ARMOR: A Secure Combinatorial Auction for Heterogeneous Spectrum

Yanjiao Chen, *Member, IEEE,* Xin Tian, Qian Wang, *Member, IEEE,*
Minghui Li, Minxin Du, and Qi Li, *Senior Member, IEEE*

Abstract—Dynamic spectrum allocation via auction is an effective solution to spectrum shortage. Combinatorial spectrum auction enables buyers to express diversified preferences towards different combinations of channels. Despite the effort to ensure truthfulness and maximize social welfare, spectrum auction also faces potential security risks. The leakage of sensitive information such as true valuation and location of bidders may incur severe economic damage. However, there is a lack of works that can provide sufficient protection against such security risks in combinatorial spectrum auction. In this paper, we propose ARMOR, to enable combinatorial auction for heterogeneous spectrum with privacy, which can preserve bidders' privacy while guaranteeing the economic-robustness of the combinatorial auction. We leverage the cryptographic methods, including homomorphic encryption, order-preserving encryption and garbled circuits, to shield the bid and location information of buyers from the auctioneer. We design a novel location protection algorithm, which allows the auctioneer to exploit spectrum reuse opportunities without knowing the exact locations of buyers. Furthermore, we propose a verifiable payment scheme based on digital signature to prevent the auctioneer from forging the payment. The extensive experiments confirm that ARMOR maintains the good performance of the combinatorial spectrum auction, in terms of buyer satisfactory ratio and social welfare, and achieves privacy preservation with acceptable computation and communication costs.

Index Terms—Spectrum Allocation, Combinatorial Auction, Privacy Preservation, Social Welfare, Verifiable Pricing.

1 Introduction

With the surging demand for wireless communication applications and services, spectrum resource limitation is becoming a bottleneck for the development of wireless communication industry. The rigid long-term licensing policy may lead to potential starvation of unlicensed users in the secondary market. To improve spectrum utilization and social welfare, dynamic spectrum allocation is proposed to redistribute under-utilized spectrum to secondary users on a short-term basis. Spectrum auction is deemed to be an effective way to realize such dynamic spectrum allocation.

Various types of auction mechanisms have been proposed to cater for different spectrum allocation requirement, *e.g.*, single spectrum auction, double spectrum auction, and combinatorial spectrum auction. In this paper, we focus on the combinatorial auction that allows bidders to submit bids for various combinations of goods, making it ideal for secondary users to pursue spectrum bundles that can most effectively support their service. Existing combinatorial spectrum auction mechanisms [1], [2], though achieving good performance in terms of economic-robustness and allocation efficiency, did not consider privacy preservation for bidders. The leakage of sensitive information may cause severe consequences and discourage bidders to participate in the auction. To be specific, in a truthful combinatorial auction, the bidding values reflect a bidder's true valuation for different channel combinations, which may be exploited by malicious business rivals to infer the bidders technological strength, market share, and business status. The location information, collected by the auctioneer to determine spectrum sharing, may reveal the user base and subscription information of the bidders. The leakage of these private information may cause potentially heavy economic loss to the bidders, which will discourage them to participate in the auction. Therefore, there is a dire need of privacy-preserving mechanisms for combinatorial auctions.

To address these problems, in this paper, we propose a truthful and privacy-preserving combinatorial spectrum auction mechanism with the following four design objectives. First, the spectrum allocation should feature *spatial reuse*. Spatial reusability is a distinctive feature of spectrum resources, and can be exploited to improve spectrum utilization. Spatial reusability is constrained by complex interference relationship among bidders. Second, the auction must be *truthful* such that the rational and selfish bidders are encouraged to report their truthful valuations for the spectrum. Third, the auction results should achieve *approximate social welfare*. Fourth, the auction mechanism should ensure *privacy preservation*, where bidders' private information is protected from the untrustworthy third-party auctioneer and rivalry bidders. To achieve these design objectives under the complicated combinatorial auction is quite challenging. We mainly face the following difficulties.

- *Conflict examination on encrypted bundles*. In combinatorial spectrum auctions, the auctioneer will check each channel in required bundles for winner determination. If two bundles contain the same channel, and the corresponding bidders interfere with each other, the two bundles cannot be won simultaneously. A bidder's required bundles may reveal her service demand and thus should be kept secret. It is easy to apply cryptographic tools to the elements in bundles to protect user privacy. However, commonly-used encryption

- *Y. Chen and X. Tian are with the School of Computer Science, Wuhan University, Wuhan, Hubei, 430072, P.R. China. E-mail:{chenyanjiao, tianxintx}@whu.edu.cn.*
- *Q. Wang, M. Li and M. Du are with the School of Cyber Science and Engineering, Wuhan University, Wuhan, Hubei, 430072, P.R. China. E-mail: {qianwang,minghuili,duminxin}@whu.edu.cn.*
- *Q. Li is with the Graduate School at Shenzhen, Tsinghua University, Shenzhen, P.R. China. E-mail: qi.li@sz.tsinghua.edu.cn.*

algorithms may support simple operations (e.g., summation or multiplication), but are unable to support conflict examination on encrypted bundles. Therefore, we need to design an effective method to enable conflict examination on encrypted bundles.

- *Privacy protection for location information*. The location information is crucial for determining spectrum spatial reuse but should be protected since it may be leveraged by rivalry bidders for malicious purposes. However, it is not enough to simply encrypt the location information, since the construction of conflict graph among bidders may reveal the relative distance between each pair of bidders. The relative distance will allow the adversary to estimate the distribution of geolocations of bidders. Therefore, a well-round protection for location information should be guaranteed.
- *Payment fraud detection*. The auctioneer has incentives to forge the payment to gain a higher profit. Without privacy preservation, payment fraud is easy to detect since all bidding values, location information and auction results are publicized for bidders to examine the payment calculated by the auctioneer. Unfortunately, in privacy-preserving auctions, all private information is protected, making it hard for bidders to verify the payment claimed by the auctioneer. Therefore, we should provide a way to detect payment fraud while protecting privacy information.

In recent years, privacy-preserving auction design has raised great concern [3]–[7]. Yokoo *et al.* [3] have incorporated a secure multi-agent dynamic programming in homomorphic encryption to protect user privacy in combinatorial auctions. Jung *et al.* [7] have proposed a privacy-preserving combinatorial auction mechanism, but it is restricted that bidders are single-minded, *i.e.*, each bidder can submit only one spectrum bundle, which greatly affects the flexibility of the combinatorial auction. Secure vickrey auction design has been explored in [4], [5]. Brandt and Sandholm [6] have investigated unconditional full privacy in sealed-bid auctions. In [8], a privacy-preserving auction is constructed by invoking secret sharing [9], [10]. However, all these works consider auctions for traditional goods and exclusive usage, whereas spectrum can be reused among non-conflicting bidders. Various privacy-preserving schemes have been proposed for spectrum auctions [11]–[15]. [11]–[14] all target at single spectrum auction and resort to homomorphic encryption to preserve bidders' bidding values, but none of them supports the combinatorial auction where the bidders' demands consist of combinations of multiple spectrums. In [15], a secure combinatorial spectrum auction mechanism, SCSA, has been proposed, which decomposes the whole network into subnetworks and auctions the channels in subnetworks, where each bidder informs her conflicting neighbors of the updates of spectrum occupancy information. Unfortunately, neither [15] nor most existing works [11]–[13] provide protection for bidders' location information, which is leveraged by the auctioneer to determine spectrum reuse but is bidders' sensitive information that should be guarded from adversaries.

In this paper, we propose ARMOR, a novel truthful and privacy-preserving combinatorial spectrum auction mechanism that has addressed all three design challenges. Consider the TV white space spectrum auction as a typical application scenario, where the TV white space channels feature both spatial and frequency heterogeneity. The framework of ARMOR under this scenario is shown in Fig. 1, where the unlicensed secondary users bid for channel combinations, and the primary user serves as the auctioneer to distribute the spectrum among bidders. ARMOR is built upon a generic combinatorial auction mechanism [2] that is truthful with approximate maximum social welfare. The design of ARMOR guarantees truthful bidding over heterogeneous spectrum among multi-minded bidders with privacy protection taken into account. We adopt cryptographic methods, including homomorphic encryption, order-preserving encryption and garbled circuits, to provide a strong protection for bidders' private information. A secure algorithm based on homomorphic encryption and garbled circuits is designed to realize spatial reusability without disclosing bidders' location information. Following the common practice in existing works [12]–[14], [16], we introduce a semi-honest agent who serves as a coordinator to interact with both the auctioneer and the bidders during the auction. The role of agent can be played by a nonprofit and well-established organization, who has incentives to correctly run the protocols without deviation, but may be curious about bidders' private information. The agent generates digital signature so that bidders can verify payment that may be forged by the untrustworthy auctioneer. Table 1 is an overview of the comparison between our construction and some other privacy-preserving spectrum auction mechanisms. In summary, We make the following key contributions:

1) As far as we are concerned, we are the first to propose a fully privacy-preserving truthful combinatorial auction mechanism that realizes spatial reuse over heterogeneous spectrum and multi-minded bidders.
2) We have integrated various cryptographic techniques to offer a strong and all-round protection of bidders' private information, including location information and bidding values.
3) We have designed a verifiable payment scheme based on digital signature to enable bidders to detect payment forging by the untrustworthy auctioneer.
4) We have theoretically proved the truthfulness and security of ARMOR, and conducted extensive simulations to evaluate its performance. The results show that ARMOR achieves a comprehensive privacy preservation with little allocation efficiency loss and acceptable overheads.

The rest of this paper is organized as follows. In Section. 2, we introduce the system models and cryptographic tools we adopted in this paper. We present our design overview in Section. 3. Section. 4 is the detailed design of ARMOR. In Section. 5, we present the theoretical analysis on the auction efficiency, security and the computation and communication complexity of ARMOR. The experimental evaluation results are given in Section. 6. In Section. 7, we review the related work, and the conclusion and future works are given in Section. 8.

2 Preliminaries

2.1 System Model

We consider a set of m heterogenous channels $\mathcal{S} = \{s_1, s_2, \dots, s_m\}$ to be auctioned to n bidders $\mathcal{B} = \{B_1, B_2, \dots, B_n\}$ by a *semi-honest* auctioneer via a combinatorial auction, in which bidders bid on a bundle instead of individual channels. We assume that bidder B_i is l_i-minded, which means that B_i can submit at most l_i bundles $b_i = \{b_{i,1}, b_{i,2}, \dots, b_{i,l_i}\}$ along with a set of bidding values $v_i = \{v_{i,1}, \dots, v_{i,l_i}\}$ that may be different from her true valuation for each bundle $V_i = \{V_{i,1}, \dots, V_{i,l_i}\}$, where $b_{i,d} \subseteq \mathcal{S}, \forall d \in [1, l_i]$. The set of all bundles from all bidders are denoted as $\mathcal{D}$. The auctioneer will

Existing Works	Strategy Proofness	Spatial Reusability	Channel Heterogeneity	Bid Diversity	Location Protection	Payment Verifiability
THEMIS [11]	✓	✓	✓	✗	✗	✗
PPS [12]	✓	✓	✗	✗	✗	✗
PRIDE [13]	✓	✓	✗	✗	✗	✓
PISA [14]	✓	✓	✗	✗	✓	✗
SCSA [15]	✓	✓	✓	✓	✗	✗
ARMOR	✓	✓	✓	✓	✓	✓

TABLE 1: Comparison with Existing Privacy-Preserving Spectrum Auction Mechanisms.

