entropy

IMPACT FACTOR 2.0

Indexed in: PubMed

CITESCORE 5.2

Article

Multi-Party Semi-Quantum Simultaneous Ascending Auction Protocol Based on Single-Particle States

Xiuqi Wu, Yu Yang, Baichang Wang, Yue Zhang and Yunguang Han

Special Issue

Quantum Information Security

Edited by

Dr. Wei Yang

MDPI

https://doi.org/10.3390/e28010039

entropy

MDPI

Article

Multi-Party Semi-Quantum Simultaneous Ascending Auction Protocol Based on Single-Particle States

Xiuqi Wu [1], Yu Yang [1], Baichang Wang [1], Yue Zhang [2] and Yunguang Han [1,*]

[1] College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 211106, China
[2] School of Computer Engineering, Nanjing Institute of Technology, Nanjing 211167, China
* Correspondence: hanyunguang@nuaa.edu.cn

Abstract

Simultaneous ascending auctions find extensive applications in spectrum licensing and advertising space allocation. However, existing quantum sealed-bid auction protocols suffer from dual limitations: they cannot support multi-item simultaneous bidding scenarios, and their reliance on complex quantum resources along with requiring full quantum operational capabilities from bidders fails to accommodate practical constraints of quantum resource-limited users. To address these challenges, this paper proposes a multi-party semi-quantum simultaneous ascending auction protocol based on single-particle states. The protocol employs a trusted honest third party (HTP) responsible for quantum state generation, distribution, and security verification. Bidders determine their groups through quantum measurements and privately encode their bid vectors. Upon successful HTP authentication, each bidder obtains a unique identity code. During the bidding phase, HTP dynamically updates quantum sequences, allowing bidders to submit bids for multiple items by performing only simple unitary operations. HTP announces the highest bid for each item in real time and iteratively generates auction sequences until no new highest bid emerges, thereby achieving simultaneous ascending auctions for multiple items. It acts as a quantum-secured signaling layer, ensuring unconditional security for bid transmission and identity verification while maintaining classical auction logic. Quantum circuit simulations validate the protocol's feasibility with current technology while satisfying critical security requirements, including anonymity, verifiability, non-repudiation, and privacy preservation. It provides a scalable semi-quantum auction solution for resource-constrained scenarios.

Keywords: quantum auction; semi-quantum protocol; quantum information security; simultaneous ascending auction; unconditional security

Academic Editors: Osamu Hirota and Wei Yang

Received: 30 September 2025
Revised: 12 December 2025
Accepted: 14 December 2025
Published: 28 December 2025

1. Introduction

Quantum cryptography, a key subfield of quantum information science, combines quantum-mechanical principles with classical cryptography. It has achieved major advances in protocol design and implementation, including Quantum Key Distribution (QKD) [1,2], Quantum Secure Direct Communication (QSDC) [3,4], and Quantum Secret Sharing (QSS) [5,6]. These technologies are increasingly deployed in practice, such as quantum voting systems [7] and quantum transaction platforms, offering new models for secure applications.

Auctions are fundamental mechanisms for resource allocation and trading [8–10]. By information transparency and bidding rules, they can be categorized into open-cry and

sealed-bid formats [11]. English and Dutch auctions are open-cry, with real-time price discovery. Sealed-bid auctions require bidders to submit offers independently and confidentially, which better preserves strategy privacy and suits anonymity-sensitive scenarios.

However, conventional sealed-bid mechanisms rely on computational assumptions in classical cryptography (e.g., integer factorization and discrete logarithms). With rapid progress in quantum computing [12,13], Shor's algorithm solves these problems in polynomial time [14] and Grover's algorithm speeds up search [15], exposing sealed-bid systems to quantum attacks [16]. This motivates security protocols grounded in physical principles.

Unlike classical schemes that offer computational security, quantum cryptographic protocols provide information-theoretic security (or unconditional security). This ensures that encrypted data remains secure even against adversaries with unlimited computing power, guaranteeing forward secrecy. In the context of auctions, this prevents historical bid data from being decrypted retroactively once powerful quantum computers become available. It is important to clarify that our proposed protocol serves as a quantum-secured signaling layer. It utilizes quantum mechanics to secure the transmission of bids and verify identities, while the underlying auction allocation logic (comparing bids and determining winners) follows the classical simultaneous ascending auction mechanism.

Against this backdrop, research on quantum sealed-bid auction (QSA) protocols has grown rapidly. The goal is to design quantum-resilient mechanisms that ensure fairness, preserve privacy, and enhance security.

The conceptual framework of quantum auctions was introduced in 2008 [17]. In 2009, Naseri [18] proposed a GHZ-based QSA enabling secure multi-party bid transmission. That scheme resisted only external attacks and was vulnerable internally. Follow-up work refined designs and security analyses. Qin et al. [19] and Yang et al. [20] exposed attacks via double CNOT and pseudo-entangled states; their fixes did not consider a dishonest auction center. In 2010, Zhao et al. [21] added post-confirmation to mitigate collusion, later refined for partial collusion. In 2014, Liu et al. [22] integrated QKD for bid encryption and hash-based confirmation. In 2016, they proposed a single-particle QSBA [23], reducing quantum resources, but Zhang et al. [24] showed coordinated attacks remained. Recent advances include QFT- and d-dimensional-state protocols [25], an anonymous QSA via the Chinese Remainder Theorem [26], and an auctioneer-free scheme with Bell-state swapping [27]. Semi-quantum secure multi-party summation (SQSMS) [28–33] has also gained attention due to its compatibility with users of varying quantum capabilities.

Despite these advancements, existing QSA research faces two primary "shortages": (1) **Capability Shortage**—most protocols require fully quantum-capable participants, which is impractical for general users. (2) **Functional Shortage**: Most studies focus on single-item sealed-bid auctions, failing to address the complexity of simultaneous ascending auctions for multiple items. To address this, we combine Milgrom's simultaneous ascending auction theory [34] with a semi-quantum design and propose a quantum simultaneous ascending auction (QSAA) framework that supports users with diverse capabilities. Under capability constraints, semi-quantum bidders obtain unique identity codes from an honest, fully quantum third party (HTP) and submit bids using simple unitary operations. The protocol preserves anonymity, privacy, fairness, verifiability, and non-repudiation: only HTP learns bids; sealed bids are disclosed simultaneously; bidders cannot repudiate submitted bids and HTP cannot deny receipts.

The remainder of this paper is organized as follows: Section 2 introduces the fundamental concepts of simultaneous ascending auction mechanisms and semi-quantum protocols. Section 3 elaborates on a multi-party semi-quantum simultaneous ascending auction protocol in detail. Section 4 presents simulation analyses. Section 5 provides performance evaluations. Finally, Section 6 concludes the paper.

https://doi.org/10.3390/e28010039

2. Preliminaries

Our protocol enables anonymous auctions for users with limited quantum capabilities. The semi-quantum simultaneous ascending auction (SQSAA) assigns each bidder a unique identity code. Bidders apply unitary operations to encode bid prices onto quantum sequences, implementing a simultaneous ascending-price auction. We first introduce the auction mechanism and the semi-quantum model used in this paper.

2.1. Simultaneous Ascending Auction Mechanism

The simultaneous ascending-price auction is a multi-item dynamic mechanism widely used in spectrum licensing and advertisement allocation. Its core characteristics include simultaneous bidding for multiple items, round-by-round price increments, and a public bidding process. In each round, bidders may raise bids on any items. After each round, each item's price updates to the highest bid received. The process repeats until no further bids are submitted, and items are allocated to the highest bidders at their final prices.

2.2. Semi-Quantum Protocol Architecture and Trust Model

The semi-quantum architecture involves two types of users:

Quantum Users (HTP)—the honest third party (HTP) possesses full quantum capabilities (preparation, manipulation, and measurement). Assumption: In this semi-quantum model, the HTP is assumed to be a trusted authority. The HTP generates and measures states correctly and does not collude with bidders to reveal bids to others, although the HTP itself learns the bid values.

Semi-Quantum Users (Bidders): Participants with constrained quantum capabilities, typically limited to Z-basis or X-basis measurements (computational or Fourier bases), applying simple unitary operations, and reflecting received quantum states. This design reduces hardware complexity and cost.

2.3. Protocol Characteristics

The semi-quantum design offers two practical advantages [30]:

System compatibility—basic quantum operations can be implemented using low-cost optical components. When devices malfunction, systems can fall back to a semi-quantum mode, enhancing robustness and easing the transition from classical to quantum infrastructures.

Cost efficiency: Limiting some users' quantum capabilities reduces dependence on expensive quantum resources and large-scale quantum memory processing, enabling economically viable deployment during the current transitional phase.

3. Multi-Party Semi-Quantum Simultaneous Ascending Auction Protocol

Assume an honest third party (HTP) with full quantum capability acts as the auction coordinator and never colludes with bidders. There are n semi-quantum participants $P_1, P_2, \ldots, P_n$ who serve as bidders with restricted capabilities: computational-basis or Fourier-basis measurement, simple unitary operations, and reflection. Each bidder P_i $(i = 1, 2, \ldots, n)$ independently generates a private randomized identity vector v_i satisfying $v_i = (v_i^1, v_i^2, \ldots, v_i^n), v_i^o \in \{0, 1\}, o = (1, 2, \ldots, n)$. These vectors serve as cryptographic identity anchors, dynamically integrated into quantum state manipulations through controlled unitary operations.

The protocol has four phases: initialization, identity encoding distribution, bidding, and result announcement. In initialization, HTP constructs differentiated quantum sequences for each bidder and collaborates with P_i to validate channel security. In identity encoding distribution, each bidder generates a private identity vector, applies unitary oper-

ations to assigned particles, HTP constructs a verification matrix, and validates integrity against predefined rules. In bidding, each bidder applies unitary operations to encode bids and computes a commitment. In the result announcement, HTP determines the highest bid and bidder per item, and others verify using commitments. The schematic diagram of the protocol is shown in Figure 1.

