软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software [doi: 10.13328/j.cnki.jos.007171]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

基于国密的数字藏品网络拍卖隐私保护方法*

邵 宽[1], 张镇勇[1,2], 杨科迪[1], 朱俊彦[1], 王 鑫[2], 田有亮[1], 马建峰[1,3]

[1](公共大数据国家重点实验室 (贵州大学), 贵州 贵阳 550025)

[2](齐鲁工业大学 (山东省科学院) 山东省计算中心 (国家超级计算济南中心), 山东 济南 250014)

[3](西安电子科技大学 网络与信息安全学院, 陕西 西安 710126)

通信作者: 张镇勇, E-mail: zhangzy@gzu.edu.cn

摘 要: 近年来, 数字藏品的线上交易越发频繁, 如阿里拍卖、OpenSea 等, 网络拍卖作为数字藏品交易的重要手段, 有效支撑了数字藏品在市场中的流通. 然而, 网络拍卖中竞标者的竞价隐私存在泄露风险. 针对此问题, 提出一种基于国密的数字藏品网络拍卖隐私保护方案, 该方案在保护用户竞价隐私同时, 兼顾了竞价信息的可用性. 具体来说, 通过设计同态加密计算方法, 加密竞标者的竞价信息和运用同态运算对竞价信息添加噪声这两个步骤, 保障拍卖过程竞标者竞价隐私. 根据网络拍卖隐私保护协议执行效率需求设计了基于 CRT-BSGS 的国密 SM2 同态算法, 相较于 Paillier 算法具有显著的效率提升. 最后, 通过实验证明了所提方案的安全性和高效性.

关键词: 数字藏品; 网络拍卖; 隐私保护; 同态加密

中图法分类号: TP309

中文引用格式: 邵宽, 张镇勇, 杨科迪, 朱俊彦, 王鑫, 田有亮, 马建峰. 基于国密的数字藏品网络拍卖隐私保护方法. 软件学报. http://www.jos.org.cn/1000-9825/7171.htm

英文引用格式: Shao K, Zhang ZY, Yang KD, Zhu JY, Wang X, Tian YL, Ma JF. Privacy-preserving Online Auction Method of Digital Collection with SM2. Ruan Jian Xue Bao/Journal of Software (in Chinese). http://www.jos.org.cn/1000-9825/7171.htm

Privacy-preserving Online Auction Method of Digital Collection with SM2

SHAO Kuan[1], ZHANG Zhen-Yong[1,2], YANG Ke-Di[1], ZHU Jun-Yan[1], WANG Xin[2], TIAN You-Liang[1], MA Jian-Feng[1,3]

[1](State Key Laboratory of Public Big Data (Guizhou University), Guiyang 550025, China)

[2](Shandong Computer Science Center (National Supercomputing Center in Jinan), Qilu University of Technology (Shandong Academy of Sciences), Jinan 250353, China)

[3](School of Cyber Engineering, Xidian University, Xi'an 710126, China)

Abstract: In recent years, online transactions of digital collections have been increasing, with platforms such as Alibaba Auctions and OpenSea facilitating their circulation in the market. However, the bidder's bidding privacy is at risk of being disclosed during an online auction. To address this issue, this study proposes a privacy-preserving online auction approach based on the homomorphic property of SM2, which not only protects the users' bidding privacy but also ensures the usability of the bidding data. Specifically, this study creates a homomorphic encryption scheme based on SM2, encrypting bidders' bidding information and constructing a piece of noisy bidding information to conceal the privacy data. The efficiency of the online auction privacy preservation approach is improved by integrating the Chinese reminder theorem and baby step giant step (CRT-BSGS) into the homomorphic encryption process with SM2, which has proved to be more efficient than the Paillier algorithm. Finally, the security and efficiency of the proposed scheme are verified in detail.

Key words: digital collection; online auction; privacy preservation; homomorphic encryption

* 基金项目: 国家自然科学基金 (62303126, 62362008); 贵州省基础研究计划 (自然科学) 一般项目 (黔科合基础-ZK[2022]一般 149); 贵州省教育厅高等学校科学研究项目 (青年项目)(黔教技 [2022]104 号); 算力互联网与信息安全教育部重点实验室开放课题 (2023ZD037)
收稿时间: 2023-08-03; 修改时间: 2023-10-23; 采用时间: 2024-02-29; jos 在线出版时间: 2024-06-14
CNKI 网络首发时间: 2024-06-17

随着虚拟世界的兴起与快速发展[1,2], 艺术品、收藏品和文物可被创造和数字化并在虚拟世界中流通, 这使得数字藏品受到了广泛关注和追捧. 不同于实体产品, 数字藏品打破了产品的物理空间限制[3], 市场流转更加高效便捷. 网络交易有效推动了数字藏品的快速流通, 为数字经济的发展提供了新的机遇和动力[4,5].

对于数字藏品的定价, 主要可分为固定定价和拍卖定价两种. 固定定价是指卖方根据市场需求和成本对数据产品制定相应的价格, 买方根据卖方定价支付相应金额获取对应商品. 拍卖是一种经济驱动的交易方案, 其目的是通过买方的竞价过程分配商品并赋予相应的价格[6]. 相较于固定定价模式, 拍卖定价模式与市场需求相关性更强, 更能体现数据藏品的价值, 十分适用于解决数字藏品定价问题[7].

目前, 存在一些第三方数字藏品交易平台, 如 OpenSea[8]、SuperRare[9]和 Nifty Gateway[10]等. 然而, 这些平台的数字藏品拍卖都是公开拍卖, 竞标者将竞价提交给中间平台, 中间平台公布竞标人竞价. 由于在拍卖过程中竞标者的竞价信息属于竞标者隐私, 一旦泄露, 在拍卖过程中会发生作弊行为, 如竞标者之间串通、竞标者与拍卖师之间串通等. 密码学技术是保护数据机密性的重要手段, 如果单是对竞价信息的加密, 会隐藏竞价信息的大小关系, 无法进行竞价比较. 因此, 设计安全的网络拍卖协议来保护竞标者竞价隐私, 同时不破坏竞价信息的大小关系是一个难题.

网络拍卖隐私保护协议一般可分为 3 种. 第 1 种: 采用安全多方计算协议[11−13], 然而, 这种方式需要多个参与者进行多轮交互, 通信成本高且影响拍卖执行效率; 第 2 种: 基于差分隐私的拍卖协议[14−17], 差分隐私需要对竞价加入一定噪声, 加入噪声后会在一定程度影响竞价的比较精度, 通常需要在竞价效用和隐私之间取得平衡. 第 3 种: 基于同态加密的拍卖方案[18−20], 这种方式一般进行一轮比较即可获取比较结果, 相较于前两种方法具有较低的通信开销.

以上拍卖协议虽然实现了竞价隐私保护, 但都不是基于国密的拍卖协议, 不利于保障国家信息安全和国家战略发展需求. 为了填补这一空白, 亟需国产化的数字藏品网络拍卖协议. 近年来, 研究人员对国密方案进行了大量的研究工作[21−24], 2022 年, 唐飞等人首次提出了基于国密 SM2 的同态加密算法[25]. 然而, 此同态加密算法的执行效率低, 严重影响拍卖协议的执行效率. 同时, 在开放的网络环境下进行拍卖, 用户群体大, 拍卖性能是一项重要指标. 上述拍卖协议通信开销和计算复杂度大多都是高阶多项式级别或线性对数级别, 随着网络拍卖参与人数增多, 方案通信和计算成本呈 $O(n^2)$ 或 $O(n\log n)$ 增长.

因此, 设计基于国密的数字藏品网络拍卖隐私保护协议还面临一些挑战: (1) 设计保护竞价信息隐私性的同时不破坏竞价信息可用性的拍卖协议较为困难. (2) 基于国密 SM2 的同态方案的解密效率较低. (3) 拍卖协议通信开销和计算复杂度高, 严重影响拍卖执行效率低. (4) 如何实现基于国密的数字藏品网络拍卖隐私保护系统.

本文基于国密 SM2 设计了面向数字藏品网络拍卖的隐私保护协议. 具体来说, 利用同态加密运算将加密和加噪相结合, 实现了在保护竞价信息隐私的同时不破坏竞价信息可用性. 首先, 对基于国密 SM2 的同态方案进行了改进, 提出了一种能够提高协议执行效率的同态运算方案. 接着, 优化了数字藏品网络拍卖协议的交互过程, 所提协议的通信和计算成本随着网络拍卖人数的增加呈线性增长. 最后, 根据实际场景在移动端平台设计了基于国密 SM2 的数字藏品网络拍卖隐私保护系统. 本文的主要工作和贡献如下:

(1) 本文首次基于国密 SM2 提出了数字藏品网络拍卖隐私保护方案, 通过设计网络拍卖隐私保护框架和协议实现了网络拍卖竞价全过程隐私保护. 本文将第三方拍卖平台划分为中间平台和计算平台, 利用中间平台来存储竞标者的加密竞价, 同时使用同态加密的技术对密文竞价加入一次性随机噪声, 中间平台仅能得到加密的竞价, 计算平台仅能得到含噪声的竞价.

