基于身份的联盟链密封电子拍卖协议

徐哲清[1], 王宇航[1], 王志伟[1], 刘 峰[2]

[1]南京邮电大学计算机学院 南京 中国 210023
[2]中国科学院信息工程研究所信息安全国家重点实验室 北京 中国 100093

摘要 密封电子拍卖是一种保护出价隐私的线上拍卖方式, 可以最大程度地减小投标者的出价策略导致的成交价格与商品真实价值的偏差。但是传统的密封电子拍卖方案依赖一个可信第三方, 这导致了高昂的拍卖成本和出价隐私泄露的风险。近年来, 去中心化的区块链技术迅速发展, 给密封电子拍卖方案的设计提供了新的思路, 一些研究提出了结合区块链的去中心化优势来减少或去除对第三方的依赖, 然而这些方案都基于公钥密码学, 由于区块链系统的开放性, 往往拥有较多的客户端数量, 维护公钥基础设施需要高昂的成本, 这使得这些方案难以在实际中应用。为了解决现有方案依赖于公钥基础设施的问题, 本文将基于身份的加法同态加密算法应用于安全多方整数比较协议, 并使用联盟链作为协议的通信交互平台, 提出一种基于身份的联盟链密封电子拍卖协议, 实现了在不需要可信第三方和公钥基础设施的情况下, 使用三轮通信交互即可完成密封拍卖的出价比较和排名证明。安全性方面, 我们通过理论证明了我们的方案在半诚实模型下, 仅有一名诚实的投标者时也不会泄露任何投标者的出价隐私。我们基于 Hyperledger Fabric 联盟链实现了我们的密封电子拍卖协议, 并进行实验与其他现有方案对比, 实验结果表明我们的方案在计算开销和通信开销方面都有较大的优势。

关键词 密封电子拍卖; 联盟链; 基于身份的加密; 同态加密; 安全多方计算
中图法分类号 TP309 DOI 号 10.19363/J.cnki.cn10-1380/tn.2025.01.03

Identity-based Sealed Bid Auction Protocol on Consortium Blockchain

XU Zheqing[1], WANG Yuhang[1], WANG Zhiwei[1], LIU Feng[2]

[1] School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China
[2] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

Abstract A type of online auction known as an electronic sealed bid auction which protects the privacy of bidders while decreasing the distance between the transaction price and the actual value of the item generated by participants' bidding strategies. On the other hand, conventional sealed electronic auction techniques all rely on a trustworthy third party, which rises the cost of the auction and increases the risk of bidder confidentiality leaks. Decentralized blockchain technology has grown rapidly in recent years, offering fresh perspectives on how to construct sealed electronic auction solutions. Some research has proposed utilizing the blockchain's decentralized benefits to reduce or do away with the need for third intermediaries. However, all these solutions rely on public key cryptography, but as blockchain systems frequently have numerous users due to property of open, maintaining a public key infrastructure is both expensive and problematic. This has made using these methods in real world situations difficult. This work uses identity-based additively homomorphic encryption algorithms to secure multi-party integer comparison protocols in order to overcome the issue of reliance on a public key infrastructure in prior solutions. It suggests an identity-based consortium blockchain sealed electronic auction system, with a consortium blockchain serving as the protocol's platform for communication and interaction. Through three rounds of communication, this protocol accomplishes the comparison and ranking evidence of sealed bids in a sealed auction without the use of a third party or a public key infrastructure. In terms of security, we present theoretical proof that, even in the case of only one single honest bidder, our protocol does not reveal any bidder's privacy in the semi-honest model. We implemented our sealed electronic auction protocol based on the Hyperledger Fabric consortium blockchain and conducted experiments to compare it with other existing approaches. The experimental results show that our solution has considerable cost-savings and efficiency benefits.

Key words sealed bid auction; consortium chain; identity-based encryption; homomorphic encryption; multi-party computation

---

通讯作者: 徐哲清, 本科, Email: 1021041521@njupt.edu.cn。

本文受到国家自然科学基金项目资助(No. 62372245)、2022 年信息安全国家重点实验室开放课题项目(No. 2022-MS-5)、江苏省研究生科研与实践创新计划项目(No. KYCX22_0987)资助。
收稿日期: 2023-05-22; 修改日期: 2023-08-14; 定稿日期: 2024-11-14

1 引言

电子拍卖作为电子商务的重要部分, 在线上交易中发挥着重要作用, 这种特殊的交易形式可以为那些难以定价的商品(如艺术品、二手商品)寻找到合适的价格, 因而极大程度地丰富了线上市场的商品种类, 促进了贸易流通。传统的拍卖形式主要分为英格兰式拍卖、荷兰式拍卖、密封投标式拍卖这三种形式, 其中密封投标式拍卖的主要优点在于任何参与拍卖的投标者都无法了解任何其他投标者的出价信息, 从而可以避免投标者在拍卖过程中使用拍卖策略使得商品成交价格与商品的真实价值产生较大偏差[1]。

在密封电子拍卖协议的设计中, 最重要的问题是在不泄露投标者的出价隐私的情况下, 计算出满足中标条件的出价[1-2]。现有的大多数方案都是基于一个可信或者半可信的第三方拍卖师构建的, 然而在现实中很难保证第三方的可信程度, 一旦第三方与恶意方勾结, 或者第三方遭到了无法预期的安全攻击, 所有投标者的出价信息都将泄露, 密封投标式拍卖也就失去了实用意义。此外, 可信第三方的存在也会进一步增加拍卖的成本, 这可能导致密封投标式拍卖无法适用于一些价值较低的商品, 因为支付给可信第三方的费用甚至可能超过了商品本身的价值。造成这些问题的本质原因是传统第三方拍卖的中心化程度过高, 整个协议的安全性依赖于对单一实体的信任。自 2008 年, 中本聪首次提出名为比特币的加密货币技术以来[3], 区块链作为一种搭建去中心化系统的新技术在过去的十年里蓬勃发展, 在全世界范围内取得了巨大的成功。区块链可以看作是一本中心化的账本, 它融合了密码学、点对点(P2P)网络和共识机制等多种技术, 账本由参与系统的所有节点共同维护, 并通过数字签名、哈希函数等密码学技术与共识机制相结合, 构建了一种全新的信任机制, 消除了对单一实体的依赖, 具有去中心化、防篡改、透明和安全等特点。2014 年, 随着以太坊的诞生, 图灵完备的智能合约为区块链带来了可编程性[4-5], 使得区块链可以应用于各种实际场景中构建去中心化系统, 如物流系统、能源交易、医疗保健等[6-9]。区块链按照去中心化程度主要可以分为公开链、联盟链和私有链。其中公开链的特点是高度去中心化, 不需要任何可信第三方, 但是由于耗时的共识算法, 公开链的效率非常低; 私有链虽然有最高的效率但是中心化程度太高, 与传统中心化系统并无本质区别; 而联盟链则在具有高通信效率、高吞吐量的情况下仍保持着较高的去中心化程度[10]。

由于区块链天然具有去中心化的特点, 因此适合用来构建去中心化的拍卖系统。事实上, 现实中早已出现使用区块链作为拍卖平台的实践。2018 年, 艺术家 Andy Warhol 所创作的价值数百万美元的艺术品通过以太坊区块链成功拍卖出售[11], 因此我们可以预见, 这种基于区块链竞拍物品所有权的机制将在未来逐渐流行。然而基于区块链搭建密封电子拍卖系统是充满挑战性的, 区块链具有去中心化、不可篡改等优势的同时, 也具有透明性, 即任何上链的信息都是公开的, 而密封电子拍卖协议却需要保护投标者的出价隐私, 这与区块链的透明性相矛盾, 也是基于区块链搭建密封电子拍卖系统的最大挑战。

