A Secure Auction Protocol without Any Dispute

JungHoon Ha, DongJin Kwak and SangJae Moon

School of Electronic & Electrical Eng., KyungPook National University

Abstract

We propose a new auction protocol scheme that uses the publicly verifiable secret sharing (PVSS) scheme. Unlike the existing scheme where a verifiable encryption scheme is employed when there is a dispute between a bidder and the auctioneer, the proposed scheme essentially removes the potential of a dispute. In addition, it has a robust registration phase and any entities participating in or observing the auction can verify the correctness of the auction process. The manager does not directly chooses the private key for the bidders, but only verifies the correctness between the private key and the public key, thereby improving the security, such as a bid submission of a malicious manager using the private key of a bidder.

I. Introduction

Auctioning is an efficient method exchanging goods in electronic commerce. Among the various auction types, the sealed-bid auction auctions are more effective for real-time applications and more suitable for a network environment [6].

Franklin and Reiter already proposed a protocol for sealed-bid auctions [4], however, their scheme results in all auctioneers knowing the full bid of all the bidders at the end of the auction. Thus, to provide privacy for losing bids, Watanabe and Imai presented a non-interactive sealed-bid auction scheme [10], yet, a losing bid can be still based on cooperation between the auctioneer and all the bidders with higher bids [6]. Thereafter, Peng *et al.* proposed a robust, publicly verifiable sealed-bid auction using the homomorphic property of Shamir's secret sharing scheme [9]. However, the procedure for verifying incorrect shares is complicated and computationally expensive when disputes between bidders and auctioneers arise.

Accordingly, the purpose of the current study is to improve the verification procedure for the incorrect shares in the proposal by Peng *et al* [7]. In addition, a robust registration phase, public verification and anonymous services are presented.

This remainder of this paper is organized as follows. The next section explains the necessary cryptographic primitives for the rest of the paper. Section 3 presents the new auction scheme. Section 4 analyzes the security and computational efficiency of the proposed scheme, and some final conclusions are given in section 5.

II. Cryptographic Primitives

1. *DLEQ* Protocol

The current study uses the $DLEQ(g_1, h_1, g_2, h_2)$ protocol overall this paper [8]. This protocol is kind of the proof of knowledge that proves $log_{g_1} h_1 = log_{g_2} h_2$ for generators $g_1, h_1, g_2, h_2 \in G_q$ where G_q is a group of prime order q, and use

the protocol by Chaum and Pedersen, originally used in the signature scheme, as a subprotocol of the *DLEQ* protocol [1]. In the proposed scheme, a modified *DLEQ* is used that adds the Fiat-Shamir technique for a non-interactive proof [3]. The modified $DLEQ(g_1, h_1, g_2, h_2)$ consists of the following steps and the prover knows □ such that $h_1 = g_1^{□}$ and $h_2 = g_2^{□}$:

1. The prover sends $a_1 = g_1^w$ and $a_2 = g_2^w$ to the verifier, with $w \in_R Z_q$.

2. The prover computes $r = w - □\ c \bmod q$.

3. The prover sends r and (g_1, h_1, g_2, h_2) to the verifier.

4. The verifier computes $c = H(h_1, h_2, a_1, a_2)$ from the received information.

5. The verifier checks that $a_1 = g_1^r h_1^c$ and $a_2 = g_2^r h_2^c$,

where H is an one-way hash function.

2. The PVSS Scheme

The PVSS scheme is a publicly verifiable secret sharing scheme with the property that the validity of the shares distributed by the dealer can be verified by any party. Schoenmaker's scheme is much simpler than other schemes and has the property that the participants not only release their shares but also provide a proof the correctness for each share released [8]. The scheme is specially modified to make suitable for the proposed auction scheme. In other words, C_j and X_i are eliminated from the original scheme. To supplement the deducted parts and preserve the security, the proposed auction scheme adds a signature scheme.

