多重集的保密计算及应用

窦家维,陈明艳
(陕西师范大学数学与信息科学学院,陕西西安 710119)

摘 要: 安全多方计算是近年来国际密码学界研究的热点问题. 多重集作为标准集的推广在实际中有广泛的应用,对于多重集的保密计算问题研究具有重要的意义. 本文主要研究两方多重集的交集、并集以及基于阈值和集的保密计算问题. 首先针对不同问题设计相应的编码方法,结合 Paillier 加密方案设计保密计算协议,并应用模拟范例方法严格证明协议的安全性. 效率分析和实验验证表明本文所设计的协议是简单高效的.

关键词: 密码学; 两方安全计算; 多重集; 同态加密; 编码方法
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2020)01-0204-05
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2020.01.025

Secure Multiset Operations and Their Applications

DOU Jia-wei, CHEN Ming-yan
(*School of Mathematics and Information Science, Shaanxi Normal University, Xi'an, Shaanxi* 710119, *China*)

Abstract: Secure multiparty computation is one focus in the international cryptographic community in recent years. The private computation of multisets is also of great practical significance. In order to privately compute on multisets, we first propose two new encoding schemes. Then based on Paillier probabilistic encryption algorithm, we design three simple and efficient secure two party protocols to compute the intersection, the union and the summation of two private multisets. We prove that they are secure in the semi-honest model. We also analyze the computational complexities and communication complexities of the protocols and test the efficiency on a PC. The test result shows that our protocols are efficient.

Key words: cryptography; secure two-party computation; multiset; homomorphic encryption; encoding scheme

1 引言

安全多方计算(Secure Multiparty Computation, SMC)是解决两个或多个互不信任的参与方之间保护隐私的协同计算问题,计算结束后,参与计算的各方除了得到设定的计算结果外,不能获得其他参与方隐私数据的任何额外信息. 安全多方计算目前已发展成为一个重要的研究方向[1~5].

多重集是集合概念的推广,它允许元素重复出现,每个元素出现的次数称为该元素在多重集中的重数. 在下文中,为了避免混淆,将不允许出现重复元素的集合称为标准集.

目前,关于多重集的保密计算研究还很少. 文献[6]应用密码学方法设计了多个多重集的交集、并集及其势,以及有关集合阈值问题的计算协议,协议具有二次计算复杂性和线性通信复杂性. 文献[7]应用信息论的方法研究标准集和多重集的多种运算,协议要求各参与者之间具有安全认证信道. 文献[8]利用编码方法与加密算法,对于几种基本集合运算设计了安全高效的计算协议,文献[8]的部分结果经过转化后可应用于解决多重集问题,但计算效率较低. 由于目前已有的关于多重集的保密计算研究成果较少,计算复杂性较高,对于多重集的保密计算问题需要寻求高效的解决方案. 本文对文献[8]的主要结果进行了改进和推广,提高了计算效率,拓宽了应用范围. 本文主要贡献如下:

(1)提出了新的编码方法,将参与者的多重集转化成矩阵形式,通过计算乘积矩阵的对角线元素得到所需结果. 为解决其他问题提供了一种思想方法.

(2)针对不同问题的具体特点采用不同的编码方法,并结合 Paillier 加密算法设计了两方多重集交集、并集以及阈值和集的保密计算协议,应用模拟范例方法证明了协议的安全性.

收稿日期:2019-05-13;修回日期:2019-09-02;责任编辑:马兰英
基金项目:国家自然科学基金(No. 61272435)

(3)应用所设计的协议解决保密计算两个数的最大公约数以及最小公倍数等实际问题.

2 预备知识

2.1 半诚实模型及安全性定义

半诚实参与者按照协议要求执行协议,但在执行协议后试图利用其获得的信息推导出其他参与者隐私数据的额外信息. 如果参与者均为半诚实参与者,称此模型为半诚实模型[9].

