Hindawi
Security and Communication Networks
Volume 2021, Article ID 1360560, 10 pages
https://doi.org/10.1155/2021/1360560

Research Article

Combinatorial Spectrum E-Auction for 5G Heterogeneous Networks: A Zether-Based Approach

Zijun Zhao,[1] **Zuobin Ying**,[2,3] **Zhiming Cai**,[3] **and Jianfeng Ma**[1]

[1]*School of Physical & Information Technology, Anhui University, Hefei 230601, China*
[2]*School of Computer Science & Technology, Anhui University, Hefei 230601, China*
[3]*Faculty of Data Science, City University of Macau, Taipa 999078, Macau*

Correspondence should be addressed to Zhiming Cai; caizhiming@cityu.mo

Received 10 September 2021; Revised 14 October 2021; Accepted 23 October 2021; Published 16 November 2021

Academic Editor: Ke Gu

5G heterogeneous network (HetNet) is a novel network topology that integrates various kinds of wireless access technologies such as 4G Long-Term Evolution (LTE), Wi-Fi, and so on. Despite greatly improving spectrum efficiency, it poses enormous challenges to spectrum e-auction. Firstly, due to high mobility, bidders may be interested in different spectrums in terms of time or geolocation. Secondly, one's bidding value should be protected against rival bidders or adversaries to avoid vicious competition as well as privacy leakage. Thirdly, the ubiquitous HetNet requires a trustworthy distributed auction framework rather than a centralized auctioneer-based pattern. Aiming at overcoming these obstacles above, we proposed a blockchain-based combinatorial spectrum e-auction framework. Different from other blockchain-based solutions of using SGX to realize trust processing in the auction phase, we adopt Zether, a privacy-preserving smart contract, as the main building block. Besides, the bidding value is preserved from the beginning to the end, even though the time-consuming Paillier homomorphic encryption and garbled circuits are absent. We provide the auction security by leveraging Σ-Bullets, a zero-knowledge proof mechanism. Theoretical analysis and extensive evaluation also indicate that our approach is better than the state-of-the-art works in terms of efficiency and effectiveness.

1. Introduction

The fifth-generation (5G) mobile network is expected to promote the connection of everything that demands a low-latency Internet connection, from IoT devices and appliances to self-driving cars, paving the way for an environment where every device is smart and connected. According to the forecast released from Cisco, the overall mobile data traffic is expected to grow to 77 exabytes per month by 2022, a sevenfold increase over 2017 [1]. As a result, the existing wireless network capacity has been unable to support the explosive growth of data traffic and the ubiquitous demand for high-quality communication. New wireless and network technologies are demanded to solve the contradiction between the limited wireless bandwidth resources of the existing network and a large number of high-speed transmission requirements. Heterogeneous network (HetNet), emerging as a novel network topology which integrates various kinds of wireless access technologies (*e.g.,* 5G, 4G Long-Term Evolution (LTE), Wi-Fi, Universal Mobile Telecommunications System (UMTS), and so on), is deemed to be the most promising solution against the above challenges. However, the scarce spectrum resource has become an obstacle in HetNet deployment. Considering the wide coverage of 5G services, 3rd Generation Partnership Project (3GPP) introduces the idea of unlicensed 5G in Release 16, which is expected to solve the problem of 5G spectrum scarcity [2]. Nevertheless, a field test released by Aviat Networks points out that the use of unlicensed equipment in the 6 GHz frequency band will affect the microwave point-to-point links operating on this frequency band and cause interference to existing users [3]. Obviously, the lack of coordination between these unlicensed frequency band applications will directly lead to interference between

different services and lead to a series of other unfavorable consequences due to no spectrum coordination. Therefore, the effective allocation of the 5G spectrum has become a key factor that affects the availability of HetNet.

Spectrum e-auction, which is considered to be one of the most effective ways of solving the spectrum allocation problem, has been widely researched in the past few years [4–7]. Recently, on account of the rise of the smart contract, some blockchain-based frameworks have also been constructed [8–11]. There are three main entities participant in the spectrum e-auction process, namely, seller(s), auctioneers, and buyer(s). The most common workflow of a spectrum e-auction is as follows. (1) Seller (maybe more than one seller, *e.g.,* double auction) releases the spectrum resources to the auctioneers. (2) Buyers (maybe only one buyer, *e.g.,* reverse auction) submit their bid values as well as other information (*e.g.,* location and account address) to the auctioneer. (3) Auctioneer judges the winner according to the bid value and then returns the result to both the seller and the bidders. (4) Auctioneer refunds the bids to those buyers who have not won in the auction. Seller and winner buyers finish the deal. This workflow could be implemented to most of the spectrum auction schemes. However, the actual application scenarios of HetNet put forward some specific requirements for spectrum auctions. We summarize the most challenging issues as follows:

(i) In HetNet, the buyer may be interested in more than one spectrum. Besides, buyer (*e.g.,* the autonomous vehicle) may not be fixed in one location but occupies the spectrum resources in a certain location within a certain period of time. That is to say, the buyer might be interested in a bundle of the spectrum related to both geolocation and time. Thus, the corresponding combinatorial auction mode has to be considered.

(ii) The buyer's bidding value should be protected against the other rival bidders or adversaries. Existing spectrum auction schemes rely either on some expensive cryptographic tools (*e.g.,* garbled circuits (GC) and homomorphic encryption) or on the implementation of trusted processors (*e.g.,* Intel SGX). These approaches would not only increase time consumption but also have to make more hypothesis.

(iii) Most of the existing sealed-bid e-auction schemes require a trusted third-party auctioneer to ensure the fairness of bidding. Alternatively, assuming that the auctioneer is semihonest, then an additional semihonest auction agent is also needed under the restriction that it would not collude with the auctioneer. A fully decentralized spectrum auction scheme without trusted third party has not been effectively constructed.

