基于同态加密的高效多方保密计算

李顺东[1],王道顺[2]
(1.陕西师范大学计算机科学学院,陕西西安 710062;2.清华大学计算机科学与技术系,北京 100084)

摘 要: 多方保密计算是信息社会隐私保护的核心技术,是国际密码学界的研究热点之一.本文首先提出了一种新的对保密数据进行编码的方案,接着利用这种新的编码方案和同态加密方案,构造了一个百万富翁问题新的解决方案,并证明了方案的安全性.新的方案更简洁、更具有普遍意义,能够对可定义全序关系的任意两个对象进行比较.最后用这个新的解决方案解决了另一个新的多方保密计算问题-两个整数的互素问题,证明了方案是安全的.

关键词: 密码学;同态加密;多方保密计算;百万富翁问题;互素问题
中图分类号: TN918.3 **文献标识码:** A **文章编号:** 0372-2112 (2013)04-0798-06
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2013.04.029

Efficient Secure Multiparty Computation Based on Homomorphic Encryption

LI Shun-dong, WANG Dao-shun
(1. *School of Computer Science, Shaanxi Normal University, Xi'an, Shaanxi* 710062, *China*;
2. *Department of Computer Science and Technology, Tsinghua University, Beijing* 100084, *China*)

Abstract: Secure multiparty computation is a key privacy-preserving technology in cyberspaces and a research focus in the international cryptographic community. We first present a new encoding scheme to encode private data. By using this encoding scheme together with homomorphic encryption scheme, we construct a new scheme for Yao's millionaires' problem and prove its privacy-preserving property. This new scheme is more concise, more general and can be applied to compare any two objects on which a total order can be defined. We finally utilize the new scheme to propose a solution to the coprime problem and prove the privacy-preserving properties of the solution.

Key words: Cryptography; homomorphic encryption; secure multiparty computation; millionaires' problem; coprime problem

1 引言

多方保密计算[1,2]是信息社会隐私保护的核心技术,是国际密码学界近年来的研究热点之一.多方保密计算包括两个或两个以上的参与者,但在学术界统称为多方保密计算,对于两个参与者的保密计算有时也称为双方保密计算.多方保密计算使拥有私有数据的多个参与者能够合作利用这些私有数据进行计算,同时又不泄露各自私有数据的机密,因而使人们能够最大限度利用私有数据而不破坏数据的隐私性.它在私有数据利用、科学计算[3]、电子商务[4]、数据挖掘[5,6]、保密存储[7]、计算外包[8]、密钥分配、入侵检测等方面有着广泛的应用.

Goldwasser[2]曾预言"多方保密计算今天所处的地位就如同公钥密码学10年前所处的地位一样重要,它是计算科学一个极其重要的工具,其实际应用现在才刚刚起步,丰富的理论将使它成为计算科学一个必不可少的组成部分."

Goldreich等[9,10]提出了多方保密计算问题的通用解决方案,并从理论上证明了一般的多方保密计算问题是可解的,引入了多方保密计算协议的安全性定义与模拟范例.但他们指出用他们的通用解决方案解决具体的多方保密计算问题是不实际的,从计算效率角度考虑,对于具体的问题应该研究具体的解决方案[9].他们还证明在半诚实参与者条件下可解的多方保密计算问题,在多数参与者半诚实,其他参与者为恶意参与者的条件下也是可解的.

Goldwasser的预言和Goldreich观察激励人们研究各种多方保密计算问题并提出这些问题的解决方案.已经研究的主要问题有:百万富翁问题[1,11,12],保密的数据挖掘[5,13,14],保密的信息比较[15,16],保密的科学计算[3],保密的远程访问[17],保密拍卖[18],保密的计算几何[19,20]等.文献[2,21]综述了多方保密计算研究与应用,文献[22]介绍了多方保密计算的最新发展.

