Hindawi
Security and Communication Networks
Volume 2021, Article ID 6690766, 12 pages
https://doi.org/10.1155/2021/6690766

Research Article

BA^{2}P : Bidirectional and Anonymous Auction Protocol with Dispute-Freeness

Ke Huang,[1] **Yi Mu**,[2] **Fatemeh Rezaeibagha**,[3] **Zheyuan He**,[1] **and Xiaosong Zhang**[1]

[1]*College for Cyber Security, University of Electronic Science and Technology of China (UESTC), Chengdu 611731, China*
[2]*Faculty of Data Science, City University of Macau, Macao, China*
[3]*Discipline of Information Technology, Murdoch University, Perth, Australia*

Correspondence should be addressed to Yi Mu; ymu.ieee@gmail.com

Received 30 November 2020; Revised 6 September 2021; Accepted 24 September 2021; Published 15 October 2021

Academic Editor: Prosanta Gope

Electronic auction is a popular platform to sell goods, task assignment, and resources' allocation due to reductions of transaction costs and has attracted a huge number of potential buyers. However, it is challenging to address the disputes between the buyer and the auctioneer. The main reason is, on the one hand, solving such problem leverages to the broad domain of research aspects, such as economic theory, engineering, and cryptography, and, on the other hand, it is difficult to arbitrate in a decentralized and anonymous setting. In this work, we consider a more general framework to solve the potential disputes by enforcing bidirectional confirmation and public verification. Hence, the bidding procedure is clear to inspect and potential disputes can be erased. To achieve this goal, we propose policy-driven chameleon hash and revised linkable-and-redactable ring signature as building blocks. We used these two tools to build a bidirectional and anonymous auction protocol called BA^{2}P. In our BA^{2}P protocol, the bidders can competitively and anonymously place their bids to outbid others. At the end of the auction protocol, everyone can verify the validity of the bidding proof and decide the winner. Thus, dispute-freeness feature is achieved. The analysis suggests that our proposal is provably secure and practically efficient, and it trades some efficiencies with dispute-freeness feature.

1. Introduction

Auction is a process to buy or sell commodities and services [1]. Specifically, the auction is a market institution in which traders or parties submit bids that can be an offer to buy or sell at a given price. Typically, an auction includes the following entities: bidder, seller, auctioneer, commodity, valuation, and price. Electronic auction (E-auction) is a fundamental part of the electronic commerce technology [2]. The Internet-turned e-auction is the most successful stories of web-based services. It removes physical limitations by enabling convenient and fast auction services remotely for audiences at any time and any space [2]. Due to the reductions in transaction costs, huge potential buyers, and independence of time and space, e-auctions are popular mechanisms to sell goods, task assignment, resources' allocation, etc. [1]. English auction and sealed-bid auctions are two most commonly known auction types. In an English auction, buyers call out their prices increasingly. In a sealed-bid auction, prices are privately submitted to the auctioneer. In addition, the auction can be categorized by the seller-side and the buyer side auction. According to different types of auctions, there could be n buyers to 1 seller, 1 buyer to n sellers, or even n buyers to m sellers [1].

Ensuring the e-auction protocol working properly is essential, especially considering the increasingly valuable assets traded in e-auction and people's increasing preference to purchase items online. Due to the heterogeneity, freely accessible, and full anonymity of the Internet, e-auction protocols suffer from frequent and unprecedented threats from insiders (malicious buyer or auctioneer) and outsiders (e.g., hackers). For example, Abe and Suzuki [3] identified the bid-rigging problem in the sealed auction where the buyer seeks to manipulate the auction by ordering other bidders to bid very low price. This problem could be considered as an insider attack. One of the most challenging

problems is dispute settlement and arbitration. During the execution of the e-auction protocol, doubts of the fairness during auction procedure and potential disputes between the buyer and the auctioneer may arise. However, solutions offer us a broad research domain: economy [4], engineering, and cryptography [5, 6]. For instance, how to reach [1] the nash equilibrium in game theory or how to achieve fair arbitration from the legal aspect. This is challenging in a totally decentralized and anonymous setting where the buyer's identity and the bids are concealed. Ring signature is generally adopted to achieve the buyer anonymity in e-auction protocols [7–9]. Unlike group signature, which requires a group manager for setup, ring signature greatly simplifies the design by removing the need for a centralized entity. However, this also brings difficulties to arbitrate disputes since every buyer is hidden in pseudonyms and no justifiable evidence and mechanism are provided to support the dispute settlement.

In this work, by using chameleon hash and ring signature, we give a solution to the aforementioned problems. Simply, Chameleon Hash or Trapdoor Commitment (TC) (also known as a trapdoor one-way hash function) [10] can be viewed as a box with a secret lock. It allows the holder of the key to change the secret (i.e., a committed value) in the box even after the box is locked. Such property allows both the buyer and the auction manager to confirm the bids securely while evidences can be revealed to the public for verification. As long as the buyer or the auction manager finds the bid suspicious or wrong, he will not confirm it. As a result, dispute-freeness is achieved since all successfully placed bids are guaranteed by dual confirmation and cryptographic proof.

In this work, we propose a bidirectional and anonymous auction protocol with dispute-freeness, called BA^{2}P. The framework of our proposal is shown in Figure 1. Similar to the English auction, but with slight adaptations, our proposal allows the buyer to place his bid competitively. The bid is placed anonymously based on ring signature and the use of anonymous cryptocurrency and pseudonym for privacy concerns. An auction manager is delegated to confirm and verify the bids. All bids are bidirectionally verified and confirmed and then revealed during the Open Phase to the public to achieve the dispute-freeness. We propose Policy-driven Chameleon Hash (PCH) and Revised Linkable-and-Redactable Ring signature (R-LRRS) as building blocks to construct our BA^{2}P scheme. Our contributions can be highlighted as below:

(1) We propose the PCH and R-LRRS as building blocks. PCH is a trapdoor one-way hash function with both deterministic and probabilistic hashing algorithms. R-LRRS is a revised version of our previously proposed ring signature [11].

(2) Our proposed BA^{2}P is divided into five phases: initiation, prebidding, bidding, confirmation, and open. Our BA^{2}P leverages PCH and R-LRRS to achieve bidirectional and anonymous bidding with dispute-freeness. Cryptocurrency and pseudonyms are used to achieve transaction and identity privacies for buyers. The buyer can competitively place his bids in order to win the auction. An auction manager is delegated to verify and confirm the bidder's proof. As each proof is dually confirmed and is publicly verifiable, dispute-freeness feature is provided.

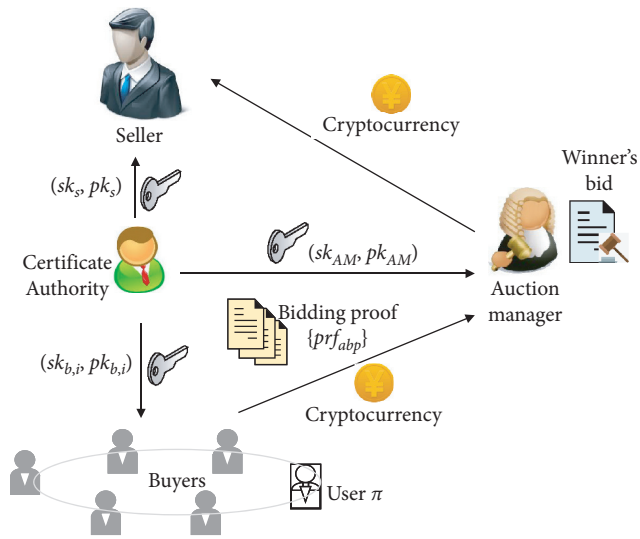

Figure 1: The framework of BA^{2}P protocol.

(3) We give the system model and several security requirements of our proposed BA^{2}P. Followed by detailed construction as well as the predefined model, we give security and complexity analysis of our scheme. The evidence suggests that our proposal is provably secure based on intractable assumptions. Meanwhile, our proposal is practically efficient.

2. Related Works

Zhang et al. [1] conducted a comprehensive survey of recent auction approaches. They systematically reviewed the auction-based applications and mechanisms in wireless and mobile systems. Their work is helpful for the reader to study this topic. We summarize the related works on auction protocols as follows.

Cryptography offers a broad range of tools for the diverse designs of early auction systems and protocols. From 1999 to 2010, a number of works have been proposed, which applied cryptographic algorithms to achieve various desired properties for auction. Naor et al. [12] proposed an efficient sealed-bid, two-server auction system. This was an early design of private auction. Later, Viswanathan and Dawson [13] proposed a simple, efficient, and secure design to achieve sealed bidding with anonymity. They utilized modular approach in the analysis and design methodology. Later, Nguyen and Traore [7] proposed a public auction protocol that utilized blind group signatures to achieve bidder privacy. Differently, they considered public auction. The design of the public auction scheme was generally diverse to private auction. Omote and Miyaji [14] proposed to achieve English auction with efficient bidding and verification by using bulletin board. Their scheme enables easy

revocation and one-time registration. Their scheme is desirable for users with limited computing capabilities. Abe and Suzuki [3] identified the bid-rigging problem in the sealed auction where the buyer seeks to manipulate the auction by ordering other bidders to bid very low price. Peng et al. [15] proposed a new concept, called relative bid privacy.