Motivated by solving the aforementioned issues simultaneously, we proposed a combinatorial spectrum e-auction for 5G HetNet by leveraging the latest privacy-preserving smart contract theory named Zether [12]. Our ultimate goal is to design a combinatorial e-auction scheme which considers both bidding value privacy and practicality. Hereby, we summarize our contributions:

(i) As far as we know, we are the unique to construct a combinatorial e-auction scheme based on Zether. We not only give the concrete construction but also design the auction procedure on the Zether smart contract. It is worth noting that our scheme could be easily extended to other account-based blockchain platforms (*e.g.*, Hyperledger Fabric, EOS, and so on).

(ii) The bidding value of the buyer is protected without introducing the expensive cryptographic tools or trusted processors. We take advantage of the additive homomorphic feature of ElGamal encryption, thereby reducing the complexity of the entire scheme. Technically speaking, this is the first blockchain-based e-auction without a trusted third party.

(iii) To ensure the correctness of the encrypted transactions, the zero-knowledge proof (ZK proof) has to be included in the smart contract, which is also the expensive part in most of the blockchain-based auction schemes. The experimental results indicate that our proposed scheme is superior than state-of-the-art works in terms of time and gas consumption.

2. Related Work

The rapid development of 5G communication as well as the new architecture of HetNet facilitates the speed and diversity of accessing the Internet. Nonetheless, the high density of network infrastructure and the mobile nodes aggravate the scarceness of the spectrum. Spectrum e-auction looks prophetic against this dilemma. Since the auction procedure can be regarded as a multi-player game among different bidders, the bid value needs to be protected to avoid malicious competitions or collude attacks. Miao Pan et al. proposed a secure spectrum auction scheme to prevent the frauds of the insincere auctioneers between the auctioneer and the bidders by utilizing the Paillier cryptosystem, namely, *THEMIS* [4]. Wang et al. extended the security concerns to geolocation and time dynamics other than bid value only by introducing *PROST* [5]. However, to achieve the design goals, *PROST* uses a series of expensive cryptographic tools such as Paillier homomorphic encryption, oblivious transfer, and garbled circuits to construct the atomic blocks for the secure auction protocol. Afterwards, *ARMOR* [6] and *PS-TAHES* [7] are proposed to tackle the security issues in the heterogeneous spectrum, respectively. Both of these works leverage Paillier homomorphic encryption and garbled circuits along with some other cryptographic tools, and the difference is that *ARMOR* concentrates on combinatorial auction, while *PS-TAHES* focuses on double auction. Cheng et al. put forward another lightweight auction framework without using Paillier algorithm, namely, *SLISA* [13]. A set of subprotocols is designed by integrating additive secret sharing and garbled

circuits. *SLISA* provides strong security guarantees related to the bidders in the double auction.

In the past few years, blockchain technology has attracted tremendous attention. As a distributed ledger with the inherent temper-resistant feature, the new paradigm of "blockchain + x (*i.e.,* everything)" reaches a consensus that it could revolutionize every aspect of our lives. The subsequent deployment of smart contract in blockchain 2.0 (i.*e.,* Ethereum) makes it more practical for financial applications. Weiss et al. proposed an idea of spectrum management via adopting blockchain. They widely examined the blockchain application in spectrum sharing and, in the meantime, specified that a number of areas would benefit from further research [15]. Thereafter, considering the spectrum shortage dilemma, Zhou et al. put forward a blockchain-based secure spectrum sharing scheme for 5G HetNet, in which the underutilized spectrum allocated to the human-to-human (H2H) users could be shared with the machine-to-machine (M2M) communications. However, security claimed in this work is just the security guaranteed by the blockchain itself. Auction between the primary user and secondary user via the smart contract is totally transparent to everyone [10]. Wu et al. first considered the collusion coalitions among selfish auction participants and constructed a decentralized collusion-resistant e-auction system on Ethereum, named *CREAM* [8]. However, since the transactions on Ethereum are public, to protect bid privacy, *CREAM* designs a two-phase bidding process, *commitBid* and *revealBid*. After bid commitment, all bidders still have to trigger the *revealBid* to launch the auction algorithm. That is to say, rival bidders could still observe the true bid of a bidder. To eliminate the hypothetical trusted auctioneer (in some studies, if the auctioneer is semitrusted, then a semitrusted auction agent would be introduced in the premises that they would not collude with each other), some Software Guard Extension (SGX) approaches were proposed [9]. Recently, Chen et al. proposed *SAFE*, a general secure e-auction framework with privacy preservation [11]. It should be noted that this framework considered all the single-round (single-round auction stands for the bidders that can only submit their bids once) auction formats. Despite the fact that *SAFE* also leverages a bundle of cryptographic tools as well as the SGX, it is certainly one of the best spectrum e-auction approaches in state-of-the-art works. Moving one step forward, in this paper, we build a combinatorial spectrum e-auction scheme with privacy preserving based on Zether. We abandon the use of Paillier homomorphic encryption, garbled circuits, and SGX. Besides, we also reduce the gas consumption in the market cleanup phase. Finally, for ease of reading, we put the feature comparison in Table 1.

3. Preliminaries

3.1. Auction Terminologies. Here we present some auction terminologies used in our schemes.

(i) *Sealed-Bid Auction*. A sealed-bid auction is an auction process in which all bidders submit sealed bids to the auctioneer at the same time so that no bidder knows the bids of other auction participants. The sealed bid will not be opened before the specified date. The person with the highest bid is usually declared the winner of the bidding process.

(ii) *Vickrey Auction*. Vickrey auction is also known as the *second-price sealed-bid auction.* All bids are sealed and sent to an auctioneer who can open all the bids. The highest bidder wins but only needs to pay the second-highest bid. It is highly centralized and does not protect the privacy of the bids [16]. If the bidder is interested in multiple items, Vickrey auction can be generalized to Vickrey–Clarke–Groves (VCG) auction.

(iii) *Combinatorial Auction*. A combinatorial auction is a type of smart market in which participants can place bids on combinations of discrete heterogeneous items, rather than individual items or continuous quantities [17].