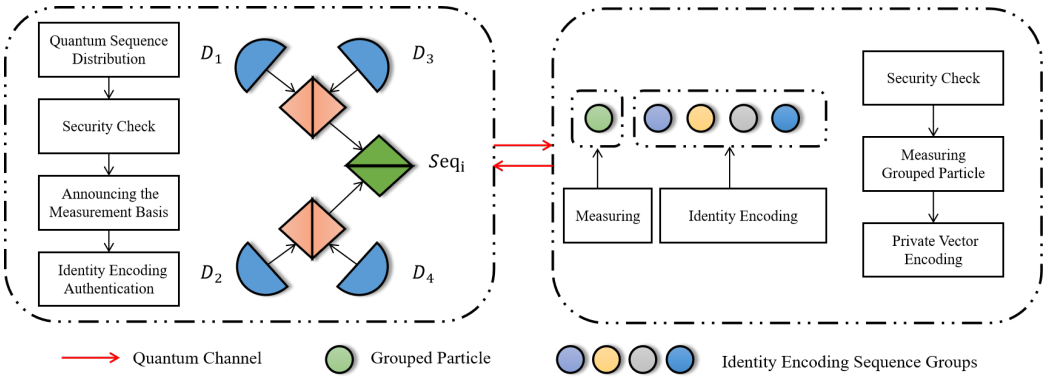

Figure 1. Workflow of identity encoding distribution and verification at HTP. (Lateral diagrams correspond to Step 4 and 5).

3.1. Initialization Phase

Step 1: HTP and each authorized bidder pre-share an authenticated key sequence $K_i = (k_i^1, k_i^2, \ldots, k_i^{4n+1+m})$, $k_i^l \in \{0,1\}$. * Note: These keys are distributed via a secure classical channel or a prior standard QKD session before the auction begins. If keys are compromised, the authentication fails; thus, key refreshment is recommended for subsequent sessions. * HTP randomly prepares $(4n+1)$ rotation-basis particles $R_i = (r_i^1, r_i^2, \ldots, r_i^{4n+1})$, $r_i^p \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and m decoy particles $C_i = (c_i^1, \ldots, c_i^m)$, $c_i^q \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ for each bidder. According to K_i, HTP determines the embedding order of decoy and rotation particles in the quantum sequence, using (1) if $k_i^l = 0$, a rotational particle r_i^p is inserted into the sequence. (2) If $k_i^l = 1$, a decoy particle c_i^q is embedded instead. HTP then produces a quantum sequence Seq_i of length $(4n+1+m)$. Repeating this for all bidders yields n sequences $(Seq_1, \ldots, Seq_n)$, which HTP sends over authenticated quantum channels.

Step 2: Upon receiving Seq_i, bidder P_i routes each particle according to k_i^l: If $k_i^l = 1$, P_i directly reflects the particle to HTP; if $k_i^l = 0$, P_i retains the particle for Step 4.

Step 3: HTP measures the reflected particles using the preparation bases indicated by k_i^l and computes the quantum bit error rate (QBER) by comparing outcomes with prepared states. If QBER exceeds a threshold η, the protocol aborts; otherwise it proceeds. Threshold Selection: The threshold η is not arbitrary; it is selected based on standard security proofs for BB84-type protocols. To tolerate environmental noise while securely detecting intercept-resend attacks (which theoretically induce $\sim 25\%$ error), η is typically set strictly below the coherent attack bound (approx. 11%), for example, in the range of 5–8% in practical scenarios.

3.2. Identity Encoding Distribution Phase

Step 4: After eavesdropping detection, each P_i discards decoy particles and keeps rotation particles. HTP designates the first rotation particle as the grouping particle and publishes its measurement basis on the bulletin board. HTP records initial states and counts bidders per group. Each P_i measures the grouping particle according to determine its group: outcomes $|0\rangle, |1\rangle, |+\rangle, |-\rangle$ map to groups 1–4.

Step 5: Each P_i generates a private n-dimensional vector v_i, then applies unitary operations to assigned particles according to: (1) if $v_i^o = 0$, it applies the Pauli-I operation

(σ_I) to the rotational particle. (2) If $v_i^o = 1$, it performs the Pauli-Y operation (σ_Y) on the rotational particle.

Afterward, P_i sends the updated sequence Seq_i' to HTP.

Step 6: Upon receiving Seq_i' from all bidders, HTP determines each bidder's group from k_i^l and the grouping particles, then measures each particle in the corresponding basis to form a mapping $f_x : x \mapsto z_i^j$ (Table 1). For both computational and Fourier bases, record $z_i^j = 1$ if the outcome flips relative to the initial state; otherwise, set $z_i^j = 0$.

$$\mathbf{Z} = \begin{bmatrix} z_1^1 & z_1^2 & \cdots & z_1^{4n} \\ \vdots & \vdots & \ddots & \vdots \\ z_n^1 & z_n^2 & \cdots & z_n^{4n} \end{bmatrix} \tag{1}$$

Table 1. Initial states and mapping results.

Initial States	Measurement Results	Mapping Results z_i
$\|0\rangle$	$\|0\rangle$	0
$\|0\rangle$	$\|1\rangle$	1
$\|1\rangle$	$\|1\rangle$	0
$\|1\rangle$	$\|0\rangle$	1
$\|+\rangle$	$\|+\rangle$	0
$\|+\rangle$	$\|-\rangle$	1
$\|-\rangle$	$\|-\rangle$	0
$\|-\rangle$	$\|+\rangle$	1

After constructing the $n \times 4n$ matrix from z_i^j of the quantum sequences Seq_i' returned by bidders, HTP checks the Hamming weight of each valid column. Identity encoding distribution succeeds iff, for every valid column j,

$$\sum_{i=1}^{n} z_i^j = 1 \tag{2}$$

and the number of bidders within each group matches HTP's initial records. Liveness and Restart: If this condition is not met (e.g., column sum $\neq 1$) or if the number of bidders in a group mismatches the record (group collision), HTP broadcasts a "Restart" signal. The current round is discarded, and the Identity Encoding Phase repeats from Step 1. This ensures the protocol remains live and reaches a valid distribution state. Columns with no embedded identity encoding are excluded from verification.

3.3. Bidding Phase

Step 7: Completing these operations, each bidder obtains a unique identity code. Repeating Steps 1–3, HTP generates a new quantum sequence $\mathrm{Seq}_i^{(r)}$ and new $K_i^{(r)}$ for each round r. In each sequence, the first $(2 + n)$ particles encode identity (2 group particles followed by n identity particles). For item w with domain $\{0, \ldots, d_w - 1\}$, the next $\lceil \log_2 d_w \rceil$ particles encode the bid.

Step 8: Assuming HTP specifies that the initial bid range for the w-th auctioned item lies within $[0, d_w - 1]$. HTP broadcasts the valid bidding range and specifies the required bit-length $L = \lceil \log_2 d_w \rceil$ for the bid vector. This ensures all bidders encode their bids using a consistent quantum sequence length. Each bidder P_i converts their bid into a corresponding private bid binary sequence $b_i^{(w)} = (b_i^{\lceil \log_2 d_w \rceil}, \ldots, b_i^2, b_i^1)$.

Each bidder first encodes their identity sequence. Based on the grouping of particles, the first two particles encode the group identifier, with the conventions 00, 01, 10, and 11

designating the first, second, third and fourth groups, respectively. For example, for group 2 (01), apply I to the first qubit and H to the second. The subsequent n particles encode the private identity code.

For all items, bits are encoded from most significant to least significant (left to right in the vector, applied right to left on qubits as specified in Step 9).

Step 9: The bidder applies the Hadamard, Pauli-Y and Pauli-I operations to the first two particles and encodes their identity vector. Subsequently, they encode their private bid binary sequence b_i^a (where $a = 1, 2, \ldots, \lceil \log_2 d_w \rceil$) onto the specific bid particle sequence from right to left. If $b_i^a = 0$, P_i performs the σ_I operation; if $b_i^a = 1$, P_i applies the σ_Y operation. Otherwise (if no bid is intended), the bidder performs no operations on any particles in the specific bid particle sequence. Then, P_i returns the newly processed particle sequence $\mathrm{Seq}_i^{(r')}$ to HTP, particle by particle. It is noteworthy that for multiple auction items, the initial-round bidding prices are encoded in the particle sequence following the first auctioned item. Correspondingly, the particle count of $\mathrm{Seq}_i^{(r)}$ is augmented according to the same rule established for the first item.

Step 10: Concurrently, in each round, each bidder P_i computes a binding, hiding commitment to their bid for each item using a collision-resistant hash function $\mathrm{Hash}(\cdot)$. Let $s_i^w \in \mathbb{Z}_N$ be a per-round random nonce. Define $\mathrm{com}_i^w = \mathrm{Hash}\big(\mathrm{round\_id} \,\|\, w \,\|\, \mathrm{id}_i \,\|\, b_i^w \,\|\, s_i^w\big)$, where b_i^w is the bidder's decimal bid for item w in that round, and $\|$ denotes concatenation. HTP records com_i^w for each bidder and item per round. Any bid update must include a fresh commitment.

3.4. Result Announcement Phase

Step 11: After receiving the quantum sequences $\mathrm{Seq}_i^{(r')}$ from all bidders, HTP first constructs a mapping result matrix according to the identity encoding distribution rules and verifies each bidder's identity encoding sequence. Subsequently, HTP measures the first two particles using the following rules. When the Pauli-I operation is applied to a qubit, the HTP measures it in the same basis as its initial state. Conversely, when the Hadamard operation is applied, measurement occurs in the conjugate basis relative to the initial state.

Taking P_2 as an example, its identity code is Group 2, Number 3. The unitary operation for its group particles consists of applying the Pauli-I operation to the first particle and the Hadamard operation to the second particle. The HTP measures the first particle using the same measurement basis as its initial state. Regardless of the initial state, if the measurement outcome matches the initial state, the HTP calculates the mapping result of the first particle as 0. For the second particle, the HTP employs the measurement basis orthogonal to the initial state: if the initial state is $|0\rangle$ or $|1\rangle$, the measurement outcome will be $|+\rangle$ or $|-\rangle$; conversely, if the initial state is $|+\rangle$ or $|-\rangle$, the measurement outcome will be $|0\rangle$ or $|1\rangle$. In this case, the HTP calculates the mapping result of the second particle as 1, as illustrated in the diagram. Please refer to Table 2 for detailed information.

Then, HTP measures the specific bid particle sequence from right to left using the corresponding basis, recording each outcome t_i^a: if the measurement result is opposite to the initial state, it is recorded as $t_i^a = 1$; otherwise, $t_i^a = 0$. Finally, HTP arranges all specific bid results t_i^a, converts the bits to a decimal bid, selects the highest first-round bid, and publishes it on the bulletin board (or via a classical channel).

