Receipt-free Sealed-bid Auction Scheme Using Cryptographic Techniques

Yong-Sork HER
* Graduate School of Information Science and Electrical Engineering, Kyushu University, JAPAN
e-mail : ysher@itslab.csce.kyushu-u.ac.jp

Abstract - Recently, a concept of bid-rigging is issued in electronic auction. To prevent this attack, Abe-Suzuki proposed firstly receipt-free scheme based on bidding-booth. Chen-Lee-Kim pointed out that Abe-Suzuki's scheme only provides receipt-freeness for losing bidders. Also, they introduced a new receipt-free sealed bid auction scheme using the homomorphic encryption technique. The main participants of their scheme are Auctioneer, Auction Issuer, Bidder and Seller. Bid-rigging can happen by a seller in their scheme. We propose receipt-free sealed-bid auction scheme using a universal re-encryption mixnet. For our receipt-free sealed-bid auction, we use Pseudo ID of a bidder and universal re-encryption technique of Golle et al. Also, our scheme satisfies privacy, correctness, public verifiability, non-reputation, and receipt-freeness.

Keywords: Sealed-bid auction, Receipt-freeness, Privacy, Security, Cryptography.

1 Introduction

1.1 Motivation

An auction is a kind of trade for special goods which have not a fixed price. In real world, a various type auctions have been enforced for decision of price. Recently, e-auctions using cryptography techniques have been proposed. An auction system is classified into English auction, Dutch auction, Sealed-bid auction and so on, according to a bidding type, and is classified into the first sealed-bid auction, the second sealed-bid auction, M+1st price auction and so on, according to a winning price. In the English auction scheme, a bidder repeatedly places a bid in real time with the bidding price seeing. After the bidding time is over, the bidding price is decided as the highest price. During bidding, all bidders can see the bidding price in the English auction. In case of a first-price sealed-bid auction, it needs only the highest price and a bidder should not know the bidding price of other bidder. A second-price sealed-bid auction is that a bidder who offers the highest price gets a good in the second highest price. The basic requirements for secure sealed-bid auction are as follows.

- **Privacy of bid**: No bid is revealed to anyone except the winner and the winning bid.
- **Proof of winner**: Everyone can verify the winner and the winning price which are decided correctly.
- **Non-repudiation**: The winner cannot repudiate his/her bidding at the winning price.
- **Accountability of bidder**: Any auctioneer can verify that bidders follow a protocol to cast their bids.
- **Correctness**: The winner and the winning price are determined correctly by a certain auction rule.
- **Bid Security**: Nobody can forge (falsify) and tap a bid.
- **Public verifiability**: Anyone can verify the correctness of the auction.
- **Robustness**: Even if a bidder sends an invalid bid, the auction process is unaffected.

Recently, the idea of a receipt-free technique to prevent bid-rigging is issued for fair auction system. A bid-rigging means collusion by a participant and outsiders (a coercer or a buyer). That is, a coercer orders other bidders to bid very low prices, he then can win the auction at an unreasonably low price [AS02]. If bid-rigging happens, the auction will fail to establish the fair winning price. To prevent bid-rigging, a bidder should not prove how he bided to a coercer or a buyer.

Abe and Suzuki [AS02] introduced firstly the concept of receipt for secure electronic auction. Chen, Lee and Kim [CLK03] pointed out that Abe and Suzuki's scheme only provides receipt-freeness for losing bidders. Also, they proposed a new receipt-free sealed bid auction scheme using the homomorphic encryption. The main participants of their scheme are Auctioneer, Auction Issuer, Bidder and Seller. A bidder and a seller generates jointly receipt-free bidding vector. They suppose that it is no reason that a seller collude with a bidder. But, there is an auction item which must carry out a bid. Then, a seller can try to make a special bidder to a winner. A bidder and a seller generate the receipt-free bidding vector $C^*_{i,j}$. A seller can provide a malicious bidder to random numbers β_j of other bidders. So, a seller can play a role as a coercer. If a malicious bidder becomes a winner, he rewards for the seller. In Table 1, we analyze security of the existed receipt-free sealed-bid auctions.

Golle et al.[GJJS04] introduced a universal re-encryption technique, and proposed a mix-net based on a universal re-encryption. A conventional cryptosystem that permits re-encryption does so only for a player with knowledge of the public key corresponding to a given ciphertext. But, their universal re-encryption can be done without knowledge of public keys. Also, an asymmetric

cryptosystem with universal re-encryption that is half as efficient as a standard ElGamal in terms of computation and storage. With these advantages, we use this universal re-encryption technique to mix only the encrypted bidding price.

