面向隐私保护的多属性逆向频谱拍卖方案

王佳琪[1]，鲁宁[1,2]，程庆丰[3,4]，巫朝霞[5]，史闻博[6]

（1. 东北大学计算机科学与工程学院，辽宁 沈阳 110819；2. 西安电子科技大学计算机科学与技术学院，陕西 西安 710126；
3. 信息工程大学四院，河南 郑州 450001；4. 数学工程与先进计算国家重点实验室，河南 郑州 450001；
5. 新疆财经大学应用数学学院，新疆 乌鲁木齐 830012；6. 东北大学秦皇岛分校计算机与通信工程学院，河北 秦皇岛 066004）

摘 要：针对现有的逆向频谱拍卖没有考虑与频谱有关的非价格属性的问题和频谱拍卖安全问题，提出了一个面向隐私保护的多属性逆向频谱拍卖方案。首先，将含有频谱价格、与频谱有关的非价格正向属性值作为频谱竞标人的竞标方案并执行拍卖判断频谱赢家。其次，为确保频谱拍卖的安全性，方案利用 Paillier 门限机制引入一组拍卖人的分治集中式频谱拍卖服务器代替传统单一的第三方代理机构，防止频谱拍卖人与频谱竞标人的“合作欺诈”。所提方案还引入匿名化技术、不经意传输技术的密码学工具，确保频谱拍卖的安全特性，使频谱拍卖安全地执行。对所提方案的安全协议进行安全分析表明，协议具有较强的安全性。对协议进行性能评估，实验结果表明，所提方案在计算开销上优于可应用在频谱拍卖场景下的多属性逆向拍卖安全方案。

关键词：频谱拍卖；多属性；隐私保护；Paillier 门限机制

中图分类号：TP309

文献标识码：A

doi: 10.11959/j.issn.1000−436x.2020121

Privacy-preserving multi-attribute reverse spectrum auction scheme

WANG Jiaqi[1], LU Ning[1,2], CHENG Qingfeng[3,4], WU Zhaoxia[5], SHI Wenbo[6]

1. School of Computer Science and Engineering, Northeastern University, Shenyang 110819, China
2. School of Computer Science and Technology, Xidian University, Xi’an 710126, China
3. Fourth Department, Information Engineering University, Zhengzhou 450001, China
4. State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China
5. School of Applied Mathematics, Xinjiang University of Finance and Economics, Urumqi 830012, China
6. School of Computer and Communication Engineering, Northeastern University at Qinhuangdao, Qinhuangdao 066004, China

Abstract: Aiming the problem that the existing reverse spectrum auctions do not take the non-price attribute of spectrum into account and the security of spectrum auction, a privacy-preserving multi-attribute reverse spectrum auction was proposed. Firstly, price and non-price positive attributes of spectrum were considered as the bidding scheme of bidders and auctions was performed to judge spectrum winners. Secondly, to ensure the security of the spectrum auction, the Paillier threshold system was used to introduce a group of spectrum auction servers of auctioneers to replace the traditional single third-party agency, which could prevent the fraud collusion between spectrum auctioneers and bidders. The cryptography tools such as the anonymization technology and oblivious transfer were introduced to achieve the secure features, which could make the spectrum auction performed securely. The security analysis shows that the security protocol has strong security. The performance of the protocol is also evaluated, and experimental results show that the security scheme is superior to the multi-attribute reverse auction security scheme that can be applied in the spectrum auction scenario in terms of computational overhead.

Key words: spectrum auction, multi-attribute, privacy-preserving, Paillier threshold mechanism

---

收稿日期：2020–02–03；**修回日期**：2020–05–27

通信作者：鲁宁，luning@neuq.edu.cn.com

基金项目：国家自然科学基金资助项目（No.U1708262, No.61601107, No.61941205, No.61872449）；中国博士后科学基金资助项目（No.2019M653568）；中央高校基本科研业务费基金资助项目（No.N2023020）

Foundation Items: The National Natural Science Foundation of China (No.U1708262, No.61601107, No.61941205, No.61872449), China Postdoctoral Science Foundation (No.2019M653568), The Fundamental Research Funds for the Central Universities (No.N2023020)

1 引言

近几年，由于无线通信业务的迅猛发展，对频谱资源的需求呈爆炸性增长趋势[1-3]。为提高其利用率，业界提出频谱拍卖的概念[4]，一方面鼓励频谱拥有者可随时自行售卖或出租空闲的频谱资源；另一方面允许频谱买家购买回收已出售的频谱资源，实现二次分配。基于此，根据拍卖活动的开展方式，频谱拍卖方案可分为“一对多”和“多对一”2种。前者是正向拍卖，其中拍卖人为频谱拥有者，竞标人则为购买用户，在每轮拍卖过程中，频谱拍卖人以最大化自身收益为目的，采用竞价方式来选定频谱赢家。后者是逆向拍卖，它以频谱买家为拍卖人，频谱拥有者为竞标人，通过采购方式来选定拍卖赢家，最大化自身利益。目前，绝大部分研究工作都偏向于频谱交易市场上更常见的“一对多”正向拍卖，忽略了可完成频谱二次分配的“多对一”逆向拍卖，而后者也是提高频谱资源利用率所需的手段。例如，美国于2017年就曾通过逆向拍卖回收部分已分配但被闲置的频谱资源，进而实现了频谱资源的二次利用[5]。因此，本文重点关注“多对一”的逆向频谱拍卖方案。

目前，政府利用逆向频谱拍卖向频谱拥有者回收闲置频谱并二次分配频谱资源，以提高频谱利用率[6]。现有逆向频谱拍卖的买卖双方只以价格展开博弈，进而确定赢家。虽然以价格展开博弈的单属性逆向频谱拍卖比较容易实现，但在实际拍卖场景中，出让频谱报价较低的卖家并不一定会成为拍卖赢家。因为政府回收闲置频谱的目的是将频谱重新打包规划，进而将其分配给那些真正需要频谱、展开频谱业务的频谱买家。因此，除了价格，政府还需参考待分配频谱买家的业务需求。例如，美国联邦通信委员会（FCC, Federal Communications Commission）在评估广播业务出让频谱的价格时，往往将服务人口、覆盖地区范围以及放弃原频段的方式等属性考虑在内。国内由于网络制式不同，所需的频率范围、带宽、不同服务地区等属性都会影响某一段频谱的价格以及再分配的利用率。由此可见，为提高频谱资源的利用率，政府应将与频谱有关的多属性因素考虑在内，开展多属性的逆向频谱拍卖。

除了上述存在的问题，网络环境的复杂性也使逆向频谱拍卖面临诸多安全风险，主要包括以下几个方面。1)隐私问题。竞标信息是敏感信息，一旦被不法分子获取并贩卖给他人，可能会导致拍卖失败，甚至给用户造成无法估量的经济损失。因此，竞标信息需要保密。2)安全的数据传输。在频谱拍卖执行时，需要确保频谱拍卖参与者之间数据传输的安全性，防止被对手恶意篡改数据，从而导致错误的拍卖结果。3)欺诈勾结。频谱拍卖的拍卖人通常由频谱拥有者或频谱买家授权的第三方代理机构所担任。拍卖人为赚取更多利润可能与一个或多个频谱竞标人合谋操纵拍卖，将拍卖结果导向对他们有利的一方致使拍卖失败。4) 公开验证。公开验证频谱赢家的合法性，证明频谱拍卖结果的正确性、频谱拍卖执行的公平性。

针对上述挑战，本文提出了一个面向隐私保护的多属性逆向频谱拍卖（PMRA, privacy-preserving multi-attribute reverse spectrum auction）方案。PMRA方案将频谱的非价格正向属性（如带宽、地理覆盖范围等属性）引入逆向频谱拍卖中，并利用多属性决策效用理论，由频谱的非价格正向属性值、频谱价格来计算频谱决策效用函数，从而确定频谱赢家以及最优的频谱资源方案。其次，逆向频谱拍卖往往忽略了频谱拍卖中所涉及的安全问题，为确保逆向频谱拍卖的安全性，PMRA方案提出多属性逆向频谱拍卖架构并设计安全协议。PMRA方案安全协议不仅利用Paillier加密及其门限机制确保了频谱拍卖服务器的安全性与可靠性，还引入了不经意传输技术、匿名化技术，保证了频谱拍卖中所需的安全特性。

2 PMRA方案

本节首先介绍PMRA方案的多属性逆向频谱拍卖架构，并给出在该架构下各个参与方的定义。其次，介绍PMRA方案在多属性逆向频谱拍卖架构下的威胁模型。

2.1 多属性逆向频谱拍卖架构

频谱拍卖中的买卖双方只针对价格展开博弈，从而确定频谱赢家，并未将与频谱有关的非价格多属性考虑在内。其次，在复杂的网络环境下，已有的频谱拍卖方案通常引入一个半诚实的第三方代理机构，频谱买家与代理机构协作共同完成频谱拍卖。但在实际应用环境中，代理人有可能被频谱竞标人收买，从而泄露重要的隐私数据，这可能导致错误的频谱拍卖结果。因此，如何使频谱买家获得最优的频谱资源并保证频谱拍卖的安全性十分重要。频谱拍卖的目的是为频谱拥有者赚取利润并满足频谱买家对频谱资源的诉求，在确保频谱拍卖安

全运行的同时合理地分配频谱资源。以此为出发点，本文将传统频谱拍卖中存在的单一半诚实代理机构由一组频谱拍卖人所取代，提出一个多属性逆向频谱拍卖架构。PMRA 方案基于此架构，利用 Paillier 门限机制可有效地防止频谱参与方任意两方的相互勾结，可避免因隐私数据的泄露而导致错误的频谱拍卖结果，从而确保了频谱拍卖服务器的可靠性与安全性。在频谱拍卖执行过程中，为确保竞标人（频谱拥有者）身份的匿名性与竞标方案的隐私性，方案利用匿名化技术隐藏竞标人的身份信息，并利用 Paillier 加密方案加密频谱竞标人的竞标信息（频谱价格与非价格正向属性值）。每个频谱拍卖人所拥有的分治集中式频谱拍卖服务器通过不经意传输技术获取频谱竞标人加密的频谱竞标方案，并计算密文状态下的频谱决策效用函数。最后，频谱买家收到服务器发送的部分解密与验证信息以还原明文，当还原所有频谱竞标人的频谱决策效用函数后，判断决策赢家完成频谱拍卖。

多属性逆向频谱拍卖架构如图 1 所示。该架构由一组数量为 m 的频谱竞标人、n 个拥有分布式频谱拍卖服务器的拍卖人以及频谱买家 3 个参与方组成。首先，每个频谱竞标人根据实际情况出让频谱资源并拟定频谱竞标方案。其次，n 个频谱拍卖人分别获取频谱竞标方案中加密后的频谱竞标价格与非价格的正向属性值，利用各自的频谱拍卖服务器计算密文状态下的频谱正向属性的权值、频谱决策效用函数值。拍卖服务器再利用子密钥解密得到部分消息。最后，频谱买家收到 n 个服务器发送的部分解密消息，还原密文状态下的频谱决策效用函数。当频谱买家还原了 m 个频谱竞标人的决策效用函数值后，则可判断拍卖赢家。