(2) 提出了基于中国剩余定理和小步大步算法 (China remainder theorem and baby step giant step, CRT-BSGS) 的同态 SM2 加密算法, 并给出了密码方案的安全性证明.

(3) 设计的拍卖协议对于每个竞标的比较操作仅通过中间平台与计算平台一次交互以及一次加噪和两次解密即可. 随着网络拍卖参与人数增多, 协议的通信和计算成本显线性增长.

(4) 基于 Android 和 Windows 平台在局域网环境下设计基于国密 SM2 数字藏品网络拍卖隐私保护系统, 并分析本文提出的密码方案、数字藏品交付以及竞标者竞标的执行性能.

本文第 1 节介绍相关工作. 第 2 节介绍基础知识. 第 3 节介绍数字藏品网络拍卖隐私保护框架. 第 4 节介绍提

出的基于 CRT-BSGS 的同态 SM2 算法. 第 5 节具体介绍本文提出的基于国密的数字藏品网络拍卖隐私保护协议. 第 6 节具体分析本文网络拍卖方案的安全性. 第 7 节详细测试拍卖方案的执行性能. 最后总结本文.

1 相关工作

数字藏品交易作为数字经济领域的前沿热点, 近年来广受关注. 数字藏品交易的流行源于其给数字经济特别是数字产权领域带来的革命性改进, 其构建起了数字创新的激励机制[26].

随着 OpenSea、SuperRare 和阿里拍卖等数字藏品交易平台的蓬勃发展, 网络拍卖作为数字藏品价值体现的重要交易方式, 打破了线下拍卖的时空局限性. 然而, 各种网络安全问题[27−29]增加了网络拍卖的难度, 网络拍卖中竞标者竞价信息的隐私泄露问题阻碍了其大规模的推广与应用, 为解决网络拍卖过程中的隐私泄露问题, 一般采用安全多方计算协议、差分隐私和同态加密等方法.

安全多方计算 (secure multi-party computation, MPC) 协议使得多方参与者在互不知完整信息的情况下完成协同计算, 例如: 多节点之间的比较、相加、聚合等. 然而, 基于安全多方计算的多方比较协议需要多个参与者执行多轮交互, 即使是恒 MPC 也需要多轮交互和复杂的近似同态加密 (somewhat homomorphic encryption, SHE) 计算. 例如, Lindell 等人[11]需要 16 轮 MPC 交互和 $O(n^3)$ 轮 SHE 计算, n 为待比较数据数量. 进一步, Lindell 等人[12]将比较协议降低到 9 轮 MPC 交互和 $O(n^2)$ 轮 SHE 计算, 还需要对一个乘法深度为 4 的电路进行 SHE 评估. Sutradhar 等人[13]提出的比较协议需要 23 轮 MPC 和 $16+10n$ 的通信开销. 这些协议都需要多方交互且通信开销高.

差分隐私是加密技术的一种变体, 它解析描述了隐私强度和噪声参数之间的关系. Li 等人[14]设计了双拍卖机制, 采用高斯噪声对参与者的估价加入干扰来保护参与者的竞价隐私. 然而, 为了保证隐私保护性能必须考虑大噪声, 这种噪音可能会导致拍卖结果变差. Hassan 等人[15]使用了双重差分隐私机制, 即同时使用了拉普拉斯机制和指数机制, 使拍卖定价策略更加安全, 确保没有敌手能够从以往拍卖记录中推断竞标者的竞价. 针对拍卖市场中的隐私攻击问题和竞价隐私保护问题, Li 等人[16]提出了一种基于贝叶斯的市场推理攻击方法来攻击基于差分隐私的网络拍卖, 攻击成功概率达到 95%, 并提出了一种抗市场推理攻击方法的个体差分隐私拍卖机制, 将攻击成功率降低到 20%. Guo 等人[17]在拍卖机制中引入差分隐私, 通过对用户的出价加入噪声, 且在不显著影响最终结算价格的情况下, 实现用户竞价信息的隐私保护. 虽然这些方案使用差分隐私保护了竞价隐私, 但通常需要在竞价隐私性和准确性之间取得一定平衡. 添加差分隐私噪声是采用差分隐私方法来保护数据隐私的一种机制, 差分隐私噪声一般采用拉普拉斯分布或高斯分布产生. 而本文提出的一次性随机噪声是基于离散型均匀分布随机产生.

同态加密方案中以加法同态加密最为典型, 满足了密文状态下的数据运算需求, 已广泛应用于数据聚合[30]、联邦学习[31]、网络拍卖[20]等实际应用场景. Jung 等人[18]设计的隐私保护拍卖方案能够保证竞价的隐私, 并对通信开销与计算开销进行了考量, 拍卖协议计算复杂度为 $O(n)$, n 为竞标数量. 然而, 在竞标结束后, 拍卖师需要竞价排序, 在此之中涉及拍卖师与多个竞标者的竞价验证交互, 带来协议的执行效率问题. Gao 等人[19]提出了一种隐私保护的大数据拍卖方案, 该方案将拍卖师与计算平台分开, 并结合同态加密, 实现拍卖过程中竞标者竞价的隐私保护, 同时采用时间复杂度为 $O(n\log n)$ 堆排序的方式进行竞价排序, 时间开销较小. 在拍卖过程中, 竞标者仅需一次加密竞标即可, 且方案将本该在竞标结束后的竞价排序工作提前到竞标中进行, 提升了拍卖效率. Blass 等人[20]设计了基于同态加密的安全比较协议, 处理复杂度为 $O(n^2)$, 实现了网络拍卖的竞价隐私保护. 然而, 此协议计算复杂度高.

商用密码 (国密) 是我国自主研发的密码标准方案, 常用的国密标准包括 SM2[32]、SM3[33]、SM4[34]、SM9[35]等, 广泛应用于我国各行各业. 近些年, 研究人员对国密进行了大量的研究[21−24]. 然而, 缺乏关于数字藏品网络拍卖中隐私保护的应用. 因此, 本文对国密 SM2 进行了扩展, 提出了基于 CRT-BSGS 的同态 SM2 算法, 设计了线性复杂度的网络拍卖协议, 实现了数字藏品网络拍卖的全过程隐私保护.

2 基础知识

SM2 密码方案[27]是基于椭圆曲线离散对数问题的密码学标准, 具有较高的安全性. 下面介绍标准的 SM2 密码方案和中国剩余定理 CRT. 本文协议中使用的关键符号, 如表 1 所示.

表 1 拍卖协议的符号含义

符号	描述
$S_s()$、$S_{bi}()$	利用卖方、竞标者的私钥签名
$V_s()$、$V_{bi}()$	利用卖方、竞标者的公钥验证签名
$PK_a()$	利用计算平台的公钥加密
$SK_a()$	利用计算平台的私钥解密
pk_s、pk_a、pk_{bi}	卖方、计算平台和竞标者的公钥信息
sk_s、sk_a、sk_{bi}	卖方、计算平台和竞标者的私钥信息
B_number	拍卖编号
P_{bi}、P_w	竞标者的竞价和拍卖中最高竞价
$SENC()$、key	对称加密算法和对称加密密钥
$\odot$	同态加法运算
$data_{\text{collection}}$、$data_{\text{bi}}$	密文藏品的密文噪声和密文竞价
$sign_{\text{collection}}$、$sign_{\text{bi}}$	数字藏品信息签名和竞标者竞价信息签名
$Noise$	竞价噪声

2.1 SM2

标准的 SM2 方案由以下部分构成.

1) $KeyGen\ () \to (PK, SK)$. 密钥生成算法. SK 为生成的私钥, PK 为生成的公钥, 其中 $PK = [SK]G$, G 为循环群的基点.

2) $Enc\ (M, PK) \to C$. 加密算法. M 为待加密的明文, PK 为加密时需要的公钥, C 为加密后的密文.

3) $Dec\ (C, SK) \to M'$. 解密算法. C 为待解密的密文, SK 为解密时需要的私钥, M' 为解密后的明文.

4) $Sign\ (data, SK) \to s$. 签名算法. $data$ 为待签名的数据, SK 为签名时需要的私钥, s 为签名后的签名.

5) $Verify\ (data, s, PK) \to flag$. 验证算法. s 为待验证的签名, PK 为验证时需要的公钥, $data$ 为验证时需要的原数据, $flag$ 为验证的结果.

SM2 方案的加解密过程如下.

设发送方是 A, 接收方是 B. A 要发送的消息表示成比特串 M, M 的长度为 klen. 加密运算如下.

