A verifiable, bidder-resolved Auction Protocol

Felix Brandt
Institut für Informatik
Technische Universität München
80290 München, Germany
brandtf@in.tum.de

ABSTRACT

Security and privacy have become crucial factors in auction design. Various schemes to ensure the safe conduction of sealed-bid auctions have been proposed recently. We introduce a new standard of privacy for auctions ("full privacy"), that prevents extraction of bid information despite any collusion of participants. This requirement is stronger than other common assumptions that prohibit the collusion of certain third-parties (e.g., distinct auctioneers). Full privacy can be obtained by applying a secret sharing scheme in which the bidders jointly compute the selling price on their own without uncovering any additional information. No auctioneers or other trusted third parties are used to resolve the auction.

The major contribution of this work is the fully private $(M+1)$st-price auction protocol in which only the winning bidders and the seller learn the selling price. To the best of our knowledge there is no other cryptographic auction protocol that achieves a similar level of privacy. The auction outcome cannot be changed or nullified by dishonest bidders because the protocol is publicly verifiable. As full privacy is our main goal, the drawback of the presented protocol is efficiency. Without relaxing any security demands, it is only applicable for high-security auctions with relatively few bidders in reasonable time.

1. INTRODUCTION

Auctions have become the major phenomenon of electronic commerce during the last years. In recent times, the need for privacy has been a factor of increasing importance in auction design. Even the world's largest internet auction house `ebay` recently introduced a "private auction", in which bids are anonymous and only the seller and the winning bidder learn the result of the auction. Obviously, privacy in these auctions is very limited as it is up to the auction house whether the bids remain confidential. Non-public, high-revenue auctions like spectrum license auctions require a much higher level of protection.

We consider a situation where one seller and n bidders or buyers intend to come to an agreement on the selling of a good[1]. Each bidder submits a sealed bid expressing how much he is willing to pay. The bidders want the highest bidder to win the auction for a price that has to be determined by a publicly known rule (e.g., the highest or second-highest bid). In order to fulfill this task, they need a trusted third-party, which is called the "auctioneer". In a regular first-price auction, there are few possibilities to cheat for the auctioneer if he has to announce the selling price at the end of the auction. He could declare a price greater than the highest bid, in order to keep the good if he thinks the bids are not high enough. No bidder would be able to discover this form of deception. In a second-price or so-called Vickrey auction [32], where the highest bidder wins by paying the amount of the second-highest bid, things are worse. The winner of an auction has to doubt whether the price the auctioneer tells him to pay is actually the second-highest bid. The auctioneer could easily make up a "second-highest" bid to increase his (or the seller's) revenue. In addition to a possibly insincere auctioneer, bidders in all sealed-bid auctions have to reveal their bids to the auctioneer. There are numerous ways to misuse these values by giving them away to other bidders or the seller [7, 6, 4]. It remains in the hands of the auctioneer whether the auction really is a *sealed*-bid auction.

Among the different auction protocols, the Vickrey auction has received particular attention in recent times because it is "incentive-compatible", i.e., bidders are always best off bidding their private valuation of a good. This is a huge advantage over first-price auctions, where bidders have to estimate the other bidders' valuations when calculating their bid. However, despite its impressive theoretical properties, the Vickrey auction is rarely used in practice. This problem has been addressed several times in the literature [24, 23, 27] and it is now common knowledge that the Vickrey auction's sparseness is due to two major reasons:

- the fear of an untruthful auctioneer and
- the reluctance of bidders to reveal their true valuations

The proposed protocol removes both crucial weaknesses of the Vickrey auction by omitting the auctioneer and distributing the calculation of the selling price on the bidders

[1] The assignment of tasks in reverse auctions works similarly.

themselves. No information concerning the bids is revealed unless all bidders share their knowledge, which obviously uncovers all bids in any auction protocol. Furthermore, our protocol is applicable to uniform-price or so-called $(M+1)$st-price auctions as well. In a $(M+1)$st-price auction, the seller offers M identical items and each bidder intends to buy *one* of them. It has been proven by Wurman et al [35] that it is an incentive-compatible mechanism to sell those items to the M highest bidders for the uniform price given by the $(M+1)$st highest bid. The Vickrey auction is just a special case of this mechanism for the selling of single goods $(M = 1)$.

The remainder of this paper is structured as follows. Section 2 summarizes existing efforts in the field of cryptographic auction protocols. Section 3 defines essential attributes that ensure a secure and private auction conduction and introduces "bidder-resolved auctions". In Section 4, we propose and analyze the bidder-resolved auction protocol vMB-SHARE. The paper concludes with a brief overview of advantages and disadvantages of vMB-SHARE and an outlook in Section 5.

2. RELATED WORK

There has been a very fast-growing interest in cryptographic protocols for auctions during the last years. In particular, Vickrey auctions, which are strategically equivalent to English auctions for bidders that privately evaluate a good, and recently $(M+1)$st-price auctions attracted much attention. Starting with the work by Franklin and Reiter [13], which introduced the basic problems of sealed-bid auctions, but disregarded the privacy of bids after the auction is finished, many secure auction mechanisms have been proposed, e.g., [1, 2, 4, 8, 14, 15, 16, 17, 18, 19, 20, 21, 25, 26, 30, 33, 34, 37].