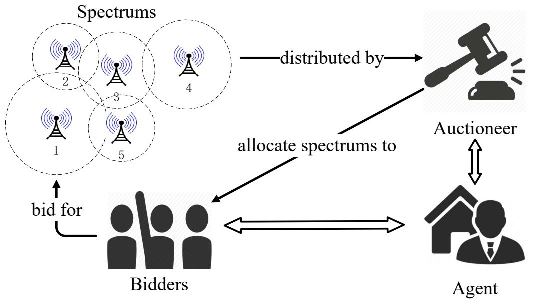


Fig. 1: The framework of ARMOR for TV white space auction.

determine a set of winners $\mathcal{W} \subseteq \mathcal{B}$ with corresponding channel allocation $\mathcal{A}$ and payment p_i for each winner $B_i \in \mathcal{W}$. The utility u_i of bidder B_i is her true valuation on her allocated bundle minus the payment, i.e., $u_i = V_{i,d} - p_i$. The design objective of the auction is to maximize social welfare, which is the sum of winning bidders' valuations on their winning bundles, while bidders are rational and selfish, aiming at maximizing their own utility.

2.2 Adversarial Model

To realize privacy preservation, we introduce a *semi-honest* agent to collaborate with the auctioneer to run the auction. At the end of the auction, no participant is supposed to learn anything about the bidders' information beyond what is revealed by the auction outcomes. Specifically, we consider two kinds of adversaries as follows.

- *Semi-Honest adversaries*: The auctioneer and the agent are semi-honest, who will correctly run the protocol as specified without any deviation but are curious about buyers' privacy. Furthermore, we consider the case where the auctioneer may commit frauds by overcharging winning buyers.
- *Rational and Selfish Bidders*: Bidders are rational and selfish, who have the incentive to misreport their bids to gain higher utilities. Besides, each bidder intends to leverage other bidders' private information to her advantage.

We assume that all participants belong to different independent organization, *i.e.*, there is no collusion between any pair of participants. We will address the problem of collusion in future works.

2.3 Cryptographic Tools and Primitives

2.3.1 Homomorphic Encryption

Homomorphic encryption ensures that results of specific computations on ciphertexts match the encrypted results of the same computations on the plaintext. Homomorphic encryption for arbitrary operations can be prohibitively slow, but it is efficient for addition operation. We employ Paillier cryptosystem [17] in Alg. 1. Let $[\![M]\!]$ denote the encryption of a message $M \in \mathbb{Z}_n$. Suppose there are two messages M_1 and M_2, we have the following homomorphic properties:

Algorithm 1 Paillier Cryptosystem

```
**System parameter**: two prime numbers $p$,$q$.
**Public key**: modulus $n = pq$, a random number $g \in \mathbb{Z}^{\star}_{n^2}$.
**Private key**: $\lambda = \mathrm{LCM}(p-1, q-1)$.
**Encryption**: $c = \mathrm{E}(M, r) = g^{M+nr} \bmod n^2$,
        where $r \in \mathbb{Z}^{\star}_{n}$ is a random number.
**Decryption**: $M = \mathrm{D}(c) = \frac{\mathrm{L}(c^{\lambda} \mod n^2)}{\mathrm{L}(g^{\lambda} \mod n^2)} \bmod n$,
        where $\mathrm{L}(x) = \frac{x-1}{n} \bmod n$.
**Self-blinding**: $\mathrm{E}(M, r) \cdot g^{nr'} = \mathrm{E}(M, r + r')$.
```

$$[\![M_1 + M_2 (\bmod n)]\!] = [\![M_1]\!] \cdot [\![M_2]\!] \,(\bmod n),$$
$$[\![M_1 \cdot M_2 \,(\bmod n)]\!] = [\![M_1]\!]^{M_2} \,(\bmod n).$$

Without confusion, we will leave out the mod operation in the rest of the paper.

2.3.2 Order-Preserving Encryption

Order-Preserving Encryption (OPE) [18] is a deterministic encryption scheme whose encryption function preserves the numerical ordering of the plaintexts, thus supporting the direct comparison operation over the encrypted data. We employ an OPE scheme that consists of a set of deterministic symmetric encryption functions $(KeyGen, Enc, Dec)$. A symmetric key is generated from the function $SK = OPE.KeyGen(1^{\epsilon})$, where ϵ is a security parameter. Let $P = \{i | 1 \leq i \leq a\}$ denote the set of plaintexts, and $C = \{i | 1 \leq i \leq b\}$ denote the set of ciphertexts, and we have $a \leq b$. The ciphertexts are encrypted as $C = Enc(P, SK)$, and the plaintexts are decrypted as $P = Dec(C, SK)$. With a valid symmetric key SK, the OPE scheme guarantees that $\forall x, x' \in P, x < x' \Leftrightarrow Enc(x, SK) < Enc(x', SK)$.

2.3.3 Garbled circuits

Yao's garbled circuits [19] are a cryptographic protocol that enables two mistrusting parties, who hold inputs a and b respectively, to jointly evaluate an arbitrary function $f(a, b)$ without the presence of a trusted third party. In the garbled circuits protocol, one party, called the circuit *garbler*, first garbles (encrypts) the function circuits and sends the garbled circuits to the other party along with her encrypted input. Then, the other party, called the circuit *evaluator*, receives her encrypted inputs through *Oblivious Transfer* (OT) [20] and evaluates (decrypts) it. Both parties will

Algorithm 2 Blinded Nyberg-Rueppel Scheme

```
System paramerter: a prime number $p$, a prime factor $q$ of $p-1$, and an element $g \in \mathbb{Z}_p^*$ of order $q$.
Key Generation: the signer picks a random number $x \in \mathbb{Z}_q$, and a random number $h \in \mathbb{Z}_p^*$ such that $g = h^{\frac{p-1}{q}} \neq 1 (\bmod p)$. The secret parameter is $x$ and the public parameters are $g, g^x (\bmod p)$.
Signing: the signer blindly signs the signee's message $M$:
    1) the signer randomly selects $\hat{k} \in \mathbb{Z}_q$ and sends $\hat{r} = g^{\hat{k}} (\bmod p)$ to the signee.
    2) the signee randomly selects $\alpha \in \mathbb{Z}_q$ and $\beta \in \mathbb{Z}_q^*$, computes $r = Mg^{\alpha} (\bmod p)$ and $\hat{M} = r\beta^{-1} (\bmod q)$ until $\hat{M} \in \mathbb{Z}_q^*$, then sends $\hat{M}$ to the signer.
    3) the signer computes $\hat{s} = \hat{M}x + \hat{k} (\bmod q)$ and sends $\hat{s}$ to the signee.
    4) the signee computes $s = \hat{s}\beta + \alpha (\bmod q)$, and the pair $(r, s)$ is the Nyberg-Rueppel signature for $M$.
Verification: check whether $M = g^{-s} y^r r (\bmod q)$.
```

gain access to the encrypted outputs without learning any intermediate values.

2.3.4 Digital Signature

Digital signature is usually used for authentication. As shown in Alg. 2, we adopt the blinded Nyberg-Rueppel scheme [21], in which the signer can generate a signature of a message without "seeing" it, while the recipients can recover the message from the signature.

Note that not all blinded signature schemes can be used in our construction. Let $\mathcal{SIG}$ denote the signing operation. The ones using homomorphic encryption E, for instance, are often subject to the following problem:

$$\mathcal{SIG}(M_1)^{M_2} = \mathrm{E}(M_1)^{M_2} = \mathrm{E}(M_1 M_2) = \mathcal{SIG}(M_1 M_2).$$

Thus, according to the properties of homomorphic encryption (Section 2.3.1), the signature of $M_1 M_2$ can be illegally obtained by the adversary from the exponentiation of $\mathcal{SIG}(M_1)$.

2.3.5 Public-key Cryptography

Public-key cryptography, *a.k.a* asymmetric cryptography, accomplishes two main functions: authentication and encryption. In such a cryptosystem, the encryption key pk is public and different from the decryption key sk, which is kept secret. RSA [22] is one of the most widely-used public-key encryption method, whose public key $pk = (n, e)$ is created based on two large prime numbers p and q. As the public key, n satisfies $n = pq$ and e is chosen from $1 < e < \lambda(n)$ and satisfies $\gcd(e, \lambda(n)) = 1$, where λ is Carmichael's totient function. The private exponent d for the private key can be calculated as $d \equiv e^{-1} \mod \lambda(n)$. The public key is publicized, and the two prime numbers are kept secret. Any sender can encrypt a message M with the encryption key from an intended recipient by performing $C \equiv M^e \mod n$, but only the recipient can decrypt the message by computing $C^d \equiv (M^e)^d \equiv M \mod n$ with her confidential decryption key sk that consists of d.

2.3.6 Secure Comparison

The secure comparison is invoked by two parties: party A, who holds the decryption key, and party B. To securely compare two ρ_1-bit numbers n_1, n_2 without disclosing their true values, we construct a novel secure primitive CombinatorialGC in Alg. 3, based on COMPARE and SUBTRACT circuits introduced in [23]. As shown in Alg. 4, party B first computes and sends $[\![n_1 + r_1]\!]$ and $[\![n_2 + r_2]\!]$, along with the garbled values of two ρ_2-bit ($\rho_2 > \rho_1$) random numbers r_1, r_2, to party A. Then, party A decrypts and obtains $n_1 + r_1$ and $n_2 + r_2$. After invoking oblivious transfer and getting the garbled inputs, party A evaluates the CombinatorialGC to get the single-bit output χ_{n_1,n_2}. If $\chi_{n_1,n_2} = 0$, we have $n_1 < n_2$; otherwise, $n_1 \geq n_2$.

Algorithm 3 CombinatorialGC

```
Input: two groups of garbled values: $(n_1 + r_1, r_1)$, $(n_2 + r_2, r_2)$
Output: the one-bit comparison result $CmpRes$
evaluate two invisible intermediate results:
        $n_1 = \mathsf{SUBTRACT}(n_1 + r_1, r_1)$,
        $n_2 = \mathsf{SUBTRACT}(n_2 + r_2, r_2)$.
evaluate the final open result:
        $CmpRes = \mathsf{COMPARE}(n_1, n_2)$.
return $CmpRes$.
```

Algorithm 4 TwoCMPMin

```
Input: two encrypted numbers $n_1$ and $n_2$
Output: the comparison result $\chi_{x_1,x_2}$
    Party $B$:
select two $\rho_2$-bit random numbers $r_1$ and $r_2$.
compute $[\![n_1 + r_1]\!]$ and $[\![n_2 + r_2]\!]$.
send $[\![n_1 + r_1]\!]$ and $[\![n_2 + r_2]\!]$ and garbled values of $r_1, r_2$ to party $A$.
    Party $A$:
decrypt and get $n_1 + r_1$ and $n_2 + r_2$.
invoke OT protocols to obtain garbled values of $n_1 + r_1$ and $n_2 + r_2$.
evaluate the circuits to obtain:
$\chi_{n_1,n_2} = \mathsf{CombinatorialGC}((n_1 + r_1, r_1), (n_2 + r_2, r_2))$.
return $\chi_{n_1,n_2}$.
```

3 Design Overview

3.1 Design Rationale

In order to achieve spatial reuse, truthfulness, approximate social welfare and privacy preservation, ARMOR carefully addresses the challenges in Section 1.

Computable encrypted bundles. In order to enable spectrum spatial reuse, we leverage the concept of virtual channel (described in details in Section 4.1) [2] to transform bundles. Then, we represent each modified bundle as a matrix. Thanks to the bundle adaptation, we are able to examine conflict in two bundles with a multiplication operation on their corresponding matrices. In this way, the conflict examination can be performed on encrypted bundles supported by homomorphic encryption to protect bidders' privacy.

All-round protection on location information. For a more comprehensive protection on bidders' locations, we design a set of new circuits in Alg. 3 to integrate with the homomorphic encryption algorithm. When building the conflict graphs, the agent adds a random number to each encrypted location information so that the auctioneer cannot derive the relative distance even if the ciphertext is decrypted. By jointly evaluating the circuits, the auctioneer and the agent can obtain a one-bit output to indicate the interference relationship between two bidders, but neither of them can learn any intermediate results.

