第36卷 第14期 计 算 机 工 程 2010年7月
Vol.36 No.14 Computer Engineering July 2010
·安全技术· 文章编号：1000—3428(2010)14—0124—03 文献标识码：A 中图分类号：TP305

姚氏百万富翁问题的高效解决方案

查 俊，苏锦海，闫少阁，闫晓芳
(解放军信息工程大学电子技术学院，郑州 450004)

摘 要：姚氏百万富翁问题是安全多方计算的典型问题，但已有解决方案多数存在效率低的问题。通过采用0编码与1编码，将百万富翁问题转换为集合交集问题，提出一种基于可交换加密函数的百万富翁问题高效解决方案，并进行了安全性证明。该方案无需复杂的模指数运算，加解密运算为 $O(n)$，通信轮数为4，整体性能优于其他方案。

关键词：百万富翁问题；编码；交集；可交换加密；安全性

Efficient Solution to Yao's Millionaires' Problem

ZHA Jun, SU Jin-hai, YAN Shao-ge, YAN Xiao-fang
(Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004)

【Abstract】 Yao's Millionaires' problem is a typical problem of secure multi-party computation, but most solutions are inefficient. Based on commutative encryption scheme, this paper proposes an efficient and secure solution to millionaires' problem, which reduces the problem to the set-intersection problem by 0-encoding and 1-encoding for private inputs. Proof of security is followed. There is no complicated modular exponentiation in this solution which only needs $O(n)$ encryption/decryption and 4 rounds of communication. It is more efficient than other solutions.

【Key words】 millionaires' problem; encoding; set-intersection; commutative encryption; security

1 概述

姚氏百万富翁问题[1]由 Andrew C.Yao 于1982年首次提出。Yao给出了一个趣味性的例子：2个争强好胜的富翁 Alice 和 Bob 在街头相遇，如何在不暴露各自财富的前提下比较出谁更富有？经过文献[2]的研究，百万富翁问题已经发展成为现代密码学中一个非常活跃的研究领域，即安全多方计算(Secure Multi-party Computation, SMC)。

文献[1]就百万富翁问题给出了一个解决方案，但效率非常低，计算复杂性为输入规模的指数函数，用于比较2个较大的数时不实用；文献[2]利用算术电路解决了一般意义上的安全多方计算问题，将其应用于百万富翁问题，计算及通信成本均与输入规模呈线性关系；文献[3]直接针对百万富翁问题，提出了一个基于茫然传输(Oblivious Transfer, OT)的解决方案，利用简单的异或运算成功地解决了该问题；还有一些学者将同态加密的思想应用于百万富翁问题[4]，也取得了很好的研究成果。

本文利用0编码与1编码，将百万富翁问题转换为集合的交集问题，提出一种基于可交换加密函数的百万富翁问题解决方案，其计算及通信复杂度明显降低。同时对该方案的安全性进行了理论证明。

2 预备知识

2.1 数学模型

安全多方计算是一种分布式协议。在这个协议中，设 $P=\{P_1,P_2,\cdots,P_n\}$ 是 n 个参与者集合，他们想要共同“安全地”计算某个给定的有 n 个输入和 n 个输出的函数 $f(x_1,x_2,\cdots,x_n)=(y_1,y_2,\cdots,y_n)$，其中，函数 f 的 n 个输入 $x_1,x_2,\cdots,x_n$ 分别由 n 个参与者 $P_1,P_2,\cdots,P_n$ 秘密地掌握而不被他人知道，在计算结束后，$P_1,P_2,\cdots,P_n$ 分别得到输出 $y_1,y_2,\cdots,y_n$。

百万富翁问题是一个典型的双方安全计算问题，其数学描述如下：参与方 Alice 和 Bob 分别具有秘密输入 x 和 y，双方协同计算以下函数：

$$f(x,y)=\begin{cases}1 & \text{if } x>y\\ 0 & \text{if } x\le y\end{cases}$$

用于解决该问题的协议 π 需要满足以下要求：

(1)参与方 Alice 和 Bob 均形式化为概率多项式时间的图灵机，且都为半诚实的。也就是说 Alice 和 Bob 在协议的执行过程中将完全执行协议，但是他们也会保留中间计算结果，试图推导出对方的输入。