When taking away all the protocols that (in their current form) are not suitable for the secure execution of *second*-price auctions or reveal (partial) information after the auction is finished [13, 34, 26, 25, 15, 19, 33, 4], the remaining work can be divided into two categories.

Most of the publications rely on computation that is distributed among auctioneers [16, 18, 17, 14, 30]. This technique requires m auctioneers, out of which a fraction (e.g., $\lfloor \frac{m-1}{3} \rfloor$) must be trustworthy (*threshold cryptography*). Bidders send shares of their bids to each auctioneer. The auctioneers jointly compute the selling price without ever knowing a single bid. This is achieved by using sophisticated techniques of secure multiparty function evaluation, mostly via distributed polynomials (see Section 4.1.1). However, a collusion of, e.g., three out of five auctioneer servers can already exploit the bidders' trust. We argue that distributing the trust onto several distinct auctioneers does not solve the privacy problem, because you can never rule out that some of them, or even *all* of them, collude. This point of view is supported in a growing number of publications [20, 21, 31].

The remaining auction protocols prune the auctioneer's ability to falsify the auction outcome and reveal confidential information by introducing a new third-party that is not *fully* trusted. However, all of these approaches make weak assumptions about the trustworthiness of this third-party. In [2, 8] the third-party may not collude with any participating bidder; in [20, 21] it is prohibited that the third-party and the auctioneer collude. A recent scheme [1, 37] uses a homomorphic, indistinguishable public-key encryption scheme like ElGamal to compute on encrypted bids. However, the private key is either held by a trusted third-party or is shared among a set of confidants.

Concluding, all present work on secure auctions more or less relies on the exclusion of third-party collusion, may it be auctioneers or other semi-trusted institutions. Additionally, to our knowledge, all existing schemes publicly announce the winner's identity and the selling price rather than making this information only visible to the seller and the winning bidder.

3. GENERAL ASSUMPTIONS

This section contains demands that our protocols will meet. Furthermore, we make several basic assumptions about bidders and collusions between them.

3.1 Privacy and Correctness

The required properties for safe conductions of sealed-bid auctions can be divided into two categories.

Privacy *No information concerning bids and the corresponding bidders' identities is revealed during and after the auction.*

The only information that naturally has to be delivered is the information that is needed to carry out the transaction, i.e., the winning bidders and the seller learn the selling price and the seller gets to know the winners' identities. As [26] pointed out, *anonymity* of the winners is crucial. Otherwise, a bidder that breaks a collusive agreement could be identified by his partners.
In several schemes, it is necessary that the auctioneer announces the selling price, in order to prevent the auctioneer from awarding a contract to a bogus bidder (which would violate *correctness*).

Privacy, as we understand it, implies that no information on any bid is revealed to the public, in particular no bid statistics (e.g., the amount of the lowest bid or an upper bound for the highest bid) can be extracted, unlike some other protocols.

Correctness *The winner and the selling price are determined correctly.*

This requirement includes *non-repudiation* (the winning bidders cannot deny having made winning bids). Bids are binding. Otherwise, bidders could control the selling price in first-price and second-price auctions by using sub-agents that default on their bids. Correctness also includes *robustness* (no subset of malicious bidders can render the auction outcome invalid). If the auction protocol is interactive, this implies that missing bidder messages will not halt the auction process.

Of course, *efficiency* is also an important factor, but as we mainly intend to obtain full privacy, we regard efficiency as secondary. Privacy and correctness have to be ensured in a hostile environment, which is described by the following assumptions.

- Each agent (bidder or seller) can have arbitrarily many bidder sub-agents, controlled by him, in any auction.
- Up to $n-1$ bidders might share their knowledge and act as a team
- Any number of auctioneers or other third-parties might share their knowledge and give it away to bidders.

3.2 Bidder-resolved Auctions

According to the assumptions of the previous section, bidders cannot trust any third-party. We therefore distribute the trust onto the bidders themselves using a secret sharing scheme. Bidders divide their bids into n shares, keep one and send one share to each other bidder.

The information sharing among bidders allows us to set a new standard for privacy. In a scenario with m auctioneers it cannot be ruled out that all of them collude. However, when distributing the computation on n bidders, we can assume that *all* bidders will never share their knowledge due to the competition between them. If they did, each of them would abandon his own privacy, resulting in an open auction.

Definition: A secure, bidder-resolved auction protocol complies with *full privacy* when no information on any bid can be retrieved unless all involved agents collude.

When using terms of secure multiparty computation [12], full privacy can be interpreted as $(n-1)$-privacy. A passive adversary that controls up to $n-1$ bidders is incapable of uncovering any information. Active adversaries, that mutilate the distributed computation will be detected if the computation is publicly verifiable.

