

On the Security of Two Sealed-Bid Auction Schemes

Kin-Woon Yeow, Swee-Huay Heng and Syh-Yuan Tan

Faculty of Information Science and Technology,

Multimedia University, Melaka, Malaysia.

Email: yeowkinwoon@gmail.com, {shheng, sytan}@mmu.edu.my

Abstract—In this paper, we cryptanalyze two sealed-bid auction schemes and show that both schemes are not secure against the known-bid attack. In the first scheme, we show that a dishonest sealer can swap the price of a sealed-bid and yet its validity remains intact; in the second scheme, we show that a dishonest auctioneer can forge a bidder's bid if the bidder was once a winning bidder. We propose a workaround for the former using a designated confirmer signature but not the latter, which is fundamentally flawed.

Keywords: sealed-bid, auction, known-bid attack, sealer

I. INTRODUCTION

An auction is a type of economic activity for goods and services trade among bidders. Ideally, auction trading takes place fairly between the auctioneer and the bidders. There are numerous types of auction [11], such as English auction, Dutch auction, and sealed-bid auction. The English auction is commonly used in selling of goods where the price in English auction is successively raised until only one bidder remained. The Dutch auction is the converse of English auction. The price is announced by the auctioneer as an initial high price which is successively reduced until one bidder accepts the current price. Sealed-bid auction is a unique auction process in which every bidder concurrently submits sealed-bids (buying price). Every submission of bid is confidential and the winning bidder is rewarded with the item for the price bid [11]. Therefore, different from the former auctions, sealed-bid auction achieved fairness which is unbiased towards the auctioneer. This property attracts the attention of researchers.

In 1996, Franklin and Reiter [3] published an electronic sealed-bid auction scheme which enhances the anonymity for bidders. The proposed scheme aims to provide confidentiality to the bid, and only the winning bidder can collect the winning item.

One of the common issues found in sealed-bid auction is bid-rigging attack which happens when the coercers place an order towards other bidders to bid at low prices in order for the coercers to win the auction. In view of this, Sakurai and Miyazaki [15] first pointed out that there exists the problem of bid-rigging in electronic auction. Furthermore, Sakurai and Miyazaki proposed a sealed-bid auction scheme that provides anonymity, confidentiality, and non-repudiation using convertible group signature and bulletin board as the intermediate verification. Subsequently, Abe and Suzuki [1] introduced the security property of receipt-freeness in sealed-

bid auction to overcome the bid-rigging attack. They made two physical assumptions, firstly, the bidding booth which enables the bidder to perform bidding freely and secondly, one-way untappable channel. However, Chen et al. [2] pointed out that Abe and Suzuki's scheme only provides receipt-freeness for losing bidders. Subsequently, Chen et al. introduced a new receipt-free sealed-bid auction scheme using homomorphic encryption technique which provides receipt-freeness for every bidder.

In 2008, Wu et al. [16] cryptanalyzed Liaw et al. [9] electronic auction scheme and proposed a sealed-bid auction scheme that provides better functionality and efficiency. Independently, Lee et al. [8] published a sealed-bid auction scheme based on group signature to achieve the properties of anonymity, confidentiality of bid, public verifiability, and non-repudiation. Similarly, Xiong et al. [17] used the technique of ring signature and verifiable key chain encryption for sealed-bid auction scheme. The security properties achieved using ring signature are anonymity, confidentiality of bid, public verifiability, and non-repudiation.

In 2011, Li et al. [10] proposed a secret electronic auction scheme that is suitable for English auction or sealed-bid auction that fulfills the security requirements, namely, anonymity, confidentiality of bid, public verifiability, non-repudiation, and traceability. In addition, Li et al.'s proposed scheme uses two managers, namely, registration manager and auction manager with zero-knowledge protocol to achieve the security requirements of anonymity, bidding privacy, confidentiality of bid, verifiability, non-repudiation, traceability, one-time registration, and easy revocation. On the other hand, Montenegro and Lopez [12] applied another approach into sealed-bid auction scheme, namely, secure multiparty computation that hides bidding information from the auctioneer. At the same time, Nojournian and Stinson [13] constructed a second-price sealed-bid auction using verifiable secret sharing. In the approach of verifiable secret sharing, each bidder can verify the consistency of their bid with other bidders in the auction.

