Non-interactive Auction Scheme with Strong Privacy

Kun Peng, Colin Boyd, Ed Dawson and Kapali Viswanathan
Information Security Research Centre
Faculty of Information Technology
Queensland University of Technology,
2, George Street, Brisbane, QLD4001, Australia
Email: k.peng,c.boyd,e.dawson,k.viswanathan@qut.edu.au

Abstract. Key chain, as an effective tool to achieve strong bid privacy non-interactively, was employed by Watanabe and Imai in an auction scheme. But in their scheme [13] bid privacy cannot be achieved unconditionally and losing bidders must trust bidders with higher bids for privacy of their bids. Moreover, their scheme is not efficient. In this paper the key chain in [13] is optimised to achieve unconditional bid privacy. In the new scheme, every losing bidder can control privacy of their own bids while no trust is needed. Computational cost of this scheme is optimised to avoid the costly verifiable encryption technique in [13] by applying homomorphic encryption.

1 Introduction

Sealed-bid auction is an ideal method to distribute merchandise. In sealed-bid auctions each bidder seals his bid (by encryption or hash function) and submits it before a set time. After that time the bids are opened and the winning price and winner are determined according to a pre-defined auction rule. Compared to other types of auction, such as open-cry auction, sealed-bid auction is more suitable in network environment. Therefore sealed-bid auction has been attracting most attention in the research of e-auction. In many auction applications it is desired to keep the losing bids private even at the end of the auction. This requirement is called bid privacy and is discussed in many papers.

Watanabe and Imai presented a non-interactive sealed-bid auction scheme [13], which provides privacy for the losing bids. The essential idea in this scheme is a technique called key chain. The advantage of that scheme is bid privacy is obtained non-interactively (the bidders need not participate in opening the bids after they submit their bids). The authors claimed that they provided satisfactory bid privacy ("... prevent even an auctioneer from getting any useful information of bids of losers ...").

However the bid privacy in this scheme is achieved based on strong trust (either a fraction of bidders, the auctioneer or a third party must be trusted). In other word, a losing bid can be revealed by a cooperation of the auctioneer and all the bidders with higher bids. This kind of bid privacy is actually not strong or satisfactory. Moreover this scheme is not efficient in computation.

In this paper a new scheme is presented. The idea of key chain is inherited, but the key chain is constructed in a different way, so that bid privacy for a losing bidder is achieved without any trust on other parties. Namely, without the cooperation of a losing bidder his bid is private. Additionally, the new scheme is simpler as the third party T

and the auctioneer A are removed. As a result, communication in the proposed scheme is more efficient than in [13]. Moreover, optional techniques to improve computation efficiency are also introduced in the new scheme.

1.1 Desired Properties in Sealed-bid Auction

There are several properties that are usually desired in e-auction schemes [**?**,**?**,12]. Their definitions are as follows.

1. **Correctness**: If every party acts honestly, the correct winning price and winner(s) are determined according to the auction rules.
2. **Soundness**: If an auction result is declared, it is a correct result even though there are some dishonest parties.
3. **Fairness**: No bidder can take advantage over other bidders. It includes:
   - No bidder knows anything about other bidders' bids before he submits his own bid.
   - After a bidder submits his bid, the bid cannot be modified.
   - No bidder can deny his bid after he submits it. This is sometimes called non-repudiation of bids.
4. **Bid Privacy**: The losing bids remain confidential until the end of the auction even to the auctioneers.
5. **Public verifiability**: The validity of the result of the auction is publicly verifiable by anyone.
6. **High Efficiency**: Computation and communication must be efficienct enough for applications.

1.2 Symbols and Outline

G is a cyclic group with a generator g. There are n bidders B_1, B_2, ..., B_n and w biddable prices p_1, p_2, ..., p_w from highest to lowest. $E_a(b)$ denotes encryption of b by a public key a. $D_a(b)$ denotes decryption of b by a private key a. $Sig_a(b)$ denotes a's signature on b. $VE_a(b)$ is verifiable encryption of b by a's key.

In section 2, related auction schemes are introduced. In section 3, the scheme by Watanabe and Imai is reviewed and analysed. In section 4, our new scheme is presented. In section 5, the security of our scheme is analysed. In section 6, efficiency improvement for our scheme is discussed.

2 Related Work

Bid privacy is a frequently desired property in auction schemes. It refers to the confidentiality of losing bids to anybody even after the auction ends. In current auction schemes, two methods are often applied to implement bid privacy.

The first method is to trust some parties to conceal the losing bids. To strengthen bid privacy, the trust is often shared among a few auctioneers, so that bid privacy can be achieved if the number of honest parties is over a threshold. This mechanism is usually

realized by sharing the capability of bid-opening among several auctioneers and requiring the cooperation of a portion of them to open the bids. Several published schemes are in this category [4, 6, 3, 5, 1, 8]. [4, 6] employ standard threshold secret sharing technique. [3] employs a special $2-2$ secret sharing. [5] also employs threshold secret sharing, but uses the degree of polynomials to stand for a bid. [1, 8] employ distributed decryption technique. [1] employs standard threshold distributed decryption. [8] employs only two auctioneers and is in fact 2-2 distributed decryption if bid decryption is defined as interpreting the meaning of bids in auction schemes. The disadvantage of this method is that the bid privacy obtained is not strong enough.

