软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2019,30(11):3535−3548 [doi: 10.13328/j.cnki.jos.005556]

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

保密社交意愿探测*

巩林明[1,2], 李顺东[2], 窦家维[3], 王道顺[4]

[1](西安工程大学 计算机科学学院,陕西 西安 710048)

[2](陕西师范大学 计算机科学学院,陕西 西安 710119)

[3](陕西师范大学 数学与信息科学学院,陕西 西安 710119)

[4](清华大学 计算机科学与技术系,北京 100084)

通讯作者: 巩林明, E-mail: glmxinjing@163.com; 窦家维, E-mail: jiawei@snnu.edu.cn

摘 要: 研究保密意愿探测问题:Alice 和 Bob 可以协同测试他们是否可以在某个理想区域共事,但不泄漏彼此的隐私信息.近年来,大部分的移动智能设备在出厂时都预装了位置感知设备,从而为开发者设计各种各样的提供位置识别与服务的应用软件提供了广阔的空间.然而很多情况下,用户间不愿意泄露自己的位置信息(或者活动范围),仅通过一比特的信息探知(或知晓)各参与方是否愿意在某个(便于彼此的)区域内共同做某件事情.保密意愿探测协议可以实现这样的功能,并且能够保证各参与方位置信息不会泄露.首先,设计了一个新的基于高阶剩余类判定性难解问题的云外包同态加密方案;然后,基于该方案构造了一个保密意愿探测协议,并在 ideal/real 模型下证明了协议的安全性.

关键词: 位置隐私;同态加密方案;保密意愿探测;外包计算;位置服务

中图法分类号: TP309

中文引用格式: 巩林明,李顺东,窦家维,王道顺.保密社交意愿探测.软件学报,2019,30(11):3535−3548. http://www.jos.org.cn/1000-9825/5556.htm

英文引用格式: Gong LM, Li SD, Dou JW, Wang DS. Private social-willing detection. Ruan Jian Xue Bao/Journal of Software, 2019,30(11):3535−3548 (in Chinese). http://www.jos.org.cn/1000-9825/5556.htm

Private Social-willing Detection

GONG Lin-Ming[1,2], LI Shun-Dong[2], DOU Jia-Wei[3], WANG Dao-Shun[4]

[1](School of Computer Science, Xi'an Polytechnic University University, Xi'an 710048, China)

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

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

[4](Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China)

Abstract: Privacy-preserving tests are studied for social-willing: Alice and Bob can test whether they are suitable to do something jointly in an ideal area without either party revealing any other information about each other's location. Nowadays, most mobile intelligent devices come pre-equipped with location (GPS) sensing capabilities, allowing developers to create a wide variety of location-aware applications and services. While location awareness provides novel features and functionality, it opens the door to many privacy nightmares. In many occasions, however, users are not willing to share their actual location or the range of their activities, but to determine whether they are able to do something in some area (a place is convenient for each user), which is practically one bit of

* 基金项目: 西安工程大学博士科研启动基金(107020331); 国家自然科学基金(61272435, 61972225, 61902164)

Foundation item: Start-up Fund of Xi'an Polytechnic University for Doctoral Research (107020331); National Natural Science Foundation of China (61272435, 61972225, 61902164)

收稿时间: 2017-03-15; 修改时间: 2017-05-11; 采用时间: 2018-01-24; jos 在线出版时间: 2018-04-27

CNKI 网络优先出版: 2018-04-27 14:58:05, http://kns.cnki.net/kcms/detail/11.2560.TP.20180427.1457.003.html

information. Private social-willing protocols allow this functionality without any further information leakage. Firstly, a homomorphic encryption scheme is developed, assisted by cloud server and based on the intractable problem of decisional composite residuosity. Then, a novel protocol is proposed based on the developed homomorphic encryption scheme, and security in ideal/real model is proved.

Key words: location privacy; homomorphic encryption scheme; private social-willing testing; outsourcing, location service

近年来,随着基于位置的服务在移动智能设备上的广泛应用,保密探测问题已经成为移动、社交网络中保护隐私的一个研究热点.保密近感探测,是保密探测问题的一个重要分支.保密近感探测问题研究的是移动网络中任意两个用户如何协同计算出他们的实时位置是否彼此临近而不泄漏各方的具体位置.时至今日,保密近感探测问题已取得了一些可喜的成果[1−21],但这些成果中除了 Mu 等人[1]取得的以外,其他协议[2−21]都是采用格栅分解技术(如果参与方在相同的格栅内,即同在一个预先设定大小的圆形区域内,则认为参与各方毗邻)实现保密近感探测的.然而,这种方法不满足移动或社交网络用户的个性化需求,如:Alice 正在颐和园度周末,她想知道她的业余划船搭档 Bob 是否也在颐和园内,是否可以和 Bob 一起参加公园里正在举办的双人划船比赛.采用格栅分解技术的近感探测只能探测到 Bob 是否处在以 Alice 为中心、预先设定半径值的圆域内.2016 年,Mu 等人[1]综合运用安全多方计算、Paillier[22]和 ElGamal[23]同态加密方案设计了一个保密探测区域为任意凸多边形的协议.该协议满足了用户个性化的需求(用户不再预先设定保密探测区域阈值的大小,保密探测区域可以是任意的多边形),非常方便用户表示保密探测区域.

但文献[1]的协议仍然存在以下两个方面的不足.

(1) 文献[1]的协议除了用 Paillier 加密系统保密计算符号外,还需要调用 K(凸多边形的顶点数)次高计算复杂度的、由 ElGamal 加密方案实现的保密比较大小运算.

(2) 文献[1]的协议并未彻底解决保密近感探测问题,只适用于解决用户参与计算区域的临近两点坐标分量差大于 0 的情形,当用户参与计算区域的临近两点坐标分量差值小于 0 时,该协议会输出错误的结果.原因是文献[1]的协议用 Paillier 加密方案直接加密负数,并在加密负数的结果上实施同态运算.

事实上,Paillier 加密方案不能直接用于加密负数,加密负数以及在加密的负数上进行同态操作需要做额外的比特密文同态运算.关于 Paillier 加密方案不能直接用于加密负数,并在加密负数的结果上实施同态运算方面的具体阐述如下.

命题 1. Paillier 加密方案不能直接用于加密负数.

证明:Paillier 加密方案的同态实质是 $Z_n\times Z_n^*$ 与 $Z_{n^2}^*$ 的同态,而同态 $f:Z_n\times Z_n^*\to Z_{n^2}^*$ 由 $f(a,b)=(1+kn)^a\cdot b^n(\mathrm{mod}\ n^2)$给出[22].从而有结论:在 $Z_{n^2}^*$ 上, $f:Z_n\times Z_n^*\to Z_{n^2}^*$ 是双射函数.也就是说,它既是满射又是单射.下面用反证法证明命题 1 的正确性.

设 $a\in Z_n, b\in Z_n^*$,$-a$ 表示负数,并假定 Paillier 加密方案能够直接加密一个负数,则由其加密算法的正确性可知:由加密运算 $Enc(-a)=f(-a,b)=((1+kn)^{-a}b^n(\mathrm{mod}\ n^2)=\dfrac{b^n(\mathrm{mod}\ n^2)}{(1+kn)^a(\mathrm{mod}\ n^2)}\ \mathrm{mod}\ n^2$ 生成的密文 $Enc(-a)$,经过解密运算 $Dec(Enc(-a))$,一定能正确恢复出消息$-a$.

事实上,由解密运算:

$$Dec(Enc(-a))=\frac{L(f^{\lambda}(a,b)\ \mathrm{mod}\ n^2)}{L(g^{\lambda}\ \mathrm{mod}\ n^2)}\ \mathrm{mod}\ n=\frac{\left(\dfrac{b^{\lambda n}(\mathrm{mod}\ n^2)}{(1+kn)^{\lambda a}(\mathrm{mod}\ n^2)}-1\right)\ \mathrm{mod}\ n^2}{((1+kn)^{\lambda}-1)\ \mathrm{mod}\ n^2}\ \mathrm{mod}\ n$$

$$=\frac{\left(\dfrac{1}{(1+\lambda kan)\ \mathrm{mod}\ n^2}-1\right)\ \mathrm{mod}\ n^2}{\lambda kn\ \mathrm{mod}\ n^2}\ \mathrm{mod}\ n=\frac{\dfrac{-\lambda kan\ \mathrm{mod}\ n^2}{(1+\lambda kan)\ \mathrm{mod}\ n^2}}{\lambda kn\ \mathrm{mod}\ n^2}\ \mathrm{mod}\ n$$

$$=\frac{-a\ \mathrm{mod}\ n^2}{(1+\lambda kan)\ \mathrm{mod}\ n^2}\ \mathrm{mod}\ n$$

得到消息$-a$的概率很小,因为$\frac{-a \bmod n^2}{(1+\lambda kan) \bmod n^2} \bmod n$要等于$-a$,则需$1\equiv(1+\lambda kan) \bmod n^2$成立.即$n|\lambda ka$因为$gcd(\lambda,n)=1$,所以$n|\lambda ka$则必有$n|ka$.而为安全起见,系统参数$k$是不会取$\kappa p$或者$\kappa q$的,所以只有当$a\equiv 0 \bmod n$,解密算法才能正确恢复出消息$-a$.因此,Paillier加密算法能够加密负数的假设不成立.

