数据相等问题的安全多方计算方案研究

窦家维[1],李顺东[2]
(1. 陕西师范大学数学与信息科学学院,陕西西安 710062;2. 陕西师范大学计算机科学学院,陕西西安 710062)

摘 要: 安全多方计算是国际密码学界近年来的研究热点. 本文主要研究科学计算中多个数据相等问题的安全多方计算,目前关于这个问题的研究还很少. 本文设计了一种新的编码方法,以新的编码方法与 ElGamal 同态加密算法为基础,分别利用秘密分享技术和门限密码体制构造了两个在半诚实模型下能够抵抗合谋攻击的保密判定协议,应用模拟范例证明了协议的安全性,效率分析表明所设计的保密计算协议是高效的协议. 并进一步设计了恶意模型下的安全计算方案.

关键词: 安全多方计算; 多数据相等判定; 编码方案; 模拟范例; 半诚实模型; 恶意模型
中图分类号: TP309.7 **文献标识码:** A **文章编号:** 0372-2112 (2018)05-1107-06
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2018.05.013

Secure Multiparty Computation for the Equality Problem

DOU Jia-wei[1], LI Shun-dong[2]
(1. *School of Mathematics and Information Science, Shaanxi Normal University, Xi'an, Shaanxi* 710062, *China*;
2. *School of Computer Science, Shaanxi Normal University, Xi'an, Shaanxi* 710062, *China*)

Abstract: Secure multiparty computation has become a focus in the international cryptographic community in recent years. In this paper, we consider how to privately determine whether multiple private data owned by different parties are equal. There is very little literature on this problem at present. To solve this problem, we first propose a new encoding scheme and then use this new encoding scheme together with the threshold ElGamal homomorphic encryption scheme and secret sharing to construct our protocols. We prove that these protocols are private in the semi-honest model by using the well-accepted simulation paradigm. These protocols are also private against collusion attack. Efficiency analysis shows that these protocols are efficient. We further construct a protocol that is secure in the malicious model.

Key words: secure multiparty computation; multi-data equality test; encoding scheme; simulation paradigm; semi-honest model; malicious model

1 引言

安全多方计算是国际密码学界近年来的研究热点[1~3]. 安全多方计算是指两个或更多参与者利用各自的保密数据联合进行的保密计算. 计算结束后,没有参与方能够获得多于规定输出的信息. 保密的科学计算是安全多方计算的一个重要方面,这方面已经取得了很多好的研究成果[4~7]. 保密判断两个数是否相等在实际中有重要应用并得到了广泛的研究[8,9]. 保密判断多个数是否相等也是科学计算中的重要问题,目前对于这个问题的研究结果还很少[10~12]. 文献[10,11]所构造的多数据相等判定方案分别需要可信的第三方或代理机构帮助实施,而寻求一个多方都信任的可信方并非易事. 文[12]所设计的多数据相等保密判定协议在多个数据不相等的情形下会泄露很多信息,且在参与者人数较多或数据范围较大时计算复杂性很高. 因此对多个数据是否相等的保密判定问题需要进一步研究. 本文研究设计了几个多数据相等问题的保密判定协议,本文的贡献如下:

(1) 提出了一种新的编码方法,使每个参与者的保密数据隐藏在一个特殊数组中. 这种编码方法可以为解决其它安全多方计算问题提供一种新的途径.

(2) 本文对安全多方计算协议的安全性定义进行了推广,即当一个实际计算协议不能完全满足该领域

收稿日期:2016-12-26;修回日期:2017-02-06;责任编辑:马兰英
基金项目:国家自然科学基金(No. 61272435)

的经典著作[13]中描述的安全性要求时(定义1),可通过与定义1进行比较以对协议的实际安全性进行描述.

(3) 利用所设计的新编码方法、ElGamal同态加密算法,以及秘密分享和门限密码体制在半诚实模型下设计了两个保密判断多数据相等问题的高效解决方案.应用模拟范例证明了协议的安全性.

(4) 在半诚实模型下保密计算协议的基础上设计了一个在恶意模型下也安全的计算协议.

2 预备知识

2.1 半诚实模型

在半诚实模型中要求所有的参与者都是半诚实的.所谓半诚实参与者是指在协议的执行过程中能按照协议要求履行协议,但他们可能会记录下协议执行过程中收集到的所有信息,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.在半诚实模型下多方计算协议的安全性通常由下面的模拟范例进行描述[13].

