软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2022,33(5):1907−1921 [doi: 10.13328/j.cnki.jos.006206]

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

向量等分量数的保密计算及应用*

窦家维[1], 陈明艳[1], 成 雯[2]

[1](陕西师范大学 数学与信息科学学院, 陕西 西安 710119)

[2](陕西师范大学 计算机科学学院, 陕西 西安 710119)

通信作者: 窦家维, E-mail: jiawie@snnu.edu.cn

摘 要: 随着信息技术的快速发展, 在保护数据隐私的条件下进行多方合作计算变得越来越普及, 安全多方计算已经成为解决这类保密计算问题的核心技术. 向量的保密计算是安全多方计算的重要研究方向, 目前有很多研究成果, 包括保密计算向量的点积, 保密的向量求和等. 但关于保密计算向量等分量数的研究成果还很少, 且主要研究向量分量在有全集限制下的两方保密计算问题. 主要研究多方参与者隐私向量的等分量数以及相关阈值的安全计算问题. 首先针对向量设计了分量-矩阵编码方法, 结合 ElGamal 门限加密系统, 构造了多方向量等分量数保密计算协议. 进一步以向量等分量数保密计算协议为基础, 研究设计了多方向量等分量数阈值问题保密计算协议. 所有向量分量没有全集的限制. 应用模拟范例方法对文中所有协议的安全性进行了严格证明. 效率分析和实验验证表明设计的协议是简单高效的. 最后, 将所设计的协议应用于解决一些实际安全计算问题.

关键词: 密码学; 安全多方计算; 向量等分量数; 同态加密; 编码方法

中图法分类号: TP309

中文引用格式: 窦家维, 陈明艳, 成雯. 向量等分量数的保密计算及应用. 软件学报, 2022, 33(5): 1907–1921. http://www.jos.org.cn/1000-9825/6206.htm

英文引用格式: Dou JW, Chen MY, Cheng W. Securely Computing Equal Components of Private Vectors and Its Applications. Ruan Jian Xue Bao/Journal of Software, 2022, 33(5): 1907–1921 (in Chinese). http://www.jos.org.cn/1000-9825/6206.htm

Securely Computing Equal Components of Private Vectors and Its Applications

DOU Jia-Wei[1], CHEN Ming-Yan[1], CHENG Wen[2]

[1](School of Mathematics and Information Science, Shaanxi Normal University, Xi'an 710119, China)

[2](School of Computer Science, Shaanxi Normal University, Xi'an 710119, China)

Abstract: With the rapid development of the information technology, it becomes more and more popular that multiparty performs cooperative computation on their private data while preserving their privacy. Secure multiparty computation is a key privacy-preserving technology to address such security issues. The secure vector computation is an active area of secure multiparty computation. At present, there are many researches into secure vector computation such as private scalar product and private vector summation. There are few researches on securely computing the number of equal components of private vectors. These researches focus on secure two-party computation that all the components of vectors are drawn from a restricted range. This study focuses on privately computing the number of equal component of vectors and determining the relationship between the number and a threshold value. To this end, a component-matrix encoding is firstly proposed to encode a component of a vector. Then based on the ElGamal cryptosystem, a simple and efficient secure multiparty protocol is designed to compute number of equal components of vectors. Based on this protocol, an efficient secure multiparty protocol is designed to determine whether the number of equal components of vectors is larger than a threshold. The protocols do not restrict the data range of components. The correctness of the protocols is analyzed and it is proved that they are secure in the semi-honest model. Theoretical efficiency analysis and experimental result show that these protocols are simple and efficient. Finally, these protocols are used as building block to solve some practical secure multiparty computation problems.

* 基金项目: 国家自然科学基金 (61272435)
收稿时间: 2020-07-24; 修改时间: 2020-10-06; 采用时间: 2020-11-08

Key words: cryptography; secure multi-party computation; number of equal components; homomorphic encryption; encoding scheme

1 引 言

随着数据时代的来临, 数据信息已成为推动产业发展的巨大驱动力. 针对不同行业与领域的业务需求, 持有数据的多个实体经常需要对这些数据进行合作分析与计算, 共享分析计算结果让其发挥更大作用. 但是实际中拥有数据的各方在计算中不愿意泄露自己数据的隐私性, 那么如何在保护参与方数据隐私性的前提下进行合作计算即成为一个重要的研究课题. 由于这些隐私保护计算问题的推动, 安全多方计算 (secure multiparty computation, SMC) 已发展成为一个重要的研究方向, 并且成为解决隐私保护问题的重要方法和有力工具[1−3]. 安全多方计算是 $n(n \geqslant 2)$ 个互不信任的参与者保护隐私数据的合作计算问题, 计算结束后, 参与计算的各方除了得到他们设定的计算结果外, 不能在协议中获取其他参与方隐私数据的任何信息. 应用安全多方计算理论方法已研究了很多实际应用问题, 主要包括了安全科学计算[4−6]; 安全统计分析[7,8]; 安全几何计算[9,10]; 安全数据挖掘[11]; 安全数据库查询[12]等.

关于向量的相关安全多方计算问题已有一些研究成果. 文献 [13] 主要研究了向量的保密求和问题, 应用 Paillier 加密系统计算得到和向量的密文, 但当对密文进行解密时, 需要可信的第三方参与计算, 将解密的私钥进行拆分, 然后分发给多个权威中心, 权威中心对密文进行联合解密进而得到所需结果. 文献 [14] 首先设计了向量的保密标量积协议, 并在此基础上提出了一种基于同态加密的无第三方参与的欧氏距离协议, 利用此协议保密计算了两个传感器节点之间的安全距离. 文献 [15] 将点与几何图形位置关系的保密判定问题转化为向量内积的保密计算问题进行研究, 并将其应用于基于位置服务的几何范围保密查询, 但是文中协议要求点与图形位置的坐标数据均在一定的范围内取值. 文献 [16] 首次提出安全向量优势问题, 将一个 n 维向量转化成一个 $4n$ 维向量, 并以百万富翁问题协议为基础对向量中对应分量分别进行大小比较, 协议计算复杂度较高. 文献 [17] 解决了在有全集限制条件下的向量优势保密计算问题, 同时统计出优势分量的数目, 并以此为基础研究了保密整除问题以及点与若干直线位置关系保密判定问题.

对于多个向量的等分量数以及相应阈值问题设计安全多方计算协议在实际中有广泛的应用. 比如, 如何在保护隐私的条件下进行记录链接是大数据时代需要解决的一个重要问题[18,19]. 记录链接是利用统计学原理, 识别不同文件中的相关记录是否描述同一个体的一项数据处理技术. 基本方法是选择一个或多个字段 (如姓名、性别、出生日期等) 作为识别字符, 根据一定的匹配规则, 判断两条或多条记录是否针对同一个体. 确定性记录链接是基于在可用数据集中匹配的单个标识符的数量来生成链接, 如果所有或某些标识符 (在特定阈值之上) 相同, 则说这些记录通过确定性记录链接程序进行匹配. 在如今的信息时代, 进行保密的记录链接是非常重要的, 如此既可以提高数据库使用者的工作效率, 又免于数据库中信息的泄露. 若 n 个不同的数据库想要合作将其数据库中描述同一个体的记录进行链接, 并且不泄露信息, 则需要对这些数据库所拥有相关记录的标识符进行保密匹配: 假设每个数据库拥有一条记录, 为了保密判断 n 个数据库中的 n 条记录是否可以进行链接, 可以将这 n 条记录所对应的标识符 (一般为多个字段) 进行标准化处理, 将其转换成数据向量形式, 并对这些向量的等分量数进行保密计算. 在此基础上进一步判断这些向量的等分量数是否达到某个阈值, 若转化后的 n 个向量的等分量数达到某个阈值, 则表明这 n 个数据库中这些相应的记录匹配成功. 如此即可将隐私保护条件下的记录链接问题转化为向量等分量数及其相应阈值的安全多方计算问题.

目前对于多个参与者所拥有的私密向量的等分量数保密计算问题的研究还较少, 与其相关的两个问题, 即数据相等保密判定以及海明距离保密计算已有较多研究[20,21]. 我们注意到, 无法通过直接调用数据相等保密判定协议解决向量等分量数保密计算问题, 因为这样做会泄露向量中具体有哪些分量相等这样的额外信息. 利用海明距离计算协议可以解决在向量分量均为 0 或 1 时的两方参与者向量的等分量数问题, 无法将其推广到多方情形, 更无法将其推广应用于十进制数据的相关计算问题. 文献 [22] 利用编码方法以及 Paillier 加密系统设计了两方向量等分量数及相关阈值问题保密计算协议, 在向量等分量数阈值协议中, 向量分量要求有全集范围的限制, 文献 [22]

的协议也仅限于两方计算, 很难将其推广应用于多方计算问题. 为了更好解决向量等分量数保密计算问题, 本文研究设计了在向量中分量数据没有全集限制情形下, 多方向量的等分量数以及相应阈值问题的保密计算协议.

本文主要贡献如下:

(1) 提出并研究关于多方参与者私密向量保密计算的新问题, 即多方向量等分量数及相关阈值问题的保密计算. 本文所研究问题及解决方案对于所有向量的分量数据没有全集范围的限制, 拓展了向量保密计算的研究.

(2) 以 ElGamal 门限加密系统为基础设计向量等分量数多方保密计算协议, 并进一步设计构造向量等分量数阈值问题保密判定协议. 应用模拟范例方法, 对所设计协议的安全性进行了严格证明.

(3) 文中最后阐明应用本文协议可以解决集合交集的势及相关阈值保密计算, 以及隐私保护下的记录链接等广泛的实际问题.