同理,已知$a\in Z_n$在Paillier加密体制下的密文$c_a=g^a r^n \bmod n^2 a\in Z_n$无法直接通过同态计算得到$c_{-ab}=g^{-ab}(r')^n \bmod n^2 a\in Z_n$,其中,$b\in Z_n$. □

用Paillier通过特殊处理可以实现对一个负数的加密,但难以实现对若干个正、负数对应密文实施若干次同态运算.目前所采用的特殊处理方法大致可以分为3类.

(1) 明文的符号由明文所处的区间隐式地确定,用这种方法能够加密明文的范围是$\left[-\frac{n+1}{2},\frac{n-1}{2}\right]$.通常是将整型区间$[0,n]$划分成两个等长的区间$\left[0,\frac{n-1}{2}\right]$和$\left[\frac{n+1}{2},n\right]$,并事先规定哪个区间内的数代表负数.例如,可以事先规定处在$\left[\frac{n+1}{2},n\right]$内表示负数,如果解密结果$m\in\left\{\frac{n+1}{2},\frac{n+3}{2},...,n\right\}$,则解密方需要在解密的基础上执行额外计算:$m'=m-n$.

(2) 用加密加法逆元的方法实现对$[-n,0]$内整数的加密:用$-a$表示负数,则在Z_n群上可将$-a$视为a的逆元$n-a$,进而可以通过加密运算$Enc(n-a)=((1+kn)^{n-a} r_1^n(\bmod n^2))$生成的密文$Enc(n-a)$,经过解密运算$Dec(Enc(n-a))$,一定能够正确恢复出消息$n-a$.而后再做运算$(n-a)-n$,可以得到$-a$.

(3) 明文的符号由加密额外的比特信息标识,用此种方法能够解决$[-n,n]$内的问题.通信双方需要事先商定符号的数字标识,通常规定"0"代表"+","1"代表"–".由运算$Enc(a)=((1+kn)^a r_1^n(\bmod n^2)), Enc(s_\mu)=((1+kn)^\mu r_2^n(\bmod n^2)), \mu\in\{0,1\}$计算出的密文$(Enc(a),Enc(s_\mu))$,通过解密运算:

$$(Dec(Enc(a),Dec(Enc(s_\mu))=\begin{cases}(a,0), & a\\ (a,1), & -a\end{cases},$$

即可恢复出消息$-a$.

但是,上述加密负数的方法在需要对差商对应的密文实施若干次同态运算的环境下将变得异常复杂:一方面,多次同态运算会导致明文运算结果所处区间的变换,这会影响多方保密计算结果的准确性;另一方面,在保密多方计算中,各参与方都不想泄露自己的、哪怕是1比特的信息(在涉及坐标运算的保密计算中,坐标符号的泄露有可能造成相对位置信息的泄露),又有哪个无私钥的参与方愿意对外透露自己的符号信息呢?

由上述分析可得,现有的基于位置服务的保密探测方法绝大多数只能解决保密探测区域在预先设定半径阈值的圆形内的情形,这不能满足用户个性化的需求(用户不再预先设定保密探测区域阈值的大小,保密探测区域可以是任意的多边形).文献[1]的协议提出了一种解决探测区域为任意凸多边形情形的很好的方法.它虽然能够满足用户个性化的需求(无需将探测区域设定为带阈值的圆形区域),但是并未彻底解决保密探测计算中保密坐标符号计算问题.因此,对于涉及到保密计算(正、负)符号的、利用同态加密实现的由多方协同参与的安全/保密几何计算问题以及基于位置服务的移动、社交网络隐私保护问题则需要另辟新径.

如今,社交网络用户又对保密地探测提出了新的个性化需求:保密社交意愿筹划,即保密社交意愿探测.保密社交意愿探测已经成为基于位置服务的社交网络用户的一个新的个性化需求.我们将如下一类问题称为保密意愿探测问题:拥有便携智能设备的用户间可以事先保密地探测他们的社交意愿——Alice由她的便携智能设备秘密地获取Bob是否处在自己愿意与Bob约会(如果Bob愿意赴约的话)的"理想区域内",Bob由自己的便携智能设备保密地表达自己是否愿意赴约的意愿,但双方都不想泄露各自的位置信息(Alice既不想泄露自己的位置,也不想泄露自己的"理想区域";Bob不想泄露自己的位置信息).

保密意愿探测可以视作保密近感探测协议[1]在移动、社交网络用户个性化需求方面的深度拓展.虽然二者都是基于位置服务的移动、社交网络用户隐私保护问题,但它们有明显的区别:保密近感探测问题研究的是两

个用户如何计算他们的实时位置是否在预先设定的距离阈值内而不泄漏双方各自的具体位置;保密意愿探测问题研究的则是参与双方如何计算出他们是否可以在某一区域内共事而不泄漏具体的共事区域与双方计划共事的具体位置,即保密社交筹划.

为了解决移动、社交网络用户在社交筹划方面隐私保护的个性化需求问题,同时也为了解决基于同态加密方案与安全多方计算的保密近感探测(如文献[1]的协议)中未能彻底解决的问题(当用户参与计算区域的临近两点坐标分量差值小于 0 时,文献[1]的协议会输出错误的结果),本文首先提出了一个基于位置服务的移动、社交网络隐私保护问题:保密社交意愿探测.然后综合采用安全多方几何计算[24−26]、保密计算分数(一种新的保密比较大小方法)、同态加密以及云外包计算等技术设计了一个高效的社交网络保密意愿探测协议.

本文的主要贡献如下:

(1) 构造了一个由云辅助计算的新型同态加密方案,该方案在预处理阶段由云服务器提前完成复杂的自模乘运算 ($r_x^2 \bmod n^2$),加密阶段的另一复杂运算 $g^m \bmod n^2$ 由等价的简单模乘运算 $m\cdot(g-1) \bmod n^2$ 代替,因此只通过几次简单的模乘运算,就可以实现一次加密.

(2) 提出了一种新的保密符号计算方法,并利用该方法和新构造的基于云计算的同态加密方案,设计了一个新的保密意愿探测协议.该协议对于半诚实参与者是安全的.

(3) 提出了一种新的加密思想:由加密一方自主确定一次加密需要执行多少次模乘运算.

1 预备知识

1.1 关于加密方案的安全性定义

定义 1(不可区分安全游戏). “加密语义安全”通常利用一个(由敌手和加密系统产生者)两方进行的思维游戏进行刻画.本文将引用文献[27]中对于文献[28]中关于公钥加密方案的选择明文攻击不可区分性(indistinguishability under chosen-plaintext attack,简称 IND-CPA)游戏 $PubK_{\mathcal{A},\mathcal{E}}^{cpa}(k)$ 的翻译表述(其中,$\mathcal{E}$为任意一个公钥加密方案,$\mathcal{A}$为任意一个概率多项式时间的敌手, $Adv_{\mathcal{A},\mathcal{E}}(k)$ 为$\mathcal{A}$在攻击$\mathcal{E}$的不可区分游戏中的成功优势).

(1) 输入系统安全参数 1^k,生成密钥对(K_{pub},K_{pri}).

(2) $\mathcal{A}$获得公钥 K_{pub},并且它能够访问加密谕言机 $Enc(\cdot)$,经过一些加密问询后输出两个相同长度的明文 m_0 和 m_1.

(3) 系统搭建者随机选择 $b\in\{0,1\}$,然后输出一个挑战密文 $c=Enc(m_b)$.

(4) $\mathcal{A}$继续调用 $Enc(\cdot)$,输出一个比特位 b'作为对 b 的猜测结果.

(5) 若 $b'=b$,则游戏输出 $PubK_{\mathcal{A},\mathcal{E}}^{cpa}(k)=1$; 否则,输出 $PubK_{\mathcal{A},\mathcal{E}}^{cpa}(k)=0$.

如果存在一个可忽略的函数δ,满足:

$$Adv_{\mathcal{A},\mathcal{E}}^{cpa}(k)=\left|\Pr[PubK_{\mathcal{A},\mathcal{E}}^{cpa}(k)=1]-\frac{1}{2}\right|\leqslant\delta(k),$$

则方案$\mathcal{E}$在选择明文攻击下具有不可区分安全性.

1.2 关于安全多方计算的安全性定义[27]

要证明一个安全多方计算协议的安全性,需要用到定义:理想保密计算协议、半诚实参与者、协议π可被用于保密计算函数 $f(a,b)$.本文将引用文献[27]中对于学者 Goldreich 关于这 3 个定义的翻译描述.

定义 2(理想保密计算协议)[27]. 假设 TTP 是网络中存在的一个绝对可信的第三方,作为协议的参与方,Alice 与 Bob 在 TTP 协助下,可以按照如下方式协作完成一次安全计算:Alice 与 Bob 各自将他们的秘密信息 a 和 b 分别秘密地发送给 TTP,由 TTP 独立计算完函数 $f(a,b)$后,再将计算出的函数值分别秘密地发送给 Alice 和 Bob.其中规定函数 f 满足:已知 a 与 b 之一以及函数值 $f(a,b)$时,不能计算出 a 与 b 中的另一个.显然,网络中这样一个简单的协议是保密程度最高的安全两方计算协议,除此之外,再也找不到一个用于计算 $f(a,b)$的实际安全两方计

算协议在安全性上可以超越该协议.