设有 m 个参与者 $P_1,\cdots,P_m$,分别具有保密数据 $x_1,\cdots,x_m$,记 $\bar{x}=(x_1,\cdots,x_m)$,他们利用协议 π 保密地计算 $f(\bar{x})$.在协议执行过程中,P_i 得到的信息序列记为

$$view_i^{\pi}(\bar{x})=(x_i,r_i,M_i^1,\cdots,M_i^t)$$

其中 $M_i^j(i=1,\cdots,m,j=1,\cdots,t)$ 表示 P_i 收到的第 j 个信息.对于部分参与者构成的子集 $I=\{P_{i_1},\cdots,P_{i_s}\}\subseteq\{P_1,\cdots,P_m\}$,记

$$view_I^{\pi}(\bar{x})=(I,view_{i_1}^{\pi}(\bar{x}),\cdots,view_{i_s}^{\pi}(\bar{x}))$$

定义1 (半诚实参与者协议的安全性[13]) 在参与者都是半诚实的情况下,如果对于任意的 $I=\{P_{i_1},\cdots,P_{i_s}\}\subseteq\{P_1,\cdots,P_m\}$,都存在概率多项式时间算法 S,使得下式成立:

$$\begin{aligned}&\{S(I,(x_{i_1},\cdots,x_{i_s}),f_I(\bar{x}))\}_{\bar{x}\in(\{0,1\}^*)^m}\\&\overset{c}{\equiv}\{(view_I^{\pi}(\bar{x})\}_{\bar{x}\in(\{0,1\}^*)^m}\end{aligned}\tag{1}$$

其中,$\overset{c}{\equiv}$ 表示计算上不可区分,则称协议 π 保密地计算了 m 元函数 f.

在实际中经常由于保密计算问题本身对安全性的要求,或基于效率方面的考虑,对某些保密计算问题不需要或不容易设计出完全满足定义1安全性要求的协议,在此情形下可通过和定义1所述的安全性进行比较来刻画一个实际多方计算协议的安全性.

2.2 恶意模型

关于恶意模型下协议的安全性定义以及如何由半诚实模型下的保密计算协议编译获得恶意模型下的安全计算协议的具体方案,可参看文[13]详细了解.

恶意模型下安全的多方计算协议应迫使各参与者像半诚实参与者一样按协议要求执行协议.但有三种恶意行为无法避免(在任意协议中),即参与者拒绝参加协议,参与者修改其原本规定的输入数据而用其它数据替代,以及参与者在协议执行过程中可能随时中止协议.因此在恶意模型下考虑协议的安全性时这几种恶意行为原则上不予考虑[13].

2.3 ElGamal同态加密系统

ElGamal加密系统是一种具有乘法同态性的公钥加密系统,并且是语义安全的.具体描述如下[14]:

密钥生成 给定安全参数 k,密钥生成算法生成一个 k 比特的大素数 p 以及 Z_p^* 的一个生成元 g,随机选取 $x\in Z_p^*$ 作为私钥,对应的公钥为 $h=g^x \bmod p$.

加密 为加密消息 $M(M\in Z_p^*)$,选择随机数 r,密文为:

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

解密 对于密文 $E(M)=(c_1,c_2)$,解密为:

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

同态性质 加密系统具有乘法同态性:

$$\begin{aligned}E(M_1)\times E(M_2)&=(g^{r_1},M_1h^{r_1})\times(g^{r_2},M_2h^{r_2})\\&=(g^{r_1+r_2},M_1\times M_2h^{r_1+r_2})\\&=E(M_1\times M_2).\end{aligned}$$

3 基于ElGamal公钥密码系统的多数据相等保密判定协议

3.1 编码方法

假设 m 个参与者 $P_i(i=1,\cdots,m)$ 分别具有保密数据 $x_i,x_i\in H=\{z_1,\cdots,z_n\}$,其中 $z_1<\cdots<z_n$.记 x_i 在 H 中的序号为 $(x_i)_{ind}$,即如果 $x_i=z_k$,则 $(x_i)_{ind}=k$.m 个参与者希望在不泄露各自保密数据的前提下合作计算函数 $y=P(\bar{x})$:如果 $x_1=\cdots=x_m$,$P(\bar{x})=1$,否则 $P(\bar{x})=0$.