目前一些研究给出了几种在区块链进行上的密封电子拍卖的方案。文献[12]基于 ZK-SNARK、安全多方计算、公钥加密和承诺等密码原语设计了基于区块链的密封电子拍卖方案, 并通过以太坊智能合约实现了系统; 类似的, 文献[13]基于同态承诺方案和范围零知识证明方案设计了密封电子拍卖方案。然而以上两种方案都需要借助第三方拍卖商, 并向第三方拍卖商打开自己的出价承诺才能完成拍卖, 并没有完全地做到对投标者的投标的隐私保护。换句话说, 虽然上述两种方案利用了区块链的透明性和不可篡改性的特点, 避免了拍卖商篡改投标的恶意攻击, 然而上述方案并没有做到完全的去中心化, 仍然需要对一个第三方拍卖商给予一定程度的信任, 一旦拍卖商与恶意投标者勾结则仍然有秘密投标被泄露的风险。此外, 上述方案涉及到的零知识证明需要多轮交互, 性能上也不够优秀。文献[14]提出一种完全不需要可信第三方的方案, 该方案将拍卖出价比较的问题转化为了安全多方计算中经典的百万富翁问题[15], 即两个百万富翁在不透露自己的资产的情况下如何比较谁更富有, 把资产换成出价即成了密封拍卖中任意两方的出价比较问题。百万富翁问题在安全多方计算领域目前研究成果广泛[16-17], 文献[14]基于同态加密下的秘密值大小比较协议以及非交互式的零知识证明实现了完全去中心化的密封电子拍卖。

目前有关密封电子拍卖的研究已经做到去中心化, 但是据我们所知目前所有的方案都是基于公钥加密体制, 例如文献[14]中需要假设所有投标者都有自己的长期公钥, 并且在协议开始进行时进行一轮可验证秘密共享来商议会话的临时私钥以及私钥的

证明, 也就是说方案需要所有投标者提供自己的公钥证书才能保证方案的安全性, 这就导致该方案需要额外的认证阶段交互轮次以及繁琐昂贵的公钥基础设施。

基于身份的密码概念由 Shamir[18]于 1984 年提出, 在这种密码体制中, 用户的任何身份信息例如 IP 地址、电子邮箱地址都可以代替数字证书作为用户的公钥用于加密和签名, 这样的密码体制不需要公钥基础设施, 从而可以极大地降低系统的复杂度。本文提出一种基于身份的密封电子拍卖方案, 目的在于解决过去的密封电子拍卖方案对公钥基础设施的依赖问题[19]。Boneh 和 Franklin[20]基于双线性配对提出了第一个实用并且安全的基于身份的加密算法, Günther 等人[21]基于 Boneh 和 Franklin 的方案进行改进, 得到了具有加法同态性质的基于身份的加密算法, 本文称之为 AIBE(Additively Homomorphic IBE)。我们的方案使用基于身份的同态加密和隐私整数比价协议, 并基于联盟链实现, 方案的主要优点如下: (1) 我们的方案同样可以在不需要可信第三方拍卖商的情况下计算出满足中标条件的出价, 并且我们使用的加密算法和签名算法都是基于身份的算法, 并不依赖于高成本的公钥基础设施, 系统的复杂度更低; (2) 我们的方案基于 Hyperledger Fabric 作为实现平台, 相比于公开链, Fabric 具有更高的效率和安全性。

本文剩余的结构如下: 第二节将介绍与本文内容相关的背景知识; 第三节中会描述本文的系统模型以及协议的具体流程; 接着第四节将会给出协议的安全性证明和成本分析; 第五节中可以看到协议的基于 Fabric 区块链实现的结果和分析; 最后第六节将对全文工作进行总结。

2 背景知识

本节将介绍我们的方案需要的密码学与区块链的背景知识。在本文中, 使用 Z 表示整数集合, p 表示一个大素数, Z_p 表示模 p 的整数集合, 即 $Z_p=\{0,1,...,p-1\}$。对于任意集合 B, $b\in_R B$ 表示 b 是从集合 B 中均匀随机抽取的元素。

2.1 双线性配对

首先我们回顾一下对称的双线性配对的定义, 假设 G 和 G_T 是具有素数阶 p 的循环群, 令 $e:G\times G\to G_T$ 为一个双线性映射, 若该双线性映射满足以下条件, 则该映射为双线性配对:

双线性: 对于 $\forall g_1,g_2\in G,a_1,a_2\in Z_p$, 满足 $e(g_1^{a_1},g_2^{a_2})=e(g_1,g_2)^{a_1a_2}$;

非退化性: $\exists g\in G$, 使得 $e(g,g)\neq 1$;

可计算性: 对于 $\forall g_1,g_2\in G$, 存在算法可以有效地计算 $e(g_1,g_2)$。

2.2 Diffie-Hellman 困难问题假设

双线性判定型 Diffie-Hellman 问题: 假设群生成算法生成一组对称的素数阶双线性群 (p,G,G_T,e)。对于一个概率多项式时间的敌手 A, 给定敌手 A 一个元组 $(g,p,e,g^{x_1},g^{x_2},g^{x_3})$, 其中 $x_1,x_2,x_3\in_R Z_p$, g 为 G 群生成元, $h_0=e(g,g)^{x_1x_2x_3}$, $h_1=e(g,g)^{\omega}$, $\omega\in_R Z_p$, $b\in_R\{0,1\}$。DBDH 难题假设敌手 A 在上述挑战的优势 $|\Pr[A(g,p,e,g^{x_1},g^{x_2},g^{x_3},h_b)=b]-1/2|$ 是可以忽略不计的。

2.3 基于身份的同态加密算法 AIBE

Günther 等人[21]提出的基于身份的同态加密算法的细节如下:

初始化 Setup(1^{κ}): 输入安全参数 κ, 生成双线性群 (p,G,G_T,e), 并随机选取生成元 $g\in_R G,g_T\in_R G_T$, 此外私钥生成中心(Private Key Generator, PKG)随机选择 $x\in_R Z_p$ 作为它的主私钥, 并令 $y=g^x$ 作为 PKG 的主公钥。然后选择一个密码学哈希函数 $H:\{0,1\}^*\to G$, 系统公共参数为 $param=(p,G,G_T,e,g,g_T,y,H)$。

提取 Extract $(x,param,ID)$: 输入公共参数 $param$、PKG 的私钥 x 以及一个身份字符串 $ID\in\{0,1\}^*$, 输出该身份对应的私钥 $d_{ID}=H(ID)^x$。

加密 Enc (y,ID,M): 输入主公钥 y、身份 ID 和明文 $m\in Z_p$, 并随机选择 $r\in_R Z_p$, 输出密文 $C=(C_1,C_2)=(g^r,g_T^m e(H(ID),y)^r)$。

解密 Dec (C,d_{ID}): 输入密文 C 和加密使用的公钥对应的私钥 d_{ID}, 输出 $\overline{m}=C_2/e(d_{ID},C_1)=g_T^m$, 然后求解 $\overline{m}$ 关于 g_T 的离散对数问题即可恢复明文 m (当 m 的取值范围较小时, 求解离散对数问题是可行的)。