定义 3(半诚实参与者)[27]. 不严格地说,作为某安全多方计算协议的半诚实参与者,在其执行协议的过程中绝对会按照协议规定,执行安全计算协议的每一步,但其可能会在协议执行过程中记录所有中间结果,并试图利用这些记录数据去计算安全多方计算协议之外的有关其他参与者的隐私信息.

将计算概率多项式函数 $f=(f_1,f_2):\{0,1\}^*\times\{0,1\}^*\to\{0,1\}^*\times\{0,1\}^*$的协议记作$\pi$.给$\pi$输入$(a,b)$,在协议执行过程中,Alice 和 Bob 的视图(view)分别记作 $view_1^{\pi}(a,b)=(a,r_d,m_{d_1},m_{d_2},...,m_{d_k})$ 和 $view_2^{\pi}(a,b)=(b,r_d,m_{d_1},m_{d_2},...,m_{d_k})$. 其中,$d\in\{1,2\}$,$r_d$ 是 Alice 或 Bob 自己选择的随机数, m_{d_1} 是 Alice 或 Bob 收到的第 i 个消息;将 Alice 和 Bob 协同执行完协议得到的结果分别记作 $output_1^{\pi}(a,b)$ 和 $output_2^{\pi}(a,b)$.

定义 4(协议π可被用于保密计算函数 $f(a,b)$)[27]. Goldreich 如下定义一个安全两方计算协议的安全性:如果存在概率多项式时间模拟算法$\mathcal{S}_1$与$\mathcal{S}_2$,使得

$$\{(\mathcal{S}_1(a,f_1(a,b)),f_2(a,b))\}_{a,b}\overset{c}{\equiv}\{(view_1^{\pi}(a,b),output_2^{\pi}(a,b))\}_{a,b} \tag{1}$$

$$\{(f_1(a,b),\mathcal{S}_2(a,f_2(a,b)))\}_{a,b}\overset{c}{\equiv}\{(output_1^{\pi}(a,b),view_2^{\pi}(a,b))\}_{a,b} \tag{2}$$

成立,则称协议π可被用于保密计算函数 $f(a,b)$.其中,$\overset{c}{\equiv}$表示计算不可区分.

Goldreich 利用比特承诺和零知识证明理论设计了一个编译器.向该编译器输入一个在半诚实参模型下安全计算 f 的协议π时,编译器会自动为我们编译输出一个安全协议π',该协议在有恶意参与者参与协同计算情况下也能安全计算 f.考虑到工程实际,本文规定本文构造协议中的参与者皆为半诚实类型.

1.3 Paillier同态加密方案[22]

Paillier 构造的方案(如图 1 所示)可以利用密文的运算在明文空间 Z_n 上实现同态加运算:$E(x+y)=E(x)\cdot E(y)$. 该方案具有第 1.1 节中定义 1 定义的安全性:将等长的两个消息 m_0 和 m_1 加密,并将它们的密文分别记作 C_0 与 C_1,对于任何实施选择明文攻击的敌手而言,计算上无法区分 C_0 与 C_1,即 $C_0\overset{c}{\equiv}C_1$.

Encryption	plaintext $m<n$
	select a random $r<n$
	cipherext $C=g^m r^n \bmod n^2$
Decryption	ciphertext $C<n^2$
	plaintext $m=\dfrac{L(C^{\lambda} \bmod n^2)}{L(g^{\lambda} \bmod n^2)} \bmod n$

注:p 与 q 为两个等长的大素数, $n=pq$, $l=lcm(p-1,q-1)$, $g=1+kn$ $(k\in Z_n^*)$

Fig.1 Paillier's encryption scheme

图 1 Paillier 加密方案

1.4 高阶剩余类判定性问题

定义 5(高阶剩余类判定性问题). 该问题在文献[11]中被称作"decisional composite residuosity problem",简称为 DCR).简单地讲,如果给定两个等长大素数的乘积 $n=pq$ (其中 p 与 q 保密)和一个与 n 互素的整数 z ,对于敌手而言,判定事件"是否存在一个 y,满足 $z\equiv y^n \bmod n^2$ "成功的概率可以表述为一个忽略的函数[11].

文献[27]从可证明安全的需求出发,将其用形式化语言描述为如下形式:

设 $\boldsymbol{D}$ 是一种区分任意两个分布 $D_{ran}=\{(n,\boldsymbol{R})\mid \boldsymbol{R}\xleftarrow{R}Z_{n^2}\}$ 和 $D_{\varepsilon}=\{(n,\boldsymbol{R})\mid \boldsymbol{R}\leftarrow\{r^n \bmod n^2\mid r\in Z_n\}\}$ 的算法,以系统安全参数τ为自变量的函数 $Adv_{\boldsymbol{D}}(\tau)$表示敌手利用区分算法 $\boldsymbol{D}$ 能够区分出 D_{ran} 与 D_{ε} 的优势函数.

如果任意选取一个分布 $(n,\boldsymbol{R})\in\{D_{ran},D_{\varepsilon}\}$发给敌手进行挑战,并把敌手里利用 $\boldsymbol{D}$ 对于$(n,\boldsymbol{R})$的区分结果记作 $\boldsymbol{D}(n,\boldsymbol{R})=D_{ran}$ 或 $\boldsymbol{D}(n,\boldsymbol{R})=D_{\varepsilon}$, 则敌手利用 $\boldsymbol{D}$ 可以区分$(n,\boldsymbol{R})$的优势函数 $Adv_{\boldsymbol{D}}(\tau)$可以形式化表示成:

$$Adv_{\boldsymbol{D}}(\tau)=|\Pr[\boldsymbol{D}(n,\boldsymbol{R})=D_{ran}]-\Pr[\boldsymbol{D}(n,\boldsymbol{R})=D_{\varepsilon}]|.$$

DCR 一直是在现代密码学中一个被公认的难解问题,关于 DCR 难解性证明或阐述请参阅 Paillier[22].所以,对于任意的敌手而言,利用任意多项式时间的概率算法 $\boldsymbol{D}$ 区分分布$(n,\boldsymbol{R})$的优势函数 $Adv_{\boldsymbol{D}}(\tau)$是一个可忽略的量,即存在一个关于安全参数$\tau$的可忽略函数$\delta(\tau)$,使得 $Adv_{\boldsymbol{D}}(\tau)$满足:

$$Adv_{\boldsymbol{D}}(\tau)\leqslant\delta(\tau).$$

2 带云辅助计算的同态加密方案

对于 Paillier 加密方案而言,主要的计算开销包括 $g^m \bmod n^2$,$r^n \bmod n^2$ 和 $c^\lambda \bmod n^2$,其中,$g=1+kn, k\in Z_n^*$.本节基于 Paillier 加密方案和云外包计算,并采下述思想 1 和思想 2 设计了一个高效的同态加密方案.

思想 1. 在执行加密算法的过程中,将运算复杂度高的模指数运算 $g^m \bmod n^2$(或 $g^\lambda \bmod n^2$)用与之运算结果等价的、运算高效的模乘运算 $1+m\cdot(g-1)(\bmod n^2)$(或 $1+\lambda\cdot(g-1)(\bmod n^2)$)替代,从而实现快速而正确的加密.

思想 2. 将计算开销大的模指数运算 $r^n \bmod n^2$ 委托给云服务器.

2.1 具体方案

此同态加密系统由 4 种随机算法组成:云外包随机数模指数运算算法(**COR**)、密钥生成算法(**KGen**)、加密算法(**Enc**)和解密算法(**Dec**),其中,云外包随机数模指数运算可以在预处理阶段完成,也可以与密钥生成算法并行执行.在此,我们将该加密方案记作$\mathcal{E}$=(**COR**,**Kgen**,**Enc**,**Dec**).

- **COR**:云服务器随机选择 $r_1,r_2,...,r_k\in Z_n^*$(其中,$k\leqslant n$),计算足够多的 $R_i=r_i^n(\bmod n^2)(1\leqslant i\leqslant k)$, 并将它们存储在集合 R 中.当加密者或者是数据运算者需要 $r_x^n(\bmod n^2)(r_x\in Z_n^{\cdot})$ 时,随时可以从该服务器上下载 R,利用集合 R 中的某些元素,通过适量的简单模乘运算,就可以秘密地得到 $r_x^n(\bmod n^2)$.
- **KGen**:产生长度相等的两个大素数 p,q,并计算二者的乘积($n=pq$)与二者分别减 1 后的最小公倍数 $(\lambda=lcm(p-1,q-1))$, 为加密方案输出公钥(K_{pub}=$(n,1+kn)$,其中, $k\in Z_n^*$)与私钥 $(K_{pri}=\lambda)$.
- **Enc**:加密一方按照如下方式执行加密计算:
  (1) 从云服务器上下载集合 R.
  (2) 自由确定适量的自模乘运算次数(θ),并从 R 上随机选择$\ell(\ell<<n)$个数(记作 $R_1,R_2,...,R_\ell\in R$),随机选择 $\chi_1,\chi_2,...,\chi_\ell\in\{0,...,\ell\}$,其中,$2\leqslant\theta\leqslant\ell$(为了表述简单,在此约定文中此后的加密运算将以两个数为例:$R_i,R_j\in R,i,j\in\{0,\ldots,\ell\}$).
  (3) 对于 $m<n$,计算 $M_g=m\cdot(g-1)(\bmod n^2), R_x=R_i^{\chi_1}\cdot R_j^{\chi_2} \bmod n^2$, 其中,
  $$(\chi_1,\chi_2\in\{0,\ldots,\ell\})\wedge(\chi_1+\chi_2\geqslant 2), c=(1+M_g(\bmod n^2))\cdot R_x \bmod n^2.$$
- **Dec**:解密方执行解密运算:
  $$m=\frac{L(c^\lambda \bmod n^2)}{L((1+\lambda\cdot(g-1)) \bmod n^2)} \bmod n,\text{其中,}L(u)=\frac{u-1}{n},u\in Z_{n^2}^*.$$

2.2 正确性验证

2.2.1 由云服务器计算 $R_i=r_i^n(\bmod n^2)(1\leqslant i\leqslant k, r_x\in Z_n^{\cdot})$ 的合理性

显然,云服务器计算 $R_i=r_i^n(\bmod n^2)$ 是否合理,就是看其是否满足以下两个条件:(1) 加密运算中引入的随机变量可以在解密运算中被成功消除,即 $R_x=R_i^{\chi_1}\cdot R_j^{\chi_2} \bmod n^2\ (\chi_1,\chi_2\in\{0,\ldots,\ell\})\wedge(\chi_1+\chi_2\geqslant 2)$在形式上依然可以表示成 $R_x=r_x^n \bmod n^2$, 其中, $r_x\in Z_n^*$;(2) 加密运算采用计算 $R_x=R_i^{\chi_1}\cdot R_j^{\chi_2} \bmod n^2$ 的方式引入随机变量,不会削弱方案的安全性.

