理性安全的公平两方比较协议

赵搏文[1]，祝遥[1]，肖阳[2]，裴庆祺[2]，李小国[3]，刘西蒙[4]

（1. 西安电子科技大学广州研究院，广东 广州 510555；2. 西安电子科技大学综合业务网国家重点实验室，陕西 西安 710071；
3. 新加坡管理大学计算与信息系统学院，新加坡 178902；4. 福州大学计算机与大数据学院，福建 福州 350108）

摘 要：现有的安全两方比较协议通常是让一方（如 Alice）先获知比较结果，然后 Alice 将比较结果告知另一方（如 Bob）。如果 Alice 拒绝或未将结果发送给 Bob，则协议无法保障参与方都拿到比较结果，协议的公平性被破坏。为解决上述问题，结合门限 Paillier 密码系统与博弈论提出一种理性安全的公平两方比较协议 TEAM。具体地，首先利用门限 Paillier 密码系统设计一种新型的安全两方比较协议。接着引入博弈论机制，探寻所提安全两方比较协议双方均获得比较结果的博弈均衡点。严格的理论分析表明，TEAM 保障理性的参与方可在不泄露各自数据的情况下正确地获得比较结果，即 TEAM 是一个正确、安全且公平的两方比较协议。实验结果显示，同等实验环境下 TEAM 的计算效率相较于现有的安全两方比较方法运行速度能提升超 50 倍。

关键词：安全比较；博弈论；同态加密；门限密码；可信计算

中图分类号：TN92

文献标志码：A

DOI: 10.11959/j.issn.1000−436x.2023220

Rational-security and fair two-party comparison protocol

ZHAO Bowen[1], ZHU Yao[1], XIAO Yang[2], PEI Qingqi[2], LI Xiaoguo[3], LIU Ximeng[4]

1. Guangzhou Institute of Technology, Xidian University, Guangzhou 510555, China
2. Xidian University State Key Laboratory of Integrated Service Networks, Xi’an 710071, China
3. School of Computing and Information Systems, Singapore Management University, Singapore 178902, Singapore
4. College of Computer and Data Science, Fuzhou University, Fuzhou 350108, China

Abstract: Existing secure two-party comparison protocols usually allowed one party (e.g., Alice) to obtain a comparison result first, and then Alice informed the other one (e.g., Bob) of the comparison result. Obviously, if Alice refused or failed to send the comparison result to Bob, Bob learned nothing about the comparison result, which broke the fairness of the two-party comparison protocol. Based on this, a rational-security and fair two-party comparison protocol TEAM was proposed by seamlessly combining the threshold Paillier cryptosystem and game theory. Specifically, a novel secure two-party comparison protocol based on the threshold Paillier cryptosystem was designed and then searched for equilibrium points at which two parties could obtain comparison results. Strict theoretical analysis demonstrate that TEAM guarantees rational two-party to always obtain the comparison result without sacrificing any of their inputs. In other words, TEAM was correct, secure, and fair. In addition, the experimental results show that TEAM improves up to 50 times in terms of efficiency compared with previous methods under the same experimental settings.

Keywords: secure comparison, game theory, homomorphic encryption, threshold cryptography, trusted computing

收稿日期：2023−07−15；**修回日期：**2023−12−01

通信作者：肖阳，yangtomas7@gmail.com

基金项目：国家重点研发计划基金资助项目（No.2022YFB3102700）；国家自然科学基金资助项目（No.62202358, No.62072109, No.62376097, No.62102295, No.62202114）；中国博士后科学基金资助项目（No.2023TQ0258）

Foundation Items: The National Key Research and Development Program of China (No.2022YFB3102700), The National Natural Science Foundation of China (No.62202358, No.62072109, No.62376097, No.62102295, No.62202114), China Postdoctoral Science Foundation (No.2023TQ0258)

0　引言

安全两方比较是指在没有可信第三方，且 2 个参与方均不透露各自输入数据 x 和 y 的情况下，输出 x 和 y 的大小关系[1]。形式上，2 个参与方 Alice 和 Bob 分别以 x 和 y 作为输入，以不泄露各自输入的方式共同执行比较函数 $f(x,y)$ 并期望分别获得比较结果 u_a 和 u_b，即 $(u_a,u_b)\leftarrow f(x,y)$。

安全两方比较源自姚期智院士于 1982 年提出的百万富翁问题[1]，目前已成为安全多方计算领域中的关键技术。百万富翁问题即 2 个百万富翁在不透露双方具体财富的情况下比较谁更富有。姚期智院士[1]提出百万富翁问题的初始解决方案，该方案由于需要进行指数次数的解密和验证操作，因此时间和空间复杂度都很高，实用性差。为提高安全两方比较协议的实用性，姚期智院士[2]于 1986 年提出一种基于混淆电路的安全两方计算方案。

此后，研究者们一直致力于设计更加高效的安全两方比较方案。Ioannidis 等[3]通过并行调用 n 轮 2 选 1 不经意传输协议来解决安全两方比较问题，其运行效率较指数级的运算有所提升。Li 等[4]使用集合求交集判断元素大小的方法并结合对称加密方法实现安全两方比较。该方法使用对称加密提升协议效率，但不适用于数据规模较大的情况。Damgard 等[5]通过 Damgard-Geisler-Kroigard 同态加密方案实现整数上的安全两方比较。相较于其他协议，该方案具有更高的运行效率，但需要大约 150 s 的初始化时间。

近年来，安全两方比较已被广泛应用于隐私保护的拍卖、机器学习和外包计算等领域[6-10]。Damle 等[6]采用半受信任的第三方代理和以太坊提出一种可验证的安全两方比较方案，由此实现隐私保护的组合拍卖协议。Zhou 等[7]提出一种修正线性单元（ReLU, rectified linear unit）函数来判断输入与 0 的大小关系，使隐私保护机器学习的效率提升近一个数量级。Liu 等[8]基于门限 Paillier 密码方案提出一套在自然数上的隐私保护外包计算方法。其包含的安全比较协议（SLT, secure less than protocol）能判断 2 个密文的大小关系。郭奕旻等[9]基于 Paillier 密码系统并结合几何理论以及安全两方比较思想设计出一种高效的有理区间保密计算协议。Zhao 等[10]设计一种密文上的安全两方比较协议，并据此构造安全排序协议，解决分布式粒子群优化中选择算子的隐私泄露问题。

尽管研究者们在提升安全两方比较协议性能和应用安全两方比较协议上做出了诸多努力，但都忽视了先获取比较结果的参与方有可能提前退出协议，从而破坏协议的公平性。安全多方计算的公平性是指在协议执行完毕后，所有参与方要么都获得预期的输出，要么都未获得预期的输出。现有的安全两方比较协议[11-14]通常是让参与比较两方中的一方（如 Alice）先获得比较结果 u_a，再由 Alice 通知另一方（如 Bob）比较结果 u_b。若 Alice 诚实，Alice 设置 $u_\mathrm{b}=u_\mathrm{a}$，并将 u_b 发送给 Bob。在这种情况下，Alice 和 Bob 获得相同的比较结果。若 Alice 提前退出协议，则 Bob 将不能获得预期的比较结果。因此，目前的安全两方比较协议难以解决下述问题。

Alice 和 Bob 这 2 个富翁都看中一处房产，但房产商规定资产多的人拥有最终购买权，且没有富翁愿意向其他人透露其总资产。直观上，采用现有的安全两方比较协议可以解决该问题。但是由于先获知比较结果的富翁（如 Alice）可以退出协议。在这种情况下，富翁 Bob 无法知道谁拥有最终购买权。

近年来，研究者们已注意到安全两方比较中的公平性问题，并开展广泛的研究。理性安全多方计算（RSMPC, rational secure multi-party computation）采用博弈论的思想探讨安全多方计算的公平性问题，使安全两方计算协议的公平性成为可能[15]。RSMPC 假定参与方是理性的，即参与方在协议执行过程中使用各自的策略追求各自利益（效用函数）最大化。协议的目标是驱使每个参与方都没有动机偏离原本协议（如中途退出等）的动机，就博弈而言，两方博弈达到纳什均衡；就协议而言，没有参与方有偏离协议的动机。只要协议设计正确，则保证要么参与方都获得预期的结果，要么都没获得预期的结果。

受理性安全多方计算的启发，本文研究一种理性安全的公平两方比较方法，实现安全两方比较协议的公平性。形式上，该方法将保证参与比较的两方 Alice 和 Bob 以私有数据 x 和 y 作为输入，执行安全两方比较协议 $(u_\mathrm{a},u_\mathrm{b})\leftarrow f(x,y)$ 后，理性参与方 Alice 和 Bob 都能获得比较结果，即满足公平性。本文的贡献可归纳为如下 3 个方面。

1) 安全两方比较。本文利用门限 Paillier 密码系统密钥的可拆分性，提出一种新型安全两方比较协议，该协议允许两方在不泄露各自输入的情况下

执行比较操作。

2) 公平的安全两方比较。本文严格分析并给出所提安全两方比较协议在理性参与方假设下两方比较的博弈均衡点。在完全信息博弈下，所提安全比较协议的均衡点为每个参与方均获得比较结果，即所提出的安全两方比较协议是公平的。

3) 安全且高效。理论分析表明本文提出的安全两方比较协议满足选择明文攻击（CPA, chosen-plaintext attack）安全。此外，相比于基于理性秘密分享的安全两方比较协议，本文提出的理性安全两方比较通信轮数固定且不需要诚实的第三方。同等实验条件下，本文协议的计算速度是同类方法的 50 倍。