In some applications stronger bid privacy is required. The strongest is unconditional bid privacy—without the cooperation of a losing bidder, his bid is confidential. A mechanism called Dutch style bid opening can be employed to achieve unconditional bid privacy. In this mechanism the bids are opened downwards from the highest biddable price, which is quite like the strategy in Dutch auction. After the winning bid is found in a downward search, cooperation from the bidders is not available, so any losing bidder's bid is kept private without trust on anybody else. Therefore, very strong absolute privacy is achieved. The disadvantage of this method is low efficiency. The scheme is interactive and inefficient in computation. Classic schemes in this category include [11], [10] and [12].

A scheme by Watanabe and Imai [13] was claimed to achieve strong bid privacy non-interactively. A cryptographic tool, key chain, is employed in this scheme. The bids are opened in a downward direction from the highest biddable price until the winning bid is found. Bid opening is non-interactive, which is an advantage over [11], [10] and [12]. However, bid privacy in [13] is not very strong.

3 Auction Scheme Based on Key Chain

3.1 Key chain

In [13] only a finite set of prices are biddable and a key chain is constructed for these prices. The principle of key chain is as follows.

1. At each price all the bids are encrypted by the same public key, which is generated by all the bidders.
2. The corresponding decrypting key is shared among the bidders. Only when all the bidders put their shares together at a price, the bids at that price can be opened.
3. If a bidder is not willing to pay a price, at that price his bidding value contains his share of the decryption key needed to open the bids at the next lower price. So if none of the bidders are willing to pay a price, the decryption key to open the bids at the next lower price can be constructed from their opened bids at the price.
4. If a bidder is willing to pay a price, his share of the decryption key needed to open the bids at the next lower price is not contained in the bid for the current price. In this case the key chain is broken and the decryption key to open the bids at the next lower price cannot be constructed, thus the confidentiality of the losing bids is protected.

3.2 The Scheme by Watanabe and Imai

There is an active auctioneer in the scheme by Watanabe and Imai. The auctioneer is responsible for constructing the public keys in the chain. To weaken the trust on the bidders, a share for each decryption key is provided by the auctioneer. Moreover, verifiable encryption is employed so that an off-line third party can interfere if a bidder is dishonest when constructing the key chain (correct shares for next decryption key is not in one of his bids). In this case the third party can recover the concealed correct share to help construct the next decryption key. Their protocol is as follows.

1. Registration phase
   - Bidder B_i chooses his secret share $x_{i,j}$ for price p_j. The corresponding public key share is $y_{i,j} = g^{x_{i,j}}$. Additionally $x_{i,j}$ is encrypted as $\beta_{i,j} = VE_T(x_{i,j})$ by a third party T's public key. Watanabe and Imai adopted Naccache-Stern encryption algorithm [7]. $\beta_{i,j}$ is recoverable by T and can be verified as a correct encryption of the secret committed in $y_{i,j}$ by zero knowledge proof of equality of logarithms [2]. B_i signs, and sends $y_{i,j}$ and $\beta_{i,j}$ for $j = 1, 2, \ldots, w$ to auctioneer A.
   - A verifies B_i's signature on $y_{i,j}$ and $\beta_{i,j}$ for $j = 1, 2, \ldots, w$ and the correctness of encryption. If the verification is successful, A sends a certificate $cert_i = (z_{i,1}, z_{i,2}, \ldots, z_{i,j})$ to B_i where $z_{i,j} = Sig_A(B_i, y_{i,j})$. Then A chooses his own secret shares x_{Aj} and generates the public keys in the chain $Y_j = g^{x_{Aj}} \prod_{i=1}^{n} y_{i,j}$ for $j = 1, 2, \ldots, w$. Finally A publishes Y_j for $j = 1, 2, \ldots, w$ and the registration information of the bidders. Key generation is illustrated in Table 1 for the case $n = 3$ and $w = 6$.
2. Bidding phase
   - B_i publishes his bid $V_{i,j} = E_{Y_j}(I_{i,j}, y_{i,j}, z_{i,j})$ for $j = 1, 2, \ldots, w$. If he is not willing to pay p_j, $I_{i,j} = (No, x_{i,j-1})$. If he is willing to pay p_j, $I_{i,j} = (Yes, proof(x_{i,j-1}))$ where $proof(x_{i,j-1})$ is a transcript for zero knowledge proof of knowledge of $x_{i,j-1}$. $I_{i,j}$ can be checked against $y_{i,j}$ and $z_{i,j}$ to show that B_i provides a valid $x_{i,j-1}$ (in a "Yes" bid) or knows its value (in a "No" bid). Bid format is illustrated in Table 2 (supposing there are 3 bidders and 5 biddable prices).
3. Opening phase
   - B_i publishes $x_{i,1}$, $y_{i,1}$ and $z_{i,1}$.
   - A calculates and publishes $X_1 = x_{A1} + \sum_{i=1}^{n} x_{i,1}$, the decryption key for the bids at p_1.
   - If no "Yes" bid is found at this price, decryption key for p_2 can be constructed and opening continues. Similarly the opening can go on along the key chain until a "yes" bid is found as winning bid and the key chain is broken.

3.3 Problems in the Scheme by Watanabe and Imai

Among the desired properties introduced in 1.1, bid privacy and high efficiency cannot be achieved satisfactorily.