A threshold-scheme, that provides t-resilience is not appropriate when information is shared among bidders, as any group of bidders might collude due to the assumptions of the previous section. As a consequence, we cannot adapt existing, successful auction protocols that were designed for m auctioneers like [14], or [16], because they rely on secure multiparty computation according to Ben-Or, Goldwasser and Widgerson [3], which in turn provides at most insufficient $\lfloor \frac{n}{2} \rfloor$-privacy due to the multiplication of degree n polynomials.

When computation is shared among bidders, it is obviously required that bidders "know" each other. This can be achieved by carrying out a registration phase, in which bidders publish their addresses on a blackboard before the actual auction begins.

In [5], we proposed the first bidder-resolved auction protocol YMB-SHARE[2]. Malicious bidders cannot reveal information in this protocol, but they can disrupt the auction. The protocol lacks verifiability, reveals information when winning bids are equal, and is only applicable to *second*-price sealed-bid auctions. All of these issues will be removed in vMB-SHARE.

4. PROTOCOL vMB-SHARE

In order to gain public verifiability, we need cryptographic primitives like verifiable secret sharing and various interactive and non-interactive proofs of correctness. As is customary in cryptology, we denote two different communicating parties by "Alice" and "Bob". Please note that interactive proofs can be made non-interactive by deriving the challenge c from the first message of the proof, e.g., by applying a suitable hash function on the message and the sender's id (to avoid proof duplication).

4.1 Building Blocks

p and q are large primes, so that q divides $p-1$. G_q is the the unique multiplicative subgroup of $\mathbb{Z}_p$ with order q. $g, g_1, g_2 \in G_q$.

4.1.1 *Verifiable secret sharing*

In Shamir's secret sharing scheme [29], a secret is shared among n participants as n points $f(i)$ $(1 \leq i \leq n)$ of an arbitrary degree $n-1$ polynomial[3] $f(x)$ with $f(0)=s$. A shared secret (SS) can be retrieved by computing $f(0)$ with Lagrange interpolation.

$$f(0) = \sum_{i=1}^{n} \gamma_i f(i) \quad \text{with} \quad \gamma_i = \prod_{j=1}^{n}\prod_{j\neq i} \frac{j}{j-i} \qquad (\text{Lagrange})$$

$n-1$ points of the polynomial yield absolutely no information about the secret value.

Lagrange interpolation can also be applied when shares are only available as exponentiated values $\hat{f}(i) = g^{f(i)}$ to compute the exponentiated shared secret (eSS) $\hat{f}(0) = g^s$.

$$\hat{f}(0) = \prod_{i=1}^{n} (\hat{f}(i))^{\gamma_i} \qquad (1)$$

The correctness of shares can be proven by using Pedersen's commitment scheme [22]. It provides non-interactive verification of shares and their linear combinations. The dealer who distributes s chooses two polynomials $f(x) = s + F_1 x + F_2 x^2 + \cdots + F_{n-1} x^{n-1}$ and $h(x) = H_0 + H_1 x + \cdots + H_{n-1} x^{n-1}$ and publishes $E_0 = g_1^s g_2^{H_0}$ and $\forall l \in \{1, 2, \ldots, n-1\}: E_l = g_1^{F_l} g_2^{H_l}$. He sends the shares $f(i)$ and $h(i)$ to participant i. Participant i can verify the correctness of the share by testing

$$g_1^{f(i)} g_2^{h(i)} = \prod_{l=0}^{n} (E_l)^{i^l}. \qquad (2)$$

4.1.2 *Proof of equality of two* SSs

Alice is capable of proving the equality of two SSs with the commitment values $E_0' = g_1^{G_0'} g_2^{H_0'}$ and $E_0'' = g_1^{G_0''} g_2^{H_0''}$ by

[2] Unfortunately, there is an error in [5]. A revised protocol specification is available from the author's homepage.

[3] For reasons of simplicity we use $1, 2, \ldots, n$ as n distinct values. As we share information among bidders, we will not make use of the threshold capabilities of this scheme and always use degree $n-1$ polynomials.

sending $t = H_0' - H_0''$ to Bob who then verifies that $\frac{E_0'}{E_0''} = g_2^t$. No information on any of the secrets is revealed [22].

4.1.3 *Verifiable linear combination computation*

There are non-interactive proofs for the correctness of any linear combination of SSs [22].

Two secrets s' and s'' are verifiably distributed. E_l' and E_l'' are the corresponding commitment values. The participants want to compute s's shares with $s = s' + s''$.
Any observer can verify that $(f(i), h(i))$ is a correct share of $s' + s''$ by testing whether $g_1^{f(i)} g_2^{h(i)} = \prod_{l=0}^{n} (E_l' E_l'')^{i^l}$.

When computing $s = as'$ for any $a \in \mathbb{Z}_q^*$, a share $(f(i), h(i))$ is correct when $g_1^{f(i)} g_2^{h(i)} = \prod_{l=0}^{n} ((E_l')^a)^{i^l}$.

A publicly known summand a can simply be added to each f-share $(f(i) = f'(i) + a)$. The share is correct when $g_1^{f(i)} g_2^{h(i)} = \prod_{l=0}^{n} (g_1^a E_l')^{i^l}$.