参与者 P_1 首先构造一个数组:

$$\bar{u}=(u_1,\cdots,u_n)\tag{2}$$

其中,$u_{(x_1)_{ind}}=1$,其它 $u_k=r_k$,$r_k\in Z_p^*$ 为不等于1的随机数.这样,P_1 拥有的数据 x_1 将转化成(2)形式的数组表达.由数组 $\bar{u}$ 的构造方法,容易证明下面结论:

命题1 m 个数据 $x_1,\cdots,x_m$ 相等的充要条件是:

$$u_{(x_2)_{ind}}\cdots u_{(x_m)_{ind}}=1\tag{3}$$

上面提出的编码方法和命题1是我们判断多个数据相等与否的基本原理.下面将应用ElGamal公钥加密系统保密判断式(3)是否成立.如果 a,b,c,d,e 均为整数,并且 $u=(a,b)$,$v=(c,d)$,下文中约定 $uv=(ac,bd)$,$ev=(ec,ed)$.

3.2 基于ElGamal公钥密码系统的多数据相等保密判定协议

协议1 多数据相等保密判定协议(半诚实模型)

输入:$P_1,\cdots,P_m$ 各自的秘密数据 $x_1,\cdots,x_m$.

输出:$y=P(\bar{x})$.

(1)P_1 应用 ElGamal 公钥系统生成私钥/公钥对 *sk/pk*,并公布公钥 *pk*.

(2)P_1 用下面方式将数据 x_1 转化为一个 $n\times 2$ 阶的秘密矩阵 $\bar{\boldsymbol{v}}=(v_1,\cdots,v_n)^{\mathrm{T}}$,其中 $v_{(x_1)_{ind}}=E(1)$,其它 $v_k=(r_k,s_k)$($E(1)$是应用公钥 *pk* 加密 1 所得的密文,$r_k,s_k\in Z_p^*$ 为随机数). P_1 公布 $\bar{v}$.

(3)每个参与者 $P_i(i=2,\cdots,m)$计算如下:

(*a*)P_i 选取随机数 $r_{it}(t=2,\cdots,m)$,使其满足:$\prod_{t=2}^{m} r_{it}\bmod p=1$,并将 r_{it} 分别发送给 $P_t(t=2,\cdots,m)$(包括给自己留一份).

(*b*)P_i 应用公钥 *pk* 加密 1,得到 $E(1)$,并将其与自己收到的所有随机数份额(包括自己保留的份额)以及 $v_{(x_i)_{ind}}$ 相乘,得到 $X_i=r_{2i}\cdots r_{mi}E(1)v_{(x_i)_{ind}}$.

(*c*)P_i 将 X_i 发送给 P_1.

(4)P_1 将收到的所有数据 $X_i(i=2,\cdots,m)$相乘,得到 $X=X_2\cdots X_m$.

(5)P_1 解密 X. 如果解密结果 $\mathrm{Dec}(X)=1$,P_1 公布 $y=1$,否则,P_1 公布 $y=0$.

3.3　协议分析

正确性分析　由协议的构造过程可知:

$$X=X_2\cdots X_m=\prod_{i=2}^{m}(E(1)v_{(x_i)_{ind}}\prod_{j=2}^{m}r_{ij})\bmod p$$

其中 $\prod_{i=2}^{m}\prod_{j=2}^{m}r_{ij}\bmod p=1$. 如果 $x_1=\cdots=x_m$,则对所有 $i=2,\cdots,m$,$v_{(x_i)_{ind}}=E(1)$,显然解密得 $\mathrm{Dec}(X)=1$,因此 $y=1$. 如果 $x_2,\cdots,x_m$ 中有一个不同于 x_1,则所得到的 X 为一个随机数,$\mathrm{Dec}(X)$也是随机数,因此 $y=0$.

安全性分析　由于在协议 1 中,参与者 $P_2,\cdots,P_m$ 的地位是平等的,为证明协议的安全性,只需分别考虑 P_1,P_m 数据的安全性. 我们将证明,P_1 的数据对于其他 $m-1$ 个参与者 $I_1=\{P_2,\cdots,P_m\}$ 构成的合谋攻击是安全的,而 P_m 的数据对于其他任意 $m-2$ 个参与者的合谋攻击是安全的(以 $I_2=\{P_1,\cdots,P_{m-2}\}$ 以及 $I_3=\{P_2,\cdots,P_{m-1}\}$ 为例说明). 进一步分析可知协议 1 的安全性与定义 1 所要求的安全性基本相同.

定理 1　协议 1 中 P_1 关于集合 I_1 以及 P_m 关于集合 I_2 和 I_3 中成员的合谋攻击都是安全的.