Ⅲ. Proposed Auction Scheme

This section describes the proposed auction scheme, which includes a more robust registration phase and more efficient computation load. In this scheme, the manager does not directly choose the private key and corresponding public key for the bidders, but only verifies the correctness of the relation of the pairs using the information sent to him from each bidder. The exchange between each bidder and the manager is run through a bulletin board. The proposed scheme also presupposes an established set of biddable prices, like other auction scheme [5]. The auction process consists of the following four phases : a system setup phase, registration phase, bid submission phase and bid opening phase.

1. System Set-up

The entities involved in the proposed scheme include the manager, n bidders b_i for $i \in Z_n$ and m auctioneers a_j for $j \in Z_m$. The manager is the trusted party who provides each bidder with an anonymous identity and manages the overall auction process. The manager also publishes the long-term public key y_M and releases the signature scheme for public verification prior to the auction run. Each auctioneer authenticates themselves in a proper manner to the manager and generates a private key $x_{a_j} \in_R Z_q^*$ and registers $y_{a_j} = G^{x_{a_j}}$ as their public key. In the proposed scheme, 2 bulletin boards are necessary, i.e., a registration bulletin board and auction bulletin board. Also, the following parameters are defined in this phase :

- The auctioneers publish the w biddable price p_l for $l \in Z_w$.
- The manager releases G_q which has group of prime order q and the independently selected generators g, G of G_q.

2. Registration Phase

The modified *DLEQ* protocol is used to achieve a robust registration phase and for a non-interactive proof. The exchange between each bidder and the manager is conducted through a public channel.

1. Every bidder b_i chooses a private key x_{b_i}.

2. The bidder computes $s_i = b_i^{x_{b_i}}$, $y_i = g^{x_{b_i}}$ and

$a_{1i} = b_i^{w_i}$, $a_{2i} = g^{w_i}$ for $w \in_R Z_q$.

3. For non-interactive proof, the bidder computes $r_i = w_i - x_{b_i} c_i$.

4. The bidder encrypts $m_i = (b_i, s_i, y_i, a_{1i}, a_{2i}, r_i)$ with the long-term public key of the manager and sends the encrypted message $E_{y_M}(m)$.

5. The manager decrypts the received message from each bidder and checks $DLEQ(b_i, s_i, g, y_i)$.

6. After verifying the correctness of the $DLEQ$ protocol, the manager computes $h_{b_i} = H(s_i, y_i)$.

7. The manager chooses bID according to h_{b_i} and sings (h_{b_i}, bID, y_i) ; $v_i = Sig(h_{b_i}, bID, y_i)$.

8. The manager publishes (h_{b_i}, bID, y_i, v_i) on the registration bulletin board.

After the registration steps from 1 to 8, each bidder finally verifies the released information on the registration bulletin board and creates a new ID, bID, for anonymity during the auction run.

3. Bid-Submission Phase

1) Evaluation of bidder

Every bidder first determines their own evaluation for the item being sold by auction, because the proposed auction scheme supposes that the biddable prices are preset before the auction run. If the bidders are willing to pay the bid at a specific price, they select $s_{i,l} = R_{i,l}$ with $R \in_R Z_q \backslash \{0\}$ and computes $S_{i,l} = G^{s_{i,l}} \bmod q$ as the secret for the bid submission. If none of the bidders wants to pay the bid for the specific price, they select $s_{i,l} = 0$ so that the secret of the bid is equal to one, $S_{i,l} = G^0 = 1 \bmod q$.

2) Calculation of share

1. Every bidder chooses a random polynomial p of a degree at most $t-1$ with the coefficient $\square \in Z_q$:

$$p_{i,l}(x) = \sum_{k=0}^{t-1} \square_{i,l,k} x^k,$$

where $p_{i,l}(x)$ presents the polynomial which the bidder chooses for the bid of a specific price p_l for $l \in Z_w$ and this polynomial meets $\square_{i,l,0} = s_{i,l}$. The bidder keeps the polynomial and coefficients secret.