They proposed a new mix network to implement an auction with relative bid privacy. Specifically, they employed ElGamal encryption and re-encryption to hide bidding information. Juels and Szydlo [23] introduced verifiable proxy oblivious transfer to address the security vulnerability in Naor et al.'s work [12]. Xiong et al. [8] proposed an efficient sealed-bidding protocol based on ring signature and variable technique of encryption key chain where the auctioneer is allowed to determine the winning bid while the losing bids are not revealed. Later, Xiong et al. [9] proposed an efficient and spontaneous privacy-preserving English auction protocol based on revocable ring signature. In comparison with their previous work [8], the new scheme in [9] offers conditional privacy-preservation and one-time registration. Most importantly, it is more efficient than the previous work in both communication and computation complexities. Following this, Nojoumian and Stinson [24] built a first-price auction protocol based on a new commitment. A multicomponent commitment is proposed as a building block, in which three schemes with diverse properties are proposed. In another work, Dong and Pang [25] formally studied the notion of receipt-freeness and bidding-price-secrecy by the formalization of observational equivalences and analysis.

From 2010 to 2021, the design of auction protocol is mainly affected by the development of cryptography as well as diverse applications. Galal and Youssef [26] proposed several cryptographic primitives as building blocks to achieve a smart contract protocol for a succinctly verifiable sealed-bid auction on the Ethereum blockchain. Here, Ethereum is a decentralized platform based on blockchain technology. Smart contract is a Turing-complete protocol to achieve arbitrary computer program in Ethereum. Galal and Youssef [22] proposed another smart contract-based verifiable sealed-bid auction on the Ethereum blockchain. Similarly, multiple cryptographic primitives are used as building blocks to achieve the design. However, these constructions are generally complex and inefficient. Galal and Youssef [27] proposed Trustee as a trusted and efficient Vickrey auction on top of Ethereum for full privacy-preservation with much lower fees for the online auction. A prototype of Trustee for the inspection and security analysis and gas costs are provided. Jiao et al. [28] proposed an auction-based market model based on proof-of-work based blockchain network for computing resource allocation. Nguyen and Thai [29] exploited smart contract and state channel technologies to achieve decentralized and trustless framework for iterative double auction. An et al. [30] exploited smart contract and greedy strategy to achieve trustless crowdsensed data trading in reverse auction. As observed, Ethereum is a promising and popular platform to develop auction protocol since it supports fast payment and provides smart contract to enable application-rich services.

We compare our scheme with relevant works in Table 1 with a focus on privacy-preservation. Similarly, we employed a standard cryptographic algorithm called chameleon hash to achieve bidder's anonymity and hidden bids. Noticeably, we do not rely on a trusted auctioneer since we can run an arbitration protocol to settle the disputes and it is publicly verifiable. To generalize, the early works have mainly focused on utilizing specific methodology or tool as solution, while current works have adopted multiple technologies. Current designs have heavily relied on multiple cryptographic building blocks [22, 26], which imposed high complexities to both design and performance. However, a work focusing on the dispute settlement or with arbitration does not exist in the literature. Therefore, once users have doubts over the process and outcomes, there is no easy way and clear evidence to justify.

3. Preliminary

We give some preliminary knowledge used in our work.

3.1. Complexity Assumptions. Let G be a cyclic multiplicative group generated by g with prime order q. We informally state the following assumptions:

Discrete logarithm problem (DLP): given $g^a \in G$, where $a \xleftarrow{R} Z_q$, computing a is hard.

Decisional Diffie–Hellman problem (DDHP): given $g, g^a, g^b, g^c \in G$, where $a, b, c \xleftarrow{R} Z_q$, deciding whether $c = ab$ is hard.

Computational Diffie–Hellman problem (CDHP): given $g, g^a, g^b \in G$, where $a, b \xleftarrow{R} Z_q$, computing g^{ab} is hard.

q-Strong Diffie–Hellman problem (q-SDHP) [31]: choose $x \xleftarrow{R} Z_q$. Given a $(q+1)$-tuple $(g, g^x, \ldots, g^{x^q}) \in G^{q+1}$ and a generator g of q-order cyclic group G, computing $(c, g^{1/(x+c)})$ for some $c \in Z_q^*$ is hard.

3.2. Bilinear Pairing. Given two multiplicative groups G and G_T with the same group order q and generator g, denote $\hat{e}: G \times G \longrightarrow G_T$ as symmetric bilinear map, where $\hat{e}(x^a, y^b) = \hat{e}(x, y)^{ab}$, for all $x, y \in G$ and $a, b \xleftarrow{R} Z_q$. Additionally, compute $\hat{e}(g, g) \neq 1$ is efficient.

3.3. Unpredictable File Source. We give the notion of "unpredictable file source" [32] as follows. This notion is used to capture the lower bound of our security given in Section 7.

Specifically, denote file source $\mathcal{M}$ as a polynomial algorithm which on input λ, it outputs $(M_0, \ldots, M_{n-1}, Z)$. Denote $M_0, \ldots, M_{n-1} \in \{0,1\}^*$ as random vectors and $Z \in \{0,1\}^*$ as auxiliary information. Fix n by $\{1, 2\}$. The guessing probability of $\mathcal{M}$ is defined by $gp_{\mathcal{M}} = Max\{gp(M_j|Z)\}$. We state that $\mathcal{M}$ is an unpredictable file source if $gp_{\mathcal{M}}$ is negligible.

Table 1: Comparison of bidding schemes.

Scheme	Technique	Auctioneer	Hidden bids	Opener of bids
Our work	Chameleon hash	Distrusted	Yes	Bidder
Franklin and Reiter [16]	Verifiable signature sharing	Distrusted	No	Auctioneer
Kikuchi et al. [17]	Secret sharing	Trusted	Yes	Auctioneer
Sako. [18]	Standard cryptographic algorithms	Trusted	Yes	Auctioneer
Suzuki and Kobayashi [19]	Verifiable encryption	Distrusted	Yes	Auctioneer
Suzuki and Yokoo [20]	Homomorphic encryption	Distrusted	Yes	Bidder
Peng et al. [21]	Secret sharing	Distrusted	Yes	Auctioneer
Xiong et al. [8]	Ring signature	Trusted	Yes	Bidder
Galal and Youssef et al. [22]	Commitment and zero-knowledge proof	Distrusted	Yes	Auctioneer

4. Building Blocks

We introduce the building blocks of our work in this section.

4.1. Policy-Driven Chameleon Hash. We propose the Policy-driven Chameleon Hash (PCH) as follows: PCH is a variant of chameleon hash (Trapdoor Commitment (TC) [10]) featured by two different hashing algorithms: Probabilistic Hashing $\mathscr{H}_{\text{PCH}}$ and Deterministic Hashing $\widehat{\mathscr{H}}_{\text{PCH}}$. To explain, $\mathscr{H}_{\text{PCH}}$ generates each hash with a freshly chosen randomness, while $\widehat{\mathscr{H}}_{\text{PCH}}$ computes each hash deterministically from the message itself (similar as hash-as-a-key method [32]). A PCH scheme consists of the following five algorithms $(\mathscr{G}_{\text{PCH}}, \mathscr{H}_{\text{PCH}}, \widehat{\mathscr{H}}_{\text{PCH}}, \mathscr{V}_{\text{PCH}}, \mathscr{R}_{\text{PCH}})$.

$\mathscr{G}_{PCH}(\lambda) \longrightarrow (\text{param}, (x, y))$: on inputting a security parameter λ, choose two groups G and G_T with prime order q and generator g. Set bilinear map as $\widehat{e}: G \times G \longrightarrow G_T$. Set hash functions as $H_2: \{0,1\}^* \longrightarrow Z_q$. Denote $\text{param} = \{g, q, G, G_T, H_2, \widehat{e}\}$. Select a random number $x \xleftarrow{R} Z_q^*$ as the trapdoor key, and compute $y = g^x$ as the hash key. Output $(\text{param}, (x, y))$.

$\mathscr{H}_{\text{PCH}}(CI\ D, y, m) \longrightarrow (\hbar, r)$: pick a customized identity $\text{CID} \in \{0,1\}^*$. Given the hash key y, compute coefficients $e = H_2(\text{CID})$ and $h_1 = g^e$. Choose a random $\alpha \xleftarrow{R} Z_q^*$ and compute probabilistic chameleon randomness $r = (r_1, r_2) = (g^\alpha, y^\alpha)$. Then, compute chameleon hash $\hbar = \widehat{e}(g,g)^{H_2(m))} \cdot \widehat{e}((h_1 \cdot y), r_1)$. Output $(\hbar, r)$.

$\widehat{\mathscr{H}}_{\text{PCH}}(\text{CID}, y, m) \longrightarrow (\widehat{\hbar}, \widehat{r})$: pick a customized identity $\text{CID} \in \{0,1\}^*$. Given a hash key y, compute coefficients $e = H_2(\text{CID})$, $h_1 = g^e$, and $k_0 = H_2(m)$. Compute deterministic chameleon randomness $\widehat{r} = (\widehat{r}_1, \widehat{r}_2) = (g^{k_0}, y^{k_0})$. Then, compute a deterministic chameleon hash $\widehat{\hbar} = \widehat{e}(\widehat{r}_1, g) \cdot \widehat{e}((h_1 \cdot y), \widehat{r}_1)$. Output $(\widehat{\hbar}, \widehat{r})$.