In 2009, Howlader, Ghosh, and Pal [5] proposes a new entity for sealed-bid auction scheme, namely, sealer to achieve receipt-freeness. The bid structure of [5] has been modified and reused in the works of Howlader, Roy, and Mal (HRM13) [7] and Howlader and Mal (HM15) [6] schemes. In HM15, a receipt-free sealed-bid electronic auction scheme was con-

structed to endure threats from public network.

The security analysis of [5], [7], [6] assumed that the sealer is not entirely trustworthy, i.e., some sealers are malicious. In [7], a clear assumption comparison of some sealed-bid auction schemes was given and it showed that the assumption of honest auctioneer is not required.

Threats of sealed-bid auction are being classified into two groups, outsiders and insiders. Outsiders attacks are usually more difficult to detect compared to insiders attacks but insiders attacks are more difficult to withstand. In the scheme of HM15 [6], the threats of seal-bid auction were listed with the consideration of attacks from both outsiders and insiders. Furthermore, the entities involved in the threats were grouped as follows.

- Auctioneer as insider is able to open the bid without depending on the bid opening phase. This causes failure in privacy of bid.
- Auctioneer is able to withdraw and submit unlawful bid. This causes deprive in fairness.
- Auctioneer is able to suppress some valid bids and promote certain bids to be winning bid. This causes lack of correctness.
- Auctioneer is able to disclose the identity of bidder with its bidding prices after the bid opening phase. This causes failure in anonymous bidding.
- Coercer as insider is able to corrupt some authorities to obtain information for bid-rigging attack. This causes failure in uncoercibility.
- Adversary as outsider or insider is able to corrupt the bid without being detected is considered failure to produce a correct output for the auction [14].

A. Our Contributions

In 2013, HRM13 [7] proposed a receipt-free sealed-bid auction in the coercive environment. Subsequently, HM15 [6] published an improved version in 2015. These two sealed-bid auction schemes are based on an entity known as sealer. Their securities were analyzed under the security model which assumes at least one of the sealers must be honest. Besides, although HM15 claimed that the scheme could withstand randomization attack, no concrete security analysis was provided.

In this paper, we present two known-bid attacks on HRM13 and HM15 respectively. The first attack, which we term as price swapping attack, views the malicious first sealer as an adversary on HRM13 [7]. Specifically, we show that the adversary is able to swap the bidding price by performing random swapping towards the bidding price bid-vector, Γ_i . Although the adversary may not be able to achieve the same outcome as in bid-rigging, the price swapping attack is sufficient to corrupt the bidding system.

Besides, we discover that HM15 [6] reveals the winning bidder's classified information, namely, *YES* mark of the winning bid (which indicates the bidding price) and bidder's secret seeds during the bid opening phase. Through these revelations, the auctioneer is able to forge a valid bid for the

subsequent bid of the winning bidder without knowing the bidder's secret key.

B. Organization

We organize the paper as follows. The basic definition of sealed-bid auction is introduced in Section 2. In Section 3, we demonstrate the price swapping attack on the sealed-bid auction scheme of HRM13 to corrupt a bid and yet preserve its validity. In Section 4, we mount a known-bid attack on HM15's scheme to forge a valid bid of a winning bidder. Section 5 provides some discussions of the price swapping attack and bid forging attack, followed by the conclusion in Section 6.

II. SEALED-BID AUCTION SCHEME

Based on sealed-bid auction (SBA) schemes of HRM13 [7] and HM15 [6], we briefly describe the definition of SBA schemes.

Definition 1. (SBA scheme) SBA scheme consists of 3-tuple algorithms (Setup, Bid, Open):

Setup: The Setup algorithm distributes several parameters such as private parameter of each entity, (i.e., auctioneer, bidder, and sealer) and public parameters.

Bid: The Bid algorithm takes in bidder's secret key. In the Bid algorithm, the bidder selects, seals and submits the bidding price. The Bid algorithm consists of **Seal** and **Verify** processes as follows.

- **Seal:** The Seal process is used to hide the bidder's bidding price. A model consisting multiple layers of sealers is used to seal the given bidding price. The sealing completes after the sealed-bid is published on the bulletin board by the final sealer.
- **Verify:** The Verify process is designed for user verification of his sealed-bid. Through bulletin board, the bidder can verify the published sealed-bid.

Open: The Open algorithm takes in the secret key of auctioneer and the random seed of sealers. The auctioneer evaluates the highest price of the price vector. After extracting the bid, the winning bidder requires to redeem the winning bid from the auctioneer.