收稿日期:2012-06-29;修回日期:2012-10-22
基金项目:国家自然科学基金(No.61070189,No.61272435,No.61170032);陕西省科技攻关计划(No.2008K01-58)

在这些已研究的问题中,百万富翁问题是其中最重要的问题之一,其协议已经成为许多多方保密计算协议的基本构成模块.但现有的解决方案都比较复杂而且只适用于自然数的比较.人们一直在努力寻求更简单、适用范围更广的解决方案.本文首先研究这个问题,提出该问题的更为简单、适用范围更广的解决方案,然后用新的解决方案来解决两个整数互素问题的多方保密计算.

本文的贡献如下:(1)提出一种对被比较的机密数据进行编码的新方法;(2)利用新的编码方案和同态加密方案提出了新的、高效的百万富翁问题解决方案并证明了其安全性,该方案更简洁、更具有普遍意义,与文献[23]提出的方案相比,效率更高、适用范围更广,可用于任何具有全序关系的两个对象之间的比较,克服了现有方案只能比较整数的不足;(3)研究了两个整数的互素问题,用百万富翁问题的解决方案解决了这个问题并证明了方案的安全性,方案基于算术基本定理,保密计算过程很容易进行,具有很高的效率.

2　预备知识

2.1　安全性定义

理想保密计算协议　假设有一个可信的第三者(Trusted Third Party,TTP),他在任何情况下都不撒谎,决不会泄露不该泄露的信息.借助于 TTP 双方保密计算可以这样实施:Alice 将 x 告诉 TTP,Bob 将 y 告诉 TTP;TTP 自己计算 $f(x,y)$,然后将结果分别告诉 Alice 和 Bob.因为 Alice 和 Bob 没有办法从协议中得到除 $f(x,y)$之外的额外信息,这样一个简单的协议是安全性最高的双方保密计算协议,任何一个计算 $f(x,y)$的实际双方保密计算协议的安全性都不可能超过这个协议.

半诚实参与者　不严格地说,一个半诚实参与者在执行协议的过程中会忠实地履行协议,但他可能会保留所有中间结果,试图从中间结果推导出协议之外的信息.

设 $f=(f_1,f_2):\{0,1\}^*\times\{0,1\}^*\to\{0,1\}^*\times\{0,1\}^*$是一个概率多项式函数,$\pi$ 是计算函数 f 的双方协议.协议的输入为(x,y),执行协议 π 时第一个参与者 Alice 的 view 记作 $\text{view}_1^\pi(x,y)=(x,r^1,m_1^1,\cdots,m_t^1)$,其中 r^1 是 Alice 自己产生的随机数,m_i^1 是她收到的第 i 个消息,Alice 的输出记作 $\text{output}_1^\pi(x,y)$.第二个参与者 Bob 的 $\text{view}_2^\pi(x,y)$和输出 $\text{output}_2^\pi(x,y)$可以类似地定义.

定义 1[10]　对于 f,我们说 π 保密地计算 $f(x,y)$如果存在概率多项式时间算法 S_1 与 S_2 使得

$$\{(S_1(x,f_1(x,y)),f_2(x,y))\}_{x,y}\overset{c}{\equiv}\{(view_1^\pi(x,y),output_2^\pi(x,y))\}_{x,y},\quad(1)$$

$$\{(f_1(x,y),S_2(y,f_2(x,y)))\}_{x,y}\overset{c}{\equiv}\{(output_1^\pi(x,y),view_2^\pi(x,y))\}_{x,y},\quad(2)$$

成立.其中$\overset{c}{\equiv}$表示计算上不可区分,S_1,S_2 称为模拟器.

Goldreich 利用比特承诺和零知识证明理论设计了一个编译器,给定一个在半诚实参与者条件下保密计算 f 的协议 π,这个编译器可以自动生成一个在恶意参与者条件下也能保密计算 f 的协议,这个新的协议可以迫使一个恶意的参与者以半诚实方式参与协议的执行,否则就会被发现.因此,很多时候只需要研究半诚实参与者条件下的多方保密计算协议即可.本文假设协议的参与者都是半诚实的.