2. Each bidder computes the shares $p_{i,l,j}(j+1)$ for $0 \leqq j \leqq m-1$ and encrypts the shares using the public key of the auctioneers.

3. The bidder computes $X_{i,l,j} = g^{p_{i,l,j}(j+1)}$ and executes the $DLEQ(g, X_{i,l,j}, y_{a_j}, Y_{i,l,j})$.

3) Information released on auction bulletin board

Every bidder signs the message related to a bid with the private key x_{b_i}. The following information is then published on the auction bulletin board :

- ID of the bidder submitting a bid : bID
- public key of the auctioneer used to encrypt a share : y_{a_j}
- encrypted shares : $m_i = (X_{i,l,j}, Y_{i,l,j}, a_{1i}, a_{2i}, r_i)$
- signature of the bidder : $\sigma_i = Sig_{x_{b_i}}(bID, y_{a_j}, m_i)$

4. Bid-Opening Phase

1) Verification of the public information

The auctioneers verify the signature using the public information (bID, y_i) on the registration board. If the verification succeeds, the auctioneers check the correctness of the encrypted shares using the modified $DLEQ$ protocol. If any verification fails, all information of the bidder related to a incorrect verification is removed in the auction proceedings.

2) Reconstruction of the secret

After verifying the signature and proof of the bidder, the auctioneers not only decrypt the encrypted shares with their private key but also

publish the proof that the decrypted value is exactly computed.

1. Using their private key x_{a_j}, each auctioneer gets the shares $S_{i,l,j} = G^{p_{i,l,j}(j+1)}$ form $Y_{i,l,j}$ by computing $S_{i,l,j} = (Y_{i,l,j})^{1/x_{a_j}}$.

2. To prove a correct decryption, each auctioneer executes $DLEQ(G, y_{a_j}, S_{i,l,j}, Y_{i,l,j})$.

3. Every auctioneer publishes $S_{i,l,j}$ plus the proof on the auction bulletin board.

4. The auctioneers pool the correct t shares out of m shares and recover the secret $G^{s_{i,l}}$ using a Lagrange interpolation :

$$\prod_{j=0}^{t-1} S_{i,l,j}^{\omega_{i,l,j+1}} = \prod_{j=0}^{t-1} (G^{p_{i,l}(j+1)})^{\omega_{i,l,j+1}} = G^{p_{i,l}(0)} = G^{s_{i,l}},$$

where $\omega_{i,l,j+1} = \prod_{k \neq j+1} \frac{k}{k-(j+1)}$ is a Lagrange coefficient.

3) Determination of winning price and winner

1. The auctioneers compute the general share $\hat{s_l} = \prod_{i=0}^{n-1} G^{s_{i,l}}$ at the biddable price p_l with $l \in Z_w$ and publish it on the auction bulletin board.

2. The upward opening is used to determine the wining price.

3. After the winning price is determined, the secret of the bidders is opened as regards the price and the winner is then determined.

4. The manager publishes all the information related to the winner bC_i and any party can identify the original identity, b_i.

Ⅳ. Analysis

1. Security

1) Anonymity

The manager provides every bidder with a new *ID*, bC_i, for the purpose of anonymity. To achieve anonymity, the manager maps the real *ID*, b_i, to the new *ID*, bC_i, using the preset value and keeps the relation between the b_i and bC_i secret.

2) Non-repudiation

Every bidder has a private key x_{b_i} and corresponding public key $y_i = g^{x_{b_i}}$ for the signature verification. This public key is checked by the manager in the registration phase and the manager sings the public key using his long-term private key.

3) Privacy

Even though the shares are released, the privacy of the losing bid is protected because all the bids are submitted anonymously and no one except the manager knows the corresponding real identity, b_i, of the losing bids.