	A	B_1	B_2	B_3	encryption key
evaluation		p_2	p_3	p_5	
p_1	$g^{x_{A1}}$	$y_{1,1} = g^{x_{1,1}}$	$y_{2,1} = g^{x_{2,1}}$	$y_{3,1} = g^{x_{3,1}}$	$Y_1 = g^{x_{A1}} \times y_{1,1} \times y_{2,1} \times y_{3,1}$
p_2	$g^{x_{A2}}$	$y_{1,2} = g^{x_{1,2}}$	$y_{2,2} = g^{x_{2,2}}$	$y_{3,2} = g^{x_{3,2}}$	$Y_2 = g^{x_{A2}} \times y_{1,2} \times y_{2,2} \times y_{3,2}$
p_3	$g^{x_{A3}}$	$y_{1,3} = g^{x_{1,3}}$	$y_{2,3} = g^{x_{2,3}}$	$y_{3,3} = g^{x_{3,3}}$	$Y_3 = g^{x_{A3}} \times y_{1,3} \times y_{2,3} \times y_{3,3}$
p_4	$g^{x_{A4}}$	$y_{1,4} = g^{x_{1,4}}$	$y_{2,4} = g^{x_{2,4}}$	$y_{3,4} = g^{x_{3,4}}$	$Y_4 = g^{x_{A4}} \times y_{1,4} \times y_{2,4} \times y_{3,4}$
p_5	$g^{x_{A5}}$	$y_{1,5} = g^{x_{1,5}}$	$y_{2,5} = g^{x_{2,5}}$	$y_{3,5} = g^{x_{3,5}}$	$Y_5 = g^{x_{A5}} \times y_{1,5} \times y_{2,5} \times y_{3,5}$
p_6	$g^{x_{A6}}$	$y_{1,6} = g^{x_{1,6}}$	$y_{2,6} = g^{x_{2,6}}$	$y_{3,6} = g^{x_{3,6}}$	$Y_6 = g^{x_{A6}} \times y_{1,6} \times y_{2,6} \times y_{3,6}$

Table 1. Key generation in the scheme by Watanabe and Imai

	B_1	B_2	B_3	A constructing decryption key
evaluation	p_2	p_3	p_5	
p_1	$E_{y_1}(x_{1,2})$	$E_{y_1}(x_{2,2})$	$E_{y_1}(x_{3,2})$	$X_1 = x_{A1} + x_{1,1} + x_{2,1} + x_{3,1}$
p_2	$\mathbf{E_{y_2}(proof(x_{1,3}))}$	$E_{y_2}(x_{2,3})$	$E_{y_2}(x_{3,3})$	$X_2 = x_{A2} + x_{1,2} + x_{2,2} + x_{3,2}$
p_3	$E_{y_3}(x_{1,4})$	$\mathbf{E_{y_3}(proof(x_{2,4}))}$	$E_{y_3}(x_{3,4})$	$\mathbf{B_1}$ and A must collude to recover $\mathbf{X_3}$
p_4	$E_{y_4}(x_{1,5})$	$E_{y_4}(x_{2,5})$	$E_{y_4}(x_{3,5})$	$\mathbf{B_1, B_2}$ and A must collude to recover $\mathbf{X_4}$
p_5	$E_{y_5}(x_{1,6})$	$E_{y_5}(x_{2,6})$	$\mathbf{E_{y_5}(proof(x_{3,6}))}$	$\mathbf{B_1, B_2}$ and A must collude to recover $\mathbf{X_5}$
p_6	$E_{y_6}(x_{1,1})$	$E_{y_6}(x_{2,1})$	$E_{y_6}(x_{3,1})$	$\mathbf{B_1, B_2, B_3}$ and A must collude to recover $\mathbf{X_6}$

Table 2. Bids in the scheme by Watanabe and Imai

Since A provides a share for each decryption key the trust for bid privacy is shared among not only the bidders but also A. Namely the trust needed for the privacy of the $i+1^{th}$ highest bid is shared among the bidders submitting the highest i bids and A. As a result, weaker trust is required, however bid privacy is still conditional and the scheme is still unfair for bidders with lower bids.

Because verifiable encryption enables T to recover a secret share once he gets its encrypted value, registration information from bidders must be transmitted through a confidential channel (this was not stated by Watanabe and Imai). Even though the registration information is encrypted, collusion of A and T still can reveal all decryption keys and thus all losing bids. That means bid privacy is based on the following two assumptions

1. A and the winner do not conspire,
2. A and T do not conspire.

These are still strong assumptions and require strong trust.

Inefficiency is also a problem. The number of opening rounds is linear in the number of biddable prices and the computational cost of each round is linear in the number of bidders. Therefore $O(nw)$ exponentiations are needed in opening phase where n is the number of bidders and w is the number of biddable prices. Moreover because an active auctioneer is involved in key chain construction and verifiable encryption is employed, computation and communication in registration phase are also costly.

Another issue affecting efficiency is bid padding. Every bidder's highest positive bid (transcript of a non-interactive zero-knowledge proof of knowledge) in a different format from other bids (encryption of an integer less than the order of G, which is in G when ElGamal encryption algorithm is employed). As the highest positive bids are much longer, other bids must be padded to the same length to make the encrypted bids indistinguishable from one another, although padding was not mentioned in the paper by Watanabe and Imai. This increases the communication burden of the scheme.

4 New Scheme

We want unconditional bid privacy, namely no trust is needed on any other party for the confidentiality of a losing bidder's bid. In the new scheme when there is a winning bid, the key chain is broken completely. One solution is to construct the key chain according to a rule: if a bidder has a positive bid at a price, he does not have a share of the decryption key for the next lower price. His share is actually shared again among all the bidders. So the public keys are generated in a special way so that the share for the decryption key at the winning price to the winner can only be extracted by a cooperation of all the bidders. Therefore any decryption key at a price lower than the winning price cannot be reconstructed without cooperation of all bidders. The modified key chain is illustrated in Figure 1 in an example where the fourth highest bid is the winning bid.