2 预备知识

2.1 半诚实模型及其安全性定义

半诚实模型[23]. 半诚实参与者应按照协议要求执行协议, 但他们可能会保留在协议中所收到的信息, 当协议执行结束, 参与者会尝试根据各自得到的信息推导出其他参与者的隐私信息. 如果在执行协议中, 参与者都为半诚实参与者, 那么这种模型为半诚实模型.

设参与者 $P_1,\ldots,P_n$ 分别持有私密数据 $x_1,\ldots,x_n$, 记 $x=(x_1,\ldots,x_n)$. $f(x)=(f_1(x),\ldots,f_n(x))$ 是概率多项式时间函数, π 表示计算 $f(x)$ 的多方协议. 对于 $i\in[1,n]=\{1,\ldots,n\}$, 参与者 P_i 的输入为 x_i, 协议中 P_i 得到的信息序列记作:

$$view_i^{\pi}(x)=(x_i,r_i,m_1^i,\ldots,m_t^i,output_i^{\pi}(x)),$$

其中, r_i 是 P_i 产生的随机数, $m_j^i, j\in[1,t]$ 是 P_i 收到的第 j 个消息, $output_i^{\pi}(x)$ 是 P_i 得到的输出结果. 对于部分参与者构成的子集 $I=\{P_{i_1},\ldots,P_{i_m}\}\subseteq\{P_1,\ldots,P_n\}$, 记:

$$view_I^{\pi}=(I,view_{i_1}^{\pi}(x),\ldots,view_{i_m}^{\pi}(x)).$$

若对任意 I, 都存在概率多项式时间算法 S, 使得下式成立:

$$\{S(I,(x_1,\ldots,x_n),f_I(x))\}_{x\in(\{0,1\}^*)^n}\overset{c}{\equiv}\{view_I^{\pi}(x)\}_{x\in(\{0,1\}^*)^n} \tag{1}$$

则表示 π 能够保密计算 f, 其中 $\overset{c}{\equiv}$ 代表计算不可区分.

要证明在半诚实模型下一个多方计算协议是安全的, 就必须构造出满足式 (1) 的 S (也称这样的算法为模拟器, 并称这样的证明方法为模拟范例方法). 本文设计的安全计算协议均为半诚实模型下的协议.

2.2 ElGamal 加密系统

公钥加密系统是进行安全多方计算的重要工具, 目前很多安全计算的研究成果都是基于具有某种同态性质的公钥加密系统来设计保密计算协议. ElGamal 加密系统具有乘法同态性, 并具有语义安全性[24]. 具体描述如下[25].

(1) 密钥生成. 首先确定一个安全参数 k, 然后选取 k 比特的素数 p 和 Z_p^* 的生成元 g, 最后随机选择私钥 $sk=x$, 公钥 $pk: h=g^x \bmod p$. 这里加密算法记为 E, 解密算法记为 D.

(2) 加密. 为加密明文消息 $m\in Z_p^*$, 选择一个随机数 r, 计算 m 的密文 $E(m)$:

$$E(m)=(c_1,c_2)=(g^r \bmod p, mh^r \bmod p).$$

(3) 解密. 对于密文消息 $C=(c_1,c_2)$, 计算对应的明文 $m=D(C)$ 为:

$$m=c_2\cdot c_1^{-x} \bmod p.$$

(4) 同态性. ElGamal 加密系统具有乘法同态性, 即有下面性质成立: 假设

$$E(m_1)=(g^{r_1} \bmod p, m_1h^{r_1} \bmod p), E(m_2)=(g^{r_2} \bmod p, m_2h^{r_2} \bmod p),$$

则有:

$$E(m_1)\times E(m_2)=(g^{r_1+r_2} \bmod p, m_1\times m_2h^{r_1+r_2} \bmod p)=E(m_1\times m_2).$$

注解 1. 在协议设计中, 当需要进行数据保密求和时希望加密系统能实现加法同态性. 我们可以对 ElGamal 加密算法 E (对应的解密算法 D) 稍加修改而实现这个功能. 具体描述如下: 将修改后的加密算法和解密算法分别记

为 $\hat{E}$ 和 $\hat{D}$.

(i) 对明文消息 m (满足 $2^m \in Z_p^*$), 令 $\hat{E}(m) = E(2^m)$. 即应用 $\hat{E}$ 算法对 m 进行加密, 实际是应用加密算法 E 对 2^m 进行加密.

(ii) 对应用 $\hat{E}$ 算法加密得到的密文 C, 令 $\hat{D}(C) = \log_2 D(C)$. 即应用 $\hat{D}$ 算法对 C 进行解密, 实际是应用解密算法 D 对 C 进行解密后再进行一次对数运算.

(iii) 显然, 如果 $C_1 = \hat{E}(m_1), C_2 = \hat{E}(m_2)$, 则有 $C_1C_2 = \hat{E}(m_1 + m_2)$. 即修改后的加密算法 $\hat{E}$ ($\hat{D}$ 为相应的解密算法) 具有加法同态性.

2.3 门限加密系统

在门限加密系统中, n 个参与者联合生成公钥, 参与者共同拥有私钥. 所有参与者都可以用公钥加密消息, 但解密时必须由 t 个参与者合作才能完成, 少于 t 个参与者联合都无法解密任何消息, 这样的加密系统称为 (t,n) 门限加密系统. 本文主要应用 ElGamal 加密系统构造 (n,n) 门限加密系统, ElGamal 门限加密系统也是语义安全的, 并具有乘法同态性. 具体构造如下.

(1) 密钥生成. n 个参与者 $P_1,\cdots,P_n$ 公开选取 ElGamal 加密系统的参数 g, p. 每个参与者 P_i 选取私钥 $sk_i = x_i$, 公布 $h_i = g^{x_i} \mod p$, 联合生成公钥 $pk: h = g^{x_1+\ldots+x_n} \mod p$. 联合拥有私钥 $sk = x_1 + \ldots + x_n$.

(2) 加密. 为加密明文消息 $m \in Z_p^*$, 选择一个随机数 r, 计算 m 的密文 $E(m)$:

$$E(m) = (c_1, c_2) = (g^r \mod p, mh^r \mod p).$$

(3) 解密. 为解密密文消息 $C = (c_1, c_2)$, 每个参与者 P_i 计算 $u_i = c_1^{x_i} \mod p$, 进一步计算 C 对应的明文 m:

$$m = c_2\left[\prod_{i=1}^{n} u_i\right]^{-1} \mod p.$$

本文主要应用 ElGamal (n,n) 门限加密系统构造协议. 在下文中如果没有特殊说明, 加密和解密算法即为 E 和 D. 如下文中出现应用 $\hat{E}$ 算法进行加密 (相应地应用 $\hat{D}$ 进行解密) 时, 均以注解 1 的加密方式 (及相应的解密方式) 理解. 显然, 在门限加密系统下, $\hat{E}$ 加密算法也具有加法同态性.

3 向量等分量数多方保密计算

3.1 问题描述及计算原理

(1) 问题描述. 考虑 n 个参与者 $P_1,\ldots,P_n$, 对于每个 $i \in [1,n]$, P_i 拥有一个 t 维向量 $X_i = (x_i^1,\ldots,x_i^t)$. 进一步假设对于任意 $i \in [1,n]$, $j \in [1,t]$, x_i^j 的十进制表示位数不超过 m 位. 定义这 n 个向量的等分量数为 $\varphi(X_1,\ldots,X_n) = \sum_{j=1}^{t} \varphi_j$, 其中, 当 $x_1^j = \ldots = x_n^j$ 时, $\varphi_j = 1$; 否则, $\varphi_j = 0$. $P_1,\ldots,P_n$ 希望合作计算 $\varphi(X_1,\ldots,X_n)$, 而不泄露任何额外信息. 为叙述简单, 下文中也简记 $X = (X_1,\ldots,X_n)$ 以及 $\varphi(X) = \varphi(X_1,\ldots,X_n)$.

(2) 计算原理. (i) 参与者 $P_i, i \in [1,n]$ 将其私密向量 X_i 的每个分量 $x_i^j, j \in [1,t]$ 表达成 m 位十进制形式 $x_i^j = y_{i1}^j \ldots y_{im}^j$, 其中 $0 \leqslant y_{ik}^j \leqslant 9, k \in [1,m]$ (如果 x_i^j 不够 m 位, 可通过在前面补 0 的方式将其补充为 m 位).

(ii) 对每个 $j \in [1,t]$, P_1 将向量 X_1 的每个分量 $x_1^j = y_{11}^j \ldots y_{1m}^j$ 分别编码为一个 $m \times 10$ 阶矩阵 A^j: 对每个 $k \in [1,m], l \in [1,10]$, 记 A^j 的第 k 行第 l 列元素为 a_{kl}^j, 令:

$$a_{kl}^j = \begin{cases} 1, \text{如果 } y_{1k}^j = l-1; \\ r, \text{否则.} \end{cases}$$

其中, 对应于不同的元组 (j,k,l), r 应选为互不相同的不等于 1 的随机数. 按照上述方式, 向量 X_1 中每个分量 x_1^j 对应一个编码矩阵 A^j, 称这样的编码方法为分量-矩阵编码方法.

(iii) 对于每一个 $i \in [2,n]$, P_i 进行如下操作.

(a) 对每个 $j \in [1,t]$, P_i 根据 $y_{i1}^j,\ldots,y_{im}^j$ 的值在矩阵 A^j 中选择元素, 选择原则如下: 对于每一个 $k \in [1,m]$, P_i 在 A^j

的第 k 行选择第 y_{ik}^j+1 列元素 $a^j_{ky_{ik}^j+1}$, P_i 在 A^j 中共选择得到 m 个元素: $a^j_{1y_{i1}^j+1},\ldots,a^j_{my_{im}^j+1}$. P_i 将这 m 个数据相乘, 结果记为:

$$v_i^j=\prod_{k=1}^{m}a^j_{ky_{ik}^j+1}.$$

(b) P_i 得到数组 $V_i=(v_i^1,\ldots,v_i^t)$.

