密码学报 ISSN 2095-7025 CN 10-1195/TN
Journal of Cryptologic Research, 2020, 7(6): 774–788
©《密码学报》编辑部版权所有.
E-mail: jcr@cacrnet.org.cn
http://www.jcr.cacrnet.org.cn
Tel/Fax: +86-10-82789618

图交集和并集的安全多方计算*

魏 琼, 李顺东, 王文丽, 杜润萌

陕西师范大学 计算机科学学院, 西安 710119
通信作者: 李顺东, E-mail: shundong@snnu.edu.cn

摘 要: 安全多方计算是密码学界研究的重要方向和热点问题, 图论是表示事物之间联系的建模工具, 因此, 要揭示事物之间的内在关联而不泄露隐私, 就需要研究图结构数据的安全多方计算. 目前, 国际密码学界对于图结构数据的安全多方计算问题的研究刚刚起步, 其中, 图的交集、并集的保密计算在科学研究和社会实践中都具有重要意义. 本文首先提出了一种新的编码方法来表示一个图, 并结合保密替换方法和门限解密方案, 研究了图的交集和并集的安全多方计算问题. 针对这两个问题, 本文分别设计了能抵抗任意程度合谋攻击的高效协议, 并应用模拟范例严格证明了协议在半诚实模型下是安全的. 最后, 对本文协议和现有方案的计算复杂性和通信复杂性分析进行了详细的分析和对比, 并通过实验进行验证. 理论分析和实验数据均表明本文所提出的方案是高效的.

关键词: 安全多方计算; 图的交 (并) 集; 门限解密; 半诚实模型

中图分类号: TP309.7 **文献标识码:** A DOI: 10.13868/j.cnki.jcr.000405

中文引用格式: 魏琼, 李顺东, 王文丽, 杜润萌. 图交集和并集的安全多方计算[J]. 密码学报, 2020, 7(6): 774–788. [DOI: 10.13868/j.cnki.jcr.000405]

英文引用格式: WEI Q, LI S D, WANG W L, DU R M. Secure multiparty computation of graph intersection and union[J]. Journal of Cryptologic Research, 2020, 7(6): 774–788. [DOI: 10.13868/j.cnki.jcr.000405]

Secure Multiparty Computation of Graph Intersection and Union

WEI Qiong, LI Shun-Dong, WANG Wen-Li, DU Run-Meng

School of Computer Science, Shaanxi Normal University, Xi'an 710119, China
Corresponding author: LI Shun-Dong, E-mail: shundong@snnu.edu.cn

Abstract: Secure multi-party computation (MPC) is an important research topic in cryptography, and graph theory is a modeling tool to represent the relations among different things. Therefore, in order to reveal the internal relations among different things without privacy disclosure, it is necessary to study the problem of secure graph computation. Privately computing the graph intersection and graph union of private graphs is of great significance. This paper proposes a new encoding method to represent a graph, and studies the MPC of graph intersection and graph union by using the private substitution method and a threshold decryption scheme. Efficient protocols for the MPC of graph intersection and graph union are designed to resist collusion attacks, and simulation paradigm is used to prove that the proposed protocols are secure in the semi-honest model. The computational complexity and communication complexity of the proposed protocols are analysed, and some comparison with the

* 基金项目: 国家自然科学基金 (61272435)
Foundation: National Natural Science Foundation of China (61272435)
收稿日期: 2019-11-07 定稿日期: 2020-02-19

existing schemes is presented. Some experiments are conducted. Both the theoretical analysis and experimental results show that the proposed protocols are efficient.

Key words: secure multi-party computation; graph intersection (union); threshold decryption; semi-honest model

1 引言

安全多方计算 (Secure Multi-party Computation, MPC) 指的是两个或更多的参与者利用各自的保密数据作为计算的输入, 联合进行的保密计算, 计算结束后没有参与方能获得多于规定输出的信息, 是信息社会隐私保护的重要技术. 通过安全多方计算, 参与者可以在互不信任的网络环境中联合计算, 以实现保密的数据挖掘 [1]、数据查询 [2,3]、外包计算 [4] 等, 解决了数据的隐私性和安全性问题, 因此安全多方计算在国际密码学界研究中具有重要地位. 安全多方计算由图灵奖获得者姚期智首次提出 [5], Goldreich、Micali 等人在此基础上做了大量研究 [6,7], 他们的研究成果奠定了安全多方计算的理论基础 [8–10]. 图灵奖获得者 Goldwasser 认为安全多方计算是密码学一个极其重要的工具, 将成为计算科学一个必不可少的组成部分 [11]. 目前研究的安全多方计算问题包括科学计算 [12–15]、计算几何 [16–19]、统计分析 [20,21] 等方面, 但此类安全多方计算问题大多限于整数数据为输入的保密计算, 未涉及描述事物关联的隐私数据的保密计算. 研究事物之间关联并发现规律, 对于认识世界、改造世界至关重要.

图论模型是一种强大而灵活的科学建模与数据分析工具, 是研究事物之间相互关联、相互影响最有效的模型. 事物之间的相互关联与影响构成了各种各样的网络, 如社交网络、交通网络、信息传播网络、疾病传播网络等, 这些网络都是图, 图可以直观地表达事物之间的关联, 有利于发现数据之间的关系, 能把纷杂的信息变得有序、直观、清晰. 图的节点可以表示任何事物, 边可以表示事物之间的任何关系, 因此几乎所有涉及事物间联系的系统都可以用图来建模与表达. 将图论方法用于医学研究破译了肝癌细胞向肺转移的预警网络信号 [22]; 社交网络分析发现一个人的信用与其朋友的信用关系密切, 可以借此对某人进行信用评级 [23]; 谷歌只是将图论中节点度的概念用于评价网页的重要程度, 就取得了出乎意料的成功. 然而很多时候, 事物之间的关联数据中存在大量的隐私数据, 即图结构形式的隐私数据, 如家族病史、基因图谱、基因缺陷、交易对象、犯罪记录、是否吸毒、政治倾向、朋友圈、喜欢或讨厌某人等数据, 以及涉及经济、军事活动的机密数据等. 如果直接利用这些数据进行联合计算以及科学研究与分析, 就有可能泄露机密信息或隐私, 导致严重的后果. 对隐私泄露的担心使得人们不愿共享这些数据. 许多国家、地区以及大型企业都对数据的使用施加严格的限制 [24], 这些限制使得很多实体采集的数据无法充分利用, 难以发掘数据的价值, 发挥其应有的作用. 如何在充分保护隐私数据机密性的前提下利用数据的价值, 使数据的社会效益与经济效益得到充分的发挥, 是亟待解决的问题, 具有非常现实和重要的意义, 这就需要研究图结构数据利用中的隐私保护问题.

目前这方面的研究才刚刚起步. 本文提出了保密求多个图的交集和并集的问题, 并给出解决方案, 这些问题都具有重要的研究意义. 比如, 几家航空公司想在某一地区开通航线, 但正式开通之前所有线路都是保密的, 为了避免某些航班的飞行班次过多而造成资源的浪费, 就需要提前知道它们在该区域内有哪些共同的航线, 各航空公司则可根据这一结果对该公司的飞行班次做出调整. 令区域内的所有城市为顶点, 其飞行路线作为边, 则该问题就抽象成多个图交集的保密计算问题. 又如, 公司内部想要在诸多员工中选出一位担任某项目组长, 这就需要多方面考查员工之间的社交关系, 如喜欢、支持、合作等, 选择在各方面关系中都与他人保持良好者担任组长, 可大大提高工作效率. 但这些社交关系均属于隐私信息, 因此不应泄露. 令每位员工为节点, 相互之间的关系为边, 则问题就抽象为多个图并集的保密计算问题. 当求出多种关系图的并集后, 并集中度最大的顶点即为度中心性最高的点, 该节点在整个网络中最重要, 那么由该节点所代表的成员担任项目组长.