设$f(x_1,x_2)=(f_1(x_1,x_2),f_2(x_1,x_2))$是概率多项式时间函数,$\pi$是计算函数$f$的协议. 参与者$P_i(i=1,2)$的输入为$x_i$,得到的信息序列记为$view_i^{\pi}=(x_i,r_i,m_1^i,\cdots,m_t^i,f_i(x_1,x_2))$,其中$r_i$是$P_i$产生的随机数,$m_1^i,\cdots,m_t^i$是$P_i$收到的消息,$f_i(x_1,x_2)$是$P_i$的输出结果.

对$f=(f_1,f_2)$,如果存在模拟器$S_i(i=1,2)$,使得下式成立:

$$\{S_i(x_i,f_i(x_1,x_2))\}_{x_1,x_2}\overset{c}{\equiv}\{view_i^{\pi}(x_1,x_2)\}_{x_1,x_2} \quad (1)$$

则称π保密地计算f,其中$\overset{c}{\equiv}$表示计算不可区分.

为证明一个协议是安全的,则需要构造出满足式(1)的模拟器,此方法即为模拟范例方法.

2.2 Paillier 加密方案

Paillier 加密方案简述如下[10].

密钥生成　对安全参数ξ,选取长度为ξ的素数p,q,令$\lambda=\mathrm{lcm}(p-1,q-1)$,$N=pq$. 定义$L(x)=\dfrac{x-1}{N}$,随机选择$g\in Z_{N^2}^*$,使得$\gcd(L(g^{\lambda}\bmod N^2),N)=1$,算法的公钥为$pk=(g,N)$,私钥为$sk=\lambda$.

加密　对于明文$m\in Z_N$,选择随机数$r\in Z_N^*$,计算密文$E(m)=g^m r^N \bmod N^2$.

解密　对于密文$c\in Z_{N^2}^*$,计算明文$D(c)=\dfrac{L(c^{\lambda}\bmod N^2)}{L(g^{\lambda}\bmod N^2)}\bmod N$.

加法同态性　加密算法具有加法同态性,即对于$m_1,m_2\in Z_N$,有:

$$E(m_1)E(m_2)=E(m_1+m_2 \bmod N) \quad (2)$$

Paillier 加密方案是语义安全的,这意味一个明文可以加密成多个不同的密文形式,并且所有密文都是计算不可区分的.

如果选取$g=1+kN$(k为正整数),应用 Paillier 加密方案加密及解密一次均需要一次模指数运算,下文中将g选为$1+kN$的形式.

2.3 多重集的表示及基本运算

下文中假设参与者拥有的多重集X,Y中元素均属于全集$Q=\{q_1,q_2,\cdots,q_n\}$. 对任意$k\in[1,n]=\{1,\cdots,n\}$,设q_k在X,Y中的重数分别为s_k,t_k(若$q_k\notin X$(或Y),则$s_k=0$(或$t_k=0$)). 若以$X\cap Y,X\cup Y,X\uplus Y$分别表示$X,Y$的交集、并集与和集,并设$\alpha_k,\beta_k,\gamma_k$分别为$q_k\in Q$在$X\cap Y,X\cup Y,X\uplus Y$中的重数,则有:

$$\alpha_k=\min\{s_k,t_k\},\beta_k=\max\{s_k,t_k\},\gamma_k=s_k+t_k \quad (3)$$

3 两方多重集交集保密计算

3.1 问题描述及计算原理

问题描述　假设 Alice 和 Bob 分别拥有私密多重集X和Y,且X,Y中元素重数均不超过m. 双方希望保密计算$X\cap Y$.

计算原理

(1)Alice 和 Bob 分别将X,Y编码成矩阵$\boldsymbol{A},\boldsymbol{B}$,记为编码 1. 具体如下:对于每一个$q_k\in Q,k\in[1,n]$.