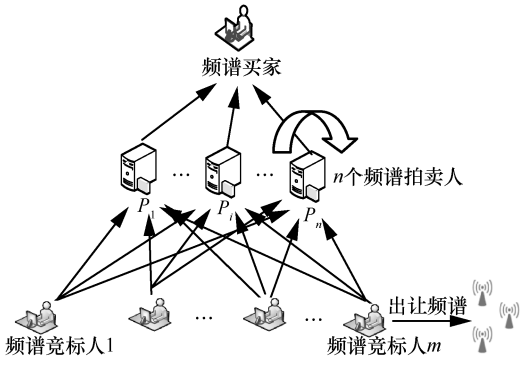

图 1　多属性逆向频谱拍卖架构

在多属性逆向频谱拍卖架构下，频谱买家、频谱竞标人与频谱拍卖人的定义如下。

定义 1　频谱买家。频谱买家是需要回收购买频谱的频谱管理部门。频谱买家主要执行 2 个步骤，一是在频谱拍卖开始前，频谱买家需要在电子公告板上发布所回收频谱资源的必要信息。二是在判断拍卖赢家阶段，频谱买家接收服务器发送来的部分解密密文、部分有效验证证明，可依次解密还原每个竞标人的频谱决策效用函数值。频谱买家通过频谱决策效用函数值判断竞标赢家。

频谱买家为获取竞标人提供最优的频谱资源时，往往要将频谱带宽、覆盖地理范围等向上增长的正向属性考虑在内，即频谱的正向属性值越大，则频谱资源越优质。由此猜想，若以频谱决策效用函数值确定频谱赢家，所计算出的频谱决策函数效用值应随着频谱的正向属性值增大而呈现线性递增的趋势。而多属性决策（MADM, multiple attribute decision making）理论中的线性加权法刚好满足这一特征。多属性决策又称为有限方案的多目标决策理论，即在考虑多个属性的情况下，需要选择最优的候选方案或对方案进行排序的决策问题。多属性决策的数学模型描述如下。设多属性决策的方案集合为 $D=\{\boldsymbol{d}_1,\boldsymbol{d}_2,\cdots,\boldsymbol{d}_m\}$，属性集合为 $A=\{\boldsymbol{a}_1,\boldsymbol{a}_2,\cdots,\boldsymbol{a}_n\}$。则矩阵 $\boldsymbol{X}(x_{ij})_{m\times n}(i=1,2,\cdots,m;\ j=1,2,\cdots,n)$ 表示方案集 D 关于属性集 A 的决策矩阵。决策矩阵 $\boldsymbol{X}$ 表示为

$$\boldsymbol{X}=\begin{array}{c} \\ \boldsymbol{d}_1 \\ \boldsymbol{d}_2 \\ \vdots \\ \boldsymbol{d}_m \end{array}\begin{array}{c} \begin{array}{cccc} \boldsymbol{a}_1 & \boldsymbol{a}_2 & \cdots & \boldsymbol{a}_n \end{array} \\ \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{m1} & x_{m2} & \cdots & x_{mn} \end{bmatrix} \end{array} \tag{1}$$

线性加权法作为多属性决策理论的方法之一，它的决策系数由属性的权重决定，将各个正向属性线性加权求和即可实现最优的决策判断。由此，PMRA 方案使用多属性决策理论中的线性加权法描述频谱决策效用函数[7]，当计算得出频谱决策效用函数的最大值时，即可确定频谱买家的最优方案。设频谱决策效用函数为 Utility($-b_i$, AS_i)，其中 b_i 表示频谱竞标人 i 的频谱竞标价格。设有 T 个与频谱有关的正向属性，则 $\mathrm{AS}_i=\{A_{i1},A_{i2},\cdots,A_{iT}\}$ 表示竞标人 i 提供的频谱正向属性值的竞标集合，$W=\{w_1,w_2,\cdots,w_T\}$ 则表示频谱正向属性的权重集合。例如实际拍卖场景下，在针对某些运营商放弃部分频谱使用权时，政府在回收频谱的过程中往往需要

考虑频谱的带宽、地理覆盖范围等正向频谱属性因素，因此带宽越大、地理覆盖范围越广，频谱资源越优质。对于政府而言，频谱竞标人的竞标价格越低，则越有利于回收。由此，在频谱决策效用函数中的频谱竞标价格取值为$-b_i$。频谱决策效用函数表示为

$$\text{Utility}(b_i,\text{AS}_i)=-b_i+\sum_{j=1}^{T}w_jA_{ij} \tag{2}$$

其中，A_{ij}为频谱竞标人i的第j个频谱正向属性值，可简记为A_j；w_j为对应的频谱属性权重值；T为频谱的正向属性个数。本文以式(2)为依据设计安全协议。由式(2)可知，除频谱竞标价格以外，频谱正向属性的权值影响频谱决策效用函数值的高低。根据上文讨论可知，在参与竞标的频谱竞标人中，计算得出频谱决策效用函数的最大值时则为频谱资源的最优方案。因此，频谱买家以式(3)确定频谱竞标赢家。

$$\text{argmax}_i\left(\text{Utility}(-b_i,\text{AS}_i)\right) \tag{3}$$

由于频谱的竞标价格与频谱属性值的单位和取值范围都不同，故难以使频谱的竞标价格与频谱的属性值直接参与频谱决策效用函数值的计算。例如，当回收网络服务提供商的部分频谱资源时，设当频谱的正向属性个数T=3时，可选定频谱的正向属性值的集合为{频谱的带宽（MHz），地理覆盖范围（km），频率范围（MHz）}。频谱的竞标方案为{频谱价格（亿元），频谱的带宽（MHz），地理覆盖范围（km），频率范围（MHz）}。由于频谱不同，属性的取值单位不同，因而无法进行频谱决策效用函数值的计算。为消除不同数量级、量纲和类型对频谱决策效用函数值的影响，需要对数值进行规范化处理，将量级、量纲和类型不同的频谱竞标价格与频谱属性利用数学变换，统一变换到相应的取值范围内。常用的方法有向量规范化、线性变换与极差变换法。因数值的规范化并非本文研究的重点，在此不做介绍。

定义 2 频谱竞标人。频谱竞标人即频谱拥有者，由一组数量为m，为获利放弃部分频谱使用权而售卖其频谱资源的卖家用户构成。设频谱竞标人i ($1\leqslant i\leqslant m$)的竞标方案为 $B_i=\{b_i,\ \text{AS}_i\}(A_j\in\text{AS}_i,1\leqslant j\leqslant T)$。频谱竞标人查看电子公告板上频谱买家发布的频谱资源需求信息，判断所拥有的频谱是否符合频谱买家的需求，从而决定是否参与频谱拍卖。若确定参与频谱拍卖，则频谱竞标人根据频谱资源的属性信息拟定频谱竞标方案。为保护频谱竞标方案的隐私性，频谱竞标人利用可信机构产生的公钥加密频谱竞标方案。

定义 3 频谱拍卖人。频谱拍卖人的数量为n，且每个频谱拍卖人都拥有各自的分布式频谱拍卖服务器$P_i(1\leqslant i\leqslant n)$, $n=T+1$。频谱拍卖服务器的主要功能有 3 个。1)存储频谱买家预先设定的频谱属性权重，即权重集合$W=\{w_1,w_2,\cdots,w_T\}$的每个权重分别存储在 $n-1$ 个频谱拍卖服务器中。2)频谱拍卖服务器$P_i(1\leqslant i\leqslant n)$获取频谱竞标人的加密竞标方案，并计算密文状态下的频谱属性的权值以及频谱决策效用函数值。3)n 个频谱拍卖服务器利用可信机构产生的子密钥与验证子密钥解密频谱决策效用函数值的部分消息，并将其发送给频谱买家。

2.2 威胁模型

在实际的频谱拍卖场景中，频谱拍卖人虽然在拍卖过程中可以完全遵守频谱拍卖规则执行，但他们为了获取更多的利润可能与某一频谱竞标人合作，并将服务器获取的敏感信息以及拍卖过程中产生的中间结果透露给频谱竞标人。这一行为可能会让频谱竞标人推测出其他竞标人的竞标信息，从而造成隐私数据的泄露，更严重时还会导致错误的频谱拍卖结果。由此可见，频谱拍卖人与频谱竞标人是半诚实的。而每位频谱竞标人都想赢得频谱拍卖，频谱竞标人之间属于竞争关系，因此并不存在频谱竞标人之间的相互勾结。频谱买家希望通过频谱拍卖寻求合适的频谱资源，因而频谱买家是诚实的。由此，该架构下的 3 个参与方构成一个频谱拍卖的半诚实模型。半诚实模型中存在着被动攻击者，换句话说，被动攻击者可以在频谱拍卖过程中获得他人信息，但无法篡改参与方在拍卖过程中的输入值与中间值，更不能使拍卖终止。半诚实模型安全定义如下[8-9]。

定义 4 半诚实模型下的隐私性。设频谱拍卖所执行的协议为$\prod$，协议$\prod$需执行的确定性功能函数为f，当存在 2 个参与方 A 和 B 时，x 和 y 分别对应参与方 A 和 B 在协议中的私有输入值，则参与方 A 和 B 在执行频谱拍卖协议$\prod$中所得到的信息值可分别记为 $\text{view}_1^{\prod}(x,y)=(x,r^1,m_1^1,m_2^1,m_k^1)$和 $\text{view}_2^{\prod}(x,y)=(x,r^2,m_1^2,m_2^2,m_k^2)$。这里的$r^1$和$r^2$表示参与方 A 和 B 生成的随机数，$m_j^i$则表示参与方 A 和 B 在频谱拍卖协议$\prod$执行过程中所接收到的第$j$条信息。参与

方 A 和 B 执行协议后的输出可分别记为 $\text{output}_1^{\prod}(x,y)$ 和 $\text{output}_2^{\prod}(x,y)$。由此可知参与方 A 和 B 执行协议后的输出实际上是 $\text{view}_1^{\prod}$ 与 $\text{view}_2^{\prod}$ 的其中一部分。因此，在执行协议∏的过程中计算确定性功能函数 f 时，存在多项式时间算法 S_1 和 S_2，应当满足

$$\left\{S_1\left(x,f(x,y)\right)\right\}_{x,y\in\{0,1\}^*}\overset{c}{\equiv}\left\{\text{view}_1^{\pi}(x,y)\right\}_{x,y\in\{0,1\}^*} \quad (4)$$

$$\left\{S_2\left(y,f(x,y)\right)\right\}_{x,y\in\{0,1\}^*}\overset{c}{\equiv}\left\{\text{view}_2^{\pi}(x,y)\right\}_{x,y\in\{0,1\}^*} \quad (5)$$