1) 选择随机数 $k \leftarrow_R \{1,2,\ldots,n-1\}$, 其中 n 为基点 G 的阶, $\leftarrow_R$ 表示在集合中随机选取一个元素;

2) 计算椭圆曲线点 $C_1 = [k]G$, 将 C_1 的数据类型转化为比特串;

3) 计算椭圆曲线点 $S = [h]PK_B$, 若 S 是无穷远点, 则报错退出; 其中 PK_B 为接收方 B 的公钥, h 为余因子;

4) 计算椭圆曲线点 $[k]PK_B = (x_2, y_2)$, 将坐标 x_2、y_2 的数据类型转化为比特串;

5) 计算 $t = \text{KDF}(x_2 \| y_2, \text{klen})$, KDF 为密钥派生函数; 若 t 为全 0 的字符串, 则返回 1);

6) 计算 $C_2 = M \oplus t$, $\oplus$ 为异或运算;

7) $C_3 = \text{Hash}(x_2 \| M \| y_2)$, Hash 为 SM3 哈希算法;

8) 输出密文 $C = C_1 \| C_2 \| C_3$.

B 收到密文 C 后, 执行以下解密运算.

1) 从 C 中取出比特串 C_1, 将表示为椭圆曲线上的点, 验证 C_1 是否满足椭圆曲线方程, 若不满足则报错并退出;

2) 计算椭圆曲线点 $S = [h]C_1$, 若 S 是无穷远点, 则报错并退出;

3) 计算 $[SK_B]C_1 = (x_2, y_2)$, 将坐标 x_2、y_2 的数据类型转化为比特串, 其中 SK_B 是接收方 B 的私钥;

4) 计算 $t = \text{KDF}(x_2 \| y_2, \text{klen})$; 若 t 为全 0 的字符串, 则报错并退出;

5) 从 C 中取出比特串 C_2, 计算 $M' = C_2 \oplus t$;

6) 计算 $u = \text{Hash}(x_2 \| M' \| y_2)$, 从 C 中取出 C_3, 若 $u \neq C_3$, 则报错并退出;

7) 输出明文 M'.

传统 SM2 方案的密文中 C 第 2 部分 C_2 为 $M \oplus t$, 其中 t 是由 $[k]PK$ 通过密钥派生函数 KDF 生成的比特串, 这

里 t 的作用近似于 $[k]PK$ 的摘要. 也就是说, 传统 SM2 加密得到密文 C 的第 2 部分 C_2 是将明文 M 与 $[k]PK$ 的摘要进行异或得到的. 这种异或操作是一种逻辑操作, 而同态运算需要算术运算操作, 故传统 SM2 方案不支持同态运算.

2.2 CRT

CRT 基于一个简单的思想, 即用一组余数 a_i 唯一地表示一个数字 X. 如将 X 用一组余数 a_i 表示就是:

$$X=\sum_{i=1}^{\ell}a_iN_iy_i(\bmod N) \tag{1}$$

其中, N 是所有素数 p_i 的积 (即 $N=\prod p_i$) 且大于 X, ℓ 为素数的数量, $N_i=N/p_i$ 和 $y_i=N_i^{-1}\bmod p_i$. 数据范围由 $[1,N]$ 转化为 $[1,p_i]$. CRT 的加法计算: 假设两个数据 $X=\sum_{i=1}^{\ell}a_iN_iy_i(\bmod N)$ 和 $Y=\sum_{i=1}^{\ell}b_iN_iy_i(\bmod N)$, 将两个数据相加可以表示为 $X+Y=\sum_{i=1}^{\ell}(a_i+b_i)N_iy_i(\bmod N)$, 表明可以使用余数相加运算来表示原数据相加运算.

2.3 BSGS

大步小步走算法 (baby step giant step, BSGS) 常被用于求解离散对数问题. 离散对数问题的公式表示为: $a^x\equiv b(\bmod p)$, 其中 a 与 p 互素, 求解 x 的值.

BSGS 算法实现离散对数问题复杂度为 $O(\sqrt{p})$ 的求解, 具体描述如下.

1) 令 $x=At-B$ 其中 $t=\lceil\sqrt{p}\rceil, A\in[1,t], B\in[1,t)$, 那么原问题则转化为了: $a^{At}\equiv a^Bb(\bmod p)$, 其中 a 与 p 互质, 求解 A 和 B 的值.

2) 将 B 在区间 $[1,t)$ 中遍历计算 $a^Bb(\bmod p)$ 的值并使用哈希表将结果存储下来, 这一步的时间复杂度为 $\mathrm{O}(\sqrt{p})$.

3) 将 A 逐步在区间 $[1,t]$ 中遍历计算 $a^{At}(\bmod p)$ 的值并在哈希表中查找是否存在相同的值, 这一步的时间复杂度为 $\mathrm{O}(\sqrt{p})$;

4) 假设查找到对应的数据为 $A=\widetilde{A}$, 在哈希表查找出来数据对应为 $B=\widetilde{B}$, 那么算法求解 x 的值为 $\widetilde{x}=\widetilde{A}t-\widetilde{B}$.

3 网络拍卖隐私保护框架

针对数字藏品网络拍卖过程中竞标者的竞价隐私问题, 本文提出了数字藏品网络拍卖隐私保护框架, 实现了网络拍卖中竞标者的竞价信息隐私保护.

3.1 网络拍卖框架

图 1 说明了网络拍卖隐私保护方案的拍卖框架, 该框架包括卖方、竞标者、中间平台和计算平台这 4 个实体.

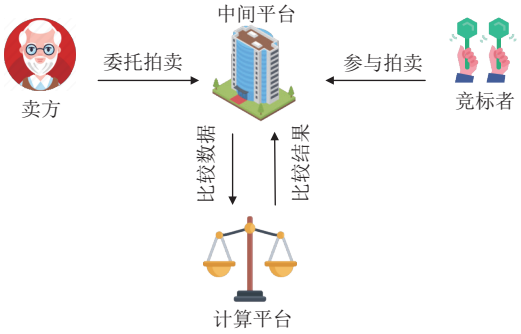

图 1 网络拍卖框架

- 卖方. 卖方是数字藏品的持有者, 其希望通过拍卖数字藏品获得一定的经济报酬.
- 竞标者. 竞标者是对数字藏品有需求的人, 其希望通过一定经济支付获得数字藏品.

● 中间平台. 在系统中与各方交互并负责计算、存储的平台, 它与计算平台独立, 作为一个半诚实的平台, 它会遵守协议的安排, 但也会好奇用户的隐私. 在拍卖过程中, 它与卖方交互, 获取数字藏品; 与竞标者交互, 获取竞标者对数字藏品网络拍卖的竞价; 与计算平台交互, 获取竞价的大小关系.

● 计算平台. 拍卖中负责竞价处理的一方, 作为一个半诚实的平台, 它会遵守协议的安排, 但也会好奇用户的隐私. 在拍卖过程中, 计算平台仅与中间平台交互, 它不断的接收来自中间平台的竞价信息, 并向中间平台反馈一个处理结果. 同时, 计算平台为个体理性的, 他不会恶意破坏竞价比较结果.

为了保护竞标者的竞价隐私, 在设计的网络拍卖框架中, 本文引入一次性随机噪声. 在拍卖框架中, 中间平台需要对密文竞价加入噪声形成中间密文, 如果由中间平台进行竞价比较, 需要将中间密文进行解密, 那么其便可知道竞价信息, 无法实现对竞标者竞价隐私的保护. 因此, 本文引入了计算平台, 将中间密文大小比较的任务转交由计算平台进行, 中间平台不具有查看竞价信息的能力, 保护了竞标者竞价隐私. 本文将在第 3.2 节对框架的安全性进行具体的分析.

3.2 安全威胁

在网络拍卖过程中, 计算平台会推断竞价、中间平台窃取竞标者的竞价, 甚至恶意竞标者可能会冒充成合法竞标者进行虚假竞标.

● 竞价信息窃取. 在拍卖过程中, 存在两种安全威胁. (1) 中间平台保留大量的竞标者的竞价, 中间平台对竞标者的竞价存在好奇, 会通过大量竞标者的来推断某个竞标者竞价; (2) 计算平台需要解密竞标者的竞标信息进行竞价比较, 在这个过程中计算平台会获取竞标者的竞价. 这两种情况都会危害竞标者的竞价隐私, 甚至破坏网络拍卖的公平性.

● 虚假竞标. 在拍卖过程中, 攻击者会在合法竞标者与中间平台通信过程中替换其竞标消息, 甚至假装是合法的竞标者来干预拍卖过程. 如果竞标被操纵, 竞标者可能会失去拍卖或支付更多费用.

3.3 设计目标

为了实现数字藏品网络拍卖中竞标者的竞价隐私保护, 框架实现以下目标.

● 真实性. 竞标者的竞价信息必须是由竞标者本人发起的.

● 不可篡改性. 竞标者的竞价信息任何人不能修改和剪切.

