# 國立交通大學

## 資訊科學系

## 碩士論文

# 可公開驗證出價合法性的彌封式拍賣系統

A Sealed-Bid Auction
with Publicly Verifiable Bid Validity

研 究 生：黃佩琳

指導教授：曾文貴　教授

中華民國 九十三 年六月

# 可公開驗證出價合法性的彌封式拍賣系統
# A Sealed-Bid Auction with Publicly Verifiable Bid Validity


研究生：黃佩琳　　Student：Pei-Lin Huang

指導教授：曾文貴　　Advisor：Wen-Guey Tzeng

國立交通大學

資訊科學系


碩士論文

A Thesis

Submitted to Department of Computer and Information Science

College of Electrical Engineering and Computer Science

National Chiao Tung University

in partial Fulfillment of the Requirements

for the Degree of

Master

in

Computer and Information Science

June 2004

Hsinchu, Taiwan, Republic of China

中華民國九十三年六月

# 可公開驗證出價合法性的彌封式拍賣系統

學生: 黃佩琳　　指導教授: 曾文貴 博士

資訊科學系

國立交通大學

## 摘要

我們提出了一個具有可公開驗證出價合法性的拍賣系統。我們的想法結合了可驗證的加密知識簽章系統及公開金鑰之重新加密的證明。我們在對管理者的設計上，使用了兩種不同的管理者，註冊管理者及拍賣管理者，避免僅用一種管理者而使得管理者的權限過大。註冊管理者確認出價者的身分及其公開金鑰之間的對應關係，拍賣管理者則是管理拍賣時的一切活動。在我們的系統中，出價合法性不只包括了對出價價格的合法性更包括了出價者身分的合法性。我們最主要的設計便是使任何第三者都可以公開的驗證出價者出價的合法性卻又得不到與出價者身分及出價價格相關的任何訊息。如果任何人發現有不合法的出價都可以向拍賣管理者檢舉進而要求拍賣管理者撤銷該筆出價。因此我們的系統可以抵抗惡意的出價者提出不合法的出價干擾拍賣。

除此之外，在我們的系統中，我們將出價者的簽章和出價價格結合當做出價內容。而我們系統中所使用的簽章簽名時需要出價者所記憶的密碼與儲存在出價者可攜式裝置中的部分私鑰一同配合使用，藉以增加安全性。

**關鍵字**: 彌封式拍賣，可公開驗證，出價合法性

# A Sealed-Bid Auction with Publicly Verifiable Bid Validity

Student: Pei-Lin Huang Advisor: Dr. Wen-Guey Tzeng

Department of Computer and Information Science

National Chiao Tung University

## Abstract

We proposed a sealed-bid auction with publicly verifiable bid validity, which is based on verifiable encryption of signature of knowledge and 1-out-of-P re-encryption proof of encryption keys. In our scheme, we have two semi-trusted managers, the registration manager RM and the auction manager AM. The registration manager RM guarantees the relationship between a bidder and his corresponding public key. The auction manager AM holds an auction and manages operations in an auction. Bid validity in our scheme contains the validity of both bidding price and the bidder. In our scheme, every one can verify the validity of the bid, but he can not get any information about the relation of the bidder's identity and his bidding price. If there are invalid bids, anyone can ask the auction manager AM to revoke them. Hence, our scheme can prevent malicious bidders to disturb the auction.

Besides, in our scheme, we combine the bidder's signature and his bidding price as the bid. The signature we use here needs the bidder's password memorized in his mind and the corresponding partial secret stored in his mobile device to increase the security.

**Keywords:** Sealed-Bid Auction, Publicly Verifiable, Bid Validity

# 誌謝

在此感謝我的指導老師曾文貴教授，在我碩士班兩年的學習過程中，不只讓我在學業上受益良多，更在生活上以及言行上給我許多教導。此外，我要感謝口試委員，交大資工系蔡錫鈞教授和清大資工系孫宏民教授，在論文上給予我許多良好的建議和指導，讓我的論文更加完善。除此之外我要感謝實驗室同學，尚宸、兆儀、振魁和坤杉的幫忙，實驗室學長成康、惠龍，學姊季穎的指導，以及實驗室學弟妹們在精神方面的鼓勵。

最後，我要感謝我的家人，不論在精神或物質上都給予我極大的支持，讓我在無後顧之憂的情況下可以順利完成學業。在此，謹以此文獻給我所有我想要感謝的人。

# Table of Contents

摘要 ..... i

Abstract ..... ii

誌謝 ..... iii

Table of Contents ..... iv

Chapter 1 Introduction ..... 1

1.1 Auction Types ..... 2

1.2 The Properties of Sealed-Bid Auctions ..... 4

1.3 Thesis organization ..... 5

Chapter 2 Preliminaries ..... 7

2.1 Interactive Zero-Knowledge Proof System of Knowledge ..... 7

2.2 Signature of Knowledge ..... 11

2.3 Verifiable Encryption of Signature of Knowledge ..... 12

2.4 1-out-of-P Re-encryption Proof of Encryption Keys ..... 15

2.5 Previous Electronic Auction Schemes ..... 18

Chapter 3 A Sealed-Bid Auction with Publicly Verifiable Bid Validity ... 22

3.1 Notations ..... 23

3.2 Our Basic Scheme ..... 24

3.3 Analysis.....32

3.3.1 Security .....32

3.3.2 Properties .....40

Chapter 4 Conclusion.....43

Bibliography .....45

# Chapter 1

# Introduction

Electronic commerce has made a rapid progress in recent years. We can find out that more and more economic transactions are conducted through auctions. As we know, there are many famous auction websites, such as Yahoo!, eBay, and so on.

In this thesis, we propose a sealed-bid auction with publicly verifiable bid validity. Our scheme is one of the first-price sealed-bid auctions. It has the properties of correctness, confidentiality, fairness, privacy, public verifiability, and robustness. Most important of all, our scheme can publicly verify the validity of the bids such that the invalid bids sent by malicious bidders can not disturb the auction.

In our scheme, we combine the bidder's signature and his bidding price as the bid using verifiable encryption of signature of knowledge, i.e. the bidder encrypts his signature using the encryption key corresponding to his bidding price, to let the others can verify the validity of the bidder, and then use 1-out-of-P re-encryption proof of encryption keys to make the others can not distinguish which encryption key the bidder uses. The signature we use here needs the bidder's password memorized in his mind and the corresponding partial secret stored in his mobile device to increase the security. We use the idea proposed in [15] that use both password and partial secret to achieve strong security. It prevents the dictionary attack that if only the password is used. It also provides basic security that the attacker need guess the password if the mobile device is lost.

Besides, similar to [6], in our scheme, we use two kinds of semi-trusted

managers, the registration manager RM and the auction manager AM, to avoid concentration of all power in a single manager. The registration manager RM guarantees the relationship between a bidder and his corresponding public key. The auction manager AM holds auctions and manages operations in an auction. Bid validity in our scheme contains not only the validity of bidding price but also the validity of the bidder. In our scheme, every one can verify the bid validity but he can not get any information about the relation of the bidder's identity and his bidding prices. If there exist some invalid bids, anyone can ask the auction manager AM to revoke those invalid bids. Hence, our protocol can prevent malicious bidders to disturb the auction.

## 1.1Auction Types

There are many different types of auctions. From [10], we can find out four basic types of auctions that are widely considered and analyzed: the increasing-price auction (also called English auction), the first-price sealed-bid auction, and the second-price sealed-bid auction (also called the Vickery auction), the decreasing-price auction (also called the Dutch auction). In the following, we describe their rules on the sale of a single item for simplicity.

***1. The increasing-price auction***

In this type of auction, an item is offered at increasing prices. At the beginning, it may be offered at $K$ tokens, and then at successive points of time $i$, it is bid at $K + i * \Delta$ tokens ($\Delta$ may be a function of previous bids and other factors). At each time period, one or more bidders can bid for the item. At the end

of the auction, the highest bidder takes the item and pays the price he bids. This type of auction has many disadvantages such as that the time needed to conduct the auction is potentially proportional to the price which the item is sold. Besides, this type of auction leaks a lot of information such that a careful observer will be able to conclude information about the price that each bidder is willing to pay for the auctioned item. However, the auction does have a very desirable feature: in economic terms, it allocates the item to the bidder with the highest valuation, since the bidder with the highest valuation will be willing to outbid all other bidders.

***2. The first-price sealed-bid auction***

In this type of auction, each bidder sends a sealed bid to an auctioneer who opens all bids. The auctioneer determines the highest bid and sells the item to the highest bidder for his bidding price. Though, this type of auction can be executed in a single round of communication between the bidders and the auctioneer, it has some disadvantages. For example, the auctioneer will know the exact price that each bidder is willing to pay. Moreover, it does not support the optimal distribution of the item.

In a sealed bid auction, bidders have beliefs about what others will bid. If a bidder believes that he has the highest bid and the second highest bid will substantially beneath that, then he has an incentive to lower his bid. For example, if he values an item at $1000, but he believes that the second highest bidder values the item at $500, then he is likely to place a bid slightly higher than $500. If the bidder is wrong about the distribution of other bids, then the final item will not be sold to him and the seller will be given a lower price than he would be

given in the increasing-price auction.

***3. The second-price sealed-bid auction***

It is a type of auction that combines the best features of the increasing-price bid and the sealed-bid auction. In this type of auction, each bidder submits a single bid to the auctioneer respectively, without seeing others' bids, and the object is sold to the bidder who makes the highest bid. However, the price he pays is the second-highest bidder's bid, or "second price". This auction is sometimes called a Vickery auction after William Vickery, who wrote the seminal (1961) paper on auctions.

***4. The decreasing-price auction***

This type of auction is similar to the increasing-price auction in which the bidding price varies over time. However, in this type of auction, the price decreases and at time $i$ is $K - i * \Delta$ tokens. The first bidder will take the item. This type of auction has the advantage of preserving maximum privacy, i.e. no information is revealed except the winning bid and bidder. However, like the increasing-price auction, it may be time consuming, and like the sealed-bid auction, it is not economically efficient.

## 1.2 The Properties of Sealed-Bid Auctions

After introducing the auction types, we present the properties of sealed-bid actions we concern.

***1. Correctness***

If all parties act honestly, the winning price and the winner(s) are determined

according to the auction rules correctly.

2. ***Confidentiality*** (of sealed bids)

   No bid information is revealed to any party (including the auctioneer) until the bid opening phase.

3. ***Fairness***

   - All bidders can look a proper polling on Internet.
   - 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-deniability.

4. ***Privacy*** (of losing bids)

   The losing bids remain confidential until the end of the auction even to the auctioneer. Differences between privacy and confidentiality of bids include

   - Privacy only deals with losing bids;
   - Privacy is the confidentiality of the losing bids even after the bid opening phase.

5. ***Public Verifiability***

   The validity of the result of the auction can be publicly verified by every one.

6. ***Robustness***

   Even if malicious bidders send invalid bids, the auction process is unaffected. In other words, the result of the auction is still correct even under the attack of malicious bidders.

## 1.3 Thesis organization

The remainder of his thesis is organized as follows: In Chapter 2, we shall briefly introduce the related theories and schemes. Then, we propose a sealed-bid auction with publicly verifiable bid validity and analyze its properties in Chapter 3. Finally, in Chapter 4, we conclude this thesis and indicate some future directions.

# Chapter 2

# Preliminaries

In this chapter, we will introduce some important theories and schemes that are involved in our scheme. In section 2.1, we will give the introduction about interactive zero-knowledge proof system of knowledge. In section 2.2, we will give basic idea of signature of knowledge. In section 2.3, we will introduce the definition of verifiable encryption of signature of knowledge. In section 2.4, we will state what 1-out-of-P re-encryption of encryption keys is and the difference between 1-out-of-P re-encryption proof and 1-out-of-P re-encryption proof of encryption keys. In section 2.5, we will introduce other auction schemes.

## 2.1 Interactive Zero-Knowledge Proof System of Knowledge

An interactive proof system $\langle P,V \rangle$ consists of two Turning machines P and V, called “Prover” and “Verifier”, respectively.

A typical interactive proof system has three rounds (commit-challenge-response). P first commits to a value. V then challenges on of two things: either the commitment has the right form or P knows the witness. P then responds to the challenge, while reveals no information about the witness. The real witness is randomized by the committed value in the first step.