1 相关工作

依据安全两方比较协议采用的底层技术，本节简要回顾基于混淆电路的安全两方比较方法、基于同态加密的安全两方比较方法以及基于秘密分享的安全两方比较方法。

1) 基于混淆电路的安全两方比较方法

该方法将安全两方比较问题转化为混淆电路的形式解决。ObliVM[11]通过编译一种 ObliVM-lang 的类 Java 语言，实现内置的高效不经意随机访问方案，提升安全两方计算的效率。ABY[12]是一种半诚实模型下基于 C++库的混合协议框架，通过不同协议之间相互转化的机制，开发者可以实现对计算效率的细粒度控制。ObliVM 和 ABY 都提供基于混淆电路（经 free xor 优化[13]）的通用安全两方计算解决方案，能支持安全两方比较。Canetti 等[14]专注于当有恶意参与方存在时安全两方比较的正确性，通过分割选择防止恶意行为。但该方法要求构造大量电路，计算和空间复杂度较高，实用性较差。

2) 基于同态加密的安全两方比较方法

由于同态加密对密文的运算能够映射到明文上，使其能够在保护隐私数据的同时完成安全两方计算任务，所以该方法十分契合安全两方比较的需求。Lin 等[16]结合 ElGamal 同态加密方案和字符串集合求交集的大小比较方法，通过比较两方的 0 编码和 1 编码并用 ElGamal 同态加密方案保证 1 编码的保密性。Liu 等[17]提出两方和多方安全比较解决方案，通过将财富值转化为向量表示并结合 Paillier 密码系统的同态性解决安全两方比较问题。李顺东等[18]提出半诚实模型和恶意模型下的最大（小）值比较协议，通过 ElGamal 同态加密方案、向量化表示财富值和零知识证明等方法实现两方或多方比较。Zhao 等[19]改进 Liu 等[8]的工作，提出整数上的安全外包计算方法 SOCI，其安全比较协议（SCMP, secure comparison protocol）支持整数上的密文比较。

3) 基于秘密分享的安全两方比较方法

Veugen 等[20]总结现有基于秘密分享的安全两方比较协议，如 GSV07。该协议通过秘密分享的随机比特实现安全两方比较。文献[17]将财富值向量化，使用秘密分享的方法替代 Paillier 同态加密保护数据隐私，降低计算复杂度，实现安全多方比较。Damgard 等[21]提出一种将某一特定秘密的多项式共享转化为比特共享的方法，通过调用秘密分享方案的乘法协议实现高效安全两方比较。

Groce 等[15]重新考虑 RSMPC 中的公平性问题，提出对于任意安全两方计算协议在不完全信息博弈下都能实现公平性。Halpern 等[22]构造出(3,3)理性秘密分享方案解决了安全两方计算中的公平性问题，但该方案存在需要在线秘密分发者，执行效率低等不足。Maitra 等[23]提出基于理性秘密分享的两方安全比较协议，该协议的秘密分发者是离线的，实现了完全信息博弈下的严格纳什均衡。

相比于现有的安全两方比较协议，本文提出的理性安全的公平两方比较（TEAM, rational-security and fair two-party comparison）协议采用门限 Paillier 密码系统实现安全的两方比较，在理性参与方的假设下，博弈分析显示 TEAM 可以实现公平的两方安全比较。表 1 给出了安全两方比较协议的比较。

表 1 安全两方比较协议的比较

协议	底层技术	公平的比较	效率
ObliVM[11]	混淆电路	否	中
ABY[12]	混淆电路	否	高
GSV07[20]	秘密分享	否	中
semiSMC[18]	同态加密	否	低
TEAM	同态加密	是	高

2 预备知识

2.1 门限 Paillier 密码系统

本文采用(2,2)门限 Paillier 密码系统，其包含密钥生成、加密、解密、密钥拆分、部分解密和门限解密等概率算法。(2,2)门限 Paillier 密码系统与传统 Paillier 密码系统[24]的主要区别在于前者将 Paillier

密码系统的私钥拆分成 2 个部分私钥。

密钥生成（KeyGen, key generation）。令 k 为安全参数，且 p 和 q 为大素数，满足 $\langle p\rangle=\langle q\rangle=k$，其中，$\langle x\rangle$ 为 x 的二进制位数。随后计算 $N=pq$，$\lambda=\dfrac{(p-1)(q-1)}{2}$ 和 $\mu=\lambda^{-1}\bmod N$。输出公钥 $\mathrm{pk}=(N,g)$ 和私钥 $\mathrm{sk}=\lambda$，其中生成元 $g=N+1$。

加密（Enc, encryption）。输入明文消息 $m\in\mathbb{Z}_N$，输出其对应密文 $[m]$。具体加密算法如下

$$[m]=\mathrm{Enc}(\mathrm{pk},m)=g^m r^N \bmod N^2 \tag{1}$$

其中，r 从 $\mathbb{Z}_N^*$ 中随机选取。

解密（Dec, decryption）。输入加密后的明文消息 $[m]$，通过私钥 $\mathrm{sk}=\lambda$ 解密后输出对应明文 m，具体解密算法如下

$$m=\mathrm{Dec}(\mathrm{sk},[m])=L([m]^\lambda \bmod N^2)\mu \bmod N \tag{2}$$

其中，$L(x)=\dfrac{x-1}{N}$。

密钥拆分（KeyS, private key splitting）。输入私钥 sk，输出拆分后的私钥 $\mathrm{sk}_1=\lambda_1$ 和 $\mathrm{sk}_2=\lambda_2$，满足 $\lambda_1+\lambda_2\equiv 0\bmod\lambda$，且 $\lambda_1+\lambda_2\equiv 1\bmod N$。由中国剩余定理[25]可以计算出满足 $\delta\equiv 0\bmod\lambda$，且 $\delta\equiv 1\bmod N$ 的 $\delta=\lambda_1+\lambda_2=\lambda\mu\bmod(\lambda N)$。此时，拆分后的私钥 $\mathrm{sk}_1=\lambda_1$ 为 σ bit 的随机数，$\mathrm{sk}_2=\lambda_2=\lambda\mu+\eta\lambda N-\lambda_1$，其中 σ 为安全参数，η 为非负整数。

部分解密（PDec, partial decryption）。输入密文消息 $[m]$ 和部分私钥 sk_i（$i\in\{1,2\}$），输出部分解密的结果 M_i，具体部分解密算法如下

$$M_i=\mathrm{PDec}([m],\mathrm{sk}_i)=[m]^{\lambda_i} \bmod N^2 \tag{3}$$

门限解密（TDec, threshold decryption）。输入一对部分解密的结果 M_1 和 M_2，输出其对应的明文 m。具体门限解密算法如下

$$m=\mathrm{TDec}(M_1,M_2)=L(M_1M_2 \bmod N^2) \tag{4}$$

门限 Paillier 密码系统的加法同态性和标量乘法同态性表现如下。

加法同态性：$\mathrm{Dec}(\mathrm{sk},[m_1+m_2 \bmod N])=\mathrm{Dec}(\mathrm{sk},[m_1][m_2])$。

标量乘法同态性：$\mathrm{Dec}(\mathrm{sk},[cm \bmod N])=\mathrm{Dec}(\mathrm{sk},[m]^c)$，其中，$c\in\mathbb{Z}_N$。

2.2　效用函数

对于理性参与方，效用函数用于描述其参与协议的动机。令 $\Gamma=\left(\{P_i\}_{i=1}^2,\{A_i\}_{i=1}^2,\{U_i\}_{i=1}^2\right)$ 表示 2 个参与方之间的博弈，其中，$\{P_i\}_{i=1}^2$ 代表参与方的集合；$\{A_i\}_{i=1}^2$ 代表参与方策略的集合，A_i 代表参与方 P_i 可能采取的策略集合；$\{U_i\}_{i=1}^2$ 代表参与方效用函数的集合，其中 $U_i:A_1\times A_2\to R$。令 $A\overset{\text{def}}{=}A_1\times A_2$，策略元组 $\boldsymbol{a}=(a_1,a_2)\in A$ 称为一个博弈结果。P_i 的效用函数 U_i 定义了参与方 P_i 对某个策略元组的偏爱程度。例如，$U_i(\boldsymbol{a})>U_i(\boldsymbol{a}')$ 表示 P_i 相对策略元组 $\boldsymbol{a}'$ 更倾向策略元组 $\boldsymbol{a}$。

效用函数的定义通常满足自私性和排他性。在策略元组 $\boldsymbol{a}=(a_1,a_2)$ 中，a_i 代表参与方 P_i 的策略（$i\in\{1,2\}$）。策略元组 $\boldsymbol{a}'=(a_i',\boldsymbol{a}\setminus\{a_i\})$ 对比策略元组 $\boldsymbol{a}$ 唯一的不同是参与方 P_i 采取了不同的策略 a_i'。令 $\chi_i(\boldsymbol{a})=1$（$\chi_i(\boldsymbol{a})=0$）代表策略元组为 $\boldsymbol{a}$ 时，参与方 P_i 获得（未获得）最终比较结果。其中，$\mathrm{num}(\boldsymbol{a})=\sum_{i=1}^2\chi_i(\boldsymbol{a})$ 代表获得比较结果的参与方个数。形式上，效用函数自私性和排他性的定义如下。

自私性：如果 $\chi_i(\boldsymbol{a})>\chi_i(\boldsymbol{a}')$ 成立，则有 $U_i(\boldsymbol{a})>U_i(\boldsymbol{a}')$。