关于图的安全多方计算问题, 已有的研究是文献 [25, 26] 以各参与者与其他参与者的边信息为基础, 在保证隐私的前提下生成某种网络图. 其中文献 [25] 主要应用秘密分享的方法构造方案, 解决方案是初级的、计算复杂性与通信复杂性都很高; 文献 [26] 应用同态加密的方法构造方案, 解决方案中需要若干个权威机构帮助实现, 且由于所用加密及密文重随机化次数较多, 计算复杂性也很高, 这些方案离实际应用还

很远. 文献 [27] 提出了一种在线社交网络中的安全链路预测技术. 文献 [28] 研究了图中最短路径的安全计算问题. 文献 [29] 假定网络信息是分布式存储的, 其中每个参与者都拥有网络的部分信息, 进而研究基础图的安全生成问题, 但方案中使用了可信第三方, 通信成本和计算成本都很高. 文献 [30] 计算近似的图编辑距离, 提出了确定容错图匹配的方案. 文献 [31] 中提出了图的交集保密计算方案, 该方案首先利用文献 [32] 中提出的第一个安全的两方保密集合交集协议 (FNP 协议) 作为子协议, 先计算出服务器和客户端两方图的顶点交集, 服务器再根据顶点交集和边构造出一个邻接矩阵并加密, 最后客户端利用 Paillier 加密系统对双方的邻接矩阵做同态加密运算, 解密结果就是两方图的交集. 但该方案存在以下问题: 调用的 FNP 协议是将集合表示成多项式的方式来计算集合的交集, 而 FNP 协议的计算复杂性与多项式的次数密切相关, 且同样使用了 Paillier 加密方案, 因此文献 [31] 中求图的交集方案的计算复杂性非常高, 并且该方案仅限于两方之间求图的交集, 对于更实际的多方求图的交集问题未能解决.

本文主要研究图交集和并集的安全多方计算问题, 给出求解这些问题的高效解决方案. 本文的主要贡献如下:

(1) 提出了一种新的编码方法, 使图中的边和顶点都可以准确的表示在一个特殊的矩阵中. 与无向图的邻接矩阵稍有不同的是, 本文编码所得矩阵的主对角线元素不全为 0, 而主对角线元素代表无向图的顶点, 故本文编码方法可以将无向图的顶点和边的都在矩阵中表示出来, 后续对于图的顶点和边的加密则可以转化为对矩阵中相应元素的加密. 这样的编码方法可以为其他图论的安全多方计算问题提供一种新的途径.

(2) 利用所提出的编码方法, 保密替换方法 [33]、Lifted-ElGamal 门限密码系统, 分别设计了求图交集和并集的安全多方计算协议, 对所提出协议的正确性进行了分析, 并通过模拟范例严格证明了协议的安全性, 得出本文协议均能抵抗任意程度合谋攻击的结论.

(3) 只需将本文协议所用 Lifted-ElGamal 门限密码系统改为 ElGamal 密码系统, 也可实现图交集和并集的安全两方计算, 比现有图交集的两方计算协议更具普适性, 应用场景和应用范围更广泛. 且通过效率分析和实验数据, 证明了本文协议与现有方案相比, 计算效率和通信效率都大大提升.

2 预备知识

2.1 安全性定义

理想模型 假设有一个通信双方都完全信任的第三方, 称为可信的第三方 (Trusted Third Party, TTP), 他在任何情况下都会严格的按照通信双方的要求执行每一步操作, 同时也不会泄露通信双方的私密信息. 安全多方计算中的理想模型可以描述为: n 个参与者 $P_1,\cdots,P_n$, 他们分别将各自的秘密 $x_1,\cdots,x_n$ 告诉可信第三方, 由他单独计算函数 f:

$$f(x_1,\cdots,x_n)=(f_1(x_1,\cdots,x_n),\cdots,f_n(x_1,\cdots,x_n))$$

然后将计算结果分别告诉 n 个参与者. 除此计算结果之外, $P_1,\cdots,P_n$ 得不到任何其他信息. 理想模型虽然安全但并不适用于实际应用, 在实际中限制性较强, 这是因为网络环境纷繁复杂, 合作计算方共同信任的第三方很难找到, 且使用可信第三方也必将花费大量时间和金钱, 导致执行协议的成本过高.

半诚实模型 本文假设所有参与者均为半诚实参与者 [6]. 所谓半诚实参与者是指参与者会按要求忠实地履行协议, 协议执行完成后, 所有参与者只知道协议的最终结果, 无法获得其他参与者输入的保密信息, 但他们可能在协议执行的过程中将收集到的所有信息记录下来, 在协议执行后试图根据记录的信息推算出其他参与者的输入.

设有 n 个半诚实参与者 $P_1,\cdots,P_n$, 分别拥有私有数据 $x_1,\cdots,x_n$, 他们合作执行一个保密计算函数 $f(x_1,\cdots,x_n)$ 的协议 Π, 并在协议完成后得到最终结果. 这种参与者都是半诚实的安全多方计算协议称为半诚实模型下的安全多方计算协议 (简称半诚实协议). 令 $X=(x_1,\cdots,x_n)$, 在执行协议过程中, 参与者 P_i 得到的消息序列记为

$$\mathrm{view}_i^{\Pi}(X)=(x_i,r_i,M_i^1,\cdots,M_i^t)$$

其中, $M_i^j(j=1,2,\cdots,t)$ 表示第 i 个参与者收到的第 j 个信息, r_i 是第 i 个参与者产生的随机数.

定义 1 半诚实参与者协议的安全性 设 $f:(\{0,1\}^*)^n\to(\{0,1\}^*)^n$ 是一个 n 元函数, $f_i(x_1,\cdots,x_n)$ 为 $f(x_1,\cdots,x_n)$ 中第 i 个元素. $I=\{P_{i_1},\cdots,P_{i_s}\}\subseteq\{P_1,\cdots,P_n\}$, 表示任意参与者的子集. $f_I(x_1,\cdots,x_n)$ 表示序列 $f_{i_1}(x_1,\cdots,x_n),\cdots,f_{i_s}(x_1,\cdots,x_n)$. $\text{output}^{\Pi}(X)$ 为协议 Π 执行后的输出结果. 在参与者都是半诚实的情况下, 如果存在概率多项式时间算法 S, 使得对于任意的 I 均有下式成立:

$$\{S(I,(x_{i_1},\cdots,x_{i_s}),f_I(X))\}_{X\in(\{0,1\}^*)^n}\overset{c}{\equiv}\{\text{view}_I^{\Pi}(X),\text{output}^{\Pi}(X)\}_{X\in(\{0,1\}^*)^n}\tag{1}$$

那么称协议 Π 保密地计算 n 元函数 f. $\overset{c}{\equiv}$ 表示计算不可区分, $\text{view}_I^{\Pi}(X)=(I,\text{view}_{i_1}^{\Pi}(X),\cdots,\text{view}_{i_s}^{\Pi}(X))$, 即 $\text{view}_I^{\Pi}(X)$ 只包括 I 中的参与者在协议执行过程中所得到的消息序列.

2.2 门限解密

在安全多方计算协议中, 当参与方数量超过两方时, 需要考虑合谋攻击的问题, 即: 几个参与者之间合作, 利用执行协议各自所得到的信息去获取其他参与者的私有信息. 解决这一问题的有力工具就是门限解密 [34,35]. 首先 n 个参与者联合生成一个门限解密的密码系统, 每个参与者持有私钥的一个份额, 公布生成的公钥. 每个参与者都可用公钥加密, 但只有 n 个参与者合作才能解密密文. 假设至少 t 个参与者合作才能解密, 那么这样的密码体制称为 (t,n) 门限密码体制, 少于 t 个参与者合作则无法得到明文信息. RSA、ElGamal、Paillier 等密码系统都可以用来构造门限密码系统, 本文利用 ElGamal 乘法同态加密方案构造一个具有加法同态性的门限密码系统—Lifted-ElGamal 门限密码系统 [36], 以此抵抗 $n-1$ 个参与者的合谋攻击. 具体构造如下:

• **KeyGen**. 给定安全参数 k, KeyGen 生成一个 k 比特的大素数 p 以及 Z_p^* 的一个生成元 g. 每个参与者 P_i 随机地选取一个私钥 $\text{sk}_i\in Z_p^*$, 并计算 $h_i=g^{\text{sk}_i}\bmod p$. 公钥即为:

$$h\equiv\prod_{i=1}^{n}h_i\bmod p\equiv g^{\Sigma_{i=1}^{n}\text{sk}_i}\bmod p$$

• **Encrypt**. 为了加密消息 $M(M\in\{0,1\})$, 选择随机数 r, 则密文为

$$E(M)=(c_1,c_2)=(g^r\bmod p,g^Mh^r\bmod p)$$

• **Decrypt**. 对于密文 $E(M)=(c_1,c_2)$, 通过下面的过程可解密出明文:

$$g^M=\frac{c_2}{\prod_{i=1}^{n}{c_1}^{\text{sk}_i}}\bmod p$$

• **同态性质**. Lifted-ElGamal 密码体制具有加法同态性:

$$\begin{aligned}E(M_1)\times E(M_2)&=(g^{r_1}\bmod p,g^{M_1}h^{r_1}\bmod p)\times(g^{r_2}\bmod p,g^{M_2}h^{r_2}\bmod p)\\&=(g^{r_1+r_2}\bmod p,g^{M_1+M_2}h^{r_1+r_2}\bmod p)\\&=E(M_1+M_2)\end{aligned}$$

2.3 密文的重随机化

在概率加密系统中, 一个明文可以有多个不可区分的密文, 很多密文都被解密为同一个明文. 无须私钥, 而将某一密文改变为同一个明文的不同密文, 这样的操作称为密文的重随机化 [37]. 事实上, 所有由概率同态加密系统加密得到的密文, 都可对其进行重随机化. 例如, 在上述 Lifted-ElGamal 密码系统中, 根据其加法同态性可知, 对于一个密文 $E(M)$, 乘 "0" 的密文就可将原有密文改变为另一个密文, 而保持明文不变, 即通过计算 $E(M)\times E(0)=E(M+0)=E'(M)$ 来实现密文的重随机化, $E'(M)$ 表示密文 $E(M)$ 重随机化后的密文, 并且 $E'(M)$ 与密文 $E(M)$ 是计算不可区分的. 因此, Lifted-ElGamal 密码系

统具有重随机化特性 (re-randomizing property).

3 基于门限解密的多个图交集的保密计算

3.1 问题描述

假设顶点集 V 和边集 E 构成一个无向完全图 $G_0 = (V, E)(\frac{m(m-1)}{2}$ 条边), 其中 $V = \{v_1, v_2, \cdots, v_m\}$. 参与者 $P_1, P_2, \cdots, P_n$ 分别拥有 G_0 的子图 $G_1, G_2, \cdots, G_n$, 他们想保密求 n 个图交集而不泄露各自信息.

3.2 计算原理

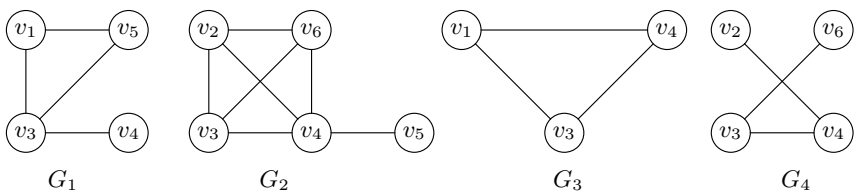
首先提出编码方法 1, 将图的顶点和边信息都存储在一个矩阵中, 编码方式如下: 当图中有顶点 v_i 时, 矩阵元素 m_{ii} 值为 1, 否则为 0. 如果顶点 v_i 和 v_j 之间有边, 那么矩阵中 m_{ij} 值为 1, 否则值为 0.

编码方法 1:

$$m_{ij} = \begin{cases} 1, & \text{顶点 } v_i, v_j \text{ 之间有边 } (i = j \text{ 且顶点 } v_i \text{ 存在}); \\ 0, & \text{顶点 } v_i, v_j \text{ 之间没有边 } (i = j \text{ 且顶点 } v_i \text{ 不存在}) \end{cases}$$

由于是无向图, 这样生成的矩阵都是关于对角线对称的, 因此参与者 P_i 只需取存储矩阵对角线及其以下的元素 (第 i 行具有 i 个元素的下三角部分, $1 \le i \le m$), 构成向量 X_i 再进行运算即可. n 个参与者根据编码方法 1 先生成图 $G_1, G_2, \cdots, G_n$ 的存储矩阵 $M_1, M_2, \cdots, M_n$, 再分别将 n 个矩阵中对角线及以下元素构成分量数均为 $t = \frac{m(m+1)}{2}$ 的向量 $X_1, X_2, \cdots, X_n$. 要计算两个图 G_1, G_2 的交集, 只需参与者 P_2 用自己向量 X_2 中值为 0 的分量去替换 X_1 中对应分量即可, X_1 中其余分量则保持不变. 可以看出, 若某个顶点或者边是 G_1, G_2 交集中的元素, 则替换之后, P_2 得到的新向量 X_2 中对应该顶点或边的分量值仍为 1; 反之, 该位置的分量值会变为 0. 将替换后的向量 X_2 还原成 $m \times m$ 矩阵的下三角部分, 即第 i 行具有 i 个元素的下三角矩阵 $(1 \le i \le m)$(上三角部分为空), 再以对角线为对称轴还原出另一半的上三角部分, 即为 G_1, G_2 交集的存储矩阵, 根据存储矩阵就可以知道具体的图. 以此类推, 参与者 P_i 可以通过用自己向量 X_i 中值为 0 的分量去替换 X_{i-1} 中的对应分量, X_{i-1} 中其余位置的分量保持不变, 然后根据替换后 P_i 得到的新向量 X_i, 可以还原出 i 个图交集的存储矩阵, 进而得到 i 个图的交集.

例: 假设顶点全集 $V = \{v_1, v_2, \cdots, v_6\}$, 参与者 P_1, P_2, P_3, P_4 分别拥有图 G_1, G_2, G_3, G_4, 如下所示:



根据编码方式 1, P_1, P_2, P_3, P_4 分别生成其存储矩阵 M_1, M_2, M_3, M_4:

$$M_1 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \quad M_2 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}$$

$$M_3=\begin{pmatrix}1&0&1&1&0&0\\0&0&0&0&0&0\\1&0&1&1&0&0\\1&0&1&1&0&0\\0&0&0&0&0&0\\0&0&0&0&0&0\end{pmatrix}\quad M_4=\begin{pmatrix}0&0&0&0&0&0\\0&1&0&1&0&0\\0&0&1&1&0&1\\0&1&1&1&0&0\\0&0&0&0&0&0\\0&0&1&0&0&1\end{pmatrix}$$

P_1,P_2,P_3,P_4 分别将 M_1,M_2,M_3,M_4 中对角线及其以下元素依次连接, 构成具有 $\frac{6\times(6+1)}{2}=21$ 个分量的向量:

$$X_1=(1,0,0,1,0,1,0,0,1,1,1,0,1,0,1,0,0,0,0,0,0)$$
$$X_2=(0,0,1,0,1,1,0,1,1,1,0,0,0,1,1,0,1,1,1,0,1)$$
$$X_3=(1,0,0,1,0,1,1,0,1,1,1,0,0,0,0,0,0,0,0,0,0)$$
$$X_4=(0,0,1,0,0,1,0,1,1,1,0,0,0,0,0,0,0,1,0,0,1)$$

那么, 经过 P_2 替换后,

$$X_2=(0,0,0,0,0,1,0,0,1,1,0,0,0,0,1,0,0,0,0,0,0)$$

经过 P_3 替换后,

$$X_3=(0,0,0,0,0,1,0,0,1,1,0,0,0,0,0,0,0,0,0,0,0)$$

经过 P_4 替换后,

$$X_4=(0,0,0,0,0,1,0,0,1,1,0,0,0,0,0,0,0,0,0,0,0)$$

最后, 根据 X_4 可以还原出一个 6×6 矩阵的下三角部分, 再以对角线为对称轴还原出另一半的上三角部分, 即为 G_1,G_2,G_3,G_4 交集的存储矩阵 M:

$$M=\begin{pmatrix}0&0&0&0&0&0\\0&0&0&0&0&0\\0&0&1&1&0&0\\0&0&1&1&0&0\\0&0&0&0&0&0\\0&0&0&0&0&0\end{pmatrix}$$

根据存储矩阵就可以知道具体的图 G:



G

以上提出的方案就是本文计算多个图交集的基本原理. 直接这样计算是无法保密的, 而在密文的条件下进行这样的操作则可以实现保密. 本文利用 Lifted-ElGamal 门限密码系统构造一个抗合谋攻击的图交集的安全多方计算协议. 对向量中的 0 和 1 进行概率加密, 使得任何参与者都无法分辨出向量中的 0 与 1. 在每个参与者完成密文替换的操作后, 将未替换过的密文进行重随机化来保证协议的安全性.