2.2　同态加密

同态加密的概念是文献[24]提出的.同态加密的特殊的性质使我们可以直接对密文进行某些运算来代替对明文的运算取得同样的效果,这样不影响明文数据的机密性.同态加密方法在云计算和多方保密计算中都将发挥重要的作用.同态加密的一个例子如图 1 所示[25].

图中 $N=pq$,p 和 q 是两个大素数.$\lambda(N)=1\text{cm}(p-1,q-1)$是 $p-1$ 和 $q-1$ 的最小公倍数.

加密过程	
	明文:$m<N$, 选择一个随机数$r<N$,
	密文:$c=g^m r^N \bmod N^2$.
解密过程	
	密文:$c<N^2$,
	明文:$m=\dfrac{L(c^\lambda \bmod N^2)}{L(g^\lambda \bmod N^2)} \bmod N$.

图1　Paillier同态加密算法

$B=\{x\mid x^{N\mu}\bmod N^2=1,\mu\in\{1,2,\cdots,\lambda\}\}$. $S_N=\{u<N^2\mid u\equiv 1\bmod N\}$.对于任意的 $u\in S_N$,定义 $L(u)$为$L(u)=\dfrac{u-1}{N}$.假设 $g\in B$,N 是公开参数,g 是公钥,(p,q)是私钥.这是一个加法同态加密算法,该算法具有下述性质:

$$E(x+y)=E(x)\cdot E(y),E(x\cdot y)=(E(x))^y.\quad(3)$$

这个性质使得仅知道 y,$E(x)$和公钥的 Bob 能够通过计算 $E(x+y)=E(x)\cdot E(y),E(x\cdot y)=(E(x))^y$ 完成对 $E(x+y)$和 $E(x\cdot y)$的计算而不需要知道 x.这是一种语义安全的概率加密算法,在这种语义安全的加密算法之下,0 的密文和 1 的密文是计算上不可区分的,即 $E(0)\overset{c}{\equiv}E(1)$.

3　问题与解决方案

3.1　百万富翁问题

百万富翁问题　百万富翁问题是说两个百万富翁想知道他们两个谁的财富多,但都不想泄露自己的财

富数据.在数学上可以抽象为 Alice 拥有数据 x,Bob 拥有数据 y,他们两个希望知道 x,y 哪个大,而不愿意泄漏 x 和 y.

这个问题是多方保密计算中最重要的问题之一,其协议是构造其他多方保密计算协议的基本模块.Yao 提出的第一个解决方案[1]的时间复杂度与空间复杂度都很高.后来,Yao[11]、Goldreich[9]等应用爬行电路(scrambled circuits)技术解决了一般的多方保密计算问题.基于爬行电路的多方保密计算协议具有重要的理论意义,但实际意义非常有限,因为即使一个非常简单的函数或者计算程序要转换成爬行电路都是非常困难的,而且在转换为爬行电路之后的计算中也需要多次调用不经意传输,每次的不经意传输都需要若干基于公钥的计算,如果考虑到转换过程和计算过程的计算复杂度与不经意传输过程的通信复杂度,用这种方法解决百万富翁问题是不实际的.另外的一些协议[12,26~28]通过直接分析问题的特征解决问题,主要致力于提高协议的效率,没有考虑算法的简洁和通用性.文献[27]将百万富翁问题归约到集合包含问题并提出了一个高效的解决方案.文献[23]将自然数编码成一个集合而把比较两个数大小的问题此归约到集合的相交问题并利用 ElGamal 同态加密算法解决了这个问题,这是一个很有创意的协议.

本文首先将保密的数据编码成一个向量,在加法同态加密算法基础上设计一个简洁、高效而且通用的解决方案,将两个数的保密比较问题归约到向量的部分标量积(scalar product)的保密计算问题.该方案很容易实施,具有实际意义.接着又通过将保密判断两个数互素问题归约到向量的标量积的保密计算来解决两个数互素问题.