(1) 加密运算中引入的随机变量可以在解密运算中被成功消除.

如果解密运算能够成功将加密运算中引入的随机变量消除,则 $R_x=R_i^{\chi_1}\cdot R_j^{\chi_2} \bmod n^2$ 必满足 $R_x^\lambda \bmod n^2\equiv 1$, 即 $R_x=r_x^n \bmod n^2$, 其中, $r_x\in Z_n^*$.令 $r_i,r_j\in Z_n^*$,则 r_ir_j 可以表示成 $r_i^{\chi_1}r_j^{\chi_2}=r_x+\gamma n$,其中, $r_x\in Z_n^*$ (因为 $r_i,r_j\in Z_n^*$,所以

$r_i^{\chi_1} r_j^{\chi_2}$ 不能被 n 整除,从而可得 $r_x \neq 0$),其中,$\gamma \in Z_{n-1}$ 之间的整数.

因为 $R_i = r_i^n (\text{mod } n^2)(1 \leqslant i \leqslant k), R_j = r_j^n (\text{mod } n^2)(1 \leqslant j \leqslant k)$,所以,

$$\begin{aligned} R_x &= R_i^{\chi_1} \cdot R_j^{\chi_2} (\text{mod } n^2) \\ &= (r_i^n)^{\chi_1} \cdot (r_j^n)^{\chi_2} (\text{mod } n^2) \\ &= (r_i^{\chi_1} r_j^{\chi_2})^n (\text{mod } n^2) \\ &= (r_x + \gamma n)^n (\text{mod } n^2) \\ &= \sum_{k=0}^{n} \binom{n}{k} r_x^{n-k} (\gamma n)^k (\text{mod } n^2) \\ &= r_x^n (\text{mod } n^2). \end{aligned}$$

(2) 加密运算采用计算 $R_x = R_i^{\chi_1} \cdot R_j^{\chi_2} \bmod n^2$ 的方式引入随机变量,在语义安全层面不会削弱方案的安全性.

R 虽然是公开的,但 $R_1, R_2, ..., R_\ell \in R$,$\ell$以及 $\chi_1, \chi_2, ..., \chi_\ell \in \{0, ..., \ell\}$ 都是加密者在加密运算中随机选择的,因此,以 $R_1, R_2, ..., R_\ell \in R$ 为随机种子,由随机函数 $R_x = R_1^{\chi_1} \cdot R_2^{\chi_2} \cdot ... \cdot R_\ell^{\chi_\ell} \bmod n^2 = r_x^n \bmod n^2$ 计算得到的 R_x 与计算 $(1+kn)^0 \cdot r_{x'}^n \bmod n^2$ (其中,$r_{x'} \in Z_n^*$ 是随机选择的)是等效的,因此,任何敌手由 R 计算 R_x 的困难性与破解 Paillier 加密方案的困难性是等价的.

综上所述,加密方案$\mathcal{E}$将计算 $R_i = r_i^n (\text{mod } n^2)(1 \leqslant i \leqslant k, r_i \in Z_n^*)$ 委托给云服务器执行,在语义安全的安全层面上是合理的.

2.2.2 替换运算的正确性

定理 1. $1+m\cdot(g-1)(\text{mod } n^2)$的结果与模指数运算 $g^m \bmod n^2$ 的结果是等价的,即

$$1+m\cdot(g-1)(\text{mod } n^2) \Leftrightarrow g^m \bmod n^2.$$

证明:因为 $g=1+kn\ (k \in Z_n^+)$,所以,

$$1+m\cdot(g-1)(\text{mod } n^2)=1+m\cdot(1+kn-1)(\text{mod } n^2)=1+m\cdot kn(\text{mod } n^2);$$

又由二项式展开定理得:

$$g^m \bmod n^2 = (1+kn)^m \bmod n^2 = \sum_{\kappa=0}^{m} \binom{m}{\kappa} 1_x^{m-\kappa} (kn)^\kappa \bmod n^2 = 1 + \binom{m}{1} \cdot kn \bmod n^2 = 1 + m \cdot kn \bmod n^2.$$

综上可得:$1+m\cdot(g-1)(\text{mod } n^2) \Leftrightarrow g^m \bmod n^2$. □

2.2.3 解密正确性

因为

$$\begin{aligned} c &= ((1+m\cdot(g-1))(\text{mod } n^2)) \cdot ((R_i \cdot R_j \bmod n^2) \bmod n^2) \bmod n^2 \\ &= (1+m\cdot(1+kn-1)(\text{mod } n^2)) \cdot (r_x^n \bmod n^2) \bmod n^2 \\ &= ((1+kn)^m \bmod n^2) \cdot (r_x^n \bmod n^2) \bmod n^2 \\ &= g^m r_x^n \bmod n^2, \end{aligned}$$

所以有:

$$\frac{L(c^\lambda \bmod n^2)}{L((1+\lambda\cdot(g-1)) \bmod n^2)} \bmod n = \frac{(c^\lambda \bmod n^2)-1}{((1+\lambda\cdot kn) \bmod n^2)-1} \bmod n = \frac{(1+m\cdot kn)-1}{(1+kn)-1} \bmod n = m.$$

2.3 安全性分析

定理 2. 如果 DCR 是难解问题,则$\mathcal{E}$=(**COR**,**Kgen**,**Enc**,**Dec**)具有第 1.1 节中定义 1 所定义的不可区分安全性.

证明:在此先回忆一下 DCR 问题挑战者的工作方式.

- 在安全时间 1^k 内,通过执行算法$\mathcal{G}(1^k)$算法产生两个大素数 p 和 q,以及它们的乘积 n.
- 在 Z_n 上随机选取一个数 r,并从{0,1}中均匀选取一个数 f.

- 若 f 为 0,则将$\mathcal{R}$置为 $r^n \bmod n^2$;若 f 为 1,则将$\mathcal{R}$置成 R.

设$\mathcal{E}$=(**COR**,**Kgen**,**Enc**,**Dec**)是 **2.1** 节中构造的方案,将攻击$\mathcal{E}$=(**COR**,**Kgen**,**Enc**,**Dec**)时,敌手使用的多项式时间算法记作$\mathcal{A}$,下面利用算法$\mathcal{A}$构造一个算法$\mathcal{B}$,用于解决 DCR 问题.该算法的具体工作方式如下.

(1) 接收 DCR 挑战者发来的(n,(n,$\mathcal{R}$));

(2) 令 pk=(n,1+kn);

(3) 将 1^n 和 pk 发送给$\mathcal{A}$;

(4) 接收$\mathcal{A}$发来的消息 m_0 和 m_1;

(5) 均匀地选取 $d\in\{0,1\}$;

(6) 令 $C^*=(n,y,y,y',y'',(g')^{m_d}\cdot\mathcal{R}(\bmod n^2))$, 并将 C^*发送给$\mathcal{A}$;

(7) 用 d'表示敌手$\mathcal{A}$对 d 的猜测结果;

(8) 输出 f'(如果 d=d',则置 f'=0;如果 $d\neq d'$,则置 f'=1).