To obtain a simpler and more effective and efficient scheme, no active auctioneer is employed and no registration phase is needed in our scheme. Nor does it need a third party or verifiable encryption. Bidders performing malicious behaviour (e.g. failing to reveal correct share in a "No" bid) can be publicly identified. Our scheme includes four phases: initial phase, pre-bidding phase, bidding phase and opening phase.

Fig. 1. Modified key chain

	B_1	B_2	B_3	encryption key
evaluation	p_2	p_3	p_5	
p_1	$y_{1,1} = g^{x_{1,1}}$	$y_{2,1} = g^{x_{2,1}}$	$y_{3,1} = g^{x_{3,1}}$	$Y_1 = y_{1,1} \times y_{2,1} \times y_{3,1}$
p_2	$y_{1,2} = g^{x_{1,2}}$	$y_{2,2} = g^{x_{2,2}}$	$y_{3,2} = g^{x_{3,2}}$	$Y_2 = y_{1,2} \times y_{2,2} \times y_{3,2}$
p_3	$\mathbf{y_{1,3} = g^{r_1} y_2 y_3}$	$y_{2,3} = g^{x_{2,3}}$	$y_{3,3} = g^{x_{3,3}}$	$Y_3 = y_{1,3} \times y_{2,3} \times y_{3,3}$
p_4	any $y_{1,4}$ in G	$\mathbf{y_{2,4} = g^{r_2} y_1 y_3}$	$y_{3,4} = g^{x_{3,4}}$	$Y_4 = y_{1,4} \times y_{2,4} \times y_{3,4}$
p_5	any $y_{1,5}$ in G	any $y_{2,5}$ in G	$y_{3,5} = g^{x_{3,5}}$	$Y_5 = y_{1,5} \times y_{2,5} \times y_{3,5}$
p_6	any $y_{1,6}$ in G	any $y_{2,6}$ in G	$\mathbf{y_{3,6} = g^{r_3} y_1 y_2}$	$Y_6 = y_{1,6} \times y_{2,6} \times y_{3,6}$

Table 3. Key generation in our scheme

1. Initial phase:
   Each bidder B_i chooses a secret x_i and publishes $Com1_i = (B_i,\ y_i,\ Sig_{B_i}(B_i, y_i))$ where $y_i = g^{x_i}$ for $i = 1, 2, \ldots, n$ on a bulletin board.
2. Pre-bidding phase:
   Every bidder publishes a public key for every biddable price. If a bidder B_i is not willing to pay p_j, his public key for p_{j+1} is $y_{i,j+1} = g^{x_{i,j+1}}$ where the corresponding secret key $x_{i,j+1}$ is kept as a secret. If bidder B_i's bidding price is p_j, his public key for p_{j+1} is $y_{i,j+1} = g^{r_i} \prod_{k=1,k\neq i}^{n} y_k$ where r_i is kept as a secret and he chooses public keys $y_{i,j+2}$, $y_{i,j+3}$, ..., $y_{i,n}$ randomly for p_{j+2}, p_{j+3}, ..., p_n.
   B_i publishes $Com2_i = (B_i,\ y_{i,1}, y_{i,2}, \ldots, y_{i,w},\ Sig_{B_i}(B_i,\ y_{i,1}, y_{i,2}, \ldots, y_{i,w}))$ on the bulletin board. Key generation is illustrated in Table 3 (supposing there are 3 bidders and 6 biddable prices). The public key for price p_j is $Y_j = \prod_{k=1}^{n} y_{k,j}$ and can be calculated by anybody using the public values available on the bulletin board.
3. Bidding phase:
   Every bidder submits a bid for each biddable price. If a bidder B_i is not willing to pay p_j, his bid at p_j is $V_{i,j} = E_{Y_j}(x_{i,j+1})$. If B_i is willing to pay p_j, $V_{i,j} = E_{Y_j}(r_i)$. At price p_j lower than his evaluation, $V_{i,j}$ is randomly chosen. B_i publishes
   $V_i = (B_i,\ V_{i,1}, V_{i,2}, \ldots, V_{i,w},\ Sig_{B_i}(B_i,\ V_{i,1}, V_{i,2}, \ldots, V_{i,w}))$ on the bulletin board. Bid format is illustrated in Table 4 (supposing there are 3 bidders and 6 biddable prices).
4. Opening phase:
   The bidders publish $Com3_i = (x_{i,1},\ Sig_{B_i}(x_{i,1}))$ for $i = 1, 2, \ldots, n$. Anybody can verify the validity of the shares against $y_{i,1}$ for $i = 1, 2, \ldots, n$, construct the decryption key for the first price $X_1 = \sum_{k=1}^{n} x_{k,1}$ and decrypt all the bids at p_1. The meaning of B_i's decrypted bid $v_{i,1}$ can be determined by testing whether $y_{i,2} = g^{v_{i,1}}$ ($v_{i,1}$ is negative bid) or $y_{i,2} = g^{v_{i,1}} \prod_{k=1,k\neq i}^{n} y_k$ ($v_{i,1}$ is positive bid). If there is no bid showing willingness to pay at p_1, all the shares $x_{i,2} = v_{i,1}$ for

$i = 1, 2, \ldots, n$ are obtained and $X_2 = \sum_{k=1}^{n} x_{k,2}$ can be recovered. Then all the bids at p_2 are opened. The opening continues until $y_{i,j+1} \neq g^{v_{i,j}}$ is met and the key chain breaks at p_{j+1}. If $y_{i,j+1} = g^{v_{i,j}} \prod_{k=1}^{n} y_k$, p_j and B_i are declared as winning price and winner. Otherwise B_i is identified as a cheater.

