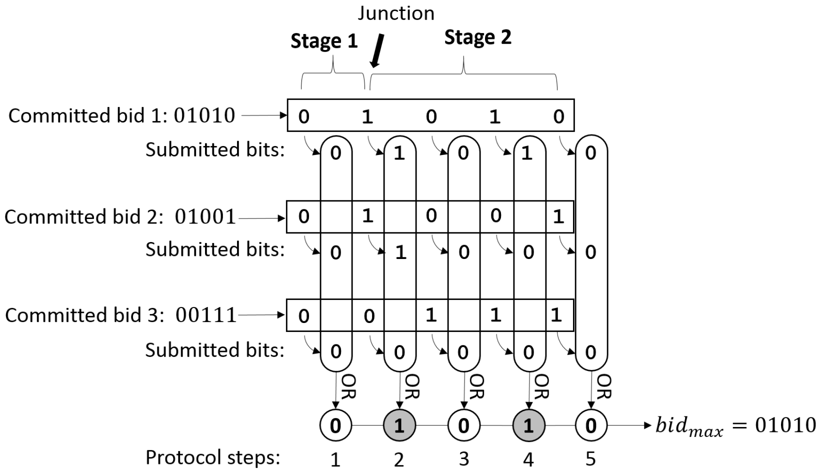


Fig. 1. Example of an execution of our protocol, starting with three bids: 10, 9, and 7, and calculating the maximum bid, i.e., 10, in five steps.

scheme as some zero-knowledge proofs will require proving the equality of the exponents. This should become clear after we explain the details of the a-auction scheme in the next section. In the rest of the article, we will simply refer to the modified anonymous veto protocol as the "veto protocol".

C. Intuition Behind the Scheme

First, we explain the high-level intuition of the protocol. Assume there are n bidders denoted as V_i, $i \in [1, n]$. The binary representation of each bid contains c bits.[1] For any bid price $p_i, i \in [1, n]$, let $p_{i1}||p_{i2}||\ldots||p_{ic}$ be the binary representation of p_i, with $||$ denoting concatenation.

The protocol has two phases. In the first phase, every bidder V_i commits their bid p_i on a public bulletin board. In the second phase, all bidders jointly compute the maximum bid bit-by-bit, starting from the most significant bit.

As an example, we start from the most significant bit position on the left, as shown in Figure 1. We denote this starting position as $j = 1$. We use the modified anonymous veto protocol as a basic building block to compute the logical OR of the input bits without revealing individual bits. Now every bidder V_i uses a bit d_{ij} $(j = 1)$ as the input to this veto protocol, with a NIZK proof to prove that $d_{ij} = p_{ij}$ without revealing the committed bit. All bidders are able to compute the logical OR of all d_{ij} bits for the first bit position $(j = 1)$.

$$T_j = d_{1j} \vee d_{2j} \vee \ldots \vee d_{nj} \tag{1}$$

At each iteration for $j = 1, 2, \ldots$, when the logical OR result T_j is 1, we call this bit position a *deciding* position; otherwise, we call it a *non-deciding* position. We use $\overleftarrow{j}$ to denote the deciding position that immediately precedes the jth bit position ($\overleftarrow{j}$ will always return a valid bit position in the context of our protocol after the first *deciding* position is past).

The first *deciding* position is called a *junction* (see Figure 1). This is where $T_j = 1$ $(j = 1, 2, \ldots)$ for the first time. After this junction, bidders still use the veto protocol to compute the logical OR of the input bits, but the rule for specifying the input bit is different. Instead of using a bit that must be the same as the committed bit, each bidder uses the bit $d_{ij} = p_{ij} \wedge d_{i\overleftarrow{j}}$, where $\overleftarrow{j}$ denotes the previous *deciding* position before j. In addition, each bidder provides a zero-knowledge proof to prove the following statement.

$$\left(d_{ij} = p_{ij} \text{ AND } d_{i\overleftarrow{j}} = 1\right) \text{ OR } \left(d_{ij} = 0 \text{ AND } d_{i\overleftarrow{j}} = 0\right) \tag{2}$$

The zero-knowledge proof statement in Equation 2 is the key to our auction protocol. Essentially, it enforces the following behavior: at each *deciding* bit position, if the bidder V_i's committed bit in the corresponding position is 0, it means V_i has lost, hence in all subsequent bit positions, V_i is enforced to use 0 as the input to the veto protocol. However, the bidders do not need to reveal whether they have already lost or they are still in the race. Losing bidders simply follow through the rest auction procedure so no information about their bids will be revealed. The guarantee of the privacy for the losing bids provides an incentive for losing bidders to follow through the rest of the process. In practice, bidders often pay a deposit and get it refunded after showing that they have honestly followed the auction rules. This gives another incentive for all bidders to complete the whole auction protocol. At the end of the auction, every bidder, as well as any observer, can compute the maximum bid, but without learning losing bids. In the next section, we will explain details of building a secure sealed-bid auction scheme based on this intuition.

III. Our Main Protocol

A. Requirements

Our main protocol is called Self-Enforcing Auction Lot.[2] We design the protocol to fulfill the following requirements.

1) *Public verifiability.* All operations in the auction process are publicly verifiable. No secret channels are required

[1] The bid may fall in a sub-range of $[0, 2^c - 1]$. We do not consider this detail since we are mainly concerned with the system complexity of the protocol.

[2] In the auction terminology, a "lot" is an item or set of items for sale.

between participants. Only an authenticated public channel is available to all participants (which can be realized by using a public bulletin board as in [8], [16], [17]).

2) *Correctness.* The protocol is guaranteed to output the highest bid with proofs that everyone is able to verify.
3) *Losing-bid privacy.* While the protocol outputs the highest bid, the privacy of losing bids should be preserved, as we formally define below.

In the generic definition of input privacy in MPC, each participant is limited to learn nothing more than their own input and the output of the function [12]. Based on this, we define *inclusive-privacy* for sealed-bid auction, in which participants perform a secure computation of a *max* function. We call it "inclusive" as the function includes inputs p_i from all participants, $i \in [1, n]$.

Definition 1 (Inclusive-privacy): In an auction protocol that satisfies *inclusive-privacy*, each bidder V_i learns nothing more than their own input and the output of the function $f_{\max}(p_1, \ldots, p_n)$.

We slightly modify the above definition by excluding the bidder's own input from the inputs of the function and introduce *exclusive-privacy* as defined below. Here we consider a more general case where a set of bidders may collude together. Let C be a set of colluding bidders and H be the rest of the bidders, i.e. $C \cup H = [1, n]$. Let θ be the size of H and $h_i \in H$, $i \in [1, \theta]$. At minimum, C contains only one bidder, but in the general case, it may contain any number of bidders.

Definition 2 (Exclusive-privacy): In an auction protocol that satisfies *exclusive-privacy*, C learns nothing more than their own input and the output of the function $f_{\max}(p_{h_1}, \ldots, p_{h_\theta})$.

The generic definition of privacy (namely, inclusive-privacy) is commonly used in the past MPC literature, whereas we consider the latter definition of privacy, i.e. exclusive-privacy in the publicly verifiable setting. Protocols that use general MPC techniques have been shown to be able to satisfy the strong notion of inclusive-privacy, but this relies on several important assumptions [12]. First of all, the privacy of inputs depends on pairwise secret channels between participants, which however do not exist in our setting. Second, normally the majority of the participants are assumed to be honest. In our case, we consider the vast majority of participants (up to $n - 2$) may be dishonest; in the extreme case, as long as there is at least another honest bidder in H, the bidder's privacy should still be preserved (if all bidders except one are dishonest, the privacy guarantee for the remaining bid would not be meaningful since dishonest bidders can trivially find out the bid by supplying zeros as their own inputs). In such a setting, general MPC protocols cannot assure any privacy of inputs at all.

Therefore, although *exclusive-privacy* is a slightly weaker notion of privacy, our protocol guarantees a much stronger assurance of privacy in practice than general MPC protocols in a setting where no pairwise secret channels exist and a vast majority of participants may be compromised. We should also highlight that even with an ideal MPC protocol (say based on a simulated trusted third party) that provides *inclusive-privacy*, colluding bidders can always find out the maximum of the inputs of the non-colluding set by supplying 0s as their inputs. Hence, the difference between the two notions is subtle. As we will explain in Section III-C, allowing a bidder to find out the maximum of the other bids can prove crucially useful in the context of an auction system, especially in constructing an efficient Vickrey auction scheme and in detecting a tie. In the following section, we will present a decentralized first-price sealed-bid auction protocol that guarantees exclusive-privacy, and in the meanwhile achieves a linear system complexity with respect to the bit length of the bid.