3.3 抗合谋攻击的多个图交集的保密计算

协议 1 基于门限解密的多个图交集保密计算协议.

输入: $P_1,\cdots,P_n$ 各自的私有图 $G_1,\cdots,G_n$.

输出: n 个图的交集: $G = G_1 \cap \cdots \cap G_n$.

(1) 在具有加法同态性的 Lifted-ElGamal 门限密码系统中, 参与者 $P_1, \cdots, P_n$ 选择各自的私钥 sk_i, 并联合生成公钥 h.

(2) P_1 按照编码方式 1 将图 G_1 转化成存储矩阵 M_1, 取 M_1 对角线及其以下元素 (共 $t = \frac{m(m+1)}{2}$ 个), 构成向量 $X_1 = (x_{11}, \cdots, x_{1t})$, 将 $E(X_1) = (E(x_{11}), \cdots, E(x_{1t}))$ 发送给 P_2.

(3) 令 $c = (c_1, \cdots, c_t) = (E(x_{11}), \cdots, E(x_{1t}))$.

(4) 参与者 $P_i (i = 2, \cdots, n)$ 计算如下:

For $i = 2$ to $n-1$

P_i computes

$E(x_{i-1,k}) \leftarrow E(x_{i,k})$ ($k = l$, where $x_{il} = 0$)

$(c_1, \cdots, c_t) \leftarrow (E'(x_{i-1,1}), \cdots, E(x_{i-1,k}), \cdots, E'(x_{i-1,t}))$

sends to P_{i+1}

End

P_n computes

$E(x_{n-1,k}) \leftarrow E(x_{n,k})$ ($k = l$, where $x_{nl} = 0$)

$(c_1, \cdots, c_t) \leftarrow (E'(x_{n-1,1}), \cdots, E(x_{n-1,k}), \cdots, E'(x_{n-1,t}))$

其中 E' 表示对原有密文进行重随机化后的密文, 若无特别说明, 下文中 E' 所表示内容均与此处相同.

(5) 计算图交集的过程如下:

$P_1, \cdots, P_n$ 联合解密 $Y = D(c)$, 根据 Y 还原出图交集的存储矩阵 M, 根据 M 和编码方式 1 的规则, 进一步还原出 n 个图的交集 G.

Output G

3.4 协议的正确性

协议 1 是正确的意味着对于任意输入的图 G_i (G_0 的子图, $1 \le i \le n$), 能正确求出 n 个图的交集 G, 协议 1 的正确性可由 3.2 节所述计算原理保证. 具体地, 如果某个顶点或者某条边在 n 个图中均存在, 则每个图 G_i 转换后的向量 X_i 中, 对应该顶点或边的分量值为 1. 在保密替换的过程中, 始终是用后者向量中的 "0" 替换前者对应位置的分量, 相当于将非交集中的所有元素表示成了 "0", 而那些任意向量 X_i 中值均为 1 的分量, 则被保留了下来, 替换过程仅仅是对其进行了重随机化, 根据保密替换完成后的最终向量, 即可恢复出交集图 G. 因此, 协议 1 是正确的.

3.5 协议的安全性

门限解密方案的安全性可以为协议 1 提供安全性保证. 由于门限 ElGamal 公钥系统的公钥是由所有参与者共同产生的, 即 $h \equiv g^{\sum_{i=1}^{n} \mathrm{sk}_i} \bmod p$, 其中 sk_i 是参与者 P_i 所持有的私钥碎片, 因此解密需要所有参与者合作才能完成. 由概率门限加密算法的语义安全性可知, 若没有全部参与者合作解密, 那么每个参与者产生的密文对其他任一参与者来说都是计算不可区分的. 因此, 只要任一参与者不参与合谋, 对其余 $n-1$ 个参与者来说, 它们执行协议时得到的 view 与用满足图交集不变的任一组输入进行模拟相比, 最终所得信息序列在计算上是不可区分的, 也就是说协议 1 可以抵抗合谋攻击.

定理 1 基于门限解密的多个图交集的保密计算协议 1 是安全的, 能抵抗任意程度的合谋攻击.

证明: 任意 $n-1$ 个参与者构成的合谋者集合, 可以产生最大程度的合谋攻击, 因此只需证明协议 1 对此合谋者结构是安全的, 则对于其他任意程度的合谋攻击都是安全的. 对于任意 $n-1$ 个参与者构成的合谋者集合 I, 构造相应的模拟器 S, 使得式 (1) 成立. 由于各参与者地位的平等性, 不妨设 $I = \{P_2, \cdots, P_n\}$, 他们试图合谋想获取 P_1 的私密图 G_1, P_1 不参与合谋, $P_2, \cdots, P_n$ 对于 P_1 的密文信息 $E(X_1) = (E(x_{11}), E(x_{12}), \cdots, E(x_{1t}))$ 无法正确解密, 根据加密方案的语义安全性可知, $E(X_1) = (E(x_{11}), \cdots, E(x_{1t}))$ 和 t 个随机数是计算不可区分的, 在此情况下:

$$I = \{P_2, \cdots, P_n\}, X = \{G_1, \cdots, G_n\}$$

$$f(X)=f_I(X)=\{G_1\cap G_2\cap\cdots\cap G_n\}$$
$$\{\mathrm{view}_I^{\Pi}(X)\}_{X\in(\{0,1\}^*)^n}=(I,\mathrm{view}_2^{\Pi}(X),\cdots,\mathrm{view}_n^{\Pi}(X))=\{I,G_2,R_2,E(X_1),\cdots,G_n,R_n,E(X_n),f_I(X)\}$$

给定输入 $(I,(G_2,\cdots,G_n),f_I(X))$, S 随机选择 $G_1'(G_0$ 的子图), 使得:

$$\begin{aligned}f(X')&=f_I(G_1',G_2,\cdots,G_n)=\{G_1'\cap G_2\cap\cdots\cap G_n\}\\&=f_I(X)=f(G_1,G_2,\cdots,G_n)=\{G_1\cap G_2\cap\cdots\cap G_n\}\end{aligned}$$

用 $G_1',G_2,\cdots,G_n$ 进行模拟, 首先按规则构造向量 X_1' 并加密得到 $E(X_1')=(E(x_{11}'),\cdots,E(x_{1t}'))$, 模拟器 S 按照协议要求进行替换操作, 最后解密出最终向量 $E(X_n')$ 得到

$$f_I(G_1',G_2,\cdots G_n)=\{G_1'\cap G_2\cap\cdots\cap G_n\}$$

令

$$S(I,(G_2,\cdots,G_n),f_I(X))=\{I,G_2,R_2,E(X_1'),\cdots,G_n,R_n,E(X_n),f_I(X')\}$$

因为所选用的概率加密方案是语义安全的, 所以 $E(X_1)\stackrel{c}{\equiv}E(X_1')$ 且 $f_I(X)=f_I(X')$, 故

$$\{S(I,(G_2,\cdots,G_n),f_I(X))\}_{X\in(\{0,1\}^*)^n}\stackrel{c}{\equiv}\{\mathrm{view}_I^{\Pi}(X)\}_{X\in(\{0,1\}^*)^n}$$

因此对于 G_1 是安全的. □

4 基于门限解密的多个图并集的保密计算

4.1 问题描述

假设顶点集 V 和边集 E 构成一个无向完全图 $G_0=(V,E)(\frac{m(m-1)}{2}$ 条边), 其中 $V=\{v_1,v_2,\cdots,v_m\}$. 参与者 $P_1,P_2,\cdots,P_n$ 分别拥有 G_0 的子图 $G_1,G_2,\cdots,G_n$, 他们想保密求 n 个图的并集而不泄露各自信息.