A. Security Properties of Sealed-Bid Auction

In order to achieve a secure and reliable sealed-bid auction scheme, three main security properties [16], [17], [8] are required, namely, non-repudiation, anonymity and confidentiality of bid.

III. PRICE SWAPPING ATTACK

A. HRM13's Sealed-Bid Auction Scheme

We describe the HRM13's sealed-bid auction scheme as follows.

Setup: Let p be a large prime such that q is a large prime divisor of $p - 1$, G be a unique subgroup of $\mathbb{Z}_p^*$ of order q , and $g \in \mathbb{Z}_p^*$.

- Set $x_{B_i} \in \mathbb{Z}_p^*$ as the private key and $h_{B_i} = g^{x_{B_i}}$ as the public key of bidder $B_i \in B$.
- Set $x_A \in \mathbb{Z}_p$ as the private key and $h_A = g^{x_A}$ as the public key of auctioneer.
- Using Distributed Key Generation protocol [4], a set of qualified sealers (*QUAL*) with public key of h_S are produced. Each sealer $S_l \in QUAL$ computes the private key of x_l . Any group of $t > k/2$ sealers that seal every bidder's encrypted bid-vector is denoted as $QRM \subseteq QUAL$. Hence, $QRM = \{S_1, S_2, \dots, S_t\}$ and sealer $S_l \in QRM$ randomly selects his sealing key as x_{S_l} .
- Each sealer publishes his public sealing key $h_{S_l} = g^{x_{S_l}}$. $h_{S/S_1, S_2, \dots, S_r} = h_S / h_{S_1} h_{S_2} \dots h_{S_r}$ is the shared public key of sealers. Ultimately, $h_{S/S_1, S_2, \dots, S_t} = 1$ where S_t is the last sealer.
- Select a random $g_y \in \mathbb{Z}_p^*$ as the *YES* mark.
- Assume that maximum estimated price of item is less than 10^D . Auctioneer publishes the price list P consisting of D vectors such that $P = P_{D-1}, P_{D-2}, \dots, P_0$. Assuming that P_i consists of 10 elements, denoted as $P = P_{k9}, P_{k8}, \dots, P_{k0}$.

Bid: Every bidder B_i selects the bidding price σ_i from the list P where $\delta_{D-1}, \delta_{D-2}, \dots, \delta_0$ are decimal values representation of P_{kj} . The $\sigma_i = \delta_{D-1}, \delta_{D-2}, \dots, \delta_0$ be the bidding price in decimal form. P_{kj} marked *YES* by representation of $j = \delta_k$ else $P_{kj} = 1$. For every price index P_{kj} , B_i selects random seeds $r_i, \hat{r}_i \in \mathbb{Z}_p$ and encrypts the price list as follows.

$$\Gamma_i = (X_i, Y_i)$$

$$X_i = g^{r_i}$$

$$Y_i = \begin{cases} (h_A h_S)^{r_i} G_{i,(k,j)} & \text{If } P_{kj} = \text{YES} \\ (h_A h_S)^{r_i} & \text{Otherwise} \end{cases}$$

$G_{i,(k,j)} = \hat{r}_i^{r_i} G^{r_i, (k,j)}$ and the *YES* mark is represented by $G = g_y^{x_{B_i}}$. The bid vector Γ_i could be represented as follows.

$$\Gamma_i = \langle X_{i,(k,j)}, Y_{i,(k,j)} \rangle |_{k=D-1, \dots, 0, j=9, \dots, 0}$$

B_i uses deniable encryption to provide a secure transfer channel over Coercion resistant MIX (*CRM*). The MIX computes the deniable decryption, permutation, and publishes the encrypted bid-vectors to the *QUAL*. The group of sealers perform in the sealing process is indicated as $QRM \subseteq QUAL$. The sealing process involves at least $t > k/2$ sealers participation to achieve the receipt-free bid-vectors. For every sealing process, each sealer performs selection of random seeds $r_{S_l i, (k,j)}, \hat{r}_{S_l i, (k,j)} \in \mathbb{Z}_p$ where $k = D-1, \dots, 0; j = 9, \dots, 0$. Once random seeds are selected, the first sealer performs the sealing process as follows.