3.2. Zether and Zether Smart Contract (ZSC) [12]. Zether is a completely decentralized and confidential payment mechanism, compatible with Ethereum and other smart contract (SC) platforms. The fundamental of Zether is to realize transaction privacy via the smart contract, that is, hide the transaction amount and the balance of the account. For this purpose, mechanisms such as ElGamal encryption, pending transfer, and rolling over are designed. The payment mechanism is similar to Ethereum, which contains setup, user algorithms, and a smart contract. User algorithms, which contain seven subroutines, specify how users interact with Zether Smart Contract (ZSC). CreateAddress and CreateBurnTx check the input public keys to make sure that each pending transfer is rolled over. CreateBurnTx utilizes ReadBalance to recover the ZTH (ZTH is the confidential token of the Zether; the value of ZTH is related to the corresponding platform; for example, if the platform is Ethereum, then 1 ZTH = 1 ETH) from the account. CreateFundTx is utilized to deposit amounts to an account and CreateTransferTX is utilized to transfer money between one account and another. If the user wants to lock her account to an Ethereum address, she can use CreateLockTx. Otherwise, she can choose CreateUnlockTx to unlock an account.

ZSC has five methods: Fund, Burn, Transfer, Lock, and Unlock. Before executing the user algorithms, these functions would initiate the checkup process, such as checking the nonce or verifying a proof. If any of the checks does not succeed, the method outputs 0. Besides, ZSC also introduces a time horizon named *epoch*. The epoch length is denoted as E, and $E \geq 1$. A block's epoch number at height h is described as $[h/E]$. In order to ensure the correctness, ZSC stipulates that a transaction should be processed in the same *epoch* as it is generated.

3.3. ElGamal Encryption. ElGamal encryption is a type of public key encryption which is proved to be secure under decisional Diffie–Hellman (DDH) assumption [18]. It has been acknowledged that ElGamal is homomorphic to multiplication, whereas Zether leverages the additive

Table 1: Features in different schemes: a comparative summary.

Schemes	Auction type	Cryptographic tools	Auction platform	Privacy	Scalability
THEMIS [4]	VCG	Paillier	Auctioneer	✓	×
PROST [5]	Double	Paillier + OT + GC	Auctioneer + agent	✓	×
ARMOR [6]	Combinatorial	Paillier + OPE + GC	Auctioneer + agent	✓	×
PS-TAHES [7]	Double	Paillier + OT + GC	Auctioneer + agent	✓	×
SLISA [13]	Double	Secret sharing + GC	Auctioneer + agent	✓	×
CREAM [8]	Single	N/A	Ethereum smart contract	×	×
Wang et al. [9]	Single	Paillier + SGX + PC	Ethereum smart contract	✓	×
SAFE [11]	Single	SGX + ZKCP	Ethereum smart contract	✓	×
Ours	Combinatorial	ElGamal + Σ-Bullets	Account-based BC + ZSC	✓	✓

Here, "OT" stands for oblivious transfer. "OPE" is order-preserving encryption. "PC" means Pedersen commitment, and the "ZKCP" represents zero-knowledge contingent payment [14]. Account-based BC can be any blockchain platform operating under the account model, such as Ethereum, Fabric, and so on.

homomorphic feature of ElGamal, so it can be used to hide the balance in exponent.

Let b and b' be two amounts that need to be protected and y be the public key. The ciphertexts can be computed as

$$\begin{aligned} C_L &= g^b y^r, C_R = g^r; \\ C'_L &= g^{b'} y^{r'}, C'_R = g^{r'}. \end{aligned} \tag{1}$$

Then, the encryption of $b + b'$ under y can be calculated as

$$C_L C'_L = g^{b+b'} y^{r+r'}; C_R C'_R = g^{r+r'}. \tag{2}$$

3.4. Σ-Bullet Zero-Knowledge Proof [12]. To ensure the encrypted transactions are correct, Zether provides with a novel ZK proof, namely, Σ-Bullets. Σ-Bullets combine Bulletproofs and Σ-protocols to make algebraically encoded form as $\exists x$: $g^x = y \wedge h^x = u \in \mathbb{G}$.

A ZK proof for the statement st: $\{(p, q, t, \ldots; l, m, n, \ldots)$: $f(p, q, t, \ldots; l, m, n, \ldots)\}$ means that the prover shows knowledge of $l, m, n, \ldots$ s.t. $f(p, q, t, \ldots; l, m, n, \ldots)$ is true, where $p, q, t, \ldots$ are public variables.

4. Zether-Based E-Auction Scheme

4.1. System Overview. Figure 1 illustrates a combinatorial spectrum auction via Zether in 5G HetNet scenario. We briefly introduce the workflow of our proposed scheme. In 5G HetNet, a buyer may be interested in more than one spectrum resource. Moreover, different buyers may be interested in a same spectrum resource simultaneously. This is because same spectrum frequency band can be reused in accordance with different geolocations. Therefore, a conflict graph over combinatorial spectrum sets should be constructed firstly. Afterwards, buyers could seal the bids according to their interests in the spectrum combinations. The bids would be locked into the ZSC. ZSC initiates spectrum auction and announces the winner. It should be noted that there may be multiple winners when they have no conflict of interest. At last, winners will be assigned the corresponding spectrum resources and the rest of the bids will be returned to the accounts, respectively. In addition, we also give some important notations in this paper, as shown in Table 2.

4.2. Detailed Construction. In this paper, we propose a combinatorial spectrum auction in 5G HetNet scenario based on Zether. As shown in Figure 2, it is mainly composed of five parts. The first is the global setting algorithm, which can create the global parameters when it runs once and deploy the ZSC. The next part is the registration of users participating in the auction. The users register a Zether account and deposit a certain amount. The third part is to execute a specific auction, lock the account to the "Secure Auction Execution (called AUC)" smart contract provided in SAFE [11], and then execute the specific auction process in the fourth part, that is, to transfer the control of the Zether account to AUC. The last part is the settlement of the funds and auction items after the auction ends. AUC is complementary to the price difference between the auction winners based on the final auction price. Through transfer, AUC simply burns the entire amount and keeps a part of it (the winner's payment) and refunds the balance of the remaining bidders.