其中，$|x|=|y|$。

3　安全协议设计

本节首先介绍 PMRA 方案安全协议的整体设计，其次详细阐述安全协议所需执行的协议的初始化、频谱拍卖的竞标以及判断拍卖赢家 3 个阶段，最后给出方案的案例评估。

3.1　协议的整体设计

频谱拍卖中存在的单一半诚实代理机构可能被某一频谱竞标人收买。当代理机构获取解密密钥解密任意加密的频谱信息时，很可能将信息透露给频谱竞标人，从而泄露数据隐私导致错误的频谱拍卖结果。由此，本文所提出的 PMRA 方案安全协议将利用 Paillier 门限机制的基本思想[10]解决上述存在的“勾结欺诈”行为。Paillier 门限机制由一个组合者、一个可信任的密钥分发者、n 个服务器 $P_i(1\leqslant i\leqslant n)$和多个用户组成。在本文方案的安全协议中，组合者即为频谱买家，n 个服务器则对应着 n 个频谱拍卖人的分治集中式频谱拍卖服务器，多个用户即为多个频谱竞标人。Paillier 门限机制是将门限机制的基本思想运用到 Paillier 公钥密码方案中。Paillier 门限系统的 Paillier 公钥加密方案以及 Paillier 方案的同态性质的定义如下[11]。

定义 5　Paillier 加密方案及其同态性质。

密钥生成。设 p 和 q 是 2 个大素数，计算 $N=pq$，$g\in Z_N^*$，g 满足 $\gcd(L(g^{\lambda} \bmod n^2), n)=1$，$L(x)=(x-1)$。公钥为 $\text{pk}=(N,g)$，私钥为 $\text{sk}=\lambda(N)=\text{lcm}(p-1,q-1)$。其中 gcd 为最小公倍数，lcm 为最大公约数。

加密阶段。随机选择任意明文 $m\in Z_N$，则设密文为 c，且 $E_{\text{pk}}(m,r)=g^m r^N \bmod N^2$。

解密阶段。解密加密后的密文 c 并还原明文 m，则 $m=D_{\text{sk}}(c)=L(c^{\lambda(N)} \bmod N^2)$。

Paillier 加密方案同态性质如下。

设 2 个明文 m_1 和 m_2，则对应密文分别为 c_1 和 c_2，$c_1=E_{\text{pk}}(m_1,r_1)=g^{m_1} r_1^N \bmod N^2$，$c_2=E_{\text{pk}}(m_1, r_2)=g^{m_2} r_2^N \bmod N^2$，有 $D_{\text{sk}}(E_{\text{pk}}(m_1,r_1)E_{\text{pk}}(m_2,r_2) \bmod N^2)=m_1+m_2 \bmod N$，$D_{\text{pk}}(E_{\text{pk}}(m_1)^k \bmod N^2)=km \bmod N$。

关于 Paillier 门限机制的具体实现内容，将会在 3.2 节～3.4 节中详细阐述。

基于 Paillier 门限机制的基本思想，PMRA 方案安全协议流程如图 2 所示。PMRA 方案安全协议的设计主体需要执行以下 3 个阶段。

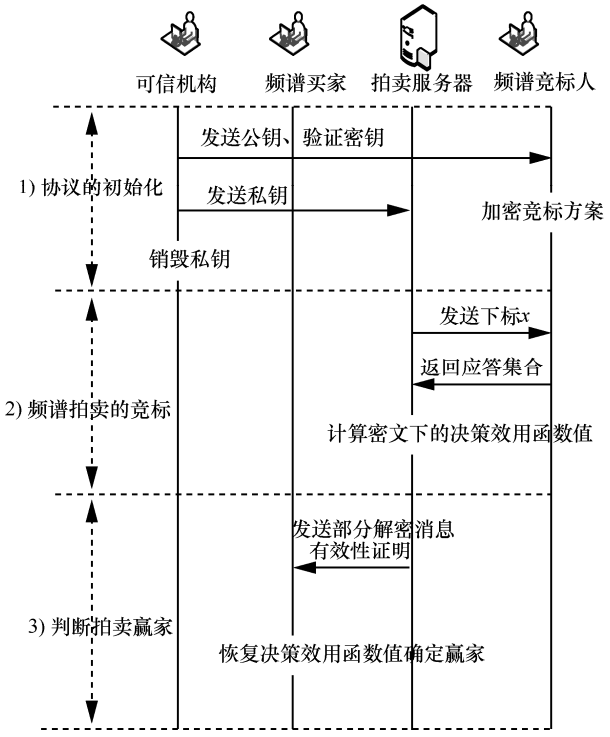

图 2　安全协议流程

1) 协议的初始化。首先，频谱买家在电子公告板上发布频谱资源的需求信息（可接受的频谱价格范围以及非价格正向属性的取值范围信息）的同时，将已经确定的 T 个非价格正向属性值的权重分别发送给对应频谱拍卖人的服务器 $P_i(1\leqslant i\leqslant n-1)$。频谱竞标人 i 查看电子公告板上频谱买家所发布的信息，拟定频谱竞标方案 $B_i=\{b_i, \text{AS}_i\}$。其次，协议的初始化阶段引入可信机构。可信机构利用 Paillier 门限机制生成密钥(pk, sk)，将公钥 pk 公开发布到电子公告板上，依次将部分密钥 sk_i、公开验证密钥(vk, vk_i)发送给每个频谱拍卖服务器。当完成上述工作后，可信机构销毁 sk 并退出该协议。

2) 频谱拍卖的竞标。首先，频谱竞标人 i 利用匿名化技术以及协议初始化产生的公钥 pk 隐藏身份信息并加密已拟定的频谱竞标方案。其次，为确

保数据传输的安全性与隐私性，每个频谱拍卖服务器 $P_i(1\leqslant i\leqslant n-1)$以不经意传输的方式分别获取对应权重的加密属性值 $E_{\mathrm{pk}}(A_j)$以及加密的频谱竞标价格 $E_{\mathrm{pk}}(-b_i)$。最后，由 n 个分布式频谱拍卖服务器相互协作，协议利用 Paillier 加密方案的同态性质计算密文状态下的各个属性的权值 $E_{\mathrm{pk}}(A_j)^{w_j}$和频谱决策效用函数值 $E_{\mathrm{pk}}(\mathrm{Utility}(-b_i,\ \mathrm{AS}_i))$以完成频谱拍卖的竞标过程。

3) 判断拍卖赢家。首先，频谱拍卖服务器 P_n 计算得到 $E_{\mathrm{pk}}(\mathrm{Utility}(-b_i,\ \mathrm{AS}_i))$并将其发送给其他 $n-1$ 个频谱拍卖服务器 $P_i(1\leqslant i\leqslant n-1)$。其次，每个拍卖人的频谱拍卖服务器$P_i(1\leqslant i\leqslant n-1)$用各自持有的部分子密钥 sk_i，验证密钥$(\mathrm{vk},\ \mathrm{vk}_i)$解密 $E_{\mathrm{pk}}(\mathrm{Utility}(-b_i,\ \mathrm{AS}_i))$，从而各自得到部分解密消息 c_i、部分有效证明 proof_i。最后，为了还原明文 $\mathrm{Utility}(-b_i, \mathrm{AS}_i)$，根据 Paillier 门限机制的基本思想，只有当频谱买家收到至少 t（这里令 $t=n$）个 proof_i 被验证正确时，协议利用 Paillier 门限机制的组合算法才能得到频谱决策效用函数值 $\mathrm{Utility}(-b_i,\ \mathrm{AS}_i)$。当获取 m 个频谱竞标人的频谱决策效用函数值后，频谱买家可计算值 $\mathrm{argmax}_i(\mathrm{Utility}(-b_i,\ \mathrm{AS}_i))$以判断频谱赢家。

3.2 协议的初始化

根据频谱买家提供的频谱资源信息，频谱竞标人 $i(1\leqslant i\leqslant m)$拟定频谱竞标方案 $B_i=\{b_i,\ \mathrm{AS}_i\}$，$A_j\in \mathrm{AS}_i,\ 1\leqslant j\leqslant T$。设频谱竞标人的 i 频谱价格为 b_i，非价格正向属性值的集合为$\{\mathrm{AS}_i\}_{1\leqslant i\leqslant m}$，则对应的权重值集合为$\{w_j\}_{1\leqslant j\leqslant n-1}$。为在频谱拍卖过程中保护频谱竞标人竞标信息的隐私性，协议还引入可信机构。可信机构通过利用 Paillier 门限机制为频谱拍卖生成公钥与私钥。频谱拍卖的密钥生成步骤如下。

步骤 1 选择一个整数 N，有 $N=pq$，p 与 q 为 2 个素数且 $p=2p'+1$，$q=2q'+1$，$\gcd(N,\Phi(N)=1$。设 $m=p'q'$，β 是 Z_N^* 中随机选择的元素，随机选择 $(a,b)\in Z_{N^2}^*$ 并且设 $g=(1+N)^a b^N \bmod N^2$。

步骤 2 设密钥 $\mathrm{sk}=\beta m$ 与 Shamir 方案共享：设 $a_0=\beta m$，在$\{0,\cdots,Nm-1\}$中随机选择 t 个值记为 a_i，且有 $f(x)=\sum_{i=0}^{t} a_i X^i$，则第 i 个拍卖服务器 P_i 子密钥 s_i 为 $f(i) \bmod Nm$。

步骤 3 产生公钥 pk，且公钥 pk 由 g、N、$\theta=L(g^{m\beta})=am\beta \bmod N$ 组成。

步骤 4 设 $\mathrm{vk}=v$ 是在 $Z_{N^2}^*$ 平方数组成循环群的生成元，验证密钥 $\mathrm{vk}_i=v^{\Delta s_i} \bmod N^2$，其中，$\Delta=n!$，$n$ 表示频谱拍卖服务器的数量[12]。

在协议的初始化阶段，首先，可信机构将部分子密钥 s_i 发送给各自对应的频谱拍卖服务器 $P_i(1\leqslant i\leqslant n)$，完成分发后则销毁密钥 sk。其次，可信机构公开公钥 pk、分发验证密钥$(\mathrm{vk},\ \mathrm{vk}_i)$后退出频谱拍卖协议。频谱买家将非价格正向属性的权重值 $w_j(1\leqslant j\leqslant n-1)$依次发送给对应的频谱拍卖服务器 $P_i(1\leqslant i\leqslant n-1)$保存。

3.3 频谱拍卖的竞标

频谱拍卖的竞标过程由频谱竞标人 i 与频谱拍卖服务器 $P_i(1\leqslant i\leqslant n)$完成各自的竞标操作，主要分为以下 3 个阶段。

阶段 1 竞标人身份信息的匿名化。频谱竞标人i利用匿名化技术[13]隐藏其真实身份R_id_i得到一个虚拟的假身份 $\mathrm{V\_id}_i$。$\mathrm{V_id}_i$的计算式为

$$\mathrm{V\_id}_i = E_{\mathrm{pk}}(\mathrm{R\_id} \,\|\, \mathrm{pad}) \,\|\, \mathrm{pk} \,\|\, n \tag{6}$$

其中，pad 代表一个将频谱需求用户的指定位置填充适当长度的随机填充位。匿名化技术的安全性与唯一性详细证明见文献[14]。当完成 m 个频谱竞标人身份信息匿名化处理后，则将每个频谱竞标人的 $\mathrm{V_id}_i(1\leqslant i\leqslant m)$发送到电子公告版上。

