姚氏百万富翁问题的高效解决方案

李顺东,戴一奇,游启友
(清华大学计算机科学与技术系,北京 100084)

摘 要: 姚氏百万富翁问题解决方案已经成为许多多方保密计算问题解决方案的一个基本模块,但现有的解决方案效率低下,因而影响到其他多方保密计算方案的效率. 本文利用长度函数与不经意传输设计了一个高效的解决方案,新方案同原有方案相比,计算复杂性明显降低.

关键词: 百万富翁问题; 多方保密计算; 不经意传输; 计算复杂性
中图分类号: TN918.2 **文献标识码**: A **文章编号**: 0372-2112 (2005) 05-0769-05

An Efficient Solution to Yao's Millionaires' Problem

LI Shun-dong, DAI Yi-qi, YOU Qi-you
(*Department of Computer Science and Technology, Tsinghua University, Beijing* 100084, *China*)

Abstract: The protocols for Yao's Millionaires' problem have been building blocks of solutions to many secure multi-party computation problems. But known solutions are not efficient enough and thus affect the efficiency of many secure multi-party computation protocols. In this paper, we construct a new efficient solution to millionaires' problem based on length function and oblivious transfer. Compared with known solutions, our new solution has much less computational complexity.

Key words: millionaires' problem; secure multi-party computation; oblivious transfer; computational complexity

1 引言

姚氏百万富翁问题首先由华裔计算机科学家、图灵奖获得者姚启智教授提出[1]. 在文献[1]中,姚提出了这样一个问题:两个百万富翁 Alice 和 Bob 想知道他们两个谁更富有,但他们都不想让对方知道自己财富的任何信息,这就是百万富翁问题. 文献[2]给出了这个问题的一些实际应用,假设 Alice 希望向 Bob 购买一些商品,但她愿意支付的最高金额为 x 元; Bob 希望的最低卖出价为 y 元. Alice 与 Bob 都非常希望知道 x 与 y 那个大,如果 $x > y$,他们就可以开始讨价还价;如果 $x < y$,他们就不用浪费口舌. 但他们都不想告诉对方自己的出价,以免自己在讨价还价中处于不利地位.

姚氏百万富翁问题经过 O Goldreich, Micali and Wigderson[3]等人的发展,已经成为现代密码学中一个非常活跃的研究领域,即多方保密计算. 在多方保密计算中,多个计算参与者希望进行一个基于他们各自提供的私有输入的计算,同时能够保证他们各自输入的保密性. S Goldwasser[5]预言:"多方保密计算今天所处的地位正是公开密钥密码学 10 年前所处的地位. 是密码学研究中一个极端重要的工具,它在计算科学中的应用才刚刚开始,丰富的理论将使它成为计算科学中一个必不可少的组成部分."

S Goldwasser 的预言激发许多研究人员从事多方保密计算研究,并取得了许多重要的研究成果. 一般的多方计算问题在理论上已经得到解决[1,3,4],但是理论解决方案可能因为效率或计算量的问题而实际上并不可解. 实际上的可解性要求能够给出问题的多项式时间的算法,理论解决方案并没有给出这样的多项式时间算法. 因此 O. Goldreich 指出[4]:理论上证明多方保密计算问题的可解并不表示不再需要对这些问题进行研究,相反,应用这类没有任何具体信息的一般条件下导出的解决方案来解决具体的多方保密计算问题可能是不实际的;基于效率的原因,对于具体的问题需要研究具体的解决方案. 具体问题中给出的信息可能使得解决方案的效率大大提高.

百万富翁问题解决方案已经成为许多多方保密计算问题解决方案的一个基本模块,但是由于百万富翁问题解决方案的效率很低,因而也影响到许多多方保密计算问题解决方案的效率. 本文利用一种特殊设计的函数与 OT_m^1 不经意传输提出了一种高效的解决方案,本文的主要贡献如下:

(1) 首先构造了一个函数,该函数能够将差别比较大的两个数的比较转化为他们的函数值的比较,这种比较比直接比较两个数要容易得多.

(2) 基于不经意传输与前述的特殊函数,设计了一个比较任意两个数的协议,这个协议使得任意两个数的比较成为现实.