	B_1	B_2	B_3	construction of decryption key
evaluation	p_2	p_3	p_5	
p_1	$E_{Y_1}(x_{1,2})$	$E_{Y_1}(x_{2,2})$	$E_{Y_1}(x_{3,2})$	$X_1 = x_{1,1} + x_{2,1} + x_{3,1}$
p_2	$\mathbf{E_{Y_2}(r_1)}$	$E_{Y_2}(x_{2,3})$	$E_{Y_2}(x_{3,3})$	$X_2 = x_{1,2} + x_{2,2} + x_{3,2}$
p_3	any bid in correct format	$\mathbf{E_{Y_3}(r_2)}$	$E_{Y_3}(x_{3,4})$	**$\mathbf{B_2}$ and $\mathbf{B_3}$ must collude to recover $\mathbf{X_3}$**
p_4	any bid in correct format	any bid in correct format	$E_{Y_4}(x_{3,5})$	**all the bidders must collude to recover $\mathbf{X_4}$**
p_5	any bid in correct format	any bid in correct format	$\mathbf{E_{Y_5}(r_3)}$	**all the bidders must collude to recover $\mathbf{X_5}$**
p_6	random bid in correct format	random bid in correct format	random bid in correct format	**all the bidders must collude to recover $\mathbf{X_6}$**

Table 4. Bids in our scheme

Figure 2 illustrates the auction procedure.

5 Analysis

The new auction scheme is analysed in this section in relation to the properties from section 1.1. It will be shown that the scheme is correct, sound, fair, publicly verifiable and achieves unconditional privacy for losing bids.

1. **Correctness**:
   An honest bidder B_i publishes $x_{i,1} = log_g y_{i,1}$. So $X_1 = \sum_{k=1}^{n} x_{k,1} = log_g Y_1$ can be reconstructed. Therefore the key chain starts correctly and the bids at p_1 can be opened. An honest bidder B_i's bids at all the biddable prices are as follows
   (a) At a price p_j no lower than his evaluation, his bid is $x_{i,j+1}$ satisfying $y_{i,j+1} = g^{x_{i,j+1}}$.
   (b) At a price p_j equal to his evaluation, his bid is r_i satisfying $y_{i,j+1} = g^{r_i} \prod_{k=1,k\neq i}^{n} y_k$.
   (c) At a price p_j lower than his evaluation, his bid is a random value.
   If at a price p_j higher than any bidder's evaluation bids are opened, the decrypted bids are $v_{i,j} = x_{i,j+1} = log_g y_{i,j+1}$ for $i = 1, 2 \ldots, n$, thus $X_{j+1} = \sum_{k=1}^{n} x_{k,j+1} = log_g Y_{j+1}$ can be reconstructed. So the key chain extends correctly one step downwards and the bids at p_{j+1} can be opened. Namely as far as all the opened bids are as expressed in (a) above, the key chain can extend on. Therefore if no bidder

Procedure of Auction

Initial Phase

1. $B_i \xrightarrow{Com1_i = (B_i,\ y_i,\ Sig_{B_i}(B_i, y_i))} BB^*$

   $y_i = g^{x_i}$

Pre-bidding Phase

2. $B_i \xrightarrow{Com2_i = (B_i,\ y_{i,1}, y_{i,2}, \ldots, y_{i,w},\ Sig_{B_i}(B_i,\ y_{i,1}, y_{i,2}, \ldots, y_{i,w}))} BB$

   negative bid: $y_{i,j+1} = g^{x_{i,j+1}}$

   positive bid: $y_{i,j+1} = g^{r_i} \prod_{k=1,k\neq i}^{n} y_k$

Bidding Phase

3. $B_i \xrightarrow{V_i = (B_i,\ V_{i,1}, V_{i,2}, \ldots, V_{i,w},\ Sig_{B_i}(B_i,\ V_{i,1}, V_{i,2}, \ldots, V_{i,w}))} BB$

   negative bid: $V_{i,j} = E_{Y_j}(x_{i,j+1})$

   positive bid: $V_{i,j} = E_{Y_j}(r_i)$

Opening Phase

4. $B_i \xrightarrow{Com3_i = (x_{i,1},\ Sig_{B_i}(x_{i,1}))} BB$

At price p_j, construct $X_j = \sum_{i=1}^{n} x_{i,j}$

Decryption: $v_{i,j} = D_{X_j}(V_{i,j})$

If $g^{v_{i,j}} = y_{i,j+1}$, $V_{i,j}$ is a negative bid

If $g^{v_{i,j}} = y_{i,j+1}/(\prod_{k=1,k\neq i}^{n} y_k)$, $V_{i,j}$ is a positive bid and opening stops.

If $v_{i,j} = x_{i,j+1}$ for $i = 1, 2, \ldots, n$ are recovered,

$X_{j+1} = \sum_{i=1}^{n} v_{i,j}$ is constructed and opening continues.

* BB: bulletin board

Fig. 2 optimistic auction procedure

has an evaluation no lower than the lowest biddable price, the key chain extends ultimately to p_w and the item on sale is not sold. Otherwise $v_{i,j} = r_i$ satisfying $y_{i,j+1} = g^{r_i} \prod_{k=1,k\neq i}^{n} y_k$ must be met for some i and j. In this case p_j is the winning price and B_i is the winner.