Payment fraud resistance. We design a verifiable pricing scheme for payment fraud resistance. Bidders encrypt their virtual bids (described in details in Section 4.1.3) with the symmetric key SK of OPE scheme that is agreed upon in consensus, and the agent blindly signs the encrypted virtual bids. When the auctioneer reports the payment to winners indirectly through the agent, the agent will attach the signature of the critical virtual bids to the message. A winner can compare the payment from the auctioneer with the one computed from the recovered virtual bid to check whether the payment is forged.

3.2 System Overview

As shown in Fig. 2, ARMOR comprises of the following key steps.

Initialization. During initialization, the key pairs of Paillier cryptosystem, Nyberg-Rueppel scheme and RSA encryption are generated. Moreover, bidders reach a consensus on the symmetric key of OPE scheme that will be used for the subsequent virtual bid encryption.

Virtual Bundle Generation. In this step, bidders generate virtual bundles by converting the required channels into virtual channels according to their received conflict graphs that are cooperatively built by the auctioneer and the agent. Based on the virtual bundles, bidders can compute their virtual bids and the number of bundles.

Winner Determination. In this step, the auctioneer holds the order-preserving-encrypted virtual bids while the agent knows the signed encrypted virtual bids and bundle numbers. Based on their individual information, they will jointly determine the winners. Bidders are not involved with the computation of this step but only providing their encrypted bundles when agent asks.

Verifiable Pricing. In this step, candidate critical bidders search conflicts with the winner with the help of the agent. Once the critical bidder is determined, the auctioneer computes the payment and informs winners of the verifiable results through the agent.

We summarize the key notations used in our construction in Table 2. Our proposed ARMOR framework can be directly applied to non-combinatorial single-unit or multi-unit forward auctions. However, there are many complicated auction models with specific formats and system models that ARMOR may not apply such as double auction and dynamic auction. We leave it to our future works to design privacy-preserving mechanisms for other auctions.

4 Our ARMOR

In this section, we propose the detailed design of ARMOR. To begin with, the auctioneer and the agent separately run the key-pair generation of the Paillier cryptosystem and the blinded Nyberg-Reuppel scheme. Each bidder generates her RSA key pair (pk_i, sk_i), and then produces a symmetric key SK for OPE scheme together with other bidders. After these initial preparation, the main auction mechanism consists of the following steps.

Notation	Implication
(pk_i, sk_i)	public and private key pair of RSA for bidder i
SK	symmetric key of OPE scheme
B_i	bidder i
s_j	channel j
$\mathcal{D}$	collection of all bundles
b_i	set of bundles for bidder i
b'_i	set of virtual bundles for bidder i
l_i	number of bundles of bidder i
v_i	set of bidding values of bidder i
V_i	set of true valuations of bidder i
$\mathcal{M}_i$	set of virtual bundle matrices for bidder i
$vc^k_{i,j}$	virtual channel on channel k for bidder i and j
ψ_i	set of virtual bids for bidder i
φ_i	set of order-preserving-encrypted virtual bids for bidder i
$\mathbb{B}$	set of number of bundles

TABLE 2: Key notations in ARMOR.

Algorithm 5 Secure Conflict Graph Generation

```
Input: encrypted geo-location $\llbracket \mathcal{L} \rrbracket$, encrypted frequency radius $\llbracket R \rrbracket$
Output: conflict graph $\mathbb{G}$
for $k = 1$ to $m$ do
    for $i = 1$ to $n$ do
        for $j = 1$ to $n$ do
            Agent:
            select three $\rho_2$-bit random integers $r_1, r_2, r_3$ from $\mathbb{Z}_{2^{\rho_2}}$.
            $X \leftarrow \llbracket x_i \rrbracket \cdot \llbracket x_j \rrbracket^{-1} \cdot \llbracket r_1 \rrbracket$.
            $Y \leftarrow \llbracket y_i \rrbracket \cdot \llbracket y_j \rrbracket^{-1} \cdot \llbracket r_2 \rrbracket$.
            $R \leftarrow \llbracket R_k \rrbracket^2 \cdot \llbracket r_3 \rrbracket$.
            send $X$, $Y$, $R$ to the auctioneer.
            Auctioneer:
            decrypt the ciphertext to get $x_i - x_j + r_1$, $y_i - y_j + r_2$, and $2R_k + r_3$.
            $XX \leftarrow (x_i - x_j + r_1)^2$, $YY \leftarrow (y_i - y_j + r_2)^2$, $RR \leftarrow (2R_k + r_3)^2$.
            send $\llbracket XX \rrbracket$, $\llbracket YY \rrbracket$, $\llbracket RR \rrbracket$ to the agent.
            Agent:
            $P_1 \leftarrow \llbracket x_i - x_j \rrbracket^{2r_1}$, $P_2 \leftarrow \llbracket y_i - y_j \rrbracket^{2r_2}$, $P_3 \leftarrow \llbracket 2R_k \rrbracket^{2r_3}$.
            $Q_1 \leftarrow \llbracket (r_1)^2 \rrbracket$, $Q_2 \leftarrow \llbracket (r_2)^2 \rrbracket$, $Q_3 \leftarrow \llbracket (r_3)^2 \rrbracket$.
            $DIS \leftarrow \llbracket XX \rrbracket \cdot P_1^{-1} \cdot Q_1^{-1} \cdot \llbracket YY \rrbracket \cdot P_2^{-1} \cdot Q_2^{-1}$, $RAD \leftarrow \llbracket RR \rrbracket \cdot P_3^{-1} \cdot Q_3^{-1}$.
            $\mathbb{G}^k_{i,j} = \mathsf{TwoCMPMin}(RAD, DIS)$.
        end for
    end for
    $\mathbb{G} = \mathbb{G} \cup \{\mathbb{G}^k\}$.
end for
return $\mathbb{G}$.
```

4.1 Secure Virtual Bundle Generation

We adopt the concept of *virtual channel* in [2] and implement it with mathematical matrix in our construction. A channel s_k in bundle $b_{i,d}$ will be turned into $vc^k_{i,j}$ if bidder B_i and B_j interfere with each other on channel s_k. Only one bundle $b_{i,d}$, whose corresponding virtual bundle $b'_{i,d}$ contains a certain virtual channel, can be granted as a winning bundle, which guarantees exclusive usage of a certain channel between conflicted bidders.

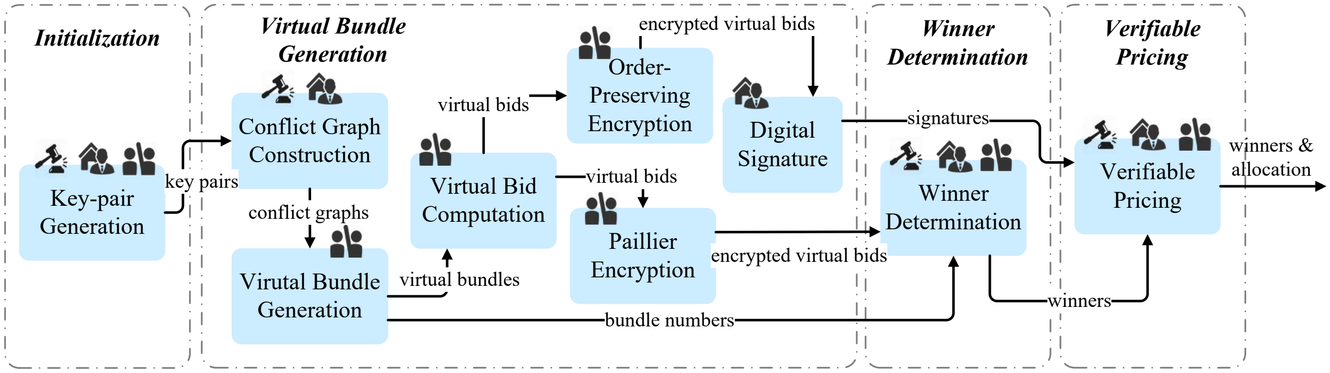


Fig. 2: System overview.

Meanwhile, spatial reusability is achieved among non-conflicted bidders. Virtual bundle generation consists of the following three steps.

4.1.1 Conflict Graph Construction

The interference area of channel s_k is represented by a circle with radius R_k. Two bidders, located at (x_i, y_i), (x_j, y_j) respectively, are in conflict if the following equation holds:

$$(x_i - x_j)^2 + (y_i - y_j)^2 \leq (2R_k)^2.$$

We use upper triangular matrices to represent conflict graphs. As shown in Alg. 5, the agent first collects all encrypted location information $\llbracket \mathcal{L} \rrbracket$ from bidders and iteratively selects three random numbers r_1, r_2 and r_3 for a pair of bidders to disturb $x_i - x_j$ and $y_i - y_j$. Based on the property of Paillier cryptosystem, the ciphertexts of $x_i - x_j + r_1$, $y_i - y_j + r_2$ and $2R_k + r_3$ can be obtained and sent to the auctioneer. Then, the auctioneer performs the square operation on the decrypted plaintexts, encrypts the result and returns it to the agent. Observing that $(x_i - x_j)^2 = (x_i - x_j + r_1)^2 - 2(x_1 - x_2)r_1 - r_1^2$, the agent can remove the noise and get DIS and RAD without decryption. By invoking primitive TwoCMPMin (Section 2.3.6), the comparison result of DIS and RAD is assigned to $\mathbb{G}^k_{i,j}$, where $\mathbb{G}^k_{i,j} = 1$ indicates that B_i and B_j are conflicted on channel s_k, while $\mathbb{G}^k_{i,j} = 0$ indicates otherwise.

After conflict graph construction, the agent permutes bidders' ID to prevent the auctioneer from linking the bidders' identity to their private information in subsequent operations. Without confusion, the bidders' IDs in the following contexts all refer to the permuted results. Along with the permuted IDs, the agent will notify bidders of the constructed conflict graphs.

4.1.2 Virtual Channel Generation

Based on the conflict graphs, each bidder generates her virtual bundle set b'_i and matrices $\mathcal{M}_i$ according to Alg. 6. Each original bundle $b_{i,d}$ is represented as an m-dimensional binary vector, where $b^k_{i,d} = 1$ indicates that channel s_k is in the bundle. For the original bundle $b_{i,d}$, we generate a virtual bundle $b'_{i,d}$ and a corresponding $m \times n$ matrix $\mathcal{M}_{i,d}$ in order to facilitate the following allocation calculation. If s_k is in $b_{i,d}$, for every conflicting buyer B_j who satisfies $\mathbb{G}^k_{i,j} = 1$, we set $\mathcal{M}^{k,j}_{i,d} = 1$ and add virtual channel $vc^k_{i,j}$ into the virtual bundle $b'_{i,d}$. Specially, we set $\mathcal{M}^{k,i}_{i,d} = 1$ (add $vc^k_{i,i}$ into $b'_{i,d}$ simultaneously) to ensure that each bidder can win at most one bundle.

Algorithm 6 Virtual Bundle Generation

```
Input: bundles set $b_i$, conflict graph $\mathbb{G}$
Output: virtual bundles set $b'_i$, virtual bundles matrices $\mathcal{M}_i$
each bidder initializes $b'_i = \mathcal{M}_i = \Phi$.
for each bundle $b_{i,d} \in b_i$ do
    for $k = 1$ to $m$ do
        if $s_k \in b_{i,d}$ then
            for $j = 1$ to $n$ do
                if $\mathbb{G}^k_{i,j} = 1$ then
                    $b'_{i,d} = \cup vc^k_{i,j}, \mathcal{M}^{k,j}_{i,d} = 1$.
                end if
            end for
        end if
    end for
end for
return $(b'_i, \mathcal{M}_i)$.
```

4.1.3 Virtual Bid Computation

After obtaining the virtual bundles, each bidder B_i computes her *virtual bids* $\psi_{i,d} = \frac{v_{i,d}}{\sqrt{|b'_{i,d}|}}$ and the number of bundles $\mathbb{B}_i = |b_i| = l_i$. With the symmetric key SK, bidders can encrypt their virtual bids as $\varphi_{i,d} = OPE.Enc(\psi_{i,d}, SK)$. Here, we assume that each virtual bid $\psi_{i,d}$ is unique and different from others[1].