(iv) $P_2,\ldots,P_n$ 分别得到数组 $V_2,\ldots,V_n$ 后, 将 $V_2,\ldots,V_n$ 中对应元素相乘, 得到 $w^j=\prod_{i=2}^{n}v_i^j,\ j\in[1,t]$. 根据上面得到的数组 $W=(w^1,\ldots,w^t)$ 可确定向量的等分量数. 具体地, 有下面结论:

命题 1. 向量 $X_1,\ldots,X_n$ 的等分量数 $\varphi(X)$ 为数组 $W=(w^1,\ldots,w^t)$ 中取值为 1 的元素个数.

证明: 由于 $x_i^j=y_{i1}^j\ldots y_{im}^j$, 显然, $x_1^j=\ldots=x_n^j$ 成立等价于下面等式同时成立:

$$y_{11}^j+1=\ldots=y_{n1}^j+1,\ \ldots,\ y_{1m}^j+1=\ldots=y_{nm}^j+1 \tag{2}$$

根据分量-矩阵编码方法, 对于每一个确定的 $j\in[1,t]$, 在 A^j 中仅有 $a^j_{1y_{11}^j+1},\ldots,a^j_{my_{1m}^j+1}$ 这 m 个元素取值为 1, 其他元素为不等于 1 的随机数.

对于某个 $i\in[2,n]$, 当 $x_i^j=x_1^j$ 时, 由计算原理第 2 步可知 P_i 在矩阵 A^j 中挑选的所有 m 个元素均为 1, 因此可知 $v_i^j=1$.

进一步, 若对所有 $i\in[2,n]$, $x_i^j=x_1^j$ 均成立, 则有 $v_2^j=\ldots=v_n^j=1$, 根据计算原理的第 3 步可知此时有 $w^j=1$.

如果存在某个 $i_0\in[2,n]$, 使得 $x_{i_0}^j\neq x_1^j$, 此时 $v_{i_0}^j$ 是一个随机数, 进而可知 $w^j=\prod_{i=2}^{n}v_i^j$ 也是随机数.

综上可知, 当且仅当对于所有的 $i\in[2,n]$, $x_i^j=x_1^j$ 均成立时, $w^j=1$. 因此如果 $w^j=1$, 则表明所有 n 个参与者向量的第 j 个分量相等.

因此向量 $X_1,\ldots,X_n$ 的等分量数 $\varphi(X)$ 即为数组 $W=(w^1,\ldots,w^t)$ 中取值为 1 的元素个数.

下面给出一个实例解释说明向量等分量数计算原理以及编码过程.

例 1. 假设 P_1 拥有向量 $X_1=(231,345,126,78)$, P_2 拥有向量 $X_2=(231,345,126,775)$, P_3 拥有向量 $X_3=(231,345,667,338)$. 已知所有向量的位数不超过 $m=3$.

(1) P_1 根据分量-矩阵编码方法对 X_1 中各分量数据进行编码, 得到下面 4 个 3×10 阶矩阵:

$$A^1=\begin{bmatrix}r&r&1&r&r&r&r&r&r&r\\r&r&r&1&r&r&r&r&r&r\\r&1&r&r&r&r&r&r&r&r\end{bmatrix},\quad A^2=\begin{bmatrix}r&r&r&1&r&r&r&r&r&r\\r&r&r&r&1&r&r&r&r&r\\r&r&r&r&r&1&r&r&r&r\end{bmatrix},$$

$$A^3=\begin{bmatrix}r&1&r&r&r&r&r&r&r&r\\r&r&1&r&r&r&r&r&r&r\\r&r&r&r&r&r&1&r&r&r\end{bmatrix},\quad A^4=\begin{bmatrix}1&r&r&r&r&r&r&r&r&r\\r&r&r&r&r&r&r&1&r&r\\r&r&r&r&r&r&r&r&1&r\end{bmatrix}.$$

(2) P_2 根据向量 $X_2=(231,345,126,775)$ 中第 j 个分量的具体数据, 在 A^j 中选择适当元素并对其进行乘积运算, 结果如下:

(i) 在 A^1 中选择元素 $a_{13}^1=1,a_{24}^1=1,a_{32}^1=1$, 并计算 $v_2^1=a_{13}^1a_{24}^1a_{32}^1=1$;

(ii) 在 A^2 中选择元素 $a_{14}^2=1,a_{25}^2=1,a_{36}^2=1$, 并计算 $v_2^2=a_{14}^2a_{25}^2a_{36}^2=1$;

(iii) 在 A^3 中选择元素 $a_{12}^3=1,a_{23}^3=1,a_{37}^3=1$, 并计算 $v_2^3=a_{12}^3a_{23}^3a_{37}^3=1$;

(iv) 在 A^4 中选择元素 $a_{18}^4=r,a_{28}^4=1,a_{36}^4=r$, 并计算 $v_2^4=a_{18}^4a_{28}^4a_{36}^4=r$.

P_2 得到数组 $V_2=(v_2^1,v_2^2,v_2^3,v_2^4)=(1,1,1,r)$.

(3) P_3 按照 (2) 中 P_2 类似的方式选择元素并进行相应计算, 相应得到数组 $V_3=(v_3^1,v_3^2,v_3^3,v_3^4)=(1,1,r,r)$.

(4) 将数组 V_2 和 V_3 的对应元素相乘, 得到一个新的数组 $W=(1,1,r,r)$. 由于 W 中有两个取值为 1 的元素, 因此, 该问题中 X_1,X_2,X_3 的等分量数为 $\varphi(X)=2$.

3.2 多方向量等分量数保密计算协议

协议 1. 多方向量等分量数保密计算协议.

输入: 参与者 $P_i, i\in[1,n]$输入私密向量 $X_i=(x_i^1,\ldots,x_i^t)$, 这里所有 $x_i^j, j\in[1,t]$的十进制表示位数均不超过 m.

输出: 向量等分量数 $\varphi(X)$.

准备: P_1 按照分量-矩阵编码方法将向量 X_1 编码成 t 个 $m\times 10$ 阶的矩阵 $A^1,\ldots,A^t$. $P_1,\ldots,P_n$ 运行 ElGamal 门限加密系统, 生成加密算法的公钥 pk 和私钥 sk, 参与者 P_i 具有的私钥份额为 sk_i.

1. P_1 将矩阵 $A^1,\ldots,A^t$ 中所有值为 1 的元素加密, 得到密文矩阵 $C^1=(c_{kl}^1)_{m\times 10},\ldots,C^t=(c_{kl}^t)_{m\times 10}$, 并将 $C^1,\ldots,C^t$ 发送给 $P_2,\ldots,P_n$.

2. 对于每个 $i\in[2,n]$, P_i 进行如下操作:

(a) 对每个 $j\in[1,t]$, P_i 在 C^j 中第 $k,k\in[1,m]$行选择元素 $c^j_{ky_{ik}^j+1}$, 并作乘积:

$$\bar{v}_i^j=\prod_{k=1}^{m}c^j_{ky_{ik}^j+1}E(1).$$

(b) P_i 构造数组 $\bar{V}_i=(\bar{v}_i^1,\ldots,\bar{v}_i^t)$, 并将 $\bar{V}_i$ 发送给 P_n.

3. P_n 进行如下运算:

(a) 对于每个 $j\in[1,t]$, P_n 计算 $\bar{w}_n^j=\prod_{i=2}^{n}\bar{v}_i^j$. 并构成数组 $\bar{W}_n=(\bar{w}_n^1,\ldots,\bar{w}_n^t)$.

(b) P_n 将数组 $\bar{W}_n$ 中元素进行随机置换得到 $Z_n=(z_n^1,\ldots,z_n^t)$, 并将 Z_n 发送给 P_{n-1}.

4. 对 $i=n-1,\ldots,2$,

(a) P_i 从 P_{i+1} 处得到数组 $Z_{i+1}=(z_{i+1}^1,\ldots,z_{i+1}^t)$, 将 $z_{i+1}^j, j\in[1,t]$ 乘 1 的不同密文, 并对 Z_{i+1} 中元素进行随机置换, 得到新数组 Z_i.

(b) P_i 将数组 Z_i 发送给 P_{i-1}.

5. P_1 将得到数组 $Z_1=(z_1^1,\ldots,z_1^t)$ 公开, 所有参与者联合解密 $z_1^j=(c_1^j,c_2^j), j\in[1,t]$. 每个 P_i 计算 $u_i^j=(c_1^j)^{sk_i}\bmod p$, 并进一步计算:

$$h^j=c_2^j\left[\prod_{i=1}^{n}u_i^j\right]^{-1}\bmod p,$$

得到 $H=(h^1,\ldots,h^t)$. 统计 H 中取值为 1 的元素个数, 记为 h, 输出 h.

3.3 协议 1 的正确性

在协议 1 中密文数组 Z_1 是由数组 $\bar{W}_n$ 经过多次随机置换以及重随机化得到的, 因此 Z_1 与 $\bar{W}_n$ 中元素为 1 的密文个数相同.

根据协议 1, 在 $\bar{W}_n=(\bar{w}_n^1,\ldots,\bar{w}_n^t)$中, 对任意给定的 $j\in[1,t]$,

$$\bar{w}_n^j=\prod_{i=2}^{n}\bar{v}_i^j=\prod_{i=2}^{n}\left[\prod_{k=1}^{m}c^j_{ky_{ik}^j+1}E(1)\right],$$

由此知 $\bar{w}_n^j$ 为 1 的密文当且仅当下式成立:

$$a^j_{ky_{ik}^j+1}=D(c^j_{ky_{ik}^j+1})=1, i\in[1,n], k\in[1,m] \tag{3}$$

根据命题 1 以及式 (2), 使得式 (3) 成立的 $j\in[1,t]$ 的个数即为 $\varphi(X)$, 因此协议 1 是正确的.