Table 2. Group mapping measurement and mapping results.

Initial State	Comp. Basis	Mapping	Fourier Basis	Mapping
$\|0\rangle$	$\|0\rangle$	0	$\|+\rangle$	1
$\|1\rangle$	$\|1\rangle$	0	$\|-\rangle$	1
$\|+\rangle$	$\|0\rangle$	1	$\|+\rangle$	0
$\|-\rangle$	$\|1\rangle$	1	$\|-\rangle$	0

Step 12: After completing initial bidding for all auctioned items, bidders collectively negotiate the bid increment range for subsequent rounds.Specifically, suppose they determine the starting price for each new round as 10% of the previous round's highest bid for that item, Starting $\text{Price}_{\text{next}} = (1 + 10\%) \times \text{Highest Bid}_{\text{previous}}$. Then, they repeat Steps 7–10 for the next round. Upon receiving quantum sequences, HTP executes Step 11.

If a bid does not exceed the current highest bid, HTP withholds updates. The auction concludes when no item receives a higher bid; HTP then publishes all final highest bids.

Step 13: Assume bidder P_e is the highest bidder for item w. He discloses b_e^w and s_e^w, enabling others to recompute $\text{com}_e^w = \text{Hash}(\text{round\_id} \,\|\, w \,\|\, \text{id}_e \,\|\, b_e^w \,\|\, s_e^w)$ and check it matches the recorded commitment. If P_e's commitment is validated by all bidders and HTP, he is confirmed as the highest bidder; otherwise, verification fails. If any bidder P_f ($f \neq e$) claims their bid exceeds HTP's published highest bid or P_e, P_f broadcasts a complaint and discloses (b_f^w, s_f^w) for verification. Successful verification mandates HTP to update the item's highest bid; failed verification maintains the current highest bid. HTP declares P_e the winner for item w only when no valid complaints are substantiated (Figure 2).

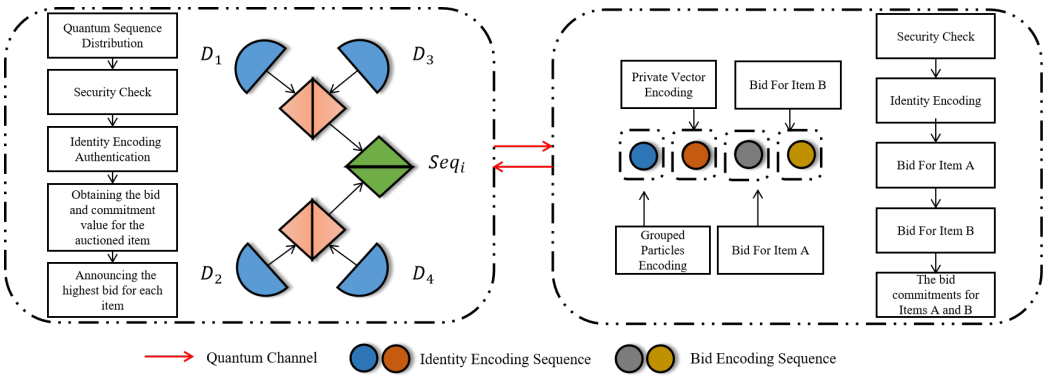

Figure 2. Overall simultaneous ascending auction workflow with identity and bid encoding.

4. Simulation of the Proposed Protocol

The Qiskit simulation presented here aims to validate the correctness of the quantum physical layer—specifically the single-particle encoding, decoding, and noise robustness—rather than to simulate the classical arithmetic logic of the auctioneer.

We illustrate the protocol with Qiskit simulations in two phases: multi-party semi-quantum identity encoding distribution and multi-party semi-quantum simultaneous ascending auction. Consider an HTP coordinating three semi-quantum bidders P_1, P_2, P_3. Bidders independently sample private vectors $v_1 = (0,1,0)$, $v_2 = (0,1,1)$, $v_3 = (1,0,1)$.

4.1. Multi-Party Semi-Quantum Identity Encoding Distribution

Assume at this stage, HTP allocates distinct key sequences K_1, K_2, K_3 to bidders P_1, P_2, P_3 respectively, where

$$K_1 = \{0,1,0,1,0,1,0,0,1,0,0,1,0,1,0,0,1,0,0,0\}$$
$$K_2 = \{1,0,0,0,1,1,0,1,0,0,0,0,1,0,1,0,0,0,0,1\}$$
$$K_3 = \{1,1,0,1,0,0,0,0,1,0,1,1,0,0,0,1,0,0,0,0\}$$

Step 1: HTP randomly generates rotation particles R_1, R_2, R_3 and decoy particles C_1, C_2, C_3 from BB84 state $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$.According to the rules specified in the aforementioned protocol, the quantum sequences Seq_1, Seq_2 and Seq_3 are formed in Table 3. The quantum circuit diagram for P_1 is illustrated in Figure 3 according to the aforementioned conditions. In this simulation, we employ a decoy state ratio of approximately 50% (1:1 with rotation particles) to maximize statistical detection sensitivity for the case study.

Table 3. Example construction of sequences Seq_1, Seq_2, Seq_3 based on keys K_1, K_2, K_3 and BB84 states.

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
K_1	0	1	0	1	0	1	0	0	1	0
R_1	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|-\rangle$	$\|-\rangle$
C_1	$\|0\rangle$	$\|-\rangle$	$\|-\rangle$	$\|0\rangle$	$\|+\rangle$	$\|+\rangle$	$\|-\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$
Seq_1	$\|0\rangle$	$\|-\rangle$	$\|+\rangle$	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|0\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$
K_2	1	0	0	0	1	1	0	1	0	0
R_2	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|0\rangle$	$\|-\rangle$	$\|+\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$
C_2	$\|-\rangle$	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$	$\|+\rangle$	$\|+\rangle$	$\|-\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$
Seq_2	$\|-\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|+\rangle$	$\|+\rangle$	$\|+\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$
K_3	1	1	0	1	0	0	0	0	1	0
R_3	$\|-\rangle$	$\|-\rangle$	$\|+\rangle$	$\|0\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|1\rangle$
C_3	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$	$\|-\rangle$	$\|0\rangle$	$\|0\rangle$	$\|-\rangle$	$\|+\rangle$
Seq_3	$\|-\rangle$	$\|0\rangle$	$\|+\rangle$	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|1\rangle$
	11	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
K_1	0	1	0	1	0	0	1	0	0	0
R_1	$\|+\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	$\|+\rangle$	$\|1\rangle$
C_1	$\|-\rangle$	$\|0\rangle$	$\|+\rangle$	$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$	$\|0\rangle$
Seq_1	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$	$\|1\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$	$\|1\rangle$
K_2	0	0	1	0	1	0	0	0	0	1
R_2	$\|0\rangle$	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$	$\|-\rangle$	$\|1\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|+\rangle$
C_2	$\|0\rangle$	$\|1\rangle$	$\|-\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$	$\|1\rangle$	$\|-\rangle$	$\|+\rangle$	$\|1\rangle$
Seq_2	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|-\rangle$	$\|+\rangle$	$\|1\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|1\rangle$
K_3	1	1	0	0	0	1	0	0	0	0
R_3	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$	$\|-\rangle$	$\|+\rangle$	$\|+\rangle$
C_3	$\|-\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|-\rangle$	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$
Seq_3	$\|-\rangle$	$\|0\rangle$	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$	$\|+\rangle$	$\|+\rangle$

BB84 states include $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$; K represents the key, R represents the receiver state, C represents the channel state, and Seq represents the resulting sequence.

Step 2: Each bidder routes particles according to K_i. P_i reflects decoy particles and retains rotation particles. HTP measures reflected particles in the corresponding bases and computes QBER. For example, in Seq_1 the particles at positions 2, 4, 6, 9, 12, 14, and 17 are reflected (Figure 4). If the error rate is below the threshold, the protocol proceeds (Figure 5).

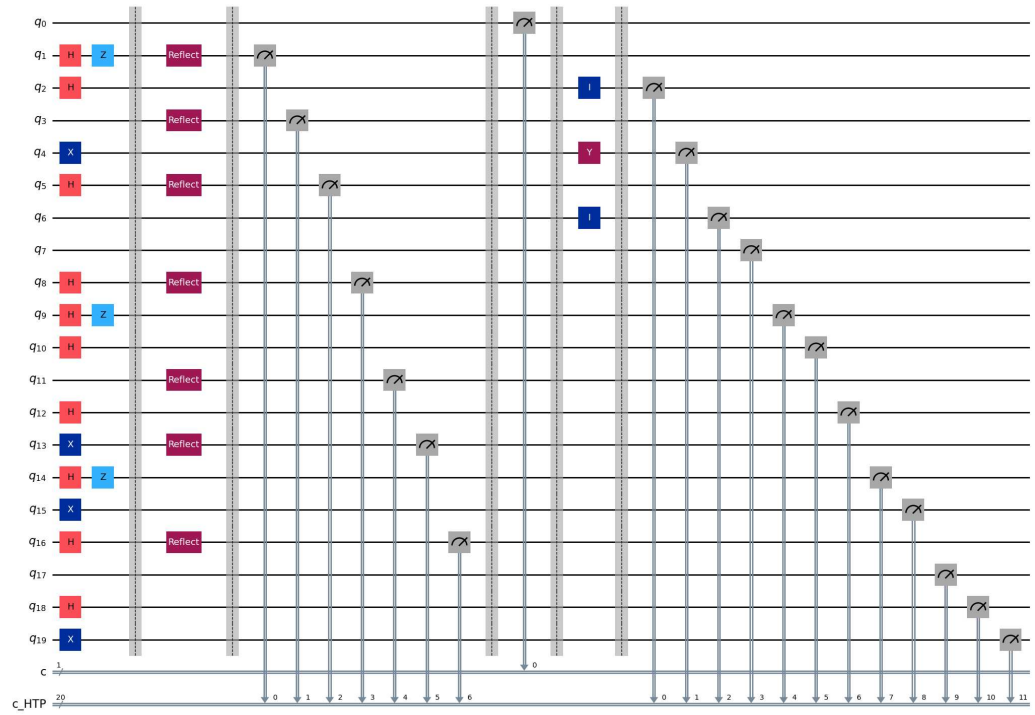

Figure 3. Circuit for identity encoding distribution using BB84 single-qubit states.