$\mathscr{V}_{\text{PCH}}(\text{CID}, y, \hbar, r, m) \longrightarrow (0,\ 1 \text{ or } deter)$: on inputting a customized identity CID, a public key y, and a tuple $(\hbar, r, m)$, where $m \in \{0,1\}^*$, compute coefficients $e = H_2(\text{CID})$ and $h_1 = g^e$. Then, check whether equation 1 holds:

$$\hbar \stackrel{?}{=} \widehat{e}(g,g)^{H_2(m)} \cdot \widehat{e}(h_1 \cdot y, r_1). \tag{1}$$

and check whether $\widehat{e}(r_1, y) \stackrel{?}{=} \widehat{e}(r_2, g)$ holds. If no, output 0; else, compute $k_0 = H_2(m)$ and check whether $r \stackrel{?}{=} (g^{k_0}, y^{k_0})$. If yes, output deter which signifies $\hbar$ is an output of $\widehat{\mathscr{H}}_{\text{PCH}}$; else, output 1 to indicate $\hbar$ is an output of $\mathscr{H}_{\text{PCH}}$. $\mathscr{R}_{\text{PCH}}((\hbar, r, m), x, m') \longrightarrow (\perp \text{ or } r')$: on inputting a tuple $(\hbar, r, m)$, a customized identity CID, a trapdoor key x, and a new message m', compute coefficients $e = h_0 = H_2(\text{CID})$ and $h_1 = g^e$. Then, compute new chameleon randomness $r' = (r_1', r_2') = (r_1 \cdot g^{(x+e)^{-1}(H_2(m) - H_2(m'))}, r_2 \cdot y^{(x+e)^{-1}(H_2(m) - H_2(m'))})$.

4.2. Revised Linkable-and-Redactable Ring Signature. Liu et al. [33] proposed 1-out-of-n Linkable Spontaneous Anonymous Group (LSAG) Signature as an extension of Spontaneous Anonymous Group (SAG) [34]. In our previous work [11], we extended Liu et al.'s LSAG [33] to a Linkable-and-Redactable Ring Signature (LRRS) [11]. In this work, we revised our previous LRRS scheme slightly to derive a Revised LRRS (R-LRRS). To note, if we use a different L for each signing, linkability will not be achieved in our R-LRRS. An R-LRRS signature consists of the following four algorithms $(\mathscr{G}_{\text{R0LRRS}}, \mathscr{S}_{\text{R0LRRS}}, \mathscr{V}_{\text{R0LRRS}}, \mathscr{R}_{\text{R0LRRS}})$.

$\mathscr{G}_{\text{R0LRRS}}(\lambda) \longrightarrow (\text{param}_{\text{R0LRRS}}, (x, y))$: on inputting a security parameter λ, choose a group G generated by g of order q. Then, set cryptographic hash function: $H_1: \{0,1\}^* \longrightarrow G$ and $H_2: \{0,1\}^* \longrightarrow Z_q$. Derive param. Finally, pick a random number $x \xleftarrow{R} Z_q^*$ as the private key, and compute $y = g^x$ as the public key. Output $(\text{param}_{\text{R0LRRS}}, (x, y))$.

$\mathscr{S}_{\text{R0LRRS}}(x, m, L, \{\hbar, r\}) \longrightarrow (\sigma_L(m) \text{or} \perp)$: input a private key x, a message $m \in \{0,1\}^*$, a list of n public keys $L = \{y_i\}_{1 \le i \le n}$, and a set of tuples $\{\hbar, r\} = \{\hbar_i, r_i\}_{1 \le i \le n}$. User π generates coefficients as follows:

(1) Set $\text{CID} = L$ as a customized identity, compute $h_0 = H_1(\text{CID})$ and $\widetilde{y}_\pi = h_0^{x_\pi}$ for $x_\pi \xleftarrow{R} Z_q$. Then, pick two random numbers $u, v \xleftarrow{R} Z_q$ and compute $s_{\pi+1} = H_2(L, \widetilde{y}_\pi, g^u, h_0^v)$.

(2) For each $1 \le i \le n$, run $\mathscr{V}_{\text{PCH}}(\text{CID}, \hbar_i, r_i, m)$. If all outputs are 1 or deter, proceed; otherwise, return $\perp$ and terminate.

(3) For each $i = \pi + 1, \ldots, n, 1, \ldots, \pi - 1$, user π picks a random number $\beta_i \xleftarrow{R} Z_q^*$, and compute $s_{i+1} = H_2(L, \widetilde{y}, \hbar_i \cdot y_i^{s_i}, h_0^{\beta_i} \cdot \widetilde{y}^{s_i})$.

(4) Then, compute $\alpha_\pi = u - x_\pi s_\pi \bmod q$, and $\beta_\pi = v - x_\pi s_\pi \bmod q$.
(5) Output $\sigma_L(m) = (s_1, r_1, \ldots, r_n, \beta_1, \ldots, \beta_n, \tilde{y}_\pi)$.

$\mathscr{V}_{\text{R0LRRS}}(L, m, \sigma_L(m), \{\hbar, r\}) \longrightarrow (0 \text{ or } 1)$: on inputting a list L of n public keys, a message m, the $\mathscr{R}_{\text{R0LRRS}}$ signature $\sigma_L(m)$, and a set of tuples $\{\hbar, r\} = \{\hbar_i, r_i\}_{1 \le i \le n}$, the signature verification algorithm proceeds as follows:

(1) Set CID = L as a customized identity. Compute coefficients L = CID, $h_0 = H_1(\text{CID})$, and $\tilde{y}_\pi = h_0^{x_\pi}$.
(2) For $i = \pi + 1, \ldots, n, 1, \ldots \pi - 1$, run $\mathscr{V}_{\text{PCH}}(L, y, \hbar_i, r_i, m)$. If all outputs are 1 or deter, proceed; otherwise, abort and terminate.
(3) For each $i = \pi + 1, \ldots, n, 1, \ldots, \pi - 1$, compute $z_i' = \hbar_i \cdot y_i^{s_i}$ and $z_i'' = h_0^{\beta_i} \cdot \tilde{y}^{s_i}$. Then, compute $s_{i+1} = H_2(L, \tilde{y}_\pi, z_i', z_i'')$, for $i \neq n$.
(4) Check whether $s_1 \stackrel{?}{=} H_2(L, \tilde{y}_\pi, z_n', z_n'')$. If it holds, output 1; else, output 0.

$\mathscr{R}_{\text{R0LRRS}}(x, L, m', \sigma_L(m)) \longrightarrow (\sigma_L(m') \text{ or } \perp)$: on inputting a private signing key x, a list L of n public keys, a new message m', and an old signature $\sigma_L(m)$, perform redaction as follows:

(1) Set CID = L as a customized identity. Compute coefficients $h_0 = H_1(\text{CID})$ and $h_1 = g^e$.
(2) For each $1 \le i \le n$, run $\mathscr{R}_{\text{PCH}}((\hbar_i, r_i, m), x, m')$ to derive r_i'. If no $\perp$ is returned, proceed; else, return $\perp$ and terminate.
(3) For each $1 \le i \le n$, run $\mathscr{V}_{\text{PCH}}(\text{CID}, y, \hbar_i, r_i, m)$. If no 0 is returned, proceed; else, return $\perp$ and terminate.
(4) Output $\sigma_L(m') = \{s_1, r_1', \ldots, r_n', \beta_1, \ldots, \beta_n, \tilde{y}_\pi\}$.

5. Definitions

In this section, we present our system model and security requirements.

5.1. System Model. The framework of our BA^{2}P is shown in Figure 1. It consists of four parties: auction manager (AM), seller, buyer, and certificate authority (CA). We briefly introduce each entity as follows:

Auction Manager (AM). Auction manager is the one who initiates the system and holds the auction on behalf of the seller. The AM also holds the buyer's deposit and publishes misbehaviors by deducting the deposit. After he verifies and confirms a winner's bid, he relays the winner's money from the buyer to the seller via anonymous cryptocurrency.

Seller. Seller is the one who wishes to sell his merchandise online. He delegates the AM to hold an auction and transacts with AM with anonymous cryptocurrency. He communicates with AM via the anonymous channel.

Buyer. Buyer is the one who involves in an auction protocol anonymously to make an offer. He places his bid competitively in order to outbid others. If he wins, he will send money to AM via cryptocurrency, as previously negotiated and confirmed. He communicates with AM via the anonymous channel.

Certificate Authority (CA). Certificate authority is a trusted third party which is responsible for assigning private and public key pairs to each buyer, seller, and AM.

5.2. Security Requirements. A secure BA^{2}P scheme satisfies the following properties:

Ours is secure if the underlying R-LRRS scheme satisfies existential unforgeability against adaptive chosen-plaintext under chosen-public-key attack (EU-ACP-CPK) [33]. The EU-ACP-CPK security is an extension of the notion of existential unforgeability under adaptive chosen-message-attacks (EUF-CMA) [35]. Unlike EUF-CMA, EU-ACP-CPK additionally allows the adversary to select an arbitrary subset of initially generated public keys during each round of signing oracle access. Given the public keys of all group members in the aforementioned way, the adversary still cannot forge a valid signature for any message m. A formal definition for EU-ACP-CPK security is given in [33, 36].