证明　我们注意到,当协议 1 的运行结果为 $y=P(\bar{x})=1$ 时,表明所有参与者的数据相等,在这种情况下不存在各参与者数据的保密性问题. 当 $y=P(\bar{x})=0$ 时,我们首先对集合 I_1 构造相应的模拟器 S_1,使得式(1)对于 $I=I_1$,$S=S_1$ 成立.

S_1 按如下方式运行:

(1)S_1 运行 ElGamal 密钥生成算法生成私钥/公钥对 *sk/pk*.

(2)对于输入$(x_2,\cdots,x_m,P(\bar{x}))$,$S_1$ 随机选择 $x_1'\in\{z_1,\cdots,z_n\}$,使得 $P(x_1',x_2,\cdots,x_m)=P(\bar{x})=0$.

(3)S_1 按照协议第 2 步的方法构造 x_1' 对应的矩阵 $\bar{\boldsymbol{v}}'=(v_1',\cdots,v_n')^{\mathrm{T}}$.

(4)S_1 模拟 $P_i(i=2,\cdots,m)$执行协议,得到 $X'=X_2'\cdots X_m'$.

(5)S_1 解密 X',得到 $P(x_1',x_2,\cdots,x_m)=0$.

在协议的执行中,$view_{I_1}^{\pi}(\bar{x})=\{x_2,\cdots,x_m,\bar{v},P(\bar{x})\}$. 令

$$S_1(I_1,(x_2,\cdots,x_m),P(\bar{x}))=\{x_2,\cdots,x_m,\bar{\boldsymbol{v}}',P(x_1',x_2,\cdots,x_m)\}$$

因为 ElGamal 加密系统是语义安全的,对于集合 I_1 中的参与者来说,密文 $\bar{v}$ 和 $\bar{v}'$ 是计算不可区分的,因此,

$$\{S_1(I_1,(x_2,\cdots,x_m),P(\bar{x}))\}_{\bar{x}\in(\{0,1\}^*)^m}\overset{c}{\equiv}\{view_{I_1}^{\pi}(\bar{x})\}_{\bar{x}\in(\{0,1\}^*)^m}.$$

下面,我们分别对集合 $I_2(I_3)$构造相应的模拟器 $S_2(S_3)$,使得式(1)对于 $I=I_2(I_3)$,$S=S_2(S_3)$成立. S_2 按如下方式运行:

(1)S_2 运行 ElGamal 密钥生成算法生成私钥/公钥对 *sk/pk*.

(2)对于输入$(x_1,\cdots,x_{m-2},P(\bar{x}))$,$S_2$ 随机选择 $x_{m-1}',x_m'\in\{z_1,\cdots,z_n\}$,使得

$$P(x_1,\cdots,x_{m-2},x_{m-1}',x_m')=P(\bar{x})=0.$$

(3)S_2 选取随机数 $r_{it}'(i=m-1,m,t=2,\cdots,m)$,使其满足 $\Pi_{t=2}^{m}r_{it}'\bmod p=1$,然后模拟协议的执行得到 $X'=X_2'\cdots X_m'$.

(4)S_2 解密 X',得到 $P(x_1,\cdots,x_{m-2},x_{m-1}',x_m')=0$.

由协议的执行过程以及 S_2 的模拟过程,有:

$$view_{I_2}^{\pi}(\bar{x})=\{x_1,\cdots,x_{m-2},r_{it},X_{m-1},X_m,P(\bar{x})\},$$

$$S_2(I_2,(x_1,\cdots,x_{m-2}),P(\bar{x}))=\{x_1,\cdots,x_{m-2},r_{it}',X_{m-1}',X_m',P(x_1,\cdots,x_{m-2},x_{m-1}',x_m')\},$$

上面两式中,$i=m-1,m$;$t=2,\cdots,m-2$,并且

$$X_{m-1}=r_{2(m-1)}r_{3(m-1)}\cdots r_{m(m-1)}E(1)v_{(x_{m-1})_{ind}},$$

$$X_m=r_{2m}r_{3m}\cdots r_{mm}E(1)v_{(x_m)_{ind}}$$

分别以 Y_1,Y_2 记上面两式中的乘积项 $E(1)v_{(x_{m-1})_{ind}}$ 以及 $E(1)v_{(x_m)_{ind}}$,注意到 I_2 中的成员能获得的关于 x_{m-1},x_m 的所有信息为:

$$\begin{aligned}&X_{m-1}=r_{2(m-1)}r_{3(m-1)}\cdots r_{m(m-1)}Y_1,\\&X_m=r_{2m}r_{3m}\cdots r_{mm}Y_2,\\&\Pi_{t=2}^{m}r_{(m-1)t}\bmod p=1,\\&\Pi_{t=2}^{m}r_{mt}\bmod p=1.\end{aligned}\tag{4}$$