阶段 2 加密属性值与数据传输。首先，频谱竞标人 i 利用公钥 pk 加密频谱竞标方案。加密的频谱价格为 $E_{\mathrm{pk}}(-b_i)=g^{-b_i} r \bmod N^2$，加密的非价格正向属性值为 $E_{\mathrm{pk}}(A_j)=g^{A_j} r \bmod N^2$，其中 $r_1,r_2\in Z_N^*$。其次，为确保数据的隐私性与数据传输的安全性，频谱拍卖服务器 $P_i(1\leqslant i\leqslant n)$利用不经意传输技术获取对应的加密的非价格正向属性值与频谱竞标价格。不经意传输技术又叫茫然传输协议，是一种应用广泛的通信协议，能使双方以一种模糊化的方式发送和接收消息，发送方无法得知接收方接收到的具体信息内容，从而保护接收方的隐私不会被泄露。不经意传输技术定义如下[15]。

定义 6 不经意传输协议。设 q 为一个大素数，G_q 为 q 阶循环群，Z_q 为拥有 q 个元素的有限加法群。$(g,\ h)$则为 G_q 的 2 个生成元。初始化参数输入$(g,\ h,\ G_q)$，发送方输入 $s_1,s_2,\cdots,s_n\in G_q$，接收方选择 $\varepsilon\in[1,n]$，也就是说，每一个接收方只能获取发送方输入其中的一个元素，且发送方并不知道接收方获取的是哪一个元素。发送方将含有 ε 的信息 $y=g^r h^{\varepsilon}$，$r\in Z_q$ 发送给接收方，然后接收方返回应答

$c_j=(g^{t_j},s_j\left(\frac{y}{h^j}\right)^{t_j})$，$t_j\in Z_q$，$1\leqslant j\leqslant n$。当发送方接收到$\{c_j\}$后，发送方由 $c_\varepsilon=(d,f)$可计算 $c_\varepsilon=\frac{f}{d^r}$。

频谱拍卖人的 n 个拍卖服务器 $P_i(1\leqslant i\leqslant n)$利用不经意传输协议并发地选取频谱竞标人 i 加密后的价格与非价格正向属性值。因此，频谱拍卖服务器 $P_i(1\leqslant i\leqslant n)$获取加密值的传输过程分别为以下 3 个步骤。

步骤 1　$P_i(1\leqslant i\leqslant n)$随机选取下标 x，发送 $y=g^rh^x$ 给匿名的频谱竞标人 i。

步骤 2　匿名的频谱竞标人 i 返回一个应答集合 $c=\{c_1, c_2,\cdots,c_n\}$，且 $c_j=\left(g^{\mu_j},a'k\left(\frac{y}{h^j}\right)^{\mu_j}\right)$，$\mu_j\in Z_N$。

步骤 3　$P_i(1\leqslant i\leqslant n)$在应答集合 $c=\{c_1,c_2,\cdots,c_n\}$中选取对应 x 的元素的 $c_x=(d,f)$。$P_i(1\leqslant i\leqslant n)$获取并计算加密的频谱正向属性值，则有 $E_{\mathrm{pk}}(A_j)=\frac{f}{d^r}=E_{\mathrm{pk}}(A_j)\cdot\frac{\left(\frac{y}{h^x}\right)^{\mu_x}}{(g^{\mu_x})^r}=E_{\mathrm{pk}}(A_j)\frac{\left(\frac{g^rh^x}{h^x}\right)^{\mu_x}}{(g^{\mu_x})^r}$。$P_n$ 计算获取频谱竞标价格 $E_{\mathrm{pk}}(-b_i)=\frac{f}{d^r}=E_{\mathrm{pk}}\left(-b_i\right)\frac{\left(\frac{y}{h^x}\right)^{\mu_x}}{(g^{\mu_x})^r}$。

阶段 3　计算密文下的频谱决策效用函数。首先，P_i 根据 Paillier 的同态乘法性质：对于明文 m，$m\in Z_N$, $r\in Z_N^*$，有 $D_{\mathrm{sk}}(E_{\mathrm{pk}}(m,r)^\lambda \bmod N^2)=\lambda m \bmod N$，计算密文状态下的频谱正向属性权重值 $E_{\mathrm{pk}}(A_j)^{w_j}=E_{\mathrm{pk}}(A_j)^{w_j}$。其次，将每个 P_i $(1\leqslant i\leqslant n-1)$计算得到的 $E_{\mathrm{pk}}(A_j)^{w_j}$ 发送到 P_n，利用 Pailier 的同态加法性质 $D_{\mathrm{sk}}(E_{\mathrm{pk}}(m_1,r_1)E_{\mathrm{pk}}\ (m_2,r_2)\ \bmod N^2)=m_1+m_2 \bmod N$，计算密文状态下的频谱正向属性的权重和为

$$E_{\mathrm{pk}}\left(\sum_{j=1}^{n-1}w_jA_j\right)=\prod_{j=1}^{n-1}E_{\mathrm{pk}}(A_j)^{w_j} \tag{7}$$

因此，P_n 可计算出密文下的决策效用函数值为

$$E_{\mathrm{pk}}\left(\mathrm{Utility}(b_i,\mathrm{AS}_i)\right)=E_{\mathrm{pk}}\left(-b_i+\sum_{j=1}^{T}w_jA_{\mathrm{ij}}\right)=E_{\mathrm{pk}}(-b_i)\left(\prod_{j=1}^{T}E_{\mathrm{pk}}(A_j)^{w_j}\right) \tag{8}$$

P_n 将式(8)计算得到的密文状态下的频谱决策效用函数值发送给其余 $n-1$ 个拍卖服务器。由此，完成频谱拍卖竞标的全部过程。

3.4　判断拍卖赢家

每个拍卖人的频谱拍卖服务器 $P_i(1\leqslant i\leqslant n)$得到密文状态下的频谱决策效用函数值之后，首先利用自己持有的子密钥 s_i 进行部分解密。设明文 $c=E_{\mathrm{pk}}(\mathrm{Utility}(-b_i,\ \mathrm{AS}_i))$，$P_i(1\leqslant i\leqslant n)$计算部分明文 $c_i=c^{2\Delta si} \bmod N$。其次，$P_i(1\leqslant i\leqslant n)$发送$(c_i,\ \mathrm{proof}_i)$给频谱买家。由 Paillier 的门限机制的组合阶段可知，如果频谱买家收到不少于 $t(t=n)$个有效$(c_i,\ \mathrm{proof}_i)$，则可成功恢复明文 $\mathrm{Utility}(-b_i,\mathrm{AS}_i)$；反之，则失败。由此，设 S 为 t 个有效部分解密，则其恢复值 $\mathrm{Utility}(-b_i,\mathrm{AS}_i)$为

$$L\left(\prod_{j\in S}c_j^{2\mu_{0,j}^S} \bmod N^2\right)\frac{1}{4\Delta^2\theta} \bmod N \tag{9}$$

其中，$2\mu_{0,j}^S=\Delta\prod_{j'\in S\setminus\{j\}}\frac{j'}{j'-1}$。

当频谱买家恢复其余 $m-1$ 个频谱竞标人的频谱决策效用函数值后，利用式(3)排序选出最优的频谱竞标方案，判断拍卖赢家。

3.5　案例评估

本节通过实例以说明本文方案的执行全过程。设频谱买家（可能为频谱的管理部门）向频谱竞标人（可能为网络服务提供商）回收频率范围在 470～600 MHz 的特高频广播电视频段的频谱资源。方案的协议执行分为以下 3 个部分。

1) 协议的初始化。频谱买家结合自身实际情况发布频谱资源的需求信息：频谱买家可接受的频谱价格范围为 1～40 亿元，且频谱买家所选择确定的频谱正向属性包括频率范围、地理覆盖范围、带宽。频谱买家根据自身需求预设对应的属性权重值，分别为 w_1=0.35、w_2=0.375、w_3=0.275，并分别发送到任意的 3 个频谱拍卖服务器中保存。频率范围根据频谱买家的实际偏好对其进行正向划分确定回收的优先级。因此，设 470～520 MHz 的优先级为 1，520～570 MHz 的优先级为 2，570～600 MHz 的优先级为 3。优先级数值越大，频谱买家越偏好该频率范围的频谱资源。频谱买家需回收的带宽范围为 5～50 MHz，地理覆盖范围在 100～500 km。存在频谱竞标人 A、B、C 根据频谱买家所发布的频谱需求信息拟定频谱竞标方案。竞标人 A、B、C 的频谱竞标方案分别为{4 亿元，10 MHz，1 级，200 km}、{5.2 亿元，14 MHz，2 级，300 km}、{4.5 亿元，8 MHz，3 级，350 km}。频谱竞标人利用线性变换将单位不

统一的属性值进行规范化处理，得到的竞标方案分别为{−0.1, 0.2,0.33,0.4}、{−0.13, 0.28, 0.67, 0.6}、{−0.1125, 0.16, 1, 0.7}。该频谱拍卖引入可信机构利用 Paillier 门限机制生成公钥 pk 与私钥 sk。可信机构将部分子密钥 s_i 发送给对应的频谱拍卖服务器 $P_i(1\leqslant i\leqslant 4)$，分发完成后销毁密钥 sk。当可信机构公开 pk 并分发验证密钥(vk, vk_i)后退出频谱拍卖。

2) 频谱拍卖的竞标。频谱竞标人 A、B、C 首先利用匿名化技术得到虚拟身份记为 V_1、V_2、V_3。其次，利用公钥 pk 加密各自的竞标方案。则加密后的竞标方案分别为 V_1: $\{E_{\mathrm{pk}}(-0.1),\ E_{\mathrm{pk}}(0.2),\ E_{\mathrm{pk}}(0.33),\ E_{\mathrm{pk}}(0.4)\}$、$V_2$: $\{E_{\mathrm{pk}}(-0.13),\ E_{\mathrm{pk}}(0.28),\ E_{\mathrm{pk}}(0.67),\ E_{\mathrm{pk}}(0.6)\}$、$V_3$: $\{E_{\mathrm{pk}}(-0.1125),\ E_{\mathrm{pk}}(0.16),\ E_{\mathrm{pk}}(1),\ E_{\mathrm{pk}}(0.7)\}$。以 V_1 为例，P_1、P_2、P_3、P_4 利用不经意传输技术分别获取对应加密后的频谱属性值与频谱竞标价格分别为 $E_{\mathrm{pk}}(0.33)$、$E_{\mathrm{pk}}(0.2)$、$E_{\mathrm{pk}}(0.4)$、$E_{\mathrm{pk}}(-0.1)$。每个频谱拍卖服务器 $P_i(1\leqslant i\leqslant 4)$ 利用 Paillier 的同态性质计算各自加密后的权值。以频谱拍卖服务器 P_1 为例，P_1 计算得到的加密权值为 $E_{\mathrm{pk}}(0.2)^{w_1}=E_{\mathrm{pk}}(0.2)^{0.35}=E_{\mathrm{pk}}(0.2\times 0.35)$。同理，$P_2$、$P_3$ 的加密权值分别为 $E_{\mathrm{pk}}(0.33)^{w_2}=E_{\mathrm{pk}}(0.33\times 0.375)$，$E_{\mathrm{pk}}(0.4)^{w_3}=E_{\mathrm{pk}}(0.4\times 0.275)$。最后，将 P_1、P_2、P_3 加密后的权值发送给 P_4。再次利用式(7)计算密文状态下，频谱属性的权重和 $E_{\mathrm{pk}}\left(\sum_{j=1}^{3} w_j A_j\right)=\prod_{j=1}^{3}(A_j)^{w_j}=E_{\mathrm{pk}}(0.2)^{0.35}E_{\mathrm{pk}}(0.33)^{0.375}E_{\mathrm{pk}}(0.4)^{0.275}=E_{\mathrm{pk}}(0.2\times 0.35+0.33\times 0.375+0.4\times 0.275)=E_{\mathrm{pk}}(0.303\ 75)$。则加密的频谱决策效用函数值可利用式(8)计算得出，有 $E_{\mathrm{pk}}(\mathrm{Utility}(-b_1,\mathrm{AS}_1))=E_{\mathrm{pk}}\left(-b_{V_1}+\sum_{j=1}^{3} w_j A_j\right)=E_{\mathrm{pk}}(-0.1)E_{\mathrm{pk}}(0.300\ 5)=E_{\mathrm{pk}}(-0.1+0.303\ 75)=E_{\mathrm{pk}}(0.203\ 75)$。将密文状态下的频谱决策效用函数值 $E_{\mathrm{pk}}(0.203\ 75)$分别发送给其他频谱拍卖服务器($P_2$, P_3, P_4)以完成频谱拍卖竞标的全过程。