Table 1. Security of the existed receipt-free sealed-bid auctions

Scheme	[AS02]		[CLK03]	
	Winner	Losing bidders	Winner	Losing bidders
Receipt-free scheme	*No*	*Yes*	Partial *Yes*	*Yes*
Disadvantage	The decision of winning price by all auctioneer		A generation of receipt-free bidding vector by a seller and a bidder	

1.2 Our contribution

In this paper, we propose a receipt-free sealed-bid auction based on a universal re-encryption mix-net. Golle et al. [GJSS04] introduced a universal re-encryption scheme and proposed mix-net based on a universal re-encryption. We use freely this scheme for our receipt-free sealed-bid auction. To apply a universal re-encryption, we modify the existed designated-verifier re-encryption proof. The modified designated-verifier re-encryption proof is used to prove the validity of mixing. Also, our scheme uses a Pseudo ID of a bidder such as a random number ID instead of a real ID. A bidder knows his Pseudo ID, but other bidders do not know it. Although a bidder opens his Pseudo ID, he can not prove whether the opened Pseudo ID is right or not. An auction issuer manages Pseudo ID and mixes the re-encrypted bidding vector. He does not join in the decision of winning price. Also, an auctioneer mixes the re-encrypted bidding vector, and decides the winning price. Then, the auctioneer recovers all bidding prices, and knows all bidding prices. But, he publishes only winning price.

2 Universal re-encryption for mixnets

Golle *et al.* [GJJS04] proposed a new type of public-key cryptosystem that permits universal re-encryption of ciphertexts. Like standard re-encryption, universal re-encryption transforms a ciphertext C into a now ciphertext C' with same corresponding plaintext. The outline is as follows.

1. Every input to the mixnet is encrypted under the public key of the recipient for whom it is intended.
2. Thus, unlike standard re-encryption mixnets, universal mixnets accept ciphertexts encrypted under the individual public keys of receivers, rather than encrypted the unique public key of the mix network.
3. The output of a universal mixnet is a set of ciphertexts.
4. Recipients can retrieve from the set of output ciphertexts those addressed to them, and decrypt them.

Key generation (*UKG*)

Output (PK,SK)= $(y = g^x, x)$ for $x \in_U Z_q$.

Encryption (*UE*)

Input comprises a message m, a public key y, and a random encryption factor $r = (k_0, k_1) \in Z_q^2$.

The output is a ciphertext $C = [(\alpha_0, \beta_0); (\alpha_1, \beta_1)] = [(my^{k_0}, g^{k_0}); (y^{k_1}, g^{k_1})]$.

We write $C = UE_{PK}(m, r)$ or $C = UE_{PK}(m)$ for brevity.

Decryption (*UD*)

Input is a ciphertext $C = [(\alpha_0, \beta_0); (\alpha_1, \beta_1)]$ under public key y. Verify $\alpha_0, \beta_0, \alpha_1, \beta_1 \in g$; if not, the decryption fails, and a special symbol $\perp$ is output. Compute $m_0 = \alpha_0 / \beta_0^x$ and $m_1 = \alpha_1 / \beta_1^x$. If $m_1 = 1$, then the output is $m = m_0$. Otherwise, the decryption fails, and a special symbol $\perp$ is output. Note that this ensures a binding between ciphertexts and keys: a given ciphertext can be decrypted only under one given key.

Re-encryption (*URe*)

Input is a ciphertext $C = [(\alpha_0, \beta_0); (\alpha_1, \beta_1)]$ with a random re-encryption factor $r' = (k_0', k_1') \in Z_q^2$.

Output is a ciphertext

$C' = [(\alpha_0', \beta_0'); (\alpha_1', \beta_1')] = [(\alpha_0 \alpha_1^{k_0'}, \beta_0 \beta_1^{k_0'}); (\alpha_1^{k_1'}, \beta_1^{k_1'})]$,

where $k_0', k_1' \in_U Z_q$.

3 Receipt-free sealed bid-auction based on Cryptographic Techniques

3.1 Physical Assumption

Bulletin Board : We use bulletin board which everyone can see a content of bulletin board, but can not modify or erase it. In a receipt-free scheme of an electronic auction and an electronic voting, it is used usually a physical assumption. In [AS02] and [BT94], they used called bidding booth or voting booth which is a stronger physical assumption. But, the other scheme [CLK03] uses a bulletin board instead of bidding booth or voting booth. In our scheme, bulletin board is used to publish a Pseudo ID of bidder and re-encrypted bidding information.

Anonymous Secret Channel: An anonymous secret channel is a both-way channel with keeping anonymity and security. This channel is stronger physical assumption than an untappable channel. Any third party can not eavesdrop a message, and know a sender and a receiver. We assume that an anonymous secret channel between a bidder and an auction issuer is available.

3.2 Overview of our receipt-free sealed bid auction

We propose a secure receipt-free sealed-bid auction based on universal re-encryption [GJJS04].