For the subsequent winner determination, bidders send their order-preserving-encrypted virtual bids to the auctioneer and the agent. The agent also receives a set of the number of bundles $\mathbb{B}$. Based on the encrypted virtual bids, the agent generates signatures $\mathcal{SIG}(\varphi)$ blindly for the payment verification.

4.2 Secure Winner Determination

Taking social welfare into account, the auctioneer allocates the channels following the steps in Alg. 7. Note that to achieve optimal social welfare by the well-known VCG mechanism [4], [5] is proved to be NP-hard as the VCG mechanism can be reduced to the exact cover problem in polynomial time. Therefor, we turn to an alternative solution with greedy channel allocation to reach a tradeoff between the computational feasibility and efficiency.

We use an $m \times n$ matrix $\mathcal{A}$ to represent the allocation result, where $\mathcal{A}^{k,i} = 0$ if channel s_k has not been allocated to anyone

[1] We leave the case where there exist virtual bids with the same bidding values to our future work.

Algorithm 7 Secure Winner Determination

```
Input: order-preserving-encrypted virtual bids $\varphi$, signatures set
    $\mathcal{SIG}(\varphi)$ and bundle numbers set $\mathbb{B}$
Output: winners set $\mathcal{W}$ and allocation matrix $\mathcal{A}$
 1: initialize $\mathcal{W} = \Phi, \mathcal{A} = 0$.
    Auctioneer:
 2: sort $\varphi$ in a non-increasing order $\mathbb{L}_1$: $\varphi^1 \geq \varphi^2 \geq \cdots \geq \varphi^{|b|}$.
 3: for $r = 1$ to $|\varphi|$ following the order in $\mathbb{L}_1$ do
 4:     Auctioneer:
        inform the agent of winner candidate $B_i$ and the index of
        her candidate virtual bundle $d$.
        Agent:
 5:     ask the candidate $B_i$ for the corresponding encrypted can-
        didate virtual bundle matrix $[\![\mathcal{M}_{i,d}^r]\!]$.
 6:     compute and send $[\![\Pi]\!] = [\![\mathcal{M}_{i,d}^r \cdot \mathcal{A}]\!] = [\![\mathcal{M}_{i,d}^r]\!]^{\mathcal{A}}$ to the
        auctioneer.
        Auctioneer:
 7:     if decrypted $\Pi = 0$ then
 8:         $r = r + 1$.
            Agent:
 9:         set $\mathcal{A}' = \mathcal{A}$.
10:         update $\mathcal{A} = \mathcal{A} + \mathcal{M}_{i,d}^r$, $\mathcal{W} = \mathcal{W} \cup B_i$ and set $\varphi_i^{r'} =$
            $0, \forall r' > r$ in $\mathbb{L}_1$.
11:     else
12:         continue.
13:     end if
14:     obtain $p_i = \mathrm{VerifiablePricing}(r, \mathbb{L}_1, B_i^r, \mathbb{B}, \mathcal{A}', \mathcal{SIG}(\varphi))$.
15: end for
16: return $(\mathcal{W}, \mathcal{A})$.
```

who conflicts with bidder B_i on channel s_k, that is, channel s_k is still available for bidder B_i. To be specific, the auctioneer sorts φ in a non-increasing order $\mathbb{L}_1$, and informs the agent of the candidate winner following the order in $\mathbb{L}_1$. The agent grants the candidate winner bundle $b_{i,d}$ if the corresponding virtual bundle $b'_{i,d}$ has no virtual channel that has already been allocated. To check whether the virtual channels in a bundle $b'_{i,d}$ have been allocated, the agent computes the scalar product Π of $\mathcal{M}_{i,d}$ and $\mathcal{A}$ over the ciphertext, and sends the result to the auctioneer, who decrypts the result and returns the result to the agent if the bundle can be allocated to the candidate winner (the scalar product equals 0). After updating the allocation matrix and the winner set, the other virtual bids of winner B_i in $\mathbb{L}_1$ are removed, *i.e.*, each bidder can win at most one bundle. The payment p_i of the selected winner is computed according to Alg. 8. The auction results of each round of winner determination, including the allocation matrix $\mathcal{A}$ and the set of winning bidders $\mathcal{W}$, will not open until the auction ends. Note that, the final result allocates the actual bundles rather than the virtual ones to the winners. In fact, during the calculation, the i-th column of matrix $\mathcal{A}$ is enough to determine whether bidder B_i can be a winner, which can greatly reduce computational costs. A toy example is given for illustration.

Toy Example. Given the conflict graphs in Fig. 3, we can generate virtual bundle matrices $\mathcal{M}_{2,1}, \mathcal{M}_{3,1}$ and $\mathcal{M}_{4,1}$ by Alg. 6 (as shown in Table 3). We use character '$*$' to represent a set of numbers on a row or a column. When bundle $b_{3,1}$ becomes the first winning bundle, the allocation matrix $\mathcal{A}$ is updated with matrix $\mathcal{M}_{3,1}$ as shown in Table 3. In this case, bundle $b_{2,1}$ can never be granted as $\mathcal{M}_{2,1}^{*,2} \cdot \mathcal{A}^{*,2} = 1 \neq 0$, which means that $b_{2,1}$ includes virtual channels that have been allocated. This is verified by the conflict graphs in Fig. 3, which shows that channel s_2 can't be reused by buyer B_2 and B_3. In contrast, bundle $b_{4,1}$ can still be a winning bundle in the following allocation as $\mathcal{M}_{4,1}^{*,4} \cdot \mathcal{A}^{*,4} = 0$. This is consistent with the observation that B_3 and B_4 can reuse s_2. This toy example confirms that only one column of $\mathcal{M}$ and $\mathcal{A}$ are needed for winner determination in each iteration.

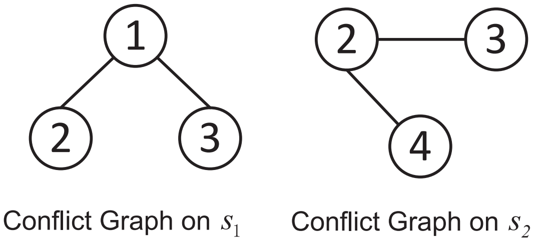


Fig. 3: A toy example: conflict graphs on s_1,s_2.

Bidder / Matrices		B_1	B_2	B_3	B_4
$\mathcal{M}_{2,1}$	s_1	1	1	0	0
	s_2	0	1	1	1
$\mathcal{M}_{3,1}$	s_1	1	0	1	0
	s_2	0	1	1	0
$\mathcal{M}_{4,1}$	s_1	0	0	0	0
	s_2	0	1	0	1
Updated $\mathcal{A}$	s_1	1	0	1	0
	s_2	0	1	1	0

TABLE 3: Virtual bundle matrices $\mathcal{M}_{2,1}, \mathcal{M}_{3,1}, \mathcal{M}_{4,1}$.

4.3 Verifiable Pricing

A winning bidder, say B_w, will pay her *critical price*, *i.e.*, the multiplication of ψ_{c,d_c} and $|b'_{w,d_w}|$, where ψ_{c,d_c} is the corresponding plaintext of φ_{c,d_c} that φ_{w,d_w} must exceed in order to make B_w a winner and b'_{w,d_w} is the corresponding virtual bundle of the winning bundle.

To obtain the critical price for winner B_w, the auctioneer and the agent cooperatively select the candidate critical bidder from the remaining non-winning bidders. This process is quite similar to line 4-13 in Alg. 7, but the conflict between the encrypted allocation matrix and candidate critical bundles is detected by bidders for privacy preservation. Once a candidate critical bidder B_c is determined, she will receive all encrypted bundles $[\![\mathcal{M}_w]\!]$ of winner B_w. Every time a bundle in b_w is found to be conflicted with the candidate critical bundle, we decrease the number of non-conflicting bundles of winner β by 1 until no bundle of B_w can be possibly granted, *i.e.*, $\beta = 0$. The last winner B_c who preempts B_w's bundle is the critical bidder of B_w. Based on the virtual bid ψ_{c,d_c} of B_c, the auctioneer calculates the payment p_w, encrypts it with B_w's public key pk_w and sends the result to B_w. After decrypting the payment with sk_w, B_w can verify the result by computing a payment with the recovered φ_{c,d_c} from the signature $\mathcal{SIG}(\varphi_{c,d_c})$. The winner can detect the fraud if the payment from the auctioneer is different from the computed payment.

5 Theoretical Analysis

In this section, we present the theoretical analysis in terms of truthfulness, social welfare, security and efficiency of ARMOR.

Algorithm 8 Verifiable Pricing

```
Input: ranking $r$, sorted norms $\mathbb{L}_1$, winner's ID $B_w$, bundle numbers set $\mathbb{B}$, allocation matrix $\mathcal{A}$ and signatures set $\mathcal{SIG}(\varphi)$
Output: winner $B_w$'s payment $p_w$
 1: set $\beta = \mathbb{B}_w$ and encrypt $\mathcal{A}$.
 2: agent ask for all encrypted virtual bundle matrices $\llbracket \mathcal{M}_w \rrbracket$ from the winner $B_w$.
    (1) Pricing $(r, \mathbb{L}_1, \mathcal{A})$:
 3: while $\beta \neq 0$ && $r < |\varphi|$ do
 4:     auctioneer informs the agent the ID $B_c^r$ and bundle index $d_c$ of the candidate critical bidder according to $\mathbb{L}_1$.
 5:     agent sends $\llbracket \mathcal{A} \rrbracket$ to bidder $B_c$ along with $d_c$.
 6:     $B_c$ computes and sends $\llbracket \Pi \rrbracket = \llbracket \mathcal{A} \rrbracket^{\mathcal{M}_{c,d_c}}$ to the auctioneer through the agent.
 7:     if $\Pi \neq 0$ then
 8:         $r = r + 1$, continue.
 9:     end if
10:     agent sends $\llbracket \mathcal{M}_w \rrbracket$ to $B_c$.
11:     for $d = 1$ to $\mathbb{B}_w$ do
12:         critical bidder $B_c$ computes $\llbracket \tau \rrbracket = \llbracket \mathcal{M}_{w,d_w} \rrbracket^{\mathcal{M}_{c,d_c}} = \llbracket \mathcal{M}_{w,d_w} \cdot \mathcal{M}_{c,d_c} \rrbracket$ and sends it to the auctioneer for decryption.
13:         if $\tau \neq 0$ then
14:             set $\beta = \beta - 1$, $\llbracket \mathcal{M}_{w,d} \rrbracket = 0$, $\llbracket \mathcal{A} \rrbracket = \llbracket \mathcal{A} \rrbracket \cdot \llbracket \mathcal{M}_{c,d_c} \rrbracket = \llbracket \mathcal{A} + \mathcal{M}_{c,d_c} \rrbracket$, break.
15:         end if
16:     end for
17:     $r = r + 1$.
18: end while
19: $B_c$ encrypts and indirectly sends $\llbracket \psi_{c,d_c} \rrbracket$ to the auctioneer.
20: auctioneer calculates $p_w = \psi_{c,d_c} \cdot \sqrt{|b'_{w,d_w}|}$, which is then encrypted by $B_w$'s public key $pk_w$ and sent back to bidder $B_w$ indirectly along with $\mathcal{SIG}(\varphi_{c,d_c})$.
21: return $p_w$.
    (2) Verification $(p_w)$:
22: bidder $B_w$ decrypts $\llbracket p_w \rrbracket$ with $sk_w$ and recovers $\varphi_{c,d_c}$ from $\mathcal{SIG}(\varphi_{c,d_c})$. Then, with the knowledge of encryption key $SK$, bidder $B_w$ can obtain $\psi_{c,d_c}$ by decrypting $\psi_{c,d_c} = OPE.Dec(\varphi_{c,d_c}, SK)$.
23: bidder $B_w$ notices that the payment is altered if $p_w > \psi_{c,d_c} \cdot \sqrt{|b'_{w,d_w}|}$.
```

5.1 Truthfulness and Social Welfare Analysis

Before we analyze the property of truthfulness of our scheme, we first formally give the definition of truthfulness, also known as *strategy-proofness*.