对保密数据的编码 不失一般性,假设 $x,y\in\{z_1,z_2,\cdots,z_m\}=U$,其中 $z_1<z_2<\cdots<z_m$.进一步假设 $x=z_k,y=z_l$,$(1\leqslant k,l\leqslant m)$,那么 $x\leqslant y$ 当且仅当 $k\leqslant l$.解决方案基于下面的观察:

根据 x,y 和 U,构造两个新的向量 $A=(a_1,a_2,\cdots,a_m),B=(b_1,b_2,\cdots,b_m)$其中 $a_i=(i\geqslant k)$,即 $a_1=a_2=\cdots=a_{k-1}=0,a_k=a_{k+1}=\cdots=a_m=1$;类似地 $b_j=(j\geqslant l)$.如果 $x\leqslant y$,那么 $k\leqslant l,b_1=b_2=\cdots=b_{l-1}=0,a_l=b_l=1$ 则

$$v=\sum_{i=1}^{l}a_ib_i=\sum_{i=1}^{k-1}a_ib_i+\sum_{i=k}^{l-1}a_ib_i+a_lb_l=1;$$

反之如果 $x>y$,那么 $k>l,a_1=a_2=\cdots=a_l=0,b_1=b_2=\cdots=b_l=0$ 则

$$v=\sum_{i=1}^{l}a_ib_i=\sum_{i=1}^{l}0\cdot0=0;$$

因此保密判定是否 $x\leqslant y$ 可以归约到保密计算 $\sum_{i=1}^{l}a_ib_i$.用加法同态加密算法[25]可以完成这项任务.Alice 用自己的公钥加密 $a_1,\cdots,a_m$ 得到 $E(a_1),\cdots,E(a_m)$并发送给 Bob,Bob 利用同态加密的性质计算

$$E(v)=\prod_{i=1}^{l}(E(a_i))^{b_i}\bmod N^2$$

得到 $E(v)$并发送给 Alice.Alice 用私钥解密得到 v 值.为便于论述,定义 $P(x,y)$如下:如果 $x\leqslant y$,$P(x,y)=1$;否则 $P(x,y)=0$.在此基础上给出百万富翁问题的解决方案如下.

协议 1 百万富翁问题的解决方案

输入: Alice 的机密数为 x,Bob 的机密数为 y,设 $x,y\in\{z_1,z_2,\cdots,z_m\}$.

输出: $P(x,y)$.

1. 假设 $x=z_k,y=z_l$,Alice 和 Bob 分别构造两个向量 $A=(a_1,a_2,\cdots,a_m),B=(b_1,b_2,\cdots,b_m)$.其中 $a_i=(i\geqslant k),b_j=(j\geqslant l)$.
2. 假设(G,E,D)是 Paillier 同态加密方案,τ 是设定的安全参数.Alice 运行 $G(\tau)$生成同态加密方案的公钥和私钥,用公钥加密向量 A 得到
$$E(A)=(E(a_1),E(a_2),\cdots,E(a_m)),$$
2. 将 $E(A)$与公钥一起发送给 Bob.
3. Bob 选择一个随机数 r,计算
$$E(v)=(r^N\prod_{i=1}^{l}(E(a_i))^{b_i})\bmod N^2=E(\sum_{i=1}^{l}a_ib_i)$$
4. 并把结果告诉 Alice.
5. Alice 用私钥解密 $E(v)$得到 v 并告诉 Bob.

3.2 分析

如果 $x\leqslant y$,那么 $k\leqslant l,b_1=\cdots=b_{l-1}=0$

$$E(v)=\sum_{i=1}^{l}a_ib_i=\sum_{i=1}^{l-1}a_ib_i+a_lb_l=1,$$

因而该方案能够正确地解决百万富翁问题.该协议中 r^N 对于保护 l 的机密性起关键作用,如果没有 r^N,则

$$E(v)=\prod_{i=1}^{l}(E(a_i))^{b_i}=(E(a_l))^1\prod_{i=1}^{l-1}(E(a_i))^0,$$

这个值其实就是 $E(a_l)$,这样就会泄露 l,进而泄露 y,而乘以 r^N 就避免了这样的事情发生,且不影响正确解密.