Bidding : Bidding : A bidder sends his real ID to the auction issuer, and receives a unique Pseudo ID ($\in Z_q^2$) through an anonymous secret channel. A bidder computes *Bidding ID vector* with a public key of auction issuer and his random number.

Also, a bidder chooses his bidding price, and generates *Bidding vector* with a public key of the auctioneer and a random encryption factor. A bidder sends *Bidding ID vector* and *Bidding vector* to the auction issuer.

The auction issuer re-encrypts *Bidding vector* with *Bidding ID vector* and his random encryption factor using universal re-encryption technique [GJJS04]. He proves his mixing to an auctioneer using the modified Designated-Verifier Re-encryption proof. Also, he posts re-encrypted *Bidding ID vector* and the proof to bulletin board in random.

Opening : The auctioneer recovers *Bidding vector*, and computes a winning price and *Bidding ID vector*. He publishes *Bidding ID vector* of the winner in bulletin board.

Trading : The winner proves his *Bidding ID vector* P_0 to the auction issuer with his Pseudo ID and random number $r_b (\in Z_q^2)$.

3.3 Participants

A bidder : A bidder offers a bid only one-time by an auction rule.

Auction issuer : An auction issuer takes part in mixing of bidding prices and manages Pseudo ID of each bidder. Also, we suppose that an auction issuer does not collude with anyone.

Auctioneer : An auctioneer mixes bidding prices like auctioneer issuer, and decides the winning price and publishes it. Also, we suppose that an auction issuer does not collude with anyone.

Client : A client commits an auction item to an auctioneer.

3.4 Procedures

Notation

x_A : A secret key of an auctioneer

y_A : A public key of an auctioneer ($y_A = g^{x_A} \bmod p$)

S_u : A secret key of an auctioneer for designated verifier re-encryption proof

y_u : A public key of an auctioneer for designated verifier re-encryption proof ($y_u = g^{S_u} \bmod p$)

x_I : A secret key of an auction issuer

y_I : A public key of an auction issuer ($y_I = g^{x_I} \bmod p$)

x_B : A secret key of a bidder

y_B : A public key of a bidder ($y_B = g^{x_B} \bmod p$)

P_{ID} : Pseudo ID of a bidder

BB : Bulletin Board

p, q : Random numbers ($p = 2q + 1$)

g' : A generator $\bmod q$ ($g = (g')^k \bmod p$

1) Registration Stage.

1.1 An auction issuer takes a bidder list. A bidder sends his Real-ID to an auction issuer through an anonymous secret channel.

1.2 An auction issuer generates a unique Pseudo ID for a bidder as follows.

Bidder's *Real-ID* → [*Pseudo ID Generator*] → Bidder's *Pseudo ID* ($P_{ID_i} \in Z_q$)

1.3 An auction issuer sends the bidder's Pseudo ID to the bidder through an anonymous secret channel. The bidder and an auction issuer know a relation between Real-ID and Pseudo-ID. However, the auction issuer does not know a bidding price yet.

2) Bidding Stage

2.1 A bidder B_i computes *Bidding ID vector* p_0 with a public key y_I of an auction issuer and his random number $r_b (\in Z_q^2)$ as follows.

$$P_0 = y_I^{P_{ID}} g^{r_b} = g^{x_I P_{ID} + r_b}$$

2.2 A bidder proves the validity of *Bidding ID vector* P_0 to auction issuer.

2.3 A bidder chooses his bidding price b_i, and generates a random encryption factor $k = (k_0, k_1) \in Z_q^2$, where $k_0 \neq k_1$. A bidder computes *Bidding vector* with a public key y_A of an auctioneer and k as follows.

$$C_0 = [(x_0, y_0), (x_1, y_1)] = [(b_i y_A^{k_0}, g^{k_0}); (y_A^{k_1}, g^{k_1})]$$

2.4 A bidder sends (P_0, C_0) to the auction issuer.

3) Mixing Stage

3.1 The auction issuer generates a random encryption factor $k' = (k_0', k_1') \in Z_q^2$, where $k_0' \neq k_1'$.

3.2 The auction issuer re-encrypts and mixes bidding vectors of each bidder and *Bidding ID vector* p_0 in random using universal re-encryption as follows.

$$C_1 = [(x_0', y_0'), (x_1', y_1')] = [(x_0 x_1^{k_0'}, y_0 y_1^{k_0'})(P_0 x_1^{k_1'}, y_1^{k_1'})]$$

3.3 The auction issuer chooses $k_1, k_2, r, t \in Z_q^2$ and

computes $[(a,b),(c,d)]=[(y^{k_1},g^{k_1}),(y^{k_2},g^{k_2})], F=g^r y_u^t$, where $y_u = g^{S_u}$ is a public key, and S_u is a private key of the auctioneer.