4.1.4 *Proof of knowledge of a discrete logarithm*

This is a classic, interactive, three-step, zero-knowledge proof by Schnorr [28]. Alice and Bob know v and g, but only Alice knows x, so that $v = g^x$.

1. Alice chooses z at random and sends $a = g^z$ to Bob.
2. Bob chooses a challenge c at random and sends it to Alice.
3. Alice sends $r = (z + cx) \mod q$ to Bob
4. Bob checks that $g^r = av^c$.

4.1.5 *Proof of equality of two discrete logarithms*

When executing the previous protocol in parallel, the equality of two discrete logarithms can be proven [9]. Alice and Bob know v, w, g_1 and g_2, but only Alice knows x, so that $v = g_1^x$ and $w = g_2^x$.

1. Alice chooses z at random and sends $a = g_1^z$ and $b = g_2^z$ to Bob.
2. Bob chooses a challenge c at random and sends it to Alice.
3. Alice sends $r = (z + cx) \mod q$ to Bob
4. Bob checks that $g_1^r = av^c$ and that $g_2^r = bw^c$.

4.1.6 *Proof that a* SS *is one out of two values*

We designed the following protocol according to the results of Cramer et al [10, 11]. Alice proves that a SS x is either z or 0. $x \in \{g_1^z g_2^t, g_2^t\}$.

1. If $x = g_1^z g_2^t$, Alice chooses r_1, d_1, and w at random and sends x, $a_1 = g_2^{r_1} x^{d_1}$, and $a_2 = g_2^w$ to Bob.
   If $x = g_2^t$, Alice chooses r_2, d_2, and w at random and sends x, $a_1 = g_2^w$, and $a_2 = g_2^{r_2} (x g_1^{-z})^{d_2}$ to Bob.
2. Bob chooses a challenge c at random and sends it to Alice.
3. If $x = g_1^z g_2^t$, Alice sends d_1, $d_2 = c - d_1 \mod q$, r_1, and $r_2 = w - d_2 t \mod q$ to Bob.
   If $x = g_2^t$, Alice sends $d_1 = c - d_2 \mod q$, d_2, $r_1 = w - d_1 t \mod q$, and r_2 to Bob.
4. Bob checks that $c = d_1 + d_2 \mod q$, $a_1 = g_2^{r_1} x^{d_1}$, and $a_2 = g_2^{r_2} (x g_1^{-z})^{d_2}$.

4.1.7 *Generation of a random* eSS *that equals* 0

It is possible to jointly create an eSS that equals 0 ($g^s = 1$). The participants choose n random values $\hat{o}(i)$, so that $\prod_{i=1}^{n} \hat{o}(i)^{\gamma_i} = 1$ (see equation 1). Participant i must not know r, so that $g^r = \hat{o}_i$.

1. Each participant i chooses $n - 1$ random values $a_{ij} \in G_q$ ($j \in \{1, 2, \ldots, n-1\}$) and publishes them (simultaneously with all other participants by using preceding commitments).
2. $a_i = \prod_{j=1}^{n} a_{ji}$ ($i \in \{1, 2, \ldots, n-1\}$) and $a_n = \left(\prod_{j=1}^{n-1} a_j \right)^{-1}$ can be publicly computed.
3. $\forall i: \; \hat{o}(i) = (a_i)^{\gamma_i^{-1}}$

4.1.8 *Verifiable random multiplication of an* eSS

In contrast to addition, multiplication of shared secrets is hard and all existing techniques require a threshold secret sharing scheme because the point-wise multiplication of polynomials generally results in a higher degree polynomial. However, for the auction protocol, we only need to multiply a SS with a jointly created random number ($s = s'M$) that is unknown to all participants ($M = \prod_{i=1}^{n} m_i$). This is obtained by raising each exponentiated share $\hat{f}(i) = g^{f(i)}$ to the power of each participant's multiplier factor m_i until $g^{f(i)M}$ is computed. It must be impossible to reveal s' or $g^{s'}$.

In order to enable "ring exponentiation", we need an ordering on bidders. $S(i)$ and $P(i)$ return the successor and predecessor to bidder i, respectively.

$$S(i) = ((i + 1) \mod n) + 1, \quad P(i) = ((i - 1) \mod n) + 1$$

Intermediate values have to be masked. Otherwise, a participant could determine g^M. For this reason, we need the random o_i generation of the previous section. We assume that s' is verifiably shared and that commitment values E_l' have been published.

1. n random values $\hat{o}_i \in G_q$ with $\prod_{i=1}^{n} \hat{o}(i)^{\gamma_i^{-1}} = 1$ are computed using 4.1.7

2. Each participant secretly chooses a random value m_i

3. Participant i publishes $E''_l = (E'_l)^{m_i}$ and proves its correctness by providing a proof for the knowledge of m_i.

4. Participant i publishes $f''(i) = f'(i)m_i$, $h''(i) = h'(i)m_i$ and $\hat{o}'(i) = \hat{o}(i)^{m_i}$ and proves $\hat{o}'(i)$'s correctness using 4.1.5.