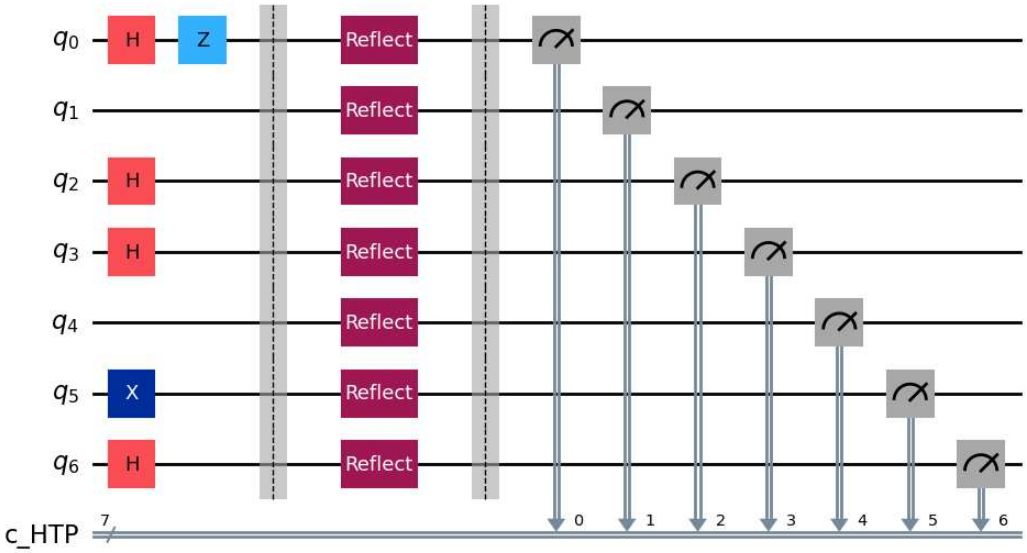

Figure 4. Decoy particle reflection and QBER estimation circuit used for channel checking.

Step 3: HTP publishes (or broadcasts via classical channel) the measurement basis for the first rotation particle on the bulletin board while recording the number of bidders in each group. Bidders P_1, P_2, P_3 measure the first particle in their respective rotation particle sequences Seq_1, Seq_2 and Seq_3 using the announced basis. Taking P_1 as an example: when the first particle in its rotation sequence is $|0\rangle$ (Figure 6) and the computational basis measurement yields 0, P_1 is assigned to Group 1. Similarly, P_2 and P_3 are assigned to Group 2 and Group 3, respectively. These grouping results are consistent with the HTP's recorded data. Then, Bidder P_1 performs unitary operations on positions 2–4 of its rotation particle sequence: specifically applying the σ_Y operation to the 3rd position and the σ_I operation to positions 2 and 4, while leaving other particles unchanged (Figure 7). Afterward, P_1

sends Seq_1' to HTP. Following the same rules, P_2 and P_3 execute their designated unitary operations and send their sequences Seq_2' and Seq_3' to HTP.

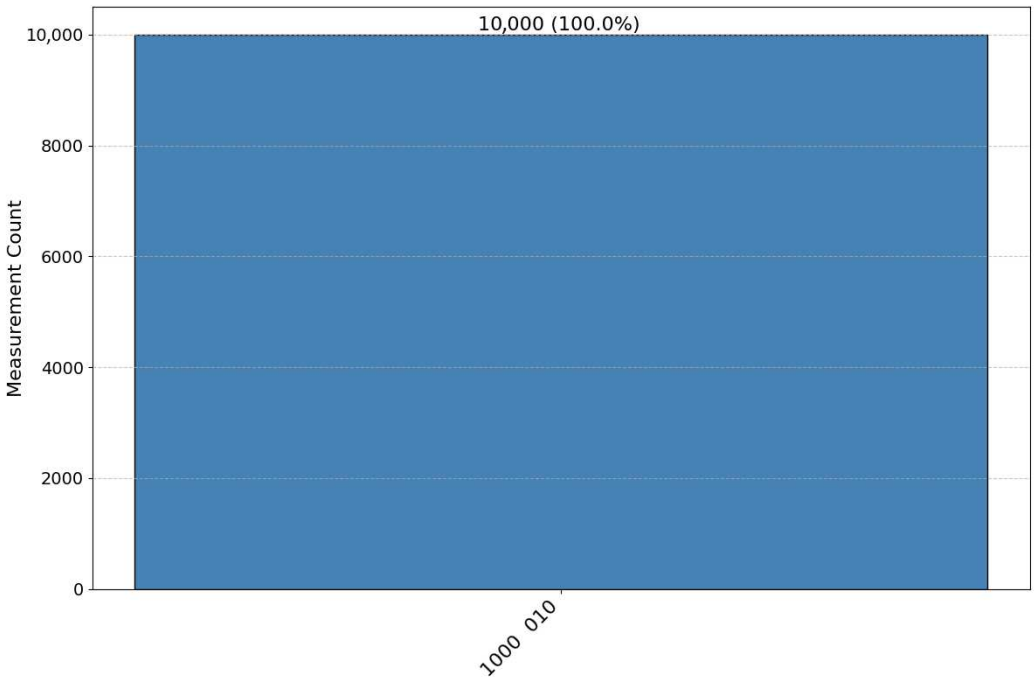

Figure 5. Example of positions reflected by bidder P_1 for decoy checking according to K_1.

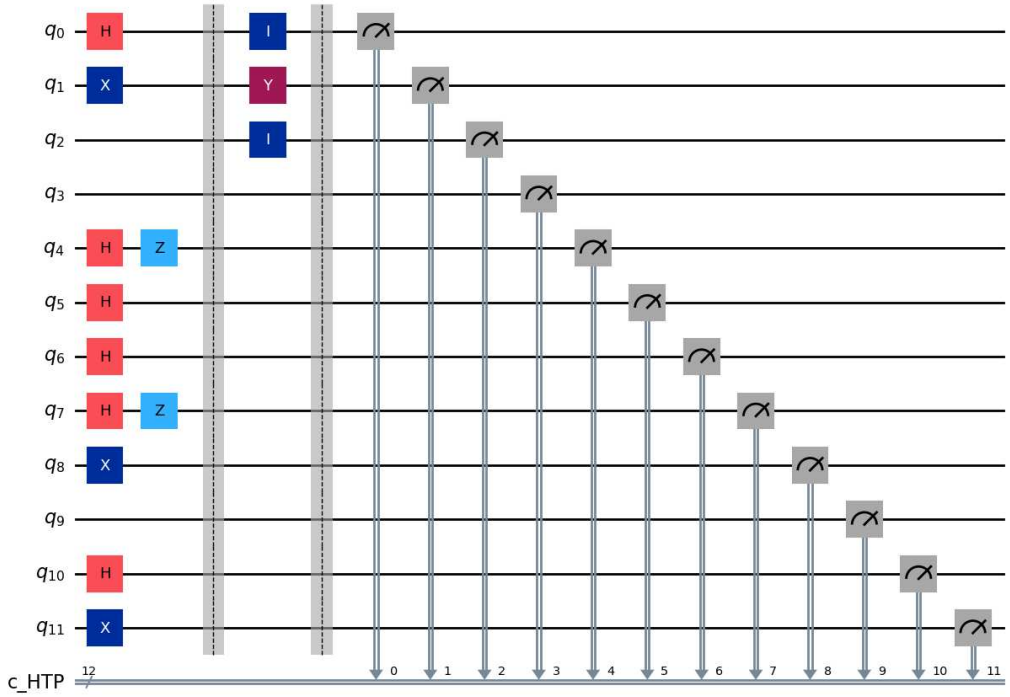

Figure 6. Circuit example of rotation-basis particle operations for identity and bid encoding.

Step 4: Upon receiving the modified quantum sequences Seq_1', Seq_2' and Seq_3' from bidders P_1, P_2 and P_3, HTP performs sequential measurements on each qubit of the sequences using the measurement basis corresponding to each bidder's group assignment. The mapping results are organized into a 3×12 matrix M, where each row represents a bidder's sequence and each column corresponds to a specific qubit position.

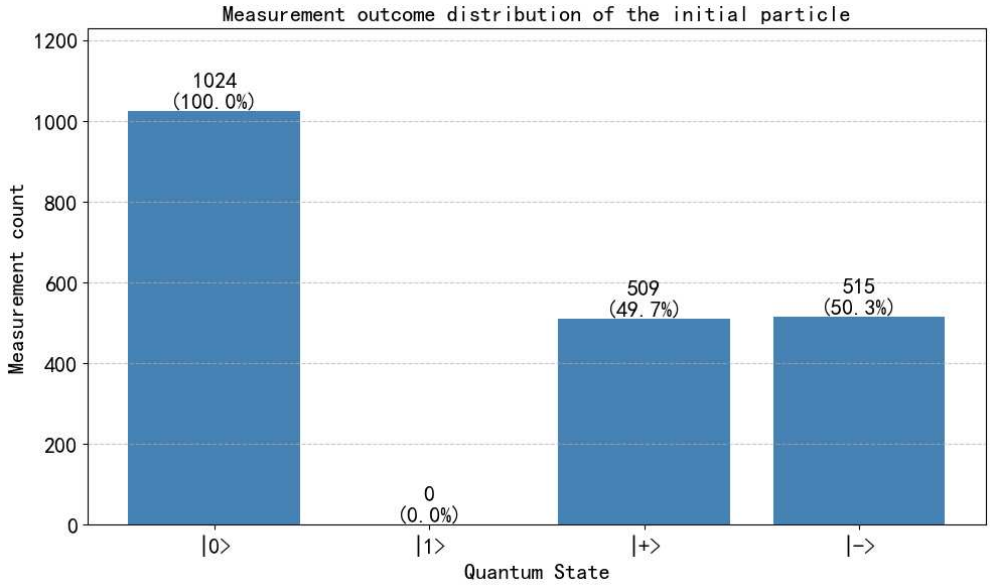

Figure 7. Grouping via the first rotation particle and unitary operations per group.