AIBE 具有加法同态性, 将两个密文的元素分别相乘后即可得到明文相加后再加密的密文结果, 即:

$$\begin{aligned} &c\cdot c' \\ &=(g^r\cdot g^{r'},\overline{g}^m\cdot e(H(ID),y)^r\cdot\overline{g}^{m'}\cdot e(H(ID),y)^{r'}) \\ &=(g^{r+r'},\overline{g}^{m+m'}\cdot e(H(ID),y)^{r+r'}) \\ &=\mathrm{Enc}(y,ID,m+m') \end{aligned} \tag{2.1}$$

同时, 一个明文与一个密文可以进行如下计算得到明文相乘后再加密的密文:

$$\begin{aligned} & c^{m'} \\ &= (g^{rm'}, \bar{g}^{mm'} \cdot e(H(ID), y)^{rm'}) \\ &= \mathrm{Enc}(y, ID, m \cdot m') \end{aligned} \tag{2.2}$$

在 DBDH 假设成立的情况下, AIBE 可以在随机预言机模型下证明为选择身份和明文攻击下的语义安全(IND-ID-CPA)。

2.4 Hyperledger Fabric

Hyperledger Fabric 是一个企业级分布式账本技术(DLT)平台, 由 Linux 基金会的 Hyperledger 项目托管和维护。它是 Hyperledger 项目中最成熟和广泛使用的平台之一, 专为构建可扩展、高性能、安全和灵活的企业级区块链解决方案而设计[22]。

相较于比特币、以太坊这种完全去中心化的区块链, Fabric 具有以下特点:

高性能: Hyperledger Fabric 使用了不同的架构并且支持多种更高效率的共识算法, 以支持高吞吐量和低延迟的交易处理, 从而适用于更多的企业级应用场景。

隐私性: Hyperledger Fabric 支持多通道, 可以在不同的通道中实现不同的隐私和访问控制策略, 通道内的账本数据仅加入到该通道内的成员可见, 从而使得企业间交互更加安全和可信。而以太坊是一个公开的区块链网络, 所有的交易都是公开的, 无法满足企业应用的隐私和安全需求。

许可性: Hyperledger Fabric 提出了成员关系服务提供者 MSP(Membership Service Provider)的概念, MSP 为 Fabric 提供了用户管理与权限验证的功能, 使得参与者可以被分配到不同的角色和权限, 从而提高了链上交易的安全性和可信度。

3 协议设计

本节将介绍我们的密封电子拍卖协议具体的设计细节, 首先我们将介绍拍卖协议的整体系统模型, 随后我们会按照协议的执行流程介绍协议执行过程中的每一轮的细节。

3.1 系统模型

本小节将从两个方面介绍方案的系统模型, 一个方面是拍卖方案的通信模型, 即模型中有哪些方以及他们之间如何交互信息; 另一方面则是对协议执行过程的概括性描述。

方案的通信模型如图 1 所示, 拍卖过程主要需要以下各方参与: n 位参与拍卖的投标者($n \geqslant 2$), 负责提供身份私钥提取服务的私钥生成中心 PKG (Private Key Generator)。PKG 需要由一个可信第三方担任, 但是该第三方在完成密钥的分配之后就不再参与之后的拍卖过程, 因此该第三方需要承担的计算量很小, 并且不需要加入到举行拍卖的 Hyperledger Fabric 通道中, 在通道的隔离机制下, 拍卖过程的交互数据对 PKG 并不可见, 因此无论是成本上还是安全性上 PKG 和一般方案中的可信第三方都存在本质区别。投标者在链下通过安全信道与 PKG 交互获取自己的身份私钥, 并且我们假设投标者彼此了解对方的身份。密钥生成完毕后, 所有投标者加入到 Hyperledger Fabric 中同一个通道中, 通道中将部署一个用于广播信息的智能合约(在 Hyperledger Fabric 中称为链码), 随后即可开始拍卖。拍卖开始后, 信息交互只发生在各个投标者之间, 所有的投标者将使用部署在通道中的智能合约进行交互, 具体来说所有投标者会将区块链视作一个广播信道, 将自己的信息公布到链上并读取其他所有投标者在链上发布的信息, 从而实现信息的交互。

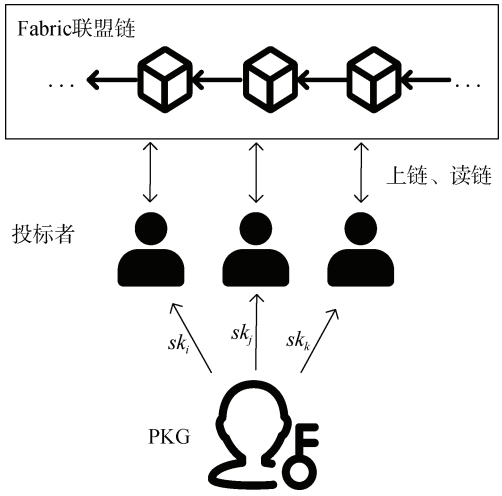

图 1 拍卖系统模型图

Figure 1 Auction system model diagram

我们的协议将密封拍卖分为 3 个阶段:

秘密投标阶段: 在本阶段, 所有的投标者选择自己的出标金额, 并在链下计算标价的加密值, 最后将得到的加密值通过智能合约发布到链上。

投标计算阶段: 在本阶段, 所有的投标者先从链上读取其他投标者发布的秘密值, 再将自己的出价和其他投标者的出价加密值进行同态运算并处理后得到一个新的加密值, 最后将这个处理后的加密值再次发布到链上, 这个加密值只能由发布者解密并查看比较结果。

中标证明阶段: 在本阶段, 所有的投标者从链上读取上一轮其他方发布的比较结果并解密, 所有

投标者将知道自己的出价排名并判断自己是否中标, 然后所有投标者会公布解密需要的信息, 从而所有投标者都可以查看其他投标者的所有比较结果, 最后中标者即可进一步进行交易。

我们的方案在攻击者假设为半诚实攻击者的情况下可以证明为安全的, 半诚实攻击者会遵循协议的执行流程, 但是会尝试从协议过程中得到的信息中推断出秘密信息。我们的方案将基于联盟链 Hyperledger Fabric 实现, 而 Hyperledger Fabric 通过设立 MSP 保证只有得到认证过的用户才能参与拍卖, 这保证了参与拍卖的投标者的身份本身就是得到认可的, 一定程度上可以保证参与的用户是会遵守规则的, 因此只要确保协议中交互的信息不会泄露出价即可满足该场景下对安全性的需求。

我们会在本节剩余部分给出 3 个阶段的所有细节, 并在第 4 节证明协议的安全性。

3.2 第一轮交互

假设存在一个可信第三方作为 PKG 提供私钥提取服务, 共 n 位投标者 $\{P_1, P_2, ..., P_n\}$ 参与拍卖, 所有投标者加入到联盟链的同一个通道中, 并假设每个投标者都有一个公开的身份, 因此通道内的投标者都知道其他人的身份公钥。协议中所有的投标者的地位和行为都是相同的, 下面我们以一位随机的投标者 P_i 为例来描述协议, 设 P_i 的身份公钥为 ID_i。接下来 P_i 向 PKG 申请调用私钥提取算法, PKG 通过安全信道将 P_i 的身份私钥 $sk_i = d_{ID_i}$ 发送给 P_i, 随后即可正式开始电子拍卖的交互流程。

确定好自己的私钥之后, P_i 开始选择自己的出价 $V_i = v_{i,l}v_{i,l-1}...v_{i,1}$, 出价需要用 l 位二进制数表示, $v_{i,l}$ 为最高位, $v_{i,1}$ 为最低位。P_i 逐位加密自己的出价得到 l 个密文 $\left\{c_{i,k} = (g^{r_{i,k}}, g_T^{v_{i,k}} e(H(ID_i), y)^{r_{i,k}}) \mid k = 1, ..., l\right\}$。