4) Robustness

- *Private keys for bidders.* The manager does not directly choose the private key for the bidders, but only verifies the correctness between the private key and the public key, thereby improving the security, such as a bid submission of a malicious manager using the private key of a bidder.
- *The relation between b_i and bC_i.* In the proposed scheme, the relation between a real identity b_i and an anonymous identity bC_i is one to one mapping. To achieve this, the manager publishes the anonymous identities that are used in the auction and inconsistently establishes a relation between bC_i and h_{b_i} after verifying the messages received from the bidders. Because the values h_{b_i} is computed by the bidder knowing the private key x_{b_i}, only he can compare it with the published h_{b_i} and identify the new related identity bC_i. The relation between bC_i and h_{b_i} is one to one mapping the same as the relation between h_{b_i} and b_i, as such the relation between b_i and bC_i is one to one mapping. This one to one mapping among b_i, bC_i, and h_{b_i} prevents the

manager from recovering a false winner in the winner identification step.

2. Computational Efficiency

In terms of computation, we assume that in the PBDV scheme [7], ElGamal signature and encryption scheme are used between bidders and auctioneers [2]. In the table, M is denoted as the number of multiplication, I as the number of inverse and E as the number of exponentiation. In addition, t is threshold values of (t,m) access structure, m is the number of auctioneer and n is the number of bidders.

Table 1. Cost comparison between the proposed scheme and the PBDV scheme

Computational cost		PBDV scheme		proposed scheme
		case 1	case 2	
Bidder	I	$m+2$	$m+2$	m
	E	$3m+2t+2$	$9m+8t+2$	$5m$
	M	$3m+2t+4$	$2(2m+t+1)$	$3m$
Auctioneer	E	$n(t+10)+2t$	$n(t+17)+8t$	$n(t+12)$
	M	$n(t+4)-1$	$n(t+6)+4t$	$n(t+2)$

We suppose that in the PBDV auction scheme, case 1 represents that all entities attending the auction are honest, whereas case 2 considers computational cost when disputes between bidders and auctioneers arrive. As result, the proposed scheme is more efficient than the PBDV scheme regardless of case 1 or case 2.

V. Conclusion

A new sealed-bid auction scheme was presented based on a modified version of the PVSS scheme. The modified PVSS scheme includes the property of a non-interactive proof and publicly verifiable secret, thereby improving the potential for disputes between the bidders and the auctioneers, plus anyone can efficiently verify the correctness of the auction procedure, as all entities publish the proof. In addition, the proposed scheme has a robust registration phase, more efficient computational loads.

Reference

[1] D. Chaum and T. P. Pedersen, "Wallet Database with Observers", *CRYPTO'92*, pp. 89-105, 1993

[2] T. ElGamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", *CRYPTO'84*, pp. 10-18, 1985

[3] A. Fiat and A. Shamir, "How to prove yourself : Practical solutions to identification and signatures problems", *EUROCRYPT'86*, pp. 186-164, 1987

[4] M. K. Franklin and M. K. Reiter, "The Design and Implementation of a Secure Auction Service", *IEEE Transaction on Software Engineering*, pp. 302-312, 1996

[5] H. Kikuchi, M. Harkavy and J. D. Tygar, "Multi-round Anonymous Auction Protocols", *1st IEEE workshop on Dependable and Real-Time E-Commerce Systems*, pp.62-69, 1998

[6] K. Peng, C. Boyd, E. Dawson and K. Viswanathan, "Non-interactive Auction Scheme with Strong Privacy", *ICISC'02*, 2002

[7] K. Peng, C. Boyd, E. Dawson and K. Viswanathan, "Robust, Privacy Protecting and Publicly Verifiable Sealed-Bid Auction", *ICICS'02*, pp. 147-159, 2002

[8] B. Schoenmakers, "A Simple Publicly Verifiable Secret Sharing Scheme and its Application to Electronic Voting", *CRYPTO'99*, pp. 148-164, 1999

[9] A. Shamir, "How to share a secret", *Communication of the ACM*, 22(11), pp, 612-613, 1979

[10] Y. Watanabe and J. Imai, "Reducing the Round Complexity of a Sealed-Bid Auction Protocol with an Off-line ttp", *STOC 2000*, pp. 80-86, 2000