3.4 The auction issuer computes $S=H(a,b,c,d,F,x_0',y_0',x_1',y_1')$, $T=k_1-a_1-a_2a_1'$ and $U=k_2-a_2a_2'$, where H is a hash function such as SHA-1 , and a_1, a_2, a_1' and a_2' are random encryption factors of the auction issuer ($a_1, a_2, a_1', a_2' \in Z_q^2$). Then, he sends (r,t,S,T,U) and C_1 to the auctioneer.

3.5 The auction issuer sends C_1 and P_0 to the Bulletin board in random order. Also, he posts the proof to the designated fields in the bulletin board.

A bidder can confirm his bidding ID vector P_0.

4) Opening Stage

4.1 The auctioneer recovers P_0 with his secret key x_A as follows.

$$x_1'/(y_1')^{x_A} = P_0 x_1'^{k_1'}/(y_1'^{k_1'})^{xz} = P_0$$

4.2 Also, the auctioneer computes the bidding price b_i as follows.

$$x_0'/(y_0')^{x_A} = b_i x_0'^{k_0'}/(y_0'^{k_0'})^{xz} = b_i$$

4.3 The auctioneer computes the winning price b_i, and publishes *Bidding ID vector* P_0 in bulletin board.

5) Trading Stage

5.1 The winner who bides the winning price b_i should prove his *Bidding ID vector* P_0 with his random number r_b.

5.2 The auction issuer recovers the winner Pseudo ID P_{ID_i} with the received random number r_b and his secret key x_I.

5.3 If the winner wants to cancel the trading, the auctioneer and the auction issuer can compute the winner's real ID with their random encryption factors and secret keys.

3.5 Security

3.5.1 Privacy

An auction issuer knows the relation between a real ID and a Pseudo ID of a bidder. But, an auction issuer does not know a bidding price because an auction issuer does not know the secret key x_A of an auctioneer. Also, an auctioneer knows only the winning price, and does not publish the losing prices. Unless an auctioneer and an auction issuer collude, the privacy can be kept.

3.5.2 Receipt-freeness

In our scheme, although a bidder knows his Pseudo ID and bidding price, he can not prove it. All pseudo ID is published in bulletin board. Although a malicious bidder provides his Pseudo ID, a coercer/buyer can not believe it, because a malicious bidder does not know the secret key x_I of the auction issuer. Moreover, a bidder can tell a lie his Pseudo ID using proof of knowledge of Pseudo ID. $F=g^r y_u^t$ can be used a trapdoor commitment like [CLK03]. A bidder knows his private key x_u, he can compute r' and t' such that $r'+x_u t' = r + x_u t$. He can open freely the commitment as he wants and generates the re-encryption proof for any bidding.

3.5.3 Non-repudiation

The auctioneer and the auction issuer can recover the bidding price, real ID, and Pseudo ID.

3.5.4 Correctness and public verifiability

No malicious bidders can affect the result of the auction due to the interactive proof of knowledge of *Bidding ID vector* and *Bidding vector*. Everyone can take the information to verify the correctness of the auction from bulletin board.

4 Conclusion

Abe-Suzuki's receipt-free scheme has a problem that all auctioneers together recover the secret seeds of each bidder to determine the winning price and the winners. Also, Chen-Lee-Kim's receipt-free scheme can be happen a bid-rigging by a seller. In real auction, a seller and a bidder can collude on an auction item which must auction off. If the malicious bidder becomes a winner, a seller can rewards the winner after bidding. In this paper, we proposed a receipt-free sealed-bid auction based on a universal re-encryption mix-net. Golle *et al.* introduced a universal re-encryption and proposed mixnet based on their universal re-encryption. For our sealed-bid re-encryption, we modified the existed designated-verifier re-encryption to apply a universal re-encryption. Moreover, our scheme satisfies privacy, correctness, public verifiability, non-reputation, and receipt-freeness.

5 References

[AS02] M.Abe and K.Suzuki.: Receipt-Free Sealed-Bid Homomorphic Encryption, Proc. Of Public Key Cryptography2002, LNCS 2274, pp191–199, 2002.

[BT94] J. Benaloh and D.Tuinstra, " Receipt-Free Secret-Ballot Elections", Proc. of STOC'94, pp544-553, 1994.

[CLK03] A.Chen, B.C.Lee and K.J.Kim.: Receipt-Free Electronic Auction Scheme Using Homomorphic Encryption. Proc. of ICISC2003, 275–290, 2003.

[GJJS04] P.Golle, M. Jakobsson, A.Juels and P.Syverson, "Universal Re-encryption for Mixnets", CT-RSA 2004, LNCS 2964, pp163-178, 2004.