4.2 计算原理

根据编码方法 1, n 个参与者先生成各自图的存储矩阵 $M_1,M_2,\cdots,M_n$, 再分别将矩阵中对角线及以下元素构成分量个数均为 $t=\frac{m(m+1)}{2}$ 的向量 $X_1,X_2,\cdots,X_n$. 要计算两个图 G_1,G_2 的并集, 只需参与者 P_2 用自己向量 X_2 中值为 1 的分量去替换对应位置的 X_1 中分量即可, X_1 中其余分量则保持不变. 可以看出, 若某个顶点或者边是 G_1,G_2 并集中的元素, 则替换之后 P_2 得到的新向量 X_2 中, 对应该顶点或边的分量值为 1; 反之, 该位置的值仍为 0. 将替换后的向量 X_2 还原成 $m\times m$ 矩阵的下三角部分, 即第 i 行具有 i 个元素的下三角矩阵 $(1\le i\le m)$(上三角部分为空), 再以对角线为对称轴还原出另一半的上三角部分, 即为 G_1,G_2 并集的存储矩阵, 根据存储矩阵就可以知道具体的图. 以此类推, 参与者 P_i 可以通过用向量 X_i 中值为 1 的分量去替换 X_{i-1} 中的对应分量, X_{i-1} 中其余分量保持不变, 然后根据替换后得到的 X_i 还原出 i 个图并集的存储矩阵, 进而得到 i 个图的并集.

例如, 上例中 P_1,P_2,P_3,P_4 分别拥有图 G_1,G_2,G_3,G_4, 根据编码方式 1, 生成各自的存储矩阵 M_1,M_2,M_3,M_4, 然后 P_1,P_2,P_3,P_4 分别将 M_1,M_2,M_3,M_4 中对角线以及以下元素依次连接, 构成具有 $\frac{6\times(6+1)}{2}=21$ 个分量的向量:

$$X_1=(1,0,0,1,0,1,0,0,1,1,1,0,1,0,1,0,0,0,0,0,0)$$
$$X_2=(0,0,1,0,1,1,0,1,1,1,0,0,0,1,1,0,1,1,1,0,1)$$
$$X_3=(1,0,0,1,0,1,1,0,1,1,0,0,0,0,0,0,0,0,0,0,0)$$
$$X_4=(0,0,1,0,0,1,0,1,1,1,0,0,0,0,0,0,0,1,0,0,1)$$

那么, 经过 P_2 替换后, 得到新向量

$$X_2 = (1,0,1,1,1,1,0,1,1,1,1,0,1,1,1,0,1,1,1,0,1)$$

经过 P_3 替换后,

$$X_3 = (1,0,1,1,1,1,1,1,1,1,1,0,1,1,1,0,1,1,1,0,1)$$

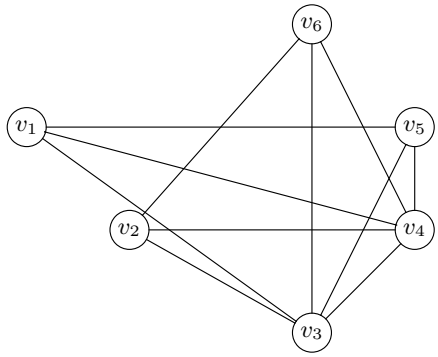
经过 P_4 替换后,

$$X_4 = (1,0,1,1,1,1,1,1,1,1,1,0,1,1,1,0,1,1,1,0,1)$$

最后, 根据 X_4 可以还原出一个 6×6 矩阵的下三角部分, 即第 i 行具有 i 个元素的下三角矩阵 $(1\le i\le 6)$, 再以对角线为对称轴还原出另一半的上三角矩阵, 即为 G_1, G_2, G_3, G_4 并集的存储矩阵 M^*:

$$M^* = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}$$

根据存储矩阵就可以知道具体的图 G^*:



G^*

以上方案就是本文计算多个图并集的基本原理. 本文利用 Lifted-ElGamal 门限密码系统构造一个抗合谋攻击的图并集的安全多方计算协议. 对向量中的 0 和 1 进行概率加密, 使得任何参与者都无法分辨出向量中的 0 与 1. 在每个参与者完成密文替换的操作后, 将未替换过的密文进行重随机化来保证协议的安全性.

4.3 抗合谋攻击的多个图并集的保密计算

协议 2 基于门限解密的多个图并集保密计算协议.

输入: $P_1,\cdots,P_n$ 各自的私有图 $G_1,\cdots,G_n$.

输出: n 个图的并集: $G^* = G_1\cup\cdots\cup G_n$.

(1) 在具有加法同态性的 Lifted-ElGamal 门限密码系统中, 参与者 $P_1,\cdots,P_n$ 选择各自的私钥 sk_i, 并联合生成公钥 h.

(2) P_1 按照编码方式 1 将图 G_1 转化成存储矩阵 M_1, 取 M_1 对角线及其以下元素 (共 $t=\frac{m(m+1)}{2}$ 个), 构成 $X_1=(x_{11},\cdots,x_{1t})$, 将 $E(X_1)=(E(x_{11}),\cdots,E(x_{1t}))$ 发送给 P_2.

(3) 令 $c=(c_1,\cdots,c_t)=(E(x_{11}),\cdots,E(x_{1t}))$.

(4) 参与者 $P_i(i=2,\cdots,n)$ 计算如下:

For $i=2$ to $n-1$

P_i computes

$E(x_{i-1,k}) \leftarrow E(x_{i,k})$ ($k=l$, where $x_{il}=1$)

$(c_1,\cdots,c_t) \leftarrow (E'(x_{i-1,1}),\cdots,E(x_{i-1,k}),\cdots,E'(x_{i-1,t}))$

sends to P_{i+1}

End

P_n computes

$E(x_{n-1,k}) \leftarrow E(x_{n,k})$ ($k=l$, where $x_{nl}=1$)

$(c_1,\cdots,c_t) \leftarrow (E'(x_{n-1,1}),\cdots,E(x_{n-1,k}),\cdots,E'(x_{n-1,t}))$

(5) 计算图并集的过程如下:

$P_1,\cdots,P_n$ 联合解密 $Y=D(c)$, 根据 Y 还原出图并集的存储矩阵 M^*, 根据 M^* 和编码方式 1 的规则, 进一步还原出并集 G^*.

Output G^*

4.4 协议的正确性

协议 2 是正确的意味着对于任意输入的图 $G_i(G_0$ 的子图, $1\le i\le n)$, 能正确求出 n 个图的并集 G^*, 协议 2 的正确性可由 4.2 节所述计算原理保证. 具体地, 如果某个顶点或者某条边是 n 个图并集中的元素, 则至少存在一个图 G_i, 其转换后的向量 X_i 中对应该顶点或边的分量值为 1. 在保密替换的过程中, 始终是用后者向量中的 "1" 替换前者对应位置的分量, 相当于将并集中的所有元素表示成了 "1". 而在任意向量 X_i 中值均为 0 的分量, 仅对其进行了重随机化, 根据保密替换完成后的最终向量, 即可恢复出并集图 G^*. 因此, 协议 2 是正确的.

4.5 协议的安全性

门限解密方案的安全性可以为协议 2 提供安全性保证. 由于门限 ElGamal 公钥系统的公钥是由所有参与者共同产生的, 即 $h\equiv g^{\sum_{i=1}^{n}\mathrm{sk}_i} \bmod p$, 其中 sk_i 是参与者 P_i 所持有的私钥碎片, 因此解密需要所有参与者合作才能完成. 由概率门限加密算法的语义安全性可知, 若没有全部参与者合作解密, 那么每个参与者产生的密文对其他任一参与者来说都是计算不可区分的. 因此, 只要任一参与者不参与合谋, 对其余 $n-1$ 个参与者来说, 它们执行协议时得到的 view 与用满足图并集不变的任一组输入进行模拟相比, 最终所得信息序列在计算上是不可区分的, 也就是说协议 2 可以抵抗合谋攻击.