随后 P_i 调用 Fabric 合约将以上密文发送到链上, 其他投标者将和 P_i 进行相同的行为, 至此第一轮交互结束。

3.3 第二轮交互

当投标者 P_i 在链上监听到所有其他投标者在上一轮发布的密文, 即可开始第二轮协议交互。在第二轮所有投标者将基于其他投标者发布的出价密文和自己的出价进行 DGK 比较计算[23], DGK 算法假设两个投标者各有一个二进制整数, 使用该算法可以让双方在不透露自己的整数的情况下了解自己的整数和对方的整数的大小关系。

这里简单介绍一下比较的原理, 首先假设两个二进制数为 $m = m_l, ..., m_1$ 和 $n = n_l, ..., n_1$, 对二进制数的每一位用如下计算公式进行计算:

$$b_k = n_k - m_k + 1 + \sum_{t=k+1}^{\ell} m_t \oplus n_t \tag{3.1}$$

其中 “$\oplus$” 表示异或运算, 若以上每一位运算结果的集合 $\{b_k \mid k = 1, ..., l\}$ 中存在任意一个元素为 0, 则说明 $m > n$, 反之若不存在元素为 0, 则 $m \leqslant n$。这是因为 b_k 为 0 的充要条件为: 1) $\sum_{t=k+1}^{\ell} m_t \oplus n_t$ 为 0; 2) $m_k = 1, n_k = 0$, 而上述两个条件又代表着二进制整数 m 和 n 的前 $l-k$ 高位相同且第 k 位上 $m_k > n_k$, 即 $m > n$。我们再将上述的异或运算用算术形式表达为: $m_k \oplus n_k = w_k = m_k + n_k - 2n_k m_k$, 即得到了 b_k 的算术计算公式。此时, 双方只需要将自己的二进制整数使用加法同态加密逐位加密后发送给对方, 对方再基于加法同态的性质将密文与自己的出价明文计算出比较结果, 双方再交换比较结果并使用自己的私钥解密所有密文, 并检查其中是否包含 0 即可知道自己的整数与对方的整数的大小关系。

在我们的方案中, 投标者 P_i 在联盟链上收到另一方的密文之后即可按照如下方法计算出比较结果的密文, 以任意的另一位投标者 P_j 发布的密文 $\left\{c_{j,k} \mid k = 1, ..., l\right\}$ 为例, P_i 基于自己的出价整数 $V_i = v_{i,l}v_{i,l-1}...v_{i,1}$ 逐位进行如下运算:

$$\begin{aligned}
d'_{i,j,k} &= \frac{\prod_{t=k+1}^{l} c'^{1-2v_{i,t}}_{j,t}}{c'_{j,k}} = g^{r_{i,j,k}} \\
d''_{i,j,k} &= \frac{g_T^{v_{i,k}+1} \cdot \prod_{t=k+1}^{l} (g_T^{v_{i,t}} \cdot c''^{1-2v_{i,t}}_{j,t})}{c''_{j,k}} \\
&= g_T^{v_{i,k} - v_{j,k} + 1 + \sum_{t=k+1}^{l} (v_{i,t} + v_{j,t} - 2v_{i,t}v_{j,t})} \cdot e(H(ID_i), y)^{r_{i,j,k}} \\
&= g_T^{b_{i,j,k}} \cdot e(H(ID_i), y)^{r_{i,j,k}}
\end{aligned} \tag{3.2}$$

其中 $r_{i,j,k} = \sum_{t=k+1}^{l} (1 - 2v_{i,t}) r_{j,t} - r_{j,k}$, 显然由公式(3.2)计算得到的密文集合 $\left\{d_{i,j,k} = (d'_{i,j,k}, d''_{i,j,k}) \mid k = 1, ..., l\right\}$ 仍然符合由 P_j 的公钥进行加密的密文格式, 并且正是投标者 P_i 与 P_j 的出价整数按照公式(3.1)计算的结果 $\left\{b_{i,j,k} \mid k = 1, ..., l\right\}$ 的加密密文 。

然而上述结果并不能直接通过联盟链发送给 P_j, 原因是任意 $b_{i,j,k}$ 都是一个范围较小的整数, P_j 收到这些计算结果后可以通过解离散对数问题直接解密

出每一位的$b_{i,j,k}$并结合自己的出价整数V_j反推出P_i的出价整数V_i。因此P_i需要对计算结果做盲化处理使得P_j只能解密出值为 0 的$b_{i,j,k}$从而隐藏其他非 0 位的信息, 对于$\{d_{i,j,k} \mid k=1,...,l\}$中的每个元素, P_i随机选择一个大整数$R_{i,j,k} \in_R Z_p$, 并进行如下运算:

$$\begin{aligned} D'_{i,j,k} &= d'^{R_{i,j,k}}_{i,j,k} = g^{r_{i,j,k} \cdot R_{i,j,k}} \\ D''_{i,j,k} &= d''^{R_{i,j,k}}_{i,j,k} = g_T^{b_{i,j,k} \cdot R_{i,j,k}} \cdot e(H(ID_i), y)^{r_{i,j,k} \cdot R_{i,j,k}} \end{aligned} \tag{3.3}$$

对于投标者P_j来说, 他仍然可以使用自己的私钥解密盲化处理后的密文集合$\{D_{i,j,k} \mid k=1,...,l\}$中的任意元素得到$g_T^{b_{i,j,k} \cdot R_{i,j,k}}$, 但是由于$R_{i,j,k}$是由$P_i$选择的大随机数, 此时如果$b_{i,j,k} \neq 0$, 求解$b_{i,j,k} \cdot R_{i,j,k}$就变成了困难级别的离散对数问题, 而当$b_{i,j,k}=0$, P_j仍然可以很容易地求解, 因为此时$b_{i,j,k} \cdot R_{i,j,k}=0$, $g_T^{b_{i,j,k} \cdot R_{i,j,k}}$即为$G_T$群的单位元。

按照公式(3.3)盲化处理后的$\{D_{i,j,k} \mid k=1,...,l\}$中如果包括解密结果为 0 的密文, 那么仍然存在一定的信息泄露, 因为 P_j可以根据解密为0的密文所在的位置判断出P_i的出价和自己的出价前几位是相同的, 这样在一定程度上泄露了P_i的出价范围。为了避免这样的信息泄露, P_i需要随机打乱$\{D_{i,j,k} \mid k=1,...,l\}$中的元素排列顺序, 可以基于简单的Benes置换网络[24]来实现这一步, 设混洗打乱后的密文集合为$S_{i,j}=\{\mathcal{D}_{i,j,k} \mid k=1,...,l\}$此时$P_j$已经无法根据解密为 0 的密文的位置来获得出价$V_i$的范围信息, P_j能从$\{\mathcal{D}_{i,j,k} \mid k=1,...,l\}$中获得的信息就只剩下是否包含解密为 0 的元素, 即自己的出价V_j和V_i的大小关系。完成上述计算后, P_i调用合约将他与所有其他投标者的比较密文集合$\mathbb{S}_i$发送到链上, 其他投标者将进行相同的行为, 至此第二轮交互结束。

3.4 第三轮交互

当所有投标者在链上监听到所有其他参与者在链上发布的第二轮比较密文后即可开始协议的第三轮交互。这一轮中所有投标者可以使用自己的私钥解密其他投标者发布的DGK比较密文来了解自己的出价在所有人中的排名并向其他人证明。