Definition 1. Let $\mathcal{SO}$ be the signing oracle which takes inputs of any public key list $L' = \left\{y, \ldots, y_{n_l}\right\}$ and any message m' as queried and outputs a signature σ' as a response such that $\mathscr{V}_{\text{R0LRRS}}(L', m', \sigma_L'(m')) = 1$. An R-LRRS scheme satisfies EU-ACP-CPK if, for any Probabilistic Polynomial Time (PPT) adversary $\mathcal{A}$ with signing oracle $\mathcal{SO}$ such that $(L, m, \sigma_L(m)) \leftarrow \mathcal{A}^{\mathcal{SO}}(L)$, $\mathcal{A}$'s probability in successfully forging a valid signature σ^* such that $\mathscr{V}(L^*, m^*, \sigma_{L^*}(m^*)) = 1$ is negligible. Here, (L^*, m^*, σ^*) is not queried to the signing oracle $\mathcal{SO}$ previously.

Like all ring signature-based auction protocols proposed in [7–9], our BA^{2P} is secure if the underlying R-LRRS scheme satisfies anonymity. This means no adversary can efficiently determine the private key used to produce the given R-LRRS signature.

Definition 2. An R-LRRS scheme satisfies anonymity if, for any PPT algorithm $\mathcal{A}$, on inputs of any message m, any list L of n public keys, any set of t private keys $X_t = \{x_1, \ldots, x_t\} \subset L$, and any valid R-LRRS signature $\sigma_L(m)$ generated by the signer π, $\mathcal{A}$'s probability in successfully linking the signature $\sigma_L(m)$ to the signer π is negligible.

Our BA^{2P} is secure if the underlying chameleon hash scheme satisfies collision-resistance (COL-RES) and indistinguishability (IND). Following Camenisch et al.'s security model [37], we formalize the security requirements of COL-RES and IND as follows. To note, since one of our PCH's subalgorithm $\widetilde{\mathscr{H}}_{\text{PCH}}$ cannot satisfy any semantic security, we prove by assuming the existence of unpredictable file source (as given in Section 3.3) to set up a lower bound [32].

Definition 3. A PCH scheme satisfies COL-RES security if, for any PPT algorithm $\mathcal{A}$, it is hard to derive a fresh hash

collision under unpredictable file source [32], i.e., collision-resistance under unpredictable file source [32], COL-UNP.

Definition 4. A PCH scheme satisfies IND security if, for any PPT $\mathcal{A}$, following the model sketched in Figure 1 of [37], it is hard to distinguish between outputs of deterministic hash (generated by $\widehat{\mathcal{H}}_{\mathrm{PCH}}$) and probabilistic hash ((generated by $\mathcal{H}_{\mathrm{PCH}}$)). Denote this security as IND-D&P.

6. The Construction of BA^{2}P

The detailed construction of our BA^{2P} is given in this section. A workflow of our BA^{2P} is given in Figure 2.

6.1. Initiation. To join BA^{2P}, each user (buyer, seller, and AM) needs to acquire a set of private and public key pairs from the CA. We assume each user is assigned with one key pair (x, y) for simplicity. The AM selects a security parameter λ and runs $\mathcal{G}_{\mathrm{PCH}}(\lambda)$ and $\mathcal{G}_{\mathrm{R0LRRS}}(\lambda)$ to initiate the system.

6.2. Prebidding Phase. During this stage, each buyer is required to place his first bid. When this stage is finished, the first bid proof is generated. In addition, a deposit is sent to the AM. The AM can fix the first bid by setting up a base price. The first bid is paid as a ticket to the auction and a deposit to ensure penalization of future misbehavior. The deposit will be refunded if it is not a winner's bid. When this phase is over, each buyer is supposed to output the first bid proof.

(1) Suppose the buyer π places his first bid $\mathrm{bid}_{\mathrm{base}}$ at time point t_π, where t_π is only known to the buyer π. He sends money to the AM via an anonymous cryptocurrency. Denote t_π as the time of the buyer π's payment generation, x_π as the private key of the buyer π and $y_\pi = g^{x_\pi}$ as the corresponding public key, and x_{AM} as the private key of AM and $y_{AM} = g^{x_{AM}}$ as the corresponding public key.

(2) Buyer π randomly collects n public keys to form a sequence of ring $L = \{y_1, \ldots, y_L\}_{1 \le i \le n}$, where y_1 is the head and y_n is the tail of the ring. Here, $\pi \in [1, L]$ is hidden in the L and unknown to the public.

(3) For each $1 \le i \le n$, the buyer π runs $(\hbar_i, r_i) \leftarrow \mathcal{H}_{\mathrm{PCH}}(\mathrm{CID}, y_\pi, t_\pi)$ and $(\widehat{\hbar}_i, \widehat{r}_i) \leftarrow \widehat{\mathcal{H}}_{\mathrm{PCH}}(\mathrm{CID}, y_\pi, t_\pi)$. Denote $\{\hbar, r\} = \{\hbar_i, r_i\}_{1 \le i \le n}$ as the first set of commitments and $\{\widehat{\hbar}_i, \widehat{r}_i\} = \{\widehat{\hbar}_i, \widehat{r}_i\}_{1 \le i \le n}$ as the second set of commitments, and both are committed to t_π.

(4) Buyer π runs $\sigma_L(t_\pi) \leftarrow \mathcal{S}_{\mathrm{R0LRRS}}(\mathrm{CID}, x_\pi, L, \{\hbar, r\})$ and $\widehat{\sigma}_L(t_\pi) \leftarrow \mathcal{S}_{\mathrm{R0LRRS}}(\mathrm{CID}, x_{AM}, L, \{\widehat{\hbar}, \widehat{r}\})$. Output $\mathrm{prf}_{\mathrm{fbp}} = \{\sigma_L(t_\pi), \widehat{\sigma}_L(t_\pi)\}$ as the first bid proof. Buyer π sends the first bid proof $\mathrm{prf}_{\mathrm{fbp}}$ to the AM.

To note, we use a different set of public keys L_i for each different signing to generate R-LRRS signature. Thus, linkability will not hold in our BA^{2P}. In other words, it is hard to detect two signatures generated by the same signer. This is vital since linkability will break the anonymity in our scheme (but is useful to detect double-spending in cryptocurrencies [33]).

6.3. Bidding Phase. During this stage, each buyer competitively places his new bids in order to outbid others. A bulletin board system (BBS) can be utilized to record the bidding history. At the end of this phase, the buyer is supposed to output the last bid proof.

(1) Set $\sigma_L = \sigma_L(t_\pi)$ and $\widehat{\sigma_L} = \widehat{\sigma_L}(t_\pi)$. Set $\mathrm{prf}_{\mathrm{lbp}} = \{\sigma_L, \widehat{\sigma_L}\}$ as the last bid proof.

(2) For a new bid $\mathrm{bid}_{\pi,\mathrm{curr}}$ placed at time $t_{\pi,\mathrm{curr}}$, suppose $t_{\pi,\mathrm{last}}$ is the time of last bid (for simplicity, assume $t_{\pi,\mathrm{last}} = t_\pi$), and the buyer π runs $\mathcal{R}_{\mathrm{R0LRRS}}(x_\pi, L, t_{\pi,\mathrm{curr}}, \sigma_L(t_{\pi,\mathrm{last}}))$ to generate a new signature $\sigma_L(t_{\pi,\mathrm{curr}})$. Then, set $\sigma_L = \sigma_L(t_{\pi,\mathrm{curr}})$.

(3) Repeat step 2 if the buyer π places another bid. When this phase is over, output $\mathrm{prf}_{\mathrm{lbp}}$. Buyer π sends the last bid proof $\mathrm{prf}_{\mathrm{lbp}}$ to the AM.

To note, $\sigma_L(bid_{\pi,\mathrm{curr}})$ is not necessarily required to be calculated immediately when the buyer π places a new bid. Ideally, it is just for the last bid. However, due to the unpredictability of the bidding process, it is undetermined which one is the last bid until this phase ends.

6.4. Confirmation Phase. In this stage, the AM is supposed to check the BBS and all last bid proofs $\{\mathrm{prf}_{\mathrm{lbp}_i}\}_{1 \le i \le j_0}$ (suppose there are j_0 buyers who have placed their bids). At the end of this phase, the AM generates a confirmation proof $\mathrm{prf}_{\mathrm{con}_i}$ for user i as follows:

(1) Parse the buyer i's last bidding proof as $\mathrm{prf}_{\mathrm{lbp}_i} = \{\sigma_L(t_i), \widehat{\sigma}_L(t_i)\}$, where t_i is the time of buyer i's first bid. Denote $t_{\pi,\mathrm{end}}$ as the time of buyer i's last bid in the bidding phase. Set buyer i's confirmation proof initially as $\mathrm{prf}_{\mathrm{con}_i} = \mathrm{prf}_{\mathrm{lbp}_i}$.