Definition 1. *A strategy-proof mechanism satisfies both* incentive compatibility *and* individual rationality*:*

- Incentive compatibility*: In an incentive compatible mechanism, the players are incentivized to tell the truth about their bidding values as truth-telling will maximize her utility regardless of other bidders' strategy profiles.*
- Individual rationality*: A mechanism is individually rational if every player gains no less utility when participating in the game than not participating in the game.*

Regarding the definition of truthfulness, we have the following theorem.

Theorem 1. *ARMOR is a strategy-proof combinatorial auction mechanism for heterogeneous channel allocation.*

Proof. First, we show that bidder B_i is incentive compatible, *i.e.*, she cannot obtain higher utility by bidding untruthfully. Since the utility of bidder B_i is:

$$u_i = \begin{cases} V_{i,d_i} - \frac{v_{j,d_j}}{\sqrt{|b'_{j,d_j}|}} \cdot \sqrt{|b'_{i,d_i}|}, & B_i \text{ is a winner} \\ 0. & \text{Otherwise} \end{cases}$$

where b_{i,d_i}, v_{j,d_j} and b_{j,d_j} are respectively stand for the winning bundle, bidding value for the critical bundle of B_i and the critical bundle of B_i. Therefore, there are two cases needed to be discussed:

- $\frac{V_{i,d_i}}{\sqrt{|b'_{i,d_i}|}} < \frac{v_{j,d_j}}{\sqrt{|b'_{j,d_j}|}}$. In this case, bidding truthfully, *i.e.*, $v_{i,d_i} = V_{i,d_i}$, brings in 0 utility for B_i as she lose the auction with a lower bidding value than B_j. Any untruthful bidding that not higher enough to beat B_j will not change the losing result of B_i as well her zero-utility. If she dishonestly bids v_{i,d_i} which is higher than $\frac{v_{j,d_j}}{\sqrt{|b'_{j,d_j}|}}$ and becomes a winner, her utility will be negative according to $u_i = V_{i,d_i} - p_i < 0$. Hence, bidders will not benefit from lying about her bidding value in this case.
- $\frac{V_{i,d_i}}{\sqrt{|b'_{i,d_i}|}} \geq \frac{v_{j,d_j}}{\sqrt{|b'_{j,d_j}|}}$. In this case, if B_i bids truthfully and becomes a winner, she will gain a positive utility. The same utility she will receive as long as her bid is not lower enough for her to lose the auction since her payment is only affected by her critical bidder's bid. Once she bids a lower bid than V_{i,d_i} and lose the auction, her utility becomes zero. Therefore, bidders will gain not extra profit from marking up or reducing the bidding value.

From the above two cases, bidders don't improve their utility by reporting a bidding value that not equal to their valuation, so our mechanism is incentive-compatible.

Second, we will show that our mechanism is individual rational. For a truthful bidder B_i, the equation $V_{i,d_i} = v_{i,d_i}$ holds. Under this condition, if she lose the auction, her utility is 0, otherwise, her utility satisfy $u_i = V_{i,d_i} - p_i = V_{i,d_i} - \frac{v_{j,d_j}}{\sqrt{|b'_{j,d_j}|}} \cdot \sqrt{|b'_{i,d_i}|}$. Since B_j is the critical bidder of B_i, the order-preserving-encrypted virtual bid of critical bundle φ_{j,d_j} must be behind that of B_i's winning bundle φ_{i,d_i} in the ordered list $\mathbb{L}_1$, which implies that $\psi_{i,d_i} = \frac{v_{i,d}}{\sqrt{|b'_{i,d_i}|}} = \frac{V_{i,d_i}}{\sqrt{|b'_{i,d_i}|}} > \frac{v_{j,d_j}}{\sqrt{|b'_{j,d_j}|}} = \psi_{j,d_j}$. Hence, a truthful bidder's utility is anyhow greater than 0.

Combining the two properties proved above, the bidders are rational to be strategy-proof, *i.e.*, truthful, so we can conclude that our mechanism is strategy-proof. □

ARMOR can also ensure truthfulness on bundles. Bidders may lie about their bundles for two reasons. First, at line 5 in Alg. 7, the candidate winner is asked for her candidate winning bundle, which will be successfully allocated only if no conflict is detected. Since the candidate winner does not know the current allocation matrix, she cannot manipulate the bundle to ensure a utility gain. Second, the candidate critical bidders may cheat on their bundles when they conduct conflict detection in verifiable pricing (line 6 and line 12 in Alg. 8). However, they have no incentives to tamper with the result which brings no utility gain. To sum up, our scheme ensures that bidders will be truthful about their bundles.

Apart from the truthfulness of bidders, ARMOR can also ensure the truthfulness of auctioneer in terms of price determination, *i.e.*, prevent the auctioneer from forging prices. As winners can verify the price, the auctioneer is forced to be truthful, since she is unable to generate the signature without a signing private key.

Theorem 2. *The approximation ratio of maximum social welfare of ARMOR is $\mathcal{O}(\zeta m)$, where ζ is the maximum degree of conflict graphs and m is the number of channels.*

Proof. Let $\mathbb{D}_{OPT}$ be the optimal spectrum allocation, and $\mathbb{D}_{ARM}$ be the allocation by ARMOR. The social welfare of the optimal solution and ARMOR are $\sum_{(i,d_i)\in\mathbb{D}_{OPT}} V_{i,d_i}$ and $\sum_{(i,d_i)\in\mathbb{D}_{ARM}} V_{i,d_i}$ respectively.

For each bundle $b'_{i,d_i} \in \mathbb{D}_{ARM}$, we use $\mathbb{D}_{OPT}^{(i,d_i)}$ to represent the set of bundles in $\mathbb{D}_{OPT}$ that cannot be selected as the winning bundles due to the existence of b'_{i,d_i}. For truthful buyers, $\mathbb{D}_{OPT}^{(i,d_i)}$ can be formally defined as

$$\mathbb{D}_{OPT}^{(i,d_i)} \triangleq \{(j,d_j) \in \mathbb{D}_{OPT} | \frac{V_{j,d_j}}{\sqrt{|b'_{j,d_j}|}} \le \frac{V_{i,d_i}}{\sqrt{|b'_{i,d_i}|}}, \\ (b'_{j,d_j} \cap b'_{i,d_i} \neq \Phi)\}.$$

Note that, for the convenience of expression, we replace φ with corresponding ψ before the order-preserving encryption, where this inequality still holds. As $\mathbb{L}_1$ is sorted by the order of φ, φ_{j,d_j} of every $b'_{j,d_j} \in \mathbb{D}_{OPT}^{(i,d_i)}$ appears after φ_{i,d_i} in the ordered list $\mathbb{L}_1$,

$$V_{j,d_j} \le \frac{V_{i,d_i} \times \sqrt{|b'_{j,d_j}|}}{\sqrt{|b'_{i,d_i}|}}.$$

Thus, we can compute

$$\sum_{(j,d_j)\in\mathbb{D}_{OPT}^{(i,d_i)}} V_{j,d_j} \le \frac{V_{i,d_i}}{\sqrt{|b'_{i,d_i}|}} \sum_{(j,d_j)\in\mathbb{D}_{OPT}^{(i,d_i)}} \sqrt{|b'_{j,d_j}|}. \quad (1)$$

Referring to the Cauchy-Schwarz inequality, we can bound

$$\sum_{(j,d_j)\in\mathbb{D}_{OPT}^{(i,d_i)}} \sqrt{|b'_{j,d_j}|} \le \sqrt{|\mathbb{D}_{OPT}^{(i,d_i)}|} \sqrt{\sum_{(j,d_j)\in\mathbb{D}_{OPT}^{(i,d_i)}} |b'_{j,d_j}|}. \quad (2)$$

By combining (1) and (2), we have

$$\sum_{(j,d_j)\in\mathbb{D}_{OPT}^{(i,d_i)}} V_{j,d_j} \le \frac{V_{i,d_i}\sqrt{|\mathbb{D}_{OPT}^{(i,d_i)}|}\sqrt{\sum_{(j,d_j)\in\mathbb{D}_{OPT}^{(i,d_i)}} |b'_{j,d_j}|}}{\sqrt{|b'_{i,d_i}|}}. \quad (3)$$

According to the exclusive usage constraint, no pair of virtual bundles in the optimal allocation should contain the same channel, *i.e.*, $\forall b'_{i,d_i}, b'_{j,d_j} \in \mathbb{D}_{OPT}$, $b'_{i,d_i} \cap b'_{j,d_j} = \Phi$. Thus, every bundle in $\mathbb{D}_{OPT}^{(i,d_i)}$ intersects with $b'_{i,d_i} \in \mathbb{D}_{ARM}$ at least one virtual channel. Since each bidder can win at most one bundle, only one other bundle of B_i may be included into $\mathbb{D}_{OPT}^{(i,d_i)}$. As a result, there are at most $|b'_{i,d_i}| + 1$ bundles in $\mathbb{D}_{OPT}^{(i,d_i)}$

$$|\mathbb{D}_{OPT}^{(i,d_i)}| \le |b'_{i,d_i}| + 1 \Rightarrow \sqrt{|\mathbb{D}_{OPT}^{(i,d_i)}|} \le \sqrt{|b'_{i,d_i}| + 1}. \quad (4)$$

Since the virtual bundle size is no greater than $(\zeta + 1)m$, we can also derive

$$\sum_{(j,d_j)\in\mathbb{D}_{OPT}^{(i,d_i)}} |b'_{j,d_j}| \le [(\zeta + 1)m + 1] \times (\zeta + 1)m. \quad (5)$$

By integrating (3), (4) and (5), we have

$$\sum_{(j,d_j)\in\mathbb{D}_{OPT}^{(i,d_i)}} V_{j,d_j} \le [(\zeta + 1)m + 1]V_{i,d_i}.$$

Since $\mathbb{D}_{OPT} = \cup_{(i,d_i)\in\mathbb{D}_{ARM}} \mathbb{D}_{OPT}^{(i,d_i)}$, we can finally obtain

$$\begin{aligned}\sum_{(i,d_i)\in\mathbb{D}_{OPT}} V_{i,d_i} &\le \sum_{(i,d_i)\in\mathbb{D}_{ARM}} \sum_{(j,d_j)\in\mathbb{D}_{OPT}^{(i,d_i)}} V_{j,d_j} \\ &\le [(\zeta + 1)m + 1] \sum_{(i,d_i)\in\mathbb{D}_{ARM}} V_{i,d_i}.\end{aligned}$$

Hence, the social welfare approximation ratio of ARMOR is $\mathcal{O}(\zeta m)$. □

5.2 Security Analysis

ARMOR can protect the private information of bidders, especially the location information and bid values, under the adversarial model in Section 2.1. We first introduce the following lemma which helps to prove that ARMOR is secure against semi-honest adversaries.

Lemma 1. *Assume that Alice runs the key generation algorithm for a semantically-secure homomorphic encryption scheme, and publishes the public key to Bob. Further assume that Alice and Bob run Protocol X, for which all messages passed from Bob to Alice are uniformly distributed (in the ciphertext range) and independent of Bob's inputs, and all messages passed from Alice to Bob are encrypted using the encryption scheme. Then protocol X is secure against semi-honest adversaries.*

To proof Lemma 1, we first present a formal definition of security against the semi-honest adversaries as follows [24].