仍然以P_i为例, P_i在收到所有基于自己的出价密文计算的DGK比较结果$\{S_{t,i} \mid t=1,...,n, t \neq i\}$后使用自己的私钥$sk_i$解密所有的密文, 根据 3.3 节的描述, P_i解密任意一组密文集合$S_{j,i}$时若其中存在一个密文$\mathcal{D}_{i,j,k}$可以解密为 0, 则P_i可以确定自己的出价V_i大于P_j的出价V_j; 若$S_{j,i}$中不存在可以解密出 0 的密文, 则P_i可以确定自己的出价$V_i < V_j$。按照这一方法, P_i解密密文集合时统计无法解密出 0 的密文集合的数量*count* (即出价大于自己的投标者的数量), 解密完所有的密文集合之后P_i即可确定自己的出价在全体投标者中的排名$rank = count + 1$。

随后P_i需要向其他投标者证明自己的排名, 但仍然不能泄露自己的具体出价, 为了满足这一要求, P_i可以让别的投标者和自己一样也能解密自己的DGK比较结果$\{S_{t,i} \mid t=1,...,n, t \neq i\}$来证明自己的排名, 但是显然$P_i$不可能直接公布自己的私钥, 否则其他投标者可以直接解密他在第一轮发布的出价密文来得到V_i。这里P_i正确的做法是公布所有密文解密过程中的中间值, 以任意密文$C=(C_1, C_2)$为例, P_i计算并公布$C^{token}=e(sk_i, C_1)$, 我们称C^{token}为*Token*, *Token*既保护了自己的私钥sk_i(我们会在第 4 节给出安全性证明), 又赋予了其他投标者解密密文的能力, 其他投标者只需要计算C_2 / C^{token}的值即可判断密文的解密结果是否为 0。

但需要注意的是, P_i必须先对每个DGK密文集合进行处理, 否则由于计算该密文集合的投标者知道他在第二轮选择的所有大随机数R以及混洗置换的顺序, 他得到解密令牌之后就有能力完全解密P_i的出价。因此P_i首先应该和第二轮一样, 重新选择大随机数对所有的比较密文集合$\{S_{t,i} \mid t=1,...,n, t \neq i\}$进行盲化处理, 并对每组比较密文再进行一轮混洗置换。最终得到新的比较密文集合$\mathbb{S}'_i = \{S'_{t,i} \mid t=1,...,n, t \neq i\}$, 新的密文集合$S'_{t,i}$定义为$\{\mathcal{D}'_{t,i,k} \mid k=1,...,l\}$, 接着计算所有密文对应的解密*Token*: $\mathbb{C}_i^{token}=\{C_{t,i,k}^{token} \mid k=1,...,l, t=1,..., n, t \neq i\}$。

最后, P_i调用合约将二元组$(\mathbb{S}'_i, \mathbb{C}_i^{token})$发布到链上, 至此所有投标者知道了自己的出价排名并向其他投标者提供了证明, 中标者可以与卖家进行下一步交易, 拍卖协议结束。

4 安全性证明与成本分析

本节将给出密封电子拍卖的安全性定义, 并证明我们的方案满足该安全性定义。此外, 本节还会从理论上分析方案的计算和通信成本。

4.1 安全性定义

为了定义密封电子拍卖体系的安全性, 我们引入理想世界的概念。定义一个理想化的世界, 其中存在一个理想的可信第三方 TTP, 该可信第三方不会向外界泄露任何额外信息。TTP 从所有投标者 P_i 处接收所有的出价整数 V_i, 然后计算所有投标者的出价两两之间的大小关系, 得到每个投标者的出价在全体投标者中的排名。最后 TTP 将这些出价的大小关系以及每个投标者的出价排名广播给所有投标者, 每个投标者除了自己的出价排名以及所有其他投标者的出价大小关系以外了解不到任何额外信息。

基于理想世界的定义, 我们定义密封电子拍卖协议的安全性: 一个安全的密封电子拍卖应当能实现上述理想世界中定义的可信第三方的所有功能, 即在不泄露出价排名以外的任何额外信息的情况下使得每个投标者了解自己以及其他投标者的出价排名。

4.2 安全性证明

本小节对我们的方案给出安全性证明。由于 Fabric 存在 MSP 机制, 只有通过身份认证的投标者才能加入到拍卖中, 即 Fabric 是一个安全性较高的环境, 因此我们认为考虑半诚实模型下的协议安全性是可以接受的, 所谓半诚实敌手即行为遵守协议规定但尝试从协议交互过程中的信息获取额外信息的敌手。我们假设参与拍卖的投标者中仅存在一位诚实的投标者, 剩余的投标者全部为半诚实敌手, 我们的方案在这种情况下满足如下定理:

定理 1: 假设参与拍卖的投标者数量为 n, 存在一个半诚实的敌手 $\mathcal{A}$ 控制了其中 $\tau < n$ 个投标者, 在 DBDH 假设难题成立的情况下, 我们的拍卖协议在随机预言机模型下实现的功能等同于理想世界中定义的可信第三方 TTP 的功能。

证明: 首先, 我们在第三节中已经介绍了我们的方案的功能, 即协议执行完成后, 每个投标者都了解了包括自己在内的所有参与者的出价排名以及出价之间的大小关系, 因此我们的方案在拍卖的功能性上和理想世界是等同的, 我们额外需要证明的是我们的方案同可信第三方一样不会泄露任何额外信息。

接下来我们的证明会分为两个部分, 第一部分将会基于模拟器证明协议中交互内容不会泄露任何有关出价的额外信息, 第二部分将证明第三轮中计算的 *Token* 不会泄露投标者的私钥信息。

4.2.1 出价隐私性证明

我们使用基于模拟的证明方式[25]来证明我们的方案不会泄露任何有关出价的额外信息。在基于模拟的证明中, 我们定义一个理想世界, 在理想世界中存在可信第三方 TTP 和一个模拟器 S, 模拟器 S 的任务是在不了解任何投标者的具体出价的情况下模拟拍卖协议中交互信息来和所有参与拍卖的投标者进行交互, 即模拟器是零知识的。如果对于所有投标者来说, 模拟器 S 每一轮发送给他们的信息和真实协议过程中的信息是不可区分的, 那么即证明了我们的方案和理想世界中的 TTP 一样不会泄露任何有关出价的额外信息。

首先, 我们需要将协议中的加密算法视为随机预言机 $\text{Oracle}_{\text{Enc}}$, 即模拟器 S 可以通过密文向预言机查询对应的明文。

协议第一轮, P_i 和 P_j 加密自己的出价整数, 并将各自的密文 C_i 和 C_j 发送给模拟器 S, 模拟器向加密预言机 $\text{Oracle}_{\text{Enc}}$ 查询得到这些密文对应的明文, 即 P_i 和 P_j 的出价整数。随后将他们的出价明文转发给理想世界中的可信第三方 TTP, TTP 比较 P_i 和 P_j 的出价的大小关系并回复给模拟器 S。注意, 这里模拟器只是将 P_i 和 P_j 的出价明文转发给 TTP, 并不直接使用他们的出价明文, 即并不违背模拟器 S 的零知识前提。