Consider the problem that the prover wants to prove that he knows the discrete

logarithm $x = \log_g y \bmod p$ of *(p, q, y)* where $p = 2q+1$, $p$, $q$ are primes, $g \in G_q - \{1\}$, and $g \in G_q$. We want to show that P really know the value $x$. We call this type of proof "proof of knowledge".

In the setting of proof of knowledge, we require that the prover P be a polynomial-time probabilistic Turing machine (PTM) with a private input (witness). We consider the binary predicate $Q$ such that for an input instance $x$ of the right form, there is a corresponding secret $\rho$ such that $Q(x, \rho) = 1$. The proof system of knowledge for $Q$ is to show that the prover P knows a witness $\rho$ for an input instance $x$. We use $\langle P(\rho), V \rangle(x)$ to denote the interactive proof system of P and V such that $x$ is the public common input and $\rho$ is the prover P's private input. If $\langle P(\rho), V \rangle(x) = 1$, it means that the verifier V accepts that the prover P really knows the witness; otherwise, it means that the verifier rejects.

Moreover, if we want to show that the interactive proof system of knowledge is zero-knowledge, we require that the interaction of the prover and the verifier can be simulated.

***Definition 2.1(Interactive Zero-Knowledge Proof System of Knowledge)***

Let P and V be both polynomial-time PTM's. An interactive zero-knowledge proof system of knowledge $\langle P, V \rangle$ for the binary predicate Q satisfies the following three conditions:

**1. *Completeness***

$\forall$x and $\forall\rho$ with Q(x, $\rho$) = 1, $\Pr[\langle P(\rho), V \rangle(x) = 1] = 1$.

**2. *Soundness***

There is a probabilistic (expected) polynomial-time knowledge extractor E such that $\forall x \in \text{Dom}(Q)$, $\forall P^*$

$$\Pr\left[\left\langle P^*(\rho), V\right\rangle(x) = 1\right] \geq \frac{1}{p(|x|)} \Rightarrow \Pr\left[E(P^*, V, x) = \rho^*, Q(x, \rho^*) = 1\right] \geq 1 - \varepsilon(|x|)$$

where Dom(Q) means the domain of Q, p(·) is a polynomial, and ε(·) is negligible.

**3. *Zero-knowledge***

For each verifier $V^*$, there is a simulator $M_{V^*}$ such that the following two distributions are polynomially indistinguishable:

- $\left\{\left\langle P(\rho), V^*\right\rangle(x)\right\}_{x \in Dom(Q), Q(x,\rho)=1}$;
- $\left\{M_{V^*}(x)\right\}_{x \in Dom(Q)}$.

Notice in the definition 2.1, we have "for each verifier $V^*$, there is a simulator", while in reality, we usually use a stronger statement "there is a *universal* simulator $M^*$ for every verifier".

To be proof-oriented, the (universal) simulator simulates the "view" of the verifier $V^*$ interacting with P on common public input x and P's private input is $\rho$. Here, "view" means the transcript (messages) exchanged by P and $V^*$.

Combining the universal simulator and the view concept, we have an alternative definition for zero-knowledge.

***Definition 2.2(Zero-Knowledge based on view and universal simulator)***

An interactive proof system of knowledge $\left\langle P(\rho), V\right\rangle(x)$ is (computational) zero-knowledge if there is a universal simulator $M^*$ such that for every possible verifier $V^*$, the following two distributions are polynomially indistinguishable, where

$M^*$ runs in expected polynomial time depending on the run time of $V^*$.

- $\{View(P(\rho), V^*, x)\}_{x \in Dom(Q), Q(x,\rho)=1}$;
- $\{M^*(V^*, x)\}_{x \in Dom(Q)}$.

Furthermore, if the real transcript $View(P(\rho), V^*, x)$ and the simulated one $M^*(V^*, x)$ are identical, the system is called a *perfect zero-knowledge* interactive proof system of knowledge.

From the above, we know that if we want to show that the interactive poof system of knowledge is zero-knowledge, we have to ensure the distributions of the simulated one and the real transcript are polynomially indistinguishable.

For simplicity, we allow the simulator $M^*$ to output $\perp$, denoting a failure round of simulation. We have another alternative definition for zero-knowledge.

***Definition 2.3(Zero-Knowledge failure)***

An interactive proof system of knowledge $\langle P(\rho), V \rangle(x)$ is (computational) zero-knowledge if for every possible verifier $V^*$, the following two distributions are polynomially indistinguishable:

- $\{View(P(\rho), V^*, x)\}_{x \in Dom(Q), Q(x,\rho)=1}$;
- $\{m^*(V^*, x)\}_{x \in Dom(Q)}$.

where $m^*(V^*, x)$ the random valuable $M^*(V^*, x)$ conditioned on $M^*(V^*, x) \neq \perp$, that is, for all z, $\Pr[m^*(V^*, x) = z] = \Pr[M^*(V^*, x) = z \mid M^*(V^*, x) \neq \perp]$ and $\Pr[M^*(V^*, x) \neq \perp]$ is non-negligible.

In the following, we will give some basic idea of non-interactive proof system.

In non-interactive proof system, the prover P produces a string of showing all the properties of an interactive proof system without interacting with the verifier. Hence, we need a random source to replace the verifier's role in the interactive system. The more realistic is to use a secure (collision-resistant) hash function H in place of the verifier.

## 2.2 Signature of Knowledge

Signature of knowledge is a non-interactive zero-knowledge proof of knowledge, but being dependent on message *m*.

For example, if the system's public parameters are a large prime *p* where *p=2q + 1*, *q* is also a large prime, a generator g of $G_q$, and a secure (collision resistant) hash function $H(\cdot):\{0,1\}^* \rightarrow Z_q$. A user, said Bob, whose secret key is x and public key is $y = g^x \bmod p$. Now, if Bob wants to sign for a message m, the pair $(c, w)$ that satisfies $c = H(m, p, g, y, g^r \bmod p)$ and $w = r - cx$ where $r \in_R Z_q$ is the signature of knowledge $x = \log_g y \bmod p$ on message m. By checking c = c', we can verify the signature on $m$ where $c' = H(m, p, y, g^w y^c \bmod p)$. This is because $g^w y^c \bmod p = g^{r-cx}(g^x)^c \bmod p = g^r \bmod p$.

Besides, in the above example, we can find out that we can also use the pair (*a, w*) to be the signature of knowledge $x = \log_g y \bmod p$ for Bob on message m. The verifier can first compute $c = H(m, p, g, y, a)$ and then verify if $a = g^w y^c \bmod p$. This is because $g^w y^c \bmod p = g^{r-cx}(g^x)^c \bmod p = g^r \bmod p = a$.

Similar to our scheme, the system's public parameters are a large prime *p* where

$p = 2q + 1$, $q$ is a large prime, two generator $g$ and $h$ of $G_q$, and a collision resistant hash function $H(\cdot):\{0,1\}^* \rightarrow Z_q$. A user, said Bob, whose secret key contains the password $\pi$ memorized in his mind and the corresponding partial secret $\alpha$ stored in his mobile device and public key is $y = g^{\alpha} h^{\pi} \bmod p$. Now, if Bob wants to sign on message m, he first computes $a = g^{r_1} h^{r_2} \bmod p$, $c = H(m, p, g, h, y, a)$, $w_1 = r_1 - c\alpha$, and $w_2 = r_2 - c\pi$ where $r_1, r_2 \in_R Z_q$, and then publishes $(a, w_1, w_2)$ as his signature of knowledge of $\alpha$ and $\pi$ such that $y = g^{\alpha} h^{\pi} \bmod p$ on message m. The verifier can verify by first computing $c = H(m, p, g, h, y, a)$ and then verifying if $a = g^{w_1} h^{w_2} y^c \bmod p$. This is because

$$g^{w_1} h^{w_2} y^c \bmod p = g^{r_1 - c\alpha} h^{r_2 - c\pi} \left(g^{\alpha} h^{\pi}\right)^c \bmod p = g^{r_1} h^{r_2} \bmod p = a$$

## 2.3 Verifiable Encryption of Signature of Knowledge

Verifiable encryption is an encryption scheme where one can prove some property of data S, which is given in encrypted form. When the encryption scheme is secure, the encrypted data should reveal no information regard S.

The setting of a verifiable encryption scheme is a two-party protocol between a prover P and a verifier V. Their common inputs are a public key *Y*, public value *m*, and a binary predicate *Q*. As a result of the protocol, V either rejects, or being convinced that the encryption of some value S under Y satisfies (*m*, S)$\in Q$. For example, *Q* is defined such that (*m*, S) $\in Q$ if and only if S is a signature of on message *m* with respect to some fixed public key *Y*. In other word, P convinces V that the encrypted data is a valid signature on *m*.

The two-party protocol should ensure that V accepts an encryption of an invalid

S with only negligible probability. Moreover, V should learn nothing except the fact that S is a valid signature with respect to *m*.

The encryption key can belong to P, but typically belongs to a third party, and even in this case the third party should not need to take part in the protocol. In other words, P does not need to know the secret key (decryption key) *X* corresponding to public key (encryption key) *Y*.

We find a definition of a secure verifiable scheme for a relation following [5].

***Definition 2.4(Secure Verifiable Encryption)***

Let $Q$ be a binary predicate and let $L_Q = \{m | \exists S : (m, S) \in Q\}$. A secure verifiable encryption scheme for a binary predicate Q consists of a two party protocol and a recovery algorithm $\Re$. We let $V_P(Y, m, k)$ denote the output of V when interacting with P on input *Y*, *m*, and *k*, where *k* is a security parameter. We require that the following three properties hold:

1. ***Completeness***

   $\forall (Y, X) \in G(1^k)$ and $\forall m \in L_Q$, if P and V are honest then $V_P(Y, m, k) \neq \perp$.

2. ***Validity***

   For all prover $P^*$ and all (Y, X)$\in$G($1^k$), for every polynomials p(·) and all sufficiently large *k*, we have

   $$\Pr\left[(m, \Re(X, b)) \notin Q \text{ and } b \neq \perp : b := V_{P^*}(Y, m, k)\right] < \frac{1}{p(k)}$$

3. ***Computational Zero-Knowledge***

   For every $V^*$ there exists a expected polynomial-time simulator $M_{V^*}$ with black-box access to $V^*$ such that for all distinguishers *A*, all polynomials *p*,

all $m \in L_Q$, and all sufficiently large $k$, we have

$$\Pr\left[A(Y,m,b_i)=i:(Y,X):=G(1^k);b_0:=M_{v^*}(Y,m,k);b_1:=V_P^*(Y,m,k);i\in\{0,1\}\right] < \frac{1}{2}+\frac{1}{p(k)}$$

In our scheme, P wants to convince the verifier V that he really knows the signature of knowledge, but V can not get any information about P's secret.

Hence, we give a modified definition of secure verifiable encryption of signature of knowledge in the version of interactive zero-knowledge proof system of knowledge introduced in section 2.1.

***Definition 2.5(Secure Verifiable Encryption of Signature of Knowledge)***

Let $Q$ be the binary predicate such that for each instance $x = (Y, m, \mathrm{E}_Y(S))$ of the right form, there is a corresponding secret $\rho$ such that $Q(x, \rho) = 1$, where $S$ is a valid signature with respect to $m$ and $\mathrm{E}_Y(S)$ means the encryption of signature on message $m$ with respect to some fixed public key $Y$. We require that the following three properties hold:

1. ***Completeness***

   $\forall x$ and $\forall \rho$ with $Q(x, \rho) = 1$, $\Pr\left[\langle P(\rho), V\rangle(x)=1\right]=1$

2. ***Validity***

   There is a probabilistic (expected) polynomial-time knowledge extractor E such that $\forall x \in \mathrm{Dom}(Q)$, $\forall \mathrm{P}^*$

   $$\Pr\left[\langle P^*(\rho), V\rangle(x)=1\right] \geq \frac{1}{p(|x|)} \Rightarrow \Pr\left[E(P^*,V,x)=\rho^*, Q(x,\rho^*)=1\right] \geq 1-\varepsilon(|x|)$$

   where $\mathrm{Dom}(Q)$ means the domain of $Q$, $p(\cdot)$ is a polynomial, and $\varepsilon(\cdot)$ is negligible.