B. Protocol

Let $G = \langle g \rangle$ be the same group mentioned in Section II-B. Our protocol has c iterations, c being the number of bits in the binary representation of bid-prices. The bid price by V_i is expressed in the binary form as: $p_i = p_{i1}||p_{i2}|| \ldots ||p_{ic}$, where $p_{ij} \in \{0, 1\}$, with p_{i1} being the most significant bit and p_{ic} the least significant bit.

a) Commit: In the Commit phase, bidders commit their bids to the public bulletin board. Each bidder V_i computes c commitments, each one for a bit of p_{ij}, for $j \in [1, c]$. In order to do this, V_i selects random $\alpha_{ij}, \beta_{ij} \in_R \mathbb{Z}_p$, $j \in [1, c]$ and computes c individual commitments for c distinct bits of p_{ij} as $\chi_i = \{\varepsilon_{ij} : j \in [1, c]\}$, where:

$$\varepsilon_{ij} = \langle g^{\alpha_{ij}\beta_{ij}} g^{p_{ij}}, g^{\alpha_{ij}}, g^{\beta_{ij}} \rangle, \quad j \in [1, c]$$

If the Decisional Diffie Hellman assumption holds true in G, $(g^{\alpha_{ij}}, g^{\beta_{ij}}, g^{\alpha_{ij}\beta_{ij}}) \overset{c}{\approx} (g^{\alpha_{ij}}, g^{\beta_{ij}}, g^{\alpha_{ij}\beta_{ij}} g)$ [22], where $\overset{c}{\approx}$ denotes computational indistinguishability. Hence, the commitment would not reveal the value of the committed bit p_{ij}, for all $i \in [1, n]$, $j \in [1, c]$. Each bidder V_i posts a NIZK proof of well formedness of each committed bit in the form of ε_{ij}. The NIZK proof shows p_{ij} is either 0 or 1 without revealing which one. The construction of this one-of-two NIZK proof can be found in [23] (also see [21]).

In the second phase, bidders jointly compute the maximum bid without revealing other bids. This proceeds in two stages as indicated in Figure 1.

b) Stage 1: Bidders start from the most significant bit position $j = 1$, and move to the less significant bit positions bit-by-bit until they reach a junction where the logical-OR computation at that bit position is 1 for the first time (see an example of the junction in Figure 1). In the jth bit position, bidders apply the two-round anonymous veto protocol described in Section II-B with private binary inputs d_{ij}, for $i \in [1, n]$, with a zero-knowledge proof to prove that the input bit is the same as the committed one, i.e., $d_{ij} = p_{ij}$.

Round 1: Each bidder $V_i, i \in [1, n]$ selects two private keys $x_{ij}, r_{ij} \in \mathbb{Z}_p$, stores the private keys and publishes the corresponding public keys $Pub_{ij} = (X_{ij}, R_{ij}) = (g^{x_{ij}}, g^{r_{ij}})$ on the bulletin board. The bidder V_i also publishes NIZK proofs of knowledge of $x_{ij} = \log_g X_{ij}$ and $r_{ij} = \log_g R_{ij}$.

Round 2: Each bidder $V_i, i \in [1, n]$ computes a cryptogram

$$b_{ij} = \begin{cases} Y_{ij}^{x_{ij}} = g^{x_{ij} y_{ij}} & \text{if } p_{ij} = 0 \text{ (0-cryptogram);} \\ R_{ij}^{x_{ij}} = g^{x_{ij} r_{ij}} & \text{if } p_{ij} = 1 \text{ (1-cryptogram).} \end{cases}$$

where $Y_{ij} = g^{y_{ij}} = \prod_{k=1}^{i-1} g^{x_{kj}} / \prod_{k=i+1}^{n} g^{x_{kj}} = g^{\sum_{k=1}^{i-1} x_{kj} - \sum_{k=i+1}^{n} x_{kj}}$. V_i also computes a proof π_{ij} of well-formedness of b_{ij}. V_i posts b_{ij} and π_{ij} on the bulletin board.

Here, b_{ij} is an encrypted ciphertext of d_{ij}, and π_{ij} is the NIZK proof that serves to prove $d_{ij} = p_{ij}$ without revealing the committed bit. Effectively, π_{ij} is a proof of the following logical statement.

$$(d_{ij} = 0 \wedge p_{ij} = 0) \vee (d_{ij} = 1 \wedge p_{ij} = 1)$$

The public parameters are $X_{ij} = g^{x_{ij}}, Y_{ij} = g^{y_{ij}}, R_{ij} = g^{r_{ij}}$. Let us assume $\varepsilon_{ij} = \langle c_{ij}, A_{ij}, B_{ij} \rangle$. If $d_{ij} = 0$, (X_{ij}, Y_{ij}, b_{ij}) and (A_{ij}, B_{ij}, c_{ij}) are two DDH tuples. Also if $d_{ij} = 1$, (X_{ij}, R_{ij}, b_{ij}) and $(A_{ij}, B_{ij}, (c_{ij}/g))$ are two DDH tuples as well. So we have to prove a statement that is a logical-OR of a pair logical-AND sub-statements such that each of the two sub-statements is logical-AND of two DDH tuples. Thus, the above statement is equivalent to the following statement (see [24], [25]):

$((b_{ij} = g^{x_{ij} y_{ij}} \wedge X_{ij} = g^{x_{ij}} \wedge Y_{ij} = g^{y_{ij}}) \wedge (c_{ij} = g^{\alpha_{ij} \beta_{ij}} \wedge A_{ij} = g^{\alpha_{ij}} \wedge B_{ij} = g^{\beta_{ij}})) \vee ((b_{ij} = g^{x_{ij} r_{ij}} \wedge X_{ij} = g^{x_{ij}} \wedge R_{ij} = g^{r_{ij}}) \wedge (c_{ij} = g^{\alpha_{ij} \beta_{ij}} g \wedge A_{ij} = g^{\alpha_{ij}} \wedge B_{ij} = g^{\beta_{ij}}))$

After the two rounds, all the bidders verify that the NIZK proofs are correct, and then compute the logical-OR of the input bits d_{ij} for the jth position: $T_j = \bigvee_{i=1}^{n} d_{ij}$. This logical-OR computation is realized by multiplying b_{ij}, $i \in [1, n]$ and comparing the result against 1 (see the veto protocol in Section II-B). If $T_j = 0$, all bidders remain in Stage 1, and move on to compute the logical-OR of the next bit position. However, if $T_j = 1$, this means the junction is reached, and all bidders move to Stage 2.

c) Stage 2: Stage 2 is almost the same as Stage 1, except that d_{ij} is defined differently. Instead of using a bit that must be the same as the committed one, every bidder now uses $d_{ij} = p_{ij} \wedge d_{i\overleftarrow{j}}$ where $d_{i\overleftarrow{j}}$ is the bit that the bidder used in the previous *deciding* bit position. For the completeness, we describe the full details of Stage 2 below. Assume this stage starts from the jth position, and iterates towards the lest significant bit position until $j = c$.

Round 1: Each bidder $V_i, i \in [1, n]$ selects two private keys $x_{ij}, r_{ij} \in \mathbb{Z}_p$, stores the private keys and publishes the corresponding public keys $Pub_{ij} = (X_{ij}, R_{ij}) = (g^{x_{ij}}, g^{r_{ij}})$ on the bulletin board. The bidder V_i also publishes NIZK proofs of knowledge of $x_{ij} = \log_g X_{ij}$ and $r_{ij} = \log_g R_{ij}$. (See [21] for the construction of this NIZK proof).