模拟器 S 得到 P_i 和 P_j 的出价大小关系后, 使用 P_i 和 P_j 的公钥对任取的明文进行加密得到密文 $C_i^{'}$ 和 $C_j^{'}$, 并将 $C_i^{'}$ 转发给 P_j, 将 $C_j^{'}$ 转发给 P_i, 对于 P_i 和 P_j 来说, 这两个密文都是由对方的公钥加密的密文, 由于在 DBDH 假设成立的情况下, AIBE 在随机预言机模型下可证明为具有语义安全性, 因此对于 P_i 和 P_j 来说, 模拟器转发给他们的消息和真实世界的协议中看到的消息是不可区分的, 模拟器的第一轮模拟完毕。

协议第二轮, P_i 和 P_j 会基于第一轮收到的密文进行 DGK 计算得到 DGK 比较密文 C_{ij} 和 C_{ji}, 模拟器 S 收到这些密文之后, 不能将这些密文转发给对应的投标者, 因为这些密文中包含了投标者的出价信息, 同时模拟器也不能再像第一轮那样随意加密一个密文, 因为这一轮的密文转发给对应的投标者

之后, 投标者是可以使用自己的私钥解密密文并根据能否解密出“0”来判断自己的出价和对方的出价的大小关系。

我们可以注意到, 模拟器 S 在第一轮从 TTP 处得知了投标者 P_i 和 P_j 的出价的大小关系, 因此模拟器 S 只需要根据这些大小关系使用 P_i 和 P_j 随机加密一组含“0”或者不含“0”的明文, 得到密文 $C_{ij}^{'}$ 和 $C_{ji}^{'}$ 并分别转发给 P_j 和 P_i。由于密文 $C_{ij}^{'}$ 和 $C_{ji}^{'}$ 确实包含了正确的出价大小关系, 并且 AIBE 具有语义安全性, 因此对于 P_i 和 P_j 来说, 这一轮他们收到的消息仍然和真实协议中的交互信息是不可区分的。

协议第三轮, P_i 和 P_j 解密第二轮收到的所有 DGK 比较密文后即得知自己的出价排名, 按照协议规定, 第三轮 P_i 和 P_j 会将自己收到的 DGK 比较密文重新混洗、盲化后得到新的密文 $\mathcal{C}_{ji}$ 和 $\mathcal{C}_{ij}$ 并计算对应的解密 *Token*。模拟器 S 收到 P_i 和 P_j 发送的消息后可以直接将消息转发给需要看到这些消息的投标者即可, 因为这一轮收到的密文本身就是基于模拟器 S 在第二轮中模拟的密文计算得到的, 也就是说其中并不包含任何与投标者的出价相关的信息, 因此直接转发也不会违反模拟器的零知识前提, 并且第二轮模拟器在模拟密文的时候也是按照正确的出价大小关系来模拟的, 因此这些密文在使用附带的 *Token* 解密之后得到验证结果也同样会是正确的。由于 AIBE 的语义安全性, 这些密文和真实世界中的密文同样是不可区分的。

至此我们即证明了我们的方案中三轮交互的信息不会泄露任何有关投标者出价的信息。

4.2.2 私钥隐私性证明

我们的方案中的交互信息中, 除了第三轮的 *Token*, 其他的交互信息都是合法的 AIBE 密文, 因此我们只需要证明我们计算的 *Token* 不会泄露投标者的私钥即可。针对 *Token* 中私钥的安全性, 我们提出以下定理:

定理 2: 假设一个概率多项式时间算法 $\mathcal{A}$, 该算法从 *Token* 中破解对应私钥 *sk* 的概率 $Pr_{\mathcal{A}}$ 定义为:

$$\Pr[\mathcal{A}(mpk, H(id), C, e(C[0], sk_{id})) \longrightarrow sk' : sk' = sk_{id}]$$

其中 *mpk* 为 PKG 的主公钥, H 为 AIBE 中使用的哈希函数, *id* 为密文 C 使用的公钥, *Token* 即为 $e(C[0], sk_{id})$。当 DBDH 假设成立时, 上述概率是可以忽略的。

证明: 下面我们基于 DBDH 假设证明定理 2 的正确性, 我们按照以下步骤构造一个敌手 $\mathcal{B}$, 利用算法 $\mathcal{A}$ 来破解 DBDH 问题:

(1) 定义敌手 $\mathcal{B}$ 尝试破解 DBDH 问题, 参照 2.2 节定义其破解成功的优势为:

$$Adv_{\mathcal{G},\mathcal{B}}^{\mathrm{DBDH}}(n) := |\Pr[\mathcal{B}(g, p, e, g^{x_1}, g^{x_2}, g^{x_3}, h_b) = b] - \frac{1}{2}|$$

(2) $\mathcal{B}$ 利用其收到的 DBDH 挑战的参数构造从 *Token* 中提取私钥的挑战: 令 $mpk = g^{x_1}$, 即 $msk = x_1$, $H(id) = g^{x_2}$, $C = (g^{x_3}, g_T^m)$, $Token = h_b$, 调用 $\mathcal{A}(mpk, H(id), C, Token)$ 并得到 $\mathcal{A}$ 的输出 sk';

(3) $\mathcal{B}$ 计算 $e(sk', g^{x_3})$ 并判断其是否等于 h_b, 若相等, $\mathcal{B}$ 输出 0, 反之输出 1。我们容易计算得出, 若 $sk' = msk \cdot H(id)$, 即 $\mathcal{A}$ 成功提取出 *id* 对应的私钥, 则 $e(sk', g^{x_3}) = h_0$。

根据上述描述, 我们容易得到:

$$\begin{aligned} Adv_{\mathcal{G},\mathcal{B}}^{\mathrm{DBDH}}(n) &= |\frac{1}{2}(1 - Pr_{\mathcal{A}}) + Pr_{\mathcal{A}} - \frac{1}{2}| \\ &= \frac{1}{2} Pr_{\mathcal{A}} \end{aligned} \tag{4.1}$$

显然若 $Pr_{\mathcal{A}}$ 是不可忽略的, 则敌手 $\mathcal{B}$ 的优势 $Adv_{\mathcal{G},\mathcal{B}}^{\mathrm{DBDH}}(n)$ 也是不可忽略的, 这与 DBDH 假设矛盾。因此在 DBDH 假设成立的情况下, 算法 $\mathcal{A}$ 从 *Token* 中破解对应私钥 *sk* 的概率 $Pr_{\mathcal{A}}$ 是可以忽略的, 定理 2 证毕。

定理 2 证明完毕后, 也就证明了我们的方案不会泄露任何有关投标者的出价或私钥的额外信息, 即我们的方案和理想世界中的可信第三方有完全相同的功能性和安全性, 定理 1 证毕。

4.3 复杂度分析

本小节对我们的方案的计算成本和通信成本进行理论上的分析。

我们假设 G 群和 G_T 群上的元素大小都为 128 字节。表 1 列出了方案中任意一位投标者的理论计算复杂度, 其中 n 为参与拍卖的投标者数量, l 为出价整数的二进制位数。表 2 列出了方案中任意一位投标者的理论通信复杂度。

5 性能分析

本节将展示我们对方案进行的一系列实验评估工作。实验设备为一台 Linux 系统、32G 内存的笔记本电脑, 处理器型号为 Intel i7 12700H, 主频 2.3 GHz。我们的实验基于 Hyperledger Fabric 2.4 版

表 1 方案的计算复杂度分析

Table 1 Computational complexity analysis of the protocol

轮次	计算复杂度
计算第一轮输入	$O(l)$
计算第二轮输入	$O(n\cdot l^2)$
计算自身排名	$O(n\cdot l)$
计算第三轮输入	$O(n\cdot l)$
验证第三轮输入	$O(n\cdot l)$