5. All participants can verify that $g_1^{f''(i)} g_2^{h''(i)} = \prod_{l=0}^{n} (E''_l)^{i^l}$ (4.1.1).

6. Each participant i computes $a(P(i), i) = \left(g^{f''(P(i))} \hat{o}'(P(i)) \right)^{m_i}$, publishes it and proves its correctness using 4.1.5.

7. For each $h \in 1, 2, \ldots, n$ each bidder i computes and publishes $a(h, i) = a(h, P(i))^{m_i}$ until all $a(i, P(i))$ are computed.

8. $\hat{f}(i) = a(i, P(i))$.

4.2 Informal Description

Like in most other protocols, we define an ordered set of k possible prices (or valuations) $\{p_1, p_2, \ldots, p_k\}$. Each bidder sets the differential bid vector

$$\Delta\vec{b}_i = (\Delta b_{i1}, \Delta b_{i2}, \ldots, \Delta b_{ik}) = (\underbrace{0, \ldots, 0}_{b_i - 1}, y, \underbrace{0, \ldots, 0}_{k - b_i}) \qquad (3)$$

according to his bid $b_i \in \{1, 2, \ldots, k\}$, (verifiably) distributes it on all bidders, and shows its correctness by proving $\forall j : \Delta b_{ij} \in \{0, y\}$ and $\sum_{j=1}^{k} \Delta b_{ij} = y$ in zero-knowledge manner. y is a commonly known number in $\mathbb{Z}_p^*$, e.g., $y = 1$. Each bidder's bid vector $\vec{b}_i$ can be derived by "integrating" $\Delta\vec{b}_i$. This method was first used by Abe and Suzuki in [1].

$$\vec{b}_i = (\underbrace{y, \ldots, y}_{b_i}, \underbrace{0, \ldots, 0}_{k - b_i}) = (\Delta b_{i1} + b_{i2}, \Delta b_{i2} + b_{i3}, \ldots, \Delta b_{ik}) \qquad (4)$$

In our protocol, we also need to "integrate" the differential bid vector "in the other direction" (upwards that is).

$$\vec{b}'_i = (\underbrace{0, \ldots, 0}_{b_i - 1}, \underbrace{y, \ldots, y}_{k - b_i + 1}) = (\Delta b_{i1}, \Delta b_{i2} + b'_{i1}, \ldots, \Delta b_{ik} + b'_{i,k-1}) \qquad (5)$$

And finally, in order to be able to locate the highest price at which $M + 1$ bidders are willing to pay, we have to shift down the components of the bid vectors.

$$\vec{b}_i^{\triangledown} = (b_{i2}, b_{i3}, \ldots, b_{ik}, 0) \qquad (6)$$

If we sum up all bid vectors $\vec{B} = \sum_{i=1}^{n} \vec{b}_i$ and shifted bid vectors $\vec{B}^{\triangledown} = \sum_{i=1}^{n} \vec{b}_i^{\triangledown}$, and subtract $(2M + 1)y\vec{e}$ with $\vec{e} = (1, \ldots, 1)$, we obtain a vector in which the component, that refers to the amount of the $(M + 1)$st highest bid, is 0. All other components are not 0 (with high probability).

By adding the upwards integrated bid vector $\vec{b}'_i$, we mask the resulting vector so that bidder i can only read the selling price if bid he bid more and thus qualifies as a winner of the auction.

$$\vec{v}_i = \vec{B} + \vec{B}^{\triangledown} - (2M + 1)y\vec{e} + (2M + 2)\vec{b}'_i \qquad (7)$$

The components of $\vec{v}_i$ are then multiplied with random multipliers M_{ij} that are jointly created and unknown to any subset of bidders. The invariant of this transformation is the single component that equals 0. As described in 4.1.8, the multiplication works on exponentiated shares and the 0 becomes a 1.

The computation is conducted so that only bidder i and the seller know v_{ij} for each j, because bidder i privately adds the final computational share. If any of these "indicators" is 1, the corresponding bidder is a winner of the auction and he and the seller can read the selling price.

$$v_{ij} = 1 \iff \text{Bidder } i \text{ won and has to pay } p_j \qquad (8)$$

4.3 Detailed Protocol

This is the step-by-step protocol specification for bidder a and his bid b_a. $i, h \in \{1, 2, \ldots, n\}$, $j, b_a \in \{1, 2, \ldots, k\}$, and $l \in \{0, 1, \ldots, n\}$ unless otherwise noted. All calculations are done in the finite field $\mathbb{Z}_p$. g_1 and g_2 are generators in the multiplicative subgroup G_q, so that no participant knows $\log_{g_1} g_2$.