### *3. Computational Zero-Knowledge*

If there is a universal simulator $M^*$ such that for every possible verifier $V^*$, the following two distributions are polynomially indistinguishable:

- $\{View(P(\rho), V^*, x)\}_{x \in Dom(Q), Q(x,\rho)=1}$;
- $\{m^*(V^*, x)\}_{x \in Dom(Q)}$.

where $m^*(V^*, x)$ the random valuable $M^*(V^*, x)$ conditioned on $M^*(V^*, x) \neq \perp$, that is, for all z,

$\Pr[m^*(V^*, x) = z] = \Pr[M^*(V^*, x) = z | M^*(V^*, x) \neq \perp]$ and $\Pr[M^*(V^*, x) \neq \perp]$ is non-negligible.

## 2.4 1-out-of-P Re-encryption Proof of Encryption Keys

In order to have a witness indistinguishable protocol, we require an algorithm for random re-encryption of a bid, such as ElGamal encryption algorithm.

Generally speaking, 1-out-of-P re-encryption proof defined in [11] means an efficient witness indistinguishable protocol, which a prover can prove that a given encrypted bid $t$, a encrypted list $t_1$, .., $t_P$, and a witness that $t_j$ is a re-encryption of $t$ for $j \in \{1,\ldots,P\}$, proves that indeed $t_j$ is a re-encryption of $t$ without revealing index $j$.

In most common electronic voting system, 1-out-of-P re-encryption proof is used for different messages. In our thesis, we use it for different encryption keys.

We show the general 1-out-of-P re-encryption proof and the 1-out-of-P re-encryption proof of encryption keys in non-interactive form in the following.

**General 1-out-of-P re-encryption proof**[1]

1. The prover generates a list $\{t_1, \ldots, t_P\}$ and publishes it

$$t_1 = (T_{11}, T_{21}) = (m_1 Y^{r_1} \bmod p, g^{r_1} \bmod p)$$
$$t_2 = (T_{12}, T_{22}) = (m_2 Y^{r_2} \bmod p, g^{r_2} \bmod p)$$
$$\vdots$$
$$t_P = (T_{11}, T_{2P}) = (m_P Y^{r_P} \bmod p, g^{r_P} \bmod p)$$

2. Suppose $t_j$ $(1 \le j \le P)$ is the re-encryption of $t = (T_1, T_2) = (m_j Y^r \bmod p, g^r \bmod p)$

i.e. $(T_{1j}, T_{2j}) = (T_1 Y^{\varepsilon} \bmod p, T_2 g^{\varepsilon} \bmod p)$.

3. The prover computes

$$(1)(u_i, v_i) = \left( \left( \frac{T_{1i}}{T_1} \right)^{d_i} Y^{f_i} \bmod p, \left( \frac{T_{2i}}{T_2} \right)^{d_i} g^{f_i} \bmod p \right), \forall j, 1 \le i \ne j \le P, d_i, f_i \in_R Z_q$$
$$(u_i, v_i) = (Y^{f_i} \bmod p, g^{f_i} \bmod p), i = j, f_i \in_R Z_q$$
$$(2)\ d = H((T_1, T_2), (T_{11}, T_{21}), \ldots, (T_{1P}, T_{2P}), (u_1, v_1), \ldots, (u_P, v_P))$$
$$(3)\ d_j = d - \sum_{i \ne j} d_i \bmod q$$
$$w_i = f_i - d_i \varepsilon \bmod q, i = j$$
$$w_i = f_i, \forall j, 1 \le i \ne j \le P$$

and publishes $(d_1, \ldots, d_P), (w_1, \ldots, w_P)$

4. The verifier verifies the proof as the follows

(1) compute $d = \sum_i d_i \bmod q = d_1 + \ldots d_P \bmod q$

(2) check if

$$d = H\left( (T_1, T_2), (T_{11}, T_{21}), \ldots, (T_{1P}, T_{2P}), \left( \left( \frac{T_{11}}{T_1} \right)^{d_1} Y^{w_1} \bmod p, \left( \frac{T_{21}}{T_2} \right)^{d_1} g^{w_1} \bmod p \right), \ldots, \left( \left( \frac{T_{1P}}{T_1} \right)^{d_P} Y^{w_P} \bmod p, \left( \frac{T_{2P}}{T_2} \right)^{d_P} g^{w_P} \bmod p \right) \right)$$

[1]The basic idea is $\log_Y \frac{T_{1j}}{T_1} = \varepsilon = \log_g \frac{T_{2j}}{T_2}$

**1-out-of-P re-encryption proof of encryption keys**[2]

1. The prover generates a list $\{t_1, \ldots, t_P\}$ and publishes it

$$t_1 = (T_{11}, T_{21}) = (mY_1^{r_1} \bmod p, g^{r_1} \bmod p)$$
$$t_1 = (T_{12}, T_{22}) = (mY_2^{r_1} \bmod p, g^{r_2} \bmod p)$$
$$\vdots$$
$$t_1 = (T_{11}, T_{2P}) = (mY_P^{r_P} \bmod p, g^{r_P} \bmod p)$$

2. Suppose $t_j$ $(1 \le j \le P)$ is the re-encryption of $t = (T_1, T_2) = (mY_j^r \bmod p, g^r \bmod p)$

i.e. $(T_{1j}, T_{2j}) = (T_1 Y_j^{\varepsilon} \bmod p, T_2 g^{\varepsilon} \bmod p)$

3. The prover computes

$$(1)\ (u_i, v_i) = \left(\left(\frac{T_{1i}}{T_1}\right)^{d_i} Y_i^{f_i} \bmod p, \left(\frac{T_{2i}}{T_2}\right)^{d_i} g^{f_i} \bmod p\right), \forall j, 1 \le i \ne j \le P, d_i, f_i \in_R Z_q$$
$$(u_i, v_i) = (Y_i^{f_i} \bmod p, g^{f_i} \bmod p), i = j, f_i \in_R Z_q$$
$$(2)\ d = H((T_1, T_2), (T_{11}, T_{21}), \ldots, (T_{1P}, T_{2P}), (u_1, v_1), \ldots, (u_P, v_P))$$
$$(3)\ d_j = d - \sum_{i \ne j} d_i \bmod q$$
$$w_i = f_i - d_i \varepsilon \bmod q, i = j$$
$$w_i = f_i, \forall j, 1 \le i \ne j \le P$$

and publishes $(d_1, \ldots, d_P), (w_1, \ldots, w_P)$

4. The verifier verifies the proof as the follows

(1) compute $d = \sum_i d_i = d_1 + \ldots d_P \bmod q$

(2) check if

$$d = H\left((T_1, T_2), (T_{11}, T_{21}), \ldots, (T_{1P}, T_{2P}), \left(\left(\frac{T_{11}}{T_1}\right)^{d_1} Y_1^{w_1} \bmod p, \left(\frac{T_{21}}{T_2}\right)^{d_1} g^{w_1} \bmod p\right), \ldots, \left(\left(\frac{T_{1P}}{T_1}\right)^{d_P} Y_P^{w_P} \bmod p, \left(\frac{T_{2P}}{T_2}\right)^{d_P} g^{w_P} \bmod p\right)\right)$$

[2]The basic idea is $\log_{Y_j} \frac{T_{1j}}{T_1} = \varepsilon = \log_g \frac{T_{2j}}{T_2}$

## 2.5 Previous Electronic Auction Schemes

We can find out that in most auctions, the validity of the bids is not verified or only verified by the auctioneer.

- The validity of the bids is not verified.

Cachin [1] proposed a private bidding and auction scheme using the millionaire's protocol to determine who is richer without disclosing anything else about their wealth between two parties. This protocol employs two semi-trusted parties, T and V, as auction servers. All bidders and T are connected to V in secure channel. The server V chooses the random values for n instances of private bidding protocol. The bidders encrypt their bids, send them to the server V, but not involve further. The server V determines the highest bid through n successive queries to the server T who oblivious compares two bids, but who does not learn anything about the bids. At the end, V leans partial order of the bids, but not more.

Noar[13] introduced a simple architecture for preserving the privacy of the bids of losing bidders while maintaining communication and computational efficiency. They employ an additional third party auction issuer that generate the programs for computing the auctions but does not take an active part in the protocol. Their protocol ensures that except collaboration of the auctioneer and the auction issuer, neither party gains any information about the bids, even after the auction is terminated. Moreover, bidders can verify the correctness of the auction.

In [2], Kikuchi presented a new protocol for (M + 1)st-price auction, a style of auction in which the highest M bidders win and pay a uniform price, determined by (M + 1)st price. The scheme uses the verifiable secret sharing technique, where the

bidding point is represented by the degree of a polynomial shared by the number of the auctioneers. In this scheme, there exist some drawbacks. For example, this scheme has an undesirable condition that the number of the auctioneers must be larger than the number of the bidding points, so it is difficult to set bidding points. Moreover, every one can anonymously disturb an auction by submitting an invalid bid.

- The validity of the bids is verified by the auctioneer before the opening phase.

  In this kind of auctions, the auctioneer often just verifies the bidding value (bidding format).

Harkavy, Tygar and Kikuchi [10] described an auction service for secure sealed-bid auctions, in which only the winning bid is disclosed. Both first-price and second-price auctions are supported. It is based on general techniques for secure multiparty computation and can tolerant up to $t \le \left\lfloor \frac{s-1}{3} \right\rfloor$ corrupted servers. However, the protocol is practical only for small value of s.

In [9], Abe and Suzuli proposed the (M + 1)st-price auction using homomorphic encryption and mix and match technique. Their scheme realizes public verifiability of a winner and the wining bid. However, each bidder must compute K+1 zero-knowledge proofs in bidding, where K is the number of bidding points. Besides, in this protocol, the bidding price (bidding format) can be verified by every one.

In [6], Omote and Miyaji proposed a second-price sealed-bid auction with public verifiability. In their scheme, they use the verifiable discriminant function of the $p_0$-root to achieve public verifiability.

- The validity of the bids is verified by the auctioneer in the opening phase.

  In this kind of auctions, the auctioneer often just concern the validity of the

winner.

In [12], Franklin and Reiter use a set of distributed auctioneers and feature an innovative primitive called verifiable secret-sharing. Their protocol can also successfully prevent a single auctioneer altering a bid or throwing an auction to a single bidder. However, the confidentiality of bids of the bidders is not achieved, since the confidentiality is as essential as fairness. Besides, their protocol will result in all auctioneers knowing all bids after the auction is decided.

The problem on privacy of losers is firstly point out by Kikuchi, Harkavy and Tyger[3]. The basic idea of the scheme is “secure addition”. However, the proposed scheme has a problem that the process of determining the winner does not work successfully when the winners with the same bidding price are multiple in the auction. In other words, this protocol can not work when two or more bidders bid at the same highest price.

In [14], Liu, Wang and Wang, proposed a new multi-round sealed-bid auction scheme based on Shamir’s (t, n)-threshold secret sharing scheme. The protocol guarantees that no information about the losing bidders is leaked, and that the seller can collect the digital money from the winning bidder. In addition, the protocol support both first-price and second-price sealed-bid auction.

In [4], Kikuchi, Hotta, Abe and Nakanishi modified [3] in which “mask” step are added to keep all bids private and only the winning bid and winner are determined by the collaboration of distributed servers. They improve the security of the protocol in [3] such that the second highest must be not known even by the winner.

Watanabe and Imai [16] introduced a totally different trust third party, the off-line trusted third party (TTP), to achieve the universally verifiable auction scheme.

They make use of a TTP in optimistic sense, i.e. the TTP takes part in the protocol only if one bidder cheats or simply crashes. However, this protocol has a disadvantage that all bidders have to participate in the auction at the beginning in the opening phase.

In [8], Suzuki, Kobayashi and Morita presented the first sealed-bid auction scheme, which is only using multiple hash functions. This method drastically reduces the time taken for bidding and opening bids. However, it is not practical for opening all the bids if one of the auctioneers is distrust or can not release his secret seed.

In [7], Peng, Boyd, Dawson and K. Viswanathan classified the published sealed-bid auction into four models according to how they deal with bid privacy and proposed a new model. Then give a comparison about the five models. In their model, they give another solution for bid privacy recovery, i.e. the registration authority an all the losing bidders cooperate to identify the dishonest winners by publishing their secrets, instead of a trust third party only being used. However, the drawback is that when the number of bidders involved is large, it is quite efficient to recover bid privacy.