因为算法$\mathcal{B}$只通过调用算法$\mathcal{A}$实现且只调用了 3 次,而作为构成算法$\mathcal{B}$的子算法$\mathcal{A}$是在多项式时间内可被完成的算法,所以通过 3 次调用算法$\mathcal{A}$而实现的算法$\mathcal{B}$是一种在多项式时间内可被完成的算法.因此,$\mathcal{G}(1^k)$也是一种在多项式时间内完成的算法.于是,构造算法$\mathcal{B}$在 DCR 安全游戏中获胜的概率可以表示成贝叶斯公式形式:

$$\left.\begin{aligned}\Pr[f=f']&=\Pr[f=0]\Pr[f=f'\mid f=0]+\Pr[f=1]\Pr[f=f'\mid f=1]\\&=\frac{1}{2}\Pr[f'=0\mid f=0]+\frac{1}{2}\Pr[f'=1\mid f=1]\\&=\frac{1}{2}\Pr[d=d'\mid f=0]+\frac{1}{2}\Pr[d\neq d'\mid f=1]\end{aligned}\right\}\tag{3}$$

当 f=0 时,DCR 挑战者置$\mathcal{R}$=$r^n \bmod n^2$.这样,由算法$\mathcal{A}$构造的算法$\mathcal{B}$呈现给掌握算法$\mathcal{A}$的敌手的视图与掌握算法$\mathcal{A}$的敌手在实际攻击$\mathcal{E}$=(**COR**,**Kgen**,**Enc**,**Dec**)的安全游戏中获取的视图相同.因此,掌握算法$\mathcal{A}$的敌手在攻击$\mathcal{E}$=(**COR**,**Kgen**,**Enc**,**Dec**)的安全游戏中获胜的概率等于 d=d'在条件 f=0 下的条件概率,即

$$\Pr[d=d'\mid f=0]=\frac{1}{2}+\delta\tag{4}$$

当 f=1 时,DCR 挑战者将$\mathcal{R}$置成 R.因为 $R\in Z_{n^2}$ 是均匀选取的,所以,执行运算 $(g')^{m_d}\cdot\mathcal{R}(\bmod n^2)$ 后的结果在群 Z/n^2Z 上是均匀分布的;又因为 3 个随机变量 m_0,m_1,d 相互独立,因此,pk 和 C^*没有暴露关于 d 的任何消息,这意味着掌握算法$\mathcal{A}$的敌手对于 d 的猜测结果 d'与 d 相互独立.若在{0,1}上随机选取 d,则 d=0 或 d=1 的概率各为 $\frac{1}{2}$,故有:

$$\Pr[d=d'\mid f=1]=\frac{1}{2}\tag{5}$$

成立.联立公式(3)~公式(5),我们可以得到:

$$\Pr[f=f']=\frac{1}{2}\left(\frac{1}{2}+\delta\right)+\frac{1}{2}\times\frac{1}{2}=\frac{1}{2}+\frac{1}{2}\delta\tag{6}$$

因此,算法$\mathcal{B}$在 DCR 安全游戏中获胜的优势为

$$\left|\Pr[f=f']-\frac{1}{2}\right|=\left|\left(\frac{1}{2}+\frac{1}{2}\delta\right)-\frac{1}{2}\right|=\frac{\delta}{2}\tag{7}$$

由第 1.1 节中定义 1 可知,在 DCR 安全性游戏中,利用算法$\mathcal{A}$构造的算法$\mathcal{B}$获胜的优势是一个可忽略的量,所以 $\frac{\delta}{2}$ 是一个可忽略的值.这意味δ也是一个可忽略的量.所以利用算法$\mathcal{A}$的敌手在攻击方案$\mathcal{E}$的 IND-CPA 安全游戏中获胜的优势是一个可忽略的量,即$\mathcal{E}$=(**COR**,**Kgen**,**Enc**,**Dec**)具有 IND-CPA 安全性. □

2.4 加密方案的效率分析

因为同态加密方案$\mathcal{E}$中的计算 $R_i=r_i^n \bmod n^2$ 是在预处理阶段由云服务器完成,并且加密者可以在加密前的预处理阶段从云服务器下载集合 $R=\{R_i \mid R_i=r_i^n \bmod n^2\}$, 加密时利用集合中的元素通过执行简单的几次模乘运算($R_x=R_i^{\chi_1}\cdot R_j^{\chi_2} \bmod n^2$, 其中,$(\chi_1,\chi_2\in\{0,\ldots,\ell\})\wedge(\chi_1+\chi_2\geqslant 2)$)即可秘密地得到 $r_x^n \bmod n^2$, 无需再做 n 次复杂的自模乘运算.同时,加密时运算复杂度高的模指数运算 $g^m \bmod n^2$(解密时 $g^\lambda \bmod n^2$)是用与之运算结果等价的、运算简单高效的模乘运算 $1+m\cdot(g-1)(\bmod n^2)$(解密时 $1+\lambda\cdot(g-1)(\bmod n^2)$)替代实现的;若忽略预处理时间,则用方案$\mathcal{E}$加密一个消息的总计需要花费 $6+\lambda$次模乘运算.而用 Paillier 方案加密一个小小的总开销绝不会少于 $2n$ 次模乘运算.表 1 是加密方案$\mathcal{E}$和 Paillier 方案在加、解密效率方面的对比.

Table 1 Comparative analysis on the efficiency of encryption and decryption

表 1 加、解密效率对比分析

类型	加密开销(自模乘运算($r_x^2 \bmod n^2$)次数)	解密开销(自模乘运算($r_x^2 \bmod n^2$)次数)	总计
Paillier 方案	不少于 n	不少于 n	不少于 $2n$
方案$\mathcal{E}$	–	$2+\lambda$	$4+\lambda$

3 保密社交意愿探测协议

3.1 保密社交意愿应用背景描述及其形式化

Alice(需求者)是保险公司的职员,某天在某一个城市推销保险产品,她只想约谈现在正好在某个区域内的客户(可能住在该区域,也可能正在该区域且有空闲时间),她与不想向不在该区域且不愿约谈的用户透露自己的活动区域,例如她想约谈客户 Bob,但 Bob 只想让 Alice 知道他是否可被约谈而不想透露自己的具体位置.Bob 和 Alice 怎样做才能同时实现他们的各自的目的呢?然而,安全多方几何计算为解决这种问题提供了一种可行的方法.我们将 Bob 和 Alice 采用安全多方几何计算思路实现保密测试社交意愿的问题称为保密社交意愿探测问题,其形式化描述如下:

Alice 拥有一个有 K 个顶点 $p_{a_1},p_{a_2},\ldots,p_{a_K}$ ($p_i=(a_{x_i},a_{y_i})$,$1\leqslant i\leqslant K$) 构成的私有凸多边形 P,表示她现在利益最大的活动范围.其中,该多边形的边是按逆时针方向标注的,如图 2 所示(以 K=7 为例).

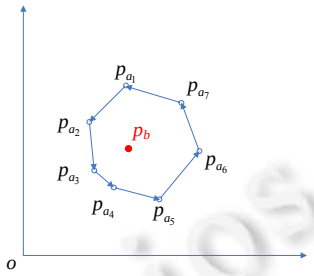


Fig.2 Abstract geometrical figure of private social-willing testing

图 2 保密社交意愿探测几何抽象图

Bob 拥有一个私有点 $p_b=(b_x,b_y)$,表示他现在所处的位置.Alice 想知道 Bob 是否处在自己的想活动的范围内,Bob 不想透露自己的具体位置.我们设计一个这样的安全多方计算协议要实现对 Alice 与 Bob 的隐私保护.

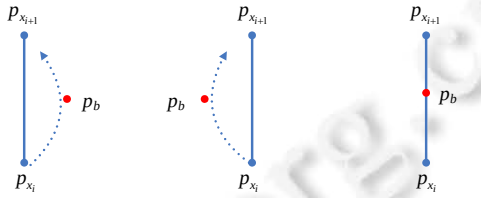
- 协议结束时,Alice 只得到一个意愿探测的结果(一个布尔值),而 Bob 的具体位置信息对于 Alice 仍然是一个秘密.
- 协议结束时,最多只得到 Alice 多边形的边数 $K-1$(Bob 没有得到意愿探测的结果),而 Alice 的活动区域的形状、位置与活动区域的大小对于 Bob 仍然是一个秘密.

3.2 保密社交意愿探测协议

3.2.1 判定凸多边形与一个点位置关系

非保密的近感探测问题实际上就是判定某个凸多边形 P(有 K 个顶点 $p_{a_1},p_{a_2},...,p_{a_K}$)是否包含一个点 p_b=(b_x,b_y)的问题.可以通过 K 次计算有向线段 $\overrightarrow{p_ip_{i+1}}$ 与点 p_b=(b_x,b_y)的位置关系来实现[24−26,29].对于点 p_i,p_b,p_{i+1} 构成的有序元组⟨p_i,p_b,p_{i+1}⟩在平面上可能对应着 3 种位置关系(如图 3 所示).

- 正向:3 个点构成的方向角∠p_i,p_b,p_{i+1} 为逆时针走向(如图 3(a)所示).
- 反向:3 个点构成的方向角∠p_i,p_b,p_{i+1} 为顺时针走向(如图 3(b)所示).
- 零向:3 个点构成的方向角∠p_i,p_b,p_{i+1}=180°,即 p_i,p_b,p_{i+1} 共线(如图 3(c)所示).



(a) 正向 (b) 反向 (c) 零向

Fig.3 Position relations between a point and a line segment

图 3 点与线段的位置关系

假设点 p_i,p_b,p_{i+1} 的坐标分别为 $p_i=(a_{x_i},a_{y_i}),p_b=(b_x,b_y),p_{i+1}=(a_{x_{i+1}},a_{y_{i+1}})$,则 3 点构成的方向角∠$p_i$,$p_b$,$p_{i+1}$ 的方向可以通过计算下列行列式来确立:

$$\left.\begin{aligned}D_i&=\begin{vmatrix}a_{x_i}-b_x & a_{y_i}-b_y\\ a_{x_{i+1}}-b_x & a_{y_{i+1}}-b_y\end{vmatrix}\\&=b_x(a_{y_{i+1}}-a_{y_i})+b_y(a_{x_i}-a_{x_{i+1}})+(a_{y_i}a_{x_{i+1}}-a_{x_i}a_{y_{i+1}})\\&=b_xa_{y_{i+1}}+b_ya_{x_i}+a_{y_i}a_{x_{i+1}}-(b_xa_{y_i}+b_ya_{x_{i+1}}+a_{x_i}a_{y_{i+1}})\end{aligned}\right\}\tag{8}$$

其中,D_i>0,D_i<0,D_i=0 分别对应着图 3(a)~图 3(c).