本文在第二部分介绍了有关的工作;第三部分给出了安全性定义并构造了一个特别的函数;第四部分提出了利用不经意传输保密比较两个数大小的方案并证明了这两种方案对半诚实参与者是安全的,这种方案又被用来构造任意两个数的比较方案;第五部分分析了方案的计算复杂性与恶意攻击者存在下的安全性;第六部分给出了结论.

收稿日期:2004-06-15;修回日期:2004-08-20
基金项目:国家自然科学基金重大项目(No. 90304014);中国博士后科学基金(No. 2004036248)

2 有关工作

2.1 方案 0:百万富翁问题解决方案[1]

这个方案用于对两个数进行比较,以确定哪一个较大. Alice 知道一个整数 i;Bob 知道一个整数 j. Alice 与 Bob 希望知道究竟是 $i \leq j$ 还是 $i > j$,但都不想让对方知道自己的数. 为简单起见,假设 i 与 j 的范围为 $[1,100]$. Bob 有一个公开密钥 E_B 与私有密钥 D_B.

(1) Alice 选择一个大随机数 x,并用 Bob 的公开密钥加密

$$c = E_B(x) \tag{1}$$

(2) Alice 计算 $c - i$,并将结果发送给 Bob.

(3) Bob 计算下面的 100 个数:

$$y_u = D_B(c - i + u),\ u = 1,2,\cdots,100 \tag{2}$$

其中 D_B 是 Bob 的私有解密密钥. Bob 选择一个大的素数 p(p 应该比 x 稍小一点,Bob 不知道 x,但 Alice 能容易地告诉他 x 的大小.) 然后计算下面的 100 个数:

$$Z_u = (y_u \bmod p),\quad u = 1,2,\cdots,100 \tag{3}$$

然后验证对于所有的 $u \neq v$

$$|z_u - z_v| \geq 2 \tag{4}$$

并对所有的 u 验证:

$$0 < z_u < p - 1 \tag{5}$$

如果不成立,Bob 就选择另一个素数并重复验证.

(4) Bob 将以下数列发送给 Alice:

$$z_1, z_2, \cdots, z_j, z_{j+1} + 1, z_{j+2} + 1, \cdots, z_{100} + 1, p$$

(5) Alice 验证这个数列的第 i 个数是否与 x 模 p 同余. 如果同余,她得出的结论是 $i \leq j$;如果不同余,它得出的结论是 $i > j$.

(6) Alice 把这个结论告诉 Bob.

假设该方案需要比较的两个数的长度(十进制表示的位数)为 n,数的范围就是 10^n,是输入规模的指数. 比如在上述例子中两个数的长度为 2,则数的范围就是 100,式(2)中要解密的次数、式(3)中模运算的次数、式(5)中要验证的次数都是 10^n,式(4)中要验证的次数为 $10^{2n}/2$. 因此计算复杂性为输入规模的指数函数. 如果输入规模为 50,那么计算复杂性为 $O(10^{50})$,这样的计算复杂性,实际上是不可能实现的. 因此这个方案对于比较两个较大的数是不实用的.

2.2 OT^1_m 不经意传输[10]

文献[10]首先提出了不经意传输的概念,文[10]中的不经意传输实际是 OT^1_2. OT^1_m 不经意传输是 OT^1_2 不经意传输的发展,是一个重要的密码学协议,这个协议能够完成下面的任务:Alice 有 m 个消息(或者数据) $\{X_1, X_2, \cdots, X_m\}$,通过执行 OT^1_m 不经意传输协议,Bob 能够基于自己的选择得到且只能得到其中的一个消息 $X_i (1 \leq i \leq m)$,而对其他消息 $\{X_1, X_2, \cdots, X_{i-1}, X_{i+1}, \cdots, X_m\}$ 则一无所知. Alice 对 Bob 选择了哪一个消息也一无所知. 文[11]和[12]提出了两个有效的 OT^1_m 不经意传输协议.

设 q 为一素数,$p = 2q + 1$ 也是一个素数. G_q 为一阶 q 群,g,h 为 G_q 的两个生成元,Z_q 表示自然数模 q 的最小剩余集,(g, h, G_q) 为双方共知,Alice 有 m 个消息:$M_1, M_2, \cdots, M_m$,Bob 希望得到其中的一个,Alice 不知道 Bob 得到了哪一个. 协议如下:

(1) Bob 选择一个希望的 $\alpha (1 \leq \alpha \leq m)$ 与一个随机数 $r \in Z_q$,计算 $y = g^r h^\alpha \bmod p$ 并将 y 发给 Alice.