$$X_{S_l i, (k,j)} = g_{S_l i, (k,j)}^{r_{S_l i, (k,j)}} X_{i, (k,j)}$$

$$Y_{S_l i, (k,j)} = \hat{r}_{S_l i, (k,j)} (h_A h_{S/S_l})^{r_{S_l i, (k,j)}} X_{i, (k,j)}^{-x_{S_l}} Y_{i, (k,j)}$$

$$R_{S_l i, (k,j)} = \left(\prod_{j=0}^9 \hat{r}_{S_l i, (k,j)} \right)$$

The first sealer outputs $(X_{S_{l-1} i}, Y_{S_{l-1} i}, R_{S_{l-1} i})$ and the subsequent sealers perform sealing process as follows.

$$\begin{aligned} X_{S_l i, (k,j)} &= g_{S_l i, (k,j)}^{r_{S_l i, (k,j)}} X_{S_{l-1} i, (k,j)} \\ Y_{S_l i, (k,j)} &= \hat{r}_{S_l i, (k,j)} (h_A h_{S/S_1, \dots, S_l})^{r_{S_l i, (k,j)}} \\ &\quad X_{S_{l-1} i, (k,j)}^{-x_{S_l}} Y_{S_{l-1} i, (k,j)} \\ R_{S_l i, (k,j)} &= \left(\prod_{j=0}^9 \hat{r}_{S_l i, (k,j)} \right) R_{S_{l-1} i} \\ &= \left(\prod_{j=0}^9 \prod_{t=1}^l \hat{r}_{S_t i, (k,j)} \right) \end{aligned}$$

After all sealers done their sealing processes, the last sealer S_t publishes the $(X_{S_t i, (k,j)}, Y_{S_t i, (k,j)}, R_{S_t i, (k,j)})$ sealed-bid on the bulletin board. Then, the auctioneer computes and publishes $\mathbb{X}_{i,k} = \left(\prod_{j=0}^9 X_{S_t i, (k,j)} \right)^{x_A}$. Next, the bidder is allowed to verify the correctness of his bid using the response published by the sealers as follows.

$$\prod_{j=0}^9 Y_{S_t i, (k,j)} \stackrel{?}{=} R_{S_t i, (k,j)} \mathbb{X}_{i,k} \prod_{j=0}^9 G_{i, (k,j)}$$

Open: After successfully executing the bidding phase, the bids are opened as per the scheduled time. Two sub-processes involved are Evaluation of *YES* Mark (EYM) and Extracting Bid having *YES* Mark (EBY). The EYM needs the cooperation between the sealers and the auctioneer. The price vector is used as input for EYM and outputs the highest price index. Let list $L = \{b_i\}$ be stack of sealed bids. All sealers cooperate and compute $V_{S_l i, (k,j)} = \prod_{X_i, Y_i \in L} \hat{r}_{S_l i, (k,j)}$ for $0 \leq j \leq 9$, the product of all random seeds used to seal the value of bidding price and send privately to the auctioneer. After receiving $V_{S_l i, (k,j)}$ from t sealers, the auctioneer computes evaluation process as follows.

$$\begin{aligned} \mathbb{V}_{k,j} &= \prod_{l=1}^t V_{S_l i, (k,j)} \\ &= \prod_{i=1}^m \prod_{l=1}^t \hat{r}_{S_l i, (k,j)} \\ \mathbb{Y}_{k,j} &= \prod_{b_i \in L} Y_{S_t i, (k,j)} X_{S_t i, (k,j)}^{-x_A} \\ &= \prod_{b_i \in L} \prod_{l=1}^t \hat{r}_{S_l i, (k,j)} [1], j \neq \delta_k \\ &= \prod_{b_i \in L} \prod_{l=1}^t \hat{r}_{S_l i, (k,j)} [G_{i, (k,j)}], j = \delta_k \end{aligned}$$

The auctioneer evaluates and outputs $\mathbb{Y}_{(k,j)}$, $\mathbb{V}_{(k,j)}$, and $\mathbb{G}_{(k,j)} = \mathbb{Y}_{(k,j)} \mathbb{V}_{(k,j)}^{-1}$. If $\mathbb{G}_{(k,j)} \neq 1$ then EBY process started.