3) 判断拍卖赢家。当所有频谱拍卖服务器均收到密文状态下的频谱决策效用函数值后，$P_i(1\leqslant i\leqslant 4)$ 则利用各自的子密钥 s_i 解密，计算得到部分解密明文以及有效验证(c_1, proof_1)、(c_2, proof_2)、(c_3, proof_3)、(c_4, proof_4)，并将其发送给频谱买家。当频谱买家收到所有部分解密与有效验证时可利用式(9)恢复频谱决策效用函数值 $\mathrm{Utility}(-b_{V_1},\mathrm{AS}_{V_1})=0.203\ 75$。同理 $\mathrm{Utility}(-b_{V_2},\mathrm{AS}_{V_2})=0.384\ 25$，$\mathrm{Utility}(-b_{V_3},\mathrm{AS}_{V_3})=0.511$。根据式(3)可知，$\mathrm{Utility}(-b_{V_3},\mathrm{AS}_{V_3})$为频谱资源的最优方案，多属性逆向频谱拍卖的获胜者为频谱竞标人 C。

4 安全分析

PMRA 方案的安全协议是基于 Paillier 密码体制提出的，频谱投标人竞标值的隐私性依赖于 Paillier 密码体制。首先，对 Paillier 加密方案的安全性进行分析。其次，在提出的 PMRA 方案中，频谱拍卖人的频谱拍卖服务器可提供验证密文属性的有效性、部分解密密钥正确性的定理，并基于零知识证明给出交互式与非交互式证明过程。这确保了频谱拍卖服务器的可靠性与安全性。最后，为说明本文提出的频谱拍卖协议具有较强的安全性，本节不仅阐述了频谱拍卖方案所满足的安全特性，还给出本文方案协议与仅考虑价格单属性的正向频谱拍卖安全方案以及可应用到频谱拍卖场景下的多属性逆向拍卖安全方案的安全性比较。

4.1 Paillier 加密方案的安全性分析

定义 7 合数幂剩余类的判定。设 $N=pq$，p,q 为 2 个大素数，对于 $z\leftarrow_R Z^*_{N^2}$，如果存在 $y\in Z^*_{N^2}$，使等式 $z\equiv y^N \bmod N^2$ 成立，则 z 叫作模 N^2 的 N 次剩余。合数幂剩余类的判定问题是指区分模 N^2 的 N 次剩余，用 CR[N]表示。CR[N]是随机自归约的。设 $z_1\equiv y_1^N \bmod N^2$，$z_2\equiv y_1^N \bmod N^2$，那么可得 $z_2\equiv (y_2y_1^{-1})^{N_{z_1}} \bmod N^2$。如果 z_1 是 N 次剩余，那么 z_2 同理。即任意 2 个实例都是多项式等价的。猜想 CR[N]被称为判定合数幂剩余类假设（DCRA, decisional composite residuosity assumption）。

定义 8 计算合数剩余类假设。设 $g\in B$，且 $B\in Z^*_{N^2}$ 表示阶为 $n\alpha$ 的元素组成的集合，B 为 $B\alpha$ 的并集，其中 $\alpha=1,2,\cdots,\lambda$。对于 $\omega\in Z^*_{N^2}$，如果存在 $y\in Z^*_{N^2}$ 使 $\omega=\Phi_g(x,y)=g^x y^N \bmod N^2$，$g$ 为阶 N 的非零倍，则称 $x\in Z_N$ 为 ω 关于 g 的 N 次剩余，记作$[[\omega]]_g$。求$[[\omega]]_g$称为 g 的 N 次剩余类问题，表示为 Class[N, g]。由证明可得，Class[N, g]的复杂性与 g 无关，可将其看成仅依赖于 N 的计算问题[16]。即已知 $\omega\in Z^*_{N^2}$，$g\in B$，计算$[[\omega]]_g$，可记为 Class[N]问题。猜想不存在求解合数幂剩余类问题的概率多项式时间算法，即 Class[N]的困难问题。显然这仍旧被认为是一个困难问题。这一猜想被称为计算合数剩余类假设（CCRA, computational composite resi-

duosity assumption）。其随机自归约性使 CCRA 的有效性只依赖于 N 的选择，可知假设 DCRA 是正确的，则 CCRA 也是正确的。

Paillier 公钥加密方案系统是基于合数幂剩余类问题。当 Class[N]是困难的，即计算合数剩余类假设 CCRA 下，Paillier 加密方案是单向的（密文计算明文是 Class[N]问题）。当 CR[N]是困难的，即判定合数幂剩余类假设 DCRA 下，Paillier 加密方案是语义安全的。由此，Paillier 加密体制选择明文下的不可区分性则可通过实验的方式验证：存在攻击者 A（Adversary）、拥有加密算法的挑战者 C（Challenger）。A 根据加密算法生成密钥对(pk,sk)，保存私钥 sk，并将公钥 pk 发布并发送给 C。A 选取 2 个长度相等、值不同的明文 M_1、M_2 发送给 C。而 C 随机选取比特值 $b\in\{0,1\}$且将密文 $C_b=E_{\text{pk}}(M_b)$发送给 A。A 获取密文 C_b 对其任意计算操作，最后得到明文结果 b'，即当确定是对 M_1 加密还是 M_2 加密时，攻击者 A 猜出 b'的正确结果的优势是可忽略的。因此有 $\text{Adv}_A(E)=|\Pr[C\leftarrow E_{\text{pk}}(M_1)]-\Pr[C\leftarrow E_{\text{pk}}(M_2)]|=\varepsilon$。其中 ε 是可忽略的。虽然 A 知道 pk、M_1 与 M_2，由于 Paillier 加密的概率特性，M_b 则是众多密文中的一个，在游戏实验中，A 始终无法得到更多优势。

4.2　密文属性有效性与部分解密密钥 s_i 的正确性

PMRA 方案所提供的验证密文属性的有效性与部分解密密钥 s_i 的正确性不仅为频谱拍卖服务器提供了安全性和可靠性，还为频谱拍卖参与者的隐私性提供了有效的验证方法。因此，本节给出 PRMA 方案密文属性有效性与解密密钥 s_i 正确性的定理，并基于零知识证明给出交互式与非交互式的证明过程[16-18]。定理与证明过程如下。

定理 1　密文属性的有效性。频谱拍卖服务器 $P_i(1\leqslant i\leqslant n)$收到的 $E_{\text{pk}}(A_j)$一定来自对应明文属性集合，且不揭露 $E_{\text{pk}}(A_j)$的真实值。

证明

交互式。输入参数值 N,$S=\{a_1,a_2,a_3\}$，$\dfrac{E_{\text{pk}}(A_j)}{g^{a_1}}$，$\dfrac{E_{\text{pk}}(A_j)}{g^{a_2}}$，$\dfrac{E_{\text{pk}}(A_j)}{g^{a_3}}$，其中，$E_{\text{pk}}(A_j)=g^{m_j}r^N \bmod N^2$，$r\in Z_N^*$，$j$ 保密。证明者 P 随机选择 $x, b_1, b_2\in Z_N$ 并计算 $u_1=g^{b_1} \bmod N^2$，$u_2=g^{b_2} \bmod N^2$；证明者 P 再次随机选择 $w_1,w_2\in Z_N$ 并计算承诺值 $v_1=u_1^N\cdot\left(\dfrac{g^{a_1}}{E_{\text{pk}}(A_j)}\right)^{w_1} \bmod N^2$，$v_2=u_2^N\left(\dfrac{g^{a_2}}{E_{\text{pk}}(A_j)}\right)^{w_2} \bmod N^2$，$v_3=g^{xN} \bmod N^2$。$P$ 发送集合$\{v_1,v_2,v_3\}$到验证者 V，V 随机产生一个应答 $w\in Z_N$，P 则计算 $w_3=w-(w_1+w_2) \bmod N^2$，$u_3^N=g^{xN}r^{Nw_3}g^{w_3(a_3'-a_3)} \bmod N^2$，其中 a_3' 是 P 所产生 $E_{\text{pk}}(A_3)$对应的真正密文。当 $a_3'\in S$，P 为诚实证明者，且 $a_3'=a_3$；否则，P 是不诚实的，且有 $a_3'\neq a_3$。当 P 发送集合$\{u_1^n, u_2^n, u_3^n, w_1, w_2, w_3\}$到 V，则 V 判断等式是否成立，即 $u_1^n\overset{?}{=}v_1\left(\dfrac{E_{\text{pk}}(A_j)}{g^{a_1}}\right)^{w_1} \bmod N^2$，$u_2^n\overset{?}{=}v_2\left(\dfrac{E_{\text{pk}}(A_j)}{g^{a_2}}\right)^{w_2} \bmod N^2$，$u_3^n\overset{?}{=}v_3\left(\dfrac{E_{\text{pk}}(A_j)}{g^{a_3}}\right)^{w_3} \bmod N^2$，$e\overset{?}{=}E_{\text{pk}}(A_1)+E_{\text{pk}}(A_2)+E_{\text{pk}}(A_3) \bmod N$，以验证 $E_{\text{pk}}(A_j)$的有效性。

非交互式。设 H 为公开且抗碰撞的哈希函数，输出长度为 L。明文集合为 $S=\{m_1,m_2,\cdots,m_p\}$，明文 m_i 的密文为 $c_i=g^{m_i}x_i^N \bmod N^2$，其中，$i$ 是保密的。证明者 P 需要向验证者 V 表明他知道 $u=\dfrac{c_i}{g^{m_i}}=x_i^N \bmod N^2$ 的高阶 N 次剩余根 x_i。V 根据高阶 N 次剩余根的难解性，相信 c_i 对应明文 m_i 在指定的集合 S 中。则非交互式证明过程步骤如下。