1. Choose random multipliers $\forall i, j : \; m_{aij} \in \mathbb{Z}_q^*$ and $2j$ random polynomials with $\Delta F_{aj0} = \begin{cases} y & \text{if } j = b_a \\ 0 & \text{else} \end{cases}$.

   $$\Delta f_{aj}(x) = \Delta F_{aj0} + \Delta F_{aj1}x + \cdots + \Delta F_{aj,n-1}x^{n-1}$$
   $$\Delta h_{aj}(x) = \Delta H_{aj0} + \Delta H_{aj1}x + \cdots + \Delta H_{aj,n-1}x^{n-1}$$

2. Publish $\forall j, l : \; \Delta E_{ajl} = g_1^{\Delta F_{ajl}} g_2^{\Delta H_{ajl}}$.

3. Prove that $\forall j : \; \Delta E_{aj0} \in \{g_1^y g_2^t, g_2^t\}$ (4.1.6).

4. Compute $\forall i, l : \; E_{ikl} = \Delta E_{ikl}$, $E'_{i1l} = \Delta E_{i1l}$ and $\forall i, j < k, l : \; E_{ijl} = \Delta E_{ijl} E_{i,j+1,l}$, and $\forall i, j > 1, l : E_{ijl} = \Delta E_{ijl} E'_{i,j-1,l}$.

5. Publish $\forall i, j, l :$
   $E^*_{ijl} = \left(\frac{\prod_{h=1}^{n} (E_{hjl} E_{h,j+1,l})(E'_{ijl})^{2M+2}}{g_1^{(2M+1)y}} \right)^{m_{aij}}$
   and prove the discrete logarithm knowledge.

6. Send $\Delta f_{aj}(i)$, and $\Delta h_{aj}(i)$ to bidder i for each $i \neq a$.

7. Verify $\forall i \neq a : \; g_1^{\Delta f_{ij}(a)} g_2^{\Delta h_{ij}(a)} = \prod_{l=0}^{n-1} (E_{ijl})^{a^l}$.

8. Compute $\forall i$: $f_{ik}(a) = \Delta f_{ik}(a)$, $h_{ik}(a) = \Delta h_{ik}(a)$, $f'_{i1}(a) = \Delta f'_{i1}(a)$, $h'_{i1}(a) = \Delta h'_{i1}(a)$, and $\forall i, j < k$: $f_{ij}(a) = \Delta f_{ij}(a) + f_{i,j+1}(a)$, $h_{ij}(a) = \Delta h_{ij}(a) + h_{i,j+1}(a)$, and $\forall i, j > 1$: $f'_{ij}(a) = \Delta f_{ij}(a) + f'_{i,j-1}(a)$, $h'_{ij}(a) = \Delta h_{ij}(a) + h'_{i,j-1}(a)$.

9. Jointly create a function $\hat{o}$, so that $\prod_{i=1}^{n} \hat{o}(i)^{\gamma_i^{-1}} = 1$ according to 4.1.7.

10. Publish $\forall i, j$:

$$v_{ij}(a) = \left(\sum_{h=1}^{n} (f_{hj}(a) + f_{h,j+1}(a)) + \right.$$
$$\left. + (2M+2) f'_{ij}(a) - (2M+1) y \right) m_{aij} \quad ,$$
$$w_{ij}(a) = \left(\sum_{h=1}^{n} (h_{hj}(a) + h_{h,j+1}(a)) + \right.$$
$$\left. + (2M+2) h'_{ij}(a) \right) m_{aij} \quad ,$$

and $\hat{o}'_{ij}(a) = \hat{o}(a)^{m_{aij}}$ and prove the correctness of $\hat{o}'_{ij}(a)$.

11. Verify $\forall i, j, h \neq a$: $g_1^{v_{ij}(h)} g_2^{w_{ij}(h)} = \prod_{l=0}^{n-1} (E^*_{ijl})^{h^l}$.

12. Compute $\forall i, j$: $\hat{v}_{ij}(P(a), a) = \left(g_1^{v_{ij}(P(a))} \hat{o}'_{ij}(a) \right)^{m_{aij}}$, publish it and prove its correctness by showing the equality of the discrete logarithms and the ones used in step 5.

13. Compute and publish $\forall i, j, h$: $\hat{v}_{ij}(h, a) = \left(\hat{v}_{ij}(h, P(a)) \right)^{m_{aij}}$ and prove its correctness by showing the equality of logarithms. Repeat this step until all $\hat{v}_{ij}(h, P(P(h)))$ are computed.

14. Compute $\forall i, j$: $\hat{v}_{ij}(S(a), a) = \left(\hat{v}_{ij}(S(a), P(a)) \right)^{m_{aij}}$ and privately send it and a proof of its correctness to the seller who publishes all $\hat{v}_{ij}(S(h), h)$ and the corresponding proofs of correctness for each $i, j, h \neq i$ after having received all of them.

15. Compute $\forall j$: $v_{aj} = \prod_{i=1}^{n} \left(\hat{v}_{aj}(i, P(i)) \right)^{\gamma_i}$.

16. If $v_{aw} = 1$ for any w, then bidder a is a winner of the auction. p_{w-1} is the selling price.

4.4 Analysis

The final ring exponentiation steps are conducted in a way that allows the seller to see all indicators before the bidders can compute them. This prevents a winning bidder from aborting the protocol after having learned the auction result. If it seems more desirable to prevent the seller from doing so, the final steps can be easily adapted.