方程组(4)中有六个未知数:$r_{it}(i,t=m-1,m)$以及Y_1,Y_2,因此无法从中解出Y_1,Y_2,也无法解密获知$v_{(x_{m-1})_{ind}}$以及$v_{(x_m)_{ind}}$的任何信息,又由于X_{m-1},X_m中的$E(1)$是分别由P_{m-1}和P_m加密的,对于I_2来说,X_{m-1},X_m与X'_{m-1},X'_m都与随机数不可区分,因此证明了式(1)对于$I=I_2,S=S_2$也成立.

S_3的构造与S_1类似,略去其构造过程. 证毕.

注1 为了全面了解协议1的安全性,下面进一步考虑P_m的数据对于其他$m-1$个参与者$I_4=\{P_1,\cdots,P_{m-1}\}$构成的合谋攻击的安全性问题. 类似于$S_2$构造中的讨论,可得到$view^{\pi}_{I_4}(\bar{x})=\{x_1,\cdots,x_{m-1},r_{mt}(t=2,\cdots,m-1),X_m,P(\bar{x})\}$. 并且$I_4$中成员能获得关于$x_m$的信息有$X_m=r_{2m}r_{3m}\cdots r_{mm}Y_2,\prod_{j=2}^{m}r_{mj}\bmod p=1$,这个方程组中含有两个未知量$r_{mm}$以及$Y_2$,从中可解出$Y_2=E(1)v_{(x_m)_{ind}}$,$P_1$进而解密$Y_2$可获知$x_m$与$x_1$是否相同.

综上可知,对于每一个$i=2,\cdots,m$,如果除P_i外的所有参与者合谋,按照定义1的要求,合谋者不应得到x_i的任何信息,而在协议1中,合谋者可获知x_i与x_1是否相等. 而在其它情形下,协议1与定义1的安全性完全相同.

4 基于门限密码体制的多数据相等保密判定协议

在门限密码体制中,m个参与者联合生成一个公钥,解密密钥由m个参与者联合持有. 如果需要m个参与者共同合作才能解密,这样的密码体制称为(m,m)门限密码系统. 下面应用ElGamal门限密码体制构造协议.

4.1 基本原理与协议

该方案的基本原理类似于命题1,这时每个参与者$P_i(i=1,\cdots,m)$首先按照式(2)的方式将秘密数据x_i转化为数组X_i. 再对这些数组进行乘积运算(对应元素相乘),显然,$x_1=\cdots=x_m$当且仅当乘积数组$(y_1,\cdots,y_n)$中有等于1的元素.

协议2 基于门限密码体制的多数据相等保密判定协议(半诚实模型)

输入:$P_1,\cdots,P_m$各自的秘密数据$x_1,\cdots,x_m$.

输出:$y=P(\bar{x})$.

(1)$P_1,\cdots,P_m$选取ElGamal公钥系统的参数g,p. 每个参与者P_i选择私钥k_i,公布$h_i=g^{k_i}\bmod p$,联合生成公钥pk:$h=g^{k_1+\cdots+k_m}\bmod p$.

(2)$P_i(i=2,\cdots,m)$将自己的数据x_i转化为一个$2\times n$矩阵:

$$\boldsymbol{M}_i=\begin{pmatrix}u_{i1} & u_{i2} & \cdots & u_{in}\\ v_{i1} & v_{i2} & \cdots & v_{in}\end{pmatrix} \tag{5}$$

其中$(u_{i(x_i)_{ind}},v_{i(x_i)_{ind}})=(g^{s_i}\bmod p,h^{s_i}\bmod p)=E(1)$,其它$(u_{it},v_{it})\in Z_p^*\times Z_p^*$为随机数对. P_i公布$\boldsymbol{M}_i$.

(3)P_1应用公钥加密1得到一个密文,记作$(u_{1(x_1)_{ind}},v_{1(x_1)_{ind}})=E(1)$,计算并公布$(u,v)=\left(\prod_{i=1}^{m}u_{i(x_1)_{ind}}\bmod p,\prod_{i=1}^{m}v_{i(x_1)_{ind}}\bmod p\right)$.