1) 取值。P 随机选取 $x_1, x_2\in_R H$，$a_1,a_2\in_R Z_N$。

2) 输入。P,V 输入 $\mu_1=x_1^N\left(\dfrac{g^{m_1}}{E_{\text{pk}}(A_j)}\right)^{a_1} \bmod N^2$，$\mu_2=x_2^N\left(\dfrac{g^{m_2}}{E_{\text{pk}}(A_j)}\right)^{a_1} \bmod N^2$，$\mu_3=g^{rN} \bmod N^2$。

3) 生成挑战 $e=H\left(\mu_1,\mu_2,\mu_3,\dfrac{E_{\text{pk}}(A_j)}{g^{m_1}},\dfrac{E_{\text{pk}}(A_j)}{g^{m_2}},\dfrac{E_{\text{pk}}(A_j)}{g^{m_3}}\right)$，并计算应答 $a_3=e-(a_1+a_2) \bmod N$，有 $x_3^N=g^{Nx}r^{Na_3}g^{a_3(m_3'-m_3)} \bmod N$。

4) V 验证等式是否成立，因此有 $e\overset{?}{=}H\left(\mu_1,\mu_2,\mu_3,\dfrac{E_{\text{pk}}(A_j)}{g^{m_1}},\dfrac{E_{\text{pk}}(A_j)}{g^{m_2}},\dfrac{E_{\text{pk}}(A_j)}{g^{m_3}}\right)$，$\mu_i^N\overset{?}{=}x_i\left(E_{\text{pk}}\left(\dfrac{A_j}{g^{m_i}}\right)\right)^{ai} \bmod N^2$，$i$=1,2,3，$e\overset{?}{=}a_1+a_2+a_3 \bmod N$。

证毕。

定理 2　解密密钥 s_i 的正确性。频谱拍卖服务器 $P_i(1\leqslant i\leqslant n)$ 可以向任意一方证明在解密 $E_{\text{pk}}(\text{Utility}(-b_i, \text{AS}_i))$时使用的 s_i 是正确的，且不揭露任何 s_i 的真实值。

证明

交互式。公共输入值 N，$p=2p'+1$，$q=2q'+1$，有$|n|=k$且$|n|$为二级制的比特长度，$\S=p'q'$，$\mathrm{vk}=v^{\Delta}\bmod N^2$，$\mathrm{vk}_i=v^{\Delta s_i}\bmod N^2$，$c=c^{4\Delta}\bmod N$，$c_i^2=c^{4\Delta s_i}\bmod N^2$。证明者 P 输入 $s_i\in Z_{n\S}$并向验证者 V 证明存在某个 $s_i\in Z_{n\S}$满足等式 $\mathrm{vk}_i=(v^{\Delta})^{s_i}\bmod n^2$，$c_i^2=(c^{4\Delta}\bmod n^2)^{s_i}\bmod N^2$。$P$ 生成随机数 $w\in Z_N$，且计算$(x,y)\to c^{4\Delta w}\bmod N^2$，$v^{\Delta w}\bmod N^2$。之后 P 向验证者 V 发送(x,y)。V 选择任意 $a\in R$，$Z_{n\S}$发送给 P。P 计算 $b=w+s_ia$，并将 b 发送给 V。V 收到 b 并判断等式是否成立，即 $c^{4\Delta b}\bmod N^2\overset{?}{=}x(c_i^2)^a$ 和 $v^{\Delta b}\bmod N^2\overset{?}{=}y(\mathrm{vk}_i)^a$，以验证解密密钥 s_i 的正确性。

非交互式。设 H 为公开且抗碰撞的哈希函数，输出长度为 L。$P_i(1\leqslant i\leqslant n)$为向任意方证明 s_i 在解密密文 c 时产生的部分解密密文 c_i，在解密过程中确保不会泄露 s_i 的任何信息，即 $u=c^{4\Delta}\bmod N^2$，$c_i^2=c^{4\Delta s_i}\bmod N^2$，验证等式 $\log_u c_i^2=s_i$ 是否成立。则非交互式证明过程步骤如下。

1) 承诺。P 计算承诺(x,y)，且 $r\in\{0,\cdots,2^{|N|}-1\}$，$|N|$表示比特长度大小。$x=u^r\bmod N^2$，$y=v^r\bmod N^2$。

2) 挑战。$e=H(x,y,u,u',v,v')$，$u'=c^2$，$v'=v^{4\Delta s_i}$，利用哈希函数 H 计算挑战。

3) 计算应答。$z=r+es_i$，$e\in\{0,\cdots,2^{L+|N|}-1\}$，并生成证明 $\mathrm{proof}_i(e,z)$。

4) V验证并判断等式是否成立，即$e\overset{?}{=}H(u^z,u^{-e},v^z,v^{-e},u,u',v,v')$。若等式成立，则部分解密密钥 s_i 有效。

证毕。

4.3 频谱拍卖方案满足的安全特性

1) 隐私性

竞标方案中价格属性与非价格正向属性值始终是在密文状态下计算的，频谱买家与频谱拍卖人的服务器 P_i 无法得知真实的竞标信息，因此保护了竞标方案信息的隐私性。

2) 匿名性

在频谱竞标阶段，每个频谱竞标人利用匿名化技术与公钥pk得到一个临时的身份假名参与频谱拍卖。因此，频谱买家与每个频谱拍卖人都无法获取频谱竞标人的真实身份信息，确保频谱竞标人的匿名性。

3) 公平性

首先，频谱拍卖方案利用不经意传输技术使频谱竞标人无法确认每个频谱拍卖服务器 P_i 到底获取了哪一个加密的非价格正向属性值。其次，PMRA 方案利用 Paillier 门限机制使每个频谱拍卖服务器只拥有部分解密密钥 s_i，任意 P_i 都无法独自恢复加密后的明文信息，即频谱买家与其他任意参与方不存在共谋攻击。因此，确保了频谱拍卖安全协议执行的公平性。

4) 公开验证

由 4.2 节可知，基于 Paillier 门限的零知识证明协议使频谱拍卖服务器 $P_i(1\leqslant i\leqslant n)$不仅可以向频谱竞标人证明密文属性的有效性，还可以向任意参与方证明部分解密密钥 s_i 的有效性。

目前，常用的频谱拍卖方案大多只考虑单一价格、“一对多”模式的频谱拍卖。本文根据实际频谱拍卖场景，提出“多对一”模式的多属性逆向频谱拍卖方案。为分析频谱拍卖场景中所需的安全特性，本文方案与仅考虑单属性的正向频谱拍卖安全方案[19-23]，以及可应用于多属性逆向频谱拍卖场景的多属性逆向拍卖安全方案[24-25]进行安全性比较。如表 1 所示，本文所提出的 PMRA 方案安全协议的安全性较强。文献[19-25]方案将在第 6 节的相关工作中做简要介绍，这里不再阐述。

表 1 PMRA 方案安全协议与各方案的安全协议的安全性比较

方案	隐私性	匿名性	防止合谋	公开验证	有无第三方
文献[19]方案	满足	不满足	不满足	不满足	有
文献[20]方案	满足	满足	不满足	满足	有
文献[21]方案	满足	满足	不满足	满足	有
文献[22]方案	满足	不满足	不满足	不满足	有
文献[23]方案	满足	不满足	不满足	不满足	有
文献[24]方案	不满足	满足	不满足	满足	无
文献[25]方案	不满足	满足	不满足	不满足	有
PMRA 方案	满足	满足	满足	满足	有

5 性能评估

本文提出的频谱拍卖安全协议的计算开销主要来自 Paillier 门限机制的随机数生成、加密与解密、模幂运算操作。为便于描述协议的计算开销，设频谱竞标人的数量为 m、属性个数为 T、公钥加密操作记为 PKE、解密操作记为 PKD、模幂运算记为 ME、随机数生成记为 R。

在协议的初始化阶段，由可信机构作为 Paillier 门限机制密钥的生成者和分发者，产生公钥 pk、部分解密密钥 s_i、验证密钥 vk_i。则计算开销为 Paillier 机制的密钥初始化，所需要执行的操作为

2R+PKD+PKE+2ME。

在频谱拍卖的竞标阶段，每个频谱竞标人利用匿名化技术隐藏身份并用 pk 加密频谱的价格属性与非价格正向属性，则需要执行的操作为(T+1)PKE。其次，当所有 P_i 得到加密后的频谱决策效用函数值时，需要用各自的部分解密密钥 s_i 解密，执行的操作为(T+1)PKD。

在判断拍卖赢家阶段，频谱买家需要收到不少于 t 个频谱拍卖服务器的有效验证值(c_i, proof$_i$)，从而恢复明文得到频谱决策效用函数值，执行的相应操作为 2ME。因此，当频谱竞标人数量为 m、属性个数为 T 时，各阶段各参与方的计算开销如表 2 所示。

据表 2 分析可知，安全协议总体的计算开销与频谱竞标人的数量 m、属性个数 T 有关。当 m 增加时，各个参与方在各阶段的计算开销均相应增加，因此，安全协议总体的计算开销增加。当 T 增加时，竞标阶段频谱拍卖服务器与频谱竞标人所需的加密解密计算开销也随之增加，然而 T 的取值并不影响频谱买家在判断拍卖赢家阶段的计算开销。

为讨论 PMRA 方案的效率，可将其与应用于多属性逆向频谱拍卖场景下的匿名与可验证的多属性逆向拍卖（VMRA, anonymous and verifiable multi-attribute reverse auction）方案[24]、安全的在线可信的第三方多属性多轮逆向拍卖（SMRA, secure multi-attribute multi-round reverse auction using on-line trusted third party）方案[25]在计算开销上进行对比。通过分析 PMRA 方案、VMRA 方案与 SMRA 方案的安全协议，给出 3 个方案在各个阶段的计算开销如表 3 所示。

通过表 3 的计算开销分析，模拟 PRMA 方案与 VMRA 方案计算开销的实验结果，计算任务都运行在一台 PC 机（Windows7 32, Intel Core i5, GHZ processor, 1.86 GB of RAM）上。通过引入 MRICAL 库的 C 语言进行仿真实验[26]。由于 RSA 的计算消耗可简化为模幂的运算操作，且哈希操作与随机数的生成操作可以忽略不计。为便于本文方案协议的实验测试，加密操作 PKE 与解密操作 PKD 都可简化为模幂运算操作且记为 ME。在模幂运算中，定义素数 p 的长度分别为 512 bit、1 024 bit，则由此可计算出单个模幂运算的平均时间分别为 1.5 ms 与 6 ms。

由表 3 可知，在准备阶段，VMRA 方案与 PMRA 方案所消耗的运行时间均可忽略不计，而 SMRA 方案的加密操作则需要花费较多时间。对于中小规模的系统设计，设当 m>T（m=50，T=10），公钥长度 p 为 512 bit、1 024 bit 时，通过实验可得 VMRA 方案、SMRA 方案与 PMRA 方案完成一次拍卖后在各阶段所消耗的运行时间。则 VMRA 方案、SMRA 方案与 PMRA 方案在各个阶段所消耗的运行时间以及 3 个方案协议所消耗的总时间分别如图 3 和图 4 所示。