4.3. Setup. The setup algorithm refers to Setup_1 and Setup_2 subalgorithms. These two subalgorithms are the setting algorithms of the proof mechanism and the signature scheme, respectively. The setting of the proof mechanism may depend on the relationship of the construction of the proof, which means that its correctness would be publicly verified. During the specific implementation, Bulletproofs [19] and Schnorr signatures [20] are utilized, both of which have untrusted settings.

The formal description of the setup algorithm is shown in Figure 3. In addition to deploy the proof and signature mechanism, it also initializes the account table f(acc) as well as the pending transfer list p(Transfers). The last transfer period table lastRollOver is to record recent account updates, the lock table is to record the address when the account is locked, the counter table ctr is to prevent replay attacks, and the variable btotal is to record the total funds of ZTH contracts controlled by the account. Besides, the setup designs an epoch length E and a maximum funds MAX.

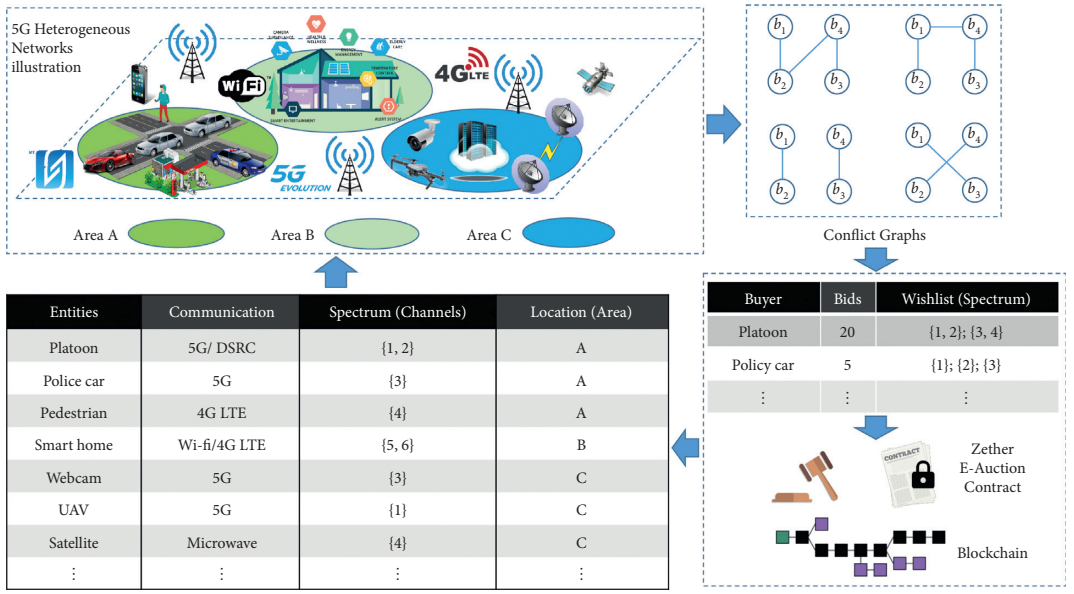

Figure 1: System overview.

Table 2: Key notations.

Notations	Descriptions
GroupGen	A polynomial-time algorithm where input 1^{λ} outputs $(p, g, \mathbb{G})$
p	$p = \Theta(\lambda)$, p is prime
g	A generator of $\mathbb{G}$
$\mathbb{G}$	A group of order p
$\mathbb{Z}_p$	Integers modulo p
y	Public key
σ_{lock}	Signature
acc	Account tables
pTransfers	Pending transfers table
E	An epoch length
Max	A maximum amount value
(ω, p)	Successful auction combination
$(C_{L,i}, C_{R,i})$	Encrypted amounts linked to key y_i

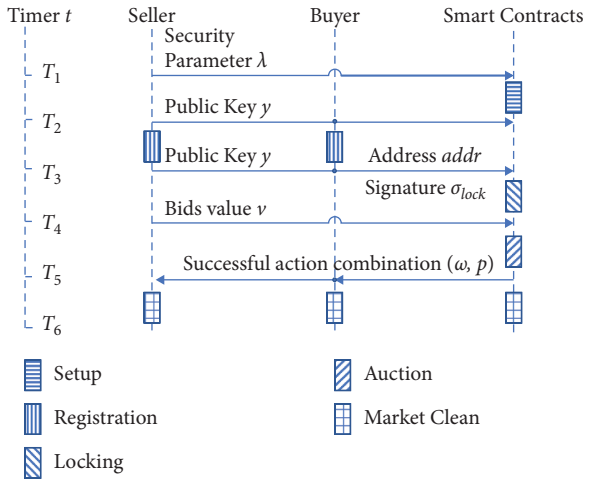

Figure 2: Workflow of e-auction via ZSC.

Input: λ(in unary).
Output: 0 or 1.
1: If $T1 < T < T_2$, go to step 2 , otherwise stop.
2: $(p,g, G) \leftarrow$ GroupGen (1^{λ}).
3: $pp_{nizk} \leftarrow Setup_1\ (1^{\lambda})$.
4: $pp_{sig} \leftarrow Setup_2\ (1^{\lambda})$.
5: Initialize:
· acc: $G \rightarrow G^2$
· pTransfers: $G \rightarrow G^2$
· lastRollOver: $G \rightarrow Z$
· lock: $G \rightarrow \{0,1\}^*$
· ctr: $G \rightarrow Z$
· total amounts $b_{total} \in Z$ to 0
6: Deploy ZSC, where (p,g, G), pp_{nizk}, pp_{sig} , acc, pTransfers, lastRollOver, lock,b_{total}, MAX, E.

Figure 3: Setup.

4.4. Registration. Anyone can fund the account by straightforward specifying the public key y as well as depositing certain ETH. The transfer algorithm is introduced in Figure 4. Transfer transfers ZTH from one account to another, and π_{transfer} ensures that the ciphertext is in the correct form and the transferor has enough money. In addition, there is a signature to avoid replay attacks. As shown in Figure 5, Fund converts ETH to ZTH. ETH is stored in SC, and ZTH is also added to the (pending) balance of y. If the account does not already exist, a new account will be created.

