第42卷 第2期 西 安 交 通 大 学 学 报 Vol. 42 №2
2008年2月 JOURNAL OF XI′AN JIAOTONG UNIVERSITY Feb. 2008

排序问题的多方保密计算协议

李顺东[1]， 张选平[2]
(1. 陕西师范大学计算机科学学院，710062，西安；2. 西安交通大学计算机科学与技术系，710049，西安)

摘要：为了解决多方参与的保密排序问题，提出了基于保密排序的隐私保护解决方案. 该方案首先假设多方保密计算的参与者为半诚实的，即参与者在协议执行过程中将忠实地执行协议，但可能保留计算的中间结果，以试图推导出其他参与者的输入，然后给定参与者与数据的对应集合关系，并利用离散对数方法计算数据数组以获取其置换结果，从而使得参与者知道且只知道自己的数据在置换后的数组中的位置. 模拟范例证明了所提方案具有一定保密性，且特别适用于解决计算机网络中的隐私保护问题.

关键词：密码学；多方保密计算；隐私保护；协议
中图分类号：TN918.2 **文献标志码**：A **文章编号**：0253-987X(2008)02-0231-03

Secure Multi-Party Computation Protocol for Sorting Problem

LI Shundong[1]， ZHANG Xuanping[2]
(1. School of Computer Science, Shaanxi Normal University, Xi′an 710062, China; 2. Department of Computer Science and Technology, Xi′an Jiaotong University, Xi′an 710049, China)

Abstract: In order to solve multi-party participating secure sort problem, schemes based on privacy-preserving are proposed, in which that all participants of a secure computation are semi-honest is first assumed, i. e. each participant will execute the protocol loyally, but he (or she) keeps a record of all his (her) intermediate computing results and might try to derive other participant's private inputs from the record. Afterwards, given a corresponding collective relation between participants and their data, and using the discrete logarithm method the array is calculated to obtain permutation result, such that a participant knows and only knows the position of his and her data in the permutation array. It is proved, by simulation paradigm, that the proposed schemes are secure, and particularly suitable for solving privacy preserving problems in network.

Keywords: cryptography; multi-party secure computation; privacy-preserving; protocol

简单地说，Alice有数据x，Bob有数据y，多方保密计算[1]就是联合计算$f(x,y)$的值，而保守x和y的秘密，这样的计算在网络世界被广泛应用. Goldwasser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，这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"[2]. Cramer认为：如果能够保密地计算任何函数，计算科学就拥有一个新的强有力的工具[3]. 多方保密方计算经过Goldreich、Micali和Wigderson等人的发展[4-5]，现已经成为国际密码学界研究的热点问题之一[2,6]. 2004年欧洲密码学年会收录的多方保密计算的论文数量，超过了密码分析的论文数量，成为论文数量最多的研究领域[7]. 本文着重研究保密排序问题，并提出了解决方案.

收稿日期：2007-04-06. 作者简介：李顺东(1962—)，男，教授. 基金项目：国家自然科学基金资助项目(60673065)；国家高技术发展计划资助项目(2005AA114160).

1 预备知识

目前,保护消费者的隐私已成为人类社会发展的趋势.以前,考试成绩并不被认为是学生的隐私,现在为了保护学生的自尊心,保守成绩秘密已经成为国际通行做法,而且在一些国家已经成为法律.问题是学生希望在自尊心与隐私得到保护的前提下,了解自己在全体学生中的名次.保密排序就是研究在没有老师参与的条件下,如何使每位同学都知道自己的名次,并不知道分数与学生的对应关系,即研究的问题是:n 个人 $P_1,P_2,\cdots,P_n$ 分别拥有数据 $x_1,x_2,\cdots,x_n$,组成一个二元组的集合$\{(P_1,x_1),(P_2,x_2),\cdots,(P_n,x_n)\}$,在不泄漏集合$\{(P_1,x_1),(P_2,x_2),\cdots,(P_n,x_n)\}$的前提下,计算$(x_1,x_2,\cdots,x_n)$的一个置换$(x_{\omega(1)},x_{\omega(2)},\cdots,x_{\omega(n)})$,使得$(x_{\omega(1)}\geqslant x_{\omega(2)}\geqslant\cdots\geqslant x_{\omega(n)})$.这个研究问题目前尚未见到有关报道,本文在此提出了这个问题的解决方案并证明方案的保密性.