由图 3 与图 4 可知，在准备阶段，VMRA 方案与 PMRA 方案的运行时间均为 0，而 SMRA 方案在准备阶段需消耗一定的时间。设运行时间为 Tim，因此在准备阶段有 Tim(SMRA)>Tim(VMRA)=Tim(PMRA)。在竞标阶段，PMRA 方案、VMRA 方案与 SMRA 方案之间所需的运行时间相差无几，且 SMRA 方案所需的运行时间最小。因此，在竞标阶段有 Tim(VRMA)> Tim (PMRA)> Tim (SMRA)。在开标阶段，PMRA 方案不需要执行任何计算，因此运行时间为 0。而 VMRA 方案与 SMRA 方案均在此阶段消耗过多的运行时间。VMRA 方案在此阶段所需的运行时间是 SMRA 方案的 3 倍左右。因此，

表 2　　PMRA 方案协议各阶段各参与方的计算开销

阶段	可信机构 D	拍卖服务器	频谱需求用户	频谱竞标人
准备阶段	2R+PKD+PKE+2ME	—	—	—
竞标阶段	—	M(T+1)PKD	—	M(T+1)PKE
判断拍卖赢家阶段	—	—	2mME	—

表 3　　PMRA 方案协议与 VMRA、SMRA 方案协议在各阶段的计算开销

方案	准备阶段	竞标阶段	开标阶段	判断拍卖赢家阶段
VRMA	HF, 2R, PKE, PKD	[m(T+1) +2T],PKE[m(T+2) +2T] PKD	2mT PKE, m(T+1) PKD	2mT PKE
SMRA	HF, 2R, (m+3) PKE	mT PKE, mT PKD	mT PKE	mT PKD
PMRA	R, 2ME, PKE, PKD	m(T+1) PKE, m(T+1) PKD	—	2m ME

在开标阶段有 Tim(VRMA)> Tim (SMRA)> Tim (PMRA)。在判断拍卖赢家阶段，同样有 Tim(VRMA)> Tim (SMRA)> Tim (PMRA)。最后，通过比较 VMRA 方案、SMRA 方案与 PMRA 方案的运行总时间可知，PMRA 方案所消耗的运行时间远远低于其他 2 个方案。

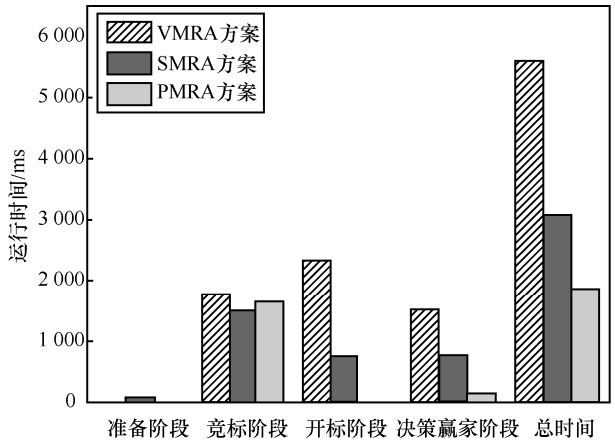

图 3　各个阶段运行时间（512 bit）

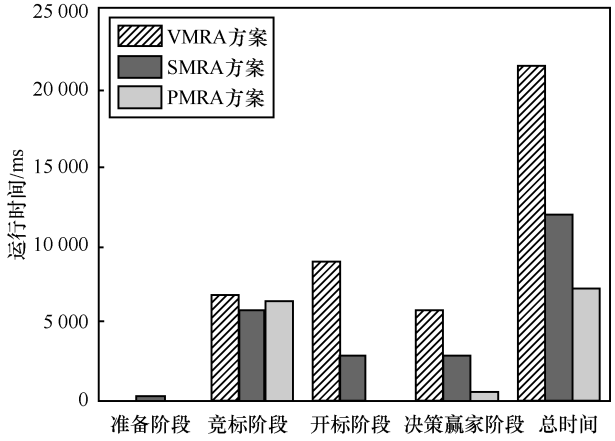

图 4　各个阶段运行时间（1 024 bit）

由于 VMRA 方案、SMRA 方案、PMRA 方案安全协议计算消耗所需的运行时间均与竞标人数 m 以及属性个数 T 有关，因此给出对于中小规模系统设计，公钥长度 p 为 512 bit 时的协议运行总时间分别与 m、T 取值关系的变化曲线（公钥长度 p 为 1 024 bit 同理，这里不再赘述），分别如图 5 和图 6 所示。

由图 5 可知，当 T=10 时，VMRA 方案、SMRA 方案与 PMRA 方案协议的运行总时间均随着竞标人数 m 的增加而呈线性递增的趋势。其中，PMRA 方案安全协议运行总时间递增的速率明显小于其他 2 个方案。由图 6 可知，当 m=50 时，VMRA 方案、SMRA 方案与 PMRA 方案协议的运行总时间随着属性个数 T 的增加呈线性递增趋势。同样地，PMRA 方案协议运行总时间的增长速率依然远小于 VMRA 方案与 SMRA 方案。由上述分析可知，随着 m 与 T 的增加，PMRA 方案的计算开销所花费的运行总时间远小于 VMRA 方案与 SMRA 方案。因此，在系统性能上，PMRA 方案要优于 VMRA 方案与 SMRA 方案。

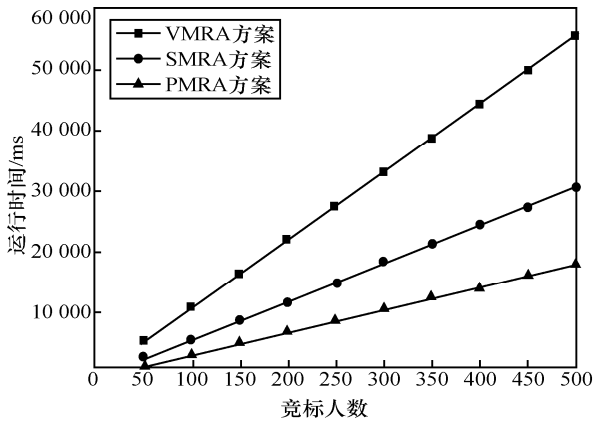

图 5　协议总运行时间（512 bit，T=10）

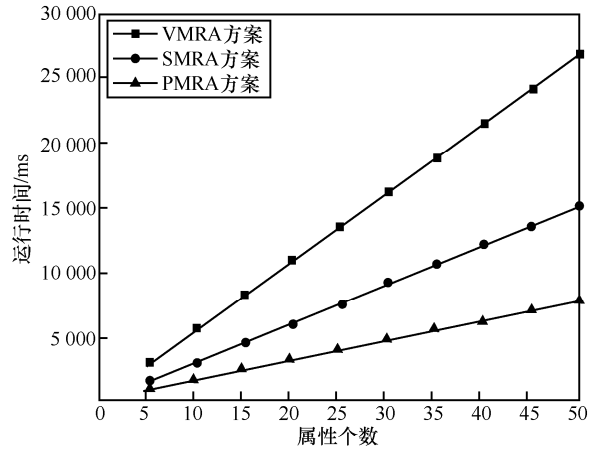

图 6　协议总运行时间（512 bit，m=50）

6　相关工作

近年来，频谱拍卖的安全性受到研究者们的广泛关注，根据频谱拍卖的应用场景和需求的不同，以价格展开博弈的单属性安全频谱拍卖主要分为三类，分别为单边频谱拍卖、双边频谱拍卖与组合频谱拍卖。

单边频谱拍卖是频谱交易市场中最常见的频谱拍卖类型之一，它广泛应用于一级频谱拍卖市场与二级频谱拍卖市场。“一对多”的正向频谱拍卖与“多对一”的逆向频谱拍卖均为单边频谱拍

卖。近年来，研究人员大都针对频谱价格这一单属性、“一对多”正向频谱拍卖的应用场景展开安全性研究。例如，Pan 等[19]提出一种安全的频谱拍卖方案，通过利用 Paillier 加密方案防止频谱竞标人与拍卖人之间的相互勾结。Huang 等[20]提出了防策略和隐私保护的频谱拍卖（SPRING, strategy-proof and privacy-preserving spectrum auction）方案，在确保竞标人隐私性的同时满足 K 匿名等特性。Wu 等[21]提出保护隐私与防策略的频谱拍卖（PRIDE, privacy-preserving and strategy-proof spectrum auction）方案，又在 SPRING 方案基础之上实现了 L-多样性。Huang 等[22]提出一个防策略的隐私保护频谱拍卖框架（PSS, privacy-preserving strategy-proof spectrum auction framework），旨在保护频谱竞标人的真实估值。Chen 等[23]提出了频谱拍卖安全框架，在保护竞标价格隐私性的同时保护了竞标人的地理位置信息。Wang 等[27]提出了可验证且隐私保护的频谱拍卖（SPSV, privacy-preserving spectrum auction with public verification）方案，在保护频谱竞标人信息隐私性的同时，提供了公开验证机制，可使方案在频谱拍卖期间不会向其他参与方透露任何敏感信息。

双边频谱拍卖广泛应用于频谱交易的二级市场。首个双边频谱拍卖方案是在 2010 年提出的，其安全问题引起了人们的关注[28]，研究人员就此展开关于双边频谱拍卖的安全性研究。例如 Chen 等[29]提出了可证明安全的双边频谱拍卖（PS-TRUST, provably secure double spectrum auction）方案，方案为半诚实的对手提供可证明的安全性，并保护了频谱竞标信息的隐私性。Chen 等[30]提出的安全、高效、实用的双边频谱拍卖（SDSA, secure, efficient and practical double spectrum auction）方案可使频谱拍卖中只揭示频谱拍卖结果，从而保护频谱竞标人的隐私性。Wang 等[31]设计的保密且真实的在线双边频谱拍卖（PROST, privacy-preserving and truthful online double auction for spectrum allocation）方案在保护频谱竞标人敏感信息的同时，确保了频谱竞标人的地理位置信息、时间动态的隐私性。

频谱组合拍卖在频谱交易市场上出现较少，组合频谱拍卖针对特定的频谱交易场景，允许频谱竞标人因频谱的多样性特点而对各种频谱进行组合竞标。Pan 等[32]首次提出了安全的组合频谱拍卖（SCSA, secure combinatorial spectrum auction）方案，该方案解决拍卖人与频谱竞标人共谋操纵投标的安全问题。Chen 等[33]提出了一种针对异构频谱的安全组合拍卖，该方案不仅保护了竞标值与地理位置信息，还提供了可验证的支付方案，以防拍卖人伪造付款。