排他性：如果 $\chi_i(\boldsymbol{a})=\chi_i(\boldsymbol{a}')$ 成立，且有 $\mathrm{num}(\boldsymbol{a})<\mathrm{num}(\boldsymbol{a}')$，则 $U_i(\boldsymbol{a})>U_i(\boldsymbol{a}')$。

值得注意的是，当仅考虑自私性和排他性时，理性参与方都会选择不发送消息给对方，导致两者都不会获得最终的比较结果（此时也满足公平性规定的双方都不获得结果）。定义效用函数时考虑声誉可以解决该问题[26]。在声誉系统中，所有实体都对应一个评估该实体可靠性的声誉值。声誉系统在电子商务等领域有广泛的应用。因此，如果一家公司想要增加与他人合作的机会，就应该在与他人互动时尽力建立良好的声誉。形式上，令 $\tau_i(\boldsymbol{a})$ 表示策略元组 $\boldsymbol{a}$ 下参与方 P_i 的声誉值。具体地，若参与方 P_i 在 TEAM 协议执行时按照协议要求发送相应消息给对方，则 $\tau_i(\boldsymbol{a})=1$，否则 $\tau_i(\boldsymbol{a})=-1$。

2.3　严格纳什均衡

定义 1　在由参与方的集合 $\{P_i\}_{i=1}^2$、参与方策略的集合 $\{A_i\}_{i=1}^2$ 以及效用函数集合 $\{U_i\}_{i=1}^2$ 组成的两方博弈 $\Gamma=\left(\{P_i\}_{i=1}^2,\{A_i\}_{i=1}^2,\{U_i\}_{i=1}^2\right)$ 中，如果对于任

何参与方 P_i 的策略 $a_i' \in A_i$，以及其他参与方的策略 a_{-i}，一个具体的策略元组 $\boldsymbol{a}$ 满足

$$U_i(a_i', a_{-i}) < U_i(\boldsymbol{a}) \tag{5}$$

则称策略元组 $\boldsymbol{a}$ 为严格纳什均衡。

3 理性安全的公平两方比较协议

本节首先介绍 TEAM 的系统模型和威胁模型，然后给出 TEAM 的详细构造。

3.1 系统模型

如图 1 所示，TEAM 包括 2 个参与方 Alice 和 Bob，他们分别有私有数据 x 和 y。为保护参与方的私有数据，Alice 采用(2,2)门限 Paillier 密码系统设置密钥参数，Bob 采用传统 Paillier 密码系统生成密钥参数。

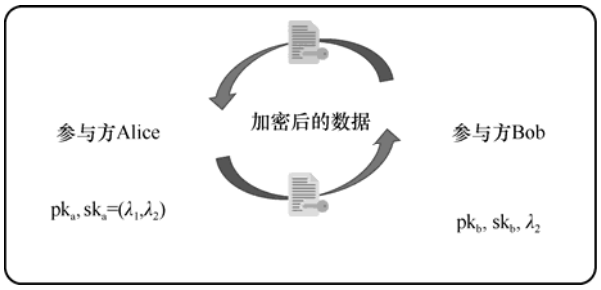

图 1 系统模型

1) 参与方 Alice。Alice 首先调用密钥生成算法 KeyGen 产生一个公私钥对 $(\mathrm{pk_a}, \mathrm{sk_a})$，其中公钥 $\mathrm{pk_a} = (N_\mathrm{a}, g_\mathrm{a})$。此外，Alice 调用 KeyS 将私钥 $\mathrm{sk_a}$ 拆分成 2 个部分私钥 λ_1 和 λ_2。

2) 参与方 Bob。Bob 调用密钥生成算法 KeyGen 产生一个 Paillier 密码系统的公私钥对 $(\mathrm{pk_b}, \mathrm{sk_b})$，其中 $\mathrm{pk_b} = (N_\mathrm{b}, g_\mathrm{b})$。

3.2 威胁模型

受理性安全的计算协议威胁模型的启发，本文也采用 fail-stop 理性安全模型[15]。fail-stop 理性安全模型假定参与方理性并遵守协议，同时在执行协议时不会改变其输入，但可以在任何时候选择退出协议。具体地，参与方 Alice 和 Bob 均为理性参与方，两者在执行安全两方比较协议时会遵守协议，但可以在任意步骤退出。

3.3 详细构造

TEAM 的详细构造过程如图 2 所示。Alice 以私有数据 x 作为输入，并拥有 $(\mathrm{pk_a}, \mathrm{sk_a})$ 和 $\mathrm{sk_a}$ 拆分后的部分私钥 $(\lambda_1, \lambda_2) \leftarrow \mathrm{KeyS}(\mathrm{sk_a})$。Bob 以私有数据 y 作为输入，拥有 $(\mathrm{pk_b}, \mathrm{sk_b})$。本文假定 $x, y \in [-2^\ell, 2^\ell]$，其中，$\ell$ 是一个整数且满足 $2^\ell \ll N$，如 $\ell = 32$。

TEAM 的 5 个步骤详细流程如下。

1) Bob 加密 y 成 $[y]_{\mathrm{pk_b}} = \mathrm{Enc}(\mathrm{pk_b}, y)$，并将加密结果 $[y]_{\mathrm{pk_b}}$ 和 $\mathrm{pk_b}$ 发送给 Alice。

2) Alice 加密 x 成 $[x]_{\mathrm{pk_b}} = \mathrm{Enc}(\mathrm{pk_b}, x)$。随后，Alice 随机选择 $s \in \{0,1\}$，并通过如下计算得到 D

$$D = \begin{cases} ([x]_{\mathrm{pk_b}} [y]_{\mathrm{pk_b}}^{N_\mathrm{b}-1})^{r_1} [r_1 + r_2]_{\mathrm{pk_b}}, & s = 0 \\ ([y]_{\mathrm{pk_b}} [x]_{\mathrm{pk_b}}^{N_\mathrm{b}-1})^{r_1} [r_2]_{\mathrm{pk_b}}, & s = 1 \end{cases} \tag{6}$$

其中，r_1 从集合 $[2^{\sigma-1}, 2^\sigma - 1]$ 中随机选取，r_2 从集合 $\left[\frac{N_\mathrm{b}}{2} - r_1 + 1, \frac{N_\mathrm{b}}{2}\right]$ 中随机选取（σ 为安全参数，且满足 $2^\ell \ll 2^\sigma \ll \frac{N_\mathrm{b}}{2}$），即随机选取的 r_1 和 r_2 满足 $r_2 \leqslant \frac{N_\mathrm{b}}{2}$，且 $r_1 + r_2 > \frac{N_\mathrm{b}}{2}$。随后，Alice 加密 s 得到

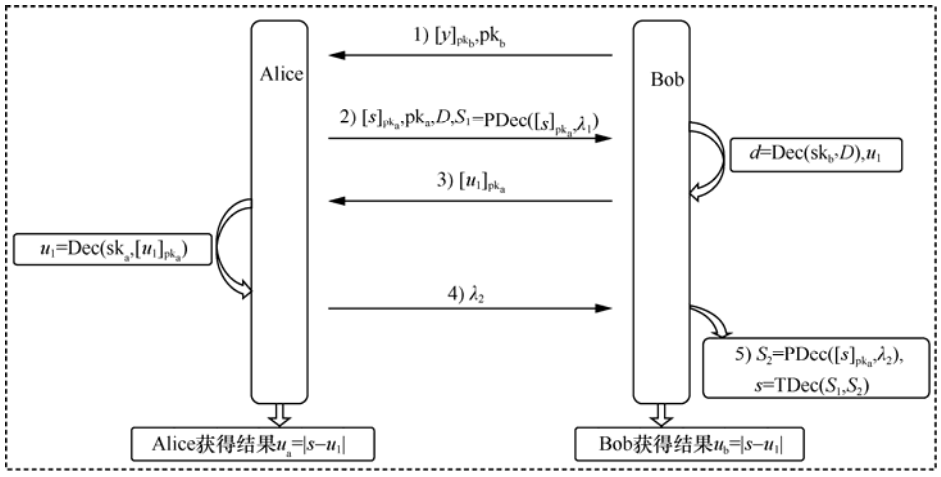

图 2 TEAM 的详细构造过程

$[s]_{\mathrm{pk_a}}=\mathrm{Enc}(\mathrm{pk_a},s)$，并调用部分解密算法部分解密$[s]_{\mathrm{pk_a}}$得到$S_1=\mathrm{PDec}([s]_{\mathrm{pk_a}},\lambda_1)$。最后，Alice 将$[s]_{\mathrm{pk_a}}$、$\mathrm{pk_a}$、$D$和$S_1$发送给 Bob。

3) Bob 收到$[s]_{\mathrm{pk_a}}$、D和S_1后，首先解密D获得$d=\mathrm{Dec}(\mathrm{sk_b},D)$。若$d>\frac{N_\mathrm{b}}{2}$，记$u_1=0$，否则记$u_1=1$。随后，Bob 加密$u_1$成$[u_1]_{\mathrm{pk_a}}=\mathrm{Enc}(\mathrm{pk_a},u_1)$。最后，Bob 将$[u_1]_{\mathrm{pk_a}}$发送给 Alice。

4) Alice 收到$[u_1]_{\mathrm{pk_a}}$后，首先解密$[u_1]_{\mathrm{pk_a}}$获得u_1，并得到比较结果$u_\mathrm{a}=|s-u_1|$。其中，$|s-u_1|$代表$s-u_1$的绝对值。随后，Alice 将λ_2发送给 Bob。

5) Bob 获得λ_2后，部分解密$[s]_{\mathrm{pk_a}}$获得$S_2=\mathrm{PDec}([s]_{\mathrm{pk_a}},\lambda_2)$，以及$s=\mathrm{TDec}(S_1,S_2)$。最后，Bob 得到比较结果$u_\mathrm{b}=|s-u_1|$。