● 时效性. 竞标者的竞价信息仅对某次拍卖有效.

4 基于 CRT-BSGS 的同态 SM2

针对基于 SM2 的同态加密算法解密效率低问题, 本文提出了一种基于 CRT-BSGS 的同态 SM2 方案.

4.1 算法定义

本文提出的同态 SM2 算法, 包含 $Setup, KeyGen, Enc, Dec, Hom$ 这 5 部分, 具体如下.

● $Setup(\lambda, \ell, b) \to Parm$. 参数设置. λ 为密码系统的安全参数, ℓ 为 CRT 中模素数的数量, b 为系统中模素数的二进制位数. $Parm$ 是密码方案的参数.

● $KeyGen(Parm) \to (pk, sk)$. 密钥生成算法. $Parm$ 为密码方案的参数, pk 为生成的公钥, sk 为生成的私钥.

● $Enc(pk, M) \to c$. 加密算法. M 为待加密的明文, pk 为加密时需要的公钥, c 为加密后的密文.

● $Dec(sk, c) \to M$. 解密算法. c 为待解密的密文, sk 为解密时需要的私钥, M 为解密后的明文.

● $Hom(c, c') \to c''$. 同态加法算法. c 和 c' 为待计算的两个密文, c'' 为同态相加后的密文.

4.2 算法构造

● $Setup(\lambda, \ell, b) \to Parm$. λ 为密码系统的安全参数, $\mathbb{G}^T$ 为椭圆曲线的加法循环群, G 为群 $\mathbb{G}^T$ 的基点. n 为基点 G 的阶. 选取 ℓ 个互不相同的 b 比特位素数作为 CRT 取模素数 p_i , N 为这些素数 p_i 的积. N_i 为 $\frac{N}{p_i}$. 计算每个 N_i 在模 p_i 下的乘法逆元 y_i , 即 $N_i y_i \equiv 1 (\bmod p_i)$. 输出 $Parm$ 为:

$$Parm=\{G,\mathbb{G}^T,n,q,p_1,\ldots,p_\ell,N,N_1,\ldots,N_\ell,y_1,\ldots,y_\ell\}. \tag{2}$$

● $KeyGen(Parm)\rightarrow(pk,sk)$. 密钥生成选择一个随机数 $x\leftarrow_R\{1,2,\ldots,n-1\}$ 作为私钥 sk 并且计算 $y=[x]G$ 作为公钥 pk . 它输出以下公私密钥对:

$$sk=x,pk=y. \tag{3}$$

● $Enc(pk,M)\rightarrow CT$. 加密算法以公钥 pk 和消息 M 作为输入. 首先, 算法生成一个随机数 $k\leftarrow_R\{1,2,\ldots,n-1\}$ 并计算 $c_0=[k]G$ 作文密文第 1 部分; 然后, 算法通过每个素数 p_i 对 M 取模, 得到 ℓ 个余数 $m_i=M \bmod p_i$; 最后, 算法计算 $c_i=[k]pk+[m_i]G$ 并将它作为密文第 2 部分. 输出以下密文:

$$\begin{cases} c_0=[k]G, \\ c_i=[k]pk+[m_i]G,\ m_i=M\bmod p_i,\ 0<i\leqslant\ell, \\ CT=(c_0,c_1,\ldots,c_\ell) \end{cases} \tag{4}$$

● $Dec(sk,CT)\rightarrow M$. 解密算法以私钥 pk 和密文 CT 作为输入. 算法对每个 c_i 计算 $[m_i]G=c_i-[sk]c_0$ 并通过 BSGS 算法计算出 m_i , 它输出以下明文:

$$M=\sum_{i=1}^{\ell}m_iN_iy_i(\bmod N),\ m_i=BSGS(c_i-[sk]c_0),\ 0<i\leqslant\ell. \tag{5}$$

● $Hom(CT,CT')\rightarrow CT''$. 同态加法算法以两个密文 $CT=(c_0,c_1,\ldots,c_\ell)$ 和 $CT'=(c'_0,c'_1,\ldots,c'_\ell)$ 作为输入, 算法将两个密文中每个部分进行相加, 输出以下密文:

$$CT''=(c_0+c'_0,c_1+c'_1,\ldots,c_\ell+c'_\ell). \tag{6}$$

这里进行同态性分析. 假设两个明文 M 和 M' 分别对应密文 $CT=(c_0=[k]G,c_1=[k]pk+[M \bmod p_1]G,\ldots,c_\ell=[k]pk+[M \bmod p_\ell]G)$ 和 $CT'=(c'_0=[k']G,c'_1=[k']pk'+[M' \bmod p_1]G,\ldots,c_\ell=[k']pk'+[M' \bmod p_\ell]G)$, 同态计算结果为:

$$\begin{aligned} CT''&=CT+CT' \\ &=(c_0+c'_0,c_1+c'_1,\ldots,c_\ell+c'_\ell) \\ &=(c''_0,c''_1,\ldots,c''_\ell) \end{aligned} \tag{7}$$

解密同态计算结果 $CT''=(c''_0,c''_1,\ldots,c''_\ell)$, 使用私钥 sk 对每个 $c''_i=c_i+c'_i$ 计算 $c''_i-[sk]c''_0=c_i-[sk]c_0+c'-[sk]c'_0$ 得到 $[m_i+m'_i]G$, 根据定理 1 由 BSGS 方法计算出 $m''_i=m_i+m'_i$, 最后对所有 m''_i 进行 CRT 求解得到 $M''=M+M'$.

5 基于国密的数字藏品网络拍卖隐私保护协议

本节分析了网络拍卖流程并设计了数字藏品网络拍卖隐私保护协议, 包括委托拍卖协议和竞标协议. 实现数字藏品网络拍卖中竞标人竞价信息隐私保护的同时不影响竞价信息可用性; 每个竞标仅通过一次交互完成比较操作, 随着网络拍卖参与人数增多, 竞标协议的计算成本呈线性增长.

5.1 拍卖流程

本文提出的拍卖流程大致可分为委托拍卖协议、竞标协议两个内容.

● 委托拍卖协议. 卖方将数字藏品加密并委托中间平台进行拍卖, 中间平台接收委托后初始化拍卖. 为了提高加解密效率, 对数字藏品的加密采用对称加密方案, 如 SM4 等. 在这个协议里数字藏品需要对各个实体保密.

● 竞标协议. 竞标协议包括竞标者出价和竞标处理两个过程. 在竞标者出价过程中, 竞标者对数字藏品出价参与拍卖, 竞标者需要将自己的竞价交给中间平台. 在这个过程中需要防止中间平台推断竞标者竞标信息以及恶意竞标者的虚假竞标攻击. 在竞标处理过程中, 中间平台将加密的竞价交予计算平台处理, 获取所有竞价中的最大值, 这个阶段需要防止中间平台窃取竞价.

数字藏品的交付采用混合加密的方法, 即在拍卖结束后, 中间平台将对称加密的数字藏品交给获胜的竞标者, 卖方使用获胜者的公钥加密对称密钥并通过中间平台交付给竞标者. 竞标者使用自己的私钥解密获取对称密钥, 使用对称密钥解密数字藏品即可.

5.2 拍卖协议

● 委托拍卖协议. 为了保护数字藏品交付的机密性, 采用对称加密算法加密数字藏品, 密钥 key 由卖方自己保留, 在拍卖结束后对 key 采用非对称加密并交付给获胜者. 协议实现数字藏品安全的委托交付. 同时, 中间平台生成随机噪声 $Noise$ 作为拍卖过程中所有竞价 P_{bi} 的噪声.

在委托拍卖期间, 卖方使用对称密钥 key 加密的数字藏品 PK_a(collection) 并签名 $S_s[PK_a(\text{collection})]$, 将密文数字藏品和签名作为委托信息发送给中间平台. 合约验证卖方的签名 $sign_{\text{collection}}$, 如果验证失败返回 $false$, 验证成功后向计算平台请求一个公钥 pk_a 作为拍卖的公钥信息 (私钥 sk_a 由计算平台自己保留), 中间平台生成一个随机噪声 $Noise$ (仅由中间平台保留) 并公开拍卖编号 B_number 后开始拍卖. 委托拍卖过程如图 2 所示.