The per-column Hamming weights (column sums) are (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0). For every valid column, the sum equals 1; therefore, bidders P_1, P_2 and P_3 are assigned the identity designations Group 1 Member 2, Group 2 Member 3, and Group 3 Member 5, respectively, satisfying the predefined condition. Thus, the identity code distribution is successful without repetition (see Figure 8).

	Group 1			Group 2			Group 3			Group 4			
Z_1	0	1	0	0	0	0	0	0	0	0	0	0	$\Leftarrow P_1$
Z_2	0	0	0	0	1	1	0	0	0	0	0	0	$\Leftarrow P_2$
Z_3	0	0	0	0	0	0	1	0	1	0	0	0	$\Leftarrow P_3$
$\oplus$	0	1	0	0	1	1	1	0	1	0	0	0	

Figure 8. Mapping results arranged into a matrix for identity verification.

4.2. Multi-Party Semi-Quantum Simultaneous Ascending Auction

In this stage, all bidders simultaneously place bids on both auction items, A and B (though the protocol permits optional single-item bidding). For demonstration clarity, we assume single-round auction completion. Suppose the initial price ranges for items A and B in the first-round auction are [0, 8] and [0, 10], respectively, with a bid increment benchmark of 10% per round. In the first round, bidders P_1, P_2 and P_3 submit their initial bids for item A as (4, 7, 5) and for item B as (7, 7, 9). All bidders reveal their true maximum willingness-to-pay (i.e., their psychological reserve prices) in the first round, implying that no bidders will revise their bids in subsequent auction rounds.

Step 1: HTP initializes the protocol by assigning distinct key sequences K_1', K_2', K_3' to bidders P_1, P_2, P_3 respectively, where

$$K_1' = \{0,1,0,1,0,1,0,1,1,0,0,1,0,1,0,1,0,0,1,0,0,1,1,0,0\}$$
$$K_2' = \{1,0,0,1,1,1,0,1,0,0,0,0,1,0,1,0,1,1,0,0,0,0,1,0,1\}$$
$$K_3' = \{1,1,0,1,0,0,0,0,1,0,1,1,0,0,1,0,1,0,1,1,0,0,0,1,0\}$$

Then, HTP randomly generates quantum sequences Seq_1'', Seq_2'' and Seq_3'' according to the rules of Step 1,where

$$\begin{aligned}
Seq_1'' = \{&|0\rangle, |-\rangle, |+\rangle, |0\rangle, |1\rangle, |+\rangle, |0\rangle, |0\rangle, |+\rangle, |-\rangle,\\
&|+\rangle, |0\rangle, |+\rangle, |1\rangle, |-\rangle, |-\rangle, |+\rangle, |0\rangle, |1\rangle, |+\rangle,\\
&|-\rangle, |+\rangle, |0\rangle, |1\rangle, |+\rangle, |+\rangle, |0\rangle, |+\rangle, |1\rangle, |-\rangle\}\\
Seq_2'' = \{&|-\rangle, |1\rangle, |-\rangle, |-\rangle, |+\rangle, |+\rangle, |+\rangle, |1\rangle, |+\rangle, |1\rangle,\\
&|0\rangle, |+\rangle, |-\rangle, |-\rangle, |+\rangle, |0\rangle, |+\rangle, |1\rangle, |-\rangle, |-\rangle,\\
&|+\rangle, |0\rangle, |+\rangle, |1\rangle, |-\rangle, |0\rangle, |+\rangle, |1\rangle, |-\rangle, |-\rangle\}\\
Seq_3'' = \{&|-\rangle, |0\rangle, |+\rangle, |+\rangle, |1\rangle, |-\rangle, |0\rangle, |+\rangle, |-\rangle, |1\rangle,\\
&|-\rangle, |0\rangle, |+\rangle, |1\rangle, |-\rangle, |+\rangle, |1\rangle, |-\rangle, |-\rangle, |+\rangle,\\
&|0\rangle, |+\rangle, |1\rangle, |-\rangle, |-\rangle, |+\rangle, |-\rangle, |-\rangle, |+\rangle, |0\rangle\}
\end{aligned}$$

Step 2: Following the aforementioned rules, we conduct channel security eavesdropping detection by referencing the case study from Simulation Experiment 4.1.

Step 3: According to the established rules, bidders P_1, P_2 and P_3 perform group encoding operations on particles located at the first and second positions of the sequence, simultaneously executing identity encoding utilizing private vectors at positions 3 through 5.

As demonstrated in Simulation Experiment 4.1, the bidder P_1 was assigned the identity code "Group 1, Member 2" (with group encoding 00). Given P_1's private vector (0, 1, 0), the identity encoding is implemented on qubits 1–5 through quantum operations: P_1 implements σ_I operations on the first and second particles within their respective rotational particle; the σ_Y operation is applied to the 4th qubit and σ_I operations are maintained on qubits 3 and 5. Following the same rules, bidders P_2 and P_3 subsequently execute their respective unitary operations in accordance with their allocated group codes and private vectors.

Step 4: P_1, P_2 and P_3 convert the decimal bid value of item A into corresponding binary sequences (0, 1, 0, 0), (0, 1, 1, 1) and (0, 1, 0, 1). Concurrently, specific bid particle encoding is implemented at positions 6–9 to comprehensively embed auction information.

Taking bidder P_1 as an example, P_1 implement unitary operations on the rotational particle. Specifically, the σ_Y operation is applied at positions 7, 11, 12, and 13, while the σ_I operation is performed at positions 6, 8, 9, and 10. Then, P_1 sends Seq_1''' to HTP. Following the same procedure, bidders P_2 and P_3 perform their corresponding quantum operations and return Seq_2''' and Seq_3''' to HTP.

Step 5: In accordance with the established rules, HTP constructs a 1×5 identity verification matrix (0, 0, 0, 1, 0) , which matches the identity encoding assigned in Simulation Experiment 4.1. Subsequently, HTP conducts the following operations: (1) Using the same measurement basis as the initial state, HTP measures qubits 6–13 of Seq_1''', obtaining a 1×8 matrix (0, 1, 0, 0, 0, 1, 1, 1) (Figure 9). The auction prices for items A and B are derived from their respective quantum sequences. When converted to decimal notation, these sequences yield the values 4 for A and 7 for B. The same verification procedure is applied to Seq_2''' and Seq_3''', revealing bids of (7, 7) and (5, 9) from P_2 and P_3, respectively, for item A and B.

(2) HTP announces the highest bid for item A in the first auction round as 7 on the public bulletin board. Item B yields respective bids of 7, 7 and 9 from P_1, P_2 and P_3, with the highest bid of 9 being similarly published. (3) Bidders P_1, P_2 and P_3 each generate hash commitments for their bids on items A and B according to Step 10. For example, for item A with bid 7, bidder P_1 samples a random nonce s_1^A and computes which is recorded by HTP.

$$\mathrm{com}_1^A = \text{SHA-256}(\text{round\_id} \,\|\, A \,\|\, \mathrm{id}_1 \,\|\, 7 \,\|\, s_1^A), \tag{3}$$

Step 6: According to the auction rules, the starting prices for items A and B in the second round are set to 7.7 and 9.9, respectively, calculated as Starting Price$_{\text{A-next}} = (1 + 10\%) \times 7 = 7.7$. Subsequently, HTP and bidders P_1, P_2 and P_3 repeat Steps 1–5 of the protocol. During Step 5, the bid matrices derived from the quantum sequences returned by the bidders to HTP are all (0, 0, 0, 0), indicating no new highest bids for either item. Next, the highest bidders for items A and B disclose their random numbers and commitment values to HTP and other bidders. Other bidders validate the commitment values, and HTP verifies both the commitment values and identity encodings.

If all verifications pass and no complaints are raised, HTP officially declares the highest bids for items A and B are 7 and 9, respectively. The winning bidders are Group 2 Member 3 for item A and Group 3 Member 5 for item B. The auction concludes upon this announcement.

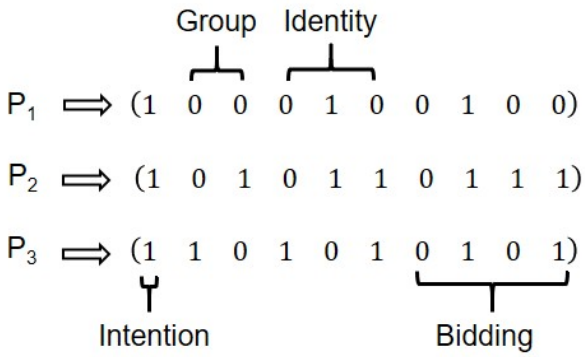

Figure 9. Recovered bid bits per item and round at HTP and highest-bid update.

5. Performance Analysis

We evaluate the proposed SQSAA protocol in terms of security, anonymity, verifiability, non-repudiation, and secrecy capacity.

5.1. External Attacks on Security

To obtain bidders' secrets, an eavesdropper Eve may attempt intercept–resend, measure–resend, or Trojan-horse attacks.

5.1.1. Intercept-Resend Attack

In Step 1 or Step 7, Eve may intercept the quantum sequence Seq_i or Seq_i'' transmitted from HTP to P_i, insert an equivalent number of single particles, and subsequently forward the altered quantum sequence to P_i. Through this method, P_i might encode the confidential information (identity codes or bidding information) onto these tampered particles. Eve then intercepts again the quantum sequence Seq_i' or Seq_i''' sent from P_i to HTP and obtains the identity codes or bidding information. It is noteworthy that the intercepted sequences Seq_i or Seq_i'' contain decoy particles, with the probability of Eve's fake particles matching the decoy particles being $\frac{1}{4}$. Without loss of generality, assuming the decoy particles prepared by HTP are in the $|0\rangle$ state, the detection probabilities for Eve's fake particles are presented in Table 4.

Therefore, if the decoy particle is in the $|+\rangle$ state and HTP measures in the Fourier basis, the probability of detecting Eve is

$$p = \frac{1}{4} \times 0 + \frac{1}{4} \times 1 + \frac{1}{4} \times \frac{1}{2} + \frac{1}{4} \times \frac{1}{2} = \frac{1}{2}. \tag{4}$$

Similarly, we can compute that the non-detection probabilities for $|-\rangle$, $|0\rangle$, and $|1\rangle$ are all $\frac{1}{2}$.

In summary, the probability that HTP detects Eve's attack is given by

$$P_1(w) = 1 - 2^{-w}, \tag{5}$$

where w represents the number of decoy particles (see Figure 10).