Definition 2. *Suppose that protocol Λ has Alice (resp. Bob) compute and output the function $f^A(x, y)$ (resp. $f^B(x, y)$), where (x, y) are the inputs of Alice and Bob, respectively. Let $VIEW_A^\Lambda(x, y)$ (resp. $VIEW_B^\Lambda(x, y)$) represent Alice's (resp. Bob's) view during an execution of Λ on (x, y). In other words, if (x, r^A) (resp. (x, r^B)) are Alice's (resp. Bob's) input and randomness, then*

$$VIEW_A^\Lambda(x, y) = (x, r^A, m_1, ..., m_t), \\ VIEW_B^\Lambda(x, y) = (y, r^B, m_1, ..., m_t),$$

where $\{m_i\}$ denote the messages passed between Alice and Bob. Let $O_A^\Lambda(x, y)$ (resp.$O_B^\Lambda(x, y)$) denote the output of Alice (resp. Bob). We say that protocol Λ is secure against semi-honest adversaries if there exist probabilistic polynomial-time (PPT) simulators S_1 and S_2 such that

$$\{(S_1(x, f^A(x, y)), f^B(x, y))\} \overset{c}{\equiv} \{VIEW_A^\Lambda(x, y), O_B^\Lambda(x, y)\}, \quad (6)$$

$$\{(S_2(y, f^B(x, y)), f^A(x, y))\} \overset{c}{\equiv} \{VIEW_B^\Lambda(x, y), O_A^\Lambda(x, y)\}, \quad (7)$$

where $\overset{c}{\equiv}$ denotes computational indistinguishability.

Now, we can prove Lemma 1 based on the above given definition.

Proof. To prove security, we consider the following two cases, where the party corrupted by the adversary is different.

Case 1: Alice is corrupted. We can simulate the messages sent from Bob to Alice. Every time Bob intends to send an encrypted message to Alice, we have simulator S_1 pick and encrypt a random element from $\mathbb{Z}_n$, and send it to Alice. Eq. (6) holds due to the fact that Alice cannot distinguish the random element (chosen by S_1) from the original one that is randomized by Bob.

Case 2: Bob is corrupted. We can simulate the messages sent from Alice to Bob. For each encrypted message that Alice intends to send to Bob, we have simulator S_2 pick and encrypt a random element from $\mathbb{Z}_n$, and send it to Bob. Eq. (7) holds due to the fact that no such PPT adversary can break the security assumptions of the encryption scheme that Alice adopts.

Based on the analysis of these two cases, we can conclude that protocol Λ is secure against semi-honest adversaries. □

In the next subsections, we will show that all steps in our auction construction satisfy Lemma 1 such that ARMOR is secure against semi-honest adversaries. Moreover, the privacy leakage to rational and selfish bidders, who can be regarded as adversaries, has also been discussed.

5.2.1 Location Information

The location information of bidders is used in Alg. 5 for the auctioneer and agent to jointly construct a conflict graph. In our construction, we employ the Paillier cryptosystem [25]–[27] to encrypt the location information.

Based on Lemma 1, the auctioneer and the agent can be viewed as Alice and Bob respectively. In Alg. 5, the messages sent from the auctioneer are encrypted by semantically-secure homomorphic encryption scheme, while the messages sent from the agent are uniformly distributed in the ciphertext space (and the corresponding decrypted messages are blinded by the randomness [28]). Moreover, the primitive TwoCMPMin invoked in Alg. 5 mainly leverages the garbled circuits which have been proved to be secure against semi-honest adversaries. Thus, Alg. 5 is secure against semi-honest adversaries based on Lemma 1. Furthermore, during the auction, no bidder has access to other bidders' location information. Therefore, the location information is secure against all adversaries in our construction.

5.2.2 Bids

The bid of a bidder contains both the bundles and bidding values, which are both preserved in our scheme.

Bundles. First, the bundles are secure against the auctioneer who has no access to the bundles during the whole auction. Second, the agent and the candidate critical bidders who receive some encrypted bundles of winning bidders cannot learn the content in these bundles without the decryption key. The winning bundles will be decrypted by the auctioneer and sent to the agent for allocation matrix update. These bundles are expected to be publicized as part of the auction results, thus there is no information leakage. Hence, the bundles are secure against the adversarial model in our scheme.

	Computation Overheads
Virtual Bundle	$\mathcal{O}(\lvert\mathcal{D}\rvert \cdot m \cdot n^2)$
Winner Determination	$\mathcal{O}(\lvert\mathcal{W}\rvert \cdot m \cdot n)$
Verifiable Pricing	$\mathcal{O}(\lvert\mathcal{W}\rvert \cdot l_w^2 \cdot m \cdot n)$
ARMOR	$\max(\mathcal{O}(\lvert\mathcal{D}\rvert \cdot m \cdot n^2), \mathcal{O}(\lvert\mathcal{W}\rvert \cdot l_w^2 \cdot m \cdot n))$

TABLE 4: Computation Overheads.

Bidding Values. The agent has the order-preserving-encrypted virtual bids φ, the set of the numbers of bundles $\mathbb{B}$, the encrypted virtual bids $[\![\psi_{c,d_c}]\!]$ of the critical bidders and the encrypted payment $[\![p_i]\!]$ of winners, but she cannot derive the virtual bid ψ without the OPE encryption key, the Paillier decryption key or the bidders' private key, thus she cannot access the real bidding values. The auctioneer can decrypt and obtain the virtual bid ψ_{c,d_c} of the critical bidder for price determination, but she can learn nothing about the virtual bundle size $|b'_{c,d_c}|$, which is necessary for bidding value recovery. The knowledge of winning bundle' size $|b_{w,d_w}|$ will not help the auctioneer infer the bidding value since she does not have SK to decrypt φ_{w,d_w} to get ψ_{w,d_w}. Similarly, no bidder can figure out the bidding values of other bidders without knowing the bundle sizes. Even if the auctioneer or the winner has deduced the actual bidding values by enumerating possible bundle sizes, the bidders' identities are masked by the agent in the ciphertext space (and the corresponding decrypted messages are blinded by the randomness [28]), making it hard to establish the relationship between the virtual bids and the corresponding critical bidder. To sum up, the bidding values of all bidders are secure against all adversaries in our construction.

In conclusion, ARMOR is privacy preserving, *i.e.*, secure against the adversarial models introduced in Section 2.1.

5.3 Efficiency

We separately investigate the computation and communication overheads in each phase of ARMOR and summarize the overall online overheads.

5.3.1 Computation Overheads

The computation complexities in each step are given in Table 4. During virtual bundle generation, the main computation is to detect the conflict relationship of every pair of bidders on each channel in each bundle (Alg. 6), resulting in a time complexity of $\mathcal{O}(|\mathcal{D}| \cdot m \cdot n^2)$. Updating allocation matrix leads to an $\mathcal{O}(|\mathcal{W}| \cdot m \cdot n)$ computation complexity for winner determination. In verifiable pricing, the conflict detection costs $\mathcal{O}(l_w \cdot |\mathcal{D}| \cdot m)$ computational time at the worst case. However, the actual number of iterations will be much fewer than $|\mathcal{D}|$ due to the decreasing number of non-winning bidders and the loop will terminate whenever a conflict happens. Hence, we consider updating encrypted allocation matrix as the dominant time-consuming process, resulting in $\mathcal{O}(|\mathcal{W}| \cdot l_w^2 \cdot m \cdot n)$ time complexity for verifiable pricing. In summary, the overall computation complexity of ARMOR is the maximum value between $\mathcal{O}(|\mathcal{D}| \cdot m \cdot n^2)$ and $\mathcal{O}(|\mathcal{W}| \cdot l_w^2 \cdot m \cdot n)$.

5.3.2 Communication Overheads

The communication overheads of ARMOR are demonstrated in Table 5, where bit_p is the length of the ciphertext and the signature (we consider the lengths to be the same by default). To construct the conflict graphs, the auctioneer and the agent exchange encrypted messages of each pair of bidders on all channels, which incurs $\mathcal{O}(bit_p \cdot mn^2)$ communication overheads. After obtaining the $\mathcal{O}(m \cdot n^2)$ conflict graphs from the agent, the virtual bundle generation is performed by bidders themselves. In winner determination, each candidate winner sends $\mathcal{O}(bit_p \cdot m \cdot n)$ encrypted bundle to the agent for conflict detection, among which only $|\mathcal{W}|$ of them will be relayed to the auctioneer for decryption as the winning bundle. Thus, the auctioneer's communication overhead is $\mathcal{O}(|\mathcal{W}| \cdot bit_p \cdot mn)$ while the communication overheads of both the agent and bidders are $\mathcal{O}(|\mathcal{D}| \cdot bit_p \cdot mn)$. In order to find the critical bidder, each

	Auctioneer	Agent	Bidders
VB	$\mathcal{O}(bit_p \cdot mn^2)$	$\mathcal{O}(bit_p \cdot mn^2)$	$\mathcal{O}(m \cdot n^2)$
WD	$\mathcal{O}(\|\mathcal{W}\| \cdot bit_p \cdot mn)$	$\mathcal{O}(\|\mathcal{D}\| \cdot bit_p \cdot mn)$	$\mathcal{O}(\|\mathcal{D}\| \cdot bit_p \cdot mn)$
VP	$\mathcal{O}(\|\mathcal{W}\|\|\mathcal{D}\| \cdot l_w \cdot bit_p)$	$\mathcal{O}(\|\mathcal{W}\|\|\mathcal{D}\|l_w \cdot bit_p \cdot mn)$	$\mathcal{O}(\|\mathcal{W}\|\|\mathcal{D}\|l_w \cdot bit_p \cdot mn)$

TABLE 5: Communication Overheads.

winner submits the encrypted bundles to the agent who will then transmit theses ciphertexts to the candidate critical bidders, which incurs $\mathcal{O}(|\mathcal{W}| \cdot |\mathcal{D}| \cdot l_w \cdot bit_p \cdot mn)$ communication overhead. The auctioneer only receives $\mathcal{O}(|\mathcal{W}| \cdot |\mathcal{D}| \cdot l_w \cdot bit_p)$ encrypted scalar products in this step.

6 Performance Evaluation

6.1 Simulation Setup

We have implemented ARMOR in Windows 10 operating system with an Intel Core i5-6400 CPU at 2.70GHz processor and 4GB RAM, and experimented on Eclipse with JRE 1.8. We use both Paillier encryption and RSA cryptosystem with a 1024-bit modulus. In the blinded Nyberg-Rueppel signature algorithm, the bit lengths p and q are 1024-bit and 160-bit respectively according to the Digital Signature Standard (DSS) [29]. We implement OPE scheme based on AES with 128-bit key length, and 80-bit wire labels for garbled circuits, which means that a security level of 80-bit is provided.

Bidders are randomly distributed in an area of 2000m×2000m, whose amount increases from 10 to 100 with 10 as a unit. The number of channels, whose interference range are randomly spanning from 50m to 150m, is set to be one of the three values: 6, 12 and 24. The bidding value of each bidder is randomly chosen from (0,1]. We also compare the case of single-minded bidder, *i.e.*, each bidder can only submit one bundle, and multi-minded bidders who can submit at most 3 bundles, denoted by $\Phi = 1$ and $\Phi = 3$ respectively. The bit length (ρ_1, ρ_2) in the garbled circuits is set to be (54,24), each of which can grow with 10 until (94,64). The results are averaged over 200 runs.