(2) For each buyer $1 \le i \le j_0$, the AM runs $\mathcal{R}_{\mathrm{R0LRRS}}(x_{AM}, L_i, t_{\pi,\mathrm{end}}, \widehat{\sigma}_L(t_i))$ to generate $\widehat{\sigma}_L(\mathrm{bid}_{\pi,\mathrm{end}})$. Set $\widehat{\sigma}_L(t_i) = \widehat{\sigma}_L(\mathrm{bid}_{\pi,\mathrm{end}})$.

(3) AM relays the confirmation proof $\mathrm{prf}_{\mathrm{con}_i}$ to each buyer i.

6.5. Open Phase. At this stage, each buyer is supposed to open his commitments to the first bid proof (i.e., inputs used to compute the first commitment). Meanwhile, AM will open his commitments to the confirmation proof (i.e., inputs used to compute the second commitment). Failure to comply leads to invalid bid. Based on the above, the public can verify the validity of the auction procedure and determine a winner. We assume each buyer has placed bids more than once and the buyer π is the winner for the ease of analysis. We show how to verify as follows.

(1) Buyer π reveals the first bid proof $\mathrm{prf}_{\mathrm{fbp}}$, the last bid proof $\mathrm{prf}_{\mathrm{lbp}}$, and corresponding commitments $\{(\hbar, r), (\widehat{\hbar}, \widehat{r})\} = \{\{\hbar_i, r_i\}_{1 \le i \le n}, \{\widehat{\hbar}_i, \widehat{r}_i\}_{1 \le i \le n}\}$ to the

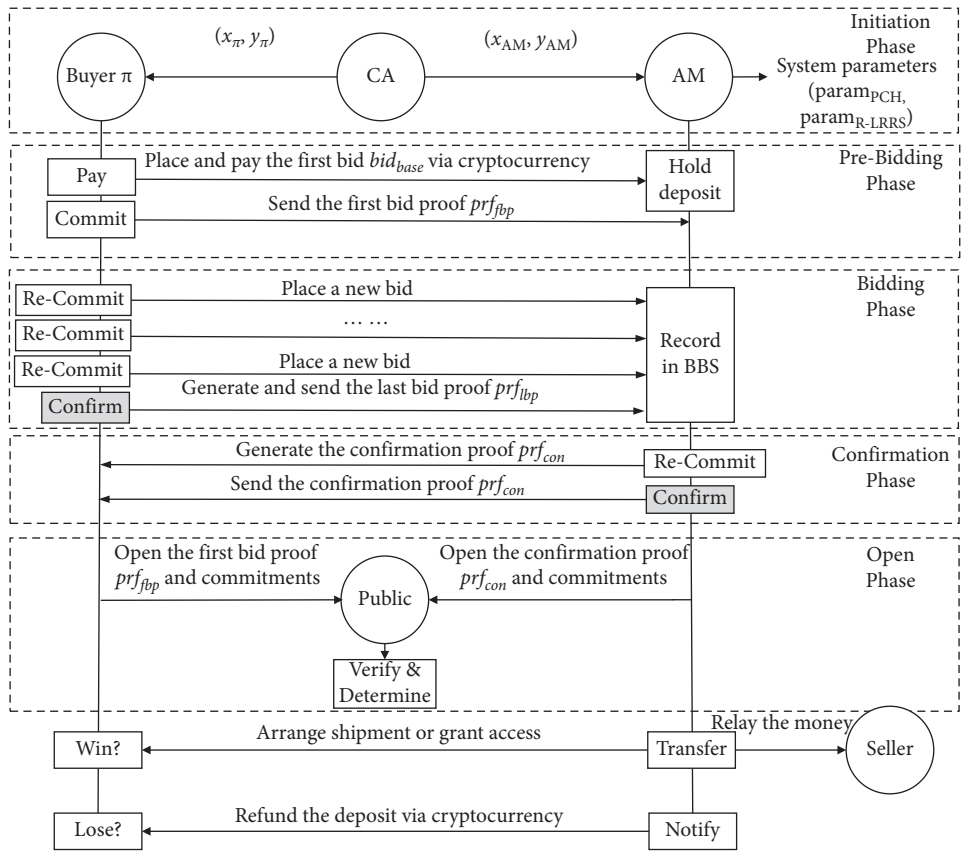

Figure 2: The workflow of BA^{2}P protocol.

public. Accordingly, the AM reveals the confirmation proof prf_{con} and corresponding commitments to the public. The public can run $\mathscr{V}_{\text{PCH}}$ and $\mathscr{V}_{\text{R0LRRS}}$ to verify the validity of these proofs and commitments.

(2) Based on the information recorded in BBS, the public can determine a winner. Since each bid is confirmed bidirectionally by the buyer and the AM, it is undeniable for either the buyer or the AM to dispute the validity of the bid. This idea is brought from undeniable signature [38].

Once the winner is determined and confirmed, the winner can transmit the money via anonymous cryptocurrency to the AM. In return, the AM will relay the money to the seller (maybe charge some transaction fees). In addition, it arranges the shipment of the purchased physical assets to the buyer or grant him access to the purchased digital assets. Accordingly, the shipment and the access are all conducted in the anonymous channel.

7. The Security Analysis of BA^{2}P

Here, we give the security analysis of our proposed scheme based on security requirements defined in Section 5.2.

Theorem 1. *If there exists a PPT adversary $\mathscr{A}$ who can break the EU-ACP-CPK property of our R-LRRS scheme, we can construct a PPT simulator $\mathscr{S}$ to solve the DLP with nonnegligible probability.*

Proof. Suppose $\mathscr{A}$ can forge an R-LRRS signature with nonnegligible probability, i.e.,

$$\Pr[\mathscr{A}(L) \longrightarrow (m,\sigma): \mathscr{V}(L,m,\sigma) = 1] > \frac{1}{Q_1(k)}, \quad (2)$$

for some polynomial Q_1. Let q_H be the maximum number of queries to H_1 and H_2 in total. Let q_S be the maximum number of queries to $\mathscr{SO}$. Then, we can construct a PPT simulator $\mathscr{S}$ which invokes $\mathscr{A}$ to solve the DLP with nonnegligible probability. Given a DLP instance (g, g^x), $\mathscr{S}$ sets $y = g^x$ where $x \in L$, and it aims to output x. $\mathscr{S}$ simulates inputs for $\mathscr{A}$ and processes outputs from $\mathscr{A}$ adaptively. We give a proof sketch as follows:

Let param be the system parameter generated in the initiation phase. Let H_1 and H_2 be random oracles controlled by $\mathscr{S}$, which return the same response to the same query by maintaining query histories. Let $\mathscr{L}$ be a list of public keys where each key is generated properly according to the prebidding phase. $\mathscr{S}$ invokes $\mathscr{A}$ adaptively based on the constructed inputs and $\mathscr{A}$'s responses. A simulation transcript tape $\mathscr{T}$ is used to record the invocation of $\mathscr{A}$. $\mathscr{S}$ can simulate $\mathscr{SO}$ by back patching [33]. Some outputs of $\mathscr{A}$ are valid forgeries of R-LRRS signatures and are used to solve DLP with nonnegligible probability. A proof of unforgeability based on rewind simulation is given in [33].

Specifically, the signature returned by $\mathcal{SO}$ is the same as the one signed by the signer π in the adversary $\mathcal{A}$'s view. To derive this conclusion, we can discuss the conditional probability of $\mathcal{A}$ in successfully forging a valid signature σ^* in each $\mathcal{A}$'s transcript and the queries made to the signing oracle $\mathcal{SO}$. Furthermore, $\mathcal{S}$ can do a rewind-simulation accordingly. By considering the equations based on two (l, π)-forgery signatures from the tape $\mathcal{T}$ and a rewind-simulation tape S$\imath$, we can derive the answer to the DLP instance and bound the $\mathcal{S}$'s probability in solving the DLP. Due to the intractability of the DLP, our R-LRRS satisfies EU-ACP-CPK security. Refer to [33], for more details. □

Theorem 2. *If there exists a PPT adversary $\mathcal{A}$ who can break the anonymity of our R-LRRS scheme, we can construct a PPT simulator $\mathcal{S}$ to solve the DDHP with a nonnegligible advantage.*

Proof. On given $g, g^a, g^b, g^c \in G$, the simulator $\mathcal{S}$ is supposed to call $\mathcal{A}$ and determine $c \stackrel{?}{=} ab$. Suppose there exists a PPT adversary $\mathcal{A}$, on inputs of any message m, a list L of n public keys, a set of t private keys $X_t = x_1, \ldots, x_t \subset L$, $0 \le t < n-1$, and a valid R-LRRS signature $\sigma_L(m)$ generated by the buyer π; the $\mathcal{A}$'s probability in successfully linking the signature $\sigma_L(m)$ to the buyer (signer) π for polynomial $Q(k)$ is

$$\Pr\left[\mathcal{A}\left(m, L, SK, \sigma_L(m)\right) \longrightarrow \pi\right] > \frac{1}{n-t} + \frac{1}{Q(k)}. \tag{3}$$

Then, we can construct a PPT simulator $\mathcal{S}$ to solve the DDHP with probability:

$$\Pr\left[\mathcal{M}\left(g, g^a, g^b, g^c\right) \longrightarrow c \stackrel{?}{=} ab\right] = \frac{1}{2} + \frac{1}{Q_2(k)}. \tag{4}$$

Refer to [33], for details.