(2) Alice 计算下列 m 个二元组的序列 $C = \{(a_1, b_1), (a_2, b_2), \cdots, (a_m, b_m)\}$ 其中

$$a_i = g^{k_i} \bmod p,\ b_i = M_i (y / h^i)^{k_i} \bmod p,\ k_i \in Z_q,\ 1 \leq i \leq m \tag{6}$$

并将序列 C 发给 Bob.

(3) 根据 $c_\alpha = (a_\alpha, b_\alpha)$,Bob 计算 $M_\alpha = (b_\alpha / (a_\alpha)^r) \bmod p$.

完成这个协议,Bob 就可以得到他希望得到的 M_α,而 Alice 对 α 则一无所知.

3 预备知识

3.1 安全性定义

半诚实参与者 本文方案的安全性均假设多方保密计算的参与者为半诚实的参与者. 简单地说,所谓半诚实参与者是指参与者在协议执行过程中将不折不扣地执行协议,但他们也会保留计算的中间结果试图推导出其他参与者的输入.

双方计算 一个双方计算是一个随机计算过程,它将随机输入对映射为输出对. 这样的过程称为一个函数,并记为 $f: \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^* \times \{0,1\}^*$,其中 $f = (f_1, f_2)$,意即对于每一对输入 (x, y),输出对是一个变化范围为一对字符串的随机变量 $(f_1(x, y), f_2(x, y))$ 并记这样的函数为 $f: (x, y) \to (f_1(x, y), f_2(x, y))$.

隐私的模拟范例 直观上,如果对于任一个半诚实的参与者,他都可以直接从执行协议时自己的输入与协议的输出,通过单独模拟协议的执行过程而得到在执行协议过程中他所能得到的任何信息,那么协议就是保密的. 即能够保证输入的隐私性. 简单地说,保密计算协议要求协议执行过程中参与者所观察到的内容仅用他自己的输入与输出就可以进行模拟. 这就是多方保密计算保密性研究中常用的模拟范例. 如果一个多方计算协议能够这样进行模拟,参与者就不能从协议的执行过程中得到任何有价值的信息,这样的多方计算过程就是保密的.

一些记号 首先引入以下记号,假设双方计算的参加方分别为 Alice 和 Bob.

- 设 $f = (f_1, f_2)$ 是一个概率多项式时间函数,π 表示计算 f 的双方计算协议.
- 当输入为 (x, y) 时,Alice (Bob) 在执行协议 π 的过程中所得到的信息序列记为 $(view_1^\pi(x, y)\ (view_2^\pi(x, y))$ 是 $(x, r^1, m_1^1, m_2^1, \cdots, m_t^1)\ ((y, r^2, m_1^2, m_2^2, \cdots, m_t^2))$,其中 $r^1\ (r^2)$ 表示 Alice (Bob) 独立的硬币抛掷结果;$m_i^1\ (m_i^2)$ 表示 Alice (Bob) 第 i 次收到的信息.
- 输入为 (x, y) 时,执行协议 π 以后,Alice (Bob) 的输出结果记为 $ouput_1^\pi(x, y)\ (output_2^\pi(x, y))$.

定义 1 (半诚实参与者的保密性[4,8]):对于一个函数 f,如果存在概率多项式时间算法 S_1 与 S_2(有时称这样的多项式时间算法为模拟器)使得

$$\{(S_1(x, f_1(x, y)), f_2(x, y))\}_{x,y}$$

$$\equiv\{(view_1^{\pi}(x,y), output_2^{\pi}(x,y))\}_{x,y} \quad (7)$$

$$\{(f_1(x,y), S_2(y, f_2(x,y)))\}_{x,y} \equiv\{(output_1^{\pi}(x,y), view_2^{\pi}(x,y))\}_{x,y} \quad (8)$$

其中 $\equiv$ 表示计算上不可区分,则认为 π 保密地计算 f.

要证明一个多方计算方案是保密的,就必须构造满足(7)和(8)的模拟器 S_1 与 S_2.

3.2 函数 F

本小节构造一个函数 $F:\{0,1\}^* \to \{0,1\}^*$,这个函数使我们能够在某些情况下将两个数的比较转换成它们相应的函数值的比较,这样的转换应该大大简化两个数的比较. 为此目的,希望函数 F 具有下面的特性.