6.2 Experiment Results

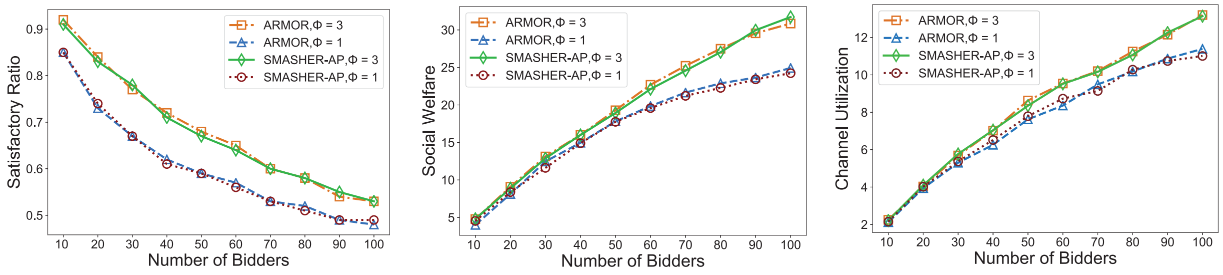
We compare ARMOR with SMASHER-AP [2], a strategy-proof combinatorial heterogeneous channel auction without privacy preservation, in terms of social efficiency, *i.e.*, satisfactory ratio, social welfare and channel utilization. Satisfactory ratio is the percentage of winning bidders, social welfare is the sum of valuations of winners on their allocated goods and channel utilization is the percentage of the total channels that all winners get allocated.

Fig. 4 shows that, with the growth of the number of bidders, the satisfactory ratio decreases due to severe competition on limited channels. Nevertheless, social welfare and channel utilization increase as there are more winners and additional channels. Fig. 5 demonstrates that a larger supply of channels will improve both the satisfactory ratio and the social welfare but make a dent in channel utilization since the excessive provision results in inadequate utilization. Moreover, submitting multiple bundle requests will up the odds of winning, so the satisfactory ratio, social welfare and channel utilization of multi-minded bidders are greater than those of single-minded bidders. In general, Fig. 4 and Fig. 5 show that ARMOR can effectively preserve the social efficiency of the original auction mechanism.

Table 6 demonstrates the computation and communication overheads of each party, where all bidders are considered as a whole. It is obvious that virtual bundle generation accounts for a vast majority of computation and communication overheads since the procedure of traversing all requested bundles of each bidder is time-consuming, and the involved complex ciphertext operation induces more computation and communication overheads. Even so, the bidders, who undertake most of the calculations in virtual bundle generation, each spends no more than 12.26 seconds on average. We can observe that the total computation time of virtual bundle generation is slightly lower than the sum of computation time of all parties, since we adopt the concurrent computation that allows different parties to perform certain computations concurrently, instead of sequentially (one party can only start after another party finishes her computation) during the conflict graph construction. The auctioneer spends a great deal of time on decrypting encrypted bundles for winner determination while the agent is subject to updating the encrypted allocation matrix in verifiable pricing. Bidders devote themselves to generating the virtual bundles. To prevent the risk of information leakages caused by direct communication between bidders and the auctioneer, the agent serves as a middle man, whose communication overheads is the same as the total communication overhead. It is shown that ARMOR can allocate 24 channels among 80 bidders in 44.34 minutes with 201.1 MB communication overheads in total, which is acceptable for a strong and comprehensive protection on bidders' private information.

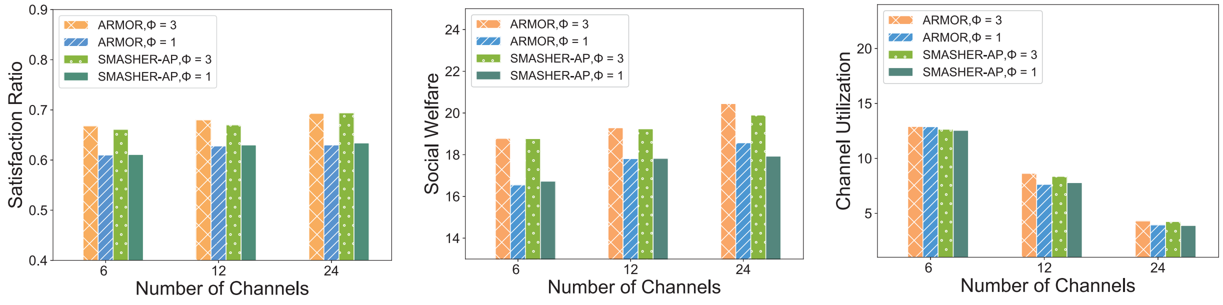
Fig. 6 and Fig. 7 illustrate the computation and communication overheads of each party in ARMOR. In Fig. 6(a), more bidders will request more bundles, leading to a longer processing time of virtual bundle generation, which is the determinant for the growth of time for bidders. Since the number of channels is fixed, it takes the auctioneer and the agent almost a constant amount of time to construct conflict graphs, but they will spend an increasing amount of time on winner and price determination as there are more bidders. Thus, the total computation overhead grows dramatically when bidder number is climbing. Fig. 6(b) confirms that the communication cost of bidders is increasing when there are more participating bidders due to submission of encrypted virtual bundles, and the auctioneer's communication cost is also increasing because of more candidate winners for winner and price determination. As a proxy between the auctioneer and the bidders, the communication overhead of the agent is identical to that of overall communication overhead.

As shown in Fig. 7(a), the bit length of garbled circuits almost has no influence the computation overheads. It is because that garbled circuits are only invoked in conflict graph construction, which is not the dominant time-consuming computation step in our design. Similarly, the auctioneer and agent are devoted to winner determination and verifiable pricing respectively such that the time increment over conflict graph construction can not be observed evidently. The fluctuation of their time costs can be attributed to the varied number of bundles. Bidders' computation overheads are also unaffected since they are not involved in conflict graph construction. By contrast, with the increment of the bit length of garbled circuits, the growth of communication overheads is more prominent as depicted in Fig. 7(b), since conflict graph construction incurs a high communication cost. As bidders are not involved in building conflict graphs, their communication overheads are not affected by the bit length of garbled circuit. The mild fluctuation is due to randomness of the number of requested



(a) (b) (c)

Fig. 4: Social efficiency comparison, $m = 12$. (a) satisfactory ratio; (b) social welfare; (c) channel utilization.

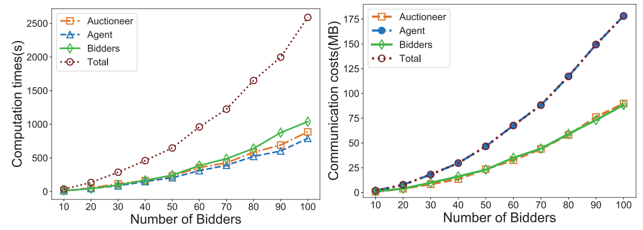


(a) (b) (c)

Fig. 5: Social efficiency comparison, $n = 50$. (a) satisfactory ratio; (b) social welfare; (c) channel utilization.

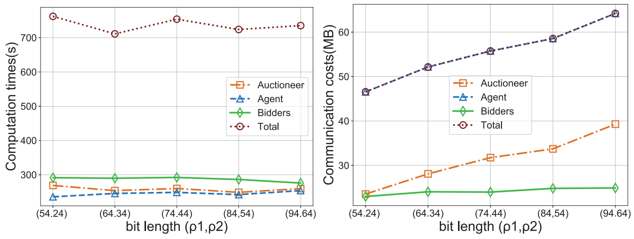
		Virtual Bundle Generation				Winner Determination				Verifiable Pricing				Total
		Auc.	Agt.	Bd.	Overall	Auc.	Agt.	Bd.	Overall	Auc.	Agt.	Bd.	Overall	
$m = 6$	Comp.	5.85	6.49	19.78	26.27	17.73	2.25	0	19.98	5.61	20.51	6.03	31.82	78.07
$n = 20$	Comm.	2.76	2.79	0.03	2.79	0.18	0.79	0.76	0.8	0.16	1.36	1.19	1.36	4.95
$m = 12$	Comp.	43.99	47.31	265.77	313.08	203.79	5.90	0	209.74	31.12	182.89	35.69	249.75	772.39
$n = 50$	Comm.	22.50	22.68	0.18	22.68	0.26	10.52	10.31	10.52	0.80	13.33	12.53	13.34	46.59
$m = 24$	Comp.	142.43	129.59	981.08	1110.67	693.78	30.41	0	724.19	44.78	750.58	74.78	825.37	2660.23
$n = 80$	Comm.	85.42	86.14	0.72	86.14	1.11	61.75	60.64	61.76	1.80	53.19	51.40	53.20	201.10

TABLE 6: The computation (second) and communication (MB) overheads of ARMOR.



(a) (b)

Fig. 6: Computation and communication overheads of ARMOR, $m = 12$. (a) computation times; (b) communication costs.



(a) (b)

Fig. 7: Computation and communication overheads of ARMOR, $n = 50, m = 12$. (a) computation times; (b) communication costs.

bundles in each round.

In conclusion, the simulation results demonstrate that ARMOR can maintain the social efficiency of the combinatorial auction, while offering an all-round strong protection on bidder's privacy with acceptable costs.

7 Related Work

Combinatorial Auction. Combinatorial auctions have been extensively studied in recent years [1], [2], [30]–[32] for a growing interest in combinatorial bidding. To achieve truthfulness, VERITA [32] has designed a greedy allocation algorithm that charges bidders according to their critical price. However, Wu *et al.* [33] showed that the allocation scheme in [32] fails to address social welfare maximization, which is proved to be NP-hard in most generic combinatorial auction design. On the account of this, a great number of works [30], [31], [34]–[36] have studied the social welfare optimization problems in combinatorial auction. Diverse local search algorithms were proposed in [30], [31], [36] for solving the winner determination problem in combinatorial auctions. References [30], [31] chose to sacrifice economic robustness in exchange for a reduced computation complexity, but they only achieved approximate truthfulness. Moreover, none of these works can be applied to spectrum auction since they did not consider spatial reusability. Several strategy-proof spectrum auctions have achieved bounded approximation ratios on social welfare [1], [2], [31]. Apart from auction, several spectrum matching frameworks are also proposed for spectrum allocation [37]–[39]. Despite the efforts of existing works on combinatorial auctions, none of them considered privacy preservation, posing potential security risks for participating bidders.

Privacy-Preserving Auctions. Various privacy-preserving auction mechanisms have been proposed [3], [11]–[13], [16], [40], [41]. Yokoo *et al.* [3] and Hu *et al.* [41] designed privacy-preserving combinatorial auctions based on homomorphic encryption and secret sharing respectively, but they both considered conventional goods, thus cannot be applied to spectrum auctions that feature spatial reuse. SPRING [16] is the first strategy-proof and privacy-preserving spectrum auction scheme, and PASS [40] is the first differentially-private spectrum auction scheme with approximate revenue maximization. By leveraging homomorphic encryption, [12], [13], [42] are designed to protect bidder privacy in homogeneous spectrum auctions. Considering spectrum heterogeneity, THEMIS [11] can prevent untrustworthy auctioneer from fraud and bid-rigging, but has introduced high computation overheads since bidders are required to bid for every possible spectrum allocation. To tackle this problem, Pan *et al.* [15] proposed SCSA, a combinatorial auction scheme that uses homomorphic encryption and secret sharing to distribute the share of secret key among bidders. However, SCSA adopts a VCG-based pricing approach, which is no longer strategy-proof in case of multi-minded bidders. Moreover, all these existing privacy-preserving auction mechanisms fail to provide sufficient protection for bidders' location information.

8 Conclusion and Future Works

In this paper, we have presented ARMOR, the first truthful and privacy-preserving combinatorial auction mechanism that can achieve a strong and comprehensive protection on bidders private information while preserving the allocation efficiency of the combinatorial auction. We have leveraged homomorphic encryption, order-preserving encryption, garbled circuits and digital signature to ensure security in every step of the auction. We have implemented and extensively evaluate the performance of ARMOR. The simulation results confirm that ARMOR achieves almost the same allocation efficiency as the benchmark combinatorial auction mechanism, while achieving privacy preservation with acceptable computation and communication overheads. In our future works, we will further strengthen the truthfulness and privacy preservation in combinatorial spectrum auctions, as well as deal with bidding tie among bidders and collusion among auction participants.