(2)正确性：协议 π 执行完以后，Alice 返回1当且仅当 $x>y$。

(3)Alice 的保密性：Alice 拥有 x 或 x' $(x\neq x')$ 对于 Bob 来说是不可区分的。

(4)Bob 的保密性：除了 x 和最终的结果 $f(x,y)$，Alice 不能得到任何信息。

2.2 安全性定义

安全多方计算中的安全性证明采用了一个特殊的方法，它通过定义一个理想模型，用理想模型仿真现实协议，如果现实协议能被理想模型所仿真，且输出结果具有不可区分性，那么现实协议就是安全的。

为了方便地给出半诚实模型下的安全性定义，首先引入下列符号。假设协议的参与方分别为 Alice 和 Bob。Alice 和 Bob 要计算的函数为 $f:\{0,1\}^*\times\{0,1\}^*\mapsto\{0,1\}^*\times\{0,1\}^*$。函数

作者简介：查 俊(1986－)，男，硕士研究生，主研方向：保密通信；苏锦海，教授；闫少阁、闫晓芳，硕士研究生

收稿日期：2009-12-22 **E-mail：**chazhajun@163.com

$f(x,y)$ 的第 1 个元素记为 $f_1(x,y)$，第 2 个记为 $f_2(x,y)$，计算函数 f 的两方协议为 π。Alice 和 Bob 在输入为 (x,y) 的情况下执行协议 π 得到的信息分别为 $VIEW_1^{\pi}(x,y), VIEW_2^{\pi}(x,y)$，其具体值为 $\{x,r_1,m_1,m_2,\cdots,m_t\}$,($\{y,r_2,m_1,m_2,\cdots,m_t\}$)，其中，r_1，r_2 表示 Alice 和 Bob 拥有的随机数，m_i 表示所收到的第 i 条消息。$OUTPUT_1^{\pi}(x,y)(OUTPUT_2^{\pi}(x,y))$ 表示 Alice(Bob)在输入为 (x,y) 的情况下执行协议 π 时得到的输出结果，显然它隐含在 $VIEW_1^{\pi}(x,y),(VIEW_2^{\pi}(x,y))$ 中。

定义 1 (半诚实模型的安全性) 对于一个函数 f，如果存在多项式时间算法(有时称为模拟器) S_1, S_2 满足以下关系：

$$\{S_1(x, f_1(x,y)), f_2(x,y)\}_{x,y} \overset{c}{\equiv} \{(VIEW_1^{\pi}(x,y), OUTPUT_2^{\pi}(x,y)\}_{x,y} \quad (1)$$

$$\{(f_1(x,y)), S_2(y, f_2(x,y))\}_{x,y} \overset{c}{\equiv} \{(OUTPUT_1^{\pi}(x,y), VIEW_2^{\pi}(x,y)\}_{x,y} \quad (2)$$

则认为协议 π 安全地计算函数 f，其中，$\overset{c}{\equiv}$ 表示计算不可区分。

因此，要证明百万富翁问题解决方案的安全性必须构建满足上述要求的模拟器 S_1, S_2。

2.3 0 编码与 1 编码

本文解决方案的核心思想是通过 0 编码与 1 编码，将百万富翁问题转换为集合交集问题，从而简化问题的求解。

令 $s = s_n s_{n-1}\cdots s_1 \in \{0,1\}^n$ 为一个长度为 n 的二进制数据流，表示需要进行比较的数据。

定义 2 二进制数据流 s 的 0 编码 S_s^0 由如下形式表示：

$$S_s^0 = \{s_n s_{n-1}\cdots s_{i+1} \mid s_i = 0, 1 \le i \le n\}$$

定义 3 二进制数据流 s 的 1 编码 S_s^1 由如下形式表示：

$$S_s^1 = \{s_n s_{n-1}\cdots s_i \mid s_i = 1, 1 \le i \le n\}$$

其中，$\left|S_s^0\right| \le n$, $\left|S_s^1\right| \le n$。

如果将数据 x 进行 1 编码 S_x^1，数据 y 进行 0 编码 S_y^0，可以得到当且仅当 S_x^1 和 S_y^0 的交集非空时，有 $x > y$。需要注意的是在进行 0, 1 编码之前，数据 x, y 的二进制数据流长度必须相等，不足的高位补 0。

定理 x 大于 y 的充分必要条件是 S_x^1，S_y^0 的交集非空。

证明见文献[4]。

3 半诚实模型下百万富翁问题解决方案

在介绍方案之前，首先说明可交换加密函数。简单地说，满足性质 $E_a(E_b(x)) = E_b(E_a(x))$ 的函数 $E(\cdot)$ 称为可交换加密函数，其中，$E_a(x)$ 表示用密钥 a 加密 x。