● 容易计算:存在多项式时间算法 A,使得对于任意 $x \in \{0,1\}^*$,$A(x) = F(x)$. 难于求逆:对于给定的 $y \in$ range(F),$F^{-1} \subset$ dimain(F). 这里 domain(F) 表示函数 F 的定义域,range(F) 表示函数 F 的值域. 即对于给定的 $y \in$ range(F),$F^{-1}(y)$ 是定义域的一个子集,而不是一个元素,所以无法判断出哪一个是真正的 $F^{-1}(y)$.

● 如果 $x_1 \geq x_2$,那么 $F(x_1) \geq F(x_2)$;如果 $x_1 \gg x_2$,那么 $F(x_1) > F(x_2)$. 如果 F 具有这种特性,当 $x_1 \gg x_2$ 时,就可以通过比较 $F(x_1)$ 与 $F(x_2)$ 实现 x_1 对 x_2 与的比较.

● 假设 $X =$ domain(F),$|X|$ 表示 X 的势;$Y =$ range(F),$|Y|$ 表示 Y 的势;那么要求 $|X| \gg |Y|$. 只有具有这一特性,比较 $F(x_1)$,$F(x_2)$ 才会比比较 x_1,x_2,简单.

如果已经找到这样的函数,当 $x_1 \gg x_2$ 时,就可以将 x_1,x_2 的比较转化为 $F(x_1)$,$F(x_2)$ 的比较,从而简化比较的计算复杂性. 下面就来构造这样的函数:

定义 2 数 x 的 N 进制表示是下述形式表示:

$$x = a_n \times N^n + a_{n-1} \times N^{n-1} + \cdots + a_0 \quad (a_n \neq 0) \quad (9)$$

其中 $0 \leq a_i < N$ $(i = 1,2,\cdots,n)$. 可以简单地写作 $x = [a_n, a_{n-1}, \cdots, a_0]_N$. 例如 $[15]_{10} = [1111]_2 = [17]_8 = [F]_{16}$.

定义 3 如果 $x = [a_n, a_{n-1}, \cdots, a_0]_N$,那么称 $n+1$ 是 x 的 N 进制表示的长度,记作 $|x|_N = n+1$. 例如:$|15|_{10} = 2$,$|15|_2 = 4$,$|15|_{16} = 1$. 令 $F_N(x) = |x|_N$,那么 $F_N(x)$ 具有我们希望的所有性质.

● 首先,F 非常容易计算;又因为 $x \to F_N(x)$ 是多对一的映射,所以难于求逆.

● 其次,当 x_1,x_2 都用 N 进制表示时,如果 $x_1 > N \times x_2$,那么 $F_N(x_1) > F_N(x_2)$. 当用二进制表示时,如果 $x_1 > 2 \times x_2$,那么 $F_2(x_1) > F_2(x_2)$;在另一些情况下,比如 $4 \leq x_2 < 8$,$x_1 \geq 8$,都有 $F_2(x) > F_2(x_2)$,所以比较结果并不能使任何一方得出 x_1 比 x_2 大多少的结论. 即 $x_1 > 2 \times x_2$ 是 $F_2(x_1) > F_2(x_2)$ 的充分条件,不是必要条件.

● 如果 $X =$ domain$(F) = \{0,1,2,\cdots,K\}$,$|X| = K$,$Y =$ range$(F_N(x)) = \{0,1,2,\cdots,\lfloor(\log_2 K)\rfloor\}$ 所以 $|X| \gg |Y|$

4 高效解决方案

方案 1 两个较小的数的比较

假设要保密比较两个自然数 a,b 的大小,为简单起见假设 $1 \leq a, b < 100$,方案如下:

方案 1 保密地比较两个数

输入:两个保密的自然数 a 与 b.

输出:$a > b$,$a < b$ 或者 $a = b$.