Table 4. Measurement results and probabilities of fake particles.

Fake Particles	Measurement Result	Probability
$\|+\rangle$	$\|+\rangle$	0
$\|-\rangle$	$\|-\rangle$	1
$\|0\rangle$	$\|+\rangle$ or $\|-\rangle$	1/2
$\|1\rangle$	$\|+\rangle$ or $\|-\rangle$	1/2

The table shows the measurement outcomes and corresponding probabilities for different types of fake particles.

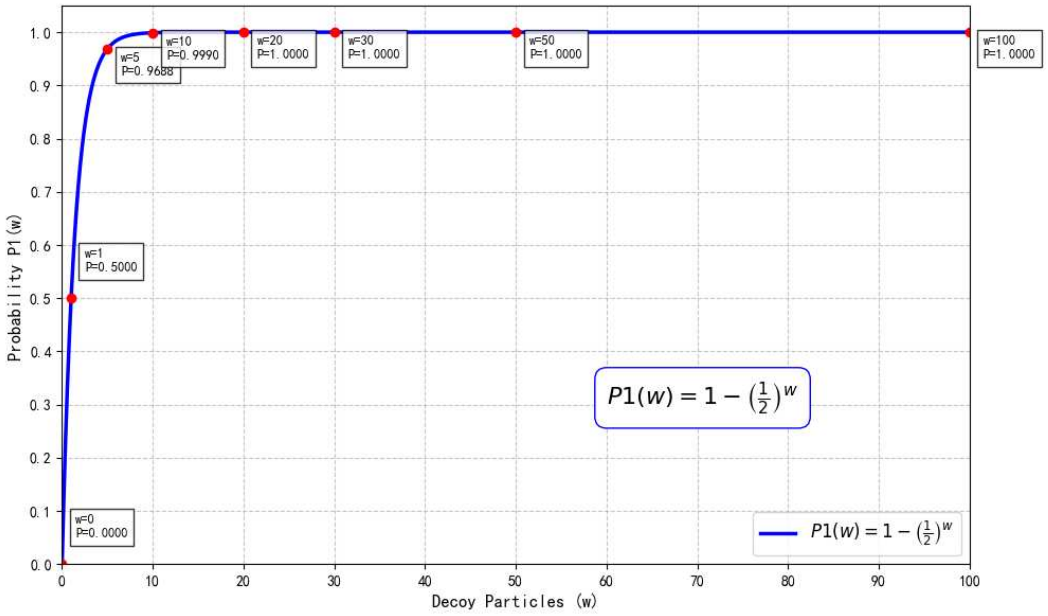

Figure 10. Detection probability $P_1(w) = 1 - 2^{-w}$ versus number of decoy particles w under intercept-resend.

Consequently, Eve's intercept-resend attack introduces an error rate in the eavesdropping detection phase that exceeds the threshold. Particularly when the number of decoy particles is sufficiently large, the probability of detecting the attack approaches 1, thereby effectively countering this attack.

5.1.2. Measure-Resend Attack

In Step 1 or Step 7, Eve intercepts and measures the quantum sequences Seq_i or Seq_i'' transmitted from HTP to P_i. Based on the measurement outcomes, she generates counterfeit quantum sequences Seq_i or Seq_i'' and transmits them to P_i. Through this approach, P_i may encode the secret information onto the tampered photons. Eve subsequently intercepts and measures the quantum sequences Seq_i' or Seq_i''' sent from P_i to HTP, thereby obtaining the secret information while simultaneously generating fake quantum sequences Seq_i' or Seq_i''' to forward to HTP.

However, Eve possesses no prior knowledge regarding either the positions or preparation bases of the decoy particles. For each decoy particle, Eve has a statistical probability of 50% to select the correct measurement basis. If Eve chooses the correct measurement basis, she can successfully pass the eavesdropping detection. Conversely, if an incorrect

basis is selected, Eve will be detected with a probability of $\frac{1}{2}$ statistically. Without loss of generality, assuming the decoy particles prepared by HTP are in the $|+\rangle$ state, the detection probabilities for Eve's modified particles are presented in Table 5.

Table 5. Probabilities of Eve's measurement choices and corresponding fake particles.

Eve's Choice	Eve's Measurement	Fake Particles	Probability
Fourier basis	$\|+\rangle$	$\|+\rangle$	0
Computational basis	$\|+\rangle$	$\|+\rangle$	0
Computational basis	$\|-\rangle$	$\|-\rangle$	1

"Eve's Choice" refers to the basis selected by Eve for measurement; "Fake Particles" are the particles Eve replaces after measurement.

Similarly, we can compute that the detection probabilities for $|-\rangle$, $|0\rangle$, and $|1\rangle$ are all $\frac{1}{4}$. Therefore, if the decoy particle is in the $|+\rangle$ state, the probability of detecting Eve is

$$p = \frac{1}{2} \times 1 \times 0 + \frac{1}{2} \times \frac{1}{2} \times 0 + \frac{1}{2} \times \frac{1}{2} \times 1 = \frac{1}{4}. \tag{6}$$

In summary, the probability that HTP detects Eve's attack is given by

$$P_2(w) = 1 - \left(\frac{3}{4}\right)^w, \tag{7}$$

where w represents the number of decoy particles (see Figure 11).

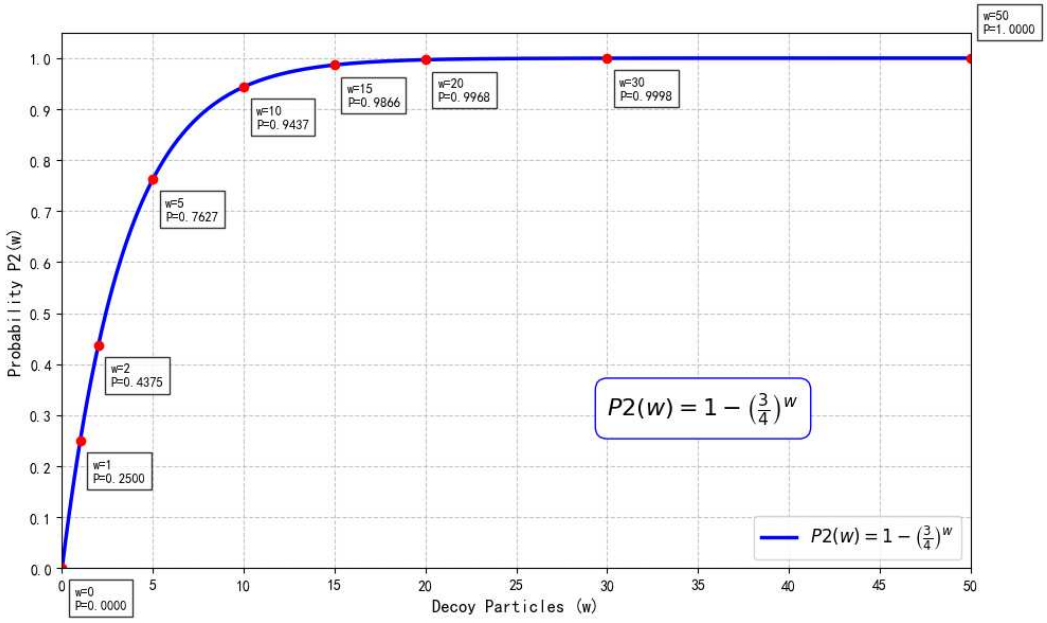

Figure 11. Detection probability $P_2(w) = 1 - (3/4)^w$ versus number of decoy particles w under measure-resend.

In practical implementations, the sequence length N is finite. Asymptotic security bounds do not strictly apply. Statistical fluctuations in the estimated error rate must be considered. Let n_{decoy} be the number of decoy bits. The probability that an attacker's induced error deviates from the expected value by a margin δ is bounded by Hoeffding's inequality. To guarantee a security failure probability ϵ_{sec}, the threshold η must be adjusted (lowered) as the sequence length decreases, ensuring that any malicious intervention is statistically distinguishable from channel noise with high confidence.

5.1.3. Trojan Horse Attack

Since the proposed protocol employs symmetric channels, it is vulnerable to Trojan horse attacks. A potential attacker, Eve, could exploit such attacks to intercept the private information of P_i. There are two primary types of Trojan horse attacks: delayed-photon attacks and invisible-photon attacks. To counter these attacks, each bidder P_i needs to be equipped with both a wavelength quantum filter and a photon-number discriminator. The wavelength filter provides protection against invisible-photon attacks, while the photon-number splitter offers defense against delayed-photon attacks. These two devices have been demonstrated to exhibit strong resistance against Trojan horse attacks. Consequently, our protocol can effectively thwart Trojan horse attacks through the implementation of these devices.

5.2. Internal Attacks on Security

We focus on investigating an extreme case where $n-1$ dishonest users collaborate to attack the remaining single honest user. Without loss of generality, assume P_1 is the honest bidder while $P_2, P_3, \ldots, P_n$ are dishonest bidders conspiring to attack P_1, with the objective of obtaining P_1's secret information.

In the SQSAA protocol, since each P_i and HTP communicate through star-shaped symmetric channels, the dishonest bidders would attempt to intercept particles transmitted between HTP and P_1 to acquire secret information. In this scenario, the dishonest bidders will be detected as external attackers. According to the protocol specifications, each bidder shares a private key with HTP, and the private key determines the positions of both decoy particles and rotation particles. Since dishonest bidders possess neither the private key shared between HTP and P_1 nor the information about quantum states prepared by HTP, any attack strategy they employ will inevitably cause quantum state disturbance and transmission errors and ultimately lead to an error rate exceeding the predetermined threshold. That is to say, our protocol can resist attacks from dishonest users.

5.3. Secrecy Capacity Analysis

Generally speaking, any secure communication protocol can be analyzed using the wiretap channel model, wherein the SQSAA protocol the quantum channel serving as the main channel transmits secret information while Eve's eavesdropping is modeled as the wiretap channel, whose specific model is illustrated in Figure 12.