4　理论分析

本节将证明 TEAM 的正确性、公平性和安全性。特别地，在安全性证明中首先介绍选择明文攻击安全性定义，并证明 TEAM 第 2)步中使用的加密方案$r_1(x-y+1)+r_2$或$r_1(y-x)+r_2$满足 CPA 安全性（为方便叙述，令$m=x-y+1,y-x$）。随后通过模拟范式证明 TEAM 的安全性。

4.1　正确性分析

声称 1　如果 Alice 和 Bob 都遵循协议，则 Alice 总能获得正确的比较结果。

证明　**情形 1**：$s=0$。输入数据$x,y\in[-2^\ell,2^\ell]$，r_1从$[2^{\sigma-1},2^\sigma-1]$中随机选择，即$r_1\in[2^{\sigma-1},2^\sigma-1]$。随机数$r_2$从$\left[\frac{N_\mathrm{b}}{2}-r_1+1,\frac{N_\mathrm{b}}{2}\right]$中随机选择。由此，当$r_1=2^\sigma-1$，$r_2=\frac{N_\mathrm{b}}{2}$，且$x-y+1=1+2^{\ell+1}$时，$(2^\sigma-1)(1+2^{\ell+1})+\frac{N_\mathrm{b}}{2}$是$d=r_1(x-y+1)+r_2$的最大值。当$r_1=2^\sigma-1$，$r_2=\frac{N_\mathrm{b}}{2}-r_1+1$，且$x-y+1=1-2^{\ell+1}$时，$2^{\ell+1}-2^{\sigma+\ell+1}+1+\frac{N_\mathrm{b}}{2}$是$d$的最小值。综上，$d$的范围为

$$d\in\left[\frac{N_\mathrm{b}}{2}+2^{\ell+1}-2^{\sigma+\ell+1}+1,\frac{N_\mathrm{b}}{2}+(2^\sigma-1)(1+2^{\ell+1})\right] \quad (7)$$

为直观展示，表 2 给出 Alice 获得的结果与真实结果的关系。具体地，由d的范围、随机数r_1和r_2的范围$\left(r_1+r_2>\frac{N_\mathrm{b}}{2},r_2\leqslant\frac{N_\mathrm{b}}{2}\right)$可得，只要$x\geqslant y$，此时$d=r_1(x-y+1)+r_2>\frac{N_\mathrm{b}}{2}$；只要$x<y$，此时$d=r_1(x-y+1)+r_2\leqslant\frac{N_\mathrm{b}}{2}$。由此，当$d>\frac{N_\mathrm{b}}{2}$时，$x\geqslant y$；否则当$d\leqslant\frac{N_\mathrm{b}}{2}$时，$x<y$。如表 2 所示。其中，$s$和$u_1$表示计算 Alice 获得最终结果所需中间值。

表 2　$s=0$，Alice 获得结果与真实结果比较

x 和 y 的大小关系	u_1	Alice 获得结果	真实结果
$x\geqslant y$	0	$\lvert s-u_1\rvert=0$	0
$x<y$	1	$\lvert s-u_1\rvert=1$	1

1) 当$x\geqslant y$时，易知$d>\frac{N_\mathrm{b}}{2}$，所以$u_1=0$。此时$u_\mathrm{a}=|s-u_1|=|0-0|=0$。由 TEAM 的输出可得$u_\mathrm{a}=0$代表$x\geqslant y$。因此，Alice 能获得正确的比较结果。

2) 当$x<y$时，易知$d\leqslant\frac{N_\mathrm{b}}{2}$，所以$u_1=0$。此时$u_\mathrm{a}=|s-u_1|=|0-1|=1$。由 TEAM 的输出可得$u_\mathrm{a}=1$代表$x<y$。因此，Alice 能获得正确的比较结果。

情形 2：$s=1$。Alice 获得结果与真实结果比较如表 3 所示。

表 3　$s=1$，Alice 获得结果与真实结果比较

x 和 y 的大小关系	u_1	Alice 获得结果	真实结果
$x\geqslant y$	1	$\lvert s-u_1\rvert=0$	0
$x<y$	0	$\lvert s-u_1\rvert=1$	1

1) 当$x\geqslant y$时，易知$d=r_1(y-x)+r_2\leqslant\frac{N_\mathrm{b}}{2}$，所以$u_1=1$。此时$u_\mathrm{a}=|s-u_1|=|1-1|=0$。由 TEAM 的输出可得$u_\mathrm{a}=0$代表$x<y$。因此，Alice 能获得正确的比较结果。

2) 当$x<y$时，易知$d=r_1(y-x)+r_2>\frac{N_\mathrm{b}}{2}$，所以$u_1=0$。此时$u_\mathrm{a}=|s-u_1|=|1-0|=1$。由 TEAM 的输出可得$u_\mathrm{a}=1$代表$x<y$。因此，Alice 能获得正确的比较结果。

综上所述，Alice 总能获得正确的比较结果。

证毕。

声称 2 如果 Alice 和 Bob 都遵循协议，则 Bob 总能获得正确的比较结果。

证明 Bob 通过 $u_b=|s-u_1|$ 得到最终比较结果。如图 2 所示，协议执行过程中 Bob 通过门限解密算法 $\mathrm{TDec}(S_1,S_2)$ 得到 s。由门限解密算法的正确性保证 Alice 和 Bob 使用相同的 s。Alice 通过解密算法 $\mathrm{Dec}(\mathrm{sk}_a,[u_1]_{\mathrm{pk}_a})$ 得到 u_1。由解密算法的正确性保证 Alice 和 Bob 使用相同的 u_1。

综上，Bob 和 Alice 生成 u_b 和 u_a 所需 s 和 u_1 是相同的。由声称 1 可知，Alice 能获得正确的两方比较结果 $u_a=|s-u_1|$，所以 Bob 能获得正确的安全两方比较结果 $u_b=|s-u_1|$。证毕。

4.2 公平性分析

分析理性安全两方比较的公平性，首先要明确理性参与方 Alice 和 Bob 的策略。依据 3.3 节的详细构造和 3.2 节的 fail-stop 理性安全模型[15]，Alice 的策略是第 1)步和第 2)步是否选择发送相应消息给 Bob。Bob 的策略是第 2)和第 4)步是否选择发送相应消息给 Alice。形式上，使用 S_i^j 和 $\overline{S}_i^j$ ($j\in\{1,2,3,4\}$, $i\in\{1,2\}$)代表参与方 P_i 在第 j)步发送和不发送相关消息给另一参与方。其中，参与方 P_1 和 P_2 分别代表 Alice 和 Bob。

本文使用和文献[26]相同的效用函数定义

$$U_i(\boldsymbol{a})=\rho_1\tau_i(\boldsymbol{a})+\rho_2\chi_i(\boldsymbol{a})+\rho_3\frac{1}{\mathrm{num}(\boldsymbol{a}+1)} \tag{8}$$

当策略元组为 $\boldsymbol{a}$ 时，$\chi_i(\boldsymbol{a})=1$（$\chi_i(\boldsymbol{a})=0$）代表参与方 P_i 获得（未获得）最终比较结果，$\tau_i(\boldsymbol{a})=1$（$\tau_i(\boldsymbol{a})=-1$）代表参与方 P_i 发送（不发送）相关消息给另一方，$\mathrm{num}(\boldsymbol{a})$ 代表获得最终比较结果的参与方个数。特别地，$\mathrm{num}(\boldsymbol{a}+1)$ 用于防止分母为 0 的情况发生。ρ_1、ρ_2 和 ρ_3 分别代表效用函数中声誉，自私性和排他性的权重，满足 $\rho_1>\rho_2>\rho_3$，表示理性参与方首先希望获得良好的声誉，然后希望得知比较结果，并希望对方不知道比较结果。

声称 3 当效用函数为式(8)时，TEAM 满足公平性。

证明 要证明 TEAM 满足公平性，即证明策略元组 $(S_1^1S_1^3,S_2^2S_2^4)$ 是博弈过程中的严格纳什均衡点。具体地，Alice 和 Bob 选择不同策略，由效用函数产生的不同博弈结果（效用矩阵）如表 4 所示。其中，$S_i^j(i\in\{1,2\},j\in\{1,2,3,4\})$ 表示参与方 P_i 向另一参与方发送第 j)步消息。$\overline{S}_i^j(i\in\{1,2\},j\in\{1,2,3,4\})$ 表示参与方 P_i 拒绝向另一参与方发送第 j)步消息。

1) $\boldsymbol{a}^1=(\overline{S}_1^1S_1^3,a_2)\cup(\overline{S}_1^1\overline{S}_1^3,a_2)$。Alice 选择不发送第 1)步消息给 Bob。此时，Alice 不论是否发送第 3)步消息以及任意 Bob 的策略 a_2，博弈双方都不能获得最终比较结果。此时，$\tau_1(\boldsymbol{a}^1)=-1$，$\tau_2(\boldsymbol{a}^1)\leqslant 1$，$\chi_1(\boldsymbol{a}^1)=\chi_2(\boldsymbol{a}^1)=0$，且 $\mathrm{num}(\boldsymbol{a}^1)=0$。所以 Alice 和 Bob 的效用值分别为 $U_1(\boldsymbol{a}^1)=-\rho_1+\rho_3$，$U_2(\boldsymbol{a}^1)\leqslant\rho_1+\rho_3$。