Theorem 3. *If there exists a PPT adversary $\mathcal{A}$ who can break the COL-UNP of our PCH scheme, we can construct an algorithm $\mathcal{B}$ to solve the q-SDHP with nonnegligible probability.*

Proof. We give a proof sketch as follows. On a given q-SDHP instance $(g, g^x, \ldots, g^{x^q})$ (parse it by $(A_0, A_1, \ldots, A_q)$, where $x \in Z_p^*$), here, $x \in Z_p^*$ is unknown. We can construct an algorithm $\mathcal{B}$ which interacts with $\mathcal{A}$ to derive an answer: $(c, g^{1/(x+c)})$, for some $c \in Z_q^*$ as follows:

(i) Setup: the algorithm $\mathcal{B}$ runs $\mathcal{G}_{\mathrm{PCH}}$ to initiate the system and derives $\{G, G_T, g, q, H_2, \hat{e}, (x, y)\}$, where $y = g^x$, and x is privately kept by $\mathcal{B}$. $\mathcal{B}$ sends $\{G, G_T, g, q, H_2, \hat{e}, y\}$ to $\mathcal{A}$.

(ii) Query: adversary $\mathcal{A}$ issues q_s distinct queries $\{\mathrm{CID}_i, m_i', (m_i, \hbar_i, r_i)\}_{i \in [1, q_s]}$ to $\mathcal{B}$ (assume $q_s = q - 1$).

(iii) Response: for each m_i, where $1 \le i \le q_s$, $\mathcal{B}$ generates responses as follows. Set polynomial $f(z) = \prod_{i=1}^{q_s} (z + e_i) = \sum_{i=1}^{q_s} a_i z^i$, where $a_0, \ldots, a_{q_s}$ are randomness of polynomial $f(z)$ and $e_i = H_2(\mathrm{CID}_i)$. Define coefficient g' and $\hat{c}$ as follows:

$$\begin{aligned} g' &= \prod_{i=0}^{q_s} (A_i)^{a_i} = g^{f(z)}, \\ \hat{c} \prod_{i=1}^{q_s} (A_i)^{a_{i-1}} &= g^{z f(z)} = g'^z. \end{aligned} \tag{5}$$

Next, define polynomial $f_i(z) = f(z)/(z + e_i) = \prod_{j=1, j \ne i}^{q_s} (z + e_i)$ and $f_i(z) = \sum_{j=0}^{q_s - 1} (b_j z^j)$. Compute s_i for each i as follows:

$$\begin{aligned} s_i &= \prod_{j=0}^{q_s - 1} \left(A_j\right)^{b_j} = \left(g'\right)^{1/\left(x + e_i\right)}, \\ e_i &= H_2\left(\mathrm{CID}_i\right). \end{aligned} \tag{6}$$

Then, $\mathcal{B}$ can compute each r_i', for each $i \in [1, q_s]$:

$$r_i' = \left(g^{\alpha_i} \cdot s_i^{H_2(m_i) - H_2(m_i')}, y^{\alpha_i} \cdot s_i^{x\left[H_2(m_i) - H_2(m_i')\right]}\right). \tag{7}$$

Since the equation holds for $\hat{e}(g, g)^{H_2(m_i)} \cdot \hat{e}(h_i \cdot y, r_{1,i}) = \hat{e}(g, g)^{H_2(m_i')} \cdot \hat{e}(h_i \cdot y, r_{1,i}')$, where $h_i = g^{e_i} = g^{H_2(\mathrm{CID}_i)}$ and $r_i' = (r_{1,i}', r_{2,i}')$ is the correct response to hold each collision. $\mathcal{B}$ replies $\mathcal{A}$ with $(r_1', \ldots, r_{q_s}')$ as a response.

Output: adversary $\mathcal{A}$ wins the game by outputting $(\mathrm{CID}, M, r, M^*, r^*, \hbar)$ such that

$$\hat{e}(g, g)^{H_2(M)} \cdot \hat{e}\left(r_1^{(e+x)}, g\right) = \hat{e}g, g^{H_2(M^*))} \cdot \hat{e}\left(r_1^{*(e+x)}, g\right), \tag{8}$$

where $h = g^e = g^{H_2(\mathrm{CID})}$, $r = (r_1, r_2)$, and $r^* = (r_1^*, r_2^*)$.

Next, we can parse r^* by

$$r^* = \left(g^{\alpha^*}, y^{\alpha^*}\right) = \left(r_1 \cdot s^{H_2(M) - H_2(M^*)}, r_2 \cdot s^{x\left[H_2(M) - H_2(M^*)\right]}\right), \tag{9}$$

where

$$s = \left(\frac{r_1^*}{r_1}\right)^{1/\left(H_2(M) - H_2(M^*)\right)} = \left(g'\right)^{1/(x+e)} = g^{f(x)/(x+e)}. \tag{10}$$

Next, we can parse f by $f(z) = \gamma(z)(z + e) + \gamma_{-1}$, for some $\gamma(y) = \sum_{i=0}^{q_s - 1} \gamma_i z^i$ and $\gamma_{-1} \in Z_q$. Then, we can deduce by

$$\frac{f(x)}{(z+e)} = \frac{\gamma_{-1}}{z+e} + \sum_{i=0}^{q_s - 1} \gamma_i z^i. \tag{11}$$

Since $\gamma_{-1} \ne 0$ and CID has never been queried before (i.e., $\mathrm{CID} \notin \left\{\mathrm{CID}_1, \ldots, \mathrm{CID}_{q_s}\right\}$), $(z + e)$ cannot divide $f(z)$. So, the algorithm $\mathcal{B}$ derives a q-SDHP answer as follows:

$$\left(e = H_2(\mathrm{CID}), g^{1/x+e} = \left(s \cdot \sum_{i=1}^{q_s} (A_i)^{-\gamma_i}\right)^{1/\gamma_{-1}}\right). \tag{12}$$

Theorem 4. *If there exists a PPT adversary $\mathcal{A}$ who can break the IND-D&P of our PCH scheme, we can construct an algorithm $\mathcal{B}$ to solve the DDHP with a nonnegligible advantage.*

Proof. Our IND-D&P is reducible to the DDHP. Suppose $\mathscr{A}$ is a PPT adversary against our IND-D&P; we prove by game hopping as follows:

Game 0: this is the original IND0D&P game.

(1) Setup: the algorithm $\mathscr{B}$ runs $\mathscr{G}_{\mathrm{PCH}}$ to initiate the system and derives $\{G, G_T, g, q, H_2, \widehat{e}, (x, y)\}$, where $y = g^x$, and x is privately kept by $\mathscr{B}$. Then, $\mathscr{B}$ sends $\{G, G_T, g, q, H_2, \widehat{e}, y\}$ to $\mathscr{A}$.

(2) Challenge: $\mathscr{S}$ flips a coin $b \in \{0, 1\}$ and proceeds differently.
For $b = 0$, compute coefficient r_0 and chameleon hash $\hbar_0$ as follows:

$$\begin{aligned} r_0 &= \left(g^{H_2(M)}, y^{H_2(M)}\right), \\ \hbar_0 &= \widehat{e}(g, g)^{H_2(M)} \cdot \widehat{e}\left(\left(h_1 \cdot y\right)^{H_2(M)}, g\right). \end{aligned} \tag{13}$$

For $b = 1$, compute coefficient r_1 and chameleon hash $\hbar_1$ as follows:

$$\begin{aligned} &\alpha \in_R Z_q,\ r_1 = \left(g^{\alpha}, y^{\alpha}\right), \\ &\widehat{\hbar}_1 = \widehat{e}(g, g)^{H_2(M)} \cdot \widehat{e}\left(\left(h_1 \cdot y\right)^{\alpha}, g\right). \end{aligned} \tag{14}$$

$\mathscr{S}$ relays $(\hbar_b, r_b)$ to the adversary $\mathscr{A}$. Suppose $\mathscr{A}$ issues at most q_s distinct queries to oracle H_2 (controlled by $\mathscr{S}$) on e_i and m_i; then, $\mathscr{S}$ returns answer to each distinct query accordingly.

(3) Output: the adversary outputs $a \in \{0, 1\}$ and wins if $b = a$.