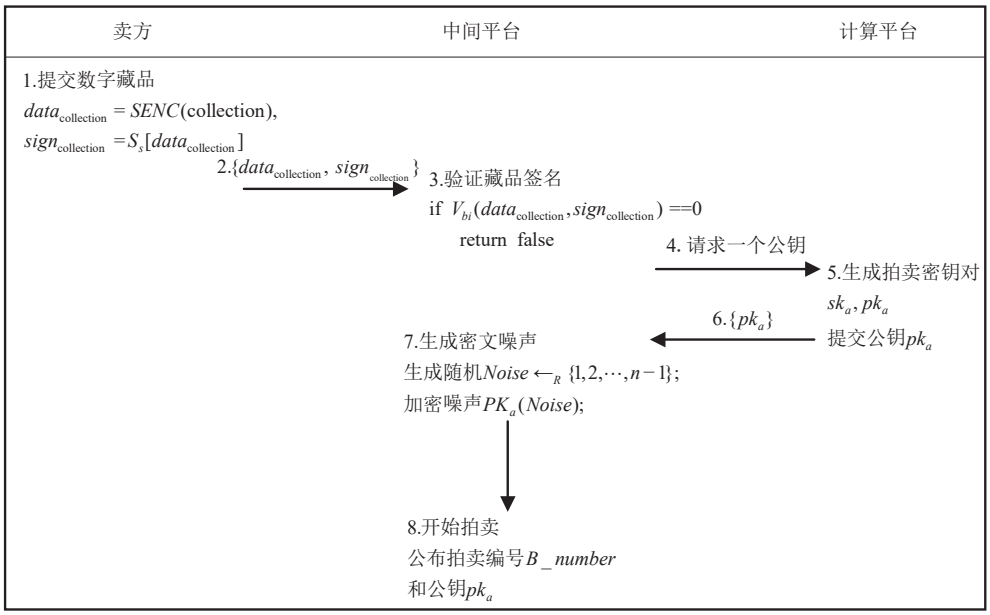

图 2 委托拍卖协议流程图

● 竞标协议. 竞标者的竞价采用 pk_a 加密, 解密密钥 sk_a 仅由计算平台保存, 中间平台无法解密获取竞标者的竞价 $PK_a(P_{bi})$. 因此, 在竞标出价过程中, 实现了竞标者的竞价隐私保护. 竞标处理过程中, 中间平台对竞标者的竞价 $PK_a(P_{bi})$ 加入了噪声 $PK_a(Noise)$, 计算平台即使解密得到的也是带有噪声的竞价 $P_{bi}+Noise$, 而噪声 $Noise$ 仅由中间平台知晓. 因此, 在竞标处理的过程中, 实现了竞标者的竞价隐私保护. 由于中间平台对待比较所有竞价加入相同大小的噪声, 故不影响所有竞价间的大小关系. 在竞标过程中, 对于每次竞标仅需要一次中间平台与计算平台的交互即可完成, 计算开销固定. 因此, 协议的计算复杂度呈线性 O(n) 增长.

在竞标期间, 竞标者使用拍卖公钥 pk_a 加密自己的竞价 P_{bi}, 并对加密竞标 $PK_a(P_{bi})$ 和编号 B_number 签名, 提交竞标信息 $\{PK_a(P_{bi}), B\_number, S_{bi}[PK(P_{bi})+B\_number]\}$ 给中间平台; 在拍卖未结束时, 中间平台接收竞标者竞标信息, 同时对竞标者的签名进行验证 $V_{bi}(S_{bi}[PK(P_{bi})+B\_number])$. 如果验证失败, 返回 false; 如果验证通过, 中间平台会执行竞标处理过程. 为了确定新传入竞价的大小, 需要将接收到的新竞价 $PK_a(P_{bi})$ 与当前最高竞价 $PK_a(P_w)$ 进行比较. 中间平台将两个加密的竞价都加入相同的噪声 $Noise$ 并发送给计算平台. 计算平台在接收到中间平台传来的两个密文后, 用私钥 sk_a 解密并比较两个加噪竞价 $\{P1, P2\}$ 的大小. 如果第 2 个数据更大, 则返回 True, 否则返回 False. 中间平台在收到计算平台的回复后, 如果返回 True 就更新此竞价为最高竞价, 否则不做任何更改. 竞标过程如图 3 所示.

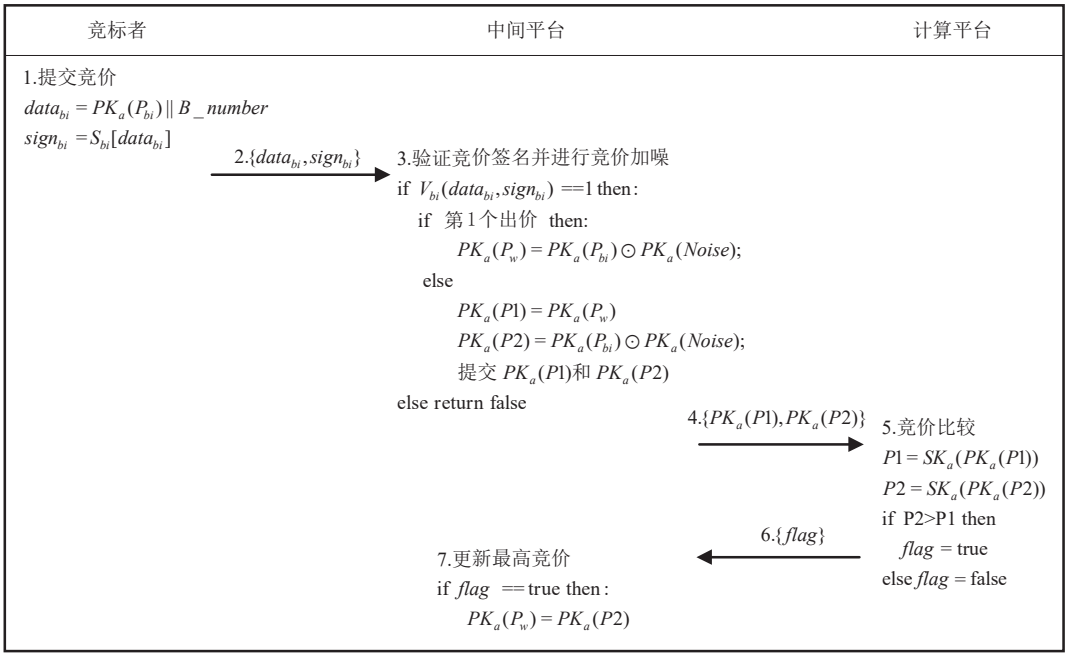

图 3 竞标协议流程图

6 数字藏品网络拍卖方案的安全性分析

本文所提出的网络拍卖隐私保护协议为竞标者的竞价隐私提供了安全保障. 在网络拍卖中, 对中间平台的保密依赖于数据加密; 对计算平台的保密依赖于对竞价的加噪操作和同态运算. 因此, 本框架的安全核心在于密文的保密性和同态性. 如果恶意竞标者可以攻破密文, 就能在拍卖中处于有利地位, 竞标者的隐私就无法保证. 如果密文同态性计算错误会造成加噪错误或失败, 计算平台窃取竞标者的竞价隐私.

在本节, 首先分析了基于 CRT-BSGS 的同态 SM2 方案的安全性, 包括正确性和保密性. 然后分析数字藏品网络拍卖协议的安全性, 包括抗竞价信息窃取和抗虚假竞标. 最后, 分析了网络拍卖框架的安全性, 涉及真实性、不可篡改性和时效性.

6.1 基于 CRT-BSGS 的同态 SM2 安全性

● 正确性分析

假设 B 收到 A 发来的密文信息 $CT = (c_0 = [k]G, c_1 = [k]pk + [M \bmod p_1]G, \ldots, c_\ell = [k]pk + [M \bmod p_l]G)$, B 使用私钥 sk 对每个 c_i 计算 $c_i - [sk]c_0$ 得到 $[m_i]G$, 根据定理 1 由 BSGS 方法计算出 m_i. 最后一步对所有 m_i 进行 CRT 求解得到 M.

定理 1. 对于一个离散对数问题 $a^x \equiv b(\bmod p)$, 已知 a 、 b 和 p 求解 x, 使用 BSGS 的方法可以将计算时间复杂度从 O(p) 降低到 O($\sqrt{p}$), 大大降低了计算的时间复杂度.

证明: 如果令 $x = \mathrm{A}t - \mathrm{B}$ 其中 $t = \sqrt{p}, A \in [1,t], B \in [1,t)$, 那么原问题则转化为了: $a^{At} \equiv a^B b(\bmod p)$, 其中 a 与 p 互质, 求解 A 和 B 的问题. 要求解此问题, 首先需要遍历 $a^B b(\bmod p)$ 并使用哈希表将结果存储下来, 这一步的时间复杂度为 O($\sqrt{p}$), 然后逐步遍历左边 $a^{At}(\bmod p)$, 并在哈希表中查找, 假设当前遍历数据为 $\widetilde{A}t$, 在哈希表查找出来数据为 $\widetilde{B}$, 那么求解的 $\widetilde{x} = \widetilde{A}t - \widetilde{B}$, 总体时间复杂度为 O($\sqrt{p}$).