2) $\boldsymbol{a}^2=(a_1,\overline{S}_2^2S_2^4)\cup(a_1\overline{S}_2^2\overline{S}_2^4)$。Bob 选择不发送第 2)步消息给 Bob。此时，Bob 不论是否发送第 4)步消息以及任意 Alice 的策略 a_1，博弈双方都不能获得最终比较结果。同理，Alice 和 Bob 的效用值分别为 $U_1(\boldsymbol{a}^2)\leqslant\rho_1+\rho_3$，$U_2(\boldsymbol{a}^2)=-\rho_1+\rho_3$。

3) $\boldsymbol{a}^3=(S_1^1S_1^3,S_2^2S_2^4)$。Alice 和 Bob 都遵循协议，博弈双方都能获得最终比较结果。此时，$\tau_1(\boldsymbol{a}^3)=\tau_2(\boldsymbol{a}^3)=1$，$\chi_1(\boldsymbol{a}^3)=\chi_2(\boldsymbol{a}^3)=1$，并且 $\mathrm{num}(\boldsymbol{a}^3)=2$。所以 Alice 和 Bob 的效用值分别为 $U_1(\boldsymbol{a}^3)=\rho_1+\rho_2+\frac{\rho_3}{3}$，$U_2(\boldsymbol{a}^3)=\rho_1+\rho_2+\frac{\rho_3}{3}$。

4) $\boldsymbol{a}^4=(S_1^1S_1^3,S_2^2\overline{S}_2^4)$。Alice 遵循协议，Bob 不发送第 4)步消息。最终，Bob 能获得最终比较结果，Alice 不能。此时，$\tau_1(\boldsymbol{a}^4)=1$，$\tau_2(\boldsymbol{a}^4)=-1$，$\chi_1(\boldsymbol{a}^4)=0$，$\chi_2(\boldsymbol{a}^4)=1$，且 $\mathrm{num}(\boldsymbol{a}^4)=1$。所以 Alice

表 4 效用矩阵

Alice(P_1)	Bob(P_2)= $S_2^2S_2^4$	Bob(P_2)= $S_2^2\overline{S}_2^4$	Bob(P_2)= $\overline{S}_2^2S_2^4$	Bob(P_2)= $\overline{S}_2^2\overline{S}_2^4$
$S_1^1S_1^3$	$\left(\rho_1+\rho_2+\frac{\rho_3}{3},\rho_1+\rho_2+\frac{\rho_3}{3}\right)$	$\left(\rho_1+\frac{\rho_3}{2},-\rho_1+\rho_2+\frac{\rho_3}{2}\right)$	$(\rho_1+\rho_3,-\rho_1+\rho_3)$	$(\rho_1+\rho_3,-\rho_1+\rho_3)$
$S_1^1\overline{S}_1^3$	$\left(-\rho_1+\rho_2+\frac{\rho_3}{2},\rho_1+\frac{\rho_3}{2}\right)$	$(-\rho_1+\rho_3,-\rho_1+\rho_3)$	$(-\rho_1+\rho_3,-\rho_1+\rho_3)$	$(-\rho_1+\rho_3,-\rho_1+\rho_3)$
$\overline{S}_1^1S_1^3$	$(-\rho_1+\rho_3,\rho_1+\rho_3)$	$(-\rho_1+\rho_3,-\rho_1+\rho_3)$	$(-\rho_1+\rho_3,-\rho_1+\rho_3)$	$(-\rho_1+\rho_3,-\rho_1+\rho_3)$
$\overline{S}_1^1\overline{S}_1^3$	$(-\rho_1+\rho_3,\rho_1+\rho_3)$	$(-\rho_1+\rho_3,-\rho_1+\rho_3)$	$(-\rho_1+\rho_3,-\rho_1+\rho_3)$	$(-\rho_1+\rho_3,-\rho_1+\rho_3)$

和 Bob 的效用值分别为 $U_1(\boldsymbol{a}^4)=\rho_1+\frac{\rho_3}{2}$，$U_2(\boldsymbol{a}^4)=-\rho_1+\rho_2+\frac{\rho_3}{2}$。

5) $\boldsymbol{a}^5=(S_1^1\overline{S}_1^3,S_2^2S_2^4)$。Bob 遵循协议，Alice 不发送第 3)步消息。最终，Alice 能获得最终比较结果，Bob 不能。同理，Alice 和 Bob 的效用值分别为 $U_1(\boldsymbol{a}^5)=-\rho_1+\rho_2+\frac{\rho_3}{2}$，$U_2(\boldsymbol{a}^5)=\rho_1+\frac{\rho_3}{2}$。

6) $\boldsymbol{a}^6=(S_1^1\overline{S}_1^3,S_2^2\overline{S}_2^4)$。Alice 和 Bob 分别不发送第 3)步和第 4)步消息。博弈双方都不能获得最终比较结果。此时，$\tau_1(\boldsymbol{a}^6)=\tau_2(\boldsymbol{a}^6)=-1$，$\chi_1(\boldsymbol{a}^6)=\chi_2(\boldsymbol{a}^6)=0$，且 $\text{num}(\boldsymbol{a}^6)=0$。所以 Alice 和 Bob 的效用值分别为 $U_1(\boldsymbol{a}^6)=-\rho_1+\rho_3$，$U_2(\boldsymbol{a}^6)=-\rho_1+\rho_3$。

综上，如表 4 所示，由效用函数定义可知 $\rho_1>\rho_2>\rho_3$。所以，$\forall i\in\{1,2\},\forall j\in\{1,2,3,4,5,6\}$，策略元组 $\boldsymbol{a}^3=(S_1^1S_1^3,S_2^2S_2^4)$ 满足

$$U_i(\boldsymbol{a}^j)\leqslant U_i(\boldsymbol{a}^3) \tag{9}$$

由定义 1 可知，策略元组 $\boldsymbol{a}^3=(S_1^1S_1^3,S_2^2S_2^4)$ 是严格纳什均衡。即 Alice 和 Bob 都能获取到最终比较结果，满足公平性。证毕。

4.3 CPA 安全性

CPA 安全通常使用计算上不可区分性实验来描述[27]，在实验中共有 2 个角色：敌手 $\mathcal{A}$ 攻击系统，挑战者 $\mathcal{C}$ 对敌手的行为进行反馈。实验 $\text{PubK}_{\mathcal{A},r_1m+r_2}^{\text{CPA}}(\sigma,\kappa)$ 具体过程如下。

1) 敌手 $\mathcal{A}$ 随机选择 2 个消息 m_0 和 m_1 发送给挑战者 $\mathcal{C}$。

2) 挑战者 $\mathcal{C}$ 随机选择比特 $b\in\{0,1\}$，并生成随机数 r_1 和 r_2，计算 $r_1m_b+r_2$ 发送给敌手 $\mathcal{A}$。

3) 敌手 $\mathcal{A}$ 输出一个比特 $b'\in\{0,1\}$ 作为对 b 的猜测。

4) 若 $b=b'$，则实验结果为 1，即 $\text{PubK}_{\mathcal{A},r_1m+r_2}^{\text{CPA}}(\sigma,\kappa)=1$，代表着敌手 $\mathcal{A}$ 攻击成功；若 $b\neq b'$，则实验结果为 0，即 $\text{PubK}_{\mathcal{A},r_1m+r_2}^{\text{CPA}}(\sigma,\kappa)=0$，代表着敌手 $\mathcal{A}$ 攻击失败。

定义 2　若加密方案 r_1m+r_2 满足对于任意概率多项式时间敌手 $\mathcal{A}$，都存在一个关于 σ 和 κ 的可忽略函数 $\text{negl}(\sigma,\kappa)$，使以下不等式成立

$$\Pr\left[\text{Pubk}_{\mathcal{A},r_1m+r_2}^{\text{CPA}}(\sigma,\kappa)=1\right]\leqslant\frac{1}{2}+\text{negl}(\sigma,\kappa) \tag{10}$$

则说明加密方案 r_1m+r_2 是 CPA 安全的。

定理 1　对于任意 $m_0,m_1\in[-2^\ell,2^\ell]$，$r_{10},r_{11}\in[2^{\sigma-1},2^\sigma-1]$，以及 $r_{20},r_{21}\in[2^{\kappa-1},2^\kappa-1]$，满足 $r_{10}m_0+r_{20}$ 和 $r_{11}m_1+r_{21}$ 在计算上是不可区分的（例如，$\ell=64,\sigma=128,\kappa=512$）。形式上，挑战者 $\mathcal{C}$ 随机选取 $m_b\in[-2^\ell,2^\ell]$（$b\in\{0,1\}$），$r_1\in[2^{\sigma-1},2^\sigma-1]$ 和 $r_2\in[2^{\kappa-1},2^\kappa-1]$ 计算 $r_1m_b+r_2$。此时对于敌手 $\mathcal{A}$，通过 $r_1m_b+r_2$ 推测出 b'，使 $b'=b$（$b'\in\{0,1\}$）的概率满足

$$\Pr\left[b'=b|\ r_1m_b+r_2\right]\leqslant\frac{1}{2}+\text{negl}(\sigma,\kappa) \tag{11}$$

其中，$\text{negl}(\sigma,\kappa)$ 是关于 σ 和 κ 的可忽略函数。说明加密方案 r_1m+r_2 满足 CPA 安全。

证明　详见附录 1。

4.4 模拟范式

模拟范式是一种广泛接受的证明多方安全计算协议安全性的方法。其通过对比理想模型与现实情况下的多方安全计算协议来定义协议的安全性，若现实情况下协议泄露的信息不会多于理想模型下泄露的信息，则可以说明该协议是安全的。