(ii) Game 1: it is the same as Game 0, except that we randomly sample $R_1 \in G$ and use it to compute $\hbar_0$. Thus, $(\hbar_0, r_0)$ is computed as follows:

$$\begin{aligned} &R_1 \in_R Z_q, \\ &r_0 = \left(g^{H_2(M)}, y^{H_2(M)}\right), \\ &\hbar_0 = \widehat{e}(g, g)^{H_2(M)} \cdot \widehat{e}\left(h_1^{H_2(M)} \cdot R_1, g\right), \end{aligned} \tag{15}$$

where $(\hbar_1, r_1)$ is computed as follows:

$$\begin{aligned} &\alpha \in_R Z_q, \\ &r_1 = \left(g^{\alpha}, y^{\alpha}\right), \\ &\hbar_1 = \widehat{e}(g, g)^{H_2(M)} \cdot \widehat{e}\left(\left(h_1 \cdot y\right)^{\alpha}, g\right). \end{aligned} \tag{16}$$

(iii) Game 2: it is the same as Game 1, except that we randomly sample $R_2 \in G$ and use it to compute $\hbar_1$. Hence, $(\hbar_0, r_0)$ is computed as follows:

$$\begin{aligned} &r_0 = \left(g^{H_2(M)}, y^{H_2(M)}\right), \\ &R_1 \in_R Z_q, \\ &\hbar_0 = \widehat{e}(g, g)^{H_2(M)} \cdot \widehat{e}\left(h_1^{H_2(M)} \cdot R_1, g\right), \end{aligned} \tag{17}$$

where $(\hbar_1, r_1)$ is computed as follows:

$$\begin{aligned} &\alpha \in_R Z_q, \\ &R_2 \in_R Z_q, \\ &r_1 = \left(g^{\alpha}, y^{\alpha}\right), \\ &\hbar_1 = \widehat{e}(g, g)^{H_2(M)} \cdot \widehat{e}\left(h_1^{\alpha} \cdot R_2, g\right). \end{aligned} \tag{18}$$

If $Q = g^{ab}$, this implies Game 0; else, $Q \xleftarrow{R} G$, this implies Game 1. Thus, we can bound $\mathscr{B}$'s advantage in solving the DDHP by $Adv_{\mathscr{B}}^{DDHP} = |\Pr[E_0] - \Pr[E_1]|$ via distinguishing among Game 0 and Game 1. Here, we denote E_i as the event for $\mathscr{A}$ winning the Game i. Analogically, we have $Adv_{\mathscr{B}}^{DDHP} = |\Pr[E_1] - \Pr[E_2]|$ via distinguishing among Game 1 and Game 2. Due to the unpredictability of file source $\mathscr{M}$, Game 2 generates $(\hbar_b, r_b)$ as the one-time pad, and therefore, we have $Adv_{\mathscr{A}}^{\mathbf{Game2}} = 1/2$.

Based on the above, we can bound $\mathscr{B}$'s advantage in solving the DDHP by $Adv_{\mathscr{A}}^{IN\ D0D\&P} \leq 2 \cdot Adv_{\mathscr{B}}^{DDHP}$. Details are omitted due to space limitations. Since each hop only made negligible changes, the modification is beyond the adversary $\mathscr{A}$'s view; otherwise, we can construct an algorithm $\mathscr{B}$ to solve the DDHP assuming the adversary $\mathscr{A}$ can distinguish among Game 0 and Game 1, or Game 1 and Game 2, subsequently. Refer to [39], for more details.

8. Performance Evaluation

In this section, we evaluate the computational complexity and experimental performance of our BA^{2P} scheme. We have given the complexity of each stage in Table 2. As shown in Table 2, during the prebidding and the bidding Phases, the buyer's computational complexity is linear with n and b_0. However, since b_0 can be fixed to 1, if we let the buyer only compute the last bidding proof (instead of for each bid), this turns our auction protocol into a sealed bidding case. In addition, suppose there are j_0 buyers who participated in the bidding. To verify the validity of all the last bidding proofs and determine the highest bidder from them, AM needs to perform j_0 times verification for each set of commitments and the last bid proof, i.e., $[(3n + 3)T_m + (2n + 4)T_e + T_p] \cdot 2j_0$ in total. The complexity of the open phase at the public side is bound by n and j_0. However, the public can choose to verify or delegate a third party to do it.

Denote n as the number of public keys in L, j_0 as the number of buyers, b_0 as the number of bids placed per bidder during the bidding Stage, T_m as the group multiplication, T_e as the group exponentiation, T_i as the group inversion, and T_p as bilinear pairing operation.

Parameter is defined as Table 2.

We also compare the complexity of our scheme with other works in Table 3. As observed in Table 3, Xiong et al.'s [9] scheme is most efficient one. The reason is Xiong et al.'s [9] scheme did not involve trapdoor commitment to achieve bidirectional confirmation between the buyer and the AM. So, undeniability (dispute-freeness) is not achieved. Therefore, when a dispute occurs, it is hard to perform fair arbitration. Alternatively, our scheme provides bidirectional confirmation to achieve dispute-freeness since both the

Table 2: The complexities in each stage.

Stages	Computational complexity	
	Buyer side	Auction manager side
Prebidding phase	$(4n+4)T_m + (5n+9)T_e + 4T_p$	0
Bidding phase	$[(7n+1)T_m + (4n+2)T_e] \cdot b_0$	0
Confirmation phase	0	$[(7n+1)T_m + (4n+2)T_e] \cdot j_0$
Open phase	$[(3n+3)T_m + (2n+4)T_e + T_p] \cdot 2j_0$	

Table 3: The comparison of complexities in related works.

Stages	Computational complexity		
	Our scheme	Xiong et al. [9] (2012)	Xiong et al. [8] (2009)
Prebidding phase	$(4n+4)T_m + (5n+9)T_e + 4T_p$	0	$(2n+1)T_m + (3n-2)T_e$
Bidding phase	$[(7n+1)T_m + (4n+2)T_e] \cdot b_0$	$(2n+2)T_m + 3T_e + T_p$	$(2n+1)T_m + (3n-2)T_e$
Confirmation phase	$[(7n+1)T_m + (4n+2)T_e] \cdot b_0$	0	0
Open phase	$[(3n+3)T_m + (2n+4)T_e + T_p] \cdot 2j_0$	0	$(2n+1)T_m + (3n-2)T_e$

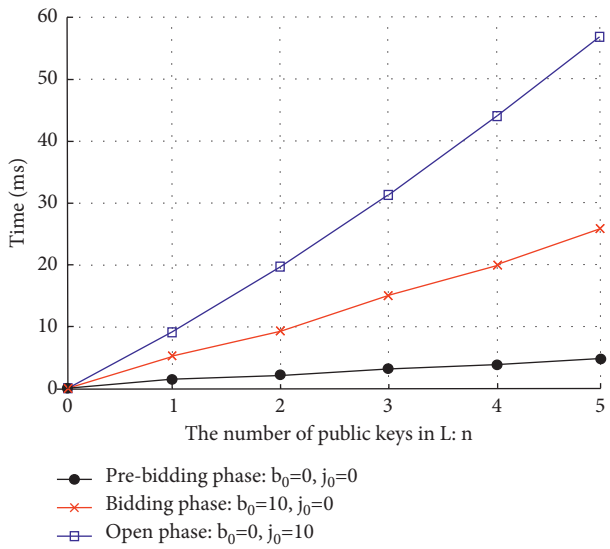

Figure 3: The running costs at the buyer side.

buyer and AM confirm every bid. These proofs are released together with the commitments during open stage and are publicly verifiable. Basically, our scheme trades efficiency with the dispute-freeness property.

Next, we conduct experiments to evaluate the running costs of our protocol at the buyer side. To simulate, we implemented our scheme using C language on a laptop with 3.5 GHz 4-cores CPU, 8 GB RAM, and 256 SSD for storage. The operating system is 32 bits Windows 7 SP1. All algorithms are implemented using PBC (version-0.5.13) for all cryptographic operations. We choose a super supersingular curve $y^2 = x^3 + x$ with embedding degree of 2. Denote $|G| \approx 160$ and $|G_T| \approx 1024$ as the binary sizes of groups $|G|$ and $|G|$, respectively. We range the number of pubic keys in L (i.e., n) from 0 to 5. We compare the running costs at the buyer side for different coefficients b_0 and j_0. We give experimental results in Figure 3. As it is shown in Figure 3, the costs at the buyer side are factored by several coefficients: n, b_0, and j_0. When these coefficients are not surprisingly large, the running costs are generally acceptable.

9. Conclusion

We proposed a bidirectional and anonymous auction protocol with the dispute-freeness property. Our proposal is based on two cryptographic schemes as building blocks: policy-driven chameleon hash and revised linkable-and-redactable ring signature. In our proposal, bidders can competitively place their bids in order to outbid others.

An auction manager is employed to verify and confirm the bidding proof generated by the buyer. Due to the bidirectional confirmation and public verifiability, our auction protocol is dispute-free. The evidence suggests that our proposal is provably secure based on intractable assumptions. Meanwhile, our proposal is practically efficient, and it trades efficiency with the dispute-freeness feature.

There is a number of additional functionalities to enrich our current design, for example, employing more standard and sophisticated cryptographic algorithms (e.g., zero-knowledge proof) to achieve practical and stronger privacy preservation. In addition, more formal security model which captures practical security threat is needed. Though some current works focus on utilizing several sophisticated cryptographic algorithms in one scheme, they suffered from inefficiency issue. Therefore, to design a practical bidding protocol for mass deployment, the complexity of the underlying cryptographic algorithms should not be the bottleneck of the whole scheme. We consider the solutions to the above problems as challenging and interesting future works.

Data Availability

No data were used to support the findings of the study.

Conflicts of Interest

The authors declare that they have no conflicts of interest or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This work was supported in part by the National Key R&D Program of China, under Grant nos. 2017YFB0802300 and 2018YFB08040505, National Natural Science Foundation of China, under Grants 62002048, 61872087, U19A2066, and 62072078, University Startup, under Grant no.Y030202059018061, and Blockchain Research Lab of UESTC, Chengdu Jiaozi Financial Holding Group Company Ltd; China Mobile Information Communication Technology Co., Ltd (Chengdu); 2020 UAV Operation Management Platform Phase II (Package 2:Safety Subsystem) (no. CMCMII-202001245).