(ⅰ)根据q_k在X中的重数s_k,构造$\boldsymbol{A}$的第k行$A_k=(a_{k1},\cdots,a_{km})$:当$0\leqslant j\leqslant s_k$时,$a_{kj}=1$;当$s_k<j\leqslant m$时,$a_{kj}=0$.

(ⅱ)根据q_k在 Y 中的重数t_k,构造$\boldsymbol{B}$的第k列$B_k=(b_{1k},\cdots,b_{mk})^T$:当$0\leqslant i\leqslant t_k$时,$b_{ik}=1$;当$t_k<i\leqslant m$时,$b_{ik}=0$.

(2)计算矩阵$\boldsymbol{C}=(c_{ij})=\boldsymbol{AB}$,则$c_{kk}=\sum_{i=1}^{m}a_{ki}b_{ik}$. 容易证明下面结论:

命题 1　$q_k\in X\cap Y\Leftrightarrow c_{kk}>0(k\in[1,n])$,且$q_k$在$X\cap Y$中的重数为$\alpha_k=c_{kk}$.

(3)根据数组$\alpha=(\alpha_1,\cdots,\alpha_n)$构造交集:若$\alpha_k=0$,则$q_k\notin X\cap Y$,若$\alpha_k>0$,则$q_k\in X\cap Y$,且在$X\cap Y$中重数为$\alpha_k$.

3.2 交集保密计算协议

协议 1　两方多重集交集保密计算协议

输入:Alice 输入多重集X,Bob 输入多重集Y.

输出:$X\cap Y$.

准备:Alice 和 Bob 利用编码 1 分别将X,Y编码成矩阵$\boldsymbol{A}=(a_{ij})$,$\boldsymbol{B}=(b_{ij})$. Alice 运行 Paillier 加密方案,生成公钥/私钥.

(1)Alice 对$\boldsymbol{A}$的每个元素加密,得到$\boldsymbol{E}(\boldsymbol{A})=(\boldsymbol{E}(a_{ij}))$,将$\boldsymbol{E}(\boldsymbol{A})$发送给 Bob.

(2)对每个$k\in[1,n]$,Bob 计算$Z_k=\prod_{i=1}^{m}E(a_{ki})^{b_{ik}}$,并将$Z_1,\cdots,Z_n$发送给 Alice.

(3)Alice 解密$Z_k(k\in[1,n])$,记$z_k=D(Z_k)$,得到$z=(z_1,\cdots,z_n)$,并根据计算原理和数组z构造交集.

3.3 协议的正确性和安全性

在协议 1 中,根据加密方案的加法同态性,Alice 解密Z_k得到$z_k=a_{k1}b_{1k}+\cdots+a_{km}b_{mk}=\alpha_k$,根据命题 1,协议 1 是正确的.

定理 1　协议 1 在半诚实模型下是安全的.

证明　应用模拟范例证明定理 1,首先构造S_1.

接受到输入$(X,f_1(X,Y)=X\cap Y)$后,S_1按如下方式运行:

(ⅰ)S_1任意选取满足$X\cap Y'=X\cap Y$的多重集Y',按照编码1构造Y'对应的矩阵$\boldsymbol{B}'=(b'_{ij})$.

(ⅱ)对任意$k\in[1,n]$,S_1计算$Z'_k=\prod_{i=1}^{m}E(a_{ki})^{b'_{ik}}$.

(ⅲ)S_1解密$Z'_k(k\in[1,n])$,记$z'_k=D(Z'_k)$,根据$z'=(z'_1,\cdots,z'_n)$构造$X\cap Y'$.

在协议执行中,$view_1(X,Y)=\{X,Z_1,\cdots,Z_n,X\cap Y\}$,令

$$S_1(X,f_1(X,Y))=\{X,Z'_1,\cdots,Z'_n,X\cap Y'\} \tag{4}$$

根据加密方案的语义安全性,$Z_k\overset{c}{\equiv}Z'_k(k\in[1,n])$.又由于$X\cap Y=X\cap Y'$,因此

$$\{S_1(X,f_1(X,Y))\}\overset{c}{\equiv}\{view_1(X,Y)\} \tag{5}$$

S_2可用类似方法构造,在此省略.因此定理1得证.