4.5. Locking. Every transaction made to an account is linked with add. The Lock algorithm is introduced in Figure 6. If the account is unlocked, you can do it from any address. However, if you lock to an address, you can only operate from add. CheckLock is an internal method to check both states. Before operating the account, all methods will invoke CheckLock. When it has y, addr, and σ_{lock}, Lock will check whether the account is operated by calling CheckLock.

4.6. Auction Execution. In Figure 7, in the auction execution stage of $T_4 < T < T_5$, the auction execution agreement first checks the deposit amount of each bidder, and the bids of bidders who do not have sufficient deposits will be ignored. Then, the auction execution agreement selects winners and payment amounts for different auction formats. Failed buyers and failed sellers do not have to pay any fees.

In combined auctions, the auction execution protocol sorts $\mathscr{V}$ in descending order $v^1 \geq v^2 \geq \ldots \geq v^n$ and greedily distributes the items in order hereafter. Buyer B_i can win her package, if the package does not include any items that have been distributed in the previous winning package. When there are no bidders or available items, the allocation stops. The key bidder is selected as B^c, and its previous bidder is the winner with the smallest bid value, namely, $v^{c-1} \in \mathscr{W}, v_{i,j}^{c-1} \leq v_{i',j'}, \forall B_{i'} \in \mathscr{W} \wedge a^j, a^{j'} \in \mathscr{A}$.

4.7. Market Cleaning. During the market cleaning, bidders and sellers run market clearing agreements to exchange their cryptocurrencies and auction items. After that, the smart contract updates the deposit record of the bidder. Since no bidder has suspended the auction, the SC refunds all funds based on records.

The way to return the deposit is Burn. As shown in Figure 8, Burn transforms ZTH to ETH, and it verifies the proof π_{burn} and st_{burn} to guarantee that the sender holds correct private key and asks for correct amount. Besides, it checks the signature on the transaction data and the counter value to avoid replay attacks. The most important point is that every transfer and destruction transaction in the auction includes ZK proof to ensure that the transferred or redeemed amount is valid without revealing its true value.

Input: $y, \bar{y}$, (C,D), $(\bar{C},D)$ π_{Transfer}, σ_{transfer}.
Output: 0 or 1.
1: If $T_2 < T < T_3$, go to step 2 , otherwise stop.
2: RollOver (y).
3: RollOver ($\bar{y}$).
4: Let (C_L, C_R) = acc[y]
5: Require:
· CheckLock (y, msg.sender) = 1
6: Let acc [y] = acc[y] (C^{-1}, D^{-1}).
7:Let p Transfers [$\bar{y}$] = pTransfers [$\bar{y}$] ∘ $(\bar{C}, D)$.
8:Let ctr[y] = ctr[y] + 1.

Figure 4: Transfer.

Input: y.
Output: 0 or 1.
1: If $T_2 < T < T_3$, go to step 2 , otherwise stop.
2: RollOver (y).
3: Set b = msg.value.
4: Require:
· $-b + b_{\text{total}} \leq$ MAX
· CheckLock (y, msg.sender) = 1
5: If acc [y] = ⊥:
· Let H = block.number, e = [H/E]
· Set acc [y] = (1, 1)
· Set pTransfers [y] = (g^b, 1)
· Set lock[y] = ⊥
· Set lastRollOver [y] = e
· Set ctr[y] = 0
Else:
· Set p Transfers [y]=pTransfers [y]∘(g^b,1)
6: Let $b_{\text{total}} = b_{\text{total}} + b$.

Figure 5: Fund.

Input: y, $addr$, σ_{lock}.
Output: 0 or 1.
1: If $T_3 < T < T_4$, go to step 2 , otherwise stop.
2: RollOver(y).
3: Require:
· CheckLock (y, msg.sender)=1
· Verify$_{nizk}$(y, ($addr$, ctr[y]), σ_{lock} = 1
4: Letlock[y] = addr
· Let H = block.number, e = [H / E].
5: Let ctr[y] = ctr[y] + 1.

Figure 6: Locking.

5. Theoretical Analysis

5.1. Transfer ZK Proof. In addition to hiding the transfer amount, anonymous transfers also hide the information of sender as well as receiver in the transfer. When someone transfers money $b^\star$ from Ethereum address y to $\overline{y}$, and he or she wants to hide the both address in a bigger range of public keys, where $y = \{y_1, \ldots, y_n\}$, let $(C_{L,i}, C_{R,i})$ be the encrypted amounts linked to key y_i, for $i \in [n]$, then the user creates n ciphertexts $(C_1, D_1), \ldots, (C_n, D_n)$ as well as proves that (i) one (jth) encrypts $b^\star$, and another one (ℓth) encrypts $-b^\star$,

1: If $T_4 < T < T_5$, go to step 2 , otherwise stop.
2: For buyer B_i:
· If DPST[B_i] ≤ max(V) (resp . DPST[G_i] ≤ max(S)), continue the loop, otherwise stop.
·Lets $v_i \leftarrow 0$(resp. $s_i \leftarrow \infty$)
3: Updates V, S, (W,P)
4: Publishes (W, P).

Figure 7: Auction.

Input: y,b, π_{burn}.
Output: 0 or 1.
1: If $T_5 < T < T_6$, go to step 2, otherwisestop.
2: RollOver (y).
3: Let (C_L, C_R) = acc[y].
4: require:
·CheckLock (y, msg.sender) = 1
·CheckLock (y, msg.sender) = 1
5: Let ctr[y] = ctr[y] + 1.
6: Let $b_{\text{total}} = b_{\text{total}} - b$.
7: Do msg.sender.transfer (b).

Figure 8: Burn.

and the remaining users encrypt 0; (ii) $b^\star$ is positive; (iii) the remaining funds in y_j (b') are positive too.

