# Receipt-free Sealed-bid Auction Based on Mix-net and Pseudo ID

Her, Yong-Sork
Graduate School of Information Science and Electrical Engineering, Kyushu University

Imamoto, Kenji
Graduate School of Information Science and Electrical Engineering, Kyushu University

Sakurai, Kouichi
Faulty of of Information Science and Electrical Engineering, Kyushu University

# Receipt-free Sealed-bid Auction Based on Mix-net and Pseudo ID

Yong-Sork Her† Kenji Imamoto† Kouichi Sakurai‡

†Graduate School of Information Science and Electrical Engineering, Kyushu University
6-10-1, Hakozaki, Higashigu, Fukuoka, 812-8581, Japan

(ysher,imamoto)@itslab.csce.kyushu-u.ac.jp

‡Faulty of of Information Science and Electrical Engineering, Kyushu University
6-10-1, Hakozaki, Higashigu, Fukuoka, 812-8581, Japan

sakurai@csce.kyushu-u.ac.jp

**Abstract** Recently, a concept of bid-rigging is issued in an electronic auction. To prevent this attack, Abe-Suzuki proposed firstly a receipt-free scheme based on the 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. We argue that it can be generated bid-rigging by a seller. Also, we propose a receipt-free sealed-bid auction which satisfies privacy, correctness, public verifiability, non-reputation and receipt-freeness. For privacy, correctness, public verifiability, non-reputation and receipt-freeness, we use Pseudo ID of a bidder and the universal re-encryption mix-net which is proposed by Golle *et al.*

## 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, Detuch 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, $M + 1^{st}$ 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 falsify and tap a bid.

**Public verifiability**: Anyone can verify the correctness of the auction.

**Robustness**: Even if a bidder sends an in-

valid 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 a 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 [9]. 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 [9] introduced firstly the concept of a receipt-freeness for secure electronic auction. Chen, Lee and Kim [1] 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 $\beta_j$ 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.
Golle *et al.* [12] 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.

### 1.2 Related work

There are many schemes for sealed-bid auction. Kikuchi, Harkavy and Tygar[4] proposed the method that deals with tie-breaking in sealed-bid auctions. Omote and Miyaji[6]proposed sealed-bid action with binary trees which is emphasized efficiency and entertainment. Naor, Pinkas and Sumner [10] introduced a sealed-bid auction that uses two-server auction system in order to ensure privacy and correctness. Juels and Szydlo [2] improved the scheme of [10] in aspect of the amount of computation and communication. Baudron and Stern [11] proposed a sealed-bid auction based on circuit evaluation using homomorphic encryption. Abe and Suzuki[8] proposed M+1-st price auction using homomorphic encryption. Lee, Kim and Ma [3] proposed public auction with one-time registration and public verifiablility.

### 1.3 Contributions

In this paper, we propose a receipt-free sealed-bid auction based on a universal re-encryption mix-net. Golle *et al.* [12] introduced a universal re-encryption scheme and proposed mix-net based on the universal re-encryption. We use freely this scheme for our receipt-free sealed-bid auction. To apply the 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 Receipt-free Sealed Bid Auction Based on Universal Re-encryption

## 2.1 Physical Assumption

**Bulletin Board**: We use a 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 [9] and [5], they used called the bidding booth or the voting booth which is a stronger physical assumption. But, other schemes [1][7] use 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.

## 2.2 Outline of our receipt-free sealed bid auction

We propose a secure receipt-free sealed-bid auction based on universal re-encryption [12].
**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 *Bid-ding 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 [12]. He proves his mixing to an auctioneer using the modified Designated-Verifier Re-encryption proof (Refer to Appendix A). 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 *Bid-ding ID vector*. He publishes *Bidding ID vector* of the winner in bulletin board.
**Trading** :
- The winner proves his *Bidding ID vector* to the auction issuer with his Pseudo ID and random number $r_b(\in Z_q^2)$

## 2.3 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.

## 2.4 Procedures

**Notation**
$x_A$ : A secret key of an auctioneer
$y_A$ : A public key of an auctioneer ($y_A = g^{x_A} mod p$)
$S_u$ : 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 ($y_u = g^{S_u} mod p$)
$x_I$ : A secret key of an auction issuer
$y_I$ : A public key of an auction issuer ($y_I = g^{x_I} mod p$)
$x_B$ : A secret key of a bidder
$y_B$ : A public key of a bidder ($y_B = g^{x_B} mod p$)
$P_{ID}$ : Pseudo ID of a bidder
$BB$ : Bulletin Board
$p, q$ : Random numbers ($p = 2q + 1$)
$g^{'}$ : A generator $mod q$ ($g = (g^{'})^k mod p$)

**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 $\longrightarrow$ [Pseudo ID Generator] $\longrightarrow$ 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* to auction issuer (See Appendix B).
**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 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 $S = H(a, b, c, d, F, x_0', y_0', x_1', y_1')$,$T = k_1 - a_1 - a_2 a_2'$ and $U = k_2 - a_2 a_2'$. 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 Bulletin board in random order. Also, he posts the proof to the designated fields in bulletin board.
**3.6** 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.

$$x_1'/(y_1')^{x_A} = P_0 x_1^{k_0'}/(y_1^{k_0'})^{x_A} = P_0$$

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

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

**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 Pseu do 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 Analysis of proposed receipt-free sealed-bid auction

## 3.1 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.

### 3.2 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 (See appendix B). In appendix A, $F = g^r y_u^t$ can be used a trapdoor commitment like [1]. 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 (See appendix A).

### 3.3 Non-repudiation

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

### 3.4 Correctness

No malicious bidders can affect the result of the auction due to the interactive proof of knowledge of *Bidding ID vector* and itshape Bidding vector.