Round 2: each bidder $V_i, i \in [1, n]$ chooses a bit $d_{ij} = p_{ij} \wedge d_{i\overleftarrow{j}}$ and computes a cryptogram of d_{ij}.

$$b_{ij} = \begin{cases} Y_{ij}^{x_{ij}} = g^{x_{ij} y_{ij}} & \text{if } p_{ij} \wedge d_{i\overleftarrow{j}} = 0; \text{ (0-cryptogram)} \\ R_{ij}^{x_{ij}} = g^{x_{ij} r_{ij}} & \text{if } p_{ij} \wedge d_{i\overleftarrow{j}} = 1. \text{ (1-cryptogram)} \end{cases}$$

where $Y_{ij} = g^{y_{ij}} = \prod_{k=1}^{i-1} g^{x_{kj}} / \prod_{k=i+1}^{n} g^{x_{kj}} = g^{\sum_{k=1}^{i-1} x_{kj} - \sum_{k=i+1}^{n} x_{kj}}$. V_i also computes a proof π_{ij} of well-formedness of b_{ij}. V_i posts b_{ij} and π_{ij} on the bulletin board.

The NIZK proof π_{ij} is a proof of the following logical statement:

$$(d_{ij} = 1 \wedge (p_{ij} \wedge d_{i\overleftarrow{j}}) = 1) \vee (d_{ij} = 0 \wedge (p_{ij} \wedge d_{i\overleftarrow{j}}) = 0)$$

This is equivalent to proving the following logical statement. $(d_{ij} = 1 \wedge p_{ij} = 1 \wedge d_{i\overleftarrow{j}} = 1) \vee (d_{ij} = 0 \wedge p_{ij} = 0 \wedge d_{i\overleftarrow{j}} = 1) \vee (d_{ij} = 0 \wedge d_{i\overleftarrow{j}} = 0)$.

Let us assume $\varepsilon_{ij} = \langle c_{ij}, A_{ij}, B_{ij} \rangle$. We express the above logical statement in terms of the ciphertexts.

$$\begin{aligned} &(b_{ij} = g^{x_{ij} r_{ij}} \wedge c_{ij} = g^{\alpha_{ij} \beta_{ij}} \cdot g \wedge b_{i\overleftarrow{j}} = g^{x_{i\overleftarrow{j}} r_{i\overleftarrow{j}}}) \\ &\quad \vee (b_{ij} = g^{x_{ij} y_{ij}} \wedge c_{ij} = g^{\alpha_{ij} \beta_{ij}} \wedge b_{i\overleftarrow{j}} = g^{x_{i\overleftarrow{j}} r_{i\overleftarrow{j}}}) \\ &\quad \vee (b_{ij} = g^{x_{ij} y_{ij}} \wedge b_{i\overleftarrow{j}} = g^{x_{i\overleftarrow{j}} y_{i\overleftarrow{j}}}) \end{aligned} \tag{3}$$

The public parameters are $X_{ij} = g^{x_{ij}}, Y_{ij} = g^{y_{ij}}$, $R_{ij} = g^{r_{ij}}, A_{ij} = g^{\alpha_{ij}}$ and $B_{ij} = g^{\beta_{ij}}, X_{i\overleftarrow{j}} = g^{x_{i\overleftarrow{j}}}, Y_{i\overleftarrow{j}} = g^{y_{i\overleftarrow{j}}}, R_{i\overleftarrow{j}} = g^{r_{i\overleftarrow{j}}}$. Notice that if $d_{ij} = 1$, $p_{ij} = 1$ and $d_{i\overleftarrow{j}} = 1$, (X_{ij}, R_{ij}, b_{ij}), $(A_{ij}, B_{ij}, c_{ij}/g)$ and $(X_{i\overleftarrow{j}}, R_{i\overleftarrow{j}}, b_{i\overleftarrow{j}})$ are three DDH tuples. Also if $d_{ij} = 0$, $p_{ij} = 0$ and $d_{i\overleftarrow{j}} = 1$, (X_{ij}, Y_{ij}, b_{ij}), (A_{ij}, B_{ij}, c_{ij}) and $(X_{i\overleftarrow{j}}, R_{i\overleftarrow{j}}, b_{i\overleftarrow{j}})$ are three DDH tuples as well. Lastly, if $d_{ij} = 0$ and $d_{i\overleftarrow{j}} = 0$, (X_{ij}, Y_{ij}, b_{ij}) and $(X_{i\overleftarrow{j}}, Y_{i\overleftarrow{j}}, b_{i\overleftarrow{j}})$ are two DDH tuples. So we have to prove a statement that is a logical-OR of three logical-AND sub-statements. In each of the three sub-statements, we essentially prove the items form valid DDH tuples such that each of the three sub-statements is a logical-AND of two/three statements in the form of DDH tuples. The construction of a NIZK proof for the above statement can be found in [24], [25] (also see [21]).

After the second round, all bidders, as well as anyone else with a read access to the bulletin board, can check all NIZK proofs, and compute $T_j = \bigvee_{i=1}^{n} d_{ij}$ based on the veto protocol described in Section II-B. The bidders follow the same procedure to iterate through the rest of bit positions. The logical-OR output from each of the c bit positions constitutes the binary representation of the highest bid, i.e. the highest bid is $T_1 || T_2 || \cdots || T_c$ in binary format. Once, the highest bid is computed, the winning bidder V_w can come forward and prove that she is indeed the real winner either by opening her commitments $\{\varepsilon_{wj} : j \in [1, c]\}$ or by revealing the randomness $x_{w\kappa} = \log_g X_{w\kappa}$ used in the last *deciding* bit position allowing everyone else to decipher the cryptogram submitted by her in the iteration corresponding to the last *deciding* bit position. It is easy to see that only the winner(s) would submit 1-cryptogram(s) in the iteration corresponding to the last *deciding* bit position. Based on x_{wk}, everyone is able to verify if there is only one winner of if there is a tie.

C. Extension to Vickrey Auction

Our main protocol is described for the first-price sealed-bid auction. A straightforward way to extend it to support second-price sealed-bid (i.e., Vickrey auction) works as follows. The protocol is first run to identify the highest bid and the winner, and then run the second time with the winner excluded to compute the second-highest bid. The bidder who commits the second-highest bid remains anonymous. The winner pays the second-highest bid in the end. (Imagine an MPC protocol on the *max* function that satisfies the generic *inclusive privacy* in Definition 1, this would naturally be the method of extension to support the second-price sealed-bid auction.) However, the highest bid will be revealed, which is not strictly necessary, and may cause some privacy concerns.

We describe a more efficient and privacy-preserving method to support the Vickrey auction. In this method, the bit iterations will only need to be run once and the highest bid remains secret. This method is only possible because it builds on the *exclusive privacy* in Definition 2. As we will show in the proof of Theorem 2, at each jth bit iteration, every bidder V_k learns nothing more than $\bigvee_{i\in[1,n]\setminus k} d_{ij}$. Therefore, at each bit iteration, the bidder who remains a winner can learn if she is the only winner in the race. Thus, if the bidder finds that she has submitted the sole one bit in that bit iteration and thus has become a confirmed winner, she declares herself as the winner and steps aside to let other bidders continue. Those losing bidders reset the output of that winning iteration to be 0 and make it a *non deciding* iteration. Losing bidders then continue executing the rest of the steps as specified in the main protocol. This would reveal the next highest bid, while hiding the $c - j$ least significant bits of the highest bid.

IV. Analysis of the SEAL Protocol

In this section, we present security proofs to prove the correctness and the privacy aspects of our protocol. We will focus on the main protocol for the first-prize sealed bid. The same proofs apply to the second-prize sealed bid straightforwardly.

A. Correctness

The following theorem proves that our scheme is correct and it yields the highest bid price of the winner.

Theorem 1: The e-auction scheme discussed above is correct.

Proof: Let us assume the c bits output by the protocol are $last[1 \rightarrow c]$. We need to show that $last[j] = p_{wj}$ for all $j \in [1, c]$, where p_w is the winning bid of the winning bidder V_w. Let m be the last iteration of Stage 1. Hence, according to the protocol $\bigvee_{i=1}^{n} p_{im} = 1$ and for all $j \in [1, m-1], last[j] = \bigvee_{i=1}^{n} p_{ij} = 0$. This essentially means that $last[j] = p_{wj}$ for $j \in [1, m]$.