Hence, we propose a sealed-bid auction protocol with public verifiable bid validity. Every one in our protocol can verify the validity of the bid which contains the validity of the bidder and the validity of the bidding price. If anyone finds some invalid bids from malicious bidders, he can ask the auction manager AM to revoke them before the opening phase.

# Chapter 3

# A Sealed-Bid Auction with Publicly Verifiable Bid Validity

In this chapter, we propose a sealed-bid auction with publicly verifiable bid validity and analyze its security and properties. Here, bid validity contains not only the validity of the bidder but also the validity of the bidder's bidding price. In our scheme, we combine the signature and the bidding price as the bid. The bidder generates his signature on message *m* using the signature of knowledge technique. The idea of our scheme is based on verifiable encryption of signature of knowledge and 1-out-of-P re-encryption proof of encryption keys.

Our scheme uses two managers, the registration manager RM and the auction manager AM. RM is the registration manager who guarantees the relationship between a bidder and his corresponding public key. AM is the auction manager who holds auctions and manages operations in an auction.

In our scheme, every one can verify the bidder' s bid to check the bid validity, but can not get any information about the identities and bidding price of the bidders. If there exist some invalid bids, anyone can indicate them and ask the auction manager AM to revoke the invalid bids. The scheme can prevent some malicious bidders who send invalid bids to disturb the auction.

## 3.1 Notations

Main notations used in our scheme are described as follows:

RM : the registration manager:

- handle the bidder's registration;
- manage RM's bulletin board system (BBS) which publishes a list of public keys;
- declare the winner.

AM : the auction manager:

- manage the bidding phase;
- manage AM's bulletin board system (BBS) which publishes the computing process of bids;
- declare the winning price.

$m$ : the unique message of the good; (e.q. the auction identity of the good)

$I$ : the number of bidders;

$i$ : the index of bidders;

$B_i$ : a bidder whose index is i (i = 1,..,$I$ );

$p$, $q$ : large primes such that $p = 2q + 1$;

$g$, $h$ : generators of $G_q$;

$\pi_i$, $\alpha_i$ : $B_i$'s private key where $\pi_i$ is the password memorized in the bidder's mind and $\alpha_i$ is the corresponding partial secret stored in the bidder's mobile device.

$y_i$ : $B_i$'s public key where $y_i = g^{\alpha_i} h^{\pi_i} \bmod p$;

$P$ : the number of prices;

$j$ : the index of prices;

$\delta_j$ : the $j$-th price ($j$ = 1,…,$P$);

$X_j$ : the decryption key corresponding to the $j$-th price;

$Y_j$ : the encryption key corresponding to the $j$-th price where

$Y_j = g^{x_j} \bmod p$ for $1 \le j \le P$ ;

$\text{Sign}_k()$ : a signature of knowledge signed by key $k$;

$E_Y()$ : ElGamal encryption with public key $Y$ such that

$E_Y(W) = (G = g^r \bmod p, M = WY^r \bmod p)$

$D_x()$ : ElGamal decryption with private key $X$ such that

$D_X(G, M) = M/G^x \bmod p$

$H()$ : a secure (collision-resistant) hash function : $\{0,1\}^* \rightarrow Z_q$

$\left(a^{(i)}, w_1^{(i)}, w_2^{(i)}\right)$ : the signature of the bidder $B_i$ on message $m$;

$\left(T_1^{(i)}, T_2^{(i)}\right)$ : the bid of the bidder $B_i$;

$\left\{\left(T_{11}^{(i)}, T_{21}^{(i)}\right),...,\left(T_{1P}^{(i)}, T_{2P}^{(i)}\right)\right\}$ : the bid list of the bidder $B_i$ used for 1-out-of-P re-encryption proof of encryption keys;

## 3.2 Our Basic Scheme

Our scheme has six main phases and their procedure is as follows:

1. Initialization.

2. Bidder registration.

3. Auction preparation.

4. Bidding.

5. Bid verification.

6. Opening.

We describe them in detail in the following:

- Initialization

The registration manager RM selects large primes $p$ and $q$ such that $p = 2q + 1$ and picks up $g$ and $h$ which are two generators of $G_q$. Besides, the registration manager RM chooses a collision-resistant hash function $H(\cdot):\{0,1\}^* \rightarrow Z_q$. Then the registration manager RM publishes $p$, $g$, $h$, and H on the RM's BBS as system public parameters.

- Bidder registration

When a bidder whose identity is Bob participates in an auction, he sends his identity and public key $y$ with the signature $Sign_{\alpha,\pi}(y)$ signed by signature of knowledge, using his password $\pi$ memorized in his mind and the partial secret $\alpha$ stored in his mobile device, to the registration manager RM as a bidder registration. After all bidders finished their registrations, the registration manager RM publishes those public keys and their corresponding indexes on the RM's bulletin boards system (BBS) but keeps the relation of the bidders' identities and their public keys in secret.

After the registration manager RM publishes the list of pairs of public keys and indexes, each bidder searches his corresponding index from the RM's BBS using his public key.

- Auction preparation

The auction manager AM publishes the price list $\{\delta_1, \ldots, \delta_P\}$ and the unique

message $m$ of the good on the AM's BBS. Then the auction manager AM generates a pair of decryption key $X_j$ and encryption key $Y_j$ corresponding to the price $\delta_j$ where $X_j \in_R Z_q$ and $Y_j = g^{x_j} \bmod p$ for 1≤ j ≤$P$. Here, we have to note that in order to stand for distinct price, so the decryption keys selected by the auction manager AM should be distinct. The auction manager AM holds the decryption keys and publishes the encryption keys on the AM's BBS.

After all those public keys are published, each bidder $B_i$ (1≤ i ≤$I$) sends his index $i$ and a list $\{(T_{11}^{(i)}, T_{21}^{(i)}),...,(T_{1P}^{(i)}, T_{2P}^{(i)})\}$ where $(T_{1j}^{(i)}, T_{2j}^{(i)}) = E_{Y_j}(Sign_{\alpha_i,\pi_i}(m))$ for 1≤ j ≤P to the AM's BBS.

In order to get the list $\{(T_{11}^{(i)}, T_{21}^{(i)}),...,(T_{1P}^{(i)}, T_{2P}^{(i)})\}$, each bidder $B_i$ has to follow the two steps described in Figure 3.1. First, each bidder has to make a signature on the unique message $m$ of the good using signature of knowledge with his secrets which are the password $\pi_i$ memorized in his mind and the partial secret $\alpha_i$ stored in his mobile device. After the generation of the signature, we can get $(a^{(i)}, w_1^{(i)}, w_2^{(i)})$ to be the signature of knowledge of password $\pi_i$ and the partial secret $\alpha_i$ such that $y_i = g^{\alpha_i} h^{\pi_i} \bmod p$ on message $m$ for the bidder $B_i$. Second, he encrypts his signature using all the encryption keys published.

Besides, it is worthy of remark that the generation of the signature of each bidder $B_i$ only need to be done once. In other words, the signature of the bidder $B_i$ used in an auction would be the same.

Moreover, our encryption function only deals with the elements $(w_1^{(i)}, w_2^{(i)})$ of the signature of the bidder $B_i$. We encrypt $(w_1^{(i)}, w_2^{(i)})$ but let $a^{(i)}$ be public. The bidder $B_i$ will publish the element $a^{(i)}$ of his signature in the bidding phase.

**Step 1**: Each bidder $B_i$ signs for the unique message $m$ of the good to get a signature

$\underline{\underline{Sign_{\alpha_i,\pi_i}(m)}}$:

1. $r_1^{(i)}, r_2^{(i)} \in_R Z_q$
   $a^{(i)} = g^{r_1^{(i)}} h^{r_2^{(i)}} \bmod p$
2. $c^{(i)} = H(m, p, g, h, y_i, a^{(i)})$
3. $w_1^{(i)} = r_1^{(i)} - c^{(i)}\alpha_i \bmod q$
   $w_2^{(i)} = r_2^{(i)} - c^{(i)}\pi_i \bmod q$

**Step 2**: Each bidder $B_i$ encrypts his signature $P$ times using different encryption keys

$\underline{\underline{E_{Y_j}(Sign_{\alpha_i,\pi_i}(m))}}: \forall j, 1 \le j \le P$

1. $e_j^{(i)} \in_R Z_q$
   $T_{1j}^{(i)} = g^{w_1^{(i)}} h^{w_2^{(i)}} (Y_j)^{e_j^{(i)}} \bmod p$
   $T_{2j}^{(i)} = g^{e_j^{(i)}} \bmod p$

Figure 3.1: Generation of the list of 1-out-of-P re-encryption proof of encryption keys

- Bidding

Each bidder $B_i$ selects his encryption key $Y_j$ corresponding to his bidding price $\delta_j$. $B_i$ then encrypts part of the signature $(w_1^{(i)}, w_2^{(i)})$ generated in the auction preparation phase using the encryption key $Y_j$ described in Figure 3.2.

$\underline{\underline{E_{Y_j}(w_1^{(i)}, w_2^{(i)})}}$:

1. $e^{(i)} \in_R Z_q$
   $T_1^{(i)} = g^{w_1^{(i)}} h^{w_2^{(i)}} (Y_j)^{e^{(i)}} \bmod p$
   $T_2^{(i)} = g^{e^{(i)}} \bmod p$

Figure 3.2: Generation of $B_i$'s bid

After the encryption done, each bidder $B_i$ sends his index $i$ and $\left(a^{(i)}, T_1^{(i)}, T_2^{(i)}\right)$ to the AM's BBS. Besides, $B_i$ also has to provide two kinds of proofs (P+1 proofs) as showed in Figure 3.3. There are P proofs for the first kind proof and 1 proof for the second proof. The two kinds of proofs are described as follows:

1. P proofs for verifiable encryption of signature of knowledge of

   (i) $r_1^{(i)}, r_2^{(i)}$, $\alpha_i$, and $\pi_i$ such that

   $$w_1^{(i)} = r_1^{(i)} - c^{(i)}\alpha_i \pmod{q},\ w_2^{(i)} = r_2^{(i)} - c^{(i)}\pi_i \pmod{q}$$

   to show that $\left(a^{(i)}, w_1^{(i)}, w_2^{(i)}\right)$ is valid signature.

   (ii) $e_j^{(i)}$ such that $\left(T_{1j}^{(i)}, T_{2j}^{(i)}\right)$ is the correct ciphertext of $w_1^{(i)}$ and $w_2^{(i)}$.

   The bidder $B_i$ has to send $\left(c_{1j}^{(i)}, s_{1j}^{(i)}, s_{2j}^{(i)}, s_{3j}^{(i)}, s_{4j}^{(i)}, s_{5j}^{(i)}\right), \forall j, 1 \le j \le P$, to AM's BBS.

2. 1-out-of-P re-encryption proof of encryption keys such that no one except $B_i$ can distinguish which encryption key is used. The bidder $B_i$ has to show that for the encrypted bid $\left(T_1^{(i)}, T_2^{(i)}\right)$, there is a re-encryption in the $\left\{\left(T_{11}^{(i)}, T_{21}^{(i)}\right), ..., \left(T_{1P}^{(i)}, T_{2P}^{(i)}\right)\right\}$. i.e. $\left(T_{1j}^{(i)}, T_{2j}^{(i)}\right) = \left(T_1^{(i)} Y_j^{\varepsilon} \bmod p, T_2^{(i)} g^{\varepsilon} \bmod p\right)$, $\left(T_{1j}^{(i)}, T_{2j}^{(i)}\right)$ is the re-encryption of $\left(T_1^{(i)}, T_2^{(i)}\right)$.

   The bidder $B_i$ has to send $\left(c_{21}^{(i)}, ..., c_{2P}^{(i)}\right), \left(z_1^{(i)}, ..., z_P^{(i)}\right)$ to AM's BBS.