表 2 方案的通信复杂度分析

Table 2 Communicational complexity analysis of the protocol

轮次	数据长度复杂度/Byte
第一轮输入	$O(l)$
第二轮输入	$O(n\cdot l)$
第三轮证明	$O(n\cdot l)$

本[26]来搭建区块链环境, 并基于 Java 语言编写链码, 链码主要实现在链上广播方案中每一轮的交互信息的功能。PKG 和链下的计算同样基于 Java 语言实现, 其中涉及到的密码学计算基于 JPBC 密码学库[27]实现, JPBC 版本为 2.0.0、JDK 版本为 17, 实验的源代码可以在文献[28]处获取。

我们首先关注的是方案的链下计算性能, 我们在同一台实验设备上基于 Java 语言测试了文献[14]的方案性能(其中零知识证明的计算基于原文提供的 C++源码计算), 图 2、图 3、图 4 对比了两个方案的三轮上链信息的计算消耗时间随着投标者数量增加而变化的曲线图。

通过分析图 2 可知, 由于我们的方案使用的加密算法与 ElGamal 加密算法相比较复杂, 因此在参与方个数较少时, 计算成本略高于文献[14]中的方案。但由于我们的方案不涉及零知识证明, 因此第一轮的计算时间复杂度为常数级, 当参与方个数较高时我们的方案在计算时间上便有较大的优势。通过分析图 3、图 4 我们可以得到类似的结论, 即在计算性能上我们的方案相较于文献[14]中的方案有较大的优势。

其次我们简单评估了我们的方案在实际中应用的成本, 由于 Hyperledger Fabric 的智能合约与以太坊不同, 并不存在类似以太坊的交易 Gas 费的概念, 因此执行合约的主要成本为区块占用存储空间的费用。我们以亚马逊云(AWS)提供的 Hyperledger Fabric 服务费用为例[29], 来估算每次拍卖所需的链上存储成本, 亚马逊云服务规定写入 Hyperledger Fabric 网络的数据价格为 0.1 美元每 GB。以上述价格为例, 我们规定拍卖中每一方的出价位数为 32 位二进制数, 并统计每一场拍卖需要写入区块链的数据大小, 从而计算一场拍卖写入 Hyperledger Fabric 网络的数据成本与投标者数量的关系, 计算结果如图 5 所示。

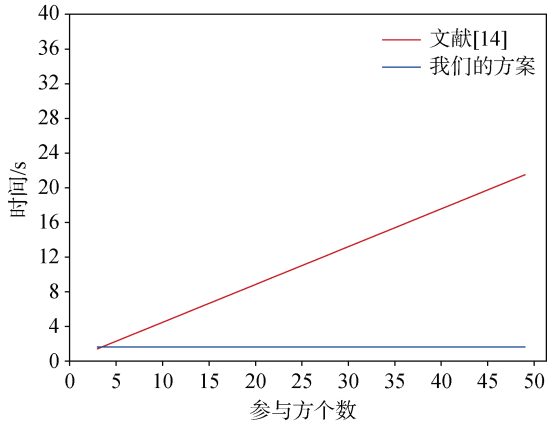

图 2 第一轮计算时间消耗

Figure 2 Time consumption of the first round

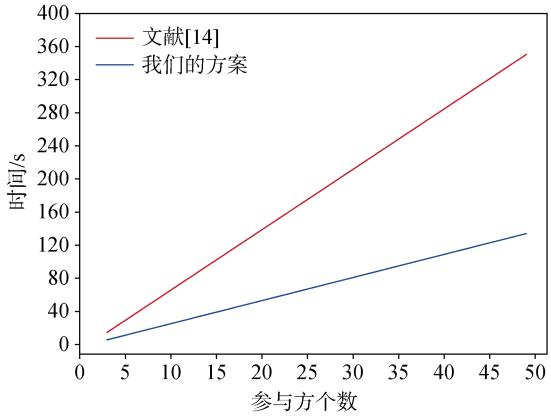

图 3 第二轮计算时间消耗

Figure 3 Time consumption of the second round

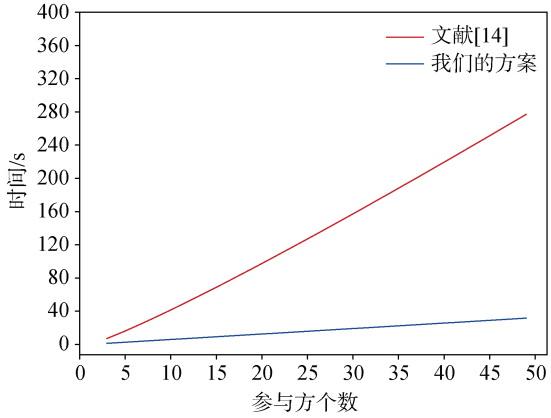

图 4 第三轮计算时间消耗

Figure 4 Time consumption of the third round

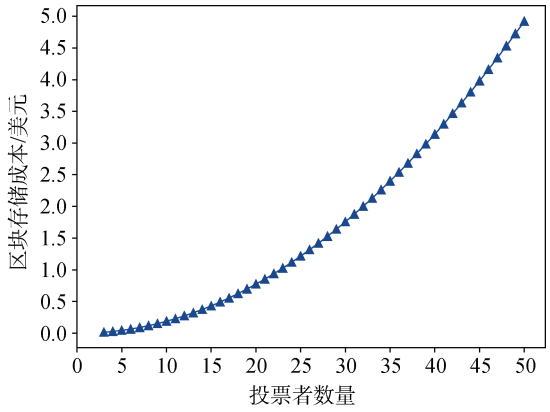

图 5 区块存储成本与投标者数量的关系

Figure 5 The trend of block storage cost changing with the number of bidders

通过分析图 5 可以看出, 我们的拍卖方案的区块存储成本与投标者数量呈指数级关系, 但是从具体的数值来说, 即使在 50 名投标者的情况下, 一场拍卖的总区块存储成本也不超过 5 美元, 显然这个数值对于一场拍卖来说是完全可以接受的, 因此我们的方案是具有较强的实用性的。

此外我们还测试了我们所使用的 Fabric 区块链的性能, 我们采用默认配置, 共识机制为 solo 共识, 以协议第一轮的上链信息为例(长度为 8381Byte), 通过多线程异步请求大量提交第一轮的消息上链请求测试 Fabric 处理交易的速度, 实验结果如图 6 所示。

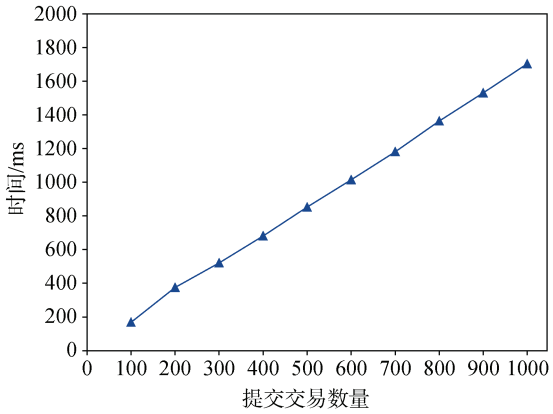

图 6 Fabric 处理上链请求的时间消耗

Figure 6 Time consumption of Fabric processing transactions

通过分析图 6 可以看出, 处理交易的时间消耗和交易处理是一个线性关系, 通过计算我们大致可以得到我们部署的环境下 Fabric 的吞吐量约为 586 tps, 即每秒大约可以处理 586 条长度为 8381Byte 的消息的上链交易, 目前流行的公链例如 Bitcoin 和 Ethereum 的理论最大吞吐量仅能达到数十 tps[30-31]。

根据 4.3 节的分析, 第二轮第三轮的上链信息的长度与投标者数量呈线性关系, 因此当投标者数量较多时, 相比公链, Fabric 会有较大的性能优势。

6 结论

本文使用基于身份的加法同态的加密算法, 并结合区块链的去中心化、不可篡改等优势, 设计了联盟链上的基于身份的密封电子拍卖系统, 解决了公钥密封电子拍卖方案需要在链上使用昂贵的公钥基础设施的问题, 并通过理论证明了方案的安全性, 实验也表明我们的方案具有优越的性能, Fabric 区块链也体现出更强的实用性。当然, 我们的方案也存在不足, 例如在恶意敌手的模型下, 方案的安全性难以得到保障, 在这一方面有待后续更深入的研究。

参考文献

[1] Shi Z S, de Laat C, Grosso P, et al. Integration of Blockchain and Auction Models: A Survey, Some Applications, and Challenges[J]. *IEEE Communications Surveys & Tutorials*, 2023, 25(1): 497-537.