(4)解密(u,v)的过程如下:对于$i=1,\cdots,m$

(a) P_i计算$w_i=u^{k_i}\bmod p$,并公布.

(b) P_i计算$z\equiv v\left[\prod_{i=1}^{m}w_i\right]^{-1}\bmod p$.

(5)如果$z=1$,$P_i(i=1,\cdots,m)$获得$y=1$,否则P_i获得$y=0$.

4.2 协议分析

正确性分析 根据ElGamal密码系统的乘法同态性,如果$x_1=\cdots=x_m$,则有:

$$(u,v)\equiv\left(g^{\sum_{i=1}^{m}s_i}\bmod p,\left(g^{\sum_{i=1}^{m}k_i}\right)^{\sum_{i=1}^{m}s_i}\bmod p\right),$$

$$\prod_{i=1}^{m}w_i\bmod p\equiv\prod_{i=1}^{m}u^{k_i}\bmod p\equiv\left(g^{\sum_{i=1}^{m}s_i}\right)^{\sum_{i=1}^{m}k_i}\bmod p,$$

因此,若记$z\equiv v\left[\prod_{i=1}^{m}w_i\right]^{-1}\bmod p$,则$z=1$.

如果$x_2,\cdots,x_m$中至少有一个与x_1不同,这时u和v是不相关的随机数,此时$z\equiv v\left[\prod_{i=1}^{m}w_i\right]^{-1}\bmod p$也是一个随机数. 因此,协议2是正确的.

安全性分析 由于协议2中公钥$h=g^{k_1+\cdots+k_m}\bmod p$,其中$k_i$是$P_i$所持有的私钥碎片,所以只有所有参与者合作才能对加密信息进行解密.

在计算过程中,$P_i(i=2,\cdots,m)$对外仅公布了加密信息$(u_{it},v_{it})(t=1,\cdots,n)$,其值或是随机数对,或是密文$E(1)$,在解密过程中对外也仅公布了$w_i=u^{k_i}\bmod p$. 在协议执行中,如果没有$P_i$的参与,无法解密得到$x_i$,因此$x_i$是完全保密的. 计算中$P_1$对外仅公布了密文$(u,v)$,由于$(u_{1(x_1)_{ind}},v_{1(x_1)_{ind}})=E(1)$是$P_1$加密的,因此$x_1$也是完全保密的. 协议2的安全性与定义1所要求的安全性完全相同. 我们给出下面的定理.

定理2 基于门限密码体制的多数据相等保密判定协议在半诚实模型下是安全的.

5 效率分析

计算效率分析 分析计算复杂性时忽略协议执行中需要的乘法运算,只考虑模指数运算. 应用ElGamal密码系统加密(或解密)一次需要进行两次(或一次)模指数运算.

在协议1中,每个参与者需要加密1得到$E(1)$,最后P_1对乘积密文进行一次解密运算. 所以协议1共需要$2m+1$次模指数运算.

在协议2中,参与者合作产生公钥需要m次模指

数运算;加密和解密过程分别需要 $2m$ 和 $m+1$ 次模指数运算,协议 2 共需要 $4m+1$ 次模指数运算.

通信效率分析　在协议 1 中,$P_2,\cdots,P_m$ 相互发送随机数需要$(m-1)(m-2)$次通信;在解密过程中,P_i,$i=2,\cdots,m$ 把 X_i 发送给 P_1 需要 $m-1$ 次通信,因此协议 1 共需要$(m-1)^2$ 次通信. 协议 2 中构造公钥以及加密、解密过程各需要 $m-1$ 次通信,协议 2 共需要 3$(m-1)$次通信.

上面分析表明,协议 2 的计算复杂性比协议 1 高. 当 $m<4$ 时,协议 2 的通信复杂性也比协议 1 略高;由于在协议 1 中 $P_2,\cdots,P_m$ 之间要相互交换信息,因此当 $m>4$ 时协议 1 的通信复杂性要高一些.

6　恶意模型下的多数据相等判定问题

6.1　协议设计

我们将根据文[13]中协议编译器的基本思想,以半诚实模型下的保密计算协议 2 为基础,利用输入承诺函数以及认证计算函数[13],零知识证明系统[15],构造在恶意模型下安全的计算协议. 为迫使所有参与者能像半诚实参与者一样按照协议 2 的要求执行,需要防止各种可能的恶意行为,为此需要做到:(1) 防止 P_1 在协议中改变其输入数据 x_1 以及构造 $E(1)$时有欺骗行为;(2) 防止 $P_i(i=2,\cdots,m)$根据数据 x_i 构造矩阵 M_i 时有两列或更多列由 $E(1)$构成;(3) 防止 P_1 在计算(u,v)的过程中偏离协议 2;(4) 保证在联合解密过程中各 P_i 提供正确的 w_i.