**1.** verifiable encryption of signature of knowledge of $r_1^{(i)}, r_2^{(i)}$, $\alpha_i$, $\pi_i$, and $e_j^{(i)}$

$\forall j, 1 \le j \le P$

(1). $k_{1j}^{(i)}, k_{2j}^{(i)}, k_{3j}^{(i)}, k_{4j}^{(i)}, k_{5j}^{(i)} \in_R Z_q$

$d_{1j}^{(i)} = g^{k_{1j}^{(i)}} \bmod p,$

$d_{2j}^{(i)} = g^{k_{2j}^{(i)}} h^{k_{3j}^{(i)}} \bmod p,$

$d_{3j}^{(i)} = g^{k_{4j}^{(i)}} h^{k_{5j}^{(i)}} \bmod p,$

$d_{4j}^{(i)} = Y_j^{k_{1j}^{(i)}} g^{k_{2j}^{(i)} - k_{4j}^{(i)}} h^{k_{3j}^{(i)} - k_{5j}^{(i)}} \bmod p$

(2). $c_{1j}^{(i)} = H(p, g, h, a^{(i)}, y_i, T_1^{(i)}, T_2^{(i)}, d_{1j}^{(i)}, d_{2j}^{(i)}, d_{3j}^{(i)}, d_{4j}^{(i)})$

(3). $s_{1j}^{(i)} = k_{1j}^{(i)} - c_{1j}^{(i)} e_j^{(i)} \bmod q,$

$s_{2j}^{(i)} = k_{2j}^{(i)} - c_{1j}^{(i)} r_1^{(i)} \bmod q,$

$s_{3j}^{(i)} = k_{3j}^{(i)} - c_{1j}^{(i)} r_2^{(i)} \bmod q,$

$s_{4j}^{(i)} = k_{4j}^{(i)} - c_{1j}^{(i)} c^{(i)} \alpha_i \bmod q,$

$s_{5j}^{(i)} = k_{5j}^{(i)} - c_{1j}^{(i)} c^{(i)} \pi_i \bmod q$

**Sends** $\left(c_{1j}^{(i)}, s_{1j}^{(i)}, s_{2j}^{(i)}, s_{3j}^{(i)}, s_{4j}^{(i)}, s_{5j}^{(i)}\right)$ to AM's BBS

**2.** 1-out-of-P re-encryption proof of encryption keys

(1). $\forall t, 1 \le t \ne j \le P, c_{2t}^{(i)}, f_t^{(i)} \in_R Z_q,$

$$\left(u_t^{(i)}, v_t^{(i)}\right) = \left( \left( \frac{T_{1t}^{(i)}}{T_1^{(i)}} \right)^{c_{2t}^{(i)}} \left(Y_t\right)^{f_t^{(i)}} \bmod p, \left( \frac{T_{2t}^{(i)}}{T_2^{(i)}} \right)^{c_{2t}^{(i)}} g^{f_t^{(i)}} \bmod p \right);$$

$t = j, f_t^{(i)} \in_R Z_q,$

$$\left(u_t^{(i)}, v_t^{(i)}\right) = \left( \left(Y_j\right)^{f_t^{(i)}} \bmod p, g^{f_t^{(i)}} \bmod p \right)$$

(2). $c_2^{(i)} = H\left(p, q, g, h, T_1^{(i)}, T_2^{(i)}, (Y_1, ..., Y_P), \left(\left(T_{11}^{(i)}, T_{21}^{(i)}\right), ..., \left(T_{1P}^{(i)}, T_{2P}^{(i)}\right)\right), \left(\left(u_1^{(i)}, v_1^{(i)}\right), ..., \left(u_P^{(i)}, v_P^{(i)}\right)\right)\right)$

(3). $c_{2j}^{(i)} = c_2^{(i)} - \sum_{t \ne j} c_{2t}^{(i)} \bmod q$

$t = j, z_t^{(i)} = f_t^{(i)} - c_{2t}^{(i)} \varepsilon \bmod q;$

$\forall t, 1 \le t \ne j \le P, z_t^{(i)} = f_t^{(i)}$

**Sends** $\left(c_{21}^{(i)}, ..., c_{2P}^{(i)}\right), \left(z_1^{(i)}, ..., z_P^{(i)}\right)$ to AM's BBS

Figure 3.3: Two kinds of proofs for the bid of the bidder $B_i$

- Bid verification

This can be done by every one. If anyone finds invalid bids, then he can ask the auction manager AM to revoke them. If we want to verify the bid validity of the bidder $B_i$, we can do as follows:

1. Compute $c^{(i)} = H(m, p, g, h, y_i, a^{(i)})$
2. $\forall j, 1 \le j \le P$, compute

$$\tilde{c}_{1j}^{(i)} = H\left( \begin{array}{l} p, g, h, a^{(i)}, y_i, T_{1j}^{(i)}, T_{2j}^{(i)}, \\ \left(T_{2j}^{(i)}\right)^{c_1^{(i)}} g^{s_{1j}^{(i)}} \bmod p, \left(a^{(i)}\right)^{c_{1j}^{(i)}} g^{s_{2j}^{(i)}} h^{s_{3j}^{(i)}} \bmod p, \\ \left(y_i^{c^{(i)}}\right)^{c_{1j}^{(i)}} g^{s_{4j}^{(i)}} h^{s_{5j}^{(i)}} \bmod p, \left(T_{1j}^{(i)}\right)^{c_{1j}^{(i)}} \left(Y_j^{(i)}\right)^{s_{1j}^{(i)}} g^{s_{2j}^{(i)}} h^{s_{3j}^{(i)}} / g^{s_{4j}^{(i)}} h^{s_{5j}^{(i)}} \bmod p \end{array} \right)$$

and verify if $\tilde{c}_{1j}^{(i)} = c_{1j}^{(i)}$. The idea of the verification is as Figure 3.4.

(1) *check* $e_j^{(i)}$

$$\left(T_{2j}^{(i)}\right)^{c_{1j}^{(i)}} g^{s_{1j}^{(i)}} = g^{c_{1j}^{(i)} e_j^{(i)}} g^{k_{1j}^{(i)} - c_{1j}^{(i)} e_j^{(i)}} = g^{k_{1j}^{(i)}} = d_{1j}^{(i)} \bmod p$$

(2) *check* $r_1^{(i)}$, $r_2^{(i)}$

$$\left(a^{(i)}\right)^{c_{1j}^{(i)}} g^{s_{2j}^{(i)}} h^{s_{3j}^{(i)}} = g^{c_{1j}^{(i)} r_1^{(i)}} h^{c_{1j}^{(i)} r_2^{(i)}} g^{k_{2j}^{(i)} - c_{1j}^{(i)} r_1^{(i)}} h^{k_{3j}^{(i)} - c_{1j}^{(i)} r_2^{(i)}} = g^{k_{2j}^{(i)}} h^{k_{3j}^{(i)}} = d_{2j}^{(i)} \bmod p$$

(3) *check* $\alpha_i$ *and* $\pi_i$

$$\left(y_i^{c^{(i)}}\right)^{c_{1j}^{(i)}} g^{s_{4j}^{(i)}} h^{s_{5j}^{(i)}} = g^{c_{1j}^{(i)} c^{(i)} \alpha_i} h^{c_{1j}^{(i)} c^{(i)} \pi_i} g^{k_{4j}^{(i)} - c_{1j}^{(i)} c^{(i)} \alpha_i} h^{k_{5j}^{(i)} - c_{1j}^{(i)} c^{(i)} \pi_i} = g^{k_{4j}^{(i)}} h^{k_{5j}^{(i)}} = d_{3j}^{(i)} \bmod p$$

(4) *check* $w_1^{(i)} = r_1^{(i)} - c^{(i)} \alpha_i, w_2^{(i)} = r_2^{(i)} - c^{(i)} \pi_i$

$$\left(T_{1j}^{(i)}\right)^{c_{1j}^{(i)}} \left(Y_j\right)^{s_{1j}^{(i)}} g^{s_{2j}^{(i)}} h^{s_{3j}^{(i)}} / g^{s_{4j}^{(i)}} h^{s_{5j}^{(i)}} = g^{c_{1j}^{(i)} w_1^{(i)}} h^{c_{1j}^{(i)} w_2^{(i)}} Y_j^{c_{1j}^{(i)} e} Y_j^{k_{1j}^{(i)} - c_{1j}^{(i)} e_j^{(i)}} g^{k_{2j}^{(i)} - c_{1j}^{(i)} r_1^{(i)}} h^{k_{3j}^{(i)} - c_{1j}^{(i)} r_2^{(i)}} / g^{k_{4j}^{(i)} - c_{1j}^{(i)} c^{(i)} \alpha_i} h^{k_{5j}^{(i)} - c_{1j}^{(i)} c^{(i)} \pi_i}$$

$$= g^{c_{1j}^{(i)} r_1^{(i)} - c_{1j}^{(i)} c^{(i)} \alpha_i} h^{c_{1j}^{(i)} r_2^{(i)} - c_{1j}^{(i)} c^{(i)} \pi_i} Y_j^{c_{1j}^{(i)} e} Y_j^{k_{1j}^{(i)} - c_{1j}^{(i)} e_j^{(i)}} g^{k_{2j}^{(i)} - c_{1j}^{(i)} r_1^{(i)}} h^{k_{3j}^{(i)} - c_{1j}^{(i)} r_2^{(i)}} / g^{k_{4j}^{(i)} - c_{1j}^{(i)} c^{(i)} \alpha_i} h^{k_{5j}^{(i)} - c_{1j}^{(i)} c^{(i)} \pi_i}$$

$$= Y_j^{k_{1j}^{(i)}} g^{k_{2j}^{(i)} - k_{4j}^{(i)}} h^{k_{3j}^{(i)} - k_{5j}^{(i)}}$$

$$= d_{4j}^{(i)} \bmod p$$

Figure 3.4: The idea of verifying the first proof in the bidding phase

3. (1) Compute $c_2^{(i)} = c_{21}^{(i)} + ... + c_{2P}^{(i)} \bmod q$ and

$$\tilde{c}_2^{(i)} = H\left(\begin{array}{l} p, g, h, T_1^{(i)}, T_2^{(i)}, (Y_1, ..., Y_P), \left(\left(T_{11}^{(i)}, T_{21}^{(i)}\right), ..., \left(T_{1P}^{(i)}, T_{2P}^{(i)}\right)\right), \\ \left(\left(\frac{T_{11}^{(i)}}{T_1^{(i)}}\right)^{c_{21}^{(i)}} Y_1^{z_1^{(i)}} \bmod p, \left(\frac{T_{21}^{(i)}}{T_2^{(i)}}\right)^{c_{21}^{(i)}} g^{z_1^{(i)}} \bmod p\right), ..., \\ \left(\left(\frac{T_{1P}^{(i)}}{T_1^{(i)}}\right)^{c_{2P}^{(i)}} Y_P^{z_P^{(i)}} \bmod p, \left(\frac{T_{2P}^{(i)}}{T_2^{(i)}}\right)^{c_{2P}^{(i)}} g^{z_P^{(i)}} \bmod p\right) \end{array}\right)$$

(2) Verify if $\tilde{c}_2^{(i)} = c_2^{(i)}$

- Opening

Starting from the highest price, the auction manager AM decrypts those ciphertexts starting on the downward prices as the follows:

For $X = X_P, X_{P-1}, \ldots$

1. $\forall i$, $1 \le i \le I$, check if

$$\begin{aligned} a^{(i)} &= D_X\left(E_{Y_j^{(i)}}\left(Sign_{\alpha_i, \pi_i}(m)\right)\right) \cdot y_i^{c^{(i)}} \\ &= D_X\left(T_1^{(i)}, T_2^{(i)}\right) \cdot y_i^{c^{(i)}} \\ &= \frac{T_1^{(i)}}{\left(T_2^{(i)}\right)^X} \cdot y_i^{c^{(i)}} \pmod p \end{aligned}$$

If the bid of the bidder $B_i$ satisfies the equation, the auction manager AM publish the winning price is δ corresponding to the decryption key X and send the winner index $i$ to the registration manager RM and then RM publishes the identity of the winner.

2. The AM publishes the decryption key $X$ on AM's BBS. If the winner's identity is published, then the auction is terminated.

## 3.3 Analysis

We shall analyze the security and the properties of our proposed scheme. We first describe the verifiable encryption of signature of knowledge is perfect zero knowledge and then state what properties our scheme has.

### 3.3.1 Security

In our scheme, we use verifiable encryption of signature of knowledge to confirm the validity of the bidders. Every one can verify the bids but can not get any information about the signature of knowledge of the bidders. Every one can be convinced that not only the signature of knowledge is of the right form but also the encrypted signature of knowledge is of the right form. We prove that the encryption used in our protocol is secure verifiable encryption of signature of knowledge in the following theorem.