Now, after iteration m the algorithm shifts from Stage 1 to Stage 2. In Stage 2, all cryptograms generated by a bidder V_i correspond to the logical-AND of the bit at the current position (d_{ij}) and the value of the bit $d_{i\overleftarrow{j}}$ submitted in the most recent *deciding* iteration $\overleftarrow{j}$ such that $last[\overleftarrow{j}] = 1$ and for all $t \in [\overleftarrow{j} + 1, j - 1]$, $last[t] = 0$. Thus, we need to prove that in any iteration j in Stage 2 if $\bigvee_{i=1}^{n} d_{ij} = 1$, then $p_{wj} = 1$ and if $\bigvee_{i=1}^{n} d_{ij} = 0$, then $p_{wj} = 0$. We prove it by method of induction. Without loss of generality, we may assume that $last[t] = p_{wt}, \forall t \in [1, j-1]$. So, we need to prove that $last[j] = p_{wj}$. Now, $last[j] = \bigvee_{i=1}^{n} d_{ij} = \bigvee_{i=1}^{n} p_{ij} \wedge d_{i\overleftarrow{j}} = p_{wj} \wedge d_{w\overleftarrow{j}} \vee \left(\bigvee_{i\in[1,n]\setminus\{w\}} p_{ij} \wedge d_{i\overleftarrow{j}}\right)$. But, according to our assumption, $d_{w\overleftarrow{j}} = 1$. Thus, $last[j] = \bigvee_{i=1}^{n} d_{ij} = \bigvee_{i=1}^{n} p_{ij} \wedge d_{i\overleftarrow{j}} = p_{wj} \vee \left(\bigvee_{i\in[1,n]\setminus\{w\}} p_{ij} \wedge d_{i\overleftarrow{j}}\right)$. If $p_{wj} = 1$, $last[j] = p_{wj}$ trivially holds. We shall have to prove that $(p_{wj} = 0) \implies \left(\bigvee_{i\in[1,n]\setminus\{w\}} p_{ij} \wedge d_{i\overleftarrow{j}}\right) = 0$. If the above statement does not hold then there will be at least one bidder $V_\eta, \eta \in [1, n] \setminus \{w\}$, such that $p_{\eta j} = d_{\eta\overleftarrow{j}} = p_{\eta\overleftarrow{j}} = 1$. This essentially means that $p_{\eta t} = last[t] = p_{wt}$ for all $t \in [1, j-1]$ and $p_{\eta j} = 1, p_{wj} = 0$. This means that the bid price p_η of V_η is higher than that of V_w. This is a contradiction as according to our assumption V_w is the highest bidder and hence $p_w \geq p_\eta$. So, we conclude that the scheme is correct and it yields the maximum bid price, that is $last[j] = p_{wj}, \forall j \in [1, c]$. □

B. Privacy of Losing Bids

In this section, we prove that our protocol satisfies the *exclusive privacy* requirement in Definition 2. More specifically, when the colluding set do not contain the winner, they will learn nothing more than their own inputs and the highest bid; in this case, the definitions of *inclusive privacy* and *exclusive privacy* are equivalent. When the colluding set contain the winner, they will learn no more than the highest bid of the non-colluding set under the Decision Diffie-Hellman (DDH) assumption [22]; they learn the highest bid of the non-colluding set only in the worse case that the winner is decided at the last bit iteration (Theorem 2).

Assumption 1 (DDH Assumption [22]): Given g, g^a, g^b and a challenge $\Omega \in \{g^{ab}, R\}$, where $R \overset{\$}{\leftarrow} G$, it is computationally hard to find whether $\Omega = g^{ab}$ or $\Omega = R$.

Lemma 1: Let G be a group in which the DDH assumption holds. Given g, g^a, g^b, g^c and a challenge $\Omega \in \{g^{ab}, g^{bc}\}$, it is computationally hard to find whether $\Omega = g^{ab}$ or $\Omega = g^{bc}$.

Proof: Let R be a random element in G. Based on the DDH assumption, $(g, g^a, g^b, g^c, g^{ab}) \overset{c}{\approx} (g, g^a, g^b, g^c, R)$. Similarly, $(g, g^a, g^b, g^c, g^{ac}) \overset{c}{\approx} (g, g^a, g^b, g^c, R)$. Since computational indistinguishability is an equivalence relation, the same is also a transitive relation. Thus, we have $(g, g^a, g^b, g^c, g^{ab}) \overset{c}{\approx} (g, g^a, g^b, g^c, g^{ac})$. □

Lemma 2: Based on the DDH assumption, given g, $S_x = \{g^{x_i} : i \in [1, n]\}, S_y = \{Y_i : i \in [1, n]\}, Y_i = g^{y_i} = \prod_{j=1}^{i-1} g^{x_j} / \prod_{j=i+1}^{n} g^{x_j}, i \in [1, n], w, t \in [1, n], w \neq t, R = \{R_i = g^{r_i} : i \in [1, n] \setminus \{w, t\}\}, g^{r_w}, g^{r_t}, \phi \subseteq \{x_i : i \in [1, n] \setminus \{w, t\}\}$ and a challenge $\Omega \in \{A, B\}$, it is computationally hard to find if $\Omega = A$ or $\Omega = B$, where:

$$A = (g, \phi, g^{x_1 z_1}, g^{x_2 z_2}, \ldots, g^{x_{w-1} z_{w-1}}, g^{x_w r_w}, g^{x_{w+1} z_{w+1}}, \ldots,$$
$$g^{x_t y_t}, \ldots, g^{x_n z_n})$$
$$B = (g, \phi, g^{x_1 z_1}, g^{x_2 z_2}, \ldots, g^{x_{w-1} z_{w-1}}, g^{x_w r_w}, g^{x_{w+1} z_{w+1}}, \ldots,$$
$$g^{x_t r_t}, \ldots, g^{x_n z_n}),$$

where z_i is either y_i or r_i for $i \in [1, n] \setminus \{w, t\}$, and ϕ is chosen by the attacker.

Proof: We show that if there exists an adversary $\mathcal{A}'$, against the statement of Lemma 2, she can be used to construct another adversary $\mathcal{A}$ against Assumption 1. $\mathcal{A}$ works as follows:

$\mathcal{A}$ receives as input g, g^a, g^b, g^c and a challenge $\Omega \in \{g^{ab}, g^{ac}\}$. Then she lets $\mathcal{A}'$ select random $x_1, x_2, \ldots, x_{w-1}, x_{w+1}, \ldots, x_{t-1}, x_{t+1}, \ldots, x_n, r \in_R \mathbb{Z}_p$.

Then she sets $X_i = g^{x_i}$ for $i \in [1, n] \setminus \{w, t\}$ and $X_w = g^{x_w} = g^b, X_t = g^{x_t} = g^a$, that is she implicitly sets $x_w = b$ and $x_t = a$. She also computes

$$Y_i = \prod_{j=1}^{i-1} X_j / \prod_{j=i+1}^{n} X_j, \forall i \in [1, n] \setminus \{w, t\}$$

She sets $\omega_i \in_R \{Y_i^{x_i}, R_i^{x_i}\}$, $\forall i \in [1, n] \setminus \{w, t\}$, and

$$\begin{aligned} \omega_w &= (X_w)^{r_w}, \\ \omega_t &= \prod_{i=1}^{w-1} (X_t)^{x_i} \prod_{i=w+1}^{t-1} (X_t)^{x_i} / \prod_{i=t+1}^{n} (X_t)^{x_i} \Omega. \end{aligned}$$

If $\Omega = g^{ab}$, then

$$\begin{aligned} \omega_t &= \prod_{i=1}^{w-1} (X_t)^{x_i} * \prod_{i=w+1}^{t-1} (X_t)^{x_i} / \prod_{i=t+1}^{n} (X_t)^{x_i} * g^{ab} \\ &= \prod_{i=1}^{t-1} (X_t)^{x_i} / \prod_{i=t+1}^{n} (X_t)^{x_i}. \end{aligned}$$