2. **Soundness**:
   As the number of biddable prices is finite, extension of the key chain must stop somewhere.
   (a) If the key chain extends to p_w and no winner is found, $y_{i,j+1} = g^{D x_j(V_{i,j})}$ for $i = 1, 2, \ldots, n$ and $j = 1, 2, \ldots, w-1$. Since $y_{i,j+1}$ and $V_{i,j}$ for $i = 1, 2, \ldots, n$ and $j = 1, 2, \ldots, w-1$ are signed by B_i, they are generated by B_i if the signature algorithm is secure. So no bidder submits a positive bid no lower than the lowest biddable price.
   (b) If p_u and B_v are declared as winning price and winner, $y_{i,j+1} = g^{D x_j(V_{i,j})}$ for $i = 1, 2, \ldots, n$, $j = 1, 2, \ldots, u-1$ and $i = 1, 2, \ldots, v-1, v+1, v+2 \ldots, n$, $j = u$. Since $y_{i,j+1}$ and $V_{i,j}$ for $i = 1, 2, \ldots, n$ and $j = 1, 2, \ldots, u$ are signed by B_i, they are generated by B_i if the signature algorithm is secure. So p_u and B_v are winning price and winner.
   (c) If B_i is declared as a cheater, the key chain must be broken at a price p_u and $y_{i,j+1} = g^{D x_j(V_{i,j})}$ for $j = 1, 2, \ldots, u-2$ and $y_{i,u} \neq g^{D x_{u-1}(V_{i,u-1})}$ and $y_{i,u} \neq g^{D x_{u-1}(V_{i,u-1})} \prod_{k=1,k\neq i}^{n} y_k$. Since $y_{i,j+1}$ and $V_{i,j}$ for $j = 1, 2, \ldots, u-1$ are signed by B_i, they are generated by B_i if the signature algorithm is secure. So B_i is a cheater.

3. **Fairness**:
   – First it is illustrated that before the opening phase, no bids are revealed. Before the opening phase only every bidder's public keys and bids for each price are published. The public keys are generated in two methods. In the first method a bidder B_i chooses a secret key $x_{i,j}$ randomly for p_l and the public key is $y_{i,j} = g^{x_{i,j}}$. Since $x_{i,j}$ is chosen from $1, 2, 3, \ldots, ord(G)$ randomly, $y_{i,j}$ has a identical distribution over G. In the second B_i chooses a random value r_i for p_l and the public key is $y_{i,j} = g^{r_i} \prod_{k=1,k\neq i}^{n} y_k$. Since r_i is chosen from $1, 2, 3, \ldots, ord(G)$ randomly, $y_{i,j}$ has a identical distribution over G too. In both cases all the public keys are in identical distribution over G, so no information about any bidder's bids is revealed from the public keys. All the submitted bids are encryptions of a random integer less than $ord(G)$, thus have an uniform distribution in the ciphertext space (G in the case of ElGamal encryption) if a semanticly secure encryption algorithm (e.g. ElGamal or Paillier's [9]) is employed . So no information about the bids is revealed from the encrypted bids although no padding operation is employed. Therefore before the opening phase all bids are confidential on the assumption that the encryption algorithm is semantically secure[1]. The only method to open any bid is to construct the key chain, which requires the cooperation of all bidders and does not happen until the opening phase.

[1] An encryption algorithm is said to be semantically secure if given that c_k is the encryption of message m_0 or m_1, it is computationally difficult to determine which is the correct message coresponding to c_k.

– No bidder can change or deny his bid after bidding phase. A bidder B_i's bidding value at a price p_j is determined by whether $y_{i,j+1} = g^{D_{X_j}(V_{i,j})}$ or $y_{i,j+1} = g^{D_{X_j}(V_{i,j})} \prod_{k=1,k\neq i}^{n} y_k$. Since $y_{i,j+1}$ and $V_{i,j}$ are published in pre-bidding phase and bidding phase respectively, they cannot be changed. So bidding values cannot be changed. $y_{i,j+1}$ and $V_{i,j}$ are signed by B_i, so B_i cannot deny his bids.

4. **Public Verifiability**
   All the information necessary to decide the auction result is published on the bulletin board, so anybody can verify the auction result using the contents of the bulletin board.
5. **Bid privacy**:
   The bidders with higher bids (e.g. the winner) cannot take advantage over other bidders even after the auction result turns out, because to open any losing bid the cooperation of all the losing bidders is necessary. When B_v is the winner and p_u is the winning price, B_v's bid at p_u is opened to be r_v satisfying $y_{v,u+1} = g^{r_v}$ while all the other bidders are opened as $x_{1,u+1}$, $x_{2,u+1}$, $\ldots x_{v-1,u+1}$, $x_{v+1,u+1}$, $x_{v+2,u+1}$, $\ldots x_{n,u+1}$. If an attacker A can decrypt any losing bid at p_{u+1}, he must know the decryption key

$$X_{u+1} = r_v + \sum_{k=1}^{v-1} x_k + \sum_{k=v+1}^{n} x_k + \sum_{k=1}^{v-1} x_{k,u+1} + \sum_{k=1}^{v-1} x_{k,u+1}$$

   on condition that the applied encryption algorithm (e.g. ElGamal or Paillier's) is secure. So he must know

$$\sum_{k=1}^{v-1} x_k + \sum_{k=v+1}^{n} x_k = X_{u+1} - \sum_{k=1}^{v-1} x_{k,u+1} - \sum_{k=v+1}^{n} x_{k,u+1} - r_v$$

   But to know

$$\sum_{k=1}^{v-1} x_k + \sum_{k=v+1}^{n} x_k = \sum_{k=1}^{v-1} log_g y_k + \sum_{k=v+1}^{n} log_g y_k$$

   the attacker needs the cooperation of all the losing bidders if Diffie-Hellman assumption is correct. So without cooperation of all the losing bidders all losing bids at p_{u+1} are confidential. That also means no share of X_{u+2} is published. Therefore without cooperation of all the losing bidders all losing bids at p_{u+2} are confidential too. Similarly all lower bids cannot be opened without cooperation of the losing bidders. So in this fashion stronger bid privacy can be achieved in our scheme than in the scheme by Watanabe and Imai [13].