本文基于 0 编码与 1 编码的结果提出了一种新的半诚实模型下百万富翁问题的解决方案。假设需要保密比较 2 个自然数 x，y 的大小，首先需要对 x，y 所对应的二进制表现形式分别进行 1 编码与 0 编码，得到集合 S_x^1，S_y^0，然后判断 2 个集合的交集是否为空，从而得到比较结果。可以看出，如果逐次比较集合 S_x^1，S_y^0 中的所有元素得到交集，需要 $O(n^2)$ 次操作，但是本文的目的不在于得到所有的交集数据，而只需要判断 S_x^1，S_y^0 的交集是否为空，因此使用可交换加密函数判断集合的交集是否为空，从而得到问题所需的比较结果。

输入 集合 S_x^1，S_y^0

输出 $\left|S_x^1 \cap S_y^0\right|$

根据前面讨论的结果，本文的解决方案如下：

Step1 Alice 和 Bob 通过协商获得一个可交换加密函数 E，并设定各自的私钥 a，b。

Step2 Alice 和 Bob 分别计算：

$$E_a(S_x^1) = \{E_a(S_{x1}^1), E_a(S_{x2}^1), \cdots, E_a(S_{xn}^1)\}$$

$$E_b(S_y^0) = \{E_b(S_{y1}^0), E_b(S_{y2}^0), \cdots, E_b(S_{yn}^0)\}$$

其中，S_{xi}^1，S_{yi}^0 $(1 \le i \le n)$分别表示编码集合 S_x^1，S_y^0 中第 i 个元素。双方交换加密结果 $E_a(S_x^1)$ 和 $E_b(S_y^0)$。

Step3 Alice 计算：

$$E_a(E_b(S_y^0)) = \{E_a(E_b(S_{y1}^0)), E_a(E_b(S_{y2}^0)), \cdots, E_a(E_b(S_{yn}^0))\}$$

将结果发送给 Bob。

Step4 Bob 计算：

$$E_b(E_a(S_x^1)) = \{E_b(E_a(S_{x1}^1)), E_b(E_a(S_{x2}^1)), \cdots, E_b(E_a(S_{xn}^1))\}$$

从而可以得到 $\left|S_x^1 \cap S_y^0\right|$。

Step5 Bob 将最终的比较结果告诉 Alice。

从上述过程可以看出 $\left|E_b(E_a(S_x^1)) \cap E_a(E_b(S_y^0))\right| = \left|S_x^1 \cap S_y^0\right|$。如果 $\left|E_b(E_a(S_x^1)) \cap E_a(E_b(S_y^0))\right| \ne 0$，则有 $x > y$，否则，$x \le y$。在方案的执行过程中，输入的数据都进行了加密处理，因此，不会导致用户信息的泄漏。

4 方案安全性及效率分析

4.1 安全性分析

下面利用安全多方计算的安全性理论证明本文方案的安全性。在本文方案的执行过程中，有：

$$OUTPUT_1^{\pi}(x,y) = f_1(x,y) = \left|E_b(E_a(S_x^1)) \cap E_a(E_b(S_y^0))\right| = \left|S_x^1 \cap S_y^0\right| \quad OUTPUT_2^{\pi}(x,y) = f_2(x,y) = \left|E_b(E_a(S_x^1)) \cap E_a(E_b(S_y^0))\right| = \left|S_x^1 \cap S_y^0\right|$$

$$VIEW_1^{\pi}(x,y) = \{x, r_1, E_a(S_x^1), E_b(S_y^0), E_a(E_b(S_y^0))\}$$

$$VIEW_2^{\pi}(x,y) = \{y, r_2, E_b(S_y^0), E_a(S_x^1), E_b(E_a(S_x^1)), E_a(E_b(S_y^0))\}$$

其中，x，y 表示 Alice 和 Bob 的输入；r_1，r_2 为随机数。假设 $\left|S_x^1 \cap S_y^0\right| = k$，首先构造 S_1 模拟 $VIEW_1^{\pi}(x,y)$ 使式(1)成立。

(1) S_1 接受 $(x, f_1(x,y)) = (x,k)$ 作为输入，同时选择一个可交换加密函数 E 和密钥 a，另外随机选择一个密钥 b'。S_1 构建一个数据 y'，使得由 y' 得到的 0 编码集合中存在 k 对 (i, j)，满足 $S_{xi_1}^1 = S_{y'j_1}^0, S_{xi_2}^1 = S_{y'j_2}^0, \cdots, S_{xi_k}^1 = S_{y'j_k}^0$。