EBY inputs the highest price index and outputs the list of sealed-bids that contain *YES* mark on the price index. List L is divided into two halves, $L1$ and $L2$. Then all sealers involved cooperate to compute $V_{S_l i, (k,j)}$ and the auctioneer

recalculates the $\mathbb{V}_{k,j}$ and $\mathbb{Y}_{k,j}$ for $L1$ and $L2$. The resultant values of $\mathbb{G}_1$ and $\mathbb{G}_2$ represent the respective lists, $L1$ and $L2$.

The checking for $L1$ is as follows. If $\mathbb{G}_1 \neq 1$ and $L1 \geq 2$ then the process of EBY repeats. Else, proceed to swapping algorithm for the list that contains YES mark. The similar checking is carried out for $L2$.

The swapping algorithm is as follows. Let the inputs be $L = \{b_1, b_2\}, V_o = \{v_1, v_2\}$. Using the $V_{S_l(k,j)}$ from t sealers, repeats $(\mathbb{Y}_{(k,j)})$ and $(\mathbb{V}_{(k,j)})$ the evaluation process to find $\mathbb{G}_{(k,j)} \neq 1$ (determines the location of YES mark).

If the YES mark located at price index P_{D-1, w_D-1} is found, the auctioneer carries out similar process until the whole winning price is $w = w_D \dots w_0$ and the list of winning bid L_0 is determined.

The auction mechanism determines the winning bid, but the identity of winner is unknown. Once the auctioneer announced the winning bid, the winning bidder comes forward to claim his winning by executing a zero-knowledge protocol with the auctioneer to verify his winning. Let w_k be his winning price for $k = 0, 1, \dots, D-1$, B_i be the winning bidder that selects $a \in \mathbb{Z}_p$, computes and sends $\alpha = g^a$ and $\beta = g_y^a$ to auctioneer. The auctioneer randomly selects $c \in \mathbb{Z}_p$ and sends to B_i . Note that, a correction has been made to the minor typing error occurs in zero-knowledge protocol's equation of the original scheme. Then, the bidder computes and sends $r = a + cx_{B_i}$ to the auctioneer. Upon receiving r , the auctioneer proves that $g_y^{x_{B_i}}$ and h_{B_i} have the common exponent over g_y and g respectively as follows.

$$\begin{aligned} g^r &\stackrel{?}{=} \alpha h_{B_i}^c \\ g_y^r &\stackrel{?}{=} \beta (g_y^{x_{B_i}})^c \end{aligned}$$

B_i discloses the random seed $\hat{r}_i$ and proves that X_i and $G_{i,(k,w_k)} \hat{r}_i^{-1}$ have similar exponent over g and $g_y^{x_{B_i}}$ respectively. The bidder computes $\hat{R}_i = \prod_{k=0}^{D-1} \hat{r}_{i,(k,w_k)}$. The sealers compute $\hat{R}_{S_l} = \prod_{k=0}^{D-1} \hat{r}_{S_l,i,(k,w_k)}$ and $R_{S_l} = \sum_{k=0}^{D-1} r_{S_l,i,(k,w_k)}$. The auctioneer computes as follows.

$$\begin{aligned} X_i &= \prod_{k=0}^{D-1} X_{S_l,i,(k,w_k)} (g^{\sum_{l=1}^t R_{S_l}})^{-1} \\ \mathbb{G} &= \prod_{k=0}^{D-1} G_{i,(k,w_k)} (\hat{R}_i)^{-1} \end{aligned}$$

B. The Attack

In this section, we show how to mount a variant of known-bid attack, namely, the price swapping attack on [7]. In particular, we consider a malicious first sealer who can successfully randomize the order of the bid without being detected. The resultant bid undergoes the validation of **Open** algorithm to prove that the bid belongs to the particular bidder. Using the knowledge of the system public parameters $(\Gamma_i, h_{B_i}, h_A, h_{S_i})$, the malicious first sealer as adversary A , can mount the attack as follows:

- 1) Once adversary A receives Γ_i that contains $X_{i,(k,j)}$ and $Y_{i,(k,j)}$ from bidder through CRM , A performs randomization process. For illustration purpose, let us consider the case of dimension $0 \leq k \leq 4$ and the available price range is $0 \leq j \leq 9$. A can perform row swaps of the top row and bottom row in the bid vector as follows:

$$\begin{array}{ccc} X_{i,(3,0)}, Y_{i,(3,0)} & \cdots & X_{i,(3,9)}, Y_{i,(3,9)} \\ \vdots & \ddots & \vdots \\ X_{i,(0,0)}, Y_{i,(0,0)} & \cdots & X_{i,(0,9)}, Y_{i,(0,9)} \\ & \downarrow & \\ X_{i,(0,0)}, Y_{i,(0,0)} & \cdots & X_{i,(0,9)}, Y_{i,(0,9)} \\ \vdots & \ddots & \vdots \\ X_{i,(3,0)}, Y_{i,(3,0)} & \cdots & X_{i,(3,9)}, Y_{i,(3,9)} \end{array}$$