定理 2 基于门限解密的多个图并集的保密计算协议 2 是安全的, 能抵抗任意程度的合谋攻击.

证明: 任意 $n-1$ 个参与者构成的合谋者集合, 可以产生最大程度的合谋攻击, 因此只需证明协议 2 对此合谋者结构是安全的, 则对于其他任意程度的合谋攻击都是安全的. 对于任意 $n-1$ 个参与者构成的合谋者集合 I, 构造相应的模拟器 S, 使得式 (1) 成立. 由于各参与者地位的平等性, 不妨设 $I=\{P_2,\cdots,P_n\}$, 他们试图合谋想获取 P_1 的私密图 G_1, P_1 不参与合谋, $P_2,\cdots,P_n$ 对于 P_1 的密文信息 $E(X_1)=(E(x_{11}),E(x_{12}),\cdots,E(x_{1t}))$ 无法正确解密, 根据加密算法的语义安全性可知, $E(X_1)=(E(x_{11}),\cdots,E(x_{1t}))$ 和 t 个随机数是计算不可区分的, 在此情况下:

$$I=\{P_2,\cdots,P_n\}, X=\{G_1,\cdots,G_n\}, f(X)=f_I(X)=\{G_1\cup G_2\cup\cdots\cup G_n\}$$

$$\{\mathrm{view}_I^{\Pi}(X)\}_{X\in(\{0,1\}^*)^n}=(I,\mathrm{view}_2^{\Pi}(X),\cdots,\mathrm{view}_n^{\Pi}(X))=\{I,G_2,R_2,E(X_1),\cdots,G_n,R_n,E(X_n),f_I(X)\}$$

给定输入 $(I,(G_2,\cdots,G_n),f_I(X))$, S 随机选择 $G_1'(G_0$ 的子图), 使得:

$$\begin{aligned} f(X') &= f_I(G_1',G_2,\cdots,G_n)=\{G_1'\cup G_2\cup\cdots\cup G_n\} \\ &= f_I(X)=f(G_1,G_2,\cdots,G_n)=\{G_1\cup G_2\cup\cdots\cup G_n\} \end{aligned}$$

用 $G_1',G_2,\cdots,G_n$ 进行模拟, 首先按规则构造向量 X_1' 并加密得到 $E(X_1')=(E(x_{11}'),\cdots,E(x_{1t}'))$,

模拟器 S 按照协议要求进行替换操作, 最后解密出最终向量 $E(X'_n)$ 得到

$$f_I(G'_1, G_2, \cdots G_n) = \{G'_1 \cup G_2 \cup \cdots \cup G_n\}$$

令

$$S(I, (G_2, \cdots, G_n), f_I(X)) = \{I, G_2, R_2, E(X'_1), \cdots, G_n, R_n, E(X_n), f_I(X')\}$$

因为所选用的概率加密方案是语义安全的, 所以 $E(X_1) \stackrel{c}{\equiv} E(X'_1)$ 且 $f_I(X) = f_I(X')$, 故

$$\{S(I, (G_2, \cdots, G_n), f_I(X))\}_{X \in (\{0,1\}^*)^n} \stackrel{c}{\equiv} \{\mathrm{view}_I^{\Pi}(X)\}_{X \in (\{0,1\}^*)^n}$$

因此对于 G_1 是安全的. □

5 性能分析

5.1 理论分析与比较

本节将本文方案与相关文献方案的效率进行对比. 由于目前关于图的交集保密计算问题仅有文献 [31] 中的方案, 尚无关于图的并集的保密计算问题的研究, 且本文计算图的交集和并集的计算复杂性基本相同, 因此将协议 1 与文献 [31] 进行比较.

计算复杂性分析 由于文献 [31] 使用了 Paillier 加密方案, 本文协议使用了 ElGamal 加密方案, 因此以开销较大的模指数运算次数作为衡量计算开销的指标, 其他忽略不计. 用 M_P 表示 Paillier 加密方案中的模指数运算, 用 M_E 表示 ElGamal 加密方案中的模指数运算.

文献 [31] 首先调用了文献 [32] 的 FNP 协议作为子协议来计算图顶点的交集. 假设文献 [31] 中服务器和客户端的图均有 m 个顶点, 顶点集分别为 $V_S = \{v_{s_1}, \cdots, v_{s_m}\}$, $V_c = \{v_{c_1}, \cdots, v_{c_m}\}$, 服务器根据每个顶点构造多项式 $P(x) = \sum_{u=0}^{m} \alpha_u x^u$, 需加密 $m+1$ 个系数, Paillier 算法加密一次需要 2 次模指数运算, 因此需要 $2(m+1)$ 次模指数运算; 客户端将自己的 m 个顶点代入 $P(x)$ 共需 m^2 次模指数运算, 对于每个 $E(P(v_{c_i}))$, 客户端选择随机数 r 计算 $E(rP(v_{c_i}) + v_{c_i})$, 该操作共需 $3m$ 次模指数运算; 服务器解密 m 个密文, 由于 Paillier 解密一次需要 2 次模指数运算, 因此共需 $2m$ 次模指数运算. 所以, 文献 [31] 调用文献 [32] 的 FNP 协议操作共需 $m^2 + 7m + 2$ 次模指数运算. 接下来, 文献 [31] 中服务器加密 $m \times m$ 矩阵共需 $2m^2$ 次模指数运算; 客户端对两矩阵进行同态运算共需 m^2 次模指数运算, 最后服务器对秘密矩阵进行解密需要 $2m^2$ 次模指数运算. 综上, 文献 [31] 计算两个图的交集协议共需 $6m^2 + 7m + 2$ 次模指数运算.

协议 1 中, 所有参与者合作产生公钥 $h = g^{\mathrm{sk}_1 + \cdots + \mathrm{sk}_n} \bmod p$ (p 代表 Lifted-ElGamal 加密系统中的公开参数), 共需要 n 次模指数运算. 加密过程中, n 个参与者最多共需要 $2nt$ 次模指数运算; 联合解密过程最多需要 nt 次模指数运算. 因此在有 n 个参与者的情况下, 协议 1 最多需要 $n(3t+1)$ 次模指数运算, 其中 $t = \frac{m(m+1)}{2}$, 即 $(\frac{3n}{2}m^2 + \frac{3n}{2}m)$ 次模指数运算. 当只有两个参与者时不需考虑合谋问题, ElGamal 加密算法即可实现, 则协议 1 加密解密仅需 $5t$ 次模指数运算, 即 $(\frac{5}{2}m^2 + \frac{5}{2}m)$ 次模指数运算.

通信复杂性分析 衡量安全多方计算协议的通信复杂性, 通常选择通信次数或通信传输的数据的比特数作为指标 (由于在每种密码体制下的每个密文比特数的平均值是确定的, 所以也可以用传输的密文个数来衡量), 我们从这两方面将文献 [31] 方案与本文方案进行分析比较. 文献 [31] 首先调用 FNP 协议求得两图顶点的交集, 在此过程中, 服务器将多项式 $P(x) = \sum_{u=0}^{m} \alpha_u x^u$ 加密发送给客户端, 传输 $m+1$ 个系数密文, 客户端将自己顶点集合元素带入 $P(X)$ 并运算后再发给服务器, 传输 m 个密文, 该过程共需要通信 2 次, 传输密文 $2m+1$ 个; 接下来, 服务器将 $m \times m$ 密文矩阵发送给客户端, 需传输 m^2 个密文, 客户端对矩阵每个元素进行同态运算后再传输给服务器, 也传输 m^2 个密文, 该过程共需要通信 2 次, 传输密文 $2m^2$ 个. 因此文献 [31] 总共需要通信 4 次, 传输密文 $2m^2 + 2m + 1$ 个.