(2)根据上述解决方案，S_1 模拟计算：

$$E_a(S_x^1) = \{E_a(S_{x1}^1), E_a(S_{x2}^1), \cdots, E_a(S_{xn}^1)\}$$

$$E_{b'}(S_{y'}^0) = \{E_{b'}(S_{y'1}^0), E_{b'}(S_{y'2}^0), \cdots, E_{b'}(S_{y'n}^0)\}$$

(3) S_1 计算 $E_a(E_{b'}(S_{y'}^0))$，$E_{b'}(E_a(S_x^1))$ 及 $\left|E_{b'}(E_a(S_x^1)) \cap (E_a(E_{b'}(S_y^0))\right|$。

(4)通过构造数据 y 得到其 0 编码，则必存在 k 对 (i, j) 满足：

$$E_{b'}(E_a(S_{xi_1}^1) = E_a(E_{b'}(S_{y'j_1}^0), E_a(E_{b'}(S_{y'j_2}^0), \cdots, E_{b'}(E_a(S_{xi_k}^1) = E_a(E_{b'}(S_{y'j_k}^0)$$

因此，有如下结论：

$$\left|(E_{b'}(E_a(S_x^1))\cap(E_a(E_{b'}(S_y^0))\right|=\left|S_x^1\cap S_y^0\right|=k$$

令 $S_1(x, f_1(x,y))=\{x, r_1', E_a(S_x^1), E_{b'}(S_{y'}^0), E_a(E_{b'}(S_{y'}^0))\}$，则有

$$S_1(x, f_1(x,y), f_2(x,y))=\{x, r_1', E_a(S_x^1), E_{b'}(S_{y'}^0), E_a(E_{b'}(S_{y'}^0)), k\}$$

$$\{VIEW_1^{\pi}(x,y), OUTPUT_2^{\pi}(x,y)\}=\{x, r_1, E_a(S_x^1), E_b(S_y^0), E_a(E_b(S_y^0)), k\}$$

由此可以推出

$$\{S_1(x, f_1(x,y)), f_2(x,y)\}_{x,y}\overset{c}{\equiv}\{(VIEW_1^{\pi}(x,y), OUTPUT_2^{\pi}(x,y)\}_{x,y}$$

用类似的方法还可以构造一个模拟器 S_2，使得

$$\{(f_1(x,y)), S_2(y, f_2(x,y))\}_{x,y}\overset{c}{\equiv}\{(OUTPUT_1^{\pi}(x,y), VIEW_2^{\pi}(x,y)\}_{x,y}$$

这样就完成了定理的证明。

4.2 效率分析

作为安全多方计算协议的一个重要组成模块，百万富翁问题解决方案的效率直接影响整个安全多方计算协议的效率。下面针对本文提出的协议分析其计算及通信复杂度，并与其他相关的百万富翁问题解决方案进行比较。

(1)计算复杂度：假设 $0<\max(|x|,|y|)=n$，其中，$|x|$ ($|y|$) 表示输入 x (y)的长度(二进制形式)。本文方案需要 $O(n)$ 次加解密运算。需要注意的是，与其他解决方案中公钥密码系统的加解密运算不同，本文方案采用的是对称的可交换加密函数，其加解密效率高于其他方案。另外，虽然模指数运算是隐藏信息的一种常用技术手段，但该运算需要消耗大量的计算资源，而本文方案不需要复杂的模指数运算(加解密算法中除外)，在这一点上，计算复杂度大大降低，其他简单运算需要 $O(n^2)$。相关方案计算复杂度比较结果见表 1。

表 1　各方案计算及通信复杂度比较

解决方案	计算复杂度			通信复杂度
	加解密	模指数运算	其他运算	
文献[1]方案	$O(2^n)$	$O(2^n)$	$O(2^{2n})$	3
文献[3]方案	无	$O(n)$	$O(2^n)$	$O(n)$
文献[5]方案	无	$O(1)$	$O(2^n)$	3
本文方案	$O(n)$	无	$O(n^2)$	4

(2)通信复杂度：衡量一个计算方案效率的首要指标是其计算复杂度，但是对于安全多方计算来说，仅计算复杂度无法全面地描述一个解决方案的优劣。在安全多方计算中，参与方相互之间要进行通信，而在通信过程中，所有参与方都需要等待自己所需的数据，因此，通信复杂度也是衡量安全多方计算效率的一个重要指标。本文用通信的轮数表示通信复杂度，提出的解决方案包括 3 轮用以传输加密结果的通信，1 轮传输最终比较结果的通信，总的通信复杂度为 4 轮。由表 1 可以看出，本文的解决方案整体性能优于其他方案。