● 令 $X = \{1,2,\cdots,99\}$,$R = \pi(X)$ 是 X 的一个随机置换. Bob 计算下面的 100 个数,得到一个数组 $Y = \{Y_1, Y_2, \cdots, Y_{100}\}$,其中:

$$Y_i = g(i,b) = \begin{cases} 0 + R_i, & \text{如果 } i - b = 0 \\ 100 + R_i, & \text{如果 } i - b > 0, \\ 200 + R_i, & \text{如果 } i - b < 0 \end{cases}$$

$$i = 1,2,\cdots,100 \quad (10)$$

● 利用 OT_{100}^1 不经意传输,Alice 能够选择她愿意得到的唯一的数 $Y_a = g(a,b)$. OT_{100}^1 不经意传输方案保证了 Alice 可以决定要得到的唯一的数,而 Bob 并不知道 Alice 选择了哪一个数. 如果 $Y_a < 100$,那么 $a = b$;如果 $100 < Y_a < 200$,那么 $a > b$,如果 $200 < Y_a < 300$,那么 $a < b$.

● Alice 将结果告诉 Bob.

定理 1 比较两个数大小的方案 1 是安全的

证明 注意到在本方案中,$f_1(a,b) = f_2(a,b) = output_1^{\pi}(a,b) = output_2^{\pi}(a,b) = g(a,b)$,$view_1^{\pi}(a,b) = (a, r, m_1, m_2, \cdots)$. 其中 a 是输入,r 是 Alice 的硬币抛掷结果,m_i 是第 i 次收到的消息. 首先构造一个模拟器 S_1 来模拟 $view_1^{\pi}$ 使得式(7)成立.

● S_1 接受输入 $(a, g(a,b))$ 作为 Alice 的输入,根据 $g(a,b)$ 的值,确定一个 b',使得 $g(a,b') = g(a,b)$. S_1 计算数组 $Y' = \{Y_1', Y_2', \cdots, Y_{100}'\}$,其中 $Y_i' = g(i,b')$.

● 模拟 OT_{100}^1 不经意传输过程,S_1 可以得到唯一的一个 $g(a,b')$,根据构造的过程 $g(a,b') = g(a,b)$. OT_{100}^1 不经意传输过程的安全性已经得到证明[12].

因为 $view_1^{\pi}(a,b) = (a, r, g(a,b))$,$output_1^{\pi}(a,b) = g(a,b)$,令 $S_1(a, f_1(a,b)) = (a, r, g(a,b'))$ 则

$$\{(S_1(a, f_1(a,b)), f_2(a,b))\} \equiv\{(view_1^{\pi}(a,b), view_1^{\pi}(a,b))\} \quad (11)$$

类似地,还可以构造一个模拟器 S_2 使得

$$\{f_1(a,b), S_2(b, f_2(a,b)))\} \equiv\{(view_1^{\pi}(a,b), view_1^{\pi}(a,b))\} \quad (12)$$

这样就完成了定理的证明.

直观上,如果 $100 < g(a,b) < 200$ 即 $a > b$,那么对于 $\forall b'$ $< a$ 都有 $100 < a, b' < 200$. 在此条件下,只有一种情况会泄露关 b 于的信息,即 $a = 2$,因为 $0 < b < 2$,所以可以推出 $b = 1$,其他情况都不会泄漏有关 b 的信息. 同样的分析可知,如果 $200 < g(a,b') < 300$,只有当 $a = 98$ 时,可以推出 $b = 99$,其他情况都不会泄露有关 b 的信息. 这两种可能泄漏信息的情况在 Yao 提出的解决方案中也无法避免.

方案 2 任意两个数的比较

设两个数为 a 与 b,它们的二进制表示为:

$$a = [a_m, a_{m-1}, \cdots, a_0]_2,\ a_i \in \{0,1\}\ (i = 1,2,\cdots,m)$$
$$b = [b_n, b_{n-1}, \cdots, b_0]_2,\ b_i \in \{0,1\}\ (j = 1,2,\cdots,n) \quad (13)$$

方案 2 任意两个数的保密比较

输入:两个数 a 与 b.

输出: $a > b$, $a < b$ 或者 $a = b$.

方案重复下面的步骤,直到比较出结果.

Alice 和 Bob 首先应用解决方案 1 保密地比较 $F_2(a)$ 与 $F_2(b)$.

(1) 如果 $F_2(a) > F_2(b)$ ($F_2(a) < F_2(b)$),那么 $a > b$ ($a < b$) 比较完成,方案终止. 否则进行第二步.