References

[1] Y. Zhang, C. Lee, D. Niyato, and P. Wang, "Auction approaches for resource allocation in wireless systems: a survey," *IEEE Communications surveys & tutorials*, vol. 15, no. 3, pp. 1020–1041, 2012.

[2] X. Zhou, S. Gandhi, S. Suri, and H. Zheng, "EBay in the sky: strategy-proof wireless spectrum auctions," in *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking*, pp. 2–13, ACM, San Francisco CA USA, March 2008.

[3] M. Abe and K. Suzuki, "Receipt-free sealed-bid auction," in *Proceedings of the International Conference on Information Security*, pp. 191–199, Springer, Seoul, Korea, October 2002.

[4] R. Singh, A. D. Dwivedi, G. Srivastava, A. Wiszniewska-Matyszkiel, and X. Cheng, "A game theoretic analysis of resource mining in blockchain," *Cluster Computing*, vol. 23, no. 3, pp. 2035–2046, 2020.

[5] L. Malina, G. Srivastava, P. Dzurenda, J. Hajny, and S. Ricci, "A privacy-enhancing framework for Internet of things services," in *Proceedings of the International Conference on Network and System Security*, pp. 77–97, Springer, Sapporo, Japan, December 2019.

[6] L. Malina, G. Srivastava, P. Dzurenda, J. Hajny, and R. Fujdiak, "A secure publish/subscribe protocol for Internet of things,," in *Proceedings of the 14th International Conference on Availability, Reliability and Security*, pp. 1–10, ACM, Canterbury CA, United Kingdom, August 2019.

[7] K. Q. Nguyen and J. Traoré, "An online public auction protocol protecting bidder privacy," in *Proceedings of the Australasian Conference on Information Security and Privacy*, pp. 427–442, Springer, Brisbane, Australia, June 2000.

[8] H. Xiong, Z. Qin, and F. Li, "An anonymous sealed-bid electronic auction based on ring signature," *International Journal of Network Security*, vol. 8, no. 3, pp. 235–242, 2009.

[9] H. Xiong, Z. Chen, and F. Li, "Bidder-anonymous English auction protocol based on revocable ring signature," *Expert Systems with Applications*, vol. 39, no. 8, pp. 7062–7066, 2012.

[10] M. Fischlin, *Trapdoor Commitment Schemes and Their Applications*, PhD thesis, Citeseer, Princeton, NJ, USA, 2001.

[11] K. Huang, X. Zhang, Y. Mu, F. Rezaeibagha, and X. Du, "Scalable and redactable blockchain with update and anonymity," *Information Sciences*, vol. 546, pp. 25–41, 2021.

[12] M. Naor, B. Pinkas, and R. Sumner, "Privacy preserving auctions and mechanism design," in *Proceedings of the 1st ACM Conference on Electronic Commerce*, pp. 129–139, November 1999.

[13] K. Viswanathan, C. Boyd, and E. Dawson, "A three hhased schema for sealed bid auction system design," in *Proceedings of the Australasian Conference on Information Security and Privacy*, pp. 412–426, Springer, Brisbane, Australia, July 2000.

[14] K. Omote and A. Miyaji, "A practical English auction with simple revocation," *IEICE - Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 85, no. 5, pp. 1054–1061, 2002.

[15] K. Peng, C. Boyd, E. Dawson, and K. Viswanathan, "Efficient implementation of relative bid privacy in sealed-bid auction," in *Proceedings of the International Workshop on Information Security Applications*, pp. 244–256, Springer, Jeju Island, Korea, August 2003.

[16] M. K. Franklin and M. K. Reiter, "The design and implementation of a secure auction service," *IEEE Transactions on Software Engineering*, vol. 22, no. 5, pp. 302–312, 1996.

[17] H. Kikuchi, M. Hakavy, and D. Tygar, "Multi-round anonymous auction protocols," *IEICE - Transactions on Info and Systems*, vol. 82, no. 4, pp. 769–777, 1999.

[18] K. Sako, "An Auction Protocol Which Hides Bids of Losers," in *Proceedings of the International Workshop on Public Key Cryptography*, pp. 422–432, Springer, Melbourne, Australia, September 2000.

[19] K. Suzuki, K. Kobayashi, and H. Morita, "Efficient sealed-bid auction using hash chain," in *Proceedings of the International Conference on Information Security and Cryptology*, pp. 183–191, Springer, Seoul, Korea, December 2000.

[20] K. Suzuki and M. Yokoo, "Secure generalized Vickrey auction using homomorphic encryption," in *Proceedings of the International Conference on Financial Cryptography*, pp. 239–249, Springer, Guadeloupe, French West Indies, January 2003.

[21] K. Peng, C. Boyd, and E. Dawson, "Optimization of electronic first-bid sealed-bid auction based on homomorphic secret sharing," in *Proceedings of the International Conference on Cryptology in Malaysia*, pp. 84–98, Springer, Kuala Lumpur, Malaysia, September 2005.

[22] H. S. Galal and A. M. Youssef, "Verifiable sealed-bid auction on the Ethereum blockchain," in *Proceedings of the International Conference on Financial Cryptography and Data Security*, pp. 265–278, Springer, Santa Barbara Beach Resort Curaçao, March 2018.

[23] A. Juels and M. Szydlo, "A two-server, sealed-bid auction protocol," in *Proceedings of the International Conference on Financial Cryptography*, pp. 72–86, Springer, Southampton, Bermuda, March 2002.

[24] M. Nojoumian and D. R. Stinson, "Unconditionally secure first-price auction protocols using a multicomponent commitment scheme," in *Proceedings of the International Conference on Information and Communications Security*, pp. 266–280, Springer, Barcelona, Spain, December 2010.

[25] N. Dong, H. Jonker, and J. Pang, "Analysis of A Receipt-Free auction protocol in the applied pi calculus," in *Proceedings of the International Workshop on Formal Aspects in Security and Trust*, pp. 223–238, Springer, Pisa, Italia, November 2010.

[26] H. S. Galal and A. M. Youssef, "Succinctly verifiable sealed-bid auction smart contract," in *Data Privacy Management, Cryptocurrencies and Blockchain Technology*Springer, New York, NY, USA, 2018.

[27] H. S. Galal and A. M. Youssef, "Trustee: full privacy preserving vickrey auction on top of ethereum," in *Proceedings of the International Conference on Financial Cryptography and Data Security*, pp. 190–207, Springer, St. Kitts, Saint Kitts and Nevis, February 2019.

[28] Y. Jiao, P. Wang, D. Niyato, and K. Suankaewmanee, "Auction mechanisms in cloud/fog computing resource allocation for

public blockchain networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 30, no. 9, pp. 1975–1989, 2019.

[29] T. D. Nguyen and M. T. Thai, "Trustless framework for iterative double auction based on blockchain," in *Proceedings of the International Conference on Security and Privacy in Communication Systems*, pp. 3–22, Springer, Orlando, VA, USA, October 2019.

[30] B. An, M. Xiao, A. Liu, G. Gao, and H. Zhao, "Truthful crowdsensed data trading based on reverse auction and blockchain," in *Proceedings of the International Conference on Database Systems for Advanced Applications*, pp. 292–309, Springer, Chiang Mai, Thailand, April 2019.

[31] D. Boneh and X. Boyen, "Short signatures without random oracles," in *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 56–73, Springer, Interlaken, Switzerland, May 2004.

[32] M. Bellare, S. Keelveedhi, and T. Ristenpart, "Message-locked encryption and secure deduplication,," in *Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 296–312, Springer, Athens, Greece, May 2013.

[33] J. K. Liu, V. K. Wei, and D. S. Wong, "Linkable spontaneous anonymous group signature for ad hoc groups," in *Proceedings of the Australasian Conference on Information Security and Privacy*, pp. 325–335, Springer, Sydney, Australia, July 2004.

[34] R. L. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret," in *Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security*, pp. 552–565, Springer, Gold Coast, Australia, December 2001.

[35] S. Goldwasser, S. Micali, and R. L. Rivest, "A digital signature scheme secure against adaptive chosen-message attacks," *SIAM Journal on Computing*, vol. 17, no. 2, pp. 281–308, 1988.

[36] M. Abe, M. Ohkubo, and K. Suzuki, "1-Out-Of-n signatures from a variety of keys," in *Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security*, pp. 415–432, Springer, Queenstown, New Zealand, December 2002.

[37] J. Camenisch, D. Derler, S. Krenn, H. C. Pöhls, K. Samelin, and D. Slamanig, "Chameleon-hashes with ephemeral trapdoors," in *Proceedings of the IACR International Workshop on Public Key Cryptography*, pp. 152–182, Springer, Amsterdam, Netherlands, March 2017.

[38] D. Chaum and H. Van Antwerpen, "Undeniable signatures," in *Proceedings of the Conference on the Theory and Application of Cryptology*, pp. 212–216, Springer, Houthalen, Belgium, April 1989.

[39] F. Rezaeibagha, Y. Mu, S. Zhang, and X. Wang, "Provably Secure Homomorphic Signcryption," in *Proceedings of the International Conference on Provable Security*, pp. 349–360, Springer, Xi'an, China, October 2017.