假设参与方 Alice 拥有输入数据 x，参与方 Bob 拥有输入数据 y，双方通过安全两方计算协议 π 联合计算一个概率多项式时间函数 $f(x,y)=(f_1(x,y),f_2(x,y))$。在执行协议 π 的过程中，定义 Alice 和 Bob 双方获得的视图分别为 $\text{view}_1^\pi(x,y)=\left(x,r,m_1,\cdots,m_t\right)$ 和 $\text{view}_2^\pi(x,y)=(y,r',m_1',\cdots,m_t')$。其中，Alice 和 Bob 执行协议时收到的消息序列分别为 $(m_1,\cdots,m_t)$ 和 $(m_1',\cdots,m_t')$。Alice 和 Bob 执行协议时抛硬币得到的结果分别为 r 和 r'。最终，Alice 和 Bob 完成协议后得到的结果分别为 $\text{output}_1^\pi(x,y)$ 和 $\text{output}_2^\pi(x,y)$ [28]。

定义 3　对于特定函数 f，如果存在概率多项式时间算法 $\mathcal{S}_1$ 和 $\mathcal{S}_2$（一般称 $\mathcal{S}_1$ 和 $\mathcal{S}_2$ 为模拟器。）满足以下条件

$$\begin{cases}\left\{\left(\mathcal{S}_1\left(x,f_1(x,y)\right),f_2(x,y)\right)\right\}_{x,y}\overset{\text{c}}{\equiv}\\ \left\{\left(\text{view}_1^\pi(x,y),\ \text{output}_2^\pi(x,y)\right)\right\}_{x,y}\\ \left\{\left(\mathcal{S}_2\left(y,f_2(x,y)\right),f_1(x,y)\right)\right\}_{x,y}\overset{\text{c}}{\equiv}\\ \left\{\left(\text{view}_2^\pi(x,y),\ \text{output}_1^\pi(x,y)\right)\right\}_{x,y}\end{cases} \tag{12}$$

则说明协议 π 保密计算了函数 f。其中，$\overset{c}{\equiv}$ 代表计算上的不可区分性。

定理 2 TEAM 在 fail-stop 理性安全模型下是安全的。

证明 详见附录 2。

5 实验评估

本节实验对比 ObliVM[11]、ABY[12]、TEAM、GSV07[20]和 semiSMC[18]在实现安全两方比较协议的性能，并测试不同公钥长度 N 和明文长度 ℓ 下 TEAM 的运行效率。

实验配置。测试时具体实验环境配置为：Intel (R) Core (TM) i5-8300H CPU 2.30 GHz；内存 16 GB；操作系统 Windows 11 64 位；编程环境：C++和 GMP6.2。具体实验时，由一台机器模拟 2 个参与方之间进行局域网通信。

5.1 效率分析

一般通过计算复杂度和通信复杂度来衡量具体协议的效率。在考虑计算复杂度时，由于模指数运算的计算复杂度远大于其他运算，例如，计算 g^r 需要 $1.5\langle r\rangle$ 次模乘运算[28]（其中，$\langle r\rangle$ 表示其二进制表示位数），因此通常忽略其他运算，只考虑协议执行过程中的模指数运算次数。考虑到参与双方在协议执行前可以进行产生和交换密钥操作，所以对协议进行效率分析时不考虑准备阶段。表 5 给出了不同协议的计算复杂度与通信复杂度的比较。其中，$\perp$ 表示实验中 ObliVM 和 ABY 使用混淆电路，其计算复杂度与电路的与门数量相关；v 表示输入数据集合的大小；N 表示公钥加密方案的模数；p 表示秘密分享方案的模数；σ 表示安全参数。

表 5 不同协议的计算复杂度与通信复杂度的比较

协议	计算复杂度	通信轮数/轮	通信开销/KB
ObliVM	$\perp$	4	14.80
ABY	$\perp$	4	10.29
GSV07	$9\langle N\rangle$	$3+\mathrm{lb}(p)$	13.75
semiSMC	$9v\langle N\rangle$	$n(n+1)$	49.90
TEAM	$10.5\langle N\rangle+6\sigma$	4	1.25

计算复杂度。如表 5 所示，通过 semiSMC 判断 2 个数的大小关系总共需要 $9v\langle N\rangle$ 次模乘运算。其中参与方的输入从一个集合中选取，v 为该集合的大小，N 为使用公钥加密方案的模数。而本文提出的 TEAM 计算复杂度为 $10.5\langle N\rangle+6\sigma$，远低于同类协议 semiSMC。虽然 TEAM 的计算复杂度高于基于秘密分享的 GSV07（$9\langle N\rangle$），但 GSV07 的通信开销对协议效率的影响要远大于计算开销。此外，ObliVM 和 ABY 这 2 种协议的计算复杂度与其对应电路的与门数量相关，难以与本文提出的基于同态加密的 TEAM 进行对比，所以其计算复杂度用 $\perp$ 替代。后续实验结果证明本文提出的 TEAM 在计算效率上是最优的。

通信复杂度。通信复杂度具体取决于通信轮数和通信开销。在通信轮数方面，semiSMC 协议运行时需要向其他参与方公布自己数据的编码向量，所以其通信轮数为 $n(n-1)$，n 为参与方数量。GSV07 的通信轮数与其使用的秘密分享方案的模数 p 相关，具体为 $3+\mathrm{lb}(p)$ 轮。而本文提出的 TEAM 仅使用 4 轮通信，与 ObliVM 和 ABY 相当。在通信开销方面，TEAM、semiSMC[18]、GSV07[20]、ObliVM[11]和 ABY[12]的通信开销分别为 1.25 KB、49.90 KB、13.75 KB、14.80 KB 和 10.29 KB。

5.2 实验测试

在实验中，本文使用预计算提升 TEAM 协议的运行效率。例如，Alice 在协议执行前预先计算 TEAM 第 2)步中的 $[s]_{\mathrm{pk_a}}$、$[r_1+r_2]_{\mathrm{pk_a}}$、$[r_2]_{\mathrm{pk_a}}$ 等变量，等到 TEAM 执行时直接使用预计算的结果，无须在协议执行过程中计算。

实验测试了 ObliVM、ABY、semiSMC、GSV07 和 TEAM 协议在不同明文长度和不同公钥长度下的运行效率。其中，公钥长度 N 具体是指 TEAM 与 semiSMC 采用加密方案的模数大小。具体地，在 TEAM 中安全参数 $\sigma=128$，Alice 和 Bob 采用的公钥长度满足 $\langle N_{\mathrm{a}}\rangle=\langle N_{\mathrm{b}}\rangle=\langle N\rangle$，且使用预计算优化。在 semiSMC 中输入方集合大小 $v=200$，在 ABY 中仅使用姚氏混淆电路，所以设置 $\mathrm{sharing}=S\_\mathrm{YAO}$。在 GSV07 中，秘密分享方案的模数 $p=128$。

明文长度为 32 bit，公钥长度的范围为 512～1 024 bit 时，不同协议的运行时间（单位为 ms）如图 3 所示。明文长度为 64 bit，公钥长度的范围为 512～1 024 bit 时，不同协议的运行时间如图 4 所示。

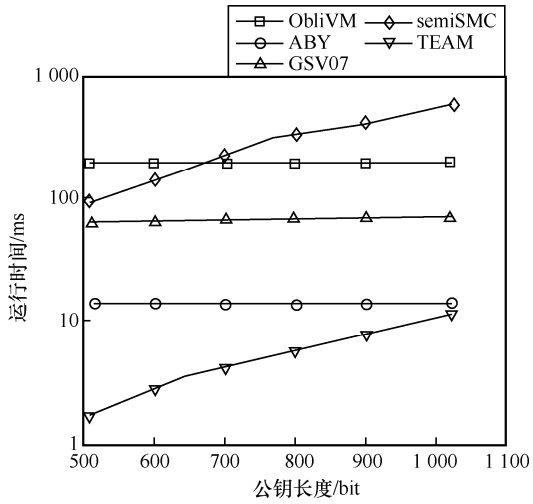

图 3　32 bit 明文在不同公钥长度下不同协议的运行时间

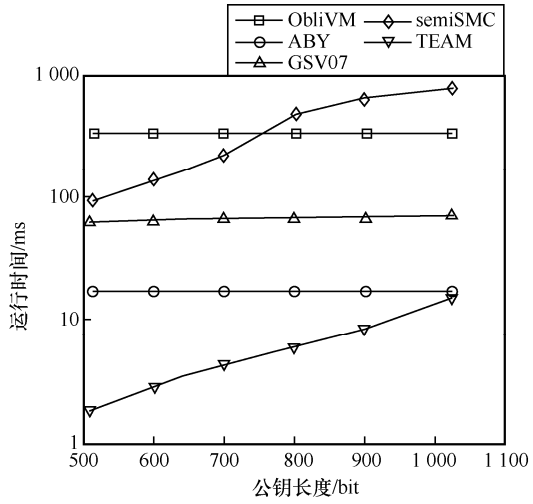

图 4　64 bit 明文在不同公钥长度下不同协议的运行时间

如图 3 所示，由于 ObliVM 和 ABY 采用混淆电路实现安全两方比较，其运行时间与公钥长度无关，因此在明文长度为 32 bit 下，这 2 种协议的运行时间不变，分别为 200.8 ms 和 13.9 ms。其次，随着公钥长度 N 的增加，GSV07 运行时间从 64.5 ms 逐步提升到 72.4 ms。再次，随着公钥长度的增加，TEAM 和 semiSMC 的运行时间逐步增加，且 semiSMC 较 TEAM 的上升趋势更显著（semiSMC 的计算复杂度大于 TEAM）。最后，在协议运行时间上，本文提出的 TEAM 表现最优，当 $\langle N\rangle=1\,024$ bit 时，相较于 ObliVM 快 189 ms，相较于 ABY 快 2.1 ms，相较于 GSV07 快 60.6 ms。特别地，相较于同类协议 semiSMC 快 587.1 ms（50.7 倍）。