安全性 协议 1 的安全性以同态加密方案的安全性为基础.Paillier 同态加密算法是语义安全的[29].应用模拟范例,可以证明协议 1 是安全的.

定理 1 协议 1 保密地计算百万富翁问题.

证明 通过构造满足(1)和(2)模拟器 S_1,S_2 来证明本定理.S_1 工作过程如下:

(1)给定输入$(x,P(x,y))$,S_1 随机选择一个 $y'\in\{z_1,z_2,\cdots,z_m\}$使得 $P(x,y')=P(x,y)$,用 x,y' 进行模拟.首先按照协议构造向量 $A=(a_1,a_2,\cdots,a_m)$与 $B'=$

$(b'_1, b'_2, \cdots, b'_m)$.

(2)加密 A 得到

$E(A) = (E(a_1), E(a_2), \cdots, E(a_m))$.

(3)选择一个随机数 r',计算

$$E(v') = (r')^N \prod_{i=1}^{l} (E(a_i))^{b'_i} \bmod N^2 = E(\sum_{i=1}^{l} a_i b'_i)$$

(4)解密 $E(v')$得到 v'.

在本协议中 $view_1(x, y) = \{A, E(A), E(v), v(= P(x, y))\}$.令 $S_1(x, P(x, y)) = \{A, E(A), E(v'), v'(= P(x, y'))\}$.因为 $P(x, y) = P(x, y')$,根据 v 的计算方法可知 $v = v'$, $E(v)_{x,y} \overset{c}{\equiv} E(v')$.所以 $\{(S_1(x, P(x, y)), P(x, y))\}_{x,y} \overset{c}{\equiv} \{(view_1^{\pi}(x, y), output_2^{\pi}(x, y))\}_{x,y}$,使 $\{(P(x, y), S_2(y, P(x, y)))\}_{x,y} \overset{c}{\equiv} \{(output_1^{\pi}(x, y), view_2^{\pi}(x, y))\}_{x,y}$成立的 S_2 可以用类似的方法构造.证毕.

方案的效率　这里将我们的方案(协议 1)和文献[23]的基于 ElGamal 乘法同态加密算法的解决方案(记作 LT 方案做一个比较.两个方案都基于同态加密算法,基本运算都是模指数运算.忽略方案中的随机数选择开销和准备阶段的计算开销,LT 方案的模为 p,本方案的模为 N^2,为便于比较统一模为 p,机密数据的长度为 n.

设 $x, y \in U, |U| = m$.协议 1 中 Alice 需要进行 $m+1$ 次模指数运算(加密 m 次,解密 1 次),因为 $(r^N \prod_{i=1}^{l} (E(a_i))^{b_i}) \bmod N^2 = r^N (E(a_l))^{b_l} \bmod N^2$, Bob 只需要计算一次模指数.总的模指数运算次数为 $m+2$.这个计算开销与 n 无关.LT 协议需要 $5n\log p + 4n - 6$ 次模指数运算,在所有的公钥加密算法中 $p >> n$(在实际应用中 $p \simeq 2^{1024}, n < 2^{32}$),所以计算复杂度为 $O(n)$,但是包含一个很大的常数.如果 m 与 n 相当,协议 1 的计算复杂度远低于 LT 协议的计算复杂度,如果 $m \sim 5n\log p$,则计算复杂度差不多.

通信复杂度　衡量通信复杂度的指标用协议交换信息的比特数,或者用通信轮数,在多方保密计算研究中通常用轮数.以通信轮数来衡量,两个方案的通信复杂度相同.用交换比特数衡量的话,协议 1 比 LT 协议为好.比较结果可以概括为表 1.