When two or more bidders have the $(M+1)$st highest bid in common, the protocol yields no winners. It is impossible for the protocol to decide who of the tieing bidders belongs to the set of winners and who does not. There is no information revelation in this case, except that there has been a tie. The items can be re-auctioned in a subsequent auction. All other ties will be handled smoothly by the protocol.

Rounds	Messages	Bandwidth/Computation
$O(n)$	$O(n)$	$O(n^2k)$

Table 1: Protocol complexity (messages and bandwidth per bidder)

Table 1 shows the number of rounds and messages, and the amount of data that has to be sent by a single bidder. The computation of personalized indicators for each bidder results in a high demand for bandwidth ($O(n^2k)$).
To give an example, in an auction with hundred bidders ($n = 100$) and 200 possible prices ($k = 200$)[4], each bidder has to compute and publish hundreds of megabytes of data when p and q are 1024-bit primes.
The computational demands can be reduced by sharing the bids and the computation among few, distinct bidders which are believed not to collude with each other. Obviously, the resulting protocol does not comply with full privacy anymore. Another possibility is to share the information on m auctioneers like in numerous other protocols. This can drastically reduce the computational amount needed in auctions with many bidders, but the obtained level of privacy is questionable as mentioned in Section 2.
When the selling price does not need to be protected, the computational complexity can be reduced to $O(nk)$ by just computing *one* value for all bidder that indicates the selling price w. Winning bidders can prove their claims to the seller by providing t, so that $E_{i,w+1,0} = g_1^y g_2^t$. However, winning bidders are able to remain silent if they dislike the selling price. Furthermore, the complexity could be decreased to $O(n \log k)$ by using binary search to find the selling price rather than computing values for each price p_j. Apparently, this would increase the number of rounds and require some changes to the protocol.

5. CONCLUSION

We presented a novel kind of secure and private auction protocols, where information is shared among bidders. The protocols comply with the highest standard of privacy possible: they are safe for a single bidder no matter how many of the participants collude.
The main contribution of this paper is the secure and verifiable $(M+1)$st-price auction protocol vMB-SHARE, in which bidders jointly compute personal indicators for each bidder and the seller. Thus, the only agent being able to discover who won the auction besides the concerned bidders is the seller. We are not aware of any auction protocol, that achieves a similar level of privacy.
As the protocol is publicly verifiable, malicious bidders that do not follow the protocol will be detected immediately and can be excluded from the set of bidders.

[4] Usually the number of different prices or valuations is much lower than one would expect, e.g., Lipmaa et al argue that $k \leq 500$ is sufficient for most auctions [20].

The drawback of vMB-share is efficiency. It can take hours, if not days, to decide auctions with very high numbers of bidders. On the other hand, auctions that require such a high standard of privacy typically include few bidders. We are currently implementing the proposed protocol in order to be able to evaluate its feasibility in real-world scenarios. In the future, we intend to apply the presented techniques to solve tractable instances of combinatorial auctions like general multi-unit or linear-good auctions while maintaining full privacy.

6. ACKNOWLEDGEMENTS

The author would like to thank Masayuki Abe for some helpful comments.

7. REFERENCES

[1] M. Abe and K. Suzuki. M+1-st price auction using homomorphic encryption. In *Proceedings of the 5th International Conference on Public Key Cryptography (PKC-02)*, 2002.

[2] O. Baudron and J. Stern. Non-interactive private auctions. In *Pre-Proceedings of the 5th Annual Conference on Financial Cryptography*, pages 300–313, 2001.

[3] M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation. In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing (STOC-88)*, pages 1–10, 1988.

[4] F. Brandt. Cryptographic protocols for secure second-price auctions. In M. Klusch and F. Zambonelli, editors, *Cooperative Information Agents V*, volume 2182 of *Lecture Notes in Artificial Intelligence*, pages 154–165, Berlin et al., 2001. Springer.

[5] F. Brandt. Secure and private auctions without auctioneers. Technical Report FKI-245-02, Institut für Informatik, Technische Universität München, 2002.

[6] F. Brandt and G. Weiß. Antisocial agents and Vickrey auctions. In J.-J. C. Meyer and M. Tambe, editors, *Intelligent Agents VIII*, volume 2333 of *Lecture Notes in Artificial Intelligence*, pages 335–347, Berlin et al., 2001. Springer. Revised papers from the 8th Workshop on Agent Theories, Architectures and Languages.

[7] F. Brandt and G. Weiß. Vicious strategies for Vickrey auctions. In *Proceedings of the 5th International Conference on Autonomous Agents*, pages 71–72. ACM Press, 2001.

[8] C. Cachin. Efficient private bidding and auctions with an oblivious third party. In *Proceedings of the 6th ACM Conference on Computer and Communications Security*, pages 120–127, 1999.

[9] D. Chaum and T. P. Pedersen. Wallet databases with observers. In *Advances in Cryptology - CRYPTO 1992, volume 740 of Lecture Notes in Computer Science*, pages 3.1–3.6. Springer, 1992.