当考虑两个参与者的情况, 本文协议 1 则不需构造门限, 只需 P_1 将向量加密发送给 P_2, P_2 完成密文替换和重随机化操作后再发给 P_1, 该过程总共需要通信 2 次, 传输密文 $2t$ 个, 其中 $t = \frac{m(m+1)}{2}$, 即传输

密文 m^2+m 个.

当考虑 n 个参与者的情况, 本文协议 1 中 n 个参与者首先构造门限, 总共需要通信 $n-1$ 次, 传输密文 $n-1$ 个; 加密和替换过程, 每个参与者将向量按规则处理后发送给下一个参与者, 每次需传输 t 个密文, 该过程共需通信 $n-1$ 次, 传输密文 $t(n-1)$ 个; 联合解密过程每次需传输 t 个密文, 该过程共需通信 $n-1$ 次, 传输密文 $t(n-1)$ 个. 因此协议 1 共需要通信 $3(n-1)$ 次, 传输密文 $2(t+1)(n-1)$ 个, 即传输密文 $(n-1)m^2+(n-1)m+n-1$ 个.

综合以上分析, 得到本文方案与文献 [31] 方案的对比如表 1.

表 **1**　本文方案与现有方案的比较

Table 1　Comparison between scheme in this paper and existing schemes

	计算开销	通信开销	通信次数
文献 [31] (两方)	$6m^2+7m+2$ M_P	$2m^2+2m+1$	4
协议 1 (两方)	$\frac{5}{2}m^2+\frac{5}{2}m$ M_E	m^2+m	2
协议 1 (n 方)	$\frac{3n}{2}m^2+\frac{3n}{2}m$ M_E	$(n-1)m^2+(n-1)m+n-1$	$3(n-1)$

从表 1 可以看出, 当研究两个参与者的情况时, 文献 [31] 在计算复杂性和通信复杂度两方面均高于本文协议. 且文献 [31] 仅限于研究两个参与者的情况, 而本文设计的两个协议则均可扩展至多个参与者的情况, 并且能够抵抗任意程度的合谋攻击.

5.2　实验测试

本文通过模拟实验测试执行文献 [31] 方案与本文协议 1 所用时间, 以此验证并对比各方案的效率.

实验模拟　本文的试验测试环境: Windows 10 64 位操作系统, 处理器是 Intel(R) Core(TM) i5-6600 CPU@3.30 GHZ, 内存是 8 GB, 用 JAVA 语言编程实现. 本文协议 1 在两方情况下使用的 ElGamal 加密系统, 素数 p 设为 512 比特, 在文献 [31] 协议中使用的 Paillier 加密系统, 两个素数 p,q 设为 256 比特. 实验以保密求两个图的交集为例, 测试在同一组参数下, 文献 [31] 方案与本文协议 1 在最坏情况下求图的交集所需时长 (仅考虑加密与解密过程所耗费的时间), 其中每组图的顶点数分别设置为 $m=10,20,\cdots,100$. 为了保证数据的准确性, 我们对每组参数设定值进行 100 次模拟实验, 取实验结果的平均值, 实验结果如图 1 所示.

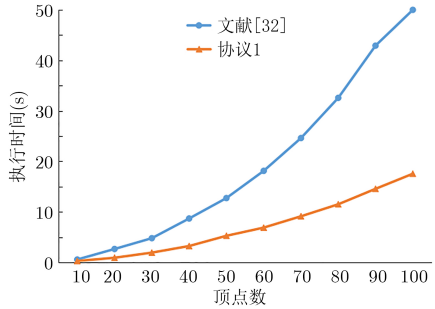


图 1　保密求两图交集的执行时间随图的顶点数增长的变化规律

Figure 1　Rule of execution time of privately computing intersection of two graphs with growth of vertex number of graphs

为进一步提高安全等级, 将协议 1 的 ElGamal 加密系统的素数 p 取为安全素数 (即 $p=rq+1$, q 是一个大素数), 即令 p 为 3072 比特, q 为 256 比特, 选取阶数为 q 的生成元 g. 文献 [31] 协议中使用的 Paillier 加密系统, 两个素数 p,q 取为 1536 比特, 随机数的取值范围不变, 实验结果如图 2 所示.

实验结果　对于两图交集的保密计算问题, 本文协议 1 将图做了简化表示成向量, 加密和解密过程的数据量不大, 且使用了效率较高的 ElGamal 加密方案, 而文献 [31] 的方案调用的子协议复杂, 对图的加密和解密量也很大, 使用的 Paillier 加密方案效率相对低. 从图 1 和图 2 可以看出, 无论在何种安全等级下, 文

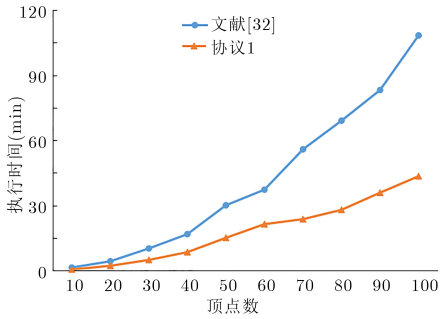


图 2 更高安全等级下保密求两图交集的执行时间随图的顶点数增长的变化规律

Figure 2 Rule of execution time of privately computing intersection of two graphs with growth of vertex number of graphs at a higher level of security

献 [31] 协议的执行时间都明显高于本文协议 1, 且随着图的顶点数增大, 文献 [31] 协议执行时间的增长速度也明显较本文协议 1 更快.

6 结论

图结构数据的安全多方计算是一个新的研究领域. 本文提出了一种新的编码方法来存储图, 以新编码方法和门限解密方案为基础, 并结合密文替换和密文重随机化的方法, 分别设计了图交集和并集的安全多方计算协议, 且只需稍加修改就能用于两方参与者的情况. 我们应用模拟范例严格证明了本文协议在半诚实模型下都是安全的, 可以抵抗任意程度的合谋攻击. 在今后的研究中, 我们将致力于更高效的图的交集、并集问题的解决方案, 以及更多具有重要意义的图论问题的安全多方计算, 并尝试开展对恶意模型下图论问题的安全多方计算研究.

参考文献

[1] YANG J, ZHAO J S, ZHANG J P. A privacy preservation method for high dimensional data mining[J]. Acta Electronica Sinica, 2013, 41(11): 2187–2192. [DOI: 10.3969/j.issn.0372-2112.2013.11.012]
杨静, 赵家石, 张健沛. 一种面向高维数据挖掘的隐私保护方法 [J]. 电子学报, 2013, 41(11): 2187–2192. [DOI: 10.3969/j.issn.0372-2112.2013.11.012]

[2] SAMANTHULA B K, ELMEHDWI Y, HOWSER G, et al. A secure data sharing and query processing framework via federation of cloud computing[J]. Information Systems, 2015, 48(3): 196–212. [DOI: 10.1016/j.is.2013.08.004]

[3] CAMPOS R, DIAS G, JORGE A M, et al. Survey of temporal information retrieval and related applications[J]. ACM Computing Surveys (CSUR), 2015, 47(2): 1–14. [DOI: 10.1145/2619088]

[4] KERSCHBAUM F. Privacy-preserving computation[C]. In: Privacy Technologies and Policy—APF 2012. Springer Berlin Heidelberg, 2014: 41–54. [DOI: 10.1007/978-3-642-54069-1_3]

[5] YAO A C. Protocols for secure computations[C]. In: Proceeding of the 23th IEEE Annual Symposium on Foundations of Computer Science. IEEE Computer Science Press, 1982: 160–164. [DOI: 10.1109/SFCS.1982.38]

[6] GOLDREICH O. Foundations of Cryptography: Basic Applications[M]. London: Cambridge University Press, 2004: 599–729. [DOI: 10.1093/logcom/exi020]

[7] BEN-OR M, GOLDWASSER S, WIGDERSON A. Completeness theorems for non-cryptographic fault-tolerant distributed computation[C]. In: Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing. ACM, 1988: 1–10. [DOI: 10.1145/62212.62213]

[8] YASIN S, HASEEB K, QURESHI R J. Cryptography based e-commerce security: A review[J]. International Journal of Computer Science Issues, 2012, 9(2): 132–137.

[9] VISHAKHA M, SHARMA R. Review paper on cryptography[J]. International Journal of Research, 2015, 2(5): 141–142.