(2) 如果 $F_2(a) = F_2(b)$,那么 $a, b > 2^{F_2(a)-1}$. 令 $a \leftarrow a - 2^{F_2(a)-1}$ $b \leftarrow b - 2^{F_2(a)1}$,回到第一步继续比较.

定理 2 保密比较任意两个数的方案 2 是安全的

证明:这个定理是定理 1 的直接结果.

5 性能分析

5.1 安全性分析

前面证明了在多方计算参与者都是半诚实的条件,两个方案 1、2 都是安全的. 现在对于参与者完全恶意情况下的安全性进行分析. 如果参与计算的双方都是恶意的参与者,那么方案没有任何意义. 本文只讨论一个恶意参与者条件下的安全性,一个恶意参与者比如说 Bob,他参与协议的目的并不是真的将他拥有的数与 Alice 的数进行比较,而是在比较的每一步提供一个猜测的数据与 Alice 的数据进行比较,目的是要知道 Alice 的数据,也就是 Alice 的财富数. 下面来分析 Bob 能够获得 Alice 的数据的概率.

在第一步的比较中,假设 $F_2(a)$ 均匀分布于 m 个可能值上,Bob 要做的是猜测一个 $F_2'(a)$,然后用 $F_2'(a)$ 与 $F_2(a)$ 进行比较,在这种情况下 Bob 攻击成功的概率 $P[F_2(a) = F_2'(a)] = \frac{1}{m}$.

在完成第一步的比较后,$F_2(a - 2^{F_2(a)-1})$ 就变成均匀分布在 $m - 1$ 个可能的值上,在此条件下,Bob 猜测正确的概率 $P[F_2(a - 2^{F_2(a)-1}) = F_2'(a - 2^{F_2(a)-1}))] = \frac{1}{m-1}$,依此类推.

如果 Bob 每次都猜测正确,它就可以成功地重构 Alice 的数据 a,而这个概率为:

$$P[\text{Bob 能准确重构 } a] = \frac{1}{m!} \tag{14}$$

假设 $F_2(a) = 10$ 那么 $\frac{1}{10!} < 10^{-6}$. 进一步分析表明,随着 $F_2(a)$ 的增大,Bob 攻击成功的概率指数地减小.

5.2 计算复杂性

方案 2 是基于方案 1 构造的,用于比较两个很大的数. 而方案 1 与方案 0 都适用于较小的数(比如两个介于 1 和 100 之间的数)的比较,因此,这里将方案 0 与方案 1 的计算复杂性做一个比较. 方案 0 在作这样的比较时,(1) 需要进行 1 次模指数运算;(2) 需要 100 次模指数运算;(3) 需要 100 次模运算;(4) 需要至少 5000 (100 ×100/2) 次比较,因为如果 $|z_u - z_v| \geq 2$ 不是对所有的 $u \neq v$ 成立,(3) (4) (5) 都要根据重新选择的 p,重新计算;(5) 需要 100 次比较.

方案 1 只需要进行 100 次加减法运算与 101 次模指数运算. 减少了大量的比较与验证. 假设 $F_2(a)$, $F_2(b)$ 均匀分布在集合 $\{1, 2, \cdots, 100\}$ 上,那么根据生日攻击的数学基础[13]可知对于任意两个数 a, b, $F_2(a)$ 与 $F_2(b)$ 相同的概率为

$$P(100, 2) = 1 - \frac{100!}{(100-2)\,100^2} = 0.01 = 1\% \tag{15}$$

$F_2(a)$ 与 $F_2(b)$ 不同的概率为 99 %. 所以方案 2 的真正价值在于对任意两个数进行比较时,在 99 %的情况下,第一步就可以完成两个数的比较. 进一步的概率分析表明:在比较两个较大的数时,方案 2 的计算复杂性的期望值远低于方案 0 的 1 %.

6 结论

本文利用 OT_m^1 不经意传输与一种单调不减的函数构造了一种新的保密比较两个数的大小的方案,方案首先利用不经意传输比较两个数的长度,如果长度不同即可以完成比较,如果长度相同需要进一步比较,许多情况下一步就可以完成比较. 还利用模拟范例证明了方案的安全性. 新方案同已有的方案相比,当比较两个较大的数时,计算复杂性的期望值远低于已有方案的,可以用于比较两个任意大小的数.