The secrecy capacity, serving as a fundamental metric for evaluating protocol security in quantum communications, represents the maximum secure information transmission rate between legitimate communicating parties (HTP and P_i) in the presence of eavesdropper Eve, which constitutes a critical parameter in SQSAA protocol analysis [35] and is expressed as C_S according to Wyner's wiretap channel theory.

$$C_s = \max_p \{ I(P_i : \mathrm{HTP}) - I(P_i : E) \} \tag{8}$$

where I(X:Y) characterizes the mutual information between random variables X and Y. Since the particles prepared by HTP have equal probabilities of being in $|0\rangle, |1\rangle, |+\rangle, |-\rangle$ states, the system exhibits a completely mixed state $\rho = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)$. Under collective attack scenarios, Eve may perform joint operations on both the transmitted qubits and the ancillary qubits she prepares.

$$\rho^{(HE)} = U(\rho \otimes |\epsilon\rangle\langle\epsilon|)U^{\dagger} \tag{9}$$

where $|\epsilon\rangle$ denotes the state of Eve's prepared ancillary qubit, and U is a unitary operator acting on the joint space of the qubit and ancillary qubit. Eve transmits the qubit to bidder

P_i while retaining her ancillary qubit until P_i forwards the qubit to HTP. Upon reception, P_i applies the σ_Y operator with probability p or the σ_I operator with probability $(1-p)$ based on secret information, evolving the qubit state to

$$\rho^{\mathrm{PHE}} = p \cdot \rho_0^{HE} + (1-p) \cdot \rho_1^{HE} \tag{10}$$

where $\rho_0^{HE} = \sigma_y \rho^{HE} \sigma_y^{\dagger}$ and $\rho_1^{HE} = \sigma_I \rho^{HE} \sigma_I^{\dagger}$. To obtain the secret information, Eve performs coherent measurements on an arbitrary number of qubits and ancillary qubits to distinguish between the quantum states ρ_0^{HE} and ρ_1^{HE} encoded by bidder P_i, where based on the Holevo bound (whose distinguishing capability is bounded by the Holevo information quantity) we obtain

$$I(P_i : E) \leq \max\left\{S(\rho^{PHE}) - p \cdot S(\rho_0^{BE}) - (1-p) \cdot S(\rho_1^{BE})\right\} \tag{11}$$

where $S(\rho)$ denotes the von Neumann entropy. The von Neumann entropy of the original quantum state $\rho = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)$ is $S(\rho) = -(\sum_{i=1}^{2} \frac{1}{2} \log_2\left(\frac{1}{2}\right)) = 1$. Therefore, the maximum mutual information between bidder P_i and eavesdropper Eve is

$$\dot{I}(P_i : E) \leq \max\{S(\rho^{ABE})\} - 1 \leq h(\xi), \tag{12}$$

where $h(\xi)$ is the binary Shannon entropy of ξ.

$$\xi = \frac{1}{2}\left(1 - \sqrt{(1-2p)^2 + [1-2(\epsilon_X + \epsilon_Z)]^2[1-(1-2p)^2]}\right) \tag{13}$$

where ϵ_X and ϵ_Z are the detection bit error rate (DBER) in the X-basis and the Z-basis, respectively. Taking into account channel losses, when denoting the maximum accessible qubit rate for Eve as Q^{Eve}, the maximum mutual information between bidder P_i and Eve consequently becomes

$$I(P_i : E) \leq Q^{\mathrm{Eve}} \cdot h(\xi) \tag{14}$$

Similarly, we denote the reception rate at HTP as Q^{HTP} and calculate the mutual information between the bidder P_i and HTP.

$$I(P_i : HTP) = Q^{\mathrm{HTP}} \cdot [h(p + \epsilon - 2p\epsilon) - h(\epsilon)] \tag{15}$$

Thus, the secrecy capacity C_S becomes

$$\begin{aligned} C_S &= \max\left\{I(P_i : \mathrm{HTP}) - I(P_i : E)\right\} \\ &= \max\left\{Q^{\mathrm{HTP}}[h(p + \epsilon - 2p\epsilon) - h(\epsilon)] - Q^{\mathrm{Eve}} h(\xi)\right\} \\ &= Q^{\mathrm{HTP}} \cdot \max[h(p + \epsilon - 2p\epsilon) - h(\epsilon) - g \cdot h(\xi)] \\ &\geq Q^{\mathrm{HTP}} \cdot [1 - h(\epsilon) - g \cdot h(\epsilon_X + \epsilon_Z)] \end{aligned} \tag{16}$$

where g represents the discrepancy rate between Q^{Eve} and Q^{HTP}, which depends on both channel loss and detector efficiency, reaching its maximum value at $p = \frac{1}{2}$.

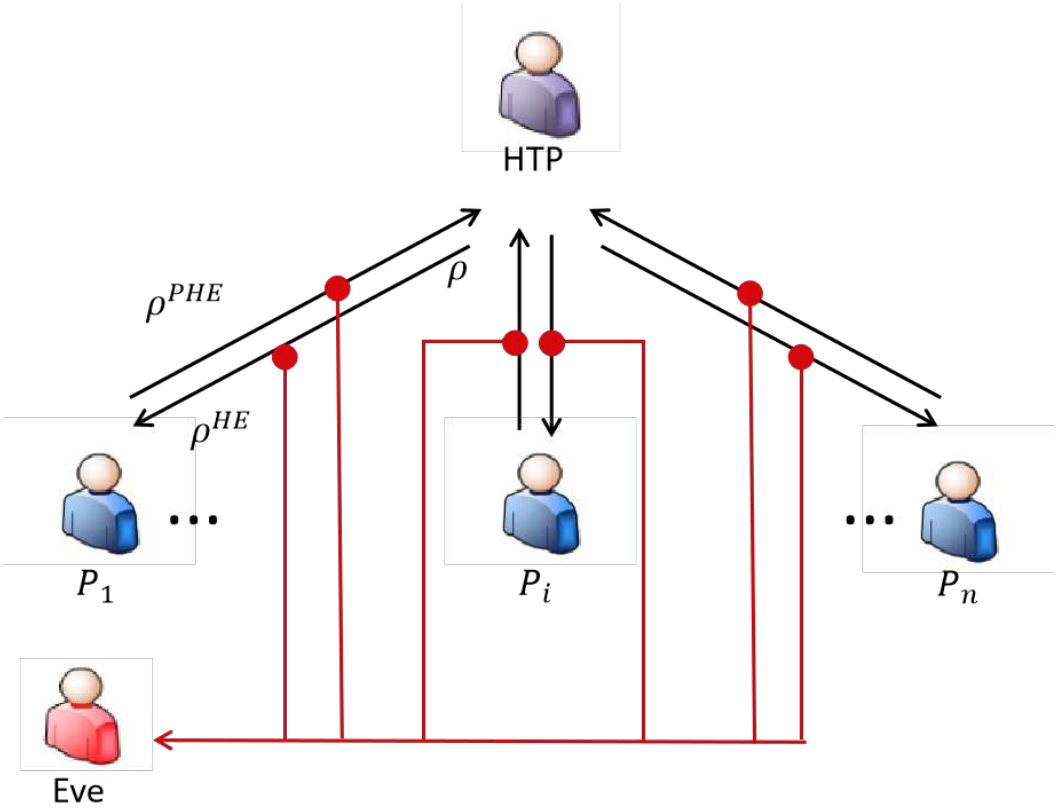

Figure 12. Wiretap channel model for secrecy capacity analysis in SQSAA.

5.4. Anonymity Analysis

According to the protocol, HTP transmits the quantum sequence Seq_i to each bidder P_i respectively, where the first particle of sequence Seq_j received by the j-th bidder P_j serves as the grouping particle. Since this particle is randomly prepared by HTP from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and the measurements of grouping particles among different bidders are mutually independent. Therefore, the mutual information between them can be quantitatively calculated as

$$\begin{aligned} I(P_j : P_l) &= S(P_j) + S(P_l) - S(P_j, P_l) \\ &= S(P_j) + S(P_l) - S(P_j) - S(P_l) \\ &= 0. \end{aligned} \tag{17}$$

where P_l denotes any dishonest bidder. Any collusion attempt by dishonest bidders to obtain P_j's identity encoding is bound to fail. Attackers can neither access other bidders' measurement results nor determine honest bidders' group affiliation through the first particle, thus failing to reconstruct complete identity encoding. Furthermore, the decoy states introduced by HTP in Seq_i ensure that any external eavesdropping will be detected due to induced errors during eavesdropping detection. Consequently, except for the trusted HTP, no bidder can obtain others' identity information, guaranteeing the protocol's anonymity.

The protocol guarantees that bidders cannot ascertain the identities or bids of other participants. However, it is important to note the Trusted HTP Assumption: The HTP knows the mapping between identity codes and real identities. Thus, the protocol provides anonymity against peers and outsiders, but not against the HTP.

5.5. Verifiability and Non-Repudiation Analysis

In Step 10 of the protocol, each bidder computes and submits the hash value of their bid to HTP, establishing a binding commitment since the original bid cannot be deduced without the random nonce. The protocol's security guarantees non-repudiation, as any bid modification would require finding a new nonce matching the original hash value—a computationally infeasible task even for quantum computers due to the collision-resistant hash function.

Distinction from Channel Disruption: It is crucial to distinguish between *channel disruption* and *repudiation*. High QBER (Step 3) indicates an active attack or denial-of-service, leading to a protocol abort. In contrast, Non-Repudiation (Step 13) prevents a legitimate bidder—who has successfully transmitted a valid bid without triggering high QBER—from later denying their submission.

The verification phase (Step 13) requires the highest bidder to reveal their nonce and hash value for public verification, where successful verification leads to HTP disclosing the winner's identity number and bid amount, while failed verification triggers a complaint mechanism that either initiates a new auction round for validated complaints or maintains the current highest bid for rejected complaints. This commitment verification framework satisfies the protocol's verifiability requirement while maintaining quantum-resistant security throughout the auction process.

6. Conclusions

We presented a multi-party semi-quantum simultaneous ascending auction protocol based on single-particle states. HTP generates, distributes, and verifies quantum states; bidders determine groups via measurements and encode private identity vectors, obtaining identity codes after HTP authentication. During bidding, HTP dynamically updates sequences, and bidders submit prices for multiple items using only simple unitary operations. HTP announces current highest bids in real time and iteratively regenerates sequences until no higher bids appear, thereby realizing simultaneous multi-item ascending auctions.