A also can perform position swaps of j at the position '0' and '1' in a specific row illustrated as follows.

$$\begin{array}{cccc} X_{i,(k,0)}, Y_{i,(k,0)} & X_{i,(k,1)}, Y_{i,(k,1)} & \cdots & X_n, Y_n \\ & \downarrow & & \\ X_{i,(k,1)}, Y_{i,(k,1)} & X_{i,(k,0)}, Y_{i,(k,0)} & \cdots & X_n, Y_n \end{array}$$

- 2) A proceeds to the sealing process with the randomized bid vector. After A seals the randomized bid vector, A passes the sealed-bid to the subsequent sealer for the sealing process as usual.
- 3) Finally, the last sealer seals and publishes $(X_{S_{ti}}, R_{S_{ti}}, Y_{S_{ti}}, R_{S_{ti}})$ on the bulletin board. Then, the auctioneer publishes $\mathbb{X}_{i,k} = (\prod_{j=0}^9 X_{S_{ti},i,(k,j)})^{x_A}$ on the bulletin board.
- 4) In the **Open** algorithm, the auctioneer opens and reveals the highest bidding price. Assuming that the randomized bidding price came out as the highest bid, no bidder will come forth to claim the bid and this results in an ambiguous case.
- 5) In the occurrence of the ambiguous case, the auctioneer finds out the winning bidder through zero knowledge protocol. The suspected bidder selects $a \in \mathbb{Z}_p$, computes and sends $\alpha = g^a$ and $\beta = g_y^a$ to the auctioneer. The auctioneer selects and sends $c \in \mathbb{Z}_p$ to the bidder. The bidder computes and sends $r = a + cx_{B_i}$ to the auctioneer. The evaluation of YES mark is computed as follows.

$$\begin{aligned} g^r &\stackrel{?}{=} \alpha h_{B_i}^c \\ g_y^r &\stackrel{?}{=} \beta (g_y^{x_{B_i}})^c \end{aligned}$$

The bidder computes the product of random seeds $\hat{R}_i = \prod_{k=0}^{D-1} \hat{r}_{i,(k,w_k)}$. The sealers compute $\hat{R}_{S_l} = \prod_{k=0}^{D-1} \hat{r}_{S_l,i,(k,w_k)}$ and $R_{S_l} = \sum_{k=0}^{D-1} r_{S_l,i,(k,w_k)}$. The eval-

uation of zero knowledge protocol provides verification of bid validity of the bidder as follows:

$$X_i = \prod_{k=0}^{D-1} X_{S_i, i, (k, w_k)} (g^{\sum_{l=1}^t R_{S_l}})^{-1}$$

$$\mathbb{G} = \prod_{k=0}^{D-1} G_{i, (k, w_k)} (\hat{R}_i)^{-1}$$

The bidder selects $b \in \mathbb{Z}_p$, computes and sends $\alpha_2 = g^b$ and $\beta_2 = g_y^{x_{B_i}}$ to the auctioneer. The auctioneer selects and sends $d \in \mathbb{Z}_p$ to bidder. The bidder computes and sends $r = b + d(res)$ to the auctioneer, where $res = \sum_{k=0}^{D-1} r_{i, (k, w_k)}$. The verification of bid validity is computed as follows.

$$g^r \stackrel{?}{=} \alpha_2 X_i^d$$

$$(g_y^{x_{B_i}})^r \stackrel{?}{=} \beta_2 (\mathbb{G})^d$$

Notice that when the swapped bid was displayed on bulletin, the actual bidder is not able to perform the verification for the randomized bid. The bidder can then raise a complaint regarding the alteration made towards his bid. Upon receiving the complaint, the auctioneer will run the zero knowledge protocol as in step 5 in the attack to confirm if the bid is corrupted. However, the result of zero-knowledge protocol turns out that the bid is valid and the complaint is not convincing. In other words, the complaint is no difference from a fake complaint of regretting a mistaken bid.