如图 4 所示，在明文长度为 64 bit 下，ObliVM 和 ABY 相较于图 3 中明文长度为 32 bit 的协议运行时间更长。其原因是采用混淆电路的 ObliVM 和 ABY 的电路大小和通信总量与明文长度正相关。具体地，在明文长度为 64 bit 下，ObliVM 和 ABY 的运行时间分别是 340.1 ms 和 17.5 ms，相较于 32 bit 明文，运行时间分别增加 139.3 ms 和 3.6 ms。结合图 3 与图 4 可知，TEAM 在相同公钥长度下，明文长度为 32 bit 和明文长度为 64 bit 的运行时间基本一致，semiSMC 与 GSV07 同样如此。其原因是 Paillier 加密算法加密明文时存在随机的乘法因子 r，导致其明文长度与协议运行时间无关。GSV07 采用基于秘密分享的比较方法，其耗时与秘密分享模数 p 正相关与明文长度无关。最后在协议运行时间上，本文提出的 TEAM 表现最优，当 $\langle N\rangle=1\,024$ bit 时，相较于 ObliVM 快 328.2 ms，相较于 ABY 快 5.6 ms，相较于 GSV07 快 60.9 ms。特别地，相较于同类方法 semiSMC 快 588.3 ms（50.4 倍）。

综上，TEAM 运行效率高于基于混淆电路的 ObliVM 和 ABY、基于秘密分享的 GSV07，以及基于同态加密的 semiSMC，即 TEAM 在实现公平性的同时，保证了协议运行效率。

6　结束语

为解决现有安全两方比较协议难以实现公平比较的问题，本文提出一种理性安全的公平两方比较协议。具体地，本文通过门限 Paillier 密码系统和博弈论设计一个满足公平性的安全两方比较协议 TEAM，实现完全信息博弈下的严格纳什均衡，且均衡点为两方均获得比较结果。相比于现有的安全两方比较协议，TEAM 不仅能实现安全且公平的比较，而且极大地提高安全两方比较协议效率。未来，笔者将尝试将理性安全两方比较范式扩展到理性安全多方通用计算。

附录 1　CPA 安全性证明

证明　不失一般性，随机选择 $m_b\in[-2^{\ell},2^{\ell}]$，$r_1\in[2^{\sigma-1},2^{\sigma}-1]$ 以及 $r_2\in[2^{\kappa-1},2^{\kappa}-1]$，所以 $r_1m_b+r_2\in[2^{\kappa-1}-2^{\ell+\sigma}+2^{\ell},2^{\kappa}+2^{\ell+\sigma}-2^{\ell}-1]$。由于 r_1 和 r_2 是挑战者 $\mathcal{C}$ 在实验 $\mathrm{PubK}^{\mathrm{CPA}}_{\mathcal{A},r_1m+r_2}(\sigma,\kappa)$ 第 2)步中随机选择的，因此 $r_1m_b+r_2$ 随机分布在 $[2^{\kappa-1}-2^{\ell+\sigma}+2^{\ell},2^{\kappa}+2^{\ell+\sigma}-2^{\ell}-1]$ 范围内，即敌手从 $r_1m_b+r_2$ 中推断出 b 的概率为

$$\Pr\left[b'=b\mid r_1m_b+r_2\right]=\frac{1}{2} \tag{13}$$

当敌手 $\mathcal{A}$ 在实验 $\mathrm{PubK}^{\mathrm{CPA}}_{\mathcal{A},r_1m+r_2}(\sigma,\kappa)$ 第 1)步中选择

$m_0=-2^{\ell}$，$m_1=2^{\ell}$ 时，敌手 $\mathcal{A}$ 推断出 b 的概率最高，具体如下。

1)若挑战者 $\mathcal{C}$ 在实验 $\mathrm{PubK}^{\mathrm{CPA}}_{\mathcal{A},r_1m+r_2}(\sigma,\kappa)$ 第 2)步选择 $b=0$，则当 $r_1m_b+r_2$ 属于 $[2^{\kappa-1}-2^{\ell+\sigma}+2^{\ell},\ 2^{\kappa-1}+2^{\ell+\sigma-1}-1]$ 时，敌手 $\mathcal{A}$ 能推断出 $b'=b=0$ 的概率为 1。

2)若挑战者 $\mathcal{C}$ 在实验 $\mathrm{PubK}^{\mathrm{CPA}}_{\mathcal{A},r_1m+r_2}(\sigma,\kappa)$ 第 2)步选择 $b=1$，则当 $r_1m_b+r_2$ 的范围属于 $[2^{\kappa}-2^{\ell+\sigma-1},2^{\kappa}+2^{\ell+\sigma}-2^{\ell}-1]$ 时，敌手 $\mathcal{A}$ 能推断出 $b'=b=1$ 的概率为 1。

综合考虑以上 2 种情况，敌手 $\mathcal{A}$ 攻击成功的概率最大为

$$\begin{aligned}&\Pr\left[b'=b|\ r_1m_b+r_2\right]=\\&\frac{1}{2}+\frac{1}{2}\cdot\frac{2^{\kappa-1}+3\cdot2^{\ell+\sigma-1}-2^{\ell}-1+1-2^{\kappa-1}}{2^{\kappa-1}}+\\&\frac{1}{2}\cdot\frac{2^{\kappa}+3\cdot2^{\ell+\sigma-1}-2^{\ell}-1+1-2^{\kappa}}{2^{\kappa-1}}=\\&\frac{1}{2}+\frac{3\cdot2^{\ell+\sigma}-2^{\ell+1}}{2^{\kappa}}\end{aligned}\tag{14}$$

由 ℓ,σ,κ 之间的大小关系（$2^{\ell}\ll2^{\sigma}\ll2^{\kappa}$）可知，$2^{\kappa}\gg3\cdot2^{\ell+\sigma}-2^{\ell+1}$，所以存在可忽略函数 $\mathrm{negl}(\kappa)=\dfrac{3\cdot2^{\ell+\sigma}-2^{\ell+1}}{2^{\kappa}}$，使以下不等式成立

$$\Pr\left[b'=b|\ r_1m_b+r_2\right]\leqslant\frac{1}{2}+\mathrm{negl}(\sigma,\kappa)\tag{15}$$

证毕。

附录 2 模拟范式证明

证明 依照定义 3 要求，分别构造模拟器 $\mathcal{S}_1$ 和 $\mathcal{S}_2$，若 2 个模拟器使式(12)成立，即可证明定理 2 的正确性。在 TEAM 中，$f_1(x,y)=u_{\mathrm{a}},f_2(x,y)=u_{\mathrm{b}}$。下面分别讨论构造模拟器 $\mathcal{S}_1$ 和 $\mathcal{S}_2$ 的这 2 种情况。

构造模拟器 $\mathcal{S}_1$ 具体的模拟流程如下。

1) $\mathcal{S}_1$ 随机选取 $y'\in[-2^{\ell},2^{\ell}]$，使 $f_1(x,y)=f_1(x,y')=u_{\mathrm{a}}$。随后加密 y' 得到 $[y']_{\mathrm{pk_b}}=\mathrm{Enc}(\mathrm{pk_b},y')$。

2) $\mathcal{S}_1$ 随机选取 $r_1\in\{0,1\}^{\sigma}\setminus\{0\}$，随机数 $r_2\in\left[\dfrac{N_{\mathrm{b}}}{2}-r_1+1,\dfrac{N_{\mathrm{b}}}{2}\right]$ 和 $s\in\{0,1\}$。随后加密 s 得到 $[s]_{\mathrm{pk_a}}=\mathrm{Enc}(\mathrm{pk_a},s)$，部分解密 $[s]_{\mathrm{pk_a}}$ 得到 $S_1=\mathrm{PDec}([s]_{\mathrm{pk_a}},\lambda_1)$。若 $s=0$，此时 $\mathcal{S}_1$ 计算 $D'=\left([x]_{\mathrm{pk_b}}[y']_{\mathrm{pk_b}}^{N_{\mathrm{b}}-1}\right)^{r_1}[r_1+r_2]_{\mathrm{pk_b}}$。若 $s=1$，则计算 $D'=\left([y']_{\mathrm{pk_b}}[x]_{\mathrm{pk_b}}^{N_{\mathrm{b}}-1}\right)^{r_1}[r_2]_{\mathrm{pk_b}}$。

3) $\mathcal{S}_1$ 解密 D' 得到 $d'=\mathrm{Dec}(\mathrm{sk_b},D')$。若 $d'>\dfrac{N_{\mathrm{b}}}{2}$，记 $u_1'=0$，否则记 $u_1'=1$。随后加密 u_1' 得到 $[u_1']_{\mathrm{pk_a}}=\mathrm{Enc}(\mathrm{pk_a},u_1')$。

4) $\mathcal{S}_1$ 解密 $[u_1']_{\mathrm{pk_a}}$ 得到 $u_1'=\mathrm{Dec}(\mathrm{sk_a},[u_1']_{\mathrm{pk_a}})$，随后计算 $u_{\mathrm{a}}'=\left|s-u_1'\right|$。

5) $\mathcal{S}_1$ 部分解密 $[s]_{\mathrm{pk_a}}$ 成 $S_2=\mathrm{PDec}([s]_{\mathrm{pk_a}},\lambda_2)$。随后完全解密 $[s]_{\mathrm{pk_a}}$ 得到 $s=\mathrm{TDec}(M_1,M_2)$，最后计算 $u_{\mathrm{b}}'=\left|s-u_1'\right|$。