4 两方多重集并集保密计算

问题描述 假设Alice和Bob分别拥有私密多重集X和Y,元素重数均不超过m.双方希望保密计算$X\cup Y$.

计算原理

(1)Alice和Bob分别将X,Y编码成矩阵$\boldsymbol{A},\boldsymbol{B}$,记为编码2.具体如下:对于每一个$q_k\in Q,k\in[1,n]$.

(ⅰ)根据q_k在X中的重数s_k,构造$\boldsymbol{A}$的第k行$\boldsymbol{A}_k=(a_{k1},\cdots,a_{km})$:当$0\leqslant j\leqslant s_k$时,$a_{kj}=0$;当$s_k<j\leqslant m$时,$a_{kj}=1$.

(ⅱ)根据q_k在Y中的重数t_k,构造$\boldsymbol{B}$的第k列$\boldsymbol{B}_k=(b_{1k},\cdots,b_{mk})^{\mathrm{T}}$:当$0\leqslant i\leqslant t_k$时,$b_{ik}=0$;当$t_k<i\leqslant m$时,$b_{ik}=1$.

(2)计算矩阵$\boldsymbol{C}=(c_{ij})=\boldsymbol{AB}$,则$c_{kk}=\sum_{i=1}^{m}a_{ki}b_{ik}$.容易证明下面结论:

命题2 $q_k\in X\cup Y\Leftrightarrow c_{kk}<m(k\in[1,n])$,且$q_k$在$X\cup Y$中的重数为$\beta_k=m-c_{kk}$.

(3)根据$v=(\beta_1,\cdots,\beta_n)$构造$X\cup Y$:若$\beta_k=0$,则$q_k\notin X\cup Y$;若$\beta_k>0$,则$q_k\in X\cup Y$,且在$X\cup Y$中重数为$\beta_k$.

协议设计 将协议1中第(3)步改为下面(3′),其他保持不变,即可得到并集协议,记为协议2.

协议2 两方多重集并集保密计算协议

(3′)Alice解密$Z_k(k\in[1,n])$,并记$z_k=m-D(Z_k)$,根据计算原理及$v=(m-z_1,\cdots,m-z_n)$构造并集.

与协议1类似,我们有下面定理,证明省略.

定理2 在半诚实模型下协议2是正确的和安全的.

5 基于阈值的多重集保密求和问题

5.1 问题描述及计算原理

问题描述 假设Alice和Bob分别拥有私密多重集X与Y,设q_k在X,Y中的重数分别为s_k,t_k,双方希望保密计算$X\uplus Y$中重数达到阈值t的元素构成的集合.将这样的集合称为X,Y的阈值和集,记为$S_t(X,Y)$.

计算原理 根据$S_t(X,Y)$的定义,容易证明下面结果.

命题3 $q_k\in S_t(X,Y)\Leftrightarrow\lambda_k=s_k+t_k\geq t(k\in[1,n])$,且$q_k$在$S_t(X,Y)$中的重数为$\gamma_k=\lambda_k$.

5.2 阈值和集保密计算协议

协议3 基于阈值的多重集保密求和计算协议

输入:Alice输入多重集X,Bob输入多重集Y.

输出:$S_t(X,Y)$.

(1)Alice运行Paillier加密方案,生成公钥/私钥;并计算$U=(E(s_1),\cdots,E(s_n))$,将U发送给Bob.

(2)(*a*)对于每一个$k\in[1,n]$,Bob加密t_k,并计算$W_k=E(s_k)E(t_k)$.

(*b*)Bob在区间$[0,t)$内选取l个随机数$r_j,j\in[1,l]$,加密得到$W_{n+j}=E(r_j)$.