因此,下面的算法可以正确计算出近感探测的结果.

凸多边形与点的关系判定算法.

输入:由 K 个按逆时针顺序访问的顶点 $p_{a_1},p_{a_2},...,p_{a_K}$ 构成的凸多边形 P,点 p_b.

输出:“1”,如果 p_b 在 P 内;“0”,否则 p_b 不在 P 内.

(1) 对于 i∈{1,2,…,K−1}计算点 p_b 与有向线段 $\overrightarrow{p_ip_{i+1}}$ 两个端点所构成的方向角∠p_i,p_b,p_{i+1} 的方向 D_i.

(2) 如果对于∀i∈{1,2,…,K−1}都有 D_i≤0,则返回“1”;否则,返回“0”.

3.2.2 保密社交意愿探测协议

利用上述凸多边形与点的位置关系判定方法、第 2.1 节中设计的带云辅助计算的同态加密方案以及一种新的保密符号计算方法,设计了一个保密社交意愿探测协议.

保密社交意愿探测协议.

输入:Alice 输入由 K 个按逆时针顺序访问的顶点 $p_{a_1},p_{a_2},...,p_{a_K}$ 构成的凸多边形 P,Bob 输入点 p_b.

输出:“1”,如果 p_b 在 P 内;“0”,否则 p_b 不在 P 内.

1. COR:云服务器随机选 $r_1,r_2,...,r_k\in Z_n^*$(其中,k≤n),计算足够多的 $R_i=r_i^n(\mathrm{mod}\ n^2)(1\leqslant i\leqslant k)$,并将它们存储在集合 R 中.当加密者或者是数据运算者需要 $r_x^n(\mathrm{mod}\ n^2)$ 时,随时可以从该服务器上下载 R,利用集合 R 中的某些元素通过一些简单的模乘运算就可以秘密地得到 $r_x^n(\mathrm{mod}\ n^2)$.

2. Alice 运行加密系统$\mathcal{E}$=(**COR**,**Kgen**,**Enc**,**Dec**)的密钥生成算法 Kgen,生成公钥 K_{pub}=(n,1+kn)和私钥 K_{pri}=λ;

3. Alice 首先从云服务器上下载集合 R 并随机选取 $R_{A_{j1}},R_{A_{j2}},...,R_{A_{j12}}\in R$,然后按照如下方式操作:

(1) 对于 $j\in\{1,2,\ldots,K-1\}$计算(假设 Alice 将χ_1,χ_2取作$\chi_1=\chi_2=1$,并置$\ell=2$):

$$E_\varepsilon(a_{y_{j+1}})\equiv(1+a_{y_{j+1}}(g-1))\cdot R_{A_{j1}}\cdot R_{A_{j2}} \bmod n^2,\ E_\varepsilon(a_{x_j})\equiv(1+a_{x_j}(g-1))\cdot R_{A_{j3}}\cdot R_{A_{j4}} \bmod n^2,$$

$$E_\varepsilon(a_{y_j}a_{x_{j+1}})\equiv(1+a_{y_j}a_{x_{j+1}}(g-1))\cdot R_{A_{j5}}\cdot R_{A_{j6}} \bmod n^2,\ E_\varepsilon(a_{y_j})\equiv(1+a_{y_j}(g-1))\cdot R_{A_{j7}}\cdot R_{A_{j8}} \bmod n^2,$$

$$E_\varepsilon(a_{x_{j+1}})\equiv(1+a_{x_{j+1}}(g-1))\cdot R_{A_{j9}}\cdot R_{A_{j10}} \bmod n^2,\ E_\varepsilon(a_{x_j}a_{y_{j+1}})\equiv(1+a_{x_j}a_{y_{j+1}}(g-1))\cdot R_{A_{j11}}\cdot R_{A_{j12}} \bmod n^2.$$

(2) 将密文元组 $(E_\varepsilon(a_{y_{j+1}}),E_\varepsilon(a_{x_j}),E_\varepsilon(a_{y_j}a_{x_{j+1}}),E_\varepsilon(a_{y_j}),E_\varepsilon(a_{x_{j+1}}),E_\varepsilon(a_{x_j}a_{y_{j+1}}))$ 记作 $E_\varepsilon(A_j)$, 其中 $j\in\{1,2,\ldots,K-1\}$,对所有密文元组 $E_\varepsilon(A_1),E_\varepsilon(A_2),...,E_\varepsilon(A_{K-1})$ 做随机置换,并将所有的密文元组 $(E_\varepsilon(a_{y_{i+1}}),E_\varepsilon(a_{x_i}),E_\varepsilon(a_{y_i}a_{x_{i+1}}),E_\varepsilon(a_{y_i}),E_\varepsilon(a_{x_{i+1}}),E_\varepsilon(a_{x_i}a_{y_{i+1}}))\in\{E_\varepsilon(A_1),E_{\mathrm{E}}(A_2),...,E_\varepsilon(A_{K-1})\}$ 发给 Bob.

4. 对于 $i\in\{1,2,\ldots,K-1\}$,Bob 收到 $E_\varepsilon(a_{y_{i+1}}),E_\varepsilon(a_{x_i}),E_\varepsilon(a_{y_i}a_{x_{i+1}}),E_\varepsilon(a_{y_i}),E_\varepsilon(a_{x_{i+1}}),E_\varepsilon(a_{x_i}a_{y_{i+1}})$ 后,按照如下方式进行:

(1) 计算: $E_\varepsilon(b_xa_{y_{i+1}})\equiv(E_\varepsilon(a_{y_{i+1}}))^{b_x} \bmod n^2, E_\varepsilon(b_ya_{x_i})\equiv(E_\varepsilon(a_{x_i}))^{b_y} \bmod n^2$.

(2) 从云服务器上下载集合 R 后,随机选择 $k_b,r_{b_1}\in Z_n$, $2\ell(\ell\leqslant k)$个数: $R_1,R_2,...,R_\ell\in R,\chi_1,\chi_2,...,\chi_\ell,\chi_1',\chi_2',...,\chi_\ell'\in\{0,...,\ell\}$, 其中,$\ell$是一个比 1 大一些的小整数.并计算:

$$E_\varepsilon(r_{b1})=(1+r_{b1}\cdot k_b\cdot(g-1)\cdot R_1^{\chi_1}\cdot R_2^{\chi_2}\cdot\ldots\cdot R_\ell^{\chi_\ell} \bmod n^2,$$

$$E_\varepsilon(k_b(b_xa_{y_{i+1}}+b_ya_{x_i}+a_{y_i}a_{x_{i+1}})+r_{b1})\equiv((E_\varepsilon(b_xa_{y_{i+1}})E_\varepsilon(b_ya_{x_i})E_\varepsilon(a_{y_i}a_{x_{i+1}}) \bmod n^2)^{k_b} \bmod n^2)E_\varepsilon(r_{b1}) \bmod n^2,$$

$$E_\varepsilon(b_xa_{y_i})\equiv(E_\varepsilon(a_{y_i}))^{b_x} \bmod n^2,$$

$$E_\varepsilon(b_ya_{x_{i+1}})\equiv(E_\varepsilon(a_{x_{i+1}}))^{b_y} \bmod n^2.$$

(3) 随机选择 $r_{b_2}\in Z_n$, 并计算:

$$E_\varepsilon(r_{b_2})=(1+r_{b_2}\cdot k_b\cdot(g-1)\cdot R_1^{\chi_1'}\cdot R_2^{\chi_2'}\cdot\ldots\cdot R_\ell^{\chi_\ell'} \bmod n^2,$$

$$E_\varepsilon(k_b(b_xa_{y_i}+b_ya_{x_{i+1}}+a_{x_i}a_{y_{i+1}})+r_{b_2})\equiv((E_\varepsilon(b_xa_{y_i})E_\varepsilon(b_ya_{x_{i+1}})E_\varepsilon(a_{x_i}a_{y_{i+1}}))^{k_b} \bmod n^2)E_\varepsilon(r_{b_2}) \bmod n^2,$$

并将 $E_\varepsilon(k_b(b_xa_{y_{i+1}}+b_ya_{x_i}+a_{y_i}a_{x_{i+1}})+r_{b_1}),E_\varepsilon(k_b(b_xa_{y_i}+b_ya_{x_{i+1}}+a_{x_i}a_{y_{i+1}})+r_{b_2})$ 按随机顺序发给 Alice.