We can let $D_1 = \cdots = D_n = D$ and use randomness in order to effectively process statement without disclosing $j, b^\star, \ell$, and b'. Besides, we introduce split-new variables $s_1, \ldots, s_n$ and $t_1, \ldots, t_n$. Value 1 for an s_i indicates that funds are being transferred from y_i and value 1 for a t_j indicates that funds are being transferred to y_j. The user will let these variables be confidential and use them to prove different claims. One of $s_1, \ldots, s_n$ and one of $t_1, \ldots, t_n$ should be 1. This can prove that any of these variables is 1 or 0, $\sum_i s_i = 1$ and $\sum_i t_i = 1$. Besides, the user proves

$$\prod_{i=1}^{n} C_i^{s_i} = g^{b^\star} \prod_{i=1}^{n} y_i^{r \cdot s_i}, \tag{3}$$

$$\prod_{i=1}^{n} C_i^{s_i + t_i} = \prod_{i=1}^{n} y_i^{r \cdot (s_i + t_i)}, \tag{4}$$

$$C_i^{(1-s_i)\cdot(1-t_i)} = y_i^{(1-s_i)\cdot(1-t_i)\cdot r} \text{ for } i \in [n], \tag{5}$$

$$\prod_{i=1}^{n} \left(\frac{C_{L,i}}{C_i} \right)^{s_i} = g^{b'} \left(\frac{\prod_{i=1}^{n} C_{R,i}^{s_i}}{D} \right)^{\text{sk}}, \tag{6}$$

$$g_{\text{epoch}}^{\text{sk}} = u. \tag{7}$$

$s_1, \ldots, s_n$ is 1, and the remaining are 0. Equation (3) indicates that the ciphertext for s_i is an effective encryption for $b^\star$. As equation (3) is subtracted from equation (4), $\prod_{i=1}^{n} C_i^{t_i} = g^{-b^\star} \prod_{i=1}^{n} y_i^{r \cdot t_i}$, which indicates that the ciphertexts of t_i is an effective encryption for $-b^\star$. Thereby, both equations (3) and (4) indicate that the ciphertext-encoded quantities are effective.

In equation (5), $(1 - s_i)(1 - t_i)$ is non-zero in the case when both s_i and t_i are 0. As the equation shows, i and C_i are an encryption of 0. Equation (6) denotes b' amounts of the account for which s_i is 1. Finally, equation (7) denotes that u is the surefire random number during the current epoch.

In addition, users need to prove $g^{\text{sk}} = \Pi y_i^{s_i}$, $b^\star$, $b' \in$ [0, MAX], and the equation associates the secret key with the public key (latter is not revealed), while the latter two equations denote that the transferred amount and the remaining amount are in the correct range. To summarize, users prove the following statement: $\text{st}_{\text{AnonTransfer}}$: $(y_i, C_{L,i}, C_{R,i}, C_i)_{i=1}^{n}$, D, u, g, g_{epoch}; sk, $b^\star$, b', r, $(s_i, t_i)_{i=1}^{n}$:

$$\prod_{i=1}^{n} C_i^{s_i} = g^{b^\star} \prod_{i=1}^{n} y_i^{r \cdot s_i}, \tag{8}$$

$$\prod_{i=1}^{n} C_i^{s_i + t_i} = \prod_{i=1}^{n} y_i^{r \cdot (s_i + t_i)}, \tag{9}$$

$$D = g^r, \tag{10}$$

$$\left(C^{(1-s_i)\cdot(1-t_i)} = y_i^{(1-s_i)\cdot(1-t_i)\cdot r} \right)_{i=1}^{n}, \tag{11}$$

$$\prod_{i=1}^{n} \left(\frac{C_{L,i}}{C_i} \right)^{s_i} = g^{b'} \left(\frac{\prod_{i=1}^{n} C_{R,i}^{s_i}}{D} \right)^{\text{sk}}, \tag{12}$$

$$g^{\text{sk}} = \prod_{i=1}^{n} y_i^{s_i}, \tag{13}$$

$$g_{\text{epoch}}^{\text{sk}} = u, \left(s_i \in \{0, 1\}, t_i \in \{0, 1\} \right)_{i=1}^{n}, \tag{14}$$

$$\sum_{i=1}^{n} s_i = 1, \ \sum_{i=1}^{n} t_i = 1, \ b^\star \in [0, \text{MAX}], \ b' \in [0, \text{MAX}]. \tag{15}$$

Finally, $\text{st}_{\text{AnonTransfer}}$ is expressed as equations (8) to (15). The statement is very complicated, but the structure is actually very deep. It turns out that the size can be logarithmic in the range and anonymity set. This is completed by integrating multiple proofs with Bulletproof to encrypt 0.

5.2. Correctness. The algorithms CreateTransferTx and CreateBurnTx scroll all public keys y according to the status of the SC. Therefore, any unfinished transfers linked with these keys will be returned to the corresponding account, and these unfinished lock requests will become effective. Then, generate the transactions of transfer and burn for the new status of the account, which matches the status of ZSC used to handle them.

Trusted users only place accounts locked to the same address in their anonymous set. When the account holders change the lock of their accounts through calling both methods of lock or unlock, both methods will set the new

Table 3: Comparison of different auction schemes in gas consumption among twenty bidders.

Stages	Consumption in gas		
	SAFE [11]	CREAM [8]	Ours
Registration	455395	2357366	262286
Allocation	0	396742	1279664
Clearing	1955742	91442	750200
Total	2411137	2845550	2292150