(*c*)Bob将数组$W=(W_1,\cdots,W_n,W_{n+1},\cdots,W_{n+l})$中元素进行随机置换(记为$\tau$),得到$W^*=(W_1^*,\cdots,W_{n+l}^*)$,并将$W^*$发送给Alice.

(3)(*a*)Alice逐分量解密W^*,得到$w^*=(w_1^*,\cdots,w_{n+l}^*)$.

(*b*)Alice根据w^*构建集合$H^*=\{(j,w_j^*)\mid w_j^*\geq t,j\in[1,n+l]\}$,将$H^*$发送给Bob.

(4)(*a*)对每个$(j,w_j^*)\in H^*$,Bob计算j的原像$\tau^{-1}(j)$,得到$(q_{\tau^{-1}(j)},w_j^*)$.

(*b*)Bob构造集合$H:q_{\tau^{-1}(j)}\in H$当且仅当$(j,w_j^*)\in H^*$,且$q_{\tau^{-1}(j)}$在H中的重数为w_j^*.

(5)输出H.

5.3 协议3的正确性

由于协议中进行随机置换τ是为保证安全性,对正确性没有影响,因此这里不妨设τ为恒等变换.此时对于任意$k\in[1,n]$,有$W_k^*=W_k$.由加密算法的加法同态性,Alice解密W_k^*后得到$w_k^*=s_k+t_k$,则$w_k=s_k+t_k$.由协议3可知:

$$s_k+t_k\geq t\Leftrightarrow w_k\geq t\Leftrightarrow(k,w_k)\in H^* \tag{6}$$

此时$q_k\in H$,且q_k在H中的重数为$w_k=s_k+t_k=\gamma_k$.根据命题3,有$H=S_t(X,Y)$,因此协议3是正确的.

5.4 协议3的安全性

定理3 在半诚实模型下协议3是安全的.

证明 应用模拟范例证明定理3,首先构造S_1.

接受到输入$(X,f_1(X,Y)=S_t(X,Y))$后,S_1 按照如下方式运行:

(ⅰ)S_1 任意选取满足 $S_t(X,Y')=S_t(X,Y)$的多重集 Y',记 $q_k(k\in[1,n])$在 Y'中的重数为 t_k'.

(ⅱ)S_1 计算 $W_k'=E(s_k)E(t_k')$,$k\in[1,n]$.

(ⅲ)S_1 在区间$[0,t)$内选取随机数 $r_j'(j\in[1,l])$,加密后得到 $W_{n+j}'=E(r_j')$. 并对 $W'=(W_1',\cdots,W_n',W_{n+1}',\cdots,W_{n+l}')$中元素进行随机置换(记为 τ'),得到 $W'^*=(W_1'^*,\cdots,W_{n+l}'^*)$.

(ⅳ)S_1 逐分量解密 W'^*,得到 $w'^*=(w_1'^*,\cdots,w_{n+l}'^*)$,根据 w'^*构建集合:

$$H'^*=\{(j,w_j'^*)\mid w_j'^*\geq t,j\in[1,n+l]\}.$$

(ⅴ)S_1 对每个$(j,w_j'^*)\in H'^*$,计算$(q_{\tau'^{-1}(j)},w_j'^*)$,并构造集合 H':$q_{\tau'^{-1}(j)}\in H'$ 当且仅当$(j,w_j'^*)\in H'^*$,并且 $q_{\tau'^{-1}(j)}$在 H'中的重数为 $w_j'^*$.