● 保密性分析

定义 1. 设 $\mathbb{G}$ 是阶为大素数 q 的群, g 为 $\mathbb{G}$ 的生成元, $x, y, z \leftarrow_R \mathbb{Z}_q$ 则以下两个分布: 随机四元组 $R = (g, g^x, g^y, g^z) \in \mathbb{G}^4$

和四元组 $D=(g,g^x,g^y,g^{xy})\in\mathbb{G}^4$ 是计算上不可区分的, 称为 DDH (decisional diffie-hellman) 假设.

定理 2. 在 DDH 假设下, 基于 CRT-BSGS 的同态 SM2 算法是选择明文攻击下的不可区分性 (indistinguishability under chosen-plaintext attack, IND-CPA) 是安全的.

证明: 假设存在一个概率多项式时间 (probabilistic polynomial time, PPT) 敌手 A 攻击基于 CRT-BSGS 的同态 SM2 方案的 IND-CPA 安全. A 输出等长消息 M_0 和 M_1, 得到 M_β 的密文, 输出猜测 β'. 若 $\beta'=\beta$, 则 A 成功. 构造一个敌手 B, B 利用 A 来攻击 DDH 假设. 设 B 输入为四元组 $T=(G,[x]G,[y]G,[z]G)$, 群 $\mathbb{G}^T$ 及其生成元 G 是公开的. $\alpha=1$ 表示四元组为 Diffie-Hellman (DH) 四元组, $\alpha=0$ 表示四元组为随机四元组.

B 构造以下模型测试 DDH 假设:

$\underline{\mathrm{B}(T)}$:

$pk=(G,[x]G)$;
$(M_0,M_1)\leftarrow \mathrm{A}(pk)$;

$\beta\leftarrow_R\{0,1\}$;

$C^*=([y]G,[z]G+[M_\beta]G)$

$\beta'=\mathrm{A}(pk,C^*)$

如果$\beta'=\beta$则输出1; 否则输出0

A 获取的优势为:

$$\mathrm{Adv}_{\mathrm{A}}^{\text{IND-CPA}}=\left|\Pr[\beta=\beta']-\frac{1}{2}\right|=\varepsilon$$

B 成功解决 DDH 假设的优势为:

$$\begin{aligned}\mathrm{Adv}_{\mathrm{B}}^{\text{IND-CPA}}&=\Pr[\mathrm{B}(T)=1|\alpha=1]\cdot\Pr(\alpha=1)+\Pr[\mathrm{B}(T)=1|\alpha=0]\cdot\Pr(\alpha=0)-\frac{1}{2}\\&=\frac{1}{2}\Pr[\mathrm{B}(T)=1|\alpha=1]+\frac{1}{2}\Pr[\mathrm{B}(T)=1|\alpha=0]-\frac{1}{2}\\&=\frac{1}{2}\left(\frac{1}{2}+\varepsilon\right)+\frac{1}{2}\cdot\frac{1}{2}-\frac{1}{2}\\&=\frac{\varepsilon}{2}\end{aligned}$$

综上所述, 如果存在一个 PPT 敌手 A 能以不可忽略的优势 ε 打破基于 CRT-BSGS 的同态 SM2 加密方案, 则可以构造挑战者 B 以不可忽略的优势 $\frac{\varepsilon}{2}$ 解决 DDH 假设. 因此, 基于 CRT-BSGS 的同态 SM2 加密方案是 IND-CPA 安全的.

6.2 协议安全性

● 竞价信息窃取. 在竞价信息窃取攻击中, 计算平台和中间平台可能会在不违反协议的情况下获取竞标者竞价信息. 为了保护竞标者的用户隐私, 竞标者的所有竞价都需要加密处理, 并且竞标的解密和比较工作放在计算平台中. 由于基于 CRT-BSGS 同态 SM2 的保密性, 中间平台无法获取竞标者的竞价. 同时, 本文引入了同态加噪方法, 中间平台会对所有的竞价都加入随机噪声, 因此, 中间平台得到的密文竞价都是加入噪声的竞价. 从而在计算平台端实现了对竞价的隐私保护.

● 虚假竞标. 在虚假竞标攻击中, 攻击者在通信过程中替换合法竞标者的竞标消息, 甚至假装是合法的竞标者来干预拍卖过程. 因此, 本文采用基于数字签名的身份认证方式防范虚假竞标攻击. 在拍卖中, 竞标者参与拍卖需要对自己的竞价信息签名, 中间平台收到竞标者的竞价后首先需要对竞标者的签名进行验证, 同时签名中加入了拍卖编号, 防止攻击者进行重放攻击.

6.3 框架安全性

● 真实性. 竞标者参与拍卖必须对自己的竞价信息进行签名, 私钥仅由竞标者本人拥有, 保证签名的唯一性,

可以真实代表竞标者的唯一身份信息.

● 不可篡改性. 在竞标者参与拍卖时, 竞标者对拍卖的编号和密文竞价都进行了签名. 因此, 任何篡改都会造成签名验证失败.

● 时效性. 在竞标者参与拍卖过程中, 需要明确指出自己要参加的拍卖编号并进行签名. 因此, 竞标者的竞价信息仅对某次拍卖有效.

7 性能评估

本文采用 Java 语言实现了基于 CRT-BSGS 的同态 SM2 密码方案, 并在局域网下进行了网络拍卖竞标模拟. 在 i5-12500H 2.50 GHz 16 GB 运行内存的环境下, 对基于 CRT-BSGS 的同态 SM2 算法、数字藏品交付和拍卖协议进行了性能测试. 结果表明, 本文的系统具有较低的时空成本和较高的拍卖处理性能.

1) 密码方案时空效率

在 128 比特安全等级 (256 位椭圆曲线、3072 位 Paillier) 下, 本文将提出的基于 CRT-BSGS 的同态 SM2 与国际中著名且广泛运用的 Paillier 算法[36]进行对比测试, 结果显示本文算法时空效率有优势.

本文对基于 CRT-BSGS 的同态 SM2 进行 4 种参数设置, 如将 32 位数据分解为 3 个 11 位数据 (32-11)、51 位数据分解为 4 个 13 位数据 (51-13)、64 位数据分解为 5 个 13 位数据 (64-13) 和 4 个 17 位数据 (64-17). 在这些参数设置下对基于 CRT-BSGS 的同态 SM2 进行 10000 次的加密算法、解密算法和同态算法时间效率测试, 同时进行密文空间成本测试, 测试数据分别为随机 32 位、51 位和 64 位整数, 测试结果如图 4 所示.

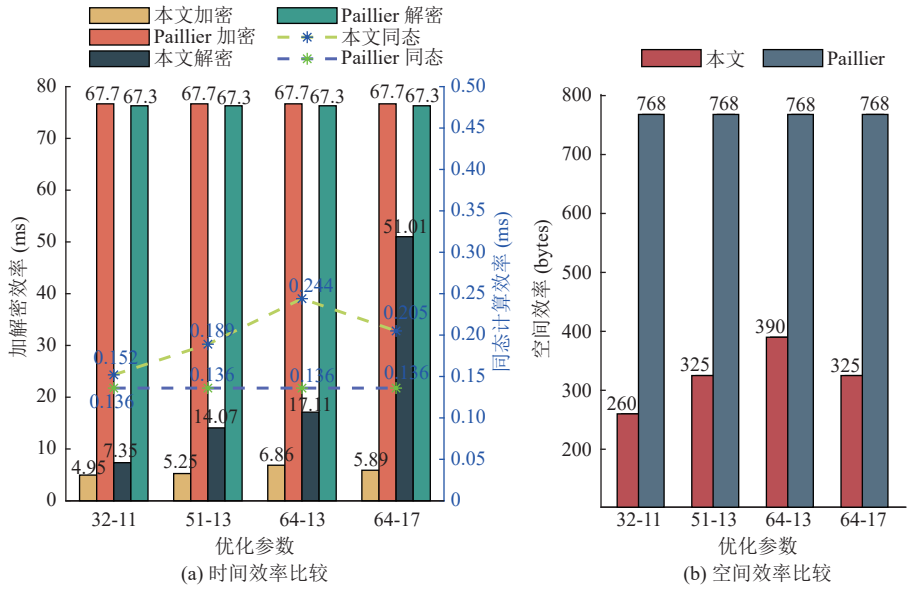

图 4 基于 CRT-BSGS 的同态 SM2 算法 (本文) 和 Paillier 算法时空效率分析

如图 4(a), 在时间效率方面, 基于 CRT-BSGS 的同态 SM2 加解密效率都要优于 Paillier 方案, 解密时间降低到 7.35 ms, 提升了数据处理效率, 同时, 本文采用优化算法后的加解密效率明显高于 Paillier 算法, 虽然同态运算为 0.152 ms, 相对于 Paillier 方案效率较低. 如图 4(b), 在空间效率方面, 本文密码的算法密文空间成本最高为 390 B, 最低为 260 B, 本文密文空间约为 Paillier 算法的 34%–50%. 在不同优化参数下, 方案的空间效率和时间效率会产生不同的变化. 空间效率随着优化参数中素数的个数增加成本呈现线性增加, 这是因为优化参数每增加一个素数需要增加一个椭圆曲线下的点. 时间效率主要与优化参数中素数的个数和优化参数中素数的大小有关, 优化参数中素数的个数影响需要计算椭圆曲线下点的个数, 优化参数中素数的大小影响进行 BSGS 算法的计算效率. 总的

来说, 时间效率和空间效率都与优化参数中素数个数呈线性关系, 时间效率与优化参数中素数的平方根呈线性关系.