***Theorem 3.1.*** *The verifiable encryption of signature of knowledge used in our scheme is secure with perfect zero-knowledge.*

**Proof.**

We will prove that our protocol has the properties defined in definition 2.5 with perfect zero-knowledge.

We first convert our verifiable encryption of signature of knowledge into interactive proof system instead of non-interactive proof system where V's challenge is constant size. For simplicity, we remove the index *i* of the bidder and the index *j* for encryption keys. We describe the system as the follows and figure it out, then show the system IP-$_{VESK}$ is perfect zero-knowledge.

**Protocol IP-$_{VESK}$**

Input: ($p$, $g$, $h$, $T_1$, $T_2$, $a$, $y$);

P's private input: ($r_1$, $r_2$, $\alpha$, $\pi$, $e$);

I. The following steps are run for $q(n)$ times

1. P→V : $d_1$, $d_2$, $d_3$, $d_4$

$k_1, k_2, k_3, k_4, k_5 \in_R Z_q$

$d_1 = g^{k_1} \bmod p$

$d_2 = g^{k_2} h^{k_3} \bmod p$

$d_3 = g^{k_4} h^{k_5} \bmod p$

$d_4 = Y^{k_1} g^{k_2 - k_4} h^{k_3 - k_5} \bmod p$

2. V→P : $c_1$

$c_1 \in \{0,1\}$

3. P→V : $s_1$, $s_2$, $s_3$, $s_4$, $s_5$

$s_1 = k_1 - c_1 e \bmod q$

$s_2 = k_2 - c_1 r_1 \bmod q$

$s_3 = k_3 - c_1 r_2 \bmod q$

$s_4 = k_4 - c_1 c\alpha \bmod q$

$s_5 = k_5 - c_1 c\pi \bmod q$

4. V verifies whether

(1) $check\ e \Rightarrow d_1 = T_2^{c_1} g^{s_1} \bmod p$

$T_2^{c_1} g^{s_1} = g^{c_1 e} g^{k_1 - c_1 e} = g^{k_1} = d_1$

(2) $check\ r_1, r_2 \Rightarrow d_2 = a^{c_1} g^{s_2} h^{s_3} \bmod p$

$a^{c_1} g^{s_2} h^{s_3} = g^{c_1 r_1} h^{c_1 r_2} g^{k_2 - c_1 r_1} h^{k_3 - c_1 r_2} = g^{k_2} h^{k_3} = d_2$

(3) $check\ \alpha, \pi \Rightarrow d_3 = (y^c)^{c_1} g^{s_4} h^{s_5} \bmod p$

$(y^c)^{c_1} g^{s_4} h^{s_5} = g^{c_1 c\alpha} h^{c_1 c\pi} g^{k_4 - c_1 c\alpha} h^{k_5 - c_1 c\pi} = g^{k_4} h^{k_5} = d_3$

(4) $check\ w_1 = r_1 - c\alpha, w_2 = r_2 - c\pi \Rightarrow d_4 = T_1^{c_1} Y^{s_1} g^{s_2} h^{s_3} / g^{s_4} h^{s_5} \bmod p$

$$\begin{aligned} T_1^{c_1} Y^{s_1} g^{s_2} h^{s_3} / g^{s_4} h^{s_5} &= g^{c_1 w_1} h^{c_1 w_2} Y^{c_1 e} Y^{k_1 - c_1 e} g^{k_2 - c_1 r_1} h^{k_3 - c_1 r_2} / g^{k_4 - c_1 c\alpha} h^{k_5 - c_1 c\pi} \\ &= g^{c_1 r_1 - c_1 c\alpha} h^{c_1 r_2 - c_1 c\pi} Y^{c_1 e} Y^{k_1 - c_1 e} g^{k_2 - c_1 r_1} h^{k_3 - c_1 r_2} / g^{k_4 - c_1 c\alpha} h^{k_5 - c_1 c\pi} \\ &= Y^{k_1} g^{k_2 - k_4} h^{k_3 - k_5} \\ &= d_4 \end{aligned}$$

II. V accepts if and only if all the above checks are correct

P ⟵ $p, g, h, T_1, T_2,$ $a = g^{r_1} h^{r_2} \bmod p,$ $y = g^{\alpha} h^{\pi} \bmod p$ ⟶ V

( $e, r_1, r_2, \alpha, \pi$ )

I. The following steps are run for $q(n)$ times

$k_1, k_2, k_3, k_4, k_5 \in_R Z_q$

$d_1 = g^{k_1} \bmod p$

1. $d_2 = g^{k_2} h^{k_3} \bmod p$

$d_3 = g^{k_4} h^{k_5} \bmod p$

$d_4 = Y^{k_1} g^{k_2 - k_4} h^{k_3 - k_5} \bmod p$

$\xrightarrow{d_1, d_2, d_3, d_4}$

2. $c_1 \in \{0,1\}$

$\xleftarrow{c_1}$

$s_1 = k_1 - c_1 e \bmod q$

$s_2 = k_2 - c_1 r_1 \bmod q$

3. $s_3 = k_3 - c_1 r_2 \bmod q$

$s_4 = k_4 - c_1 c\alpha \bmod q$

$s_5 = k_5 - c_1 c\pi \bmod q$

$\xrightarrow{s_1, s_2, s_3, s_4, s_5}$

(1) $check\ e \Rightarrow d_1 = T_2^{c_1} g^{s_1} \bmod p$

$T_2^{c_1} g^{s_1} = g^{c_1 e} g^{k_1 - c_1 e} = g^{k_1} = d_1$

(2) $check\ r_1, r_2 \Rightarrow d_2 = a^{c_1} g^{s_2} h^{s_3} \bmod p$

$a^{c_1} g^{s_2} h^{s_3} = g^{c_1 r_1} h^{c_1 r_2} g^{k_2 - c_1 r_1} h^{k_3 - c_1 r_2} = g^{k_2} h^{k_3} = d_2$

(3) $check\ \alpha, \pi \Rightarrow d_3 = (y^c)^{c_1} g^{s_4} h^{s_5} \bmod p$

4. $(y^c)^{c_1} g^{s_4} h^{s_5} = g^{c_1 c\alpha} h^{c_1 c\pi} g^{k_4 - c_1 c\alpha} h^{k_5 - c_1 c\pi} = g^{k_4} h^{k_5} = d_3$

(4) $check\ w_1 = r_1 - c\alpha, w_2 = r_2 - c\pi \Rightarrow d_4 = T_1^{c_1} Y^{s_1} g^{s_2} h^{s_3} / g^{s_4} h^{s_5} \bmod p$

$T_1^{c_1} Y^{s_1} g^{s_2} h^{s_3} / g^{s_4} h^{s_5} = g^{c_1 w_1} h^{c_1 w_2} Y^{c_1 e} Y^{k_1 - c_1 e} g^{k_2 - c_1 r_1} h^{k_3 - c_1 r_2} / g^{k_4 - c_1 c\alpha} h^{k_5 - c_1 c\pi}$

$= g^{c_1 r_1 - c_1 c\alpha} h^{c_1 r_2 - c_1 c\pi} Y^{c_1 e} Y^{k_1 - c_1 e} g^{k_2 - c_1 r_1} h^{k_3 - c_1 r_2} / g^{k_4 - c_1 c\alpha} h^{k_5 - c_1 c\pi}$

$= Y^{k_1} g^{k_2 - k_4} h^{k_3 - k_5}$

$= d_4$

II. V accepts if and only if all the above checks are correct.

***Completeness***

If P has the knowledge of e, $r_1$, $r_2$, $\alpha$, and $\pi$, then

$$\Pr\left[\left\langle P(e, r_1, r_2, \alpha, \pi), V\right\rangle(p, g, h, a, y, T_1, T_2) = 1\right] = 1$$

***Validity***

For any $P^*$, the view of $\left\langle P(e, r_1, r_2, \alpha, \pi), V\right\rangle(p, g, h, a, y, T_1, T_2)$ is

$$\left(\begin{array}{l} D_1^1, D_2^1, D_3^1, D_4^1, C_1^1, S_1^1, S_2^1, S_3^1, S_4^1, S_5^1, \ldots, \\ \qquad \ldots, D_1^{q(n)}, D_2^{q(n)}, D_3^{q(n)}, D_4^{q(n)}, C_1^{q(n)}, S_1^{q(n)}, S_2^{q(n)}, S_3^{q(n)}, S_4^{q(n)}, S_5^{q(n)} \end{array}\right)$$

where $\left(D_1^l, D_2^l, D_3^l, D_4^l, C_1^l, S_1^l, S_2^l, S_3^l, S_4^l, S_5^l\right)$ is the view of $l$th iteration.

Consider the extractor $E\left(\left\langle P^*(e, r_1, r_2, \alpha, \pi), V\right\rangle(p, g, h, a, y, T_1, T_2)\right)$ to compute the secrets $e$, $r_1$, $r_2$, $\alpha$, and $\pi$.

1. Run $\left\langle P^*(e, r_1, r_2, \alpha, \pi), V\right\rangle(p, g, h, a, y, T_1, T_2)$ to get an instance $(d_1^1, d_2^1, d_3^1, d_4^1, c_1^1, s_1^1, s_2^1, s_3^1, s_4^1, s_5^1, \ldots, d_1^i, d_2^i, d_3^i, d_4^i, c_1^i, s_1^i, s_2^i, s_3^i, s_4^i, s_5^i, \ldots, d_1^{q(n)}, d_2^{q(n)}, d_3^{q(n)}, d_4^{q(n)}, c_1^{q(n)}, s_1^{q(n)}, s_2^{q(n)}, s_3^{q(n)}, s_4^{q(n)}, s_5^{q(n)})$
2. Randomly select $l$, $1 \le l \le q(n)$ and rewind to the point (in $l$th iteration) where $d_1^1, d_2^1, d_3^1, d_4^1, c_1^1, s_1^1, s_2^1, s_3^1, s_4^1, s_5^1, \ldots, d_1^i, d_2^i, d_3^i, d_4^i$ is produced. Continue to run $\left\langle P^*(e, r_1, r_2, \alpha, \pi), V\right\rangle(p, g, h, a, y, T_1, T_2)$ from the rewinding point, set $\bar{c}_1^l$ and obtain the rest $s_1^{i\prime}, s_2^{i\prime}, s_3^{i\prime}, s_4^{i\prime}, s_5^{i\prime}, \ldots$

Note that it is important to randomly select $l$ in step 2, we describe the reason as follows.

Let T be the computation tree of $E\left(\left\langle P^*(e, r_1, r_2, \alpha, \pi), V\right\rangle(p, g, h, a, y, T_1, T_2)\right)$ and $l$th

level correspond to $\left(D_1^l, D_2^l, D_3^l, D_4^l, C_1^l, S_1^l, S_2^l, S_3^l, S_4^l, S_5^l\right)$. There are total q(n) levels. Nodes in the *q(n)*th level are accepting nodes. Let $N_i$ be the number of nodes in the *i*th level of T. There must be *i* such that $N_{i+1} \geq \frac{4}{3} N_i$ since otherwise the accepting probability of $\left\langle P^*(e, r_1, r_2, \alpha, \pi), V\right\rangle(p, g, h, a, y, T_1, T_2)$ is negligible. We call this level *heavy*. For this *i*, at least a third of $N_i$ nodes have two children, i.e. for each such node, $c_1^i$ and $\bar{c}_1^i$ leads to acceptance. We figure out the computation tree T roughly as Figure 3.5.