结合上述模拟步骤，模拟器 $\mathcal{S}_1$ 得到的视图为

$$\begin{aligned}\mathcal{S}_1\left(x,f_1(x,y)\right)=\big(&x,[x]_{\mathrm{pk_b}},s,[y']_{\mathrm{pk_b}},[s]_{\mathrm{pk_a}},\\&S_1,S_2,D',d',u_1',f_1(x,y')\big)\end{aligned}\tag{16}$$

真实视图为

$$\begin{aligned}\mathrm{view}_1^{\pi}(x,y)=\big(&x,[x]_{\mathrm{pk_b}},s,[y]_{\mathrm{pk_b}},[s]_{\mathrm{pk_a}},\\&S_1,S_2,D',d',u_1',f_1(x,y')\big)\end{aligned}\tag{17}$$

模拟器 $\mathcal{S}_1$ 得到的结果 $\mathrm{output}_2^{\pi}(x,y)=u_{\mathrm{b}}'$，真实的结果 $f_2(x,y)=u_{\mathrm{b}}$。由于 $f_1(x,y)=f_1(x,y')$，所以 $u_{\mathrm{a}}=u_{\mathrm{a}}'$，从而 $u_1=u_1'$，进一步得出 $d=d'$ 以及 $\mathrm{output}_2^{\pi}(x,y)\overset{\mathrm{c}}{\equiv}f_2(x,y)$。又因为 Paillier 加密是语义安全的，所以 $[y]_{\mathrm{pk_b}}\overset{\mathrm{c}}{\equiv}[y']_{\mathrm{pk_b}}$，且 $D\overset{\mathrm{c}}{\equiv}D'$，即存在模拟器 $\mathcal{S}_1$ 满足

$$\begin{aligned}&\left\{\left(\mathcal{S}_1\left(x,f_1(x,y)\right),f_2(x,y)\right)\right\}_{x,y}\overset{\mathrm{c}}{\equiv}\\&\left\{\left(\mathrm{view}_1^{\pi}(x,y),\ \mathrm{output}_2^{\pi}(x,y)\right)\right\}_{x,y}\end{aligned}$$

同理，存在模拟器 $\mathcal{S}_2$ 满足

$$\begin{aligned}&\left\{\left(\mathcal{S}_2\left(y,f_2(x,y)\right),f_1(x,y)\right)\right\}_{x,y}\overset{\mathrm{c}}{\equiv}\\&\left\{\left(\mathrm{view}_2^{\pi}(x,y),\ \mathrm{output}_1^{\pi}(x,y)\right)\right\}_{x,y}\end{aligned}$$

证毕。

参考文献：

[1] YAO A C. Protocols for secure computations[C]//Proceedings of the 23rd Annual Symposium on Foundations of Computer Science. Piscataway: IEEE Press, 1982: 160-164.

[2] YAO A C C. How to generate and exchange secrets[C]//Proceedings of the 27th Annual Symposium on Foundations of Computer Science. Piscataway: IEEE Press, 1986: 162-167.

[3] IOANNIDIS I, GRAMA A. An efficient protocol for Yao's millionaires' problem[C]//Proceedings of the 36th Annual Hawaii International Conference on System Sciences. Piscataway: IEEE Press, 2003: 6.

[4] LI S D, WANG D S, DAI Y Q, et al. Symmetric cryptographic solution to Yao's millionaires' problem and an evaluation of secure multiparty computations[J]. Information Sciences, 2008, 178(1): 244-255.

[5] DAMGARD I, GEISLER M, KROIGARD M. Homomorphic encryption and secure comparison[J]. International Journal of Applied Cryptography, 2008, 1(1): 22-31.

[6] DAMLE S, FALTINGS B, GUJAR S. Blockchain-based practical multi-agent secure comparison and its application in auctions[C]//Proceedings of IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology. New York: ACM Press, 2021: 430-437.

[7] ZHOU L J, WANG Z Y, CUI H R, et al. Bicoptor: two-round secure three-party non-linear computation without preprocessing for privacy-preserving machine learning[C]//Proceedings of 2023 IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE Press, 2023: 534-551.

[8] LIU X M, CHOO K K R, DENG R H, et al. Efficient and privacy-preserving outsourced calculation of rational numbers[J]. IEEE Transactions on Dependable and Secure Computing, 2018, 15(1): 27-39.

[9] 郭奕旻, 周素芳, 窦家维, 等. 高效的区间保密计算及应用[J]. 计算机学报, 2017, 40(7): 1664-1679.
GUO Y M, ZHOU S F, DOU J W, et al. Efficient privacy-preserving interval computation and its applications[J]. Chinese Journal of Computers, 2017, 40(7): 1664-1679.

[10] ZHAO B W, LIU X M, SONG A, et al. PriMPSO: a privacy-preserving multiagent particle swarm optimization algorithm[J]. IEEE Transactions on Cybernetics, 2023, 53(11): 7136-7149.

[11] LIU C, WANG X S, NAYAK K, et al. ObliVM: a programming framework for secure computation[C]//Proceedings of 2015 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2015: 359-376.

[12] DEMMLER D, SCHNEIDER T, ZOHNER M. ABY - a framework for efficient mixed-protocol secure two-party computation[C]// Proceedings of Network and Distributed System Security Symposium. Reston: Internet Society, 2015: 1-15.

[13] KOLESNIKOV V, SCHNEIDER T. Improved garbled circuit: free xor gates and applications[C]//International Colloquium on Automata, Languages, and Programming. Berlin: Springer, 2008: 486-498.

[14] CANETTI R, POBURINNAYA O, VENKITASUBRAMANIAM M. Equivocating Yao: constant-round adaptively secure multiparty computation in the plain model[C]//Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing. New York: ACM Press, 2017: 497-509.

[15] GROCE A, KATZ J. Fair computation with rational players[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2012: 81-98.

[16] LIN H Y, TZENG W G. An efficient solution to the millionaires' problem based on homomorphic encryption[C]//Applied Cryptography and Network Security. Berlin: Springer, 2005: 456-466.

[17] LIU X, LI S D, CHEN X B, et al. Efficient solutions to two-party and multiparty millionaires' problem[J]. Security and Communication Networks, 2017, 2017: 1-11.

[18] 李顺东, 徐雯婷, 王文丽, 等. 恶意模型下的最大(小)值保密计算[J]. 计算机学报, 2021, 44(10): 2076-2089.
LI S D, XU W T, WANG W L, et al. Secure maximum (minimum) computation in malicious model[J]. Chinese Journal of Computers, 2021, 44(10): 2076-2089.

[19] ZHAO B W, YUAN J M, LIU X M, et al. SOCI: a toolkit for secure outsourced computation on integers[J]. IEEE Transactions on Information Forensics and Security, 2022, 17: 3637-3648.

[20] VEUGEN T, BLOM F, HOOGH S J A D, et al. Secure comparison protocols in the semi-honest model[J]. IEEE Journal of Selected Topics in Signal Processing, 2015, 9(7): 1217-1228.

[21] DAMGARD I, FITZI M, KILTZ E, et al. Unconditionally secure constant-rounds multi-party computation for equality, comparison, bits and exponentiation[C]//Theory of Cryptography. Berlin: Springer, 2006: 285-304.

[22] HALPERN J, TEAGUE V. Rational secret sharing and multiparty computation: extended abstract[C]//Proceedings of the Thirty-Sixth Annual ACM Symposium on Theory of Computing. New York: ACM Press, 2004: 623-632.

[23] MAITRA A, PAUL G, PAL A K. Revisiting secure two-party computation with rational player[J]. Cryptology ePrint Archive, 2015: 1-13.

[24] PAILLIER P. Public-key cryptosystems based on composite degree residuosity classes[C]//Proceedings of the 17th International Conference on Theory and Application of Cryptographic Techniques. New York: ACM Press, 1999: 223-238.

[25] DING C, PEI D Y, SALOMAA A. Chinese remainder theorem: applications in computing, coding, cryptography[M]. Singapore: World Scientific, 1996.

[26] ACHIM O M, POP F, CRISTEA V. Reputation based selection for services in cloud environments[C]//Proceedings of 2011 14th International Conference on Network-Based Information Systems. Piscataway: IEEE Press, 2011: 268-273.

[27] KATZ J, LINDELL Y. Introduction to modern cryptography[M]. Florida: Chapman and Hall/CRC, 2020.

[28] GOLDREICH O. Foundations of cryptography: volume 2, basic applications[M]. Cambridge: Cambridge University Press, 2009.

[作者简介]

赵搏文（1992−），男，湖南双峰人，博士，西安电子科技大学副教授、硕士生导师，主要研究方向为隐私计算方法与隐私保护的计算智能。

祝遥（2000− ），男，湖北孝感人，西安电子科技大学硕士生，主要研究方向为隐私计算及其应用。

肖阳（1991− ），男，新疆石河子人，博士，西安电子科技大学讲师、硕士生导师，主要研究方向为图神经网络、信任评估和区块链。

裴庆祺（1974− ），男，陕西西安人，博士，西安电子科技大学教授、博士生导师，主要研究方向为无线网络安全。

李小国（1991− ），男，山西夏县人，博士，新加坡管理大学研究员，主要研究方向为可信计算、安全计算和公钥密码系统。

刘西蒙（1988− ），男，陕西西安人，博士，福州大学教授、博士生导师，主要研究方向为安全计算、应用密码学和大数据安全。