2) 数字藏品交付

本文通过对数字藏品交付的混合加密效率和空间成本测试来评估数字藏品交付的性能. 其中数字藏品的对称加密采用国密 SM4, 密钥加密采用国密 SM2, 假设数字藏品为像素 250×325 和像素 $3\,840\times2\,160$ 的 jpg 图片. 测试的结果如表 2 所示, 混合总时间分别为 0.143 s 和 141.993 s, 随着数字藏品数据的增大, 数字藏品交付的计算成本也增大.

表 2 混合加密性能 (ms) 与空间成本 (bytes)

数字藏品大小	像素250×325		像素$3\,840\times2\,160$	
操作类型	加密	解密	加密	解密
数字藏品加解密	76.723	63.270	71 376.108	70 613.454
密钥加解密	2.609	1.024	2.609	1.024
混合加密性能	143.626		141 993.195	
明文空间成本	20 369		584 623	
密文空间成本	20 384		584 624	

3) 竞标协议性能检测

本文分别对 100 次、1 000 次和 10 000 次 32 位竞价的竞标进行模拟处理, 其中按照 5% 的比例通过伪造签名或重用以往竞标签名进行虚假竞标, 得到均次竞标处理时间效率和虚假竞标检测成功率如表 3 所示. 本文方案单次竞标处理性能控制在 30 ms 以内, 10 000 次竞价可以在 5 min 内处理完, 远低于以往方案 (EPPAS)[19](由于以往方案并未公布源码, 这里直接采用对方的测试结果). 主要由于 EPPAS 采用了时间复杂度为 $O(n\log n)$ 堆排序方法; 而本文仅保留了最高竞价, 时间复杂度为 $O(n)$, 具有较低的时间复杂度. 同时本文的方案除了同态加噪, 其他任何一项基本操作效率指标都明显高于以往方案. 因此, 本文方案具有更高的性能.

表 3 本方案系统与以往系统均次竞标处理的时间效率 (ms) 和虚假竞标检测成功率

方案类型	100次	1 000次	10 000次	虚假竞标检测成功率 (%)
EPPAS[19]	516.87	505.88	504.75	100
本文	25.33	22.833	29.216 2	100

4) 拍卖后的竞标者竞价隐私分析

针对拍卖中竞标者的隐私保护, 本文采用门限 Paillier 也做了相关实验, 直到人数达到设定的阈值才公开拍卖结果. 本文通过基于 Sharmir 门限的思想实现了门限 Paillier, 构建了基于门限 Paillier 的网络拍卖方案. 相关实验的设计如下, 将密钥分别分发给 100 个、500 个和 1 000 个待参加拍卖的人, 规定当其中真实参与竞标的人数分别达到门限阈值 60、300 和 600 时停止竞标, 实验门限设计分别表示为 (60, 100)、(300, 500) 和 (600, 1 000), 得到的方案执行效率如表 4 所示. 实验结果显示, 随着门限阈值的增加, 恢复密钥所需时间会增加, 解密竞价所需时间也会增加. 同时, 表明基于门限的拍卖能够保护拍卖中竞标者的竞价隐私, 但存在拍卖后的竞价泄露问题. 本文通过双平台 (中间平台和计算平台) 和对密文竞价加噪的方式, 构建了隐私保护的拍卖方案, 保护了拍卖全流程竞标者竞价的隐私. 因此, 本文提出的拍卖方案更适用于隐私保护下的网络拍卖.

表 4 基于门限 Paillier 的网络拍卖方案执行性能 (ms)

门限设计	(60, 100)	(300, 500)	(600, 1 000)
密钥分发	16.748	130.923	461.548
密钥恢复	121.082	477.455	1 695.636
加密竞价	4 542.432	22 465.726	45 511.317
解密竞价	4 444.626	22 120.309	44 809.267

8 总 结

针对数字藏品网络拍卖的竞价隐私保护需求, 本文提出了数字藏品网络拍卖隐私保护方案. 本文首次将国密与网络拍卖相结合, 设计了基于国密的数字藏品网络拍卖隐私保护方法, 在此方案中, 网络拍卖协议的竞标处理复杂度仅为 $O(n)$. 针对网络拍卖隐私保护协议执行效率需求设计了基于 CRT-BSGS 的国密 SM2 算法, 相较于 Paillier 算法具有显著的效率提升. 最后, 通过实验证明了本文所提同态算法和网络拍卖方案的安全性和高效性.

References:

[1] Zhang YD, Zhang HL. Metaverse in the field of consumption: A review and prospects. Foreign Economics & Management, 2023, 45(8): 118–136 (in Chinese with English abstract). [doi: 10.16538/j.cnki.fem.20230426.301]

[2] Ma ZG, Wang XQ. Construction of NFT mapping rights in the metaverse. Journal of Xi'an Jiaotong University (Social Sciences), 2023, 43(2): 162–175 (in Chinese with English abstract). [doi: 10.15896/j.xjtuskxb.202302016]

[3] Odom W, Zimmerman J, Forlizzi J. Placelessness, spacelessness, and formlessness: Experiential qualities of virtual possessions. In: Proc. of the 2014 Conf. on Designing Interactive Systems. New York: Association for Computing Machinery, 2014. 985–994. [doi: 10.1145/2598510.2598577]

[4] Wilson KB, Karg A, Ghaderi H. Prospecting non-fungible tokens in the digital economy: Stakeholders and ecosystem, risk and opportunity. Business Horizons, 2022, 65(5): 657–670. [doi: 10.1016/j.bushor.2021.10.007]

[5] Ko H, Son B, Lee Y, Jang H, Lee J. The economic value of NFT: Evidence from a portfolio analysis using mean-variance framework. Finance Research Letters, 2022, 47: 102784. [doi: 10.1016/j.frl.2022.102784]

[6] Liu ZX, Shen YY, Guan XP. A VCG-auction based distributed mechanism for network resource allocation. Acta Electronica Sinica, 2010, 38(8): 1929–1934 (in Chinese with English abstract).

[7] Zhang XW, Jiang D, Yuan Y. A survey of game theory and auction-based data pricing. Big Data Research, 2021, 7(4): 61–79 (in Chinese with English abstract). [doi: 10.11959/j.issn.2096-0271.2021039]

[8] OpenSea. https://opensea.io/

[9] SuperRare. https://superrare.com

[10] Nifty Gateway. https://www.niftygateway.com

[11] Lindell Y, Pinkas B, Smart NP, Yanai A. Efficient constant-round multi-party computation combining BMR and SPDZ. Journal of Cryptology, 2019, 32(3): 1026–1069. [doi: 10.1007/s00145-019-09322-2]

[12] Lindell Y, Smart NP, Soria-Vazquez E. More efficient constant-round multi-party computation from BMR and SHE. In: Proc. of the 14th Int'l Conf. on Theory of Cryptography. Beijing: Springer, 2016. 554–581. [doi: 10.1007/978-3-662-53641-4_21]

[13] Sutradhar K, Om H. A privacy-preserving comparison protocol. IEEE Trans. on Computers, 2023, 72(6): 1815–1821. [doi: 10.1109/TC.2022.3215640]

[14] Li DH, Yang QY, Yu W, An D, Zhang Y, Zhao W. Towards differential privacy-based online double auction for smart grid. IEEE Trans. on Information Forensics and Security, 2020, 15: 971–986. [doi: 10.1109/TIFS.2019.2932911]

[15] Ul Hassan M, Rehmani MH, Chen JJ. DEAL: Differentially private auction for blockchain-based microgrids energy trading. IEEE Trans. on Services Computing, 2020, 13(2): 263–275. [doi: 10.1109/TSC.2019.2947471]

[16] Li DH, Yang QY, Li C, An D, Shi Y. Bayesian-based inference attack method and individual differential privacy-based auction mechanism for double auction market. IEEE Trans. on Automation Science and Engineering, 2023, 20(2): 950–968. [doi: 10.1109/TASE.2022.3181570]

[17] Guo JX, Ding XJ, Wang T, Jia WJ. Combinatorial resources auction in decentralized edge-thing systems using blockchain and differential privacy. Information Sciences, 2022, 607: 211–229. [doi: 10.1016/j.ins.2022.05.128]