在协议执行中 $view_1(X,Y)=\{X,W^*=(W_1^*,\cdots,W_{n+l}^*),S_t(X,Y)\}$,令:

$$S_1(X,f_1(X,Y))=\{X,W'^*=(W_1'^*,\cdots,W_{n+l}'^*),S_t(X,Y')\} \tag{7}$$

Alice 解密 $W_k^*(k\in[1,n])$后仅得到 $w^*=(w_1^*,\cdots,w_{n+l}^*)$. 由于 w^*的 $n+l$ 个元素中,其中 n 个元素分别为 $q_1,\cdots,q_n$ 在 $X\uplus Y$ 中的重数,另外 l 个元素是小于 t 的随机数. 对于 w^*中大于等于 t 的所有元素 w_k^*,根据输出集合 $S_t(X,Y)$是能够推导出来的,不存在信息泄漏问题. 对于 w^*中小于 t 的元素 w_k^*(假设这些元素构成集合 M),由于 M 里混有 l 个随机数,又由于对 M 中的数据进行过随机置换,根据概率论知识,Alice 能准确猜测所有未达到阈值元素的重数的概率为 $P=(C_{l+h}^h h!)^{-1}=[(l+h)(l+h-1)\cdots(l+1)]^{-1}$. 因此当 l 取得适当大时,Alice 无法判断 M 中哪些元素可能是某个 s_k+t_k,哪些可能是随机数,更无法获得 Q 中元素和这些数的对应关系,即 Alice 从 w^*中无法得到多重集 Y 中元素的任何额外信息. 故有 $W^*\overset{c}{\equiv}W'^*$. 又由于 $S_t(X,Y)=S_t(X,Y')$,因此,

$$\{S_1(X,f_1(X,Y))\}\overset{c}{\equiv}\{view_1(X,Y)\} \tag{8}$$

S_2 可用类似方法构造. 定理 3 得证.

6　效率分析和实验测试

计算复杂性和通信复杂性　计算复杂性仅考虑最费时的模指数运算;通信复杂性以协议需要的通信次数衡量.

协议 1(2)中 Alice 加密矩阵 $\boldsymbol{A}$,解密 $Z_k(k\in[1,n])$. 协议共需 $n(m+1)$次模指数运算;通信次数为 3 次.

协议 3 中需要加密 s_k,t_k 以及 $r_1,\cdots,r_l$,解密数组 W^*. 协议共需 $3n+2l$ 次模指数运算;通信次数为 4 次.

协议效率实验测试

实验环境　Windows 10 64 位操作系统,处理器参数为 Intel(R) Core(TM) i5-4590s CPU@3.00GHz,4GB 内存. 用 Java 语言在 Eclipse 上运行实现.

由于协议 1(2)执行时间与全集的势 n 以及多重集中元素最大重数 m 有关. 协议 3 执行时间仅与 n 有关. 实验中固定 $m=10$(或 $n=10$),考察协议执行时间随 n(或 m)的变化情况,参看图 1(或图 2).

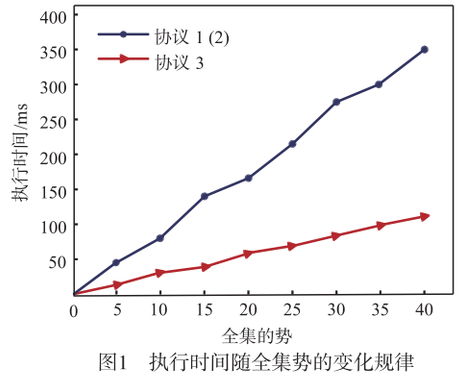


图1　执行时间随全集势的变化规律

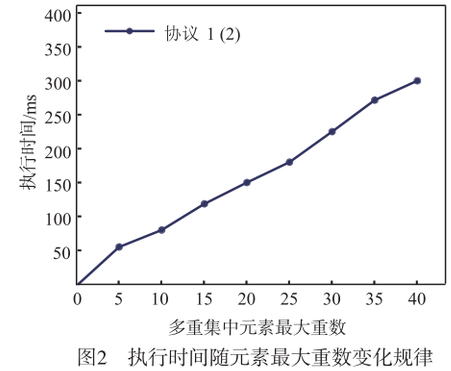


图2　执行时间随元素最大重数变化规律

由上图知,当 m(或 n)固定时,协议的执行时间随 n(或 m)的增加而线性增长.