[2] Bogetoft P, Christensen D L, Damgård I, et al. Secure Multiparty Computation Goes Live[M]. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009: 325-343.

[3] Squarepants S. Bitcoin: A Peer-to-Peer Electronic Cash System[J]. *SSRN Electronic Journal*, 2008: 21260.

[4] Buterin V. A Next-generation smart contract and decentralized application platform[J]. *white paper*, 2014, 3(37): 2-1.

[5] Wood G. Ethereum: A secure decentralised generalised transaction ledger[J]. *Ethereum project yellow paper*, 2014, 151(2014): 1-32.

[6] Di Francesco Maesa D, Mori P. Blockchain 3.0 Applications Survey[J]. *Journal of Parallel and Distributed Computing*, 2020, 138: 99-114.

[7] Wang H M, Zheng Z B, Xie S A, et al. Blockchain Challenges and Opportunities: A Survey[J]. *International Journal of Web and Grid Services*, 2018, 14(4): 352.

[8] Chen H S, Jarrell J T, Carpenter K A, et al. Blockchain in Healthcare: A Patient-Centered Model[J]. *Biomedical Journal of Scientific & Technical Research*, 2019, 20(3): 15017-15022.

[9] Li Z T, Kang J W, Yu R, et al. Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things[J]. *IEEE Transactions on Industrial Informatics*, 2018, 14(8): 3690-3700.

[10] Dib O, Brousmiche K L, Durand A, et al. Consortium blockchains: Overview, applications and challenges[J]. *Int. J. Adv. Telecommun*, 2018, 11(1): 51-64.

[11] Andy Warhol's Multi-Million Dollar Painting Tokenized and Sold on Blockchain[EB/OL]. https://finance.yahoo.com/news/andy-warhol-multi-million-dollar-162928721.html.

[12] Galal H S, Youssef A M. Succinctly verifiable sealed-bid auction smart contract[C]. *Data Privacy Management, Cryptocurrencies and Blockchain Technology: ESORICS 2018 International Workshops, DPM 2018 and CBT 2018,* 2018: 3-19.

[13] Galal H S, Youssef A M. Verifiable sealed-bid auction on the

ethereum blockchain[C]. *Financial Cryptography and Data Security: FC 2018 International Workshops, BITCOIN, VOTING, and WTSC, Revised Selected Papers 22*. 2019: 265-278.

[14] Blass E O, Kerschbaum F. BOREALIS: Building Block for Sealed Bid Auctions on Blockchains[C]. *The 15th ACM Asia Conference on Computer and Communications Security*, 2020: 558-571.

[15] Yao A C. Protocols for Secure Computations[C]. *23rd Annual Symposium on Foundations of Computer Science*, 1982: 160-164.

[16] Furukawa J, Lindell Y, Nof A, et al. High-Throughput Secure Three-Party Computation for Malicious Adversaries and an Honest Majority[M]. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2017: 225-255.

[17] Nakai T, Misawa Y, Tokushige Y, et al. How to Solve Millionaires' Problem with Two Kinds of Cards[J]. *New Generation Computing*, 2021, 39(1): 73-96.

[18] Shamir A. Identity-Based Cryptosystems and Signature Schemes[M]. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007: 47-53.

[19] Anand D, Khemchandani V, Sharma R K. Identity-Based Cryptography Techniques and Applications (a Review)[C]. *2013 5th International Conference and Computational Intelligence and Communication Networks*, 2013: 343-348.

[20] Boneh D, Franklin M. Identity-based encryption from the Weil pairing[C]. *Advances in Cryptology—CRYPTO 2001: 21st Annual International Cryptology Conference,* 2001: 213-229.

[21] Günther F, Manulis M, Peter A. Privacy-Enhanced Participatory Sensing with Collusion Resistance and Data Aggregation[M]. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2014: 321-336.

[22] Androulaki E, Barger A, Bortnikov V, et al. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains[C]. *The Thirteenth EuroSys Conference*, 2018: 1-15.

[23] Damgård I, Geisler M, Krøigaard M. Efficient and secure comparison for on-line auctions[C]. *Information Security and Privacy: 12th Australasian Conference,* 2007: 416-430.

[24] Beneš V E. Optimal Rearrangeable Multistage Connecting Networks[J]. *The Bell System Technical Journal*, 1964, 43(4): 1641-1656.

[25] Lindell Y. How to Simulate It – a Tutorial on the Simulation Proof Technique[M]. Information Security and Cryptography. Cham: Springer International Publishing, 2017: 277-346.

[26] Hyperledger Fabric[CP/OL]. https://github.com/hyperledger/fabric.

[27] JPBC - Java Pairing-Based Cryptography Library: Introduction[CP/OL]. http://gas.dia.unisa.it/projects/jpbc/#.ZGHsrXZBxD8.

[28] Ind1stinguishable. Fabric-Based-Sealed-bid-auction[CP/OL]. https://github.com/W1tnezz/Fabric-Based-Sealed-bid-auction.

[29] Amazon Managed Blockchain Pricing[EB/OL]. https://aws. amazon.com/managed-blockchain/pricing/hyperledger.

[30] Georgiadis E. How many transactions per second can bitcoin really handle? Theoretically[EB/OL]. 2019: Cryptology ePrint Archive: 2019/416.

[31] Leal F, Chis A E, González–Vélez H. Performance Evaluation of Private Ethereum Networks[J]. *SN Computer Science*, 2020, 1(5): 285.

徐哲清 于 2021 年在南京邮电大学应用物理专业获得学士学位。现在南京邮电大学网络空间安全专业攻读硕士学位。研究兴趣包括: 区块链、安全多方计算。Email: 1021041521@njupt.edu.cn。

王宇航 于 2021 年在海南大学信息安全专业获得学士学位。现在南京邮电大学网络空间安全专业攻读硕士学位。研究兴趣包括: 多重签名、聚合签名、区块链。Email: 1021041520@njupt.edu.cn。

王志伟 于 2009 年在北京邮电大学密码学专业获得博士学位。现任南京邮电大学计算机学院, 软件学院, 网络空间安全学院教授。研究领域为: 云/雾计算安全、区块链、密码协议等。Email: zhwwang@njupt.edu.cn。

刘峰 于 2009 年在中科院软件所获得博士学位。现任中国科学院信息工程研究所研究员, 博士生导师。研究领域为: 信息安全体系与战略, 网络攻防演化理论, 视觉安全理论与技术。Email: fengliu.cas@gmail.com。