Now we consider the success probability of $E\left(\left\langle P^*(e, r_1, r_2, \alpha, \pi), V\right\rangle(p, g, h, a, y, T_1, T_2)\right)$. The success probability of step 1 is *1/p(n)*. The probability that *l* (in step 2) hits a heavy level is at least *1/q(n)*. The probability that we choose the rewinding point $\bar{c}_1^l$ (in step 2) is *1/3*. Overall, the probability of getting the knowledge from

$(d_1^1, d_2^1, d_3^1, d_4^1, c_1^1, s_1^1, s_2^1, s_3^1, s_4^1, s_5^1, \ldots, \underline{d_1^l, d_2^l, d_3^l, d_4^l, 0, s_1^l, s_2^l, s_3^l, s_4^l, s_5^l},$
$\ldots, d_1^{q(n)}, d_2^{q(n)}, d_3^{q(n)}, d_4^{q(n)}, c_1^{q(n)}, s_1^{q(n)}, s_2^{q(n)}, s_3^{q(n)}, s_4^{q(n)}, s_5^{q(n)})$

and $(d_1^1, d_2^1, d_3^1, d_4^1, c_1^1, s_1^1, s_2^1, s_3^1, s_4^1, s_5^1, \ldots, \underline{d_1^l, d_2^l, d_3^l, d_4^l, 0, s_1^{l\prime}, s_2^{l\prime}, s_3^{l\prime}, s_4^{l\prime}, s_5^{l\prime}}, \ldots)$

is 1/(*3p(n)q(n)*). Thus, we can first compute c = H(m, p, g, h, y, a) and then compute $e = s_1^l - s_1^{l\prime}$, $r_1 = s_2^l - s_2^{l\prime}$, $r_2 = s_3^l - s_3^{l\prime}$, $\alpha = \frac{1}{c}\left(s_4^l - s_4^{l\prime}\right)$, and $\pi = \frac{1}{c}\left(s_5^l - s_5^{l\prime}\right)$ with probability 1/(*3p(n)q(n)*) for each execution $E\left(\left\langle P^*(e, r_1, r_2, \alpha, \pi), V\right\rangle(p, g, h, a, y, T_1, T_2)\right)$. If we repeated *3np(n)q(n)* times, the success probability is at least $1-2^{-n}$.

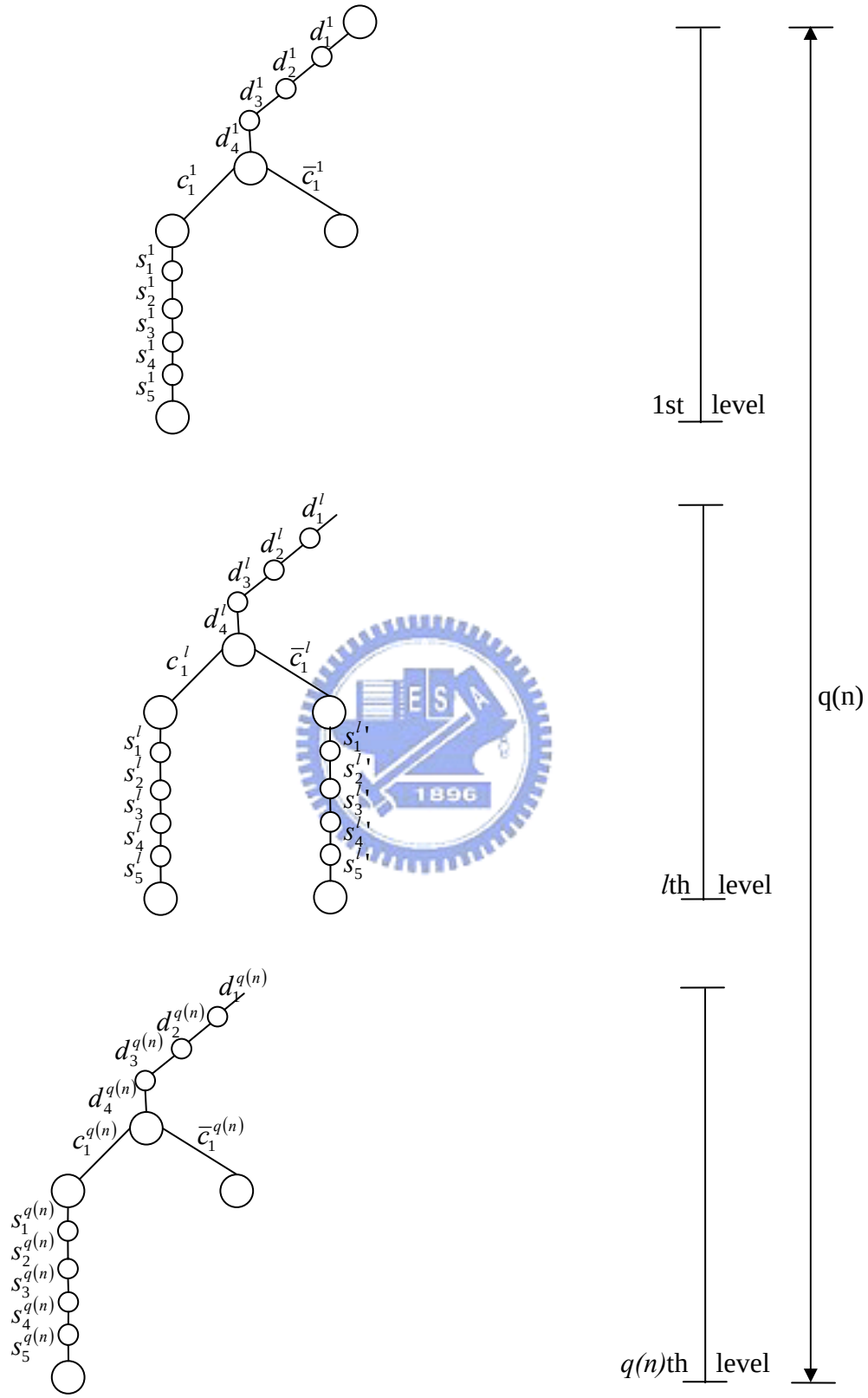


Figure 3.5: The computation tree of $E\left(\left\langle P^*(e, r_1, r_2, \alpha, \pi), V\right\rangle(p, g, h, a, y, T_1, T_2)\right)$

***Perfect Zero-knowledge***

Let *r* be the *q(n)*-bit random string used by $V^*$, $V^*$'s view of interaction with P on $(p, g, h, a, y, T_1, T_2)$ is ($r$, $d_1$, $d_2$, $d_3$, $d_4$, $c_1$, $s_1$, $s_2$, $s_3$, $s_4$, $s_5$), where $(p, g, h, a, y, T_1, T_2)$ is discarded for notational simplicity. We observe that $c_1$ depends on $(p, g, h, a, y, T_1, T_2)$, $r$, $d_1$, $d_2$, $d_3$, and $d_4$, that is, $\tilde{V}^*((p, g, h, a, y, T_1, T_2), r, d_1, d_2, d_3, d_4) = c_1$. Therefore, for any fixed $\tilde{r}$, $\tilde{d}_1$, $\tilde{d}_2$, $\tilde{d}_3$, $\tilde{d}_4$, $\tilde{c}_1$, $\tilde{s}_1$, $\tilde{s}_2$, $\tilde{s}_3$, $\tilde{s}_4$, $\tilde{s}_5$ with constraints $\tilde{d}_1 = T_2^{\tilde{c}_1} g^{\tilde{s}_1} \bmod p$, $\tilde{d}_2 = a^{\tilde{c}_1} g^{\tilde{s}_2} h^{\tilde{s}_3} \bmod p$, $\tilde{d}_3 = (y^c)^{\tilde{c}_1} g^{\tilde{s}_4} h^{\tilde{s}_5} \bmod p$, and $\tilde{d}_4 = T_1^{\tilde{c}_1} Y_j^{\tilde{s}_1} g^{\tilde{s}_2} h^{\tilde{s}_3} / g^{\tilde{s}_4} h^{\tilde{s}_5} \bmod p$, we have

$$\Pr\left[(R, D_1, D_2, D_3, D_4, C_1, S_1, S_2, S_3, S_4, S_5) = (\tilde{r}, \tilde{d}_1, \tilde{d}_2, \tilde{d}_3, \tilde{d}_4, \tilde{c}_1, \tilde{s}_1, \tilde{s}_2, \tilde{s}_3, \tilde{s}_4, \tilde{s}_5)\right]$$
$$= \frac{||\tilde{V}^*((p,g,h,a,y,T_1,T_2),\tilde{r}, \tilde{d}_1, \tilde{d}_2, \tilde{d}_3, \tilde{d}_4) = \tilde{c}_1||}{2^{q(n)} \cdot q^3}$$

The simulator *M* simulates the view $((p, g, h, a, y, T_1, T_2), \tilde{r}, \tilde{d}_1, \tilde{d}_2, \tilde{d}_3, \tilde{d}_4, \tilde{c}_1, \tilde{s}_1, \tilde{s}_2, \tilde{s}_3, \tilde{s}_4, \tilde{s}_5)$ of $\langle P(e, r_1, r_2, \alpha, \pi), V^* \rangle (p, g, h, a, y, T_1, T_2)$ as follows.

1. Randomly select a bit string r'.
2. Randomly select a bit $c_1$'' and $s_1$', $s_2$', $s_3$', $s_4$', $s_5$'$\in Z_q$, and compute

   $d_1' = T_2^{c_1''} g^{s_1'} \bmod p$, $d_2' = a^{c_1''} g^{s_2'} h^{s_3'} \bmod p$,
   $d_3' = (y^c)^{c_1''} g^{s_4'} h^{s_5'} \bmod p$, $d_4' = T_1^{c_1''} Y^{s_1'} g^{s_2'} h^{s_3'} / g^{s_4'} h^{s_5'} \bmod p$
3. *M* runs $\tilde{V}^*((p, g, h, a, y, T_1, T_2), r', d_1', d_2', d_3', d_4') = c_1'$. If $c_1$' = $c_1$'', output $(r', d_1', d_2', d_3', d_4', c_1', s_1', s_2', s_3', s_4', s_5')$; otherwise, output $\perp$.

In step 2, *V** does not know *M*'s selection $c_1$'', which means

$$\Pr_{C_1'',S_1,S_2,S_3,S_4,S_5}\left[\tilde{V}^*\left(\begin{matrix}(p,g,h,a,y,T_1,T_2),r',\\ T_2^{c_1''}g^{S_1},a^{C_1''}g^{S_2}h^{S_3},(y^c)^{C_1''}g^{S_4}h^{S_5},T_1^{C_1''}Y^{S_1}g^{S_2}h^{S_3}/g^{S_4}h^{S_5}\end{matrix}\right)=C_1''\right]$$

$$=\frac{1}{2\cdot q^5}\cdot\sum_{s_1',s_2',s_3',s_4',s_5'}\left(\begin{matrix}\left\|\tilde{V}^*\left(\begin{matrix}(p,g,h,a,y,T_1,T_2),r',\\ T_2^0g^{s_1'},a^0g^{s_2'}h^{s_3'},(y^c)^0g^{s_4'}h^{s_5'},T_1^0Y^{s_1'}g^{s_2'}h^{s_3'}/g^{s_4'}h^{s_5'}\end{matrix}\right)=0\right\|\\ +\left\|\tilde{V}^*\left(\begin{matrix}(p,g,h,a,y,T_1,T_2),r',\\ T_2^1g^{s_1'},a^1g^{s_2'}h^{s_3'},(y^c)^1g^{s_4'}h^{s_5'},T_1^1Y^{s_1'}g^{s_2'}h^{s_3'}/g^{s_4'}h^{s_5'}\end{matrix}\right)=1\right\|\end{matrix}\right)$$

$$=\frac{1}{2\cdot q^5}\cdot q^2\cdot\sum_{d_1',d_2',d_3',d_4'}\left(\begin{matrix}\left\|\tilde{V}^*\left((p,g,h,a,y,T_1,T_2),r',d_1',d_2',d_3',d_4'\right)=0\right\|\\ +\left\|\tilde{V}^*\left((p,g,h,a,y,T_1,T_2),r',d_1',d_2',d_3',d_4'\right)=1\right\|\end{matrix}\right)$$

$$=\frac{1}{2\cdot q^3}\cdot q^3$$

$$=\frac{1}{2}$$

Hence, for $\tilde{r},\tilde{d}_1,\tilde{d}_2,\tilde{d}_3,\tilde{d}_4,\tilde{c}_1,\tilde{s}_1,\tilde{s}_2,\tilde{s}_3,\tilde{s}_4,\tilde{s}_5$