3.4 协议 1 的安全性

首先对协议 1 的安全性进行分析.

在协议第 1–3 步中:

(i) P_1 数据的安全性: P_1 向外公布了密文矩阵 $C^j, j\in[1,t]$, 这些密文矩阵中的元素或是 1 的不同密文, 或是随机数. 由于门限加密系统具有语义安全性, 没有 P_1 参与合作, 这些矩阵元素均与随机数计算不可区分.

(ii) $P_i, i\in[2,n]$ 数据的安全性: $P_i, i\in[2,n-1]$ (或 P_n) 向外公布了密文数组 $\bar{V}_i=(\bar{v}_i^1,\ldots,\bar{v}_i^t)$ (或 $Z_n=(z_n^1,\ldots,z_n^t)$), 这些密文数组中每个元素都乘了一个由 P_i (或 P_n) 加密的密文 $E(1)$. 由于门限加密系统具有语义安全性, 没有 P_i

(或P_n) 参与合作, 这些数组元素均与随机数计算不可区分.

因此, 上面操作不会泄露参与者输入数据的任何信息.

在协议第 3(b)–5 步中: $P_i, i\in[2,n-1]$(或P_n) 向外公布了密文数组$Z_i=(z_i^1,\ldots,z_i^t)$(或$Z_n=(z_n^1,\ldots,z_n^t)$), 这些密文数组是经过对Z_{i+1}的元素重随机化以及随机置换 (或对$\bar{W}_n$的元素进行随机置换) 后而得到的, 由于$Z_i, i\in[2,n-1]$中元素都进行了重随机化, 这些操作显然不会泄露参与者输入数据的任何信息. 进一步, 由于在这一计算过程中每个参与者都参与了随机置换, 从最后的解密结果$H=(h^1,\ldots,h^t)$中仅能获知$X_1,\ldots,X_n$的等分量数个数, 即使有$n-1$个参与者合谋也无法获知具体有哪些分量具有相等关系.

进一步, 由于在协议中所有参与者最终要对密文数组$Z_1=(z_1^1,\ldots,z_1^t)$中每个元素进行合作解密, 根据离散对数问题的困难性, 解密过程也不会泄露关于任意参与者私钥份额的有关信息.

综上所述, 执行协议 1 仅能获得规定输出结果, 无法获得任何额外信息.

为对协议 1 的安全性进行严格证明, 我们给出了定理 1.

定理 1. 协议 1 在半诚实模型下是安全的, 且能够抵抗任意参与者进行合谋攻击.

证明: 通过模拟范例方法证明定理 1, 我们需要对参与者中任意$n-1$个合谋攻击者所构成的集合I来构造满足式 (1) 的模拟器S.

不失一般性, 对于合谋者集合为$I=\{P_1,\ldots,P_{n-1}\}$的情形, 构造相应的模拟器S, 使得式 (1) 成立. 对于其他合谋者集合情形可类似证明. 为叙述简单, 下面记$X_I=(X_1,\ldots,X_{n-1})$.

接受到输入$(X_I, f_I(X)=\varphi(X))$后, S按照如下方式运行:

(i) S运行 ElGamal 门限加密系统生成公钥pk', 其对应的私钥份额为$sk_i', i\in[1,n]$, 对应的加密算法记为E', 解密算法记为D'.

(ii) S任意选取向量$X_n'=(x'^1_n,\ldots,x'^t_n)$(记$x'^j_n, j\in[1,t]$的十进制表达为$x'^j_n=y'^j_{n1},\ldots,y'^j_{nm}$), 使其满足$\varphi(X_I,X'_n)=\varphi(X)$.

(iii) 对每个$i\in[2,n-1]$, $j\in[1,t]$, S应用pk'加密矩阵A^j中的元素 1, 得到相应的加密矩阵$C'^j=(c'^j_{kl})_{m\times 10}$. S在C'^j中第$k,k\in[1,m]$行选择元素$c'^j_{ky^j_{ik}+1}$以及$c'^j_{ky'^j_{nk}+1}$, 并计算: $\bar{v}'^j_i=\prod_{k=1}^m c'^j_{ky^j_{ik}+1}$以及$\bar{v}'^j_n=\prod_{k=1}^m c'^j_{ky'^j_{nk}+1}$.

(iv) S构造数组$\bar{V}'_i=(\bar{v}'^1_i,\ldots,\bar{v}'^t_i), i\in[2,n]$.

(v) S计算$\bar{w}'^j_n=\prod_{i=2}^n \bar{v}'^j_i$, 构成数组$\bar{W}'_n=(\bar{w}'^1_n,\ldots,\bar{w}'^t_n)$. S将$\bar{W}'_n$中元素进行随机置换, 得到新数组Z'_n.

(vi) S对Z'_n中元素进行重随机化, 然后进行随机置换, 得到$Z'_1=(z'^1_1,\ldots,z'^t_1)$.

(vii) S解密$z'^j_1=(c'^j_1,c'^j_2), j\in[1,t]$. 计算$u'^j_i=(c'^j_1)^{sk'_i} \mod p, i\in[1,n]$, 并进一步计算:

$$h'^j=c'^j_2\left[\prod_{i=1}^n u'^j_i\right]^{-1} \mod p,$$

得到向量$H'=(h'^1,\ldots,h'^t)$. 进而得到H'中取值为 1 的元素个数h'.

在协议的执行中,

$$view_I^{\pi}(X)=\{X_I, Z_1=(z_1^1,\ldots,z_1^t), u_n^1,\ldots,u_n^t,\varphi(X)\}.$$

令:

$$S(X_I,f_I(X))=\{X_I, Z'_1=(z'^1_1,\ldots,z'^t_1), u'^1_n,\ldots,u'^t_n,\varphi(X_I,X'_n)\}.$$

由于 ElGamal 门限加密系统有语义安全性, 缺少一位参与者都不能解密, 对每个$j\in[1,t]$, z_1^j中含有P_n加密的密文$E(1)$, 对I中合谋者来说z_1^j与z'^j_1计算不可区分, 进一步由于P_n在构造$Z_n=(z_n^1,\ldots,z_n^t)$时进行了随机置换, 所以对I中合谋者来说, Z_1是经过P_n随机置换后得到的. 因此有$Z_1\overset{c}{\equiv}Z'_1$(包括两个数组中元素的先后顺序也是不可区分的). 又由于对每个$j\in[1,t], u_n^j=(c_1^j)^{sk_n} \mod p$, 其中$sk_n$为$P_n$的私钥份额, 由于离散对数问题是困难的, I中合谋者从u_n^j中无法获得sk_n的任何额外信息, 因此有$u_n^j\overset{c}{\equiv}u'^j_n$. 进一步由于$\varphi(X_I,X'_n)=\varphi(X)$, 故有下式成立:

$$\{S_I(X_I, f_I(X))\} \overset{c}{\equiv} \{view_I^{\pi}(X)\}.$$

因此, 协议 1 在半诚实模型下是安全的, 且能够抵抗任意参与者进行合谋攻击.

4 向量等分量数阈值问题多方保密计算

4.1 问题描述及计算原理

(1) 问题描述. 考虑 n 个参与者 $P_1,\dots,P_n$, 对于每个 $i\in[1,n]$, P_i 拥有一个 t 维向量 $X_i=(x_i^1,\dots,x_i^t)$. 进一步假设对于任意 $i\in[1,n], j\in[1,t]$, x_i^j 的十进制表示不超过 m 位. 所有参与者希望合作保密判定 $\varphi(X)$ 是否达到某个给定的阈值 $b(b\leqslant t)$, 而不泄露任何额外信息.

(2) 计算原理. 从协议 1 可知在数组 $\bar{W}_n$ 中取值为 $E(1)$ 的元素个数即为 $\varphi(X)$. 为判定 $\varphi(X)$ 与阈值 b 的大小关系, 同时避免泄露 $\varphi(X)$ 的具体数值, 参与者需要在 $\bar{W}_n$ 的基础上进一步进行下面操作:

(i) 首先, 所有参与者 $P_i, i=n,\dots,1$ 依次对于 $\bar{W}_n$ 添加 l_i 个 1 的不同密文以及 r_i 个随机数, 这样即将数组 $\bar{W}_n$ 扩充为一个 $t+\Sigma_{i=1}^n(l_i+r_i)$ 维的数组 Z_1; 参与者通过合作解密而获得明文数组 z_1, 并可得到 z_1 取值为 1 的元素个数, 记为 α. 如此, 即可将 $\varphi(X)\geqslant b$ 是否成立的判定问题转化为 $b+\Sigma_{i=1}^n l_i-\alpha\leqslant 0$ 是否成立的判定问题. 为了技术方面的考虑, 下面进一步将问题转化为判定 $k_1=b+\Sigma_{i=1}^n l_i-\alpha+s\leqslant s$ 是否成立的问题 (其中 $s>t$ 为一个适当大的正整数).

(ii) 为了解决转化后的保密判定问题, 参与者 $P_i, i\in[1,n]$ 选取 q_i 个小于等于 s 的随机数, o_i 个大于 s 的随机数, 与 k_1 一起构成一个 $\Sigma_{i=1}^n(q_i+o_i)+1$ 维数组 z_2, 如果将 z_2 中小于等于 s 的元素个数记为 β, 并记 $k_2=\beta-\Sigma_{i=1}^n q_i$, 显然, 当 $k_1\leqslant s$ 时, $k_2=1$; 当 $k_1>s$ 时, $k_2=0$.