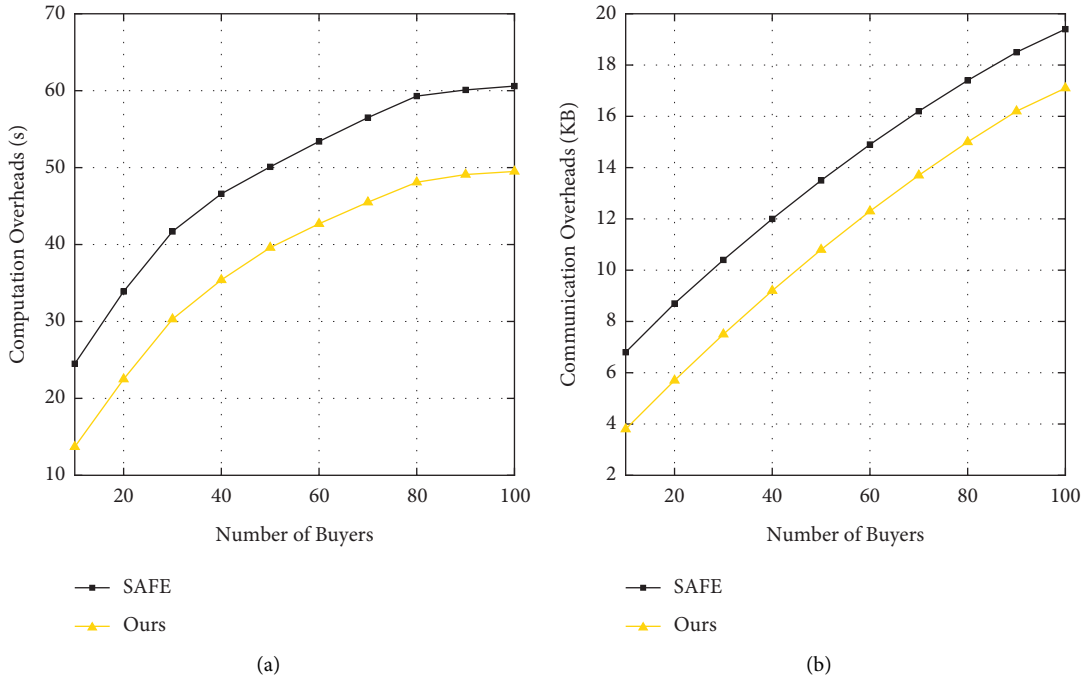

Figure 9: The impact of the quantity of buyers' overheads on (a) computation and (b) communication.

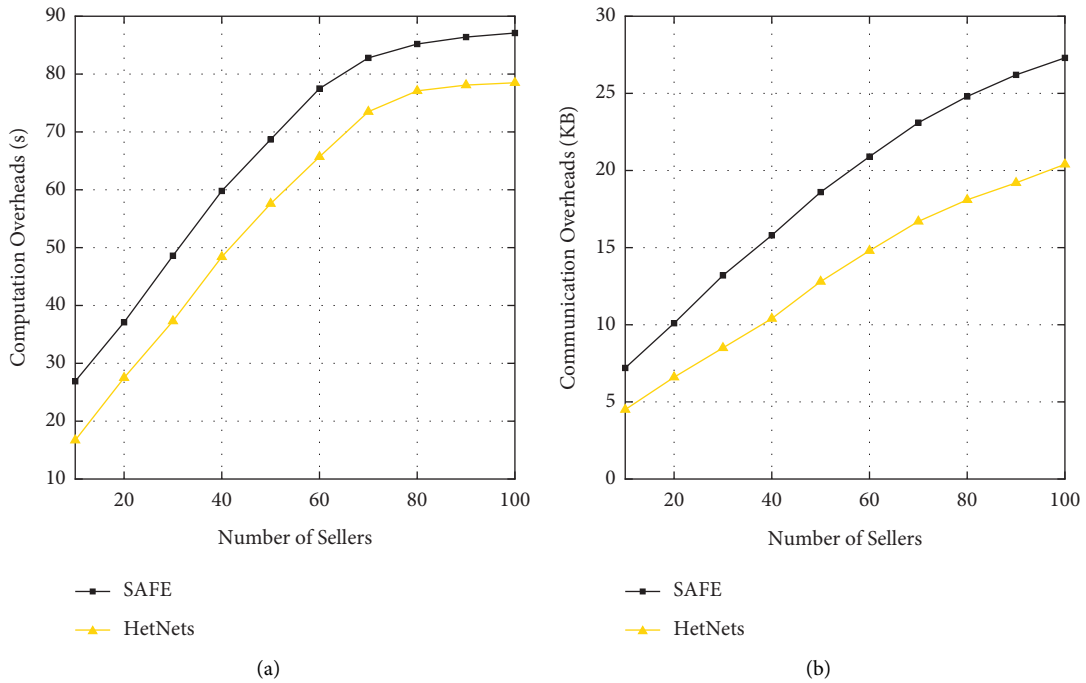

Figure 10: The impact of the quantity of sellers' overheads on (a) computation and (b) communication.

lock address as a suspended lock. Therefore, transactions generated during this period will not have an impact.

The remaining of the correctness is the ElGamal encryption in homomorphic properties and the proof system. Although the encrypted value is in $\mathbb{Z}_p$ and ideally deals with positive integers, it has no effect because ZSC only accepts deposits with the maximum amount of MAX, and the constant is smaller than p. Therefore, homomorphic operations will not lead to overflow.

5.3. Experiment Performance. In order to correctly evaluate the proposed smart contracts and show their feasibility, we run contracts in the form of SC. This implementation indicates that our scheme is practical and it is able to run on the Ethereum Virtual Machine (EVM). In order to show the superiority of our scheme, we also compared it with existing research work.

Our proposed implementation of the Ethereum-based smart contract is written in the Solidity language, and some observations have been analyzed and utilized. Ethereum recently introduced a precompiled contract for elliptic curve operations on the BN-128 curve. Compared with direct implementation, these precompiled contracts lower the cost of performing these operations. The reason is that miners can utilize special software to execute these functions more efficiently. These operations are initially introduced to support pair-based ZK-SNARK. Σ-Bullets do not need to be paired. Curve BN-128 is not the best choice for the efficiency or safety of Bulletproofs Σ-Bullets. Despite this, we still choose to use this curve to implement experiment because it is natively supported and the implementation cost is relatively lower.

5.4. Gas Consumption and Overheads. We first measured the gas consumption used to implement basic contract operations. We measure gas consumption including registration, allocation, and clearing. As shown in Table 3, in a combined auction with 20 bidders, combined with SAFE [11] and CREAM [8], our scheme consumed the least gas.