$$\Pr\left[\begin{matrix}(R',D_1',D_2',D_3',D_4',C_1',S_1',S_2',S_3',S_4',S_5')\\ =(\tilde{r},\tilde{d}_1,\tilde{d}_2,\tilde{d}_3,\tilde{d}_4,\tilde{c}_1,\tilde{s}_1,\tilde{s}_2,\tilde{s}_3,\tilde{s}_4,\tilde{s}_5)\end{matrix}\middle|M(V^*,(p,g,h,a,y,T_1,T_2))\neq\perp\right]$$

$$=\frac{\Pr\left[\begin{matrix}(R',D_1',D_2',D_3',D_4',C_1',S_1',S_2',S_3',S_4',S_5')\\ =(\tilde{r},\tilde{d}_1,\tilde{d}_2,\tilde{d}_3,\tilde{d}_4,\tilde{c}_1,\tilde{s}_1,\tilde{s}_2,\tilde{s}_3,\tilde{s}_4,\tilde{s}_5)\\ and\ \ M(V^*,(p,g,h,a,y,T_1,T_2))\neq\perp\end{matrix}\right]}{\Pr\left[M(V^*,(p,g,h,a,y,T_1,T_2))\neq\perp\right]}$$

$$=\frac{\sum_{C_1''}\left(\begin{matrix}\Pr[R'=\tilde{r},S_1'=\tilde{s}_1,S_2'=\tilde{s}_2,S_3'=\tilde{s}_3,S_4'=\tilde{s}_4,S_5'=\tilde{s}_5,C_1''=c_1'']\cdot\\ \left\|\begin{matrix}\tilde{d}_1=T_2^{\tilde{c}_1}g^{\tilde{s}_1}\bmod p,\tilde{d}_2=a^{\tilde{c}_1}g^{\tilde{s}_2}h^{\tilde{s}_3}\bmod p,\\ \tilde{d}_3=(y^c)^{\tilde{c}_1}g^{\tilde{s}_4}h^{\tilde{s}_5}\bmod p,\tilde{d}_4=T_1^{\tilde{c}_1}Y^{\tilde{s}_1}g^{\tilde{s}_2}h^{\tilde{s}_3}/g^{\tilde{s}_4}h^{\tilde{s}_5}\bmod p,\\ \tilde{V}^*\left((p,g,h,a,y,T_1,T_2),\tilde{r},\tilde{d}_1,\tilde{d}_2,\tilde{d}_3,\tilde{d}_4\right)=c_1'',c_1''=\tilde{c}_1\end{matrix}\right\|\end{matrix}\right)}{\Pr\left[\tilde{V}^*\left((p,g,h,a,y,T_1,T_2),\tilde{r},\tilde{d}_1,\tilde{d}_2,\tilde{d}_3,\tilde{d}_4\right)=c_1'',c_1''=\tilde{c}_1\right]}$$

$$= \frac{\left\| \begin{array}{l} \tilde{d}_1 = T_2^{\tilde{c}_1} g^{\tilde{s}_1} \bmod p, \tilde{d}_2 = a^{\tilde{c}_1} g^{\tilde{s}_2} h^{\tilde{s}_3} \bmod p, \\ \tilde{d}_3 = (y^c)^{\tilde{c}_1} g^{\tilde{s}_4} h^{\tilde{s}_5} \bmod p, \tilde{d}_4 = T_1^{\tilde{c}_1} Y^{\tilde{s}_1} g^{\tilde{s}_2} h^{\tilde{s}_3} / g^{\tilde{s}_4} h^{\tilde{s}_5} \bmod p, \\ \tilde{V}^*\left((p,g,h,a,y,T_1,T_2),\tilde{r}, \tilde{d}_1, \tilde{d}_2, \tilde{d}_3, \tilde{d}_4\right) = \tilde{c}_1 \end{array} \right\|}{2 \cdot 2^{q(n)} \cdot q^3}$$

$$= \frac{\left\| \tilde{V}^*\left((p,g,h,a,y,T_1,T_2),\tilde{r}, \tilde{d}_1, \tilde{d}_2, \tilde{d}_3, \tilde{d}_4\right) = \tilde{c}_1 \right\|}{2^{q(n)} \cdot q^3}$$

for $\tilde{d}_1 = T_2^{\tilde{c}_1} g^{\tilde{s}_1} \bmod p, \tilde{d}_2 = a^{\tilde{c}_1} g^{\tilde{s}_2} h^{\tilde{s}_3} \bmod p,$

$\tilde{d}_3 = (y^c)^{\tilde{c}_1} g^{\tilde{s}_4} h^{\tilde{s}_5} \bmod p, \tilde{d}_4 = T_1^{\tilde{c}_1} Y^{\tilde{s}_1} g^{\tilde{s}_2} h^{\tilde{s}_3} / g^{\tilde{s}_4} h^{\tilde{s}_5} \bmod p$

The expected run time of $M(V^*,(p, g, h, a, y, T_1, T_2))$ is $2 \cdot \text{time}_{V^*}(p, g, h, a, y, T_1, T_2)$, which is polynomial bounded. Therefore, the protocol is secure with perfect zero-knowledge.

## 3.3.2 Properties

We can find out that our scheme has the properties of correctness, confidentiality, fairness, privacy, public verifiability, and robustness. And most important of all, our scheme has the property of publicly verifiable bid validity. We describe them more detail in the following.

- **Correctness**

  If all parties act honestly, the winning price and the winner (s) are determined according to our auction rule correctly.

- **Confidentiality**

  We use the registration manager RM to hold the relationship between the bidder's identity and his public key and the auction manager AM to hold the

decryption keys for all bidding prices. Hence, even every one can verify the validity of the bids, but no one can get any information about the bidder's identity and his bidding price.

- **Fairness**

  All bidders can look a proper polling on Internet and after each bidder submits his bid, he can not modify it. Besides, each bid contains the bidder's signature and no bidder can deny.

- **Privacy**

  In our scheme, even after the opening phase, the bidding prices of the losing bidders can be kept secret since the remainders of the decryption keys are not published by the auction manager AM.

- **Public Verifiability**

  In the opening phase, the auction manager AM would publish the decryption keys corresponding to the bidding prices downwards until the winner is published. Every one can verify the result of the auction with those decryption keys published. Hence, the validity of the result in our auction can be publicly verified by every one.

- **Robustness**

  In our scheme, every one can verify the validity of the bid. If there exist some invalid bids, anyone can ask the auction manager AM to revoke those invalid bids. Hence, our scheme can prevent malicious bidder sending invalid bids to disturb the auction. In other word, even there are invalid bids from malicious bidders, the result of our scheme is correct.

- **Public Verifiable Bid Validity**

In our scheme, every one can verify the validity of the bidder and the validity of the bidder's bidding price with the proofs for verifiable encryption of signature of knowledge.

# Chapter 4

# Conclusion

In this thesis, we have proposed a sealed-bid auction with publicly verifiable bid validity. Our scheme is one of the first-price sealed-bid auctions. It has the properties of correctness, confidentiality, fairness, privacy, public verifiability, and robustness. Most important of all, in our scheme, every one can publicly verify the validity of the bid such that malicious bidders can not send invalid bids to disturb the auction.

In our scheme, we combine the bidder's signature and his bidding price as the bids using verifiable encryption of signature of knowledge and then use 1-out-of-P re-encryption proof of encryption keys. The signature we use here needs the bidder's password memorized in bidder's mind and the corresponding partial secret stored in his mobile devices to increase the security.

Bid-validity in our scheme contains not only the validity of bidding price but also the validity of the bidder. In our scheme, every one can verify the bid validity but he can not get any information about the bidder's identity and his bidding price. If there exist some invalid bids, anyone can ask the auction manager AM to revoke those invalid bids. Hence, our protocol can prevent malicious bidder sending invalid bids to disturb the auction.

In our scheme, if the registration manager RM is attacked, only the information about the relation of the bidder's identity and his public key is leaked, no one can have the idea about the bidding price that the bidder bids. If the auction manager AM is attacked, only the information about the bidding price of the bidder is leaked, no

one can get the idea about the relation between the bidder's identity and his public key. In other words, in our scheme, if one manager is attacked, our scheme can achieve weak confidentiality. But if two managers collaborate, they can know the relation of the bidding price and the corresponding bidder's identity. Besides, in the bidding phase of our scheme, each bidder has to send his bid with (P+1) proofs. The number of proofs needs to depend on the size of the price list. Hence, in future work, we hope to avoid the collaboration attack of the managers and reduce the number of proofs.

# Bibliography


[1] C. Cachin, “Efficient private bidding and auctions with an oblivious third party,” In *Proceedings of the 6th ACM conference on Computer and communications security*, pages 120-127. ACM Press, 1999.

[2] H. Kikuchi, “(M + 1)-st price auction,” In Paul F. Syverson, editor, *Financial Cryptography, 5th International Conference, FC 2001*, volume 2339 of *Lecture Notes in Computer Science*, pages 351-363. Springer-Verlag, 2002.

[3] H. Kikuchi,M. Harkavy, and J. D. Tygar, “Multi-round anonymous auction protocols,” In *Proceedings of the First IEEE Workshop on Dependable and Real-Time E-Commerce Systems*, pages 62-69, 1998.

[4] H. Kikuchi, S. Hotta, K.Abe, and S. Nakanishi, “Distributed auction servers resolving winner and winning bid without revealing privacy of bids,” In *Proceedings of International Workshop on Next Generation Internet (NGITA 2000)*, pages 307-312, 2000.

[5] J. Camenisch and I. Damgard, “Verifiable encryption, group encryption, and their Applications to separable group signatures and signature sharing schemes,” In Tatsuaki Okamoto, editor, *Advances in Cryptology* - ASIACRYPT *2000*, volume 1976 of *Lecture Notes in Computer Science*, pages 331-345. Springer-Verlag, 2000.

[6] K. Omote and A. Miyaji, “A second-price sealed-bid auction with verifiable discriminant of $p_0$-th root,” In Matt Blaze, editor, *Financial Cryptography, 6th*

*International Conference, FC 2002*, volume 2357 of *Lecture Notes in Computer Science*, pages 57-71. Springer-Verlag, 2003.

[7] K. Peng, C. Boyd, E. Dawson, and K. Viswanathan, "Five sealed-bid auction models," In *Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003*, pages 77-86. Australian Computer Society, 2003.

[8] K. Suzuki, K. Kobayashi, and H. Morita, "Efficient sealed-bid auction using hash chain," In Dongho Won, editor, *Information Security and Cryptology - ICISC 2000*, volume 2015 of *Lecture Notes in Computer Science*, pages 183-191. Springer-Verlag, 2000.

[9] M. Abe and K. , "M + 1-st price auction using homomorphic encryption," In David Naccache and Pascal Paillier, editor, *Public Key Cryptography, 5th International Workshop on Practice and Theory in Public Key Cryptosystems, PKC 2002*, volume 2274 of *Lecture Notes in Computer Science*, pages 115-124. Springer-Verlag, 2002.

[10] M. Harkavy and J. D. Tygar and H. Kikuchi, "Electronic auctions with private bids," In *Proceeding of 3rd USENIX Workshop on Electronic Commerce*, 1998.

[11] M. Hirt and K. Sako, "Efficient receipt-free voting based on homomorphic encryption," In Bart Preneel, editor, *Advances in Cryptology - EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Computer Science*, pages 539-556. Springer-Verlag, 2000.

[12] M. K. Franklin and M. K. Reiter, "The design and implementation of a secure

,” In *IEEE Transactions on Software Engineering*, pages 302-312, IEEE Computer Society, 1996.

[13] M. Naor, B. Pinkas and R. Sumner, “Privacy preserving auctions and mechanism design,” In *Proceedings of the 1st ACM conference on Electronic commerce*, pages 129-139. ACM Press, 1999.

[14] S. Liu, C. Wang, and Y. Wang, “A secure multi-round electronic auction scheme,” In *Proceedings of the EUROCOMM 2000*, pages 330-334. Germany, May 2000.

[15] S. Shin, K. kobara, and H. Imai, “Leakage-resilient authenticated key establishment protocols,” In Chi-Sung Laih, editor, *Advances in Cryptology - ASIACRYPT 2003*, volume 2894 of *Lecture Notes in Computer Science*, pages 155-172. Springer-Verlag, 2000.

[16] Y. Watanabe and H. Imai, “Reducing the round complexity of a sealed-bid auction protocol with an off-line TTP,” In *Proceedings of the 7th ACM Conference on Computer and Communications Security*, pages 80-86. ACM Press, 2000.