综上所述, 我们得到下面等价关系式:

$$\varphi(X)\geqslant b\Leftrightarrow k_1=b+\Sigma_{i=1}^n l_i-\alpha+s\leqslant s\Leftrightarrow k_2=\beta-\Sigma_{i=1}^n q_i=1;\varphi(X)<b\Leftrightarrow k_1>s\Leftrightarrow k_2=0. \tag{4}$$

为方便起见, 定义函数 $P(X)$ 如下: 如果 $\varphi(X)\geqslant b$, 令 $P(X)=1$, 否则, 令 $P(X)=0$.

4.2 向量等分量数阈值问题多方保密计算协议

协议 2. 向量等分量数阈值问题多方保密计算协议

输入: 参与者 $P_i, i\in[1,n]$ 输入 t 维向量 $X_i=(x_i^1,\dots,x_i^t)$, 每个 x_i^j 不超过 m 位. 给定阈值 b.

输出: $y=P(X)$.

准备: P_1 按照第 3.1 节的分量-矩阵编码方法将向量 X_1 编码成 t 个 $m\times 10$ 阶矩阵 $A^1,\dots,A^t$. 所有参与者共同商定一个随机数 $s>t$, 并公布 s. 生成 ElGamal 门限加密系统的公钥 pk 和私钥 sk, 将 P_i 具有的私钥份额记为 sk_i.

协议 2 的前 2 步与协议 1 完全相同, 下面从第 3 步开始.

3. P_n 进行如下运算.

(a) 对于每个 $j\in[1,t]$, P_n 计算 $\bar{w}_n^j=\prod_{i=2}^n \bar{v}_i^j$, 构成数组 $\bar{W}_n=(\bar{w}_n^1,\dots,\bar{w}_n^t)$.

(b) P_n 在 $\bar{W}_n$ 中分别添加 l_n 个 1 的不同密文以及 r_n 个不同随机数, 得到一个 $s_n=t+l_n+r_n$ 维数组, 进一步对数组元素进行随机置换, 将最终得到的数组记为 T_n.

(c) P_n 计算密文 $L_n=\hat{E}(l_n)$, 并将密文数组 T_n 与 L_n 发送给 P_{n-1}.

4. 令 $i=n-1$, P_i 操作如下.

(a) 将收到的 s_{i+1} 维密文数组 T_{i+1} 的各个元素分别乘以 1 的不同密文, 再对其添加 l_i 个 1 的不同密文以及 r_i 个不同随机数得到一个 $s_i=s_{i+1}+l_i+r_i$ 维数组, 并对数组元素进行随机置换, 将最终得到的数组记为 T_i. 进一步计算密文 $L_i=L_{i+1}\hat{E}(l_i)$.

(b) 如果 $i>1$, P_i 将密文数组 T_i 与 L_i 发送给 P_{i-1}. 令 $i\leftarrow i-1$, 并返回第 4 步. 如果 $i=1$, P_1 将密文数组 T_1 公开.

5. 所有参与者联合解密数组 T_1(逐项解密), P_1 得到解密后的数组 t_1.

6. P_1 计算如下.

(a) P_1 统计 t_1 中取值为 1 的元素数目, 记为 α. 并进一步计算:

$$K_1 = L_1\hat{E}(b)(\hat{E}(\alpha))^{-1}\hat{E}(s).$$

(b) P_1 分别选择q_1 个小于等于s 的随机数, o_1 个大于s 的随机数, 利用$\hat{E}$ 算法对其进行加密, 与K_1 构成$m_1 = q_1 + o_1 + 1$ 维密文数组, 并对其进行随机置换, 将最终得到的数组记H_1.

(c) P_1 计算密文$Q_1 = \hat{E}(q_1)$, 并将H_1 与Q_1 发送给P_2.

7. 令$i = 2$, P_i 操作如下.

(a) 将收到的m_{i-1} 维密文数组H_{i-1} 的各个元素分别乘以 1 的不同密文, 再分别选择q_i 个小于等于s 的随机数, o_i 个大于s 的随机数, 利用$\hat{E}$ 算法对其进行加密, 得到一个$m_i = m_{i-1} + q_i + o_i$ 维数组, 进一步对数组元素进行随机置换, 将最终得到的数组记为H_i. P_i 计算$Q_i = Q_{i-1}\hat{E}(q_i)$.

(b) 如果$i < n$, P_i 将密文数组H_i 与Q_i 发送给P_{i+1}. 令$i \leftarrow i + 1$, 并返回第 7 步. 如果$i = n$, P_n 将密文数组H_n 公开.

8. 所有参与者应用$\hat{D}$ 算法联合解密数组H_n, P_n 得到解密后的数组h_n.

9. P_n 统计h_n 中小于等于s 的元素个数, 将其记为β. P_n 计算下面K_2 并公布:

$$K_2 = \hat{E}(\beta)Q_n^{-1}.$$

10. 所有参与者应用$\hat{D}$ 算法联合解密K_2 得到k_2, 并输出k_2.

4.3 协议 2 的正确性

由于协议 2 的前两步与协议 1 相同, 由协议 1 可知在协议 2 第 3(a) 中得到的数组$\bar{W}_n$ 中, 取值为$E(1)$ 的元素个数等于$\varphi(X)$. 在计算中, 我们通过选择适当大的正整数$s > t$, 将$b - \varphi(X) \leqslant 0$ 是否成立的保密判定转化成$b - \varphi(X) + s \leqslant s$ 是否成立的保密判定. 此做法是为了保证$k_1 = b - \varphi(X) + s \in Z_p^*$, 由于在 ElGamal 加密系统中, 明文空间为Z_p^*, 由此可知只要条件$k_1 \in Z_p^*$ 满足, 则可保证$D(E(k_1)) = k_1$ 成立, 如此即可保证解密结果的正确性.

根据协议 2 第 3(b)–6(a) 步的操作, 可知$\alpha = \varphi(X) + \sum_{i=1}^{n} l_i$, 进一步根据$\hat{E}$ 算法的加法同态性, 有:

$$K_1 = \hat{E}\left(\sum_{i=1}^{n} l_i + b - \alpha + s\right) = \hat{E}\left[\sum_{i=1}^{n} l_i + b - (\varphi(X) + \sum_{i=1}^{n} l_i) + s\right] = \hat{E}(b - \varphi(X) + s).$$

根据协议 2 第 6(b)–9(a) 步的操作以及计算原理可知, 当$\varphi(X) < b$ 时, $\beta = \sum_{i=1}^{n} q_i$; 当$\varphi(X) \geqslant b$ 时, $\beta = \sum_{i=1}^{n} q_i + 1$, 再根据$\hat{E}$ 算法的加法同态性, 有:

$$K_2 = \hat{E}(\beta)Q_n^{-1} = \hat{E}\left(\beta - \sum_{i=1}^{n} q_i\right),$$

对K_2 应用$\hat{D}$ 算法解密后得到k_2, k_2 的值或为 0, 或为 1. 如果$k_2 = 0$, 则$\beta = \sum_{i=1}^{n} q_i$, 即有$\varphi(X) < b$; 如果$k_2 = 1$, 则$\beta = \sum_{i=1}^{n} s_i + 1$, 即有$\varphi(X) \geqslant b$. 因此协议 2 是正确的.

4.4 协议 2 的安全性

对协议 2 的安全性详细分析如下.

在协议 2 第 1–3 步中关于私密向量$X_1, \ldots, X_n$ 的安全性分析与协议 1 类似, 并可知此过程不会泄露参与者输入数据的任何信息.

在协议 2 第 3(b)-5 步中: $P_i, i \in [1, n-1]$ (或P_n) 向外公布了密文数组T_i (或T_n), 这些密文数组是经过对T_{i+1} 的元素重随机化, 并添加了一些 1 的不同密文以及随机数元素, 进一步进行随机置换 (或对$\bar{W}_n$ 的元素添加了一些 1 的不同密文以及随机数元素并进行随机置换) 后而得到的, 由于$T_i, i \in [1, n]$ 中元素都进行了重随机化, 且在这一计算过程中每个参与者都参与了随机置换, 这些操作保证了不会泄露参与者所添加数据的任何信息. 由于应用门限加密系统进行保密计算, 解密前即使有$n-1$ 个参与者合谋也无法获得其他参与者数据的任何信息. 从最后解密得到的数组t_1 中也仅能获知t_1 中取值为 1 的元素个数, 即使有$n-1$ 个参与者合谋也无法获知具体有哪些元素取值为 1.

这一过程主要为在解密T_1 后保护$\bar{W}_n$ 中取值为密文$E(1)$ 的元素个数$\varphi(X)$ 的隐私性. 对于每一个$i_0 \in [1, n]$, 由于l_{i_0}, r_{i_0} 为P_{i_0} 选择的私密数据, 即使P_{i_0} 以外的所有$n-1$ 个参与者合谋, 从最后的解密结果t_1 中也无法获知$\varphi(X)$ 以及l_{i_0}, r_{i_0} 的任何信息.

在协议 2 第 6(b)-8 步中参与者所添加数据的安全性与第 3(b)–5 步中所添加数据的安全性分析完全类似. 即从最后解密得到的数组 h_n 中仅能获知 h_n 中取值小于等于 s 的元素个数 β, 即使有 $n-1$ 个参与者合谋也无法获知具体有哪些元素取值小于等于 s.

这一过程主要在不解密 K_1 的情况下, 保密判断 K_1 对应的明文 k_1 与 s 的大小关系, 而获得 $\varphi(X)$ 与 b 的大小关系.