1.1 安全性定义

半诚实参与者 假设多方保密计算的参与者为半诚实的,即参与者在协议执行过程中将忠实地执行协议,但有可能保留计算的中间结果,以试图推导出其他参与者的输入.多方保密计算一般只研究半诚实参与者模型下的保密计算问题,本文亦是如此.

令 $\bar{x}=(x_1,x_2,\cdots,x_n)$,设 $f:(\{0,1\}_1^*,\cdots,\{0,1\}_n^*)\to(\{0,1\}_1^*,\cdots,\{0,1\}_n^*)$ 是一个 n 元函数,$f(\bar{x})=(f_1(\bar{x}),\cdots,f_n(\bar{x}))$,其中 $f_i(\bar{x})$ 表示 $f(\bar{x})$ 的第 i 个元素.$P_i(i=1,2,\cdots,n)$ 参与保密计算的目的是要得到 $f_i(\bar{x})$,而不想泄漏 x_i.设 π 表示计算 f 的协议,那么在执行协议 π 的过程中,P_i 所得到的信息序列 $v_i^\pi(\bar{x})$ 记为$(x_i,r_i,m_i^1,\cdots,m_i^t)$,其中 m_i^j 表示 P_i 第 j 次收到的信息.在执行了协议 π 以后,协议的输出结果记为 $o^\pi(\bar{x})$.

定义 1[5] 在半诚实参与者之间,计算函数 f 的协议 π 如果存在概率多项式时间算法 S,使得

$$\{(S(x_i,f_i(\bar{x})),f(\bar{x}))\}\overset{c}{\equiv}\{(v_i^\pi(\bar{x}),o^\pi(\bar{x}))\} \tag{1}$$

其中,$\overset{c}{\equiv}$表示计算上不可区分,则可以认为 π 保密地计算了f.

1.2 百万富翁问题解决方案

所谓百万富翁问题就是 2 个百万富翁 Alice 和 Bob 想知道他们 2 个谁更富有,而不想泄漏各自财富的具体数据,即保密地确定 2 个自然数 a、b 的大小关系,而保守 a、b 的秘密,姚期智教授提出并解决了这个问题.

1.3 离散对数假设

用记号 N 表示自然数集,自然数模 p 的最小剩余集记作 $Z_p=\{0,1,\cdots,n-1\}$.$\phi(p)$称为欧拉函数,它表示 Z_p 中与 p 互素的元素个数.Z_p 中与 p 互素的元素所组成的乘法群记为 Z_p^*,如果 p 是一个素数,则 $Z_p^*=\{1,2,\cdots,p-1\}$.如果 $\alpha\in Z_p^*$ 并且 $\alpha^{\phi(p)}\bmod p=1$,那么称 α 是 Z_p^* 的生成元.同时,用$|B|$表示集合 B 中元素的个数.

离散对数假设[7] 给定(α,β,p),其中 p 是一个大素数,$\alpha\in Z_p^*$ 是一个生成元.$(\beta\in Z_p^*)\wedge(\alpha^b\equiv\beta \bmod p)(b\in N)$,若不存在多项式时间算法 A 且满足 $A(\alpha,\beta,p)=b$,可使得 $b=\log_\alpha\beta$.

费马小定理[8] 如果 m 是一个素数,a 不是 m 的倍数,那么有

$$a^{m-1}\bmod m\equiv 1 \tag{2}$$

推论 如果 p 是一个素数,$\alpha\in Z_p^*$ 是一个生成元,$r\in Z_p^*$ 是一个随机数,$\beta\equiv\alpha^r\bmod p$,那么

$$\beta\alpha^{p-r-1}\bmod p\equiv 1 \tag{3}$$

证明 $\beta\alpha^{p-r-1}\bmod p\equiv\alpha^r\alpha^{p-r-1}\bmod p\equiv\alpha^{p-1}\bmod p\equiv 1$.

离散对数假设和这个推论是本文方案的主要理论基础.