Acknowledgments

Yanjiao's research is supported in part by the National Natural Science Foundation of China under Grant 61702380, in part by the Hubei Provincial Natural Science Foundation of China under Grant 2017CFB134, and in part by the Hubei Provincial Technological Innovation Special Funding Major Projects under Grant 2017AAA125. Qian's research is supported in part by the National Natural Science Foundation of China (Grant Nos. 61822207 and U1636219), in part by Equipment Pre-Research Joint Fund of Ministry of Education of China (Youth Talent), and in part by the Outstanding Youth Foundation of Hubei Province under Grant 2017CFA047. Qi's research is supported by the National Natural Science Foundation of China (Grant Nos. 61572278 and U1736209). *(Corresponding author: Qian Wang.)*

References

[1] M. Dong, G. Sun, X. Wang, and Q. Zhang, "Combinatorial auction with time-frequency flexibility in cognitive radio networks," in *Proc. of INFOCOM'12*. IEEE, 2012, pp. 2282–2290.

[2] Z. Zheng, F. Wu, and G. Chen, "A strategy-proof combinatorial heterogeneous channel auction framework in noncooperative wireless networks," *IEEE Transactions on Mobile Computing*, vol. 14, no. 6, pp. 1123–1137, 2015.

[3] M. Yokoo and K. Suzuki, "Secure multi-agent dynamic programming based on homomorphic encryption and its application to combinatorial auctions," in *Proc. of AAMS'02*. Springer, 2002, pp. 112–119.

[4] K. Suzuki and M. Yokoo, "Secure generalized vickrey auction using homomorphic encryption," in *Proc. of FC'03*. Springer, 2003, pp. 239–249.

[5] M. Yokoo and K. Suzuki, "Secure generalized vickrey auction without third-party servers," in *Proc. of FC'04*. Springer, 2004, pp. 132–146.

[6] F. Brandt and T. Sandholm, "On the existence of unconditionally privacy-preserving auction protocols," *IEEE Transactions on Information and System Security*, no. 2, p. 6, 2008.

[7] T. Jung, X. Li, L. Zhang, and H. Huang, "Efficient, verifiable and privacy-preserving combinatorial auction design," *CoRR*, vol. abs/1308.6202, 2013.

[8] M. Nojoumian and D. R. Stinson, "Efficient sealed-bid auction protocols using verifiable secret sharing," in *Proc. of LNCS'14*. Springer, 2014, pp. 302–317.

[9] T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," in *Proc. of CRYPTO'91*. Springer, 1991, pp. 129–140.

[10] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

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

[12] H. Huang, X. Li, Y. Sun, and H. Xu, "PPS: Privacy-preserving s-trategyproof social-efficient spectrum auction mechanisms," *IEEE/ACM Transactions on Networking*, vol. 26, no. 5, pp. 1393–1404, 2013.

[13] F. Wu, Q. Huang, Y. Tao, and G. Chen, "Towards privacy preservation in strategy-proof spectrum auction mechanisms for noncooperative wireless networks," *IEEE/ACM Transactions on Networking*, vol. 23, no. 4, pp. 1271–1285, 2015.

[14] Q. Huang, Y. Gui, F. Wu, and G. Chen, "A general privacy-preserving auction mechanism for secondary spectrum markets," *IEEE/ACM Transactions on Networking*, vol. 24, no. 3, pp. 1881–1893, 2015.

[15] M. Pan, X. Zhu, and Y. Fang, "Using homomorphic encryption to secure the combinatorial spectrum auction without the trustworthy auctioneer," *Wireless Networks*, vol. 18, no. 2, pp. 113–128, 2012.

[16] Q. Huang, Y. Tao, and F. Wu, "Spring: A strategy-proof and privacy preserving spectrum auction mechanism," in *Proc. of INFOCOM'13*. IEEE, 2013, pp. 827–835.

[17] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proc. of EUROCRYPT'99*. Springer, 1999, pp. 223–238.

[18] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order preserving encryption for numeric data," in *Proc. of SIGMOD'04*. ACM, 2004, pp. 563–574.

[19] A. C. Yao, "Protocols for secure computations," in *Proc. of FOCS'82*. IEEE, 1982, pp. 160–164.

[20] M. O. Rabin, "How to exchange secrets with oblivious transfer." *IACR Cryptology ePrint Archive*, vol. 2005, p. 187, 2005.

[21] J. Camenisch, J.-M. Piveteau, and M. Stadler, "Blind signatures based on the discrete logarithm problem," in *Proc. of EUROCRYPT'95*. Springer, 1995, pp. 428–432.

[22] R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[23] V. Kolesnikov, A. R. Sadeghi, and T. Schneider, “Improved garbled circuit building blocks and applications to auctions and computing minima,” in *Proc. of ACNS’09*. Springer, 2009, pp. 1–20.

[24] O. Goldreich, *Foundations of cryptography: volume 2, basic applications*. Cambridge university press, 2009.

[25] Q. Wang, M. He, M. Du, S. S. M. Chow, R. W. F. Lai, and Q. Zou, “Searchable encryption over feature-rich data,” *IEEE Transactions on Dependable and Secure Computing*, vol. 15, pp. 496–510, 2016.

[26] S. Hu, Q. Wang, J. Wang, Z. Qin, and K. Ren, “Securing sift: Privacy-preserving outsourcing computation of feature extractions over encrypted image data,” *IEEE Transactions on Image Processing*, vol. 25, no. 7, pp. 3411–3425, 2016.

[27] Q. Wang, M. Du, X. Chen, Y. Chen, P. Zhou, X. Chen, and X. Huang, “Privacy-preserving collaborative model learning: The case of word vector training,” *IEEE Transactions on Knowledge and Data Engineering*, vol. PP, pp. 1–1, DOI: 10.1109/TKDE.2018.2 819 673, 2018.

[28] Y. Huang, L. Malka, D. Evans, and J. Katz, “Efficient privacy-preserving biometric identification,” in *Proc. of NDSS’11*. ISOC, 2011.

[29] P. Gallagher, “Digital signature standard (dss),” *Federal Information Processing Standards Publications, volume FIPS*, pp. 186–3, 2013.

[30] D. Lehmann, L. I. Oćallaghan, and Y. Shoham, “Truth revelation in approximately efficient combinatorial auctions,” *Journal of the ACM (JACM)*, vol. 49, no. 5, pp. 577–602, 2002.

[31] A. Mu’Alem and N. Nisan, “Truthful approximation mechanisms for restricted combinatorial auctions,” *Games and Economic Behavior*, vol. 64, no. 2, pp. 612–631, 2008.

[32] X. Zhou, S. Gandhi, S. Suri, and H. Zheng, “eBay in the Sky:strategy-proof wireless spectrum auctions,” in *Proc. of MOBICOM’08*. ACM, pp. 2–13.

[33] Y. Wu, B. Wang, K. R. Liu, and T. C. Clancy, “A multi-winner cognitive spectrum auction framework with collusion-resistant mechanisms,” in *Proc. of DySPAN’08*. IEEE, 2008, pp. 1–9.

[34] H. Zhang, S. Cai, C. Luo, and M. Yin, “An efficient local search algorithm for the winner determination problem,” *Journal of Heuristics*, vol. 23, no. 5, pp. 367–396, 2017.

[35] Y. Zhou, J.-K. Hao, and A. Goëffon, “Push: A generalized operator for the maximum vertex weight clique problem,” *European Journal of Operational Research*, vol. 257, no. 1, pp. 41–54, 2017.

[36] M. Dowlatshahi and V. Derhami, “Winner determination in combinatorial auctions using hybrid ant colony optimization and multi-neighborhood local search,” *Journal of AI and Data Mining*, vol. 5, no. 2, pp. 169–181, 2017.

[37] Y. Chen, L. Lin, G. Cao, Z. Chen, and B. Li, “Stable combinatorial spectrum matching,” in *Proc. of INFOCOM’18*. IEEE, 2018, pp. 1664–1672.

[38] Y. Chen, Y. Xiong, Q. Wang, X. Yin, and B. Li, “Stable matching for spectrum market with guaranteed minimum requirement,” in *Proc. of MobiHoc’17*. ACM, 2017, pp. 4–13.

[39] ——, “Ensuring minimum spectrum requirement in matching-based spectrum allocation,” *IEEE Transactions on Mobile Computing*, 2018.

[40] R. Zhu and K. G. Shin, “Differentially private and strategy-proof spectrum auction with approximate revenue maximization,” in *Proc. of INFOCOM’15*. IEEE, 2015, pp. 918–926.

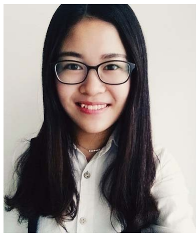
[41] C. Hu, R. Li, B. Mei, W. Li, A. Alrawais, and R. Bie, “Privacy-preserving combinatorial auction without an auctioneer,” *EURASIP Journal on Wireless Communications and Networking*, vol. 2018, no. 1, p. 38, 2018.

[42] Z. Chen, L. Huang, L. Li, W. Yang, H. Miao, M. Tian, and F. Wang, “PS-TRUST: Provably secure solution for truthful double spectrum auctions,” in *Proc. of INFOCOM’14*. IEEE, pp. 1249–1257.

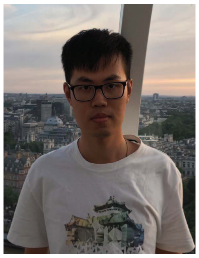
Yanjiao Chen received her B.E. degree in Electronic Engineering from Tsinghua University in 2010 and Ph.D. degree in Computer Science and Engineering from Hong Kong University of Science and Technology in 2015. She is currently a Professor in Wuhan University, China. Her research interests include computer networks, wireless system security, and network economy.

Xin Tian received her B.S. degree in Software Engineering from Dalian University of Technology, China, in 2016. She is currently working towards the Master degree in the School of Computer Science, Wuhan University, China. Her research interest focuses on information security, blockchain and applied cryptography.

Qian Wang is a Professor with the School of Cyber Science and Engineering, Wuhan University. He received the Ph.D. degree from Illinois Institute of Technology, USA. His research interests include AI security, data storage, search and computation outsourcing security and privacy, wireless systems security, big data security and privacy, and applied cryptography etc. Qian received National Science Fund for Excellent Young Scholars of China in 2018. He is also an expert under National “1000 Young Talents Program” of China. He is a recipient of the 2016 IEEE Asia-Pacific Outstanding Young Researcher Award. He is also a co-recipient of several Best Paper and Best Student Paper Awards from IEEE ICDCS’17, IEEE TrustCom’16, WAIM’14, and IEEE ICNP’11 etc. He serves as Associate Editors for IEEE Transactions on Dependable and Secure Computing (TDSC) and IEEE Transactions on Information Forensics and Security (TIFS). He is a Member of the IEEE and a Member of the ACM.



Minghui Li received her B.S. degree in Information Security from Wuhan University, China, in 2016. She is currently working towards the Master degree in the School of Computer Science, Wuhan University, China. Her research interest focuses on information security, cloud computing, artificial intelligence security.



Minxin Du received his B.S. degree in Computer Science and Technology from Wuhan University, China, in 2015. He is currently working towards the Master degree in the Computer School in Wuhan University. His research interests include cloud computing, information security, and applied cryptography.

Qi Li is an associate professor in the Graduate School at Shenzhen, Tsinghua University. His research interests include system and network security, particularly in Internet security, mobile security, and security of large-scale distributed systems. Li has a PhD in computer science from Tsinghua University. Contact him at qi.li@sz.tsinghua.edu.cn.