与文献[8]中相关结果进行比较

当输入集为标准集时,本文协议 1(2)与文献[8]协议 1(2)分别需要 $2n$ 与 $5n$ 次模指数运算. 本文协议 3 与文献[8]协议 6 分别需要 $3n+2l$ 与 $3n+4k$ 次模指数运算(其中 k 为各参与者私密集合的势),此外,后者还需调用 $(t-1)n$ 次 IsEq 协议. 输入集为多重集时,本文协议 1(2)与文献[8]中协议 1(2)分别需要 $n(m+1)$与 $5mn$ 次模指数运算,文献[8]协议 6 无法解决多重集的问题. 因此本文结果对文献[8]的主要结果进行了改进和推广.

7　协议的推广应用

保密计算两个数的最大公约数和最小公倍数　假设 Alice 和 Bob 各自拥有数据 a,b,双方希望保密计算

a,b 的最大公约数(最小公倍数).

计算方案 Alice 和 Bob 首先分别将 a,b 写成素数幂的乘积:$a=p_1^{x_1}p_2^{x_2}\cdots p_n^{x_n}$,$b=q_1^{y_1}q_2^{y_2}\cdots q_m^{y_m}$. 将所有素数作为多重集中相异元素,相应幂指数作为对应元素的重数,得到多重集 X,Y. 再分别以 X,Y 为输入执行协议 1(2)即可.

参考文献

[1] Freedman M J, Hazay C, Nissim K, et al. Efficient set intersection with simulation-based security[J]. Journal of Cryptology, 2016, 29(1): 115 – 155.

[2] Cramer R, Damgard I B, Nielsen J B. Secure Multiparty Computation[M]. London: Cambridge University Press, 2015.

[3] Yao A C. Protocols for secure computations[A]. The 23th IEEE Symposiumon Foundations of Computer Science [C]. Chicago, Illinois, USA, 1982. 160 – 164.

[4] 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.

[5] Hirofumi M, Noritaka S, Hiromi M. A proposal of profit sharing method for secure multiparty computation[J]. International Journal of Innovative Computing Information and Control, 2018, 14(2): 727 – 735.

[6] Kissner L, Song D. Privacy-preserving set operations[A]. The 25th Annual International Cryptology Conference[C]. Santa Barbara, California, USA, 2005. 241 – 257.

[7] Blanton M, Aguiar E. Private and oblivious set and multiset operations[J]. International Journal of Information Security, 2016, 15(4): 493 – 518.

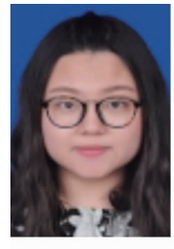
[8] 窦家维,刘旭红,周素芳,等. 高效的集合安全多方计算协议及应用[J]. 计算机学报,2018,41(8):1844 – 1860.
Dou Jia-wei, Liu Xu-hong, Zhou Su-fang, et al. Efficient secure multiparty set operations protocols and their application [J]. Chinese Journal of Computers, 2018, 41(8): 1844 – 1860. (in Chinese)

[9] Goldreich O. The Fundamental of Cryptography: Basic Applications[M]. London: Cambridge University Press, 2004. 599 – 764.

[10] Paillier P. Public-key cryptosystems based on composite degree residuosity classes[A]. International Conference on the Theory and Application of Cryptographic Techniques[C]. Prague, Czech Republic, 1999. 223 – 238.

作者简介

窦家维 女,1963 年生于陕西. 现为陕西师范大学数学与信息科学学院硕士生导师. 主要研究方向为应用数学和密码学.
E-mail: jiawei@ snnu. edu. cn



陈明艳 女,1996 年生于内蒙古. 研究生. 主要研究方向为应用数学和密码学.
E-mail: chenmingyan@ snnu. edu. cn