Let, $\omega = (g, \phi, \omega_1, \omega_2, \ldots, \omega_n)$. Hence, if $\Omega = g^{ab}$,

$$\begin{aligned} \omega &= (g, \phi, g^{x_1 z_1}, g^{x_2 z_2}, \ldots, g^{x_{w-1} z_{w-1}}, g^{x_w r_w}, g^{x_{w+1} z_{w+1}}, \ldots, \\ &\quad g^{x_t y_t}, \ldots, g^{x_n z_n}) \\ &= A, \end{aligned}$$

where $x_w = b$ and $x_t = a$. Alternatively, if $\Omega = g^{ac}$, then

$$\begin{aligned} \omega_t &= \prod_{i=1}^{w-1} (X_t)^{x_i} * \prod_{i=w+1}^{t-1} (X_t)^{x_i} / \prod_{i=t+1}^{n} (X_t)^{x_i} * g^{ac} \\ &= (g^{x_t})^{c + \sum_{i=1}^{w-1} x_i + \sum_{i=w+1}^{t-1} x_i - \sum_{i=t+1}^{n} x_i} \\ &= g^{x_t r_t}, \end{aligned}$$

where $r_t = c + \sum_{i=1}^{w-1} x_i + \sum_{i=w+1}^{t-1} x_i - \sum_{i=t+1}^{n} x_i$ or $g^{r_t} = g^c * g^{\sum_{i=1}^{w-1} x_i + \sum_{i=w+1}^{t-1} x_i - \sum_{i=t+1}^{n} x_i}$. Thus, if $\Omega = g^{ac}$,

$$\begin{aligned} \omega &= (g, \phi, g^{x_1 z_1}, g^{x_2 z_2}, \ldots, g^{x_{w-1} z_{w-1}}, g^{x_w r_w}, g^{x_{w+1} z_{w+1}}, \ldots, \\ &\quad g^{x_t r_t}, \ldots, g^{x_n z_n}) \\ &= B. \end{aligned}$$

Now, $\mathcal{A}$ can send $S_x = \{X_i : i \in [1, n]\}$, g^{r_w}, g^{r_t} and ω to $\mathcal{A}'$. $\mathcal{A}'$ will identify ω as either A or B. If $\omega = A$, then $\Omega = g^{ab}$. Else if $\omega = B$, then $\Omega = g^{ac}$. Thus, with the help of $\mathcal{A}'$, we can construct an adversary $\mathcal{A}$ that can break Assumption 1. Hence, the lemma holds. □

Lemma 3: Let C be a set of colluding bidders and H be the set of honest bidders. $C \cup H = [1, n]$. Let $\theta = |H|$. Let us assume $d_{h_i j}$ is the bit corresponding to the cryptogram submitted in iteration j by V_{h_i} for $h_i \in H, i \in [1, \theta]$ and $d_{c_i j}$ is the bit corresponding to the cryptogram submitted in iteration j by V_{c_i} for $c_i \in C, i \in [1, n - \theta]$. The colluding bidders learn nothing more than $\bigvee_{i=1}^{\theta} d_{h_i j}$.

Proof: In an iteration $j \in [1, c]$, if $K_j = \bigvee_{i=1}^{\theta} d_{h_i j} = 0$, the colluding bidders will obviously learn that $d_{h_i j} = 0$ for all $h_i \in H, i \in [1, \theta]$. We shall have to prove that when $K_j = \bigvee_{i=1}^{\theta} d_{h_i j} = 1$, the colluding bidders will not learn any other information. In order for proving this fact it is sufficient to show that

1) the colluding bidders will not be able to distinguish between the two cases where $K_j = \bigvee_{i=1}^{\theta} d_{h_i j} = 1$, but the number of bidders who submitted 1-cryptogram is different.
2) if two honest bidders who submitted different bits exchange their inputs, then this cannot be detected by the adversary.

We choose two scenarios in which a particular honest bidder submits different cryptograms: i.e in one scenario the bidder submits a 0-cryptogram and in the other one she submits a 1-cryptogram. We show that if the value of K_j is 1 in both the scenarios, then the two scenarios will be indistinguishable to the adversary (colluding bidders). Once we prove these results, they could be easily extended to show that the statement of the above lemma holds. Let us assume that the public keys used by the colluding bidders are $(X_{c_i}, R_{c_i}) = (g^{x_{c_i}}, g^{r_{c_i}}), c_i \in C, i \in [1, |C|]$. Similarly, the public keys of the honest bidders will be $(X_{h_i}, R_{h_i}), h_i \in H, i \in [1, \theta]$. The cryptograms of the colluding bidders will be $g^{x_{c_i} z_{c_i}}$, where $z_{c_i} \in \{y_{c_i}, r_{c_i}\}$. Let, $\phi = \{x_{c_i} : i \in [1, |C|]\}$. Now, let us assume that one honest bidder V_{h_w} has submitted a 1-cryptogram in the form: $g^{x_{h_w} r_{h_w}}$. As such we need to show that the colluding bidders will not be able to find whether or not there is another bidder $V_{h_t}, h_t \in H, t \in [1, \theta]$ who also submitted a 1-cryptogram. If V_{h_t} submitted a 1-cryptogram, then her cryptogram will be this: $b_{h_t} = g^{x_{h_w} r_{h_w}}$, and if she submitted a 0 cryptogram, her cryptogram should look like this: $b'_{h_t} = g^{x_{h_t} y_{h_t}}$, where the notations bear usual meanings as they do in the article. Now, according to Lemma 2, no adversary can distinguish between A and B, where

$$\begin{aligned} A &= (\phi, b_1, b_2, \ldots, b_{h_w}, \ldots, b_{h_t}, \ldots, b_n) \\ B &= (\phi, b_1, b_2, \ldots, b_{h_w}, \ldots, b'_{h_t}, \ldots, b_n). \end{aligned}$$

Hence, the colluding bidders will not be able to distinguish between two cases where the value of $K_j = \bigvee_{i=1}^{\theta} d_{h_i j}$ is 1, but the number of bidders $V_{h_i}, h_i \in H$ who submitted 1-cryptogram in iteration j is different.

Let us assume $b_{h_e} = g^{x_{h_e} r_{h_e}}$ and $b'_{h_e} = g^{x_{h_e} y_{h_e}}$ for $e \in \{w, t\}$. Now, observe that

$$\begin{aligned} B &= (\phi, b_1, b_2, \ldots, b_{h_w}, \ldots, b'_{h_t}, \ldots, b_n) \\ &\overset{c}{\approx} (\phi, b_1, b_2, \ldots, b_{h_w}, \ldots, b_{h_t}, \ldots, b_n) \\ &\overset{c}{\approx} (\phi, b_1, b_2, \ldots, b'_{h_w}, \ldots, b_{h_t}, \ldots, b_n). \end{aligned}$$

Hence, the colluding adversary will not be able to distinguish between two cases where a pair of honest bidders exchange the value of their submitted bits whose values are complement to each other. This way anyone can prove that as long as at least one bidder submits a 1-cryptogram in any iteration, the colluding bidders will not be able to distinguish between the set of all possible cryptograms corresponding to all possible values of the bits submitted by honest bidders. What the colluding bidders learn is the logical-OR of all bits submitted by all honest bidders which is given by $K_j = \bigvee_{i=1}^{\theta} d_{h_i j}$, $j \in [1, c]$. □

Theorem 2: The proposed e-auction scheme satisfies the *exclusive-privacy* in Definition 2.

TABLE I

THE NUMBER OF EXPONENTIATIONS IN COMPUTATIONAL LOAD. HERE, c IS THE LENGTH OF THE BINARY REPRESENTATION OF A BID-PRICE. n IS THE TOTAL NUMBER OF BIDDERS AND τ IS THE NUMBER OF ITERATIONS OF STAGE 1

	Setup		**Stage 1**			**Stage 2**			
Entity	**Commitment**	**ZKP**	**Key**	**Cryptogram**	**ZKP**	**Key**	**Cryptogram**	**ZKP**	**Total**
Bidder	$3c$	$8c$	2τ	τ	14τ	$2(c-\tau)$	$(c-\tau)$	$30(c-\tau)$	$44c-16\tau$
Verifier	-	$12nc$	-	-	$20n\tau$	-	-	$36n(c-\tau)$	$48nc-16n\tau$

Proof: Based on Lemma 3, at each bit iteration the colluding set learn nothing more than $K_j = \bigvee_{i=1}^{\theta} d_{h_i j}$, $j \in [1, c]$. Here $d_{h_i j}$ is the bit submitted by V_{h_i} at the jth iteration; it is equal to the actual bid value $b_{h_i j}$ only if the bidder V_{h_i} remains in the race (she will have to submit 0 if she has lost in the race as enforced by the ZKP in Eq. 2). Assume the winner is decided at the βth iteration, $1 \leq \beta \leq c$. If the colluding set do not contain the winner, the bit value K_j that they learn is the same as the jth most significant bit in the highest bid. In other words, they learn nothing more than the highest bid of all bidders. However, if the colluding set contain the winner, they can learn $K_1||K_2||\ldots||K_\beta$, which are the β most significant bits of the maximum bid of the non-colluding set H. The colluding set will learn the maximum bid of the non-colluding set in the worse case when $\beta = c$ (namely, the winner is only decided in the last bit iteration). Hence, the result. □