5. 对于 $i\in\{1,2,\ldots,K-1\}$,收到 $E_\varepsilon(k_b(b_xa_{y_{i+1}}+b_ya_{x_i}+a_{y_i}a_{x_{i+1}})+r_{b_1}),E_\varepsilon(k_b(b_xa_{y_i}+b_ya_{x_{i+1}}+a_{x_i}a_{y_{i+1}})+r_{b_2})$ 以后,Alice 计算:

$$\theta_i=\frac{\dfrac{L((E_\varepsilon(k_b(b_xa_{y_{i+1}}+b_ya_{x_i}+a_{y_i}a_{x_{i+1}})+r_{b1}))^\lambda \bmod n^2)}{L(g^\lambda)}}{\dfrac{L((E_\varepsilon(k_b(b_xa_{y_i}+b_ya_{x_{i+1}}+a_{x_i}a_{y_{i+1}})+r_{b2}))^\lambda) \bmod n^2}{L(g^\lambda)}}=\frac{L(E_\varepsilon(k_b(b_xa_{y_{i+1}}+b_ya_{x_i}+a_{y_i}a_{x_{i+1}})+r_{b1}))^\lambda \bmod n^2)}{L((E_\varepsilon(k_b(b_xa_{y_i}+b_ya_{x_{i+1}}+a_{x_i}a_{y_{i+1}})+r_{b2}))^\lambda \bmod n^2)}.$$

6. 通过判断θ_i与“1”的关系,确定 D_i 的符号:

$$Sign(D_i)=\begin{cases}1, & \theta_i>1\\ 0, & \theta_i=1\\ -1, & \theta_i<1\end{cases},$$

其中,$Sign(\cdot)$为符号函数.

7. 如果对于$\forall i\in\{1,2,\ldots,K-1\}$都有 $D_i\leqslant 0$,则返回“D=1”;否则,返回“D=0”.

3.3 保密社交意愿探测协议保密性分析

定理 3. 保密社交意愿探测协议可以安全地实现 Alice,Bob 两方的社交意愿探测.

证明:该协议安全与否的关键是协议执行后有没有造成参与者私有信息的泄露.接下来,我们将证明保密意愿探测协议在安全计算约谈意愿的过程中,Alice(持有凸多边形的活动区域 P,由顶点 $p_{a_1},p_{a_2},...,p_{a_K}$ 构成)、Bob (持有位置 p_b)两方除了得到“是否约谈”外,都无法获得有关对方私有数据的其他任何信息,即协议未给 Alice、Bob 两方造成信息泄露.

- 对于 Alice 数据的安全性

我们首先构造一个模拟保密探测协议执行的模拟器$\mathcal{S}_{\boldsymbol{B}}$.该模拟器的输入为:Alice 随机选择一个凸的活动区域 $p'_{a_1}, p'_{a_2}, ..., p'_{a_K}$, Bob 的私有位置 p_b,那么由模拟器$\mathcal{S}_{\boldsymbol{B}}$ 产生的视图为($p_b, E'_{\mathcal{E}}(a_{y_{i+1}}), E'_{\mathcal{E}}(a_{x_i}), E'_{\mathcal{E}}(a_{y_i}a_{x_{i+1}}), E'_{\mathcal{E}}(a_{y_i}), E'_{\mathcal{E}}(a_{x_{i+1}}), E'_{\mathcal{E}}(a_{x_i}a_{y_{i+1}})$),其中,$1\leqslant i\leqslant k$;而保密社交意愿探测协议的实际执行产生的视图为($p_b, E_{\mathcal{E}}(a_{y_{i+1}}), E_{\mathcal{E}}(a_{x_i}), E_{\mathcal{E}}(a_{y_i}a_{x_{i+1}}), E_{\mathcal{E}}(a_{y_i}), E_{\mathcal{E}}(a_{x_{i+1}}), E_{\mathcal{E}}(a_{x_i}a_{y_{i+1}})$),其中 $1\leqslant i\leqslant k$.因为 Alice 传输给 Bob 的信息是用自己的公钥$(n,n+1)$对自己的私有信息加密后的密文,又因方案$\mathcal{E}$已被证明在选择明文攻击下具有语义不可区分安全,所以由加密方案$\mathcal{E}$产生的密文是语义不可区分的,可得 $E'_{\mathcal{E}}(a_{y_{i+1}}), E'_{\mathcal{E}}(a_{x_i}), E'_{\mathcal{E}}(a_{y_i}a_{x_{i+1}}), E'_{\mathcal{E}}(a_{y_i}), E'_{\mathcal{E}}(a_{x_{i+1}}), E'_{\mathcal{E}}(a_{x_i}a_{y_{i+1}})$ 与 $E_{\mathcal{E}}(a_{y_{i+1}}), E_{\mathcal{E}}(a_{x_i}), E_{\mathcal{E}}(a_{y_i}a_{x_{i+1}}), E_{\mathcal{E}}(a_{y_i}), E_{\mathcal{E}}(a_{x_{i+1}}), E_{\mathcal{E}}(a_{x_i}a_{y_{i+1}})$ 是不可区分的.从而可得 $\mathcal{S}_{\boldsymbol{B}}(E'_{\mathcal{E}}(a_{y_{i+1}}), E'_{\mathcal{E}}(a_{x_i}), E'_{\mathcal{E}}(a_{y_i}a_{x_{i+1}}), E'_{\mathcal{E}}(a_{y_i}), E'_{\mathcal{E}}(a_{x_{i+1}}), E'_{\mathcal{E}}(a_{x_i}a_{y_{i+1}}), p_b)$ 与真实视图 $view_{\boldsymbol{B}}^{\Pi}(E_{\mathcal{E}}(a_{y_{i+1}}), E_{\mathcal{E}}(a_{x_i}), E_{\mathcal{E}}(a_{y_i}a_{x_{i+1}}), E_{\mathcal{E}}(a_{y_i}), E_{\mathcal{E}}(a_{x_{i+1}}), E_{\mathcal{E}}(a_{x_i}a_{y_{i+1}}), p_b)$ 是不可区分的,也就是说,满足定义关系式(2).

- 对于 Bob 位置信息的私密性

我们构造一个 Bob,输入其私有位置信息以及由其随机选择的 $k_b, r_{b_1}, r_{b_2}\in Z_n$, 就能模拟 Alice 视图的模拟器$\mathcal{S}_{\boldsymbol{A}}$.于是,由模拟器$\mathcal{S}_{\boldsymbol{A}}$产生的视图为

$$(p_{a_1}, p_{a_2}, ..., p_{a_K}, E_{\mathcal{E}}(k_b(b_x a_{y_{i+1}} + b_y a_{x_i} + a_{y_i}a_{x_{i+1}}) + r_{b_1}), E_{\mathcal{E}}(k_b(b_x a_{y_i} + b_y a_{x_{i+1}} + a_{x_i}a_{y_{i+1}}) + r_{b_2}), D).$$

因密文 $E_{\mathcal{E}}(k_b(b_x a_{y_{i+1}} + b_y a_{x_i} + a_{y_i}a_{x_{i+1}}) + r_{b_1}), E_{\mathcal{E}}(k_b(b_x a_{y_i} + b_y a_{x_{i+1}} + a_{x_i}a_{y_{i+1}}) + r_{b_2})$ 是 Bob 由密文 $E_{\mathcal{E}}(a_{y_{i+1}}), E_{\mathcal{E}}(a_{x_i}), E_{\mathcal{E}}(a_{y_i}a_{x_{i+1}}), E_{\mathcal{E}}(a_{y_i}), E_{\mathcal{E}}(a_{x_{i+1}}), E_{\mathcal{E}}(a_{x_i}a_{y_{i+1}})$ 通过同态运算计算得到的,Alice 获得 $E_{\mathcal{E}}(k_b(b_x a_{y_{i+1}} + b_y a_{x_i} + a_{y_i}a_{x_{i+1}}) + r_{b_1}), E_{\mathcal{E}}(k_b(b_x a_{y_i} + b_y a_{x_{i+1}} + a_{x_i}a_{y_{i+1}}) + r_{b_2})$ 后,通过解密运算,最多只能得到两个各包含 5 个未知数的方程,通过联立方程组计算出具体的 (b_x, b_y) 是不可行的,故 $(p_{a_1}, p_{a_2}, ..., p_{a_K}, E_{\mathcal{E}}(k_b(b_x a_{y_{i+1}} + b_y a_{x_i} + a_{y_i}a_{x_{i+1}}) + r_{b_1}), E_{\mathcal{E}}(k_b(b_x a_{y_i} + b_y a_{x_{i+1}} + a_{x_i}a_{y_{i+1}}) + r_{b_2}), D)$ 与实际执行中的视图是计算不可区分的,即满足安全定义中的等式(1).

综上所述,Alice 和 Bob 的私密性满足安全定义的形式化等式(1)和等式(2).所以,保密社交意愿探测协议可以安全地实现 Alice、Bob 两方社交意愿的探测. □

4 保密社交意愿探测协议效率分析

不失一般性,我们假定 Alice 和 Bob 为文献[1]的协议和本文协议的参与者,并假定 Bob 的坐标为(b_x,b_y),Alice 提供的意愿区域为 K 个顶点构成的凸多边形.为了进行公平比较,此处将执行协议时花费的总开销统一用一次自模乘运算($r_x^2 \bmod n^2$)作为统计的基本单位.