### 3.5 Public verifiability

Everyone can take the information to verify the correctness of the auction from bulletin board.

## 4 Conclusions

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 generated 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 reward the winner after bidding. In this paper, we proposed the receipt-free sealed-bid auction based on the universal re-encryption mix-net. Golle *et al.* introduced a universal re-encryption and proposed mix-net based on their universal re-encryption. For our sealed-bid re-encryption, we modified the existed desi gnated-verifier re-encryption to apply a universal re-encryption. Moreover, our scheme satisfies privacy, correctness, public verifiability, non-reputation, and receipt-free.

**ACKNOWLEDGEMENT**
The research was partly supported by the Grant-in-Aid for Creative Scientific Research No.14G S0218 of the Ministry of Education, Science and Culture (MEXT) and by the 21st Century COE Program ‘ Reconstruction of Social Infrastructure Related to Information Science and Electrical Engineering ’.

## References

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

[2] A.Juels and M.Szydlo, “ A Two-Server, Sealed-Bid Auction Protocol ”, Proc. of Financial Cryptography 2002, 2002.

[3] B.C.Lee, K.J.Kim and J.S.Ma, “ Efficient Public Auction with One-Time Registration and Public Verifiability ”, Indocrypt 2001, 2001.

[4] H.Kikuchi, M.Harkavy and J.D.Tygar, “ Multi-round Anonymous Auction Protocols ”,Proceeding of Third USENIX Workshop on Electronic Commerce, pp61-74,1998.

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

[6] K.Omote and A.Miyaji, " An anonymous auction protocol with a single non-trusted center binary trees ", Information security workshop-Proc. of ISW2000, LNCS 1975, Springer-Verlag, pp108-120, 2000.

[7] K.Sako and J.Kilian, "Receipt-Free Mix-type Voting Scheme ", Proceeding of Eurocrypt '95, LNCS921, Springer-Verlag, pp393-403,1995.

[8] M.Abe and K.Suzuki, " M+1-st Price Auction using Homomorphic Encryption ", Proc. of Public Key Crytpography 2002, LNCS 2274, pp.115-124, 2002.

[9] M.Abe and K.Suzuki, " Receipt-Free Sealed-Bid Auction ", ISC2002, LNCS2433, pp191-199,2002.

[10] M.Naor, B.Pinkas and R.Summer, " Privacy Preserving Auctions and Mechanism Design ", Proceeding of ACM conference of E-commerce, pp129-139, 1999.

[11] O.Baudron and J.Stern, "Non-interactive Private Auctions ", Proc. of Financial Cryptography 2001, 2001.

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

[13] T.Okamoto, "Receipt-Free Electronic Voting Scheme for Large Scale Elections ", Security Protocols Workshop, 1997

## APPENDIX

### A. Designated-Verifier Re-encryption proof for Universal Re-encryption

We modified Designated-Verifier Re-encryption proof for universal re-encryption. The modified proof is used the proof of the re-encrypted bidding prices by the auction issuer and the auctioneer. Let$[(x_0, y_0), (x_1, y_1)] = [(my^{a_1}, g^{a_1}) ; (y^{a_2}, g^{a_2})]$ be an original encrypted ElGamal ciphertext by universal re-encryption scheme for the message $m$ and a random encryption factor $(a_1, a_2) \in Z_q^2$ , and $[(x_0^{'}, y_0^{'}), (x_1^{'}, y_1^{'})] = [(x_0 x_1^{a_1^{'}}, y_0 y_1^{a_1^{'}}); (x_1^{a_2^{'}}, y_1^{a_2^{'}})]$ be a re-encrypted ciphertext by a prover. The prover wants to prove that $(x_0^{'}, y_0^{'})$ and $(x_1^{'}, y_1^{'})$ have exponents $a_1^{'}$ and $a_2^{'}$ without exposing the values $a_1^{'}$ and $a_2^{'}$. We suppose that a public key $y_u = g^{s_u}$ is a public key of the verifier.

| Prover | | Verifier |
|---|---|---|
| $k_1, k_2, r, t \in Z_q^2$ | | |
| Compute | | |
| $[(a,b)(c,d)] =$ | | |
| $[(y^{k_1}, g^{k_1}), (y^{k_2}, g^{k_2})]$ | | |
| $F = g^r y_u^t$ | | |
| $S = H(a, b, c, d, F,$ | | |
| $x_0^{'}, x_0^{'}, x_0^{'}, x_0^{'}, x_0^{'})$ | | |
| $T = k_1 - a_1 - a_2 a_1^{'}$ | | |
| $U = k_2 - a_2 a_2^{'}$ | | |
| | $(r, t, S, T, U)$ | |
| | $\longrightarrow$ | Accept the proof if |
| | | $S = (y^T x_0^{'}, g^T y_0^{'},$ |
| | | $y^U x_1^{'}, g^U y_1^{'}, g^r y_u^t,$ |
| | | $x_0^{'}, y_0^{'}, x_1^{'}, y_1^{'})$ |

### B. Proof of Knowledge of Pseudo ID

A prover with possession a Pseudo ID $P_{ID} \in Z_q$ wants to show that $log_g u = log_y v$ while without exposing a Pseudo ID $P_{ID}$, where $u = g^{P_{ID}}, v = y^{P_{ID}}$.

| Prover | | Verifier |
|---|---|---|
| $w \in Z_q$ | | |
| Compute | | |
| $a = g^w, b = y^w$ | $(a, b)$ | $c \in Z_q$ |
| | $\longrightarrow$ | |
| | c | |
| | $\longleftarrow$ | |
| Compute | | |
| $r = w + cP_{ID}$ | | |
| | r | accept the proof if |
| | $\longrightarrow$ | |
| | | $g^r = au^c, y^r = bv^c$ |