V. EFFICIENCY OF THE SCHEME

First, we discuss the computation overhead of our protocol. Since exponentiation is the costliest operation in our scheme, we measure the computation cost in terms of the number of exponentiations performed by a single entity. During the setup phase, each bidder generates commitments to each of the c bits of its bid-price. Each commitment requires 3 exponentiations. Hence, the total number of exponentiations required is $3c$. In order for generating NIZK proof of well-formedness of the commitments, the bidder needs to do $8c$ exponentiations. In every iteration of Stage 1, a bidder generates a pair of keys, publishes the public key and a cryptogram which encrypts a single bit. Computation of the public key requires 2 exponentiations. Also, the computation of the cryptogram requires 1 exponentiation. The zero knowledge proofs in Stage 1 require 14 exponentiations. Thus for one each iteration of Stage 1 a bidder needs to do 17 exponentiations. If there are τ iterations of Stage 1, then each bidder will need to perform 17τ exponentiations. Similar to Stage 1, in Stage 2, each bidder will need to perform 3 exponentiations in order to generate the keys and the cryptogram in an iteration. Again, computation of the NIZK proofs requires at most 30 exponentiations in every iteration of Stage 2. Hence, each bidder needs to perform 33 exponentiations per iteration of Stage 2. Since, the sum of all iterations of Stage 1 and Stage 2 is c, the total number of iterations of Stage 2 is $c - \tau$. Thus, each bidders performs $33(c - \tau)$ exponentiations in all the $c - \tau$ iterations of Stage 2. Therefore, the total number of exponentiations done by a single bidder during all the 3 phases (Setup, Stage 1 and Stage 2) is $44c - 16\tau$. The verifier needs to perform $48c - 16\tau$ exponentiations in order to check all the NIZK proofs generated by a single bidder during the auction process. Table I shows a break-down of the computation overhead on a bidder and a verifier.

During the setup phase a bidder generates c commitments corresponding to c bits of the bid-price. Each commitment is a 3-tuple. The bidder also generates NIZK proof of well-formedness of the c commitments. Each of such proof consists of 14 elements. Thus during the setup phase each bidder generates information of size $17c$. During one iteration of Stage 1, a bidder publishes a key of size 2, a cryptogram of size 1 and three NIZK proofs of total size 20. Hence, for τ iterations of Stage 1, the total bandwidth consumed is 23τ. During one iteration of Stage 2, a bidder generates a key of size 2, a cryptogram of size 1, three NIZK proofs of total size equal to 33. So, for $c-\tau$ iterations, the total space complexity turns out to be $36(c-\tau)$. In aggregate, each bidder generates a total of $53c-13\tau$ units of data. The verifier needs to download all the data generated by n distinct bidders for examining the authenticity of the NIZK proofs. Hence, the communication overhead on the verifier is n times that of a common bidder. Table II shows a break-down of the communication overhead on a bidder and a verifier.

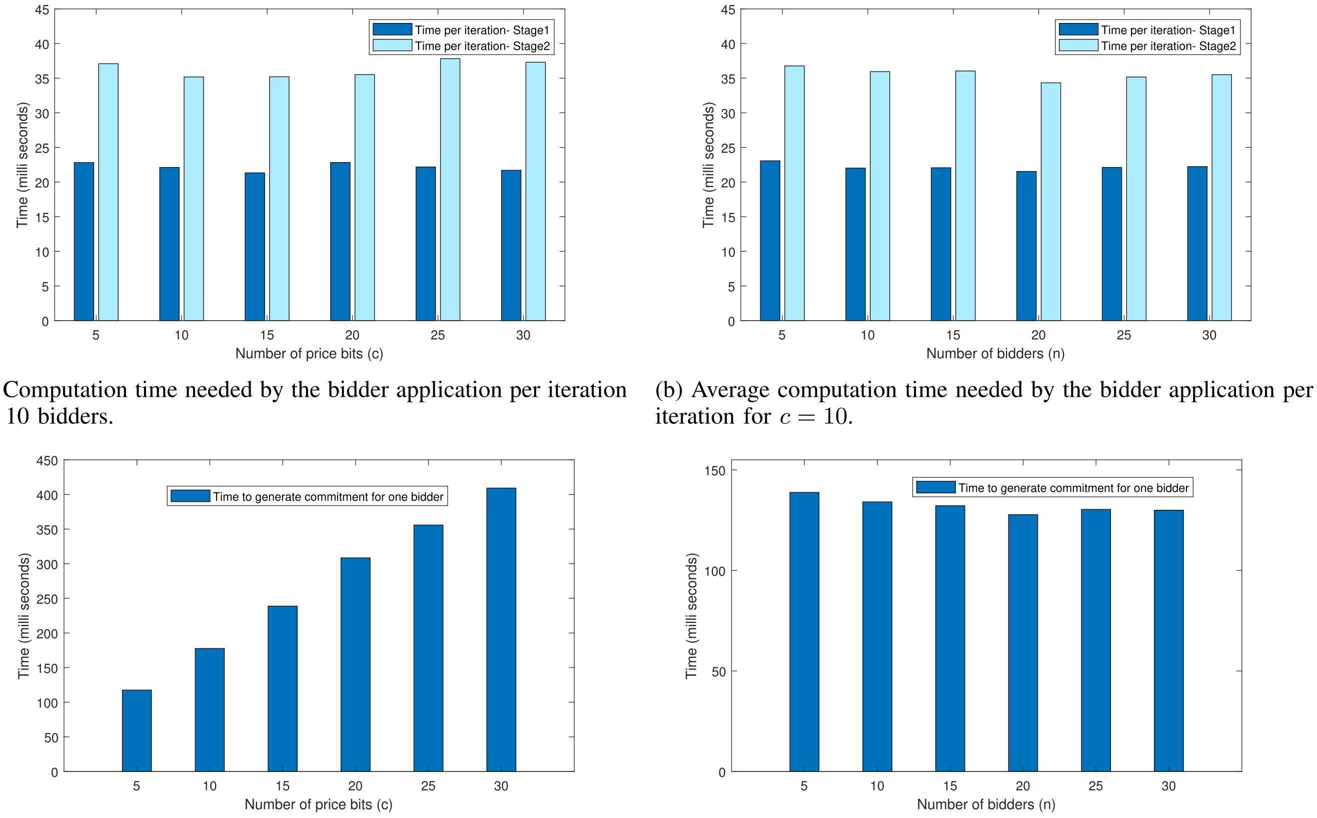
Based on Table I and II, we can conclude that with respect to the bit length c of the bid price, our protocol incurs a linear complexity $O(c)$ for both the computational load and the bandwidth usage. The computation per bidder remains roughly unchanged with the number of participants n, although the verification cost increases linearly with more participants. Assuming that every bidder is also a verifier, responsible for checking every other bidder's ZKPs, our protocol incurs a linear computational and communication complexity $O(n)$, with respect to the number of participants n. These are the best possible system complexities that one may hope for. In practice, the verification of the ZKPs may be centrally performed by the public bulletin board before the data is published and every observer is able to check at any time. This can alleviate each bidder's task in verifying the ZKPs.

We have implemented the SEAL auction scheme using Java on a Linux platform. The experiment was done on an Asus A Series Core i3 laptop (2.10 GHz with 4 GB RAM). We have plotted four graphs on the basis of the data obtained from this experiment. Figure 2a depicts the average time needed to generate the parameters in one iteration of Stage 1 and Stage 2 for different values of c, i.e., the bit-length of the maximum bid-price. Here we have fixed the number of bidders n at 10. Figure 2b shows the average time needed to generate the parameters in one iteration of Stage 1 and Stage 2 for different values of n, the number of bidders. Here, we have fixed the value of c at 10. Figure 2c depicts the average time needed to

TABLE II

COMMUNICATION BANDWIDTH (IN TOTAL NUMBER OF G AND Z_p ELEMENTS). HERE, c IS THE LENGTH OF THE BINARY REPRESENTATION OF A BID-PRICE. n IS THE TOTAL NUMBER OF BIDDERS AND τ IS THE NUMBER OF ITERATIONS OF STAGE 1

	Setup		**Stage 1**			**Stage 2**			
Entity	**Commitment**	**ZKP**	**Key**	**Cryptogram**	**ZKP**	**Key**	**Cryptogram**	**ZKP**	**Total**
Bidder	$3c$	$14c$	2τ	τ	20τ	$2(c-\tau)$	$(c-\tau)$	$33(c-\tau)$	$53c-13\tau$
Verifier	$3nc$	$14nc$	$2n\tau$	$n\tau$	$20n\tau$	$2n(c-\tau)$	$n(c-\tau)$	$33n(c-\tau)$	$53nc-13n\tau$



(a) Computation time needed by the bidder application per iteration for 10 bidders.