我们注意到如果直接解密 K_1 会泄露信息. 这是由于: 假设解密 K_1 得到对应的明文 k_1, 则知 k_1 包含有 $l_1,\ldots,l_n,b,\alpha,s$, 如果除 P_{i_0} 以外的 $n-1$ 个参与者合谋, 则他们根据 k_1 的值以及根据 b,α,s 和 $l_i,i\in[1,n],i\neq i_0$ 能推断出 l_{i_0} 的值, 进而能推断出 $\varphi(X)$ 的值.

通过构造数组 H_n, 并对其解密得到 h_n, 可以在保密 k_1 的情况下判定其与 s 的大小关系. 对于每一个 $i_0\in[1,n]$, 由于 q_{i_0} 和 o_{i_0} 是 P_{i_0} 选择的私密数据, 即使除 P_{i_0} 以外的 $n-1$ 个参与者合谋, 他们根据 h_n 仅能推断出 $\eta=\beta-(q_1+\ldots+q_{i_0-1}+q_{i_0+1}+\ldots+q_n)$ 个数据是小于等于 s 的, 这个数据中是否包含有 k_1 他们却无从知晓. 因此合谋者无法从 h_n 中得到 k_1 的任何信息.

在协议 2 中所有参与者要对密文 T_1,H_n,K_2 进行合作解密, 根据离散对数问题的困难性, 解密过程也不会泄露关于任意参与者私钥份额的有关信息.

综上所述, 执行协议 2 仅能获得规定输出结果, 无法获得任何额外信息.

类似于定理 1, 为对协议 2 的安全性进行严格证明, 我们给出了定理 2. 在此省略证明过程, 仅叙述下面定理.

定理 2. 协议 2 在半诚实模型下是安全的, 且能够抵抗任意参与者进行合谋攻击.

5 效率分析

本节对上面所设计的关于向量等分量数以及相关阈值问题的保密计算协议进行效率分析, 并与已有研究结果进行比较.

本文协议主要以 ElGamal 加密系统为基础进行设计, 本文协议计算效率仅考虑模指数运算次数. 在 ElGamal 门限加密系统中, 应用 E 或 $\hat{E}$ 加密 1 个密文需要 2 次模指数运算, 当 n 个参与者参与计算时, 应用 D 或 $\hat{D}$ 解密 1 个密文均需要 n 次模指数运算.

5.1 复杂性分析

(1) 计算复杂性. 在协议 1 中, 每个参与者 P_i 分别拥有一个 t 维向量 X_i, 所有向量的每一个分量位数不超过 m. P_1 加密编码矩阵中取值为 1 的元素, 需要 $2tm$ 次模指数运算; 解密数组 Z_1 需要 tn 次模指数运算. 因此协议 1 共需 $t(n+2m)$ 次模指数运算.

在协议 2 中应用 E 加密编码矩阵中值为 1 的元素以及 $l_1,\ldots,l_n$ 个 1 的密文, 需要 $2tm+2\sum_{i=1}^{n}l_i$ 次模指数运算; 应用 D 解密 T_1 需要 $(t+\sum_{i=1}^{n}(l_i+r_i))n$ 次模指数运算. 在应用 $\hat{E}$ 加密 $l_i,q_i,i\in[1,n],q_1,\ldots,q_n,o_1,\ldots,o_n$ 个密文以及 α,β,b,s 时, 需要 $4n+2\sum_{i=1}^{n}(q_i+o_i)+8$ 次模指数运算; 在利用 $\hat{D}$ 解密数组 H_n,K_2 时, 需要 $(2+\sum_{i=1}^{n}(q_i+o_i))n$ 次模指数运算. 协议 2 共需要进行 $2\sum_{i=1}^{n}(q_i+o_i+l_i)+n\sum_{i=1}^{n}(q_i+o_i+l_i+r_i)+t(n+2m)+6n+8$ 次模指数运算.

(2) 通信复杂性. 本文应用执行协议所需要的通信轮数衡量通信复杂性.

在协议 1 中 $P_2,\ldots,P_n$ 挑选元素进行 1 轮通信, 对 $\bar{W}_n$ 进行随机置换和重随机化需要 1 轮通信, 合作解密需要 1 轮通信. 协议 1 共需 3 轮通信.

在协议 2 中 $P_2,\ldots,P_n$ 挑选元素进行 1 轮通信, 在 $\bar{W}_n$ 中添加虚假元素需要 1 轮通信, 构造 H_n 需要 1 轮通信, 解密 T_1,H_n,K_2 需要 3 轮通信. 协议 2 共需 6 轮通信.

5.2 与已有结果进行比较

文献 [22] 设计了两方向量等分量数以及等分量数阈值问题保密计算协议, 与本文研究的问题类似, 下面对本文协议与文献 [22] 中的相关协议进行分析比较.

文献 [22] 中协议 1 设计了两方向量等分量数的保密计算协议, 主要以编码方法和 Paillier 加密系统为基础进

行设计, 但在协议 1 中限制所有分量数据在一个全集内取值. 假设两方参与者为 Alice 和 Bob, 文献 [22] 中协议 1 主要思想是 Alice 根据给定的全集对其向量进行 0-1 编码, Bob 根据自己的数据在 Alice 的编码矩阵进行选择, 结合应用 Paillier 加密系统的加法同态性, 得到两方参与者向量的等分量数. 这种方案只能解决两方参与者计算向量等分量数问题, 不能直接推广到多方计算情形. 文献 [22] 中协议 2 对两方参与者分量数据取消了全集限制条件, 主要应用性质"$r_i(u_i-v_i) \mod N=0$ 当且仅当 $u_i=v_i$", 其中 u_i,v_i 分别是 Alice 和 Bob 所拥有向量 U,V 的分量. 由此可以看出文献 [22] 中协议 2 也很难推广到多方计算情形. 文献 [22] 中协议 3 在其协议 1 的基础上, 设计了两方向量等分量数阈值问题的保密计算协议. 文献 [22] 协议 3 中参与者的分量也存在全集限制条件, 并且也很难将其推广到多方计算情形.

显然如果取 $n=2$ 时, 本文协议 1 和协议 2 能够解决文献 [22] 中的相应问题, 由于本文协议适用于任意 n 个参与者, 并且对参与者数据范围没有全集限制条件, 因此本文对于向量等分量数及相关阈值多方保密计算问题的研究更加深入和广泛. 下面就 $n=2$ 这种特殊情形对本文协议和文献 [22] 中协议的性能进行分析与比较.

由于本文协议与文献 [22] 中协议都是通过计算过程中所需的模指数运算次数来衡量计算复杂性, 因此在对计算复杂性进行比较时, 我们通过模指数运算次数对本文协议与文献 [22] 中协议进行比较. 由于当 $n=2$ 时只有两个参与者, 在协议中不需考虑合谋问题, 因此本文不需要门限加密系统即可完成两方协议. 在 ElGamal 加密系统中, 应用加密算法 E 或 $\hat{E}$ 加密 1 次均需要 2 次模指数运算, 应用解密算法 D 或 $\hat{D}$ 解密 1 次均需要 1 次模指数运算. 文献 [22] 主要应用 Paillier 加密系统, 且文献 [22] 进一步强调在 Paillier 加密系统中, 加密 1 次均需要 2 次模指数运算, 解密 1 次均需要 1 次模指数运算. 由于文献 [22] 中大部分协议是在有全集限制的情况下进行的, 在下面分析中假设文献 [22] 中全集的势为 N, 并设本文与文献 [22] 中向量维数为 t, 本文中各分量位数不超过 m.

首先对本文协议 1 与文献 [22] 中协议 1 和协议 2 进行计算复杂性分析与比较. 本文协议 1 所需的模指数运算次数为 $t(2m+1)$, 文献 [22] 中协议 1, 协议 2 所需的模指数运算次数分别为 $2tN+1, 6t$. 由此可知, 在向量维数一致的情况下, 本文协议 1 的计算复杂性与各分量位数 m 呈线性关系, 文献 [22] 中协议 1 的计算复杂性与全集的势 N 呈线性关系. 当本文设向量各分量位数不超过 m 时, 由于不超过 m 位的非负整数共有 10^m 个, 因此相当于文献 [22] 协议 1 中全集的势 $N=10^m$. 例如当本文取 $m=3$ 时, 则说明向量分量的取值范围为 [0, 999], 此时文献 [22] 协议 1 中全集的势为 $N=10^3$. 因此本文协议 1 与文献 [22] 中协议 1 相比具有较高的效率. 在向量分量位数 $m\leqslant 2$ 时本文协议 1 与文献 [22] 中协议 2 相比具有较高的效率. 在 $m>2$ 时本文协议 1 与文献 [22] 协议 2 相比效率有所降低.

其次对本文协议 2 与文献 [22] 中协议 3 进行计算复杂性分析与比较. 本文协议 2 所需要的模指数运算次数为 $t(2m+1)+3(l_2+q_2+o_2)+r_2+14$, 文献 [22] 中协议 3 所需要的模指数运算次数为 $2tN+5$. 与本文协议 1 和文献 [22] 中协议 1 分析与比较过程类似, 若合理选择 q_2,o_2,l_2,r_2 的值, 本文协议 2 与文献 [22] 中协议 3 相比也具有较高的效率.

最后再对本文的两个协议与文献 [22] 中协议的通信复杂性进行分析与比较. 本文协议与文献 [22] 中协议都是通过通信过程中所需的通信轮数来衡量通信复杂性, 因此在对通信复杂性进行比较时, 我们通过通信轮数来对本文协议与文献 [22] 中协议进行比较. 在 $n=2$ 的情况下, 本文协议 1 与文献 [22] 中协议 1 和协议 2 都需要 1 轮通信. 本文协议 2 需要 3 轮通信, 文献 [22] 中协议 3 需要 1 轮通信. 但是文献 [22] 只能够解决两方向量等分量数以及等分量数阈值问题, 本文对其进行了扩展, 能够解决任意 $n,n\geqslant 2$ 方向量等分量数以及等分量数阈值问题.