The protocol serves as a quantum-secured signaling layer, providing information-theoretic security for bid transmission and identity verification over a classical auction mechanism. The protocol offers several practical advantages over prior art. First, it accommodates heterogeneous participants by requiring only semi-quantum capabilities on the bidder side (Z/X measurements, reflections, and elementary single-qubit operations), and it relies solely on single-particle resources, substantially lowering implementation cost. Second, it scales naturally to multi-item settings: identity is encoded in the first $(2+n)$ particles, while each item uses $\lceil \log_2 d_w \rceil$ particles for prices, enabling parallel, round-by-round price discovery. Third, the use of per-round hash commitments provides a simple, auditable path for public verification, supporting non-repudiation and complaint resolution without revealing secret randomness until the end.

From a deployment perspective, the protocol parameters are straightforward to tune. The decoy rate and QBER threshold η control eavesdropping detectability and robustness; the per-item bit width $\lceil \log_2 d_w \rceil$ balances price granularity and sequence length; and the basic operation set (I, H, σ_Y, Z/X measurements) matches today's photonic toolchains. Computational and storage complexity at bidders is minimal, and HTP's classical processing (matrix checks and bit-to-decimal conversion) scales linearly in the number of bidders and items per round.

Finally, we must emphasize that theoretical validity does not automatically translate to immediate real-world applicability. Bridging the gap between our theoretical model and a fully operational real-world deployment remains a significant future challenge. This

requires rigorous validation under realistic physical conditions, deep integration with existing technological infrastructures, and further study on practical device imperfections.

There remain limitations and opportunities for future work. The current model assumes a trusted HTP; relaxing this with distributed trust (e.g., threshold HTP, verifiable computation, or lightweight MPC among multiple centers) is an important direction. A finite-size and composable security analysis under realistic device imperfections and channel loss would strengthen the guarantees. On the systems side, building a prototype with time-bin or polarization-encoded photonics, integrating authenticated classical channels, and benchmarking end-to-end latency would support practical adoption. Finally, extending to richer auction formats (e.g., combinatorial or budget-constrained bidding), adaptive increment rules, and privacy-enhanced analytics while preserving semi-quantum feasibility are promising avenues.

Author Contributions: Methodology, X.W.; software, X.W.; formal analysis, X.W.; writing—original draft preparation, X.W.; validation, B.W. and Y.Y.; supervision, Y.H.; writing—review and editing, Y.Z. and Y.H. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the National Natural Science Foundation of China (Grant No. 62201252) and the Fundamental Research Funds for the Central Universities (NO. NS2025030). We also acknowledge the support from the Jiangsu Province Engineering Research Center of IntelliSense Technology and System.

Institutional Review Board Statement: Not applicable.

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Zhang, W.; van Leent, T.; Redeker, K.; Garthoff, R.; Schwonnek, R.; Fertig, F.; Eppelt, S.; Rosenfeld, W.; Scarani, V.; Lim, C.C.W.; et al. A device-independent quantum key distribution system for distant users. *Nature* **2022**, *607*, 687–691. [CrossRef]
2. Zahidy, M.; Ribezzo, D.; De Lazzari, C.; Vagniluca, I.; Biagi, N.; Müller, R.; Occhipinti, T.; Oxenløwe, L.K.; Galili, M.; Hayashi, T.; et al. Practical high-dimensional quantum key distribution protocol over deployed multicore fiber. *Nat. Commun.* **2024**, *15*, 1651. [CrossRef]
3. Sheng, Y.B.; Zhou, L.; Long, G.L. One-step quantum secure direct communication. *Sci. Bull.* **2022**, *67*, 367–374. [CrossRef]
4. Sun, X.F.; Fan, L.; Cao, C.; Yu, W.S. Measurement-device-independent quantum secure multiparty summation based on entanglement swapping. *Laser Phys. Lett.* **2023**, *20*, 125201. [CrossRef]
5. Li, C.; Ye, C.; Tian, Y.; Chen, X.B.; Li, J. Cluster-state-based quantum secret sharing for users with different abilities. *Quantum Inf. Process.* **2021**, *20*, 385. [CrossRef]
6. Ma, R.H.; Gao, F.; Cai, B.B.; Lin, S. Quantum Secret Reconstruction. *Adv. Quantum Technol.* **2024**, *7*, 2300273. [CrossRef]
7. Wang, Q.; Yu, C.; Gao, F.; Qi, H.; Wen, Q. Self-tallying quantum anonymous voting. *Phys. Rev. A* **2016**, *94*, 022333. [CrossRef]
8. Borjigin, W.; Ota, K.; Dong, M. In broker we trust: A double-auction approach for resource allocation in NFV markets. *IEEE Trans. Netw. Serv. Manag.* **2018**, *15*, 1322–1333. [CrossRef]
9. Bag, S.; Hao, F.; Shahandashti, S.F.; Ray, I.G. SEAL: Sealed-bid auction without auctioneers. *IEEE Trans. Inf. Forensics Secur.* **2019**, *15*, 2042–2052. [CrossRef]
10. Borjigin, W.; Ota, K.; Dong, M. Multiple-Walrasian auction mechanism for tree valuation service in NFV market. *IEEE Trans. Comput. Soc. Syst.* **2022**, *10*, 61–71. [CrossRef]
11. Ye, C.Q.; Li, J.; Chen, X.B.; Dong, M.; Ota, K. Measurement-based quantum sealed-bid auction. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2023**, *70*, 5352–5365. [CrossRef]
12. Dowling, J.P.; Milburn, G.J. Quantum technology: The second quantum revolution. *Philos. Trans. R. Soc. Lond. Ser. A Math. Phys. Eng. Sci.* **2003**, *361*, 1655–1674. [CrossRef] [PubMed]
13. Nielsen, M.A.; Chuang, I.L. *Quantum Computation and Quantum Information*; Cambridge University Press: Cambridge, UK, 2010.
14. Shor, P.W. Algorithms for quantum computation: Discrete logarithms and factoring. In Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA, 20–22 November 1994; pp. 124–134.

15. Grover, L.K. A fast quantum mechanical algorithm for database search. In Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, Philadelphia, PA, USA, 22–24 May 1996; pp. 212–219.
16. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.* **2014**, *560*, 7–11. [CrossRef]
17. Piotrowski, E.W.; Sładkowski, J. Quantum auctions: Facts and myths. *Phys. A Stat. Mech. Its Appl.* **2008**, *387*, 3949–3953. [CrossRef]
18. Naseri, M. Secure quantum sealed-bid auction. *Opt. Commun.* **2009**, *282*, 1939–1943. [CrossRef]
19. Qin, S.J.; Gao, F.; Wen, Q.Y.; Meng, L.M.; Zhu, F.C. Cryptanalysis and improvement of a secure quantum sealed-bid auction. *Opt. Commun.* **2009**, *282*, 4014–4016. [CrossRef]
20. Yang, Y.G.; Naseri, M.; Wen, Q.Y. Improved secure quantum sealed-bid auction. *Opt. Commun.* **2009**, *282*, 4167–4170. [CrossRef]
21. Zhao, Z.; Naseri, M.; Zheng, Y. Secure quantum sealed-bid auction with post-confirmation. *Opt. Commun.* **2010**, *283*, 3194–3197. [CrossRef]
22. Liu, W.J.; Wang, F.; Ji, S.; Qu, Z.G.; Wang, X.J. Attacks and improvement of quantum sealed-bid auction with EPR pairs. *Commun. Theor. Phys.* **2014**, *61*, 686. [CrossRef]
23. Liu, W.J.; Wang, H.B.; Yuan, G.L.; Xu, Y.; Chen, Z.Y.; An, X.X.; Ji, F.G.; Gnitou, G.T. Multiparty quantum sealed-bid auction using single photons as message carrier. *Quantum Inf. Process.* **2016**, *15*, 869–879. [CrossRef]
24. Zhang, R.; Shi, R.H.; Qin, J.Q.; Peng, Z.W. An economic and feasible Quantum Sealed-bid Auction protocol. *Quantum Inf. Process.* **2018**, *17*, 35. [CrossRef]
25. Shi, R.H. Quantum sealed-bid auction without a trusted third party. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2021**, *68*, 4221–4231. [CrossRef]
26. Shi, R.H. Anonymous quantum sealed-bid auction. *IEEE Trans. Circuits Syst. II Express Briefs* **2021**, *69*, 414–418. [CrossRef]
27. Shi, R.H.; Li, Y.F. A feasible quantum sealed-bid auction scheme without an auctioneer. *IEEE Trans. Quantum Eng.* **2022**, *3*, 2100212. [CrossRef]
28. Zhang, C.; Huang, Q.; Long, Y.; Sun, Z. Secure three-party semi-quantum summation using single photons. *Int. J. Theor. Phys.* **2021**, *60*, 3478–3487. [CrossRef]
29. Yang, C.W.; Tsai, C.W.; Chen, C.A.; Lin, J. Robust Semi-Quantum Summation over a Collective-Dephasing Noise Channel. *Mathematics* **2023**, *11*, 1405. [CrossRef]
30. Ye, C.Q.; Li, J.; Chen, X.B.; Dong, M.; Ota, K.; Khalique, A.; Durad, M.H. Semi-Quantum Secure Multiparty Summation and its Applications to Anonymous Auction and Ranking. *Adv. Quantum Technol.* **2024**, *7*, 2300347. [CrossRef]
31. Tian, Y.; Zhang, N.; Ye, C.; Bian, G.; Li, J. Different secure semi-quantum summation models without measurement. *EPJ Quantum Technol.* **2024**, *11*, 35. [CrossRef]
32. Ye, T.Y.; Xu, T.J.; Geng, M.J.; Chen, Y. Two-party secure semiquantum summation against the collective-dephasing noise. *Quantum Inf. Process.* **2022**, *21*, 118. [CrossRef]
33. Hu, J.L.; Ye, T.Y. Three-party secure semiquantum summation without entanglement among quantum user and classical users. *Int. J. Theor. Phys.* **2022**, *61*, 170. [CrossRef]
34. Milgrom, P. Putting auction theory to work: The simultaneous ascending auction. *J. Political Econ.* **2000**, *108*, 245–272. [CrossRef]
35. Li, G.D.; Liu, J.C.; Wang, Q.L.; Sun, W.Q. Employing single photons for measurement-device-independent quantum secure direct communication with identity authentication. *IEEE Commun. Lett.* **2024**, *28*, 473–477. [CrossRef]