(b) Average computation time needed by the bidder application per iteration for $c = 10$.

(c) Computation time needed by the bidder application in the Commit phase for 10 bidders

(d) Computation time needed by the bidder application in the Commit phase for a fixed $c = 10$

Fig. 2. Time required by a bidder at different stages.

generate the c commitments by one bidder for different values of c with $n = 10$. Figure 2d depicts the average time needed to generate the commitments by one bidder for different values of n with $c = 10$.

It can be observed from Figure 2a and 2b that the time required to finish one iteration in Stage 1 and Stage 2 remains almost the same irrespective of the number of bidders or the value of c. In other words, if there are a iterations of Stage 1 and $c-a$ iterations of Stage 2, then the total time to complete all the c iterations will be $a \cdot t_1 + (c-a) \cdot t_2$, where t_1 and t_2 are the time required to complete exactly one iteration at Stage 1 and 2 respectively. So, the time to execute all the c iterations will be upper-bounded by the the time to complete c iterations of Stage 2. Figure 2c shows that the time taken to generate all the commitments for all the c bits of one bid-price also increases linearly with the increase of the value of c when the number of bidders is constant. Additionally, Figure 2d shows that the time to compute the commitments for all the c bits of the bid-price of one bidder does not depend on the number of bidders. We therefore conclude that the overall time required to finish the auction protocol per bidder (including the time to generate commitments and the time to execute c iterations of the main protocol) is linear in the bit length c of the highest bid-price irrespective of the number of bidders. This corroborates the theoretical analysis in Table I. Obviously, the communication bandwidth per bidder scales linearly with the bit length of the bid price as well given the constant size of the message sent at each bit iteration for both Stage 1 and 2 (see Table II).

VI. RELATED WORK

Sealed-bid e-auction can be regarded as an instance of secure multiparty computation (MPC) on a *max* function, where participants jointly compute the maximum of a set of inputs while preserving the privacy of other input values. Generic MPC techniques generally require pairwise secret channels between the participants, in addition to an authenticated public channel [12]. However, pairwise secret channels are difficult to realize among bidders who are mutually distrustful. In addition, generic MPC techniques suffer from various efficiency issues [14]. For these reasons, although inspiring in theory, they are not directly applicable to build a decentralized sealed-bid e-auction scheme. In the following, we will review main e-auction schemes in the literature.

Since the early work by Franklin and Reiter in 1996 [3], researchers have proposed many sealed-bid e-auction schemes [2]–[4], [6]–[10], [16], [17], [26], [27]. Most of these schemes involve the role of an "auctioneer", which mirrors a similar role in traditional auctions. Hence, the mainstream research in this field focuses on applying cryptography to distribute trust on the "auctioneer". In general, there are two main approaches.

The first approach is to apply threshold cryptography, or MPC techniques [10] to distribute the trust from a single auctioneer to several auctioneers. Franklin et al. presented a second-price sealed-bid auction scheme in [3]. In this scheme, a number of servers play the role of the auctioneer, and they apply Shamir's secret sharing to split each bid among themselves so no single server sees all bids. However, if a sufficient number of servers collude, the secrecy of all bids is lost. Sako proposed a similar scheme based on threshold cryptography to let auctioneers jointly decrypt submitted bids [4]. Kurosawa and Ogata proposed a bit-slice approach for auctioneers to determine the highest bid, bit by bit, assuming the majority of the auctioneers are honest [17]. Their system involves m bidders and n auctioneers. The auctioneers apply secure multi-party computation on a bit-slice circuit, and decrypt the result at each bit position using verifiable threshold decryption. The threshold is set such that compromising the decryption requires compromising at least the majority of the auctioneers. The number of rounds required for threshold decryption is $O(n \cdot c)$, c being the bit length of the bid and n being the number of participants in the decryption process. The Kurosawa-Ogata's method, like many other works [3], [9]–[11], performs encryption and decryption of bids as two separate phases. By comparison, in our protocol, the encryption and decryption operations are more integrated within the constant 2-round Boolean-OR computation (veto protocol) at each bit iteration, which results in $O(c)$ rounds in total regardless of the number of participants. Furthermore, our protocol is free from any auctioneers. Bogetoft et al. proposed to apply secure MPC to sealed-bid auction [9], [10]. Their solution was used in Denmark for auction sales on sugar beets. In Bogetoft et al.'s solution, the role of the auctioneer is played by three parties. It is assumed that at least 2 parties must be honest. Cartlidge et al. proposed an e-auction scheme for dark pools/markets where all bids are encrypted under a global public key and the decryption is performed by auctioneers using MPC [11]. They presented two implementations based on the SCALE-MAMBA library: the first uses the SPDZ protocol [11] to implement the role of "auctioneer" as two servers assuming at least one is trustworthy; the second uses Shamir's secret sharing to implement the auctioneers as three servers assuming at least one of them is trustworthy. In all these auctioneer-based protocols, if auctioneers collude all together, they can trivially break the privacy of sealed bids.

The second approach is to introduce more trusted third parties in addition to auctioneers. Naor et al. presented a second-price sealed auction scheme in [5]. This scheme uses two different auction servers who communicate using an oblivious transfer protocol. One server takes the role as an auctioneer and the other as an auction issuer. The two servers are assumed not to collude. However, the original Naor et al.'s scheme has a weakness in which one of the two servers can cheat to modify bids without detection. This weakness was later addressed by Juels and Szydlo in [8], but the revised scheme still requires the two servers must not collude. In [27], Abe and Suzuki proposed an (M + 1)-st price sealed bid auction using homomorphic encryption and the mix and match technique. The scheme involves an auctioneer and a trusted authority, who are assumed not to collude. In [28], Montengero et al. propose a sealed-bid online auction scheme that employs an auctioneer and a randomness server. The randomness server is trusted to provide the randomness for the bidders in the protocol and not to collude with the auctioneer. In [26], Lipmaa et al. proposed Vickrey auction schemes that involve a seller and an auction authority. The seller and the authority authority are assumed not to collude. In [29], Galal and Youssef proposed a Vickrey auction system by using the Intel SGX enclave as a trusted hardware device to compute the winner. Here, the SGX enclave essentially plays the role as an auctioneer. Similar solutions based on trusted computing are presented in [30].

Brandt was among the first to argue that neither of the above approaches is desirable due to the involvement of trusted auctioneers or third parties. He proposed the notion of "bidder-resolved auction" and a concrete auctioneer-free solution in [7] by applying secret sharing techniques. Follow-up works by Brandt, with improvement in efficiency, are published in [2], [13], [14]. In all these "bidder-resolved auction" schemes, a seller is actively involved in the protocol and is assumed not to collude with bidders. However, as pointed out by Dreier *et al.* [31], if the seller colludes with a subset of bidders in Brandt's bidder-resolved auctions schemes, they can learn the bids of other participants. Another major limitation in Brandt's schemes is that they incur exponential computational and communication complexities $O(2^c)$, where c is the bit length of the bid price. Motivated by Brandt's initial 2002 scheme [7], Wu et al. remove the seller and propose a decentralized sealed-bid auction scheme based on a general socialist millionaire protocol. However, a critical downside of their system is that the computational load and the bandwidth usage per bidder is exponential $O(2^c)$ with respect to the bit length of the bid price, which makes their scheme less than practical.

VII. Conclusion

In this article, we propose a publicly verifiable sealed bid auction scheme that does not require any auctioneer and has a linear system complexity in terms of computation and communication with respect to the bit length of the bid. The bidders execute the protocol themselves and compute the highest bid while preserving the privacy of losing bids.