表 1　计算复杂性与通信复杂性(以轮数为基准)比较

	协议 1	LT 协议
Alice 计算开销	$m+1$	$3n\log p$
Bob 计算开销	1	$2n\log p + 4n - 6$
总开销	$m+2$	$5n\log p + 4n - 6$
通信复杂性	3	3

通用性比较　现有的所有解决方案只适用于自然数的比较,如果 x, y 是实数,现有的方案都无法使用.协议 1 适用于全序集的任何子集上任意两个对象的比较.如自然数集、整数集、有理数集、实数集、按字典序排成的字符串集,只要按照全序进行排序,并给出被比较的对象所在的子集范围,就可以利用协议 1 进行比较,对于大范围的数可以利用分治思想分段进行比较,因而适用范围更广,更具有普遍意义.仅就比较两个自然数来看,如果 m 比较小,而 $n\log p$ 比较大($m << 5n\log p$),比如 x, y 是某个企业中代表职工姓名的两个字符串,协议 1 有明显的优势;而如果 n, m 都是较小的自然数比如 $x, y < 100$,则两方案性能差不多.此外,LT 协议可能以小概率给出错误的结果,而协议 1 不会出错.

3.3　互素问题

互素问题　Alice 有整数 x, Bob 有整数 y.他们想知道 $gcd(x, y)$是否为 1,而不想泄露 x, y.互素问题是密码学一个非常重要的问题,因为密码学很多应用都需要选择一些具有互素关系的数.

根据算数基本定理, x, y 可以表示成

$x = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}, y = p_1^{f_1} p_2^{f_2} \cdots p_m^{f_m} (e_i, f_i \geqslant 0)$,

其中 p_i 表示第 i 个素数,即 $p_1 = 2, p_2 = 3, \cdots$.令 $[p] = \{p_1, p_2, \cdots, p_m\}$.解决该问题基于下面的观察.

利用 x, y 和 $[p]$构造向量 $A = (a_1, a_2, \cdots, a_m)$和向量 $B = (b_1, b_2, \cdots, b_m)$, $a_i = (e_i > 0)$, $b_i = (f_i > 0)$.设 $m = 20$, A, B 看上去如下:

$A = (1,0,0,1,0,0,1,0,1,0,1,0,1,0,1,1,0,1,1,0)$.

如果 x, y 有公因子 $p_i (1 \leqslant i \leqslant m)$,那么 $a_i = b_i = 1$,因而 $a_i b_i = 1$.若 x, y 无公因子,一定有 $(\forall i)\ a_i b_i = 0$.所以 $gcd(x, y) = 1 \Leftrightarrow v = \sum_{i=1}^{m} a_i b_i = 0$.因此保密确定 x, y 是否互素的问题可以归约到保密地计算两个向量的标量积 v 的问题.

协议 2　互素问题的多方保密计算协议

输入　Alice, Bob 的机密数 x, y,公共的集合 $[p] = \{p_1, p_2, \cdots, p_m\}$

输出　x, y 是否互素

1. Alice, Bob 构造 $A = (a_1, a_2, \cdots, a_m)$, $B = (b_1, b_2, \cdots, b_m)$,其中 $a_i = (e_i > 0)$, $b_i = (f_i > 0)$.
2. Alice 运行 (G, E, D)的算法 G 生成同态加密算法的公钥、私钥并用公钥加密 A,得到
$$E(A) = (E(a_1), E(a_2), \cdots, E(a_m))$$
然后发给 Bob.
3. Bob 选择随机数 r, s_i,然后计算
$$E(v) = (r^N \prod_{i=1}^{m} (E(a_i))^{b_i s_i}) \bmod N^2 = E(\sum_{i=1}^{m} s_i a_i b_i)$$
然后把计算结果发回给 Alice.
4. Alice 用自己的私钥解密 $E(v)$,得到 v.如果 $v = 0, gcd(x, y) = 1, x, y$ 互素,否则不互素.Alice 将结果告诉 Bob.