6 Efficiency Improvement

As stated before, [13] is not efficient in computation and communication. Our scheme improves communication efficiency greatly as bid length is much shorter in our scheme

and communication with an active auctioneer is avoided. However the scheme is still not efficienct enough in computation.

If homomorphic encryption algorithm is employed to encrypt the bids, computational cost can be reduced. For example, assume Paillier's encryption scheme [9] is employed. In the appendix A, Paillier's encryption scheme is introduced. After this improvement, the cource of auction becomes as follows.

1. Initial phase:
   Each bidder B_i chooses a secret x_i and publishes $Com1_i = (B_i,\ y_i,\ Sig_{B_i}(B_i, y_i))$ where $y_i = g^{x_i}$ for $i = 1, 2, \ldots, n$ on a bulletin board.
2. Pre-bidding phase:
   Every bidder publishes a public key for every biddable price. If a bidder B_i is not willing to pay p_j, his public key for p_{j+1} is $y_{i,j+1} = g^{x_{i,j+1}}$ where the corresponding secret key $x_{i,j+1}$ is kept as a secret. If bidder B_i's bidding price is p_j, his public key for p_{j+1} is $y_{i,j+1} = g^{r_i} \prod_{k=1,k\neq i}^{n} y_k$ where r_i is kept as a secret and he chooses public keys $y_{i,j+2}, y_{i,j+3}, \ldots, y_{i,n}$ randomly for $p_{j+2}, p_{j+3}, \ldots, p_n$.
   B_i publishes $Com2_i = (B_i,\ y_{i,1}, y_{i,2}, \ldots, y_{i,w},\ Sig_{B_i}(B_i,\ y_{i,1}, y_{i,2}, \ldots, y_{i,w}))$ on the bulletin board. Key generation is illustrated in Table 3 (supposing there are 3 bidders and 6 biddable prices). The public key for price p_j is $Y_j = \prod_{k=1}^{n} y_{k,j}$ and can be calculated by anybody using the public values available on the bulletin board.
3. Bidding phase:
   Every bidder submits a bid for each biddable price. If a bidder B_i is not willing to pay p_j, his bid at p_j is $V_{i,j} = E_{Y_j}(x_{i,j+1})$. If B_i is willing to pay p_j, $V_{i,j} = E_{Y_j}(r_i)$. At price p_j lower than his evaluation, $V_{i,j}$ is randomly chosen. B_i publishes
   $V_i = (B_i,\ V_{i,1}, V_{i,2}, \ldots, V_{i,w},\ Sig_{B_i}(B_i,\ V_{i,1}, V_{i,2}, \ldots, V_{i,w}))$ on the bulletin board. Bid format is illustrated in Table 4 (supposing there are 3 bidders and 6 biddable prices).
4. Opening phase:
   The bidders publish $Com3_i = (x_{i,1},\ Sig_{B_i}(x_{i,1}))$ for $i = 1, 2, \ldots, n$. Anybody can verify the validity of the shares against $y_{i,1}$ for $i = 1, 2, \ldots, n$, construct the decryption key for the first price $X_1 = \sum_{k=1}^{n} x_{k,1}$ and decrypt all the bids at p_1. The meaning of B_i's decrypted bid $v_{i,1}$ can be determined by testing whether $y_{i,2} = g^{v_{i,1}}$ ($v_{i,1}$ is negative bid) or $y_{i,2} = g^{v_{i,1}} \prod_{k=1,k\neq i}^{n} y_k$ ($v_{i,1}$ is positive bid). If there is no bid showing willingness to pay at p_1, all the shares $x_{i,2} = v_{i,1}$ for $i = 1, 2, \ldots, n$ are obtained and $X_2 = \sum_{k=1}^{n} x_{k,2}$ can be recovered. Then all the bids at p_2 are opened. The opening continues until $y_{i,j+1} \neq g^{v_{i,j}}$ is met and the key chain breaks at p_{j+1}. If $y_{i,j+1} = g^{v_{i,j}} \prod_{k=1}^{n} y_k$, p_j and B_i are declared as winning price and winner. Otherwise B_i is identified as a cheater.

When the decryption key X_l at price p_l is recovered, the bids $V_{i,l}$ for $i = 1, 2, \ldots n$ are not opened separately. Instead

$$X'_{l+1} = D_{X_l}(\prod_{i=1}^{n} V_{i,l})$$

is recovered with only one decryption. There are two possibilities for X'_{l+1}.

1. If $G^{X'_{l+1}} = Y_{l+1}$, decryption key $X_{l+1} = \sum_{i=1}^{n} x_{i,l+1} = X'_{l+1}$ is recovered. That means the winning bid is not at p_l and X_{l+1} can be used to decrypt the product of bids at p_{l+1}.
2. If $G^{X'_{l+1}} \neq Y_{l+1}$, the winning bid must be at p_l. So all the bids at p_l are decrypted separately.
   - If $g^{D_{X_l}(V_{i,l})} = y_{i,l+1}$, B_i is not the winner.
   - If $g^{D_{X_l}(V_{i,l})} \neq y_{i,l+1}$, B_i is the winner. Moreover,

$$g^{D_{X_l}(V_{i,l})} \prod_{k=1,k\neq i}^{n} y_k = y_{i,l+1}$$

   is checked to ensure that the winner is not able to open the second highest bid.