Furthermore, our protocol does not require any secret channels and all operations are publicly verifiable. Overall, our work removes the dependence on any auctioneer and drastically reduces the system complexity associated with existing state-of-the-art auction schemes. This brings secure e-auction much closer to practice.

REFERENCES

[1] V. Krishna, *Auction Theory*. New York, NY, USA: Academic, 2009.

[2] F. Brandt, "How to obtain full privacy in auctions," *Int. J. Inf. Secur.*, vol. 5, no. 4, pp. 201–216, 2006.

[3] M. K. Franklin and M. K. Reiter, "The design and implementation of a secure auction service," *IEEE Trans. Softw. Eng.*, vol. 22, no. 5, pp. 302–312, May 1996.

[4] K. Sako, "An auction protocol which hides bids of losers," in *Proc. Int. Workshop Public Key Cryptogr.* Berlin, Germany: Springer, 2000, pp. 422–432.

[5] M. Naor, B. Pinkas, and R. Sumner, "Privacy preserving auctions and mechanism design," *Proc. EC*, Nov. 1999, pp. 129–139.

[6] W. Qianhong, W. Changjie, C. Xiaofeng, and W. Yumin, "Publicly verifiable auctions with minimal leakage," in *Proc. 28th Annu. Int. Comput. Softw. Appl. Conf. (COMPSAC)*, Sep. 2004, pp. 384–389.

[7] F. Brandt, "Secure and private auctions without auctioneers," Institut für Informatick, Technische Universität München, Munich, Germany, Tech. Rep. FKI-245–02, 2002.

[8] A. Juels and M. Szydlo, "A two-server, sealed-bid auction protocol," in *Proc. Int. Conf. Financial Cryptogr.* Berlin, Germany: Springer, 2002, pp. 72–86.

[9] P. Bogetoft, I. Damgård, T. Jakobsen, K. Nielsen, J. Pagter, and T. Toft, "A practical implementation of secure auctions based on multiparty integer computation," in *Financial Cryptography and Data Security*, vol. 4107. Berlin, Germany: Springer, 2006, pp. 142–147.

[10] P. Bogetoft *et al.*, "Secure multiparty computation goes live," in *Financial Cryptography and Data Security*, vol. 5628. Berlin, Germany: Springer, 2009, pp. 325–343.

[11] J. Cartlidge, N. P. Smart, and Y. T. Alaoui, "MPC joins the dark side," in *Proc. ACM Asia Conf. Comput. Commun. Secur.*, 2019, pp. 148–159.

[12] O. Goldreich, S. Micali, and A. Wigderson, "How to play ANY mental game," in *Proc. 19th Annu. ACM Symp. Theory Comput.*, 1987, pp. 218–229.

[13] F. Brandt, "Fully private auctions in a constant number of rounds," in *Financial Cryptography*. Berlin, Germany: Springer, 2003, pp. 223–238.

[14] F. Brandt and T. Sandholm, "Efficient privacy-preserving protocols for multi-unit auctions," in *Financial Cryptography and Data Security* (Lecture Notes in Computer Science), vol. 3570. Berlin, Germany: Springer, 2005, pp. 298–312.

[15] R. Cramer, I. Damgård, S. Dziembowski, M. Hirt, and T. Rabin, "Efficient multiparty computations secure against an adaptive adversary," in *Advances in Cryptology—EUROCRYPT*. Berlin, Germany: Springer, 1999, pp. 311–326.

[16] M. Jakobsson and A. Juels, "Mix and match: Secure function evaluation via ciphertexts," in *Advances in Cryptology—ASIACRYPT*. Berlin, Germany: Springer, 2000, pp. 162–177.

[17] K. Kurosawa and W. Ogata, "Bit-slice auction circuit," in *Computer Security—ESORICS*. Berlin, Germany: Springer, 2002, pp. 24–38.

[18] F. Hao and P. Zieliński, "A 2-round anonymous veto protocol," in *Proc. Int. Workshop Secur. Protocols*. Berlin, Germany: Springer, 2006, pp. 202–211.

[19] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof systems," *SIAM J. Comput.*, vol. 18, no. 1, pp. 186–208, Feb. 1989.

[20] M. Blum, P. Feldman, and S. Micali, "Non-interactive zero-knowledge and its applications," in *Proc. 20th Annu. ACM Symp. Theory Comput.*, 1988, pp. 103–112.

[21] S. Bag, F. Hao, S. F. Shahandashti, and I. G. Ray, "SEAL: Sealed-bid auction without auctioneers," Int. Assoc. Cryptol. Res., Tech. Rep. 2019/1332, 2019. [Online]. Available: https://eprint.iacr.org/2019/1332

[22] D. Boneh, "The decision Diffie-Hellman problem," in *Proc. Int. Algorithmic Number Theory Symp.* Berlin, Germany: Springer, 1998, pp. 48–63.

[23] R. Cramer, I. Damgård, and B. Schoenmakers, "Proofs of partial knowledge and simplified design of witness hiding protocols," in *Proc. Annu. Int. Cryptol. Conf.* Berlin, Germany: Springer, 1994, pp. 174–187.

[24] J. Camenisch and M. Stadler, "Proof systems for general statements about discrete logarithms," Dept. Comput. Sci., ETH Zürich, Zürich, Switzerland, Tech. Rep. 260, 1997.

[25] S. A. Brands, *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy*. Cambridge, MA, USA: MIT Press, 2000.

[26] H. Lipmaa, N. Asokan, and V. Niemi, "Secure vickrey auctions without threshold trust," in *Proc. Int. Conf. Financial Cryptogr.* Berlin, Germany: Springer, 2002, pp. 87–101.

[27] M. Abe and K. Suzuki, "M+ 1-st price auction using homomorphic encryption," in *Public Key Cryptography*, vol. 2274. Berlin, Germany: Springer, 2002, pp. 115–124.

[28] J. A. Montenegro, M. J. Fischer, J. Lopez, and R. Peralta, "Secure sealed-bid online auctions using discreet cryptographic proofs," *Math. Comput. Model.*, vol. 57, nos. 11–12, pp. 2583–2595, 2013.

[29] H. S. Galal and A. M. Youssef, "Verifiable sealed-bid auction on the ethereum blockchain," in *Financial Cryptography Data Security*. Berlin, Germany: Springer, 2018, pp. 265–278.

[30] R. Ankele, K. A. Küçük, A. Martin, A. Simpson, and A. Paverd, "Applying the trustworthy remote entity to privacy-preserving multiparty computation: Requirements and criteria for large-scale applications," in *Proc. Int. IEEE Conf. Ubiquitous Intell. Comput., Adv. Trusted Comput., Scalable Comput. Commun., Cloud Big Data Comput., Internet People, Smart World Congr. (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld)*, Jul. 2016, pp. 414–422.

[31] J. Dreier, J.-G. Dumas, and P. Lafourcade, "Brandt's fully private auction protocol revisited," in *Progress in Cryptology—AFRICACRYPT*. Berlin, Germany: Springer, 2013, pp. 88–106.

Samiran Bag received the M.Tech. degree in computer science and the Ph.D. degree from the Indian Statistical Institute. He is currently a Research Fellow with the Department of Computing Science, University of Warwick, U.K. His primary research areas are electronic voting, cryptocurrency, and secure multiparty computation.

Feng Hao received the Ph.D. degree in computer science from the University of Cambridge in 2007. After working in security industry for several years, he joined the School of Computing, Newcastle University, as a Lecturer in 2010, became a Reader in 2014, and a Professor in 2018. He is currently a Professor in security engineering with the Department of Computer Science, University of Warwick. His research interests include applied cryptography, system security, and efficient computing algorithms.

Siamak F. Shahandashti received the Ph.D. degree from the University of Wollongong, Australia. He has been with Victoria University, Sydney, École Normale Supérieure, Paris, and Newcastle University, U.K. He is currently a Lecturer (Assistant Professor) with the University of York, U.K. His research interests include applied cryptography, privacy-preserving protocols, electronic voting, and usable security.

Indranil Ghosh Ray received the M.C.A. degree in computer applications from the University of Kalyani and the Ph.D. degree from the Indian Statistical Institute.

He is currently a Research Fellow with the Department of Computing Science, University of Warwick, U.K. His primary research interests include privacy preserving cloud computing, PAKE, electronic voting, searchable encryption, MDS codes, and their applications in lightweight cryptography.