5.3 协议效率实验测试

为测试执行本文协议所需的时间, 本节对协议 1, 协议 2 进行了模拟实验.

实验环境. Windows 10 64 位操作系统, 处理器参数为 Intel(R) Core(TM)i5-6200U CPU@2.30 GHz, 8 GB 内存, 用 Java 语言在 Eclipse 上运行实现, 本文所有模拟实验均在此环境下进行. 本文协议 1, 2 均使用 ElGamal 加密系统进行模拟, 并且全部忽略预处理所需时间.

由于协议 1 与协议 2 的执行时间与向量的维数 t 以及向量的分量位数 m 都有关, 在实验中首先固定向量的分量位数 $m=10$, 取向量的维数分别为 $t=5,10,15,20,25,30,35,40$, 观察执行时间随向量维数 t 的增长而变化的情

况 (模拟结果如图 1 所示). 为了观察协议 1 与协议 2 执行时间随向量分量位数 m 的增长而变化的情况, 固定向量的维数 $t=10$, 并分别取向量分量位数 $m=2,4,6,8,10,12,14,16$ (模拟结果如图 2 所示).

由图 1 (或图 2) 可知, 在向量分量位数 (或向量维数) 固定的情况下, 协议 1 和协议 2 的执行时间都随着向量维数 (或向量分量位数) 的增加而线性增长.

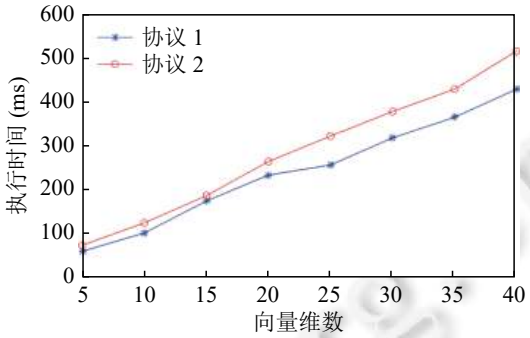

图 1 协议执行时间随向量维数增加的变化规律

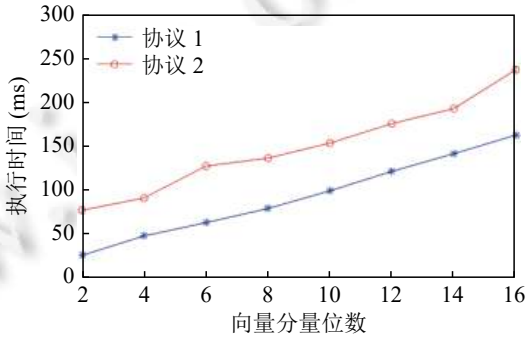

图 2 协议执行时间随向量分量位数增加的变化规律

6 推广应用

6.1 两方集合交集势的保密计算

应用向量等分量数保密计算的解决思想可以保密计算两个集合交集的势, 此时对集合中的元素没有数据范围的限制要求.

(1) 问题描述. 假设 Alice 和 Bob 分别拥有私密集合 X 和 Y, 集合 X 和 Y 的势分别为 d 和 e, 并假设 d 和 e 均不超过 t, 所有集合元素以十进制方式表示时均不超过 m 位. Alice 和 Bob 希望保密计算 X 和 Y 的交集的势 $\varphi(X,Y)=|X\cap Y|$, 而不泄露任何额外信息.

(2) 计算原理. 集合交集势指的是在不同集合中, 统计元素相同的个数. 向量等分量数指的是在不同向量中, 统计对应位置分量相同的个数. 由此可看出两个问题相同之处在于都是统计相同元素的个数, 不同之处在于向量中分量是有顺序的, 而集合中元素是无顺序的. 由于集合中元素的无序性, 不能通过统计集合对应位置元素相同的个数来得到集合交集的势. 因此若能够解决集合元素的无序性带来的问题, 则可以用向量等分量数保密计算问题的解决方案解决集合交集势保密计算问题. 协议 1 中由于向量的分量是有顺序的, 因此当 $P_2,\ldots,P_n$ 在根据自己的向量挑选时, 只需要挑选 P_1 的对应位置的编码矩阵中的元素即可. 在本问题中, 由于集合中元素的无序性, Bob 不能只挑选 Alice 的对应位置的编码矩阵中的元素, 而是要遍历 Alice 的所有编码矩阵. 剩下的协议执行步骤与协议 1 相同. 下面详细说明集合交集势的保密计算原理.

(i) Alice 根据第 3.1 节中的分量-矩阵编码方法对 X 中每个元素进行编码, 得到 d 个编码矩阵, 如果 $d<t$, 再添加 $t-d$ 个随机编码矩阵 (矩阵中所有元素均为不等于 1 的随机数), 如此即得到 t 个 $m\times 10$ 阶的编码矩阵, 记为 $A^j=(a^j_{kl})_{m\times 10}, j\in[1,t]$.

(ii) Bob 在 Alice 的编码矩阵 $A^1,\ldots,A^t$ 中按下述方式选择元素并做相应运算.

(a) 对于每个 $j\in[1,t]$, Bob 应用与协议 1 中 P_i 根据 x^j_i 的值在 A^j 中选择元素相同的法则, 对于 Y 中每个元素 $y=y_{a1}\ldots y_{am}, a\in[1,e]$ 在 A^j 中选择元素, Bob 在 A^j 中共选择得到 m 个元素:

$$a^j_{1y_{a1}+1},\ldots,a^j_{my_{am}+1}.$$

Bob 将这 m 个数据相乘, 得到 $u^j_a=\prod_{k=1}^{m}a^j_{ky_{ak}+1}$. 因此 Bob 得到 $u^j_1,\ldots,u^j_e$.

(b) 对于所有矩阵 $A^1,\ldots,A^t$ 完成元素选择及相应乘积运算后, Bob 得到数组:

$$U=(u^1_1,\ldots,u^1_e,\ldots,u^t_1,\ldots,u^t_e).$$

(c) 为保护集合 Y 的势 e 的私密性, 在数组 U 中通过添加不等于 1 的随机数元素, 将数组扩充到 t^2 维, 并将得到的新数组记为 H. 由协议 1 可知 H 中取值为 1 的元素个数即为 X 和 Y 的交集的势 $\varphi(X,Y)$.

协议 3. 两方集合交集势的保密计算协议.

输入: Alice 输入私密集合 X, Bob 输入私密集合 Y. X,Y 中各元素的位数均不超过 m, 势均不超过 t.

输出: $\varphi(X,Y)=|X\cap Y|$

准备: Alice 按照计算原理所述构造 t 个 $m\times 10$ 阶编码矩阵 (可能包括随机矩阵); Alice 运行 ElGamal 加密系统, 生成加密算法的私钥 sk 和公钥 pk, 并将 pk 发送给 Bob.

1. Alice 将矩阵 $A^1,\ldots,A^t$ 中所有取值为 1 的元素进行加密, 得到密文矩阵 $C^1=(c^1_{kl})_{m\times 10},\ldots,C^t=(c^t_{kl})_{m\times 10}$, 并将 $C^1,\ldots,C^t$ 发送给 Bob.

2. (a) 对于 $a\in[1,e]$, Bob 在矩阵 C^j 中第 $k,k\in[1,m]$ 行选择元素 $c^j_{ky_{ak}+1}$, 并且作乘积:

$$\bar{u}^j_a=\prod_{k=1}^{m}c^j_{ky_{ak}+1}.$$

(b) 遍历完集合 Y 中所有元素得到 $\bar{u}^j_1,\ldots,\bar{u}^j_e$.

(c) Bob 在所有矩阵 $C^1,\ldots,C^t$ 中挑选完元素后得到数组 $\bar{U}=(\bar{u}^1_1,\ldots,\bar{u}^1_e,\ldots,\bar{u}^t_1,\ldots,\bar{u}^t_e)$, 然后添加随机数, 将数组 $\bar{U}$ 变为 t^2 维数组 $\bar{H}=(\bar{h}^1_1,\ldots,\bar{h}^t_t)$. 将 $\bar{H}$ 随机置换以及重随机化后发送给 Alice.

3. Alice 对数组 $\bar{H}$ 解密 (逐项解密), 并记 $h^j_i=D(\bar{h}^j_i), i,j\in[1,t]$, 得到数组 $H=(h^1_1,\ldots,h^t_t)$. 公布数组 H 中值为 1 的元素个数 h.

定理 3. 协议 3 是正确的, 且在半诚实模型下是安全的.

证明:由计算原理可知, 协议 3 是在协议 1 的基础上设计的, 由协议 1 的正确性以及安全性可知, 协议 3 是正确的, 且在半诚实模型下是安全的.

注解 2. 协议 3 利用协议 1 的方案解决了两方集合交集势的保密计算问题, 协议 2 在协议 1 的基础上解决了向量等分量阈值问题. 因此利用协议 2, 在协议 3 的基础上即可设计两方集合交集势相关阈值问题的保密计算协议, 在此不做详细说明.