5　结束语

本文利用 0 编码与 1 编码构造了一种新的百万富翁问题解决方案。该方案避免了复杂的模指数运算，有效地减小了计算与通信复杂度，同时利用安全多方计算中理想模型与现实协议相比较的方法，证明了方案的安全性。因此，本文方案是一个安全的解决方案，高效地解决了无信息泄漏的数值比较问题。

参考文献

[1] Yao A C. Protocols for Secure Computation[C]//Proceedings of the 23rd IEEE Symposium on Foundations of Computer Science. Los Alamitos, CA, USA: IEEE Computer Society Press, 1982: 160-164.

[2] Goldreich O, Micali S, Wigerson A. How to Play Any Mental Game[C]//Proceedings of the 19th Annual ACM Conference on Theory of Computing. New York, USA: ACM Press, 1987: 218-229.

[3] Ioannidis I, Grama A. An Efficient Protocol for Yao's Millionaires' Problem[C]//Proceedings of the 36th Hawaii International Conference on System Sciences. Hawaii, USA: [s. n.], 2003.

[4] Schoenmakers B, Tuyls P. Practical Two-party Computation Based on the Conditional Gate[C]//Proceedings of Asiacrypt'04. Jeju, Korea: [s. n.], 2004.

[5] Li Shundong, Dai Yiqi, You Qiyou. An Efficient Solution to Yao's Millionaires' Problem[J]. ACTA Electronica Sinica, 2005, 33(5): 769-773.

编辑　张正兴

(上接第 123 页)

原始签名者的身份标识、代理签名者 B 的身份标识及 B 的代理权限，使得本文提出的方案还具有强可识别性、强不可否认性及抗滥用性。

(3)安全性的其他方面

该方案中规定了代理终止时间 $\tilde{t}$，从而具有限制代理权期限的功能；代理授权过程无需安全信道，便于实现；签名验证同时使用原始签名者和代理签名者的公钥，有效地分离了签名权和代理权。

4.3 前向安全性

在特殊的情况下，代理签名者第 i 时段的代理签名密钥泄漏，由于 $\delta_i=\sigma x_{B_i}^{e_i} \bmod N$ 攻击者无法得到 x_{B_i}，即使是原始签名人联合也只能得到 $x_{B_i}^{e_i} \bmod N$，由强 RSA 假定还是不能求出 x_{B_i}。即使是更不幸的情况，代理签名者第 i 时段的私钥 x_{B_i} 泄漏，攻击者仍无法伪造代理签名者在第 $j(j<i)$ 时段的代理签名，因为由强 RSA 假定攻击者无法从 $x_{B_i}=x_{B_{i-1}}^2 \bmod N=x_{B_{i-2}}^{2^2} \bmod N=\cdots=x_{B_j}^{2^{i-j}} \bmod N$ 得到 x_{B_j}。因而本文提出的方案具有前向安全性。

5　结束语

在传统的代理多重签名方案中，仍没有有效的方法解决如何减少由于代理者私钥或是代理密钥泄漏所带来的损失。本文基于前向安全的思想提出了一个前向安全的代理多重签名方案，在 Hash 函数的安全性假设及强 RSA 假定下分析了方案的安全性，证明该方案不仅满足一般代理多重签名方案的安全性，而且具有前向安全性。

参考文献

[1] 牛江品, 张建中. 基于双线性对的前向安全代理签名方案[J]. 计算机工程, 2009, 35(6): 164-165.

[2] 陈海滨, 杨晓元, 梁中银, 等. 一种无证书的前向安全代理签名方案[J]. 计算机工程, 2010, 36(2):156-157.

[3] 王玲玲, 张国印, 马春光. 基于环 Zn 上圆锥曲线的前向安全环签名方案[J]. 计算机工程, 2008, 34(6): 33-34.

[4] Abdalla M, Reyzin L. A New Forward-secure Digital Signature Scheme[C]//Proc. of Asiacrypt'76. Berlin, Germany: Springer, 1976: 116-129.

[5] 王玲玲, 张国印, 马春光. 前向安全的多重数字签名方案[J]. 计算机学报, 2004, 27(9): 1177-1181.

[6] Itkins G, Reyzin L. Forward-secure Signatures with Optimal Signing and Verifying[C]//Proc. of Crypto'01. Berlin, Germany: Springer, 2001: 332-354.

编辑　索书志