因为本方案采用的同态加密方案是语义安全的[29],应用证明定理 1 所用的方法很容易证明下面的

推论,这里省略证明过程.

推论 1 互素问题的多方协议 2 能够保密计算互素问题.

4 结论

百万富翁问题协议是许多多方保密计算协议的基本组成部分,它已经有一些解决方案,但都不够简洁,适用范围有限,不具有普遍意义.本文提出一个基于输入编码和同态加密的非常简洁、高效的协议并证明了协议的保密性,协议的适用范围几乎没有限制,只是在某些情况下效率会比较低.最后用这个新的百万富翁问题协议作为构造模块,设计一个协议解决了两个数互素问题,并证明解决方案的安全性.该方案适合规模适当的数,当两个数都非常大时如何判断,还有待进一步的研究.

参考文献

[1] A C Yao. Protocols for secure computations [A]. Proceedings of the 23th IEEE Symposium on Foundations of Computer Science [C]. Piscataway: IEEE Press, 1982. 160 – 164.

[2] S Goldwasser. Multi-party computations: Past and present [A]. Proceedings of the 16th Annual ACM Symposium on Principles of Distributed Computing [C]. NY: ACM Press, 1997. 1 – 6.

[3] W L Du, M J Atallah. Privacy-preserving cooperative scientific computations [A]. Proceedings of 14th IEEE Computer Security Foundations Workshop Lecture [C]. Piscataway: IEEE Press, 2001. 273 – 282.

[4] S G Choi, K W Hwangy, J Katz, et al. Secure multi-party computation of boolean circuits with applications to privacy in online marketplaces [A]. Lecture Notes in Computer Science 7178 [C]. NY: Springer, 2012. 416 – 432.

[5] R Agrawal, R Srikant. Privacy-preserving data mining [A]. Proceedings of ACM International Conference on Management of Data and Symposium on Principles of Database Systems [C]. NY: ACM Press, 2000. 439 – 450.

[6] 杨高明,杨静,张健沛.聚类的(α,k)-匿名数据发布[J].电子学报,2011,39(8):1941 – 1946.
YANG Gao-ming, YANG Jing, ZHANG Jian-pei. Achieving (α,k)- anonymity via clustering in data publishing [J]. Acta Electronica Sinica, 2011, 39(8): 1941 – 1946. (in Chinese)

[7] T Toft. Secure data structures based on multi-party computation [A]. Proceedings of the 30th Annual ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing [C]. NY: ACM Press, 2011. 291 – 292.

[8] J Loftus, N P Smart. Secure outsourced computation [A]. Lecture Notes in Computer Science 6737 [C]. NY: Springer, 2010. 1 – 20.

[9] O Goldreich, S Micali, A Wigderson. How to play any mental game [A]. Proceedings of the Nineteenth Annual ACM Conference on Theory of Computing [C]. Piscataway: IEEE Press, 1987. 218 – 229.

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

[11] A C Yao. How to generate and exchange secrets [A]. Proceedings of 27th Annual Symposium on Foundations of Computer Science [C]. Piscataway: IEEE Press, 1986. 162 – 167.

[12] I Ioannidis, A Grama. An efficient protocol for yao's millionaires' problem [A]. Proceedings of the 36th Hawaii International Conference on System Science [C]. Piscataway: IEEE Press, 2003. 1 – 6.

[13] C Clifton, D Marks. Security and privacy implications of data mining [A]. Proceedings of the ACM SIGMOD Workshop on Research Issues on Data Mining and Knowledge Discovery [C]. NY: ACM Press, 1996. 15 – 19.

[14] 王波,杨静.一种基于逆聚类的个性化隐私匿名方法[J].电子学报,2012,40(5):883 – 890.
WANG Bo, YANG Jing. A personalized privacy anonymous method based on inverse clustering [J]. Acta Electronica Sinica, 2012, 40(5): 883 – 890. (in Chinese)

[15] Fagin R, Naor M, Winklery P. Comparing information without leaking it [J]. Communications of the ACM, 1996, 39(5): 77 – 85.