6.2 隐私保护下的记录链接

记录链接是指利用统计学原理, 识别不同文件中的相关记录是否描述同一个体. 在很多方向的应用前景非常广泛, 例如: 医疗、金融等领域. 但是, 在这些领域中, 保护数据信息的隐私是非常有必要的, 因此我们必须要考虑在将不同数据进行记录链接的基础上同时保证所有数据的隐私性. 若 n 个不同的数据库想要合作将其数据库中描述同一个体的记录进行链接, 并且不泄露信息, 则需要对这些数据库所拥有相关记录的标识符进行保密匹配: 假设在 n 个数据库中分别存储着 1 条医疗健康的数据记录, 保密判断这 n 条记录是否属于同一个实体, 也就是保密判断这 n 条记录的所有标识符匹配后相同个数是否达到某个阈值 b. 首先我们可以对标识符进行分属性处理 (例如,

姓名、性别、出生日期等), 假设有 t 个属性, 则每个属性为一个字符串, 将字符串编码成数字形式. 例如可采用 ASCII 码将字符串的每一个字符进行转换, 在转换时要注意, 由于 ASCII 码中一共 128 个字符, 因此, 在将字符转换成数字时, 保证每一个字符转换成位数为 3 的数字 (若不满 3 位, 可通过在前面添 0 的方式将其补充为 3 位). 经过这样的编码, 这 n 个数据库分别拥有 1 个 t 维的向量. 利用本文协议 2 即可保密判断这 n 个 t 维向量的等分量数是否大于阈值 b. 因此能够保密判断这 n 条记录是否能够进行链接.

7 结 论

本文设计了新的编码方法, 将参与者的向量分量转化为矩阵的形式, 结合 ElGamal 加密系统, 解决了有关向量等分量数的保密计算问题; 以向量等分量数保密计算协议为基础, 进一步研究了向量等分量数阈值问题的保密计算, 并证明了所设计协议的安全性. 根据上述协议的思想, 有效地解决了两个集合交集势以及交集势阈值的保密计算问题. 本文中的所有数据均不受全集的限制. 本文设计的多方向量等分量数以及相关阈值问题保密计算协议在记录链接的隐私保护方面有重要的作用. 在后续的工作中, 我们将进一步研究恶意模型下有关的向量等分量数安全计算问题以及其他向量的安全计算问题.

References:

[1] Goldreich O. Secure multi-party computation. 1998. 1–107.

[2] Lin HY, Tzeng WG. An efficient solution to the millionaires' problem based on homomorphic encryption. In: Proc. of the 3th Int'l Conf. on Applied Cryptography and Network Security. New York: Springer, 2005. 456–466. [doi: 10.1007/11496137_31]

[3] Zhang SG, Xian HQ, Wang LM, Liu HY. Secure cloud encrypted data deduplication method. Ruan Jian Xue Bao/Journal of Software, 2019, 30(12): 3815–3828 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5610.htm [doi: 10.13328/j.cnki.jos.005610]

[4] Collins MJ. Efficient secure multiparty computation of sparse vector dot products. Journal of Discrete Mathematical Sciences and Cryptography, 2018, 21(5): 1107–1117. [doi: 10.1080/09720529.2018.1453623]

[5] Grigoriev D, Shpilrain V. Yao's millionaires' problem and decoy-based public key encryption by classical physics. Int'l Journal of Foundations of Computer Science, 2014, 25(4): 409–417. [doi: 10.1142/S0129054114400036]

[6] Miyajima H, Shigei N, Miyajima H, Shiratori N. A proposal of profit sharing method for secure multiparty computation. Int'l Journal of Innovative Computing, Information and Control, 2018, 14(2): 727–735.

[7] Bogdanov D, Kamm L, Laur S, Pruulmann-Vengerfeldt P, Talviste R, Willemson J. Privacy-preserving statistical data analysis on federated databases. In: Proc. of the 2nd Annual Privacy Forum. Athens: Springer, 2014. 30–55. [doi: 10.1007/978-3-319-06749-0_3]

[8] Ge SS, Zeng P, Lu RX, Choo KKR. FGDA: Fine-grained data analysis in privacy-preserving smart grid communications. Peer-to-peer Networking and Applications, 2018, 11(5): 966–978. [doi: 10.1007/s12083-017-0618-9]

[9] Gong LM, Li SD, Dou JW, Guo YM, Wang DS. Homomorphic encryption scheme and a protocol on secure computing a line by two private points. Ruan Jian Xue Bao/Journal of Software, 2017, 28(12): 3274–3292 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5239.htm [doi: 10.13328/j.cnki.jos.005239]

[10] Liu L, Chen XF, Lou WJ. Secure three-party computational protocols for triangle area. Int'l Journal of Information Security, 2016, 15(1): 1–13. [doi: 10.1007/s10207-015-0284-y]

[11] Shao Y, Hong WJ, Li ZJ. A new method to compute ratio of secure summations and its application in privacy preserving distributed data mining. IEEE Access, 2019, 7: 20756–20766. [doi: 10.1109/ACCESS.2019.2894682]

[12] Qaosar M, Zaman A, Siddique MA, Annisa, Morimoto Y. Privacy-preserving secure computation of skyline query in distributed multi-party databases. Information, 2019, 10(3): 119. [doi: 10.3390/info10030119]

[13] Damgård I, Jurik M. A generalisation, a simplification and some applications of paillier's probabilistic public-key system. In: Proc. of the 4th Int'l Workshop on Practice and Theory in Public Key Cryptosystems. Cheju Island: Springer, 2001. 119–136. [doi: 10.1007/3-540-44586-2_9]

[14] Huang HP, Gong TH, Chen P, Malekian R, Chen T. Secure two-party distance computation protocol based on privacy homomorphism and scalar product in wireless sensor networks. Tsinghua Science and Technology, 2016, 21(4): 385–396. [doi: 10.1109/TST.2016.7536716]

[15] Wang BY, Li M, Xiong L. FastGeo: Efficient geometric range queries on encrypted spatial data. IEEE Trans. on Dependable and Secure

Computing, 2019, 16(2): 245–258. [doi: 10.1109/TDSC.2017.2684802]
[16] Atallah MJ, Du WL. Secure multi-party computational geometry. In: Proc. of the 7th Workshop on Algorithms and Data Structures. Providence: Springer, 2001. 165–179. [doi: 10.1007/3-540-44634-6_16]
[17] Li SD, Zuo XJ, Yang XL, Gong LM. Secure vector dominance protocol and its applications. Acta Electronica Sinica, 2017, 45(5): 1117–1123 (in Chinese with English abstract). [doi: 10.3969/j.issn.0372-2112.2017.05.014]
[18] Han SM, Shen DR, Nie TZ, Kou Y, Yu G. Multi-party privacy-preserving record linkage approach. Ruan Jian Xue Bao/Journal of Software, 2017, 28(9): 2281–2292 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5187.htm [doi: 10.13328/j.cnki.jos.005187]
[19] Essex A. Secure approximate string matching for privacy-preserving record linkage. IEEE Trans. on Information Forensics and Security, 2019, 14(10): 2623–2632. [doi: 10.1109/TIFS.2019.2903651]
[20] Liu W, Wang YB. Secure multi-party comparing protocol and its applications. Acta Electronica Sinica, 2012, 40(5): 871–876 (in Chinese with English abstract). [doi: 10.3969/j.issn.0372-2112.2012.05.002]
[21] Jarrous A, Pinkas B. Secure computation of functionalities based on Hamming distance and its application to computing document similarity. Int'l Journal of Applied Cryptography, 2013, 3(1): 21–46. [doi: 10.1504/IJACT.2013.053433]
[22] Wang YN, Dou JW, Ge X. Privately computing number of equal components of two private vectors and its applications. Journal of Cryptologic Research, 2020, 7(2): 145–157 (in Chinese with English abstract). [doi: 10.13868/j.cnki.jcr.000356]
[23] Goldreich O. Fundamental of Cryptography II: Basic Applications. Cambridge: Cambridge University Press, 2004. 599–764.
[24] Tsiounis Y, Yung M. On the security of ElGamal based encryption. In: Proc. of the 1st Int'l Workshop on Practice and Theory in Public Key Cryptography. Yokohama: Springer, 1998. 117–134. [doi: 10.1007/BFb0054019]
[25] Elgamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. on Information Theory, 1985, 31(4): 469–472. [doi: 10.1109/TIT.1985.1057074]

附中文参考文献:

[3] 张曙光, 咸鹤群, 王利明, 刘红燕. 云加密数据安全重复删除方法. 软件学报, 2019, 30(12): 3815–3828. http://www.jos.org.cn/1000-9825/5610.htm [doi: 10.13328/j.cnki.jos.005610]
[9] 巩林明, 李顺东, 窦家维, 郭奕旻, 王道顺. 同态加密方案及安全两点直线计算协议. 软件学报, 2017, 28(12): 3274–3292. http://www.jos.org.cn/1000-9825/5239.htm [doi: 10.13328/j.cnki.jos.005239]
[17] 李顺东, 左祥建, 杨晓莉, 巩林明. 安全向量优势协议及其应用. 电子学报, 2017, 45(5): 1117–1123. [doi: 10.3969/j.issn.0372-2112.2017.05.014]
[18] 韩姝敏, 申德荣, 聂铁铮, 寇月, 于戈. 一种基于隐私保护下的多方记录链接方法. 软件学报, 2017, 28(9): 2281–2292. http://www.jos.org.cn/1000-9825/5187.htm [doi: 10.13328/j.cnki.jos.005187]
[20] 刘文, 王永滨. 安全多方信息比较相等协议及其应用. 电子学报, 2012, 40(5): 871–876. [doi: 10.3969/j.issn.0372-2112.2012.05.002]
[22] 王颖囡, 窦家维, 葛雪. 向量等分量数的两方保密计算及推广应用. 密码学报, 2020, 7(2): 145–157. [doi: 10.13868/j.cnki.jcr.000356]

窦家维(1963－), 女, 博士, 副教授, 主要研究领域为密码学, 应用数学.

成雯(1996－), 女, 硕士, 主要研究领域为密码学, 安全多方计算.

陈明艳(1996－), 女, 硕士, 主要研究领域为密码学, 应用数学.