[10] R. Cramer, I. Damgård, and B. Schoenmakers. Proofs of partial knowledge and simplified design of witness hiding protocols. In *Advances in Cryptology - CRYPTO 1994, volume 893 of Lecture Notes in Computer Science*, pages 174–187. Springer, 1994.

[11] R. Cramer, R. Gennaro, and B. Schoenmakers. A secure and optimally efficient multi-authority election scheme. In *Advances in cryptology - EUROCRYPT 1997, volume 1233 of Lecture Notes in Computer Science*, pages 103–118. Springer, 1997.

[12] M. Franklin, Z. Galil, and M. Yung. An overview of secure distributed computing. Technical Report TR CUCS-008-92, Columbia University, 1992.

[13] M. Franklin and M. Reiter. The design and implementation of a secure auction service. *IEEE Trans. on Software Engineering*, 22(5):302–312, 1996.

[14] M. Harkavy, J. Tygar, and H. Kikuchi. Electronic auctions with private bids. In *Proceedings of the 3rd USENIX Workshop on Electronic Commerce*, pages 61–74, 1998.

[15] M. Jakobsson and A. Juels. Mix and match: Secure function evaluation via ciphertexts. In *Proceedings of Asiacrypt-00*, pages 162–177, 2000.

[16] H. Kikuchi. (M+1)st-price auction protocol. In *Proceedings of Financial Cryptography (FC 2001)*, 2001.

[17] H. Kikuchi, M. Harkavy, and J. Tygar. Multi-round anonymous auction protocols. In *Proceedings of the First IEEE Workshop on Dependable and Real-Time E-Commerce Systems*, pages 62–69, 1998.

[18] H. Kikuchi, S. Hotta, K. Abe, and S. Nakanishi. Resolving winner and winning bid without revealing privacy of bids. In *Proceedings of the International Workshop on Next Generation Internet (NGITA)*, pages 307–312, 2000.

[19] M. Kudo. Secure electronic sealed-bid auction protocol with public key cryptography. *IEICE Trans. Fundamentals*, E81-A(1), 1998.

[20] H. Lipmaa, N. Asokan, and V. Niemi. Secure Vickrey auctions without threshold trust. In *Proceedings of the 6th Annual Conference on Financial Cryptography*, 2002. to appear.

[21] M. Naor, B. Pinkas, and R. Sumner. Privacy preserving auctions and mechanism design. In *ACM Conference on Electronic Commerce*, pages 129–139, 1999.

[22] T. Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. In J. Feigenbaum, editor, *Advances in Cryptology - CRYPTO 1991, volume 576 of Lecture Notes in Computer Science*, pages 129–140. Springer, 1991.

[23] M. Rothkopf and R. Harstad. Two models of bid-taker cheating in Vickrey auctions. *Journal of Business*, 68(2):257–267, 1995.

[24] M. Rothkopf, T. Teisberg, and E. Kahn. Why are Vickrey auctions rare? *Journal of Political Economy*, 98(1):94–109, 1990.

[25] K. Sakurai and 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*, pages 180–187, 1999.

[26] K. Sakurai and S. Miyazaki. An anonymous electronic bidding protocol based on a new convertible group signature scheme. In *Proc. ACISP2000. Fifth Australasian Conference on Information Security and Privacy*, Lecture Notes in Computer Science, 2000.

[27] T. Sandholm. Limitations of the Vickrey auction in computational multiagent systems. In *Proceedings of the 2nd International Conference on Multiagent Systems (ICMAS-96)*, pages 299–306, Menlo Park, CA, 1996. AAAI Press.

[28] C. P. Schnorr. Efficient signature generation by smart cards. *Journal of Cryptology*, 4(3):161–174, 1991.

[29] A. Shamir. How to share a secret. *Communications of the ACM*, 22:612–613, 1979.

[30] D. Song and J. Millen. Secure auctions in a publish/subscribe system. Available at http://www.csl.sri.com/users/millen/, 2000.

[31] S. Stubblebine and P. Syverson. Fair on-line auctions without special trusted parties. In *Proceedings of Financial Cryptography (FC 1999)*, volume 1648 of *Lecture Notes in Computer Science*, pages 230–240, 1999.

[32] W. Vickrey. Counter speculation, auctions, and competitive sealed tenders. *Journal of Finance*, 16(1):8–37, 1961.

[33] K. Viswanathan, C. Boyd, and E. Dawson. A three phased schema for sealed bid auction system design. In *Australasian Conference for Information Security and Privacy (ACISP 2000)*, Lecture Notes in Computer Science, pages 412–426, 2000.

[34] Y. Watanabe and 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*, pages 80–86. ACM Press, 2000.

[35] P. Wurman, W. Walsh, and M. Wellman. Flexible double auctions for electronic commerce: Theory and implementation. *Decision Support Systems*, 24:17–27, 1998.

[36] A. Yao. How to generate and exchange secrets. In *Proceedings of the 27th Symposium on Foundations of Computer Science*, pages 162–167. IEEE Computer Society Press, 1986.

[37] M. Yokoo and 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 Multi-Agent Systems*, pages 112–119. ACM Press, 2002.