当频谱管理部门回收频谱资源时，“多对一”逆向的频谱拍卖往往需要考虑除频谱竞标价格以外的频谱正向属性因素，以保证在未来重新分配频谱时，为不同服务业务的频谱需求用户提供更优质的频谱资源，从而提高频谱利用率。已有的多属性逆向拍卖安全方案[24-25]可应用到上述提出的逆向频谱拍卖的场景当中。Srinath 等[24]提出了 VMRA 方案。该方案主要为多属性逆向拍卖提供了公开可验证性与匿名性。同年，他又提出了 SMRA 方案[25]，为竞标人提供了匿名性、不可否认性等安全特性，在一定程度上保护了多属性逆向拍卖的安全性。虽然 VMRA 方案与 SMRA 方案都可应用到多属性的逆向频谱拍卖中，但根据第 4.3 节的安全特性分析可知，VMRA 方案与 SMRA 方案并不能满足频谱拍卖所需的安全性。并且在第 5 节的性能评估中，PMRA 方案的系统效率要优于其他 2 个方案，PMRA 方案的系统所需运行时间远低于 VMRA 方案与 SMRA 方案。因此，本文方案在所提出的逆向频谱拍卖场景中，可确保频谱拍卖的安全性并使频谱管理部门高效、合理地回收优质的频谱资源。

7　讨论

本节主要讨论频谱拍卖系统的扩展性。由 PMRA 方案可知，频谱拍卖服务器的数量和频谱属性呈正相关。当频谱属性增加时，频谱拍卖服务器也随之增加。在实际频谱拍卖的应用中，系统不可能因属性的增多而增加相同数量的频谱拍卖服务器。针对这一问题，本文可以将多个属性值（价格与非价格正向属性值）按照一定的规则进行分组，以小组的形式分别对应特定的频谱拍卖服务器，从而进行相应的数据运算以提高系统的扩展性。而当频谱拍卖服务器或频谱竞标人增加时，频谱竞标人与频谱拍卖服务器、频谱买家与频谱拍卖服务器之间的通信量都会随之增加，这可能导致系统性能的下降。另外，作为以拍卖交易而盈利的频谱拍卖人，随着频谱拍卖服务器的增加，频谱拍卖人的交易费

用也随之增加，这也增加了系统的额外交易费用。如何优化系统性能并减少频谱拍卖人的交易费用是本文今后需要研究的内容。

8 结束语

本文提出一个面向隐私保护的 PMRA 方案。首先，PMRA 方案将除频谱价格外其他影响频谱二次分配的频谱正向属性考虑在内，频谱竞标人提供含有频谱竞标价格与频谱正向属性值的竞标方案参与频谱拍卖。利用 Paillier 加密方案及其门限机制、匿名化技术以及不经意传输技术的密码学工具确保频谱拍卖所需的安全特性，使频谱拍卖协议安全地执行。其次，PMRA 方案的安全分析表明，本文所提出的频谱拍卖协议具有较强的安全性。对 PMRA 方案进行性能评估，实验结果表明，PMRA 方案的效率优于已有的多属性逆向拍卖 VMRA 方案和 SMRA 方案。最后，讨论了 PMRA 方案系统的扩展性问题。

本文仅考虑当频谱买家所选择的频谱属性均为正向属性时，通过利用线性加权法以计算频谱决策效用函数值来判断频谱拍卖赢家。然而在实际复杂的逆向频谱拍卖场景中，频谱的非价格属性例如原频谱的不同服务地区、原频谱的服务人口数量等因素并非都为正向属性。而在讨论 PRMA 方案的系统扩展性问题时，随着服务器的增加，频谱拍卖人的交易费用也随之额外增加。因此，如何设计出更适用于复杂逆向频谱拍卖场景下的频谱决策效用函数，以及如何优化系统性能以减少系统额外的交易费用等问题则是未来工作中需要研究和探讨的主要内容。

参考文献：

[1] AL-KINANI A, WANG C X, ZHOU L, et al. Optical wireless communication channel measurements and models[J]. IEEE Communications Surveys & Tutorials, 2018, 20(3): 1939-1962.

[2] CHOWDHURY M Z, HASAN M K, SHAHJALAL M, et al. Opportunities of optical spectrum for future wireless communications[C]//2019 International Conference on Artificial Intelligence in Information and Communication. Piscataway: IEEE Press, 2019: 4-7.

[3] ZHAO F, TANG Q. A KNN learning algorithm for collusion-resistant spectrum auction in small cell networks[J]. IEEE Access, 2018, 6: 45796-45803.

[4] YADAV I, KULKARNI A A, KARANDIKAR A. Strategy-proof spectrum allocation among multiple operators[C]//2019 IEEE Wireless Communications and Networking Conference. Piscataway: IEEE Press, 2019: 1-6.

[5] 万屹. 全球首次频谱资源激励拍卖带给我们的启示[J]. 中国无线电, 2017(11): 37-38.
WAN Y. Enlightenment from the world's first spectrum resource incentive auction[J]. China Radio, 2017(11): 37-38.

[6] 余莉娟. 激励拍卖: 利用市场手段加速频谱转让的新手段[J]. 世界电信, 2015(12): 50-53.
YU L J. Incentive auction: new means to use market to accelerate spectrum transfers [J]. World Telecommunications, 2015(12): 50-53.

[7] TEICH J E, WALLENIUS H, WALLENIUS J, et al. A multi-attribute e-auction mechanism for procurement: Theoretical foundations[J]. European Journal of Operational Research, 2006, 175(1): 90-100.

[8] GOLDREICH O. On the foundations of cryptography[M]. NewYork: ACM Books, 2019: 411-496.

[9] BRICKELL J, SHMATIKOV V. Privacy-preserving graph algorithms in the semi-honest model[C]//International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2005: 236-252.

[10] FOUQUE P A, POUPARD G, STERN J. Sharing decryption in the context of voting or lotteries[C]//International Conference on Financial Cryptography. Berlin: Springer, 2000: 90-104.

[11] PAILLIER P. Public-key cryptosystems based on composite degree residuosity classes[C]//International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 1999: 223-238.

[12] SHOUP V. Practical threshold signatures[C]//International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2000: 207-220.

[13] BEIL D R, WEIN L M. An inverse-optimization-based auction mechanism to support a multiattribute RFQ process[J]. Management Science, 2003, 49(11): 1529-1545.

[14] SCHARTNER P, SCHAFFER M. Unique user-generated digital pseudonyms[C]//International Workshop on Mathematical Methods, Models, and Architectures for Computer Network Security. Berlin: Springer, 2005: 194-205.

[15] TZENG W G. Efficient 1-out-of-n oblivious transfer schemes with universally usable parameters[J]. IEEE Transactions on Computers, 2004, 53(2): 232-240.

[16] BAUDRON O, FOUQUE P A, POINTCHEVAL D, et al. Practical multi-candidate election system[C]//Proceedings of the Twentieth Annual ACM Symposium on Principles of Distributed Computing. New York: ACM Press, 2001: 274-283.

[17] DAMGÅRD I, JURIK M. A generalisation, a simplication and some applications of paillier's probabilistic public-key system[C]// International Workshop on Public Key Cryptography. Berlin: Springer, 2001: 119-136.

[18] FIAT A, SHAMIR A. How to prove yourself: practical solutions to identification and signature problems[C]//Conference on the Theory and Application of Cryptographic Techniques. Berlin: Springer, 1986: 186-194.

[19] PAN M, SUN J, FANG Y. Purging the back-room dealing: secure spectrum auction leveraging paillier cryptosystem[J]. IEEE Journal on Selected Areas in Communications, 2011, 29(4): 866-876.

[20] HUANG Q, TAO Y, WU F. Spring: a strategy-proof and privacy preserving spectrum auction mechanism[C]//2013 Proceedings IEEE INFOCOM. Piscataway: IEEE Press, 2013: 827-835.

[21] WU F, HUANG Q, TAO Y, et al. Towards privacy preservation in strategy-proof spectrum auction mechanisms for noncooperative wireless networks[J]. IEEE/ACM Transactions on Networking, 2014, 23(4):

1271-1285.

[22] HUANG H, LI X Y, SUN Y, et al. PPS: privacy-preserving strategy-proof social-efficient spectrum auction mechanisms[J]. IEEE Transactions on Parallel and Distributed Systems, 2014, 26(5): 1393-1404.

[23] CHEN Z, CHEN L, HUANG L, et al. Towards secure spectrum auction: both bids and bidder locations matter: poster[C]//Proceedings of the 17th ACM International Symposium on Mobile Ad Hoc Networking and Computing. New York: ACM Press, 2016: 361-362.

[24] SRINATH T R, SINGH M P, PAIS A R. Anonymity and verifiability in multi-attribute reverse auction[J]. arXiv Preprint, arXiv: 1109.0359, 2011.

[25] SRINATH T R, KELLA S, JENAMANI M, et al. A new secure protocol for multi-attribute multi-round e-reverse auction using online trusted third party[C]//International Conference on Emerging Applications of Information Technology. Piscataway: IEEE Press, 2011: 149-152.

[26] NJAH H, JAMOUSSI S, MAHDI W. Deep Bayesian network architecture for big data mining[J]. Concurrency and Computation: Practice and Experience, 2019, 31(2): e4418.

[27] WANG J, KARUPPIAH M, KUMARI S, et al. A privacy-preserving spectrum auction scheme using paillier cryptosystem with public verification[J]. Journal of Intelligent & Fuzzy Systems, 2019, doi: 10.3233/JIFS-169979.

[28] WANG S G, XU P, XU X H, et al. TODA: truthful online double auction for spectrum allocation in wireless networks[C]//2010 IEEE Symposium on New Frontiers in Dynamic Spectrum. Piscataway: IEEE Press, 2010: 1-10.

[29] CHEN Z, HUANG L, LI L, et al. PS-TRUST: provably secure solution for truthful double spectrum auctions[C]//IEEE INFOCOM 2014-IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2014: 1249-1257.

[30] CHEN Z, WEI X, ZHONG H, et al. Secure, efficient and practical double spectrum auction[C]//2017 IEEE/ACM 25th International Symposium on Quality of Service. Piscataway: IEEE Press, 2017: 1-6.

[31] WANG Q, HUANG J, CHEN Y, et al. $ PROST $: privacy-preserving and truthful online double auction for spectrum allocation[J]. IEEE Transactions on Information Forensics and Security, 2018, 14(2): 374-386.

[32] PAN M, ZHU X, FANG Y. Using homomorphic encryption to secure the combinatorial spectrum auction without the trustworthy auctioneer[J]. Wireless Networks, 2012, 18(2): 113-128.

[33] CHEN Y, TIAN X, WANG Q, et al. ARMOR: a secure combinatorial auction for heterogeneous spectrum[J]. IEEE Transactions on Mobile Computing, 2019, 18(10): 2270-2284.

[作者简介]

王佳琪（1989− ），女，吉林长春人，东北大学博士生，主要研究方向为网络信息安全、电子拍卖安全、频谱拍卖安全。

鲁宁（1984− ），男，内蒙古包头人，博士，东北大学副教授，主要研究方向为网络安全。

程庆丰（1979− ），男，辽宁朝阳人，博士，信息工程大学副教授，主要研究方向为公钥密码学、密码协议。

巫朝霞（1975− ），女，广东揭西人，博士，新疆财经大学副教授，主要研究方向为信息安全。

史闻博（1980− ），男，河北唐山人，博士，东北大学秦皇岛分校教授，主要研究方向为应用密码学、网络安全、信息系统安全、网络攻击与防范、信息隐藏理论与技术、物联网安全、网络对抗。