[10] KUMAR S N. Review on network security and cryptography[J]. Science and Education, 2015, 3(1): 1–11.

[11] GOLDWASSER S. Multi-party computations: Past and present[C]. In: Proceedings of the 16th Annual ACM Symposium on Principles of Distributed Computing. ACM, 1997: 1–6. [DOI: 10.1145/259-380.259405]

[12] LI S D, WANG D S. Efficient secure multiparty computation based on homomorphic encryption[J]. Acta Elec-

tronica Sinica, 2013, 41(4): 798–803. [DOI: 10.3969/j.issn.0372-2112.2013.04.029]
李顺东, 王道顺. 基于同态加密的高效多方保密计算 [J]. 电子学报, 2013, 41(4): 798–803. [DOI: 10.3969/j.issn.0372-2112.2013.04.029]
[13] GRIGORIEV D, SHPILRAIN V. Yao's millionaires' problem and decoy-based public key encryption by classical physics[J]. International Journal of Foundations of Computer Science, 2014, 25(4): 409–417. [DOI: 10.1142/S0129054114400036]
[14] KARIMIAN A N. Efficient Non-interactive Secure Two-party Computation for Equality and Comparison[D]. Calgary, AB, Canada: University of Calgary, 2015.
[15] LI S D, GUO Y M, ZHOU S F, et al. Efficient protocols for the general millionaires' problem[J]. Chinese Journal of Electronics, 2017, 26(4): 696–702. [DOI: 10.1049/cje.2017.06.014]
[16] YANG X L, LI S D, ZUO X J. Secure multi-party geometry computation[J]. Journal of Cryptologic Research, 2016, 3(1): 33–41. [DOI: 10.13868/j.cnki.jcr.000107]
杨晓莉, 李顺东, 左祥建. 计算几何问题的多方保密计算 [J]. 密码学报, 2016, 3(1): 33–41. [DOI: 10.13868/j.cnki.jcr.000107]
[17] DU W, ATALLAH M J. Secure multi-party computation problems and their applications: A review and open problems[C]. In: Proceedings of the 2001 Workshop on New Security Paradigms. ACM, 2001: 13–22. [DOI: 10.1145/508171.508174]
[18] LI S D, WU C Y, WANG D S, et al. Secure multiparty computation of solid geometric problems and their applications[J]. Information Sciences, 2014, 282: 401–413. [DOI: 10.1016/j.ins.2014.04.004]
[19] LIU L, CHEN X F, LOU W J. Secure three-party computational protocols for triangle area[J]. International Journal of Information Security, 2016, 15(1): 1–13. [DOI: 10.1007/s10207-015-0284-y]
[20] DU W L, ATALLAH M J. Privacy-preserving cooperative statistical analysis[C]. In: Proceedings of the 17th Annual Conference of Computer Security Applications. IEEE, 2001: 102–110. [DOI: 10.1109/ACSAC.2001.991526]
[21] JAWUREK M, KERSCHBAUM F. Fault-tolerant privacy-preserving statistics[C]. In: Privacy Enhancing Technologies—PETS 2012. Springer Berlin Heidelberg, 2012: 221–238. [DOI: 10.1007/978-3-642-31680-7_12]
[22] YANG B W, LI M Y, TANG W Q, et al. Dynamic network biomarker indicates pulmonary metastasis at the tipping point of hepatocellular carcinoma[J]. Nature Communications, 2018, 9(1): 1–14. [DOI: 10.1038/s41467-018-03024-2]
[23] WEI Y H, YILDIRIM P, Bulte C V D, et al. Credit scoring with social network data[J]. Marketing Science, 2015, 35(2): 234–258. [DOI: 10.2139/ssrn.2475265]
[24] PARTNER I J. Data protection in the United States: Overview[OL]. http://us.practicallaw.com/6-502-0467
[25] KUKKALA V B, IYENGAR S R S, SAINI J S. Secure multiparty graph computation[C]. In: Proceedings of the 8th International Conference on Communication Systems and Networks (COMSNETS). IEEE, 2016: 1–2. [DOI: 10.1109/COMSNETS.2016.7439973]
[26] AKAVIA A, MORAN T. Topology-hiding computation beyond logarithmic diameter[C]. In: Advances in Cryptology—EUROCRYPT 2017, Part III. Springer Cham, 2017: 609–637. [DOI: 10.1007/978-3-319-56617-7_21]
[27] ZHENG Y, WANG B, LOU W, et al. Privacy-preserving link prediction in decentralized online social networks[C]. In: Computer Security—ESORICS 2015, Part II. Springer Cham, 2015: 61–80. [DOI: 10.1007/978-3-319-24177-7_4]
[28] ALY A, CUVELIER E, MAWET S, et al. Securely solving simple combinatorial graph problems[C]. In: Financial Cryptography and Data Security—FC 2013. Springer Berlin Heidelberg, 2013: 239–257. [DOI: 10.1007/978-3-642-39884-1_21]
[29] FRIKKEN K B, GOLLEN P. Private social network analysis: How to assemble pieces of a graph privately[C]. In: Proceedings of the 5th ACM Workshop on Privacy in Electronic Society. ACM, 2006: 89–98. [DOI: 10.1145/1179601.1179619]
[30] MANDAL K, ALOMAIR B, POOVENDRAN R. Secure error-tolerant graph matching protocols[C]. In: Cryptology and Network Security—CANS 2016. Springer Cham, 2016: 265–283. [DOI: 10.1007/978-3-319-48965-0_16]
[31] ZHOU F, XU Z F, LI Y X, et al. Private graph intersection protocol[C]. In: Information Security and Privacy—ACISP 2017, Part II. Springer Cham, 2017: 235–248. [DOI: 10.1007/978-3-319-59870-3_13]
[32] FREEDMAN M J, NISSIM K, PINKAS B. Efficient private matching and set intersection[C]. In: Advances in Cryptology—EUROCRYPT 2004. Springer Berlin Heidelberg, 2004: 1–19. [DOI: 10.1007/978-3-540-24676-3_1]
[33] YANG X Y, LI S D, KANG J. Private replacement and its applications in scientific computation[J]. Chinese Journal of Computers, 2018, 41(5): 1132–1142. [DOI: 10.11897/SP.J.1016.2018.01132]
杨晓艺, 李顺东, 亢佳. 保密替换及其在保密科学计算中的应用 [J]. 计算机学报, 2018, 41(5): 1132–1142. [DOI: 10.11897/SP.J.1016.2018.01132]

[34] DESMEDT Y, RANKEL Y. Threshold cryptosystems[C]. In: Advances in Cryptology—CRYPTO '89. Springer New York, 1990: 307–315. [DOI: 10.1007/3-540-57220-1_47]
[35] LONG Y, CHEN K, MAO X. New constructions of dynamic threshold cryptosystem[J]. Journal of Shanghai Jiaotong University (Science), 2014, 19(4): 431–435. [DOI: 10.1007/s12204-014-1520-8]
[36] FREEDMAN M, HAZAY C, NISSIM K, et al. Efficient set intersection with simulation-based security[J]. Journal of Cryptology, 2016, 29(1): 115–155. [DOI: 10.1007/s00145-014-9190-0]
[37] PAILLIER P. Public-key cryptosystems based on composite degree residuosity classes[C]. In: Advances in Cryptology—EUROCRYPT '99. Springer Berlin Heidelberg, 1999: 223–238. [DOI: 10.1007/3-540-48910-X_16]

作者信息



魏琼 (1994–), 陕西渭南人, 硕士研究生. 主要研究领域为密码学与信息安全.
weiqiong@snnu.edu.cn



李顺东 (1963–), 河南平顶山人, 教授, 博士生导师. 主要研究领域为密码学与信息安全.
shundong@snnu.edu.cn



王文丽 (1991–), 河南周口人, 博士研究生. 主要研究领域为密码学与信息安全.
wenliwang@snnu.edu.cn



杜润萌 (1994–), 山西永济人, 硕士研究生. 主要研究领域为密码学与信息安全.
durunmeng@snnu.edu.cn