Table-5 compares efficiency of the scheme by Watanabe and Imai, our original scheme and our scheme after optimisation (supposing Paillier's encryption scheme and RSA signature are employed). Our scheme is better than [13] not only in bid privacy but also in efficiency.

Scheme	Computational cost of a bidder (exponentiations)	Computational cost of auctioneer (exponentiations)
Scheme by Watanabe and Imai	$8w + 1$	$5.5nw + w + 4n$
Our original scheme	$1.5w + 2$	$nw/2 + 2n + 1$
Our scheme with homomorphic encryption	$1.5w + 2$	$w/2 + 3n + 1$

Table 5. Efficiency comparison

Efficiency improvement in this section has no negative effect on other properties of the scheme. After the efficiency improvement, the only thing different in all the phases except opening phase is that homomorphic encryption algorithm must be employed. If the homomorphic encryption algorithm is semantically secure itself (such as Paillier's), there is no compromise in these phases. In the opening phase, different opening method is employed. However the only difference is that new opening method reveals less information. So no achieved properties are compromised by the improvement on computation efficiemcy.

7 Conclusion

The key chain in the scheme by Watanabe and Imai[13] is modified, so that stronger bid privacy can be achieved in the proposed auction scheme. So far, this is the only scheme that can achieve non-interaction, public verifiability and unconditional privacy for losing bids at the same time. Efficiency is also improved in this scheme compared to [13].

References

1. Masayuki Abe and Koutarou Suzuki. M+1-st price auction using homomorphic encryption. In *Public Key Cryptology 2002*, pages 115–124, Berlin, 2002. Springer-Verlag. Lecture Notes in Computer Science Volume 2288.
2. D. Chaum and T. P. Pedersen. Wallet databases with observers. In Ernest F. Brickell, editor, *Advances in Cryptology - Crypto '92*, pages 89–105, Berlin, 1992. Springer-Verlag. Lecture Notes in Computer Science Volume 740.
3. Koji Chida, Kunio Kobayashi, and Hikaru Morita. Efficient sealed-bid auctions for massive numbers of bidders with lump comparison. In *Information Security, 4th International Conference, ISC 2001*, pages 408–419, Berlin, 2001. Springer-Verlag. Lecture Notes in Computer Science Volume 2200.
4. H Kikuchi, Michael Harkavy, and J D Tygar. Multi-round anonymous auction. In *Proceedings of the First IEEE Workshop on Dependable and Real-Time E-Commerce Systems*, pages 62–69, June 1998.
5. Hiroaki Kikuchi. (m+1)st-price auction. In *The Fifth International Conference on Financial Cryptography 2001*, pages 291–298, Berlin, February 2001. Springer-Verlag. Lecture Notes in Computer Science Volume 2339.
6. Hiroaki Kikuchi, Shinji Hotta, Kensuke Abe, and Shohachiro Nakanishi. Distributed auction servers resolving winner and winning bid without revealing privacy of bids. In *proc. of International Workshop on Next Generation Internet (NGITA2000), IEEE*, pages 307–312, July 2000.
7. David Naccache and Jacques Stern. A new public key cryptosystem based on higher residues. In *ACM Computer Science Conference 1998*, pages 160–174, 1998.
8. Kazumasa Omote and Atsuko Miyaji. A second-price sealed-bid auction with the discriminant of the p-th root. In *Financial Cryptography 2002*, Berlin, 2002. Springer-Verlag.
9. P Paillier. Public key cryptosystem based on composite degree residuosity classes. In *Eurocrypt'99*, pages 223–238, Berlin, 1999. Springer-Verlag. Lecture Notes in Computer Science Volume 1592.
10. K Sako. An auction scheme which hides the bids of losers. In *Public Key Cryptology 2000*, pages 422–432, Berlin, 2000. Springer-Verlag. Lecture Notes in Computer Science Volume 1880.
11. Kouichi 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, Hong Kong, 1999. City University of Hong Kong Press.
12. Koutarou Suzuki, Kunio Kobayashi, and Hikaru Morita. Efficient sealed-bid auction using hash chain. In *International Conference on Information Security and Cryptology 2000*, pages 183–191, Berlin, 2000. Springer-Verlag. Lecture Notes in Computer Science 2015.
13. Yuji Watanabe and Hideki Imai. Reducing the round complexity of a sealed-bid auction protocol with an off-line ttp. In *STOC 2000*, pages 80–86. ACM, 2000.

A Paillier's Encryption Scheme

Paillier's encryption scheme is as follows.

1. **Key Generation**: Choose a RSA modulus $N = pq$, where p and q are large prime integers. Choose an integer g so that its order $\alpha N$is a multiple of N modulo N^2. The public key is N and g and the secret key is $\lambda(N)$, where $\lambda(N) = lcm(p - 1, q - 1)$.

2. **Encryption**: To encrypt a message $m \in Z_N$, choose a random integer $x \in Z_N^*$ and compute the ciphertext $c = g^M x^N \mod N^2$.
3. **Decryption**: To decrypt c, compute $M = L(c^{\lambda(N)} \mod N^2)/L(g^{\lambda(N)} \mod N^2) \mod N$ where $L : \{u < N^2 | u = 1 \mod N\} \rightarrow Z_N$ and $L(u) = \frac{u-1}{N}$.