[16] 刘文,王永滨.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 Wen, WANG Yong-bin. Secure multi-party comparing protocol and its applications [J]. Acta Electronica Sinica, 2012, 40(5): 871 – 876. (in Chinese)

[17] W L Du, M J Atallah. Protocols for secure remote database access with approximate matching [A]. Advance of E-Commerce and Privacy [C]. NY: Springer, 2001. 87111.

[18] C Cachin. Efficient private bidding and auctions with an oblivious third party [A]. Proceedings of the 6th ACM Conference on Computer and Communications Security [C]. NY: ACM Press, 1999. 120 – 127.

[19] M J Atallah, W L Du. Secure multi-party computational geometry [A]. Lecture Notes in Computer Science 2125 [C]. NY: Springer, 2001. 165 – 179.

[20] Li S D, Dai Y Q. Secure two-party computational geometry [J]. Journal of Computer Science and Technology, 2005, 20(2): 258 – 263.

[21] W L Du, M J Atallah. Secure multi-party computation problems and their applications: A review and open problems [A]. Proceedings of New Security Paradigms Workshop 2001 [C]. NY: ACM Press, 2001. 11 – 20.

[22] Sheikha R, Mishra D K, Kumar B. Secure multiparty computation: From millionaires problem to anonymizer [J]. Information Security Journal: A Global Perspective, 2011, 20(1): 25 –

33.

[23] H Y Lin, W G Tzeng. An efficient solution to the millionaires' problem based on homomorphic encryption [A]. Proceedings of Applied Cryptography and Network Security 2005 (LNCS3531)[C]. NY: Springer, 2005. 456 – 466.

[24] R Rivest, L Adleman, M Dertouzos. On data banks and privacy homomorphisms [A]. Foundations of Secure Computation [C]. Liverpool: Academic Press, 1978. 169 – 177.

[25] P Paillier. Public-key cryptosystems based on composite degree residuosity classes [A]. Lecture Notes in Computer Science 1592 [C]. NY: Springer, 1999. 223 – 238.

[26] M Fischlin. A cost-effective pay-per-multiplication comparison method for millionaires[A]. Proceedings of the 2001 Conference on Topics in Cryptology: The Cryptographer's Track at RSA (LNCS2020)[C]. NY: Springer, 2001. 457 – 472.

[27] 李顺东,戴一奇,尤启友.姚氏百万富翁问题的高效解决方案[J].电子学报,2005,2005,33 (5):770 – 773.
LI Shun-dong, DAI Yi-qi, YOU Qi-you. An efficient solution to yao's millionaires' problem [J]. Acta Electronica Sinica, 2005, 33(5): 770 – 773. (in Chinese)

[28] Li S D, Wang D S, Dai Y Q, et al. Symmetric cryptographic solution to yao's millionaires' problem and an evaluation of secure multiparty computations [J]. Information Sciences, 2008, 178(2): 244 – 255.

[29] C Gentry. A fully homomorphic encryption scheme (PhD thesis)[OL]. http://crypto.stanford.edu/craig/ (2009)

作者简介

李顺东　男,1963 年 12 月生,河南平顶山人.1984、1987 年在西安工程大学获工学学士、硕士学位;2003 年在西安交通大学获计算机科学与技术工学博士学位.现为陕西师范大学计算机科学学院教授、博士生导师.主要从事密码学与信息安全研究.

E-mail: shundong@snnu.edu.cn

王道顺　男,1964 年 12 月生,四川苍山人.1987 年获兰州大学数学学士学位,2001 年获四川大学数学博士学位.现为清华大学计算机科学与技术系副教授,博士生导师.主要研究兴趣为密钥管理、数字水印与多媒体安全.

E-mail: daoshun@tsinghua.edu.cn