根据上面的要求,我们将在协议 2 的基础上构造恶意模型下的安全计算协议.

协议 3　恶意模型下多数据相等问题安全判定协议

输入:$P_1,\cdots,P_m$ 各自的秘密数据 $x_1,\cdots,x_m$;ElGamal 门限密码系统:每个 P_i 选择 k_i,并公布 $h_i=g^{k_i}\bmod p$,公钥为 $h=g^{k_1+\cdots+k_m}\bmod p$;一个安全参数 N.

输出:所有参与者得到 $y=P(\bar{x})$.

(1)P_1 应用输入承诺函数将 x_1 进行承诺,公布承诺值.

(2)P_1 加密 N 个 1 得到不同形式的密文 $E_k=E(1),k=1,\cdots,N$,并对这些密文进行承诺,公布承诺值.

(3)$P_2,\cdots,P_m$ 随机选取 P_1 在上一步所做的一个承诺进行保留,并揭示剩余的 $N-1$ 个承诺,验证其是否均为对 $E(1)$的承诺,若验证通过,则继续,否则,中止协议. 协议未中止情形下,对所保留的一个承诺,记其所承诺的私密信息为 $\bar{E}=E(1)$.

(4)参与者 $P_i(i=2,\cdots,m)$

(a) 将 x_i 按照式(5)的方法构造 N 个不同形式的矩阵 $\boldsymbol{M}_i^k,k=1,\cdots,N$,并对每个矩阵的列进行随机置换,公布置换后的矩阵.

(b) 其他参与者随机选取 P_i 所构造的 N 个矩阵中的一个保留,将其记为 $\overline{\boldsymbol{M}}_i$,解密并验证其它矩阵是否恰有一列为 $E(1)$. 若验证通过则继续,否则,中止协议.

(c) 协议未中止情形下,P_i 对所保留的矩阵 $\overline{\boldsymbol{M}}_i$ 再作变换,将其各列变回到原来顺序. 将恢复列顺序后的矩阵表示如下:

$$\boldsymbol{M}_i=\begin{pmatrix}u_{i1} & u_{i2} & \cdots & u_{in}\\ v_{i1} & v_{i2} & \cdots & v_{in}\end{pmatrix}$$

(5)如果第 3 步对 P_1 所承诺数据的验证以及第 4(b)步对所有 $P_2,\cdots,P_m$ 所构造矩阵的验证全部通过,所有参与者调用认证计算函数计算:

$(u,v)=\left(\prod_{i=1}^{m}u_{i(x_1)_{ind}}\bmod p,\ \prod_{i=1}^{m}v_{i(x_1)_{ind}}\bmod p\right)$,其中$(u_{1(x_1)_{ind}},v_{1(x_1)_{ind}})=\bar{E}=E(1)$.

(6)解密(u,v)的过程如下:对于 $i=1,\cdots,m$

(a)P_i 计算 $w_i=u^{k_i}\bmod p$,并公布.

(b) 应用零知识证明系统证明 w_i 的有效性,即验证 $w_i=u^{k_i}\bmod p$ 和 $h_i=g^{k_i}\bmod p$ 中的 k_i 是否相同. 若验证未全部通过,则中止协议. 若验证全部通过,则继续.

(c) P_i 计算 $z\equiv v\left[\prod_{i=1}^{m}w_i\right]^{-1}\bmod p$.

(7)如果 $z=1$,$P_i(i=1,\cdots,m)$得到 $y=1$,否则 P_i 得到 $y=0$.

6.2　安全性分析

(1) 首先要求 P_1 对 x_1 以及对某一 $\bar{E}=E(1)$进行承诺,其目的是在后面计算(u,v)时,根据认证计算函数,由相应的承诺信息就能保证(u,v)计算结果的正确性. 协议 3 中要求 P_1 对 N 个不同的 $E(1)$进行承诺,其他参与者随机验证其中的 $N-1$ 个,如果验证能通过,所保留的承诺亦可认为是正确的.