Alice 和 Bob 在执行文献[1]的协议时,总共至少需要 $K(8n+b_x+b_y+2\lambda)$次自模乘运算($r_x^2 \bmod n^2$).因为基于云外包计算的同态加密方案$\mathcal{E}$中的计算 $R_i = r_i^n \bmod n^2$ 可以在预处理阶段由云服务器完成,并且 Alice 和 Bob 在预处理阶段可以随时随地地从云服务器下载集合 $R=\{R_i \mid R_i = r_i^n \bmod n^2\}$,所以得到集合 $R=\{R_i \mid R_i = r_i^n \bmod n^2\}$ 的时间可以忽略不计;又因为 Alice 和 Bob 在得到集合 $R=\{R_i \mid R_i = r_i^n \bmod n^2\}$ 后,利用集合中的元素,通过执行有限次的模乘运算($r_x^2 \bmod n^2$),即可秘密地得到 $r_x^n \bmod n^2$, 不再需要做 n 次自模乘运算($r_x^2 \bmod n^2$).因此,基于同态加密方案$\mathcal{E}$的保密社交意愿探测协议时,Alice 和 Bob 总计需要花费 $K(18+2b_x+2b_y+2k_b+2(\ell+2)+2\lambda)$次自模乘运算($r_x^2 \bmod n^2$).显然,本文的协议比文献[1]的协议在运算效率上有了质变性的提升.

基于同态加密方案$\mathcal{E}$的保密社交意愿探测协议可以解决 Alice 出具的 K 个顶点相邻顶点坐标差小于 0 的情形;而对于文献[1]的协议而言,当 Alice 出具的 K 个顶点相邻顶点坐标差小于 0 时,它无法正确运行.此外,文献[1]的协议只能用于解决实时位置的近感探测问题,已经不能满足社交网络用户新的个性化需求;而本协议不仅可以用于彻底解决文献[1]的协议提出的近感探测问题,还能满足社交网络用户日益增长的个性化需求:保密社交筹划,即保密社交意愿探测,解决的是保密探测领域中的新问题.下表是保密社交探测协议和协议在效率(用执行协议时各参与方在加密和解密算法中花费的计算开销总和体现)、解决问题的能力(从能否解决保密探测区域相邻两点坐标差商小于 0 的情形体现)以及能够解决的问题这 3 个方面的对比.保密探测协议与文献[1]的协

议的对比分析见表 2.

Table 2 Comparative analysis on private social-willing test and the protocol of Ref.[1]

表 2 保密探测协议与文献[1]的协议的对比分析

类型	Alice 和 Bob 总开销 (自模乘运算($r_x^2 \bmod n^2$)次数)	解决问题的能力(能否解决保密探测区域相邻两点坐标差商小于 0 的情形)	能解决的问题
文献[1]的协议	至少为 $K(8n+b_x+b_y+2\lambda)$	×	保密近感探测
本协议	$K(18+2b_x+2b_y+2k_b+2(\ell+2)+2\lambda)$	√	保密社交意愿探测 保密近感探测

√表示具有某种性能,×表示不具有某种性能

5 结束语

本文对保密意愿探测问题进行了研究.为了高效地解决这一问题,首先设计了一个带云辅助计算的同态加密方案;然后,利用该加密方案设计了一个高效的保密意愿探测协议.分析结果表明,此协议在效率和安全性方面都优于先前的类似协议,并且其安全性是在标准的 ideal/real 模型下实现的.

References:

[1] Mu B, Bakiras S. Private proximity detection for convex polygons. Tsinghua Science and Technology, 2016,21(3):270−280.

[2] Jing T, Lin P, Lu Y, Hu C, Huo Y. FPODG: A flexible and private proximity testing based on'one degree' grid. Int'l Journal of Sensor Networks, 2016,20(3):199−207.

[3] Zheng Y, Li M, Lou WJ, Hou T. Location based handshake and private proximity test with location tags. IEEE Trans. on Dependable and Secure Computing, 2017,14(4):406−419.

[4] Faber S, Petrlic R, Tsudik G. Unlinked: Private proximity-based off-line OSN interaction. In: Proc. of the 14th ACM Workshop on Privacy in the Electronic Society. New York: ACM Press, 2015. 121−131.

[5] Kotzanikolaou P, Patsakis C, Magkos E, Michalis K. Lightweight private proximity testing for geospatial social networks. Computer Communications, 2016,73:263−270.

[6] Zhuo G, Jia Q, Guo L, Li M, Fang Y. Privacy-preserving verifiable proximity test for location-based services. In: Proc. of the 2015 IEEE Global Communications Conf. (GLOBECOM). New York: IEEE Press, 2015. 1−6.

[7] Gong X, Chen X, Xing K, Shin D, Zhang M, Zhang J. Personalized location privacy in mobile networks: A social group utility approach. In: Proc. of the 2015 IEEE Conf. on Computer Communications (INFOCOM). New York: IEEE Press, 2015. 1008−1016.

[8] Werner M. Privacy-protected communication for location-based services. Security and Communication Networks, 2016,9(2): 130−138.

[9] Zhong G, Goldberg I, Hengartner U. Louis, Lester and Pierre: Three protocols for location privacy. In: Proc. of the Int'l Workshop on Privacy Enhancing Technologies. Berlin, Heidelberg: Springer-Verlag, 2007. 62−76.

[10] Narayanan A, Thiagarajan N, Lakhani M, Michael H, Boneh D. Location privacy via private proximity testing. In: Proc. of the 18th Annual Network & Distributed System Security Symp. (NDSS 2011). IETF, 2011. 1−17.

[11] Šikšnys L, Thomsen JR, Šaltenis S, Yiu M, Andersen O. A location privacy aware friend locator. In: Proc. of the Int'l Symp. on Spatial and Temporal Databases. Berlin, Heidelberg: Springer-Verlag, 2009. 405−410.

[12] Šikšnys L, Thomsen JR, Šaltenis S, Yiu M. Private and flexible proximity detection in mobile social networks. In: Proc. of the 2010 11th IEEE Int'l Conf. on Mobile Data Management (MDM). New York: IEEE Press, 2010. 75−84.

[13] Mascetti S, Freni D, Bettini C, Wang X, Jajodia S. Privacy in geo-social networks: Proximity notification with untrusted service providers and curious buddies. The VLDB Journal—The Int'l Journal on Very Large Data Bases, 2011,20(4):541−566.

[14] Hallgren P, Ochoa M, Sabelfeld A. Innercircle: A parallelizable decentralized privacy-preserving location proximity protocol. In: Proc. of the 2015 13th IEEE Annual Conf. on Privacy, Security and Trust (PST). New York: IEEE Press, 2015. 1−6.

[15] Patsakis C, Kotzanikolaou P, Bouroche M. Private proximity testing on steroids: An NTRU-based protocol. In: Proc. of the Int'l Workshop on Security and Trust Management. Berlin, Heidelberg: Springer-Verlag, 2015. 172−184.

[16] Halevi T, Ma D, Saxena N, Xiang T. Secure proximity detection for NFC devices based on ambient sensor data. In: Proc. of the European Symp. on Research in Computer Security. Berlin, Heidelberg: Springer-Verlag, 2012. 379–396.

[17] Zhuo G, Jia Q, Guo L, Li M, Fang Y. Privacy-preserving verifiable proximity test for location-based services. In: Proc. of the 2015 IEEE Global Communications Conf. (GLOBECOM). New York: IEEE Press, 2015. 1–6.

[18] Nielsen JD, Pagter JI, Stausholm MB. Location privacy via actively secure private proximity testing. In: Proc. of the 2012 IEEE Int'l Conf. on Pervasive Computing and Communications Workshops (PERCOM Workshops). New York: IEEE Press, 2012. 381–386.

[19] Niu B, Zhang T, Zhu X, Li H, Lu Z. Priority-aware private matching schemes for proximity-based mobile social networks. arXiv preprint arXiv:1401.8064, 2014. https://arxiv.org/pdf/1401.8064

[20] Shrestha B, Saxena N, Truong HTT, Asokan N. Contextual proximity detection in the face of context-manipulating adversaries. arXiv preprint arXiv:1511.00905, 2015. https://arxiv.org/pdf/1511.00905.pdf

[21] Li HP, Hu H, Xu J. Nearby friend alert: Location anonymity in mobile geosocial networks. IEEE Pervasive Computing, 2013,12(4): 62–70.

[22] Paillier P. Public-key cryptosystems based on composite degree residuosity classes. In: Proc. of the Int'l Conf. on the Theory and Applications of Cryptographic Techniques. Berlin, Heidelberg: Springer-Verlag, 1999. 223–238.

[23] ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. on Information Theory, 1985,31(4):469–472.

[24] Thomas T. Secure two-party protocols for point inclusion problem. arXiv preprint arXiv:0705.4185, 2007. https://arxiv.org/pdf/0705.4185.pdf

[25] Yang B, Shao ZY, Zhang WZ. Secure two-party protocols on planar convex hulls. Journal of Information, 2012,9(4):915–929.

[26] Yun Y, Liusheng H, Wei Y, Youwen Y. Efficient protocols for point-convex hull inclusion decision problems. Journal of Networks, 2010,5(5):559–567.

[27] 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]

[28] Katz J, Lindell Y. Introduction to Modern Cryptography. 2nd ed., New York: CRC Press, 2014. 389–398.

[29] Atallah MJ, Du W. Secure multi-party computational geometry. In: Proc. of the Workshop on Algorithms and Data Structures. Berlin, Heidelberg: Springer-Verlag, 2001. 165–179.

附中文参考文献:

[27] 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]

巩林明(1975－),男,山东青岛人,博士,讲师,主要研究领域为公钥密码,安全多方计算.

窦家维(1963－),女,博士,副教授,主要研究领域为公钥密码,应用数学.

李顺东(1963－),男,博士,教授,博士生导师,主要研究领域为公钥密码,安全多方计算.

王道顺(1964－),男,博士,副教授,博士生导师,主要研究领域为密码算法,视频智能行为分析,多媒体安全与取证.