IV. KNOWN-BID ATTACK

A. HM15's Sealed-Sid Auction Scheme

Due to similarities with HRM13's scheme [7], we summarize and highlight only the relevant portion as follows.

Setup: Similar to **Setup** in Section III-A.

Bid: Similar to **Bid** in Section III-A.

Open: Similar to **Open** in Section III-A. A significant difference found in the sub-process known as **Trade**. **Trade** is used to determine the winner since the winning bid is anonymous. Let bidder B_i be the winning bidder who reveals the *YES* mark, $G = g_y^{x_{B_i}}$, and all her secret seeds, $r_{i, (k, w_k)}$ and $\hat{r}_{i, (k, w_k)}$ for $k = 0, 1, \dots, D-1$. Similarly, every sealers reveal all their secret seeds, $\hat{r}_{S_i, i, (...)}$ and $r_{S_i, i, (...)}$. The revelation enables the auctioneer to perform the verification of winning bidder identity. For detailed algorithm, please refer to [6].

B. The Attack

In the **Trade** of HM15 [6], it stated that the bidder reveals all her secret seeds when she claims the winning bid. With the revelation of the *YES* mark and the bidder's secret seeds of $r_{i, (k, w_k)}$ and $\hat{r}_{i, (k, w_k)}$, we show that a malicious auctioneer A_2 , is able to forge a valid bid. In the auction scheme, **Trade**

exposes $g_y^{x_{B_i}}$ of the winning bidder. A_2 can perform bid forging as follows.

- 1) The bidder creates $g_y \in \mathbb{Z}_p^*$ and performs the bidding.
- 2) In **Trade**, A_2 gets the value of $g_y^{x_{B_i}}$.
- 3) A_2 alters the value into $g_y^{k x_{B_i}} = (g_y^{x_{B_i}})^k$ where $k \in \mathbb{Z}_p^*$ is selected randomly.

The auctioneer can always make the winning bidder bids for the highest price in the subsequent round of the auction. When the bidder raises complaint or performs verification on the bid, the bid is always valid because the bidder's secret key, x_{B_i} is bound with the *YES* mark. In this attack, the success rate is always 100% on the winning bidder in the subsequent auction.

V. DISCUSSION

HRM13 [7] and HM15 [6] assumed some of the sealers are malicious, i.e. some sealers are corruptible and no assumption of honest sealers are required. Thus, there exists the possibility that the first sealer is dishonest.

The similarities found on both schemes are that both contain three algorithms, namely, {Setup, Bid, Open}, similar bid component $\Gamma_i = (X_i, Y_i)$ and price list P . Since similar bid structure is used in HRM13 and HM15, the price swapping attack mounted on HRM13 is also applicable to HM15.

The causes of the price swapping attack are the usage of matrices vector as price indication and the identity of the bidder which is only bound to the *YES* mark. The use of bid-vectors causes alteration on the price; when the identity of the bidder only binds to the *YES* mark, this further simplified the attack.

As for the remedial action for the price swapping attack, we propose an integration with a designated confirmer signature scheme [18] in the bidding stage where the bidder is required to create and publish an extra signature on the bid vector Γ_i that includes the placement of *YES* mark. With the publication of Γ_i , the bidder who suffers from the price swapping attack can now prove that alterations have been done on his bid by running the confirmation and disavowal protocols of the designated confirmer signature. Besides that, the security properties required, namely, bidder's anonymity and confidentiality of bid remain intact with the integration of a designated confirmer signature.

In the second known-bid attack, revelation of *YES* mark and all the winning bidder's secret seeds cause the malicious auctioneer to extract the values $g_y^{x_{B_i}}$. Since this is a fundamental flaw, we do not recommend any solution for the problem. As the alternatives, we recommend the use of the fixed HRM13 and other secure schemes, such as [16], [8], [17], [10], [12], [13].

VI. CONCLUSION

We presented a known-bid attack on HRM13's scheme [7] and HM15's scheme [6] respectively. In the former, we showed that a malicious first sealer can randomize the bidding price without corrupting the bid; in the latter, we show that a malicious auctioneer in HM15's scheme [6] can forge a

bidder's bid after he won once. We managed to repair the former scheme by using a designated confirmer signature but not the latter which is vitally defected.