As shown in Figures 9 and 10, we evaluated the system overhead of quantity of buyers and sellers, As buyers' quantity increases but is less than the quantity of items in the combined auction, time and storage consumption will soar because of the high growth rate of the winners. When the quantity of buyers' items exceeds the quantity of buyers, the quantity of winners will remain unchanged, resulting in an increase in overhead during the market clearing phase. The increase in the quantity of sellers or projects will increase the quantity of winners, and the main expense is in the market clearing phase. Overall, our solution has better performance than SAFE.

6. Conclusions

In this paper, we present a Zether-based approach in dealing with the combinatorial spectrum e-auction challenges in 5G HetNet. The e-auction is executed in the ZSC without adopting SGX. Besides, our approach also achieves bidding value preservation without introducing time-consuming cryptographic tools such as Paillier homomorphic encryption, garbled circuits, and so on. We deploy our approach on Ethereum and testify the effectiveness as well as scalability. Given that gas consumptions in some auction phases are higher than that in state-of-the-art research, we leave these in our future work.

Data Availability

The experimental data required for this article cannot be shared at this time because these data are also part of ongoing research.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this article.

Acknowledgments

This research was supported by MF2009 Project (Trusted Joint Computing on Cross-Border Data) and MOST-FDCT Projects (0058/2019/AMJ) (Research and Application of Cooperative Multi-Agent Platform for Zhuhai-Macao Manufacturing Service).

References

[1] G. Forecast, "Cisco visual networking index: global mobile data traffic forecast update, 2017–2022," *Update*, vol. 2017, p. 2022, 2019.

[2] P. Wang, B. Di, H. Zhang, K. Bian, and L. Song, "Cellular V2X communications in unlicensed spectrum: harmonious coexistence with VANET in 5g systems," *IEEE Transactions on Wireless Communications*, vol. 17, no. 8, pp. 5212–5224, 2018.

[3] A. Networks, "Field test report: Aviat participates in field testing on 6 ghz unlicensed devices with ameren and epri," 2021, https://blog.aviatnetworks.com/field-test-report-aviat-participates-in-field-testing-on-6-ghz-unlicensed-devices-with-ameren-and-epri/.

[4] M. Miao Pan, J. Jinyuan Sun, and Y. Yuguang Fang, "Purging the back-room dealing: secure spectrum auction leveraging paillier cryptosystem," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 4, pp. 866–876, 2011.

[5] Q. Wang, J. Huang, Y. Chen, C. Wang, F. Xiao, and X. Luo, "$PROST$: privacy-preserving and truthful online double auction for spectrum allocation," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 2, pp. 374–386, 2019.

[6] Y. Chen, X. Tian, Q. Wang, M. Li, M. Du, and Q. Li, "ARMOR: a secure combinatorial auction for heterogeneous spectrum," *IEEE Transactions on Mobile Computing*, vol. 18, no. 10, pp. 2270–2284, 2019.

[7] Q. Wang, J. Huang, Y. Chen, X. Tian, and Q. Zhang, "Privacy-preserving and truthful double auction for heterogeneous spectrum," *IEEE/ACM Transactions on Networking*, vol. 27, no. 2, pp. 848–861, 2019.

[8] S. Wu, Y. Chen, Q. Wang, M. Li, C. Wang, and X. Luo, "Cream: a smart contract enabled collusion-resistant e-auction," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 7, pp. 1687–1701, 2019.

[9] J. Wang, N. Lu, Q. Cheng, L. Zhou, and W. Shi, "A secure spectrum auction scheme without the trusted party based on the smart contract," *Digital Communications and Networks*, vol. 7, no. 2, pp. 223–234, 2020.

[10] Z. Zhou, X. Chen, Y. Zhang, and S. Mumtaz, "Blockchain-empowered secure spectrum sharing for 5g heterogeneous networks," *IEEE Network*, vol. 34, no. 1, pp. 24–31, 2020.

[11] Y. Chen, X. Tian, Q. Wang, J. Jiang, M. Li, and Q. Zhang, "Safe: a general secure and fair auction framework for wireless markets with privacy preservation," *IEEE Transactions on Dependable and Secure Computing*, vol. 2020, Article ID 3045449, 2020.

[12] B. Bünz, S. Agrawal, M. Zamani, and D. Boneh, "Zether: towards privacy in a smart contract world," in *Proceedings of the International Conference on Financial Cryptography and Data Security*, pp. 423–443, Springer, Berlin, Germany, February 2020.

[13] K. Cheng, L. Wang, Y. Shen, Y. Liu, Y. Wang, and L. Zheng, "A lightweight auction framework for spectrum allocation with strong security guarantees," in *Proceedings of the IEEE INFOCOM 2020-IEEE Conference on Computer Communications*, pp. 1708–1717, IEEE, Toronto, Canada, July 2020.

[14] M. Campanelli, R. Gennaro, S. Goldfeder, and L. Nizzardo, "Zero-knowledge contingent payments revisited: attacks and payments for services," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pp. 229–243, New York, NY, USA, October 2017.

[15] M. B. H. Weiss, K. Werbach, D. C. Sicker, and C. E. C. Bastidas, "On the application of blockchains to spectrum management," *IEEE Transactions on Cognitive Communications and Networking*, vol. 5, no. 2, pp. 193–205, 2019.

[16] D. Tygar, "Auction types," 2021, https://www.usenix.org/legacy/publications/library/proceedings/ec98/full˙papers/harkavy/harkavy˙html/node2.html.

[17] Wikipedia, "Combinatorial auction," 2021, https://en.wikipedia.org/wiki/Combinatorial˙auction.

[18] Y. Tsiounis and M. Yung, "On the security of elgamal based encryption," in *Proceedings of the International Workshop on Public Key Cryptography*, pp. 117–134, Springer, Berlin, Germany, May 1998.

[19] B. Bünz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, and G. Maxwell, "Bulletproofs: short proofs for confidential transactions and more," in *Proceedings of the 2018 IEEE Symposium on Security and Privacy (SP)*, pp. 315–334, IEEE, San Francisco, CA, USA, May 2018.

[20] C.-P. Schnorr, "Efficient identification and signatures for smart cards," in *Proceedings of the Conference on the Theory and Application of Cryptology*, pp. 239–252, Springer, Houthalen, Belgium, April 1989.