(2) $P_i(i=2,\cdots,m)$由 x_i 构造 M_i 的过程中,需要保证 M_i 中仅有一列数据为 $E(1)$. 为此要求 P_i 将 x_i 按式(5)的方法构造 N 个不同形式的矩阵,并对每个矩阵的列进行随机置换. 其他参与者随机验证 $N-1$ 个矩阵是否都恰有一列为 $E(1)$. 如果验证能通过,所保留的承诺亦可认为是正确的.

(3) 如果前面的计算过程都通过验证而没有中止协议,最后还需要正确执行解密. 根据 g,p 以及 h_i,w_i 能够零知识证明 w_i 的有效性.

综上所述,协议 3 能迫使参与者以半诚实的方式正确执行协议 2,如有任何不当行为都会被发现而导致协议中止,在未中止情形下各方均可获得正确的局部输出 y. 限于篇幅,关于协议 3 安全性的严格证明在此省略. 仅叙述下面结论.

定理 3 协议 3 是恶意模型下关于多数据相等判定问题的安全计算协议.

7 结论与讨论

本文设计了新的编码方法,以新的编码方法与 ElGamal 同态加密算法为基础,分别利用秘密分享和门限密码体制构造了两个半诚实模型下多数据相等问题的保密计算协议,两个协议均可抵抗合谋攻击. 在协议 2 的基础上,进一步设计了恶意模型下的安全计算协议.

本文提出的方案适合保密数据的范围属于某个确定集合 H 的情形,当 H 的势较大时协议的效率比较低. 恶意模型下的安全计算协议是应用文献[13]中所提供的一般方法设计的,复杂性较高. 今后将进一步研究保密数据的范围未知情形下的保密计算协议,并设计恶意模型下高效的安全计算方案.

参考文献

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

[2] Goldwasser S. Multi-party computations: past and present[A]. The 16th Annual ACM Symposium on Principles of Distributed Computing[C]. Santa Barbara, California, USA, 1997. 1 – 6.

[3] Cramer R, et al. Secure Multiparty Computation[M]. London: Cambridge University Press, 2015.

[4] 李顺东,等. 基于同态加密的高效安全多方计算[J]. 电子学报,2013,41(4):798 – 803.
Li S D, et al. Efficient secure multiparty computation based on homomorphic encryption[J]. Acta Electronica Sinica, 2013, 41(4): 798 – 803. (in Chinese)

[5] Fang L, et al. Encrypted scalar product protocol for outsourced data mining[A]. IEEE 7th International Conference on Cloud Computing[C]. Anchorage, Alaska, USA, 2014. 336 – 343.

[6] Bringer J, et al. Shade: Secure hamming distance computation from oblivious transfer[A]. International Conference on Financial Cryptography and Data Security[C]. Okinawa, Japan, 2013. 164 – 176.

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

[8] Chen X B, et al. An efficient protocol for the private comparison of equal information based on the triplet entangled state and single-particle measurement[J]. Optics communications, 2010. 283(7): 1561 – 1565.

[9] Du W L. A study of several specific secure two-party computation problems[D]. Purdue University, 2001.

[10] Ma S, et al. Public key encryption with delegated equality test in a multi-user setting[J]. The Computer Journal, 2015. 58(4): 986 – 1002.

[11] Sepehri M, et al. A scalable multi-party protocol for privacy-preserving equality test[A]. International Conference on Advanced Information Systems Engineering[C]. Valencia, Spain, 2013. 466 – 477.

[12] 刘文,等. 安全多方信息比较相等协议及其应用[J]. 电子学报,2012. 40(5):871 – 876.
Liu W, et al. Secure multi-party comparing protocol and its applications[J]. Acta Electronica Sinica, 2012, 40(5): 871 – 876. (in Chinese)

[13] Goldreich O. The Fundamental of Cryptography: Basic Applications[M]. London: Cambridge University Press, 2004.

[14] ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms[J]. IEEE transactions on information theory, 1985. 31(4): 469 – 472.

[15] Chaum D, et al. An improved protocol for demonstrating possession of discrete logarithms and some generalizations[A]. Workshop on the Theory and Application of Cryptographic Techniques[C]. Amsterdam, the Netherlands, 1987. 127 – 141.

作者简介

窦家维(通信作者) 女,1963 年 3 月生于西安. 副教授,硕士生导师. 研究方向为密码学、应用数学.
E-mail: jiawei@ snnu. edu. cn

李顺东 男,1963 年 12 月生于河南. 教授,博士生导师. 研究方向为密码学、信息安全.
E-mail: shundong@ snnu. edu. cn