VII. ACKNOWLEDGMENT

The authors would like to thank the Malaysia government's Fundamental Research Grant Schemes (FRGS/2/2014/ICT04/MMU/03/1) and (FRGS/1/2015/ICT04/MMU/03/5) for supporting this work.

REFERENCES

- [1] Abe, M., Suzuki, K.: Receipt-free sealed-bid auction Information Security: 5th International Conference, ISC 2002 Sao Paulo, 191-199 (2002)
- [2] Chen, X., Lee, B., Kim, K.: Receipt-free electronic auction schemes using homomorphic encryption, Information Security and Cryptology - ICISC 2003: 6th International Conference, 259-273 (2003)
- [3] Franklin, M.K., Reiter M.K.: The design and implementation of a secure auction service, IEEE Transactions on Software Engineering, 302-312 (1996)
- [4] Gennaro, R., Jarecki, S., Krawczyk, H., Rabin, T.: Secure distributed key generation for discrete-log based cryptosystems, Journal of Cryptology, 51-83 (2007)
- [5] Howlader, J., Ghosh, A., Pal, T.D.: Secure receipt-free sealed-bid electronic auction, Contemporary Computing: Second International Conference, IC3 2009, Noida, India, 228-239 (2009)
- [6] Howlader, J., Mal, A.K.: Sealed-bid auction: a cryptographic solution to bid-rigging attack in the collusive environment. Security and Communication Networks, 3415-3440 (2015)
- [7] Howlader, J., Mal, A.K., Roy, S.K.: Practical receipt-free sealed-bid auction in the coercive environment, In International Conference on Information Security and Cryptology, 418-434 (2013)
- [8] Lee, C.C., Ho, P.F., Hwang, M.S.: A secure e-auction scheme based on group signatures, Information Systems Frontiers, 11(3), 335-343 (2009)
- [9] Liaw, H.T., Juang, W.S., Lin, C.K.: An electronic online bidding auction protocol with both security and efficiency, Applied mathematics and computation, 174(2), 1487-1497 (2006)
- [10] Li, M.J., Juan, J.S. T., Tsai, J.H.C.: Practical electronic auction scheme with strong anonymity and bidding privacy, Information Sciences, 181(12), 2576-2586 (2011)
- [11] McAfee, R.P., McMillan, J.: Auctions and bidding, Journal of Economic Literature, 699-738 (1987)
- [12] Montenegro, J.A., Lopez, J.: A practical solution for sealed bid and multi-currency auctions, Computers & Security, vol 45, 186-198 (2014)
- [13] Nojoumian, M., Stinson, D.R.: Efficient sealed-bid auction protocols using verifiable secret sharing, International Conference on Information Security Practice and Experience, 302-317 (2014)
- [14] Juels A., Catalano, D., Jakobsson, M.: Coercion-resistant electronic elections, ACM workshop on Privacy in the electronic society, 61-70 (2005)
- [15] Sakurai, K., Miyazaki, S.: An anonymous electronic bidding protocol based on a new convertible group signature scheme, Lecture Notes in Computer Science, 385-399 (2000)
- [16] Wu, C.C., Chang, C.C., Lin, I.C.: New sealed-bid electronic auction with fairness, security and efficiency, Journal of Computer Science and Technology, 253-264 (2008)
- [17] Xiong, H., Qin, Z., Li, F.: An anonymous sealed-bid electronic auction based on ring signature, International Journal of Network Security, 8(3), 235-242 (2009)
- [18] Zeng, S., Xiong, H.: Privacy-enhanced designated confirmer signature without random oracles, International Journal of Network Security, 16(5), 331-339 (2014)



Kin-Woon Yeow is a M.Sc. (I.T.) student under the Faculty of Information Science and Technology in Multimedia University, Malaysia. His research interests are applied cryptography and network security.



Swee-Huay Heng received her B.Sc (Hons) and M.Sc degrees from Universiti Putra Malaysia (UPM), and her Doctor of Engineering degree from the Tokyo Institute of Technology, Japan. She currently holds the position of Professor in the Faculty of Information Science and Technology, Multimedia University, Malaysia. Her research interest is in Cryptography and Information Security. She served in numerous technical Program Committees of international security conferences.



Syh-Yuan Tan received his Ph.D. from Universiti Tunku Abdul Rahman in 2015. He is currently attached to the Faculty of Information Science and Technology, Multimedia University, Malaysia as a senior lecturer. His research interests are Cryptography and Network Security, particularly on the provable security techniques.