[18] Jung T, Li XY. Enabling privacy-preserving auctions in big data. In: Proc. of the 2015 IEEE Conf. on Computer Communications Workshops. IEEE, 2015. 173–178. [doi: 10.1109/INFCOMW.2015.7179380]

[19] Gao WC, Yu W, Liang F, Grant Hatcher W, Lu C. Privacy-preserving auction for big data trading using homomorphic encryption. IEEE Trans. on Network Science and Engineering, 2020, 7(2): 776–791. [doi: 10.1109/TNSE.2018.2846736]

[20] Blass EO, Kerschbaum F. BOREALIS: Building block for sealed bid auctions on blockchains. In: Proc. of the 15th ACM Asia Conf. on Computer and Communications Security. New York: Association for Computing Machinery, 2020. 558–571. [doi: 10.1145/3320269.3384752]

[21] Lin C, Huang XY, He DB. Efficient range proof protocols based on Chinese cryptographic SM2. Chinese Journal of Computers, 2022,

45(1): 148–159 (in Chinese with English abstract). [doi: 10.11897/SP.J.1016.2022.00148]

[22] Chen XS, Jiang C, Wang W, Jin X, Lan X. Research on the extension of Chinese commercial cryptographic algorithms for virtual trusted platform module. Advanced Engineering Sciences, 2020, 52(3): 141–149 (in Chinese with English abstract). [doi: 10.15961/j.jsuese.201900866]

[23] Chen J, Peng CG, Fan MM, Ding HF, Zhao YY. SM4-FPE: A format-preserving encryption algorithm based on SM4 for numeric data. Journal of Chinese Computer Systems, 2019, 40(6): 1274–1279 (in Chinese with English abstract). [doi: 10.3969/j.issn.1000-1220.2019.06.025]

[24] Lai JC, Huang XY, He DB, Ning JT. CCA secure broadcast encryption based on SM9. Ruan Jian Xue Bao/Journal of Software, 2023, 34(7): 3354–3364 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/6531.htm [doi: 10.13328/j.cnki.jos.006531]

[25] Tang F, Ling GW, Shan JY. Additive homomorphic encryption schemes based on SM2 and SM9. Journal of Cryptologic Research, 2022, 9(3): 535–549 (in Chinese with English abstract). [doi: 10.13868/j.cnki.jcr.000532]

[26] Qu SN. NFT industry: Theoretical deconstruction, market logic and trend outlook. Reform, 2023, (4): 70–80 (in Chinese with English abstract).

[27] Yang KD, Zhang ZY, Tian YL, Ma JF. A secure authentication framework to guarantee the traceability of avatars in metaverse. IEEE Trans. on Information Forensics and Security, 2023, 18: 3817–3832. [doi: 10.1109/TIFS.2023.3288689]

[28] Zhang ZY, Deng RL, Tian YL, Cheng P, Ma JF. SPMA: Stealthy physics-manipulated attack and countermeasures in cyber-physical smart grid. IEEE Trans. on Information Forensics and Security, 2023, 18: 581–596. [doi: 10.1109/TIFS.2022.3226868]

[29] Zhang ZY, Cheng P, Wu JF, Chen JM. Secure state estimation using hybrid homomorphic encryption scheme. IEEE Trans. on Control Systems Technology, 2021, 29(4): 1704–1720. [doi: 10.1109/TCST.2020.3019501]

[30] Shi SS, Sun WH, Jiang MJ, Qu HP. Research on smart grid privacy protocol based on distributed data aggregation. Netinfo Security, 2015(12): 59–65 (in Chinese with English abstract). [doi: 10.3969/j.issn.1671-1122.2015.12.010]

[31] Wibawa F, Catak FO, Kuzlu M, Sarp S, Cali U. Homomorphic encryption and federated learning based privacy-preserving CNN training: COVID-19 detection use-case. In: Proc. of the 2022 European Interdisciplinary Cybersecurity Conf. Barcelona: ACM, 2022. 85–90. [doi: 10.1145/3528580.3532845]

[32] The State Encryption Administration. GM/T 0003-2012 Public key cryptographic algorithm SM2 based on elliptic curves. Beijing: Standards Press of China, 2012 (in Chinese).

[33] The State Encryption Administration. GM/T 0004-2012 SM3 cryptographic hash algorithm. Beijing: Standards Press of China, 2012 (in Chinese).

[34] The State Encryption Administration. GM/T 0002-2012 SM4 block cipher algorithm. Beijing: Standards Press of China, 2012 (in Chinese).

[35] The State Encryption Administration. GM/T 0044-2016 Identity-based cryptographic algorithms SM9. Beijing: Standards Press of China, 2016 (in Chinese).

[36] Paillier P. Public-key cryptosystems based on composite degree residuosity classes. In: Proc. of the Int'l Conf. on Theory and Application of Cryptographic Techniques. Prague: Springer, 1999. 223–238. [doi: 10.1007/3-540-48910-X_16]

附中文参考文献:

[1] 张宇东, 张会龙. 消费领域的元宇宙: 研究述评与展望. 外国经济与管理, 2023, 45(8): 118–136. [doi: 10.16538/j.cnki.fem.20230426.301]

[2] 马治国, 王雪琪. 元宇宙 NFT 映射权之构建. 西安交通大学学报 (社会科学版), 2023, 43(2): 162–175. [doi: 10.15896/j.xjtuskxb.202302016]

[6] 刘志新, 申妍燕, 关新平. 一种基于 VCG 拍卖的分布式网络资源分配机制. 电子学报, 2010, 38(8): 1929–1934.

[7] 张小伟, 江东, 袁野. 基于博弈论和拍卖的数据定价综述. 大数据, 2021, 7(4): 61–79. [doi: 10.11959/j.issn.2096-0271.2021039]

[21] 林超, 黄欣沂, 何德彪. 基于国密 SM2 的高效范围证明协议. 计算机学报, 2022, 45(1): 148–159. [doi: 10.11897/SP.J.1016.2022.00148]

[22] 陈兴蜀, 蒋超, 王伟, 金鑫, 兰晓. 针对虚拟可信平台模块的国密算法扩展技术研究. 工程科学与技术, 2020, 52(3): 141–149. [doi: 10.15961/j.jsuese.201900866]

[23] 陈佳, 彭长根, 樊玫玫, 丁红发, 赵园园. SM4-FPE: 基于 SM4 的数字型数据保留格式加密算法. 小型微型计算机系统, 2019, 40(6): 1274–1279. [doi: 10.3969/j.issn.1000-1220.2019.06.025]

[24] 赖建昌, 黄欣沂, 何德彪, 宁建廷. 基于 SM9 的 CCA 安全广播加密方案. 软件学报, 2023, 34(7): 3354–3364 http://www.jos.org.cn/1000-9825/6531.htm [doi: 10.13328/j.cnki.jos.006531]

[25] 唐飞, 凌国玮, 单进勇. 基于国密 SM2 和 SM9 的加法同态加密方案. 密码学报, 2022, 9(3): 535–549. [doi: 10.13868/j.cnki.jcr.000532]
[26] 渠慎宁. NFT 产业: 理论解构、市场逻辑与趋势展望. 改革, 2023, (4): 70–80.
[30] 石沙沙, 孙文红, 江明建, 曲海鹏. 基于分布式数据聚合的智能电网隐私保护协议研究. 信息网络安全, 2015(12): 59–65. [doi: 10.3969/j.issn.1671-1122.2015.12.010]
[32] 国家密码管理局. GM/T 0003-2012 SM2 椭圆曲线公钥密码算法. 北京: 中国标准出版社, 2012.
[33] 国家密码管理局. GM/T 0004-2012 SM3 密码杂凑算法. 北京: 中国标准出版社, 2012.
[34] 国家密码管理局. GM/T 0002-2012 SM4 分组密码算法. 北京: 中国标准出版社, 2012.
[35] 国家密码管理局. GM/T 0044-2016 SM9 标识密码算法. 北京: 中国标准出版社, 2016.

邵宽(2000－), 男, 硕士, 主要研究领域为数据交易, 应用密码学.

王鑫(1991－), 男, 博士, 副研究员, 主要研究领域为联邦学习, 数据隐私保护, 协同计算/优化, 工业互联网安全.

张镇勇(1991－), 男, 博士, 教授, CCF 专业会员, 主要研究领域为人工智能安全, 智能电网安全, 工控系统安全.

田有亮(1982－), 男, 博士, 教授, 博士生导师, CCF 专业会员, 主要研究领域为算法博弈论, 密码学与安全协议, 大数据安全与隐私保护.

杨科迪(1990－), 男, 博士生, CCF 学生会员, 主要研究领域为元宇宙安全, 数据溯源, 区块链技术.

马建峰(1963－), 男, 博士, 教授, 博士生导师, CCF 会士, 主要研究领域为应用密码学, 无线网络安全, 数据安全, 移动智能系统安全.

朱俊彦(2000－), 男, 硕士, 主要研究领域为数据交易, 博弈论.