参考文献:

[1] A Yao. Protocols for secure computations[A]. Proceeding of the 23th IEEE Symposium on Foundations of Computer Science[C]. Los Alamitos, CA: IEEE Computer Society Press, 1982. 160 - 164.

[2] C Cachin. Efficient private bidding and auction with an obvious third party[A]. Proceeding of the 6th ACM conference on computer and communication security[C]. New York: ACM Press, 1999. 120 - 127.

[3] Oded Goldreich, Silvio Micali, Avi Wigderson. How to play ANY mental game[A]. Proceedings of the nineteenth annual ACM conference on Theory of computing[C]. New York: ACM Press, 1987. 218 - 229.

[4] O Goldreich. Secure multi-party computation (working draft)[OL]. http://www.wisdom.weizmann.ac.il/home/oded/public_html/foc.html, 2002.

[5] S Goldwasser. Multi-party computations: Past and present[A]. Proceedings of the sixteenth annual ACM symposium on Principles of distributed computing[C]. New York: ACM Press, 1997. 21 - 24.

[6] Wenliang Du, Atallah J. Secure multi-party computation problems and their applications: A review and open problems[A]. New Security Paradigms Workshop 2001[C]. Cloudcroft, New Mexico, USA, Sep. 11 - 13, 2001. 11 - 20.

[7] Mikhail J Atallah, Wenliang Du. Secure multi-party computational geometry[A]. In Seventh International Workshop on Algorithms and Data Structures (WADS 2001), Lecture Note in Computer Science 2125[C]. New York: Springer-verlag, 2001. 165 - 179.

[8] Y Lindell, B Pinkas. Privacy preserving data mining[J]. Journal of Cryptology, 2002, 15(3): 177 - 206.

[9] Ronald Fagin, Moni Naor, Peter Einkler. Comparing information without leaking it[J]. Communications of the ACM, 1996, 39(5): 77 - 85.

[10] M Rabin. How to exchange secrets by oblivious transfer[R]. Technical Report TR-81, Aiken Computation Laboratory, Harvard Univ, 1981.

[11] M Naor, B Pinkas. Efficient oblivious transfer protocols[A]. Proc 12th Ann Symp Discrete Algorithms[C]. New York: ACM Press, 2001. 448 - 457.

[12] Wen-Guey Tzeng. Efficient 1-out-of-n oblivious transfer schemes with universally usable parameters[J]. IEEE TRANSACTIONS ON COMPUTERS, 2004, 53(2): 232 - 240.

[13] William Stallings. Cryptography and Network Security: Principles and Practice (2nd ed) [M]. Beijing: Tsinghua University Press, 2003. 264 - 269.

作者简介:

李顺东　男,1963 年 12 月生于河南,2003 年在西安交通大学获工学博士学位,现为清华大学计算机科学与技术系博士后,副教授,研究方向为密码学理论与应用,多方保密计算,电子商务等. E-mail: shundong@mails.tsinghua.edu.cn.

戴一奇　男,1946 年 10 月生于浙江,1970 年毕业于清华大学,现为清华大学计算机科学与技术系教授,博士生导师,主要研究方向为网络信息安全、算法设计与分析.

游启友　男,1978 年 9 月生于湖北,2002 年毕业于中国科学技术大学计算机科学与技术系,现为清华大学计算机科学与技术网络所硕士研究生,研究方向为网络信息安全、信息隐藏和电子商务安全.

征 订 启 事

为推动我国通信和计算机技术的发展,更好地为迅猛发展的信息产业服务,《电子学报》编辑部已于 2004 年年底编辑出版《新一代移动通信与计算机》专刊. 本专刊主要内容涉及移动通信和计算机理论与技术研究的诸多方面,作者对许多国际、国内的热点问题发表了自己的观点和看法. 这对从事通信与计算机科学技术,特别是对从事该领域科学研究及教学的学者、专家均有很高的参考价值. 每册定价 25 元. 凡中国电子学会会员或会员所在单位订阅价格为 20 元(包括邮寄费),欢迎广大会员订阅. 请订阅者与《电子学报》编辑部王辉同志联系. 同时将订刊款项由邮局汇至:

北京 165 信箱《电子学报》编辑部王辉同志收.

邮编:100036　**电话**:010 - 68279116 - 803,68285082 - 803).

发票和专刊一并寄回. 订阅日期到 2005 年 5 月 31 日止.