2 解决方案

朴素的想法认为,重复运用百万富翁问题的解决方案,对集合的所有元素进行两两比较,最后得到所有元素的大小关系,就可以实现保密排序.问题是这样的保密排序,计算复杂度非常高,其根本问题是这将泄漏参与者与元素的对应关系,而这正是要保密的内容.

保密排序问题 有集合 $X=\{(P_1,x_1),(P_2,x_2),\cdots,(P_n,x_n)\}$,$Y=\{y_1,y_2,\cdots,y_m\}$ $(y_1\geqslant y_2\geqslant\cdots\geqslant y_m)$,对于任意的 $i\neq j$,有 $x_i\neq x_j$ 且$\{x_1,x_2,\cdots,x_n\}\subseteq Y$,$H:X\to Y$ 是 X 上的全函数,定义为 $H(P,x)=x$,X 的子集为 T_y,则有

$$\forall y,\ T_y=\{(P,x)\mid(P,x)\in X\wedge(P,x)=y\} \tag{4}$$

如果知道 H,对于 $\forall y\in Y$ 可以很容易地计算 $|T_y|$.保密排序问题就是在保守 H 秘密的前提下,计算出 $|T_{y_1}|,\cdots,|T_{y_m}|$,使得 P_i 知道 x_i 在集合 $(x_{\omega(1)},x_{\omega(2)},\cdots,x_{\omega(n)})$中的顺序 $\omega(i)$.

假设参与者 $P_i(i=1,2,\cdots,n)$ 的公钥/私钥对

为 V_i/S_i,p 为一个大素数,$\alpha\in Z_p^*$ 是一个生成元,则有如下解决方案.

协议 1　保密排序问题解决方案.

输入:$X=\{(P_1,x_1),(P_2,x_2),\cdots,(P_n,x_n)\}$,$Y=\{y_1,y_2,\cdots,y_m\}$ $(y_1\geqslant y_2\geqslant\cdots\geqslant y_m)$.

输出:$|T_{y_1}|,\cdots,|T_{y_m}|$.

(1)P_1 选择 m 个随机数 $r_1,r_2,\cdots,r_m\in Z_p^*$,并分别计算

$$\alpha_1\equiv\alpha^{r_1}\bmod p,\cdots,\alpha_m\equiv\alpha^{r_m}\bmod p \tag{5}$$

得到集合 $\alpha=\{\alpha_1,\alpha_2,\cdots,\alpha_m\}$.

(2)如果 $H(P_1,x_1)=y_j(1\leqslant j\leqslant m)$,保持 α 的其他元素不变,将 α_j 修改为 $\alpha_j\leftarrow\alpha_j\alpha \bmod p$.

(3)$P_i(i=1,2,\cdots,n)$将修改后的 $\alpha=\{\alpha_1,\alpha_2,\cdots,\alpha_k\}$ 用 $P_{(i+1)\bmod n}$ 的公钥 $V_{(i+1)\bmod n}$ 加密,得到 $V_{(i+1)\bmod n}(\alpha)=\{V_{(i+1)\bmod n}(\alpha_1),\cdots,V_{(i+1)\bmod n}(\alpha_k)\}$,然后发给 $P_{(i+1)\bmod n}$.

(4)$P_{(i+1)\bmod n}$在收到 P_i 发来的用自己的公钥加密的消息后,再用自己的私钥 $S_{(i+1)\bmod n}$ 解密消息,得到 $\alpha=\{\alpha_1,\alpha_2,\cdots,\alpha_m\}$. 如果 $H(P_{(i+1)\bmod n},x_{(i+1)\bmod n})=y_j(1\leqslant(i+1)\bmod n\leqslant m)$, $P_{(i+1)\bmod n}$ 对 α 中的 α_j 将作如下修改,即 $\alpha_j\leftarrow\alpha_j\cdot\alpha \bmod p$.

(5)最后,P_1 在得到集合 α 后,对 α 再作如下修改,即

$$\alpha_j\leftarrow\alpha_j\cdot\alpha^{p-r_j-1}\bmod p\quad(j=1,2,\cdots,m) \tag{6}$$

从而得到新的集合 $\alpha=\{\alpha_1,\alpha_2,\cdots,\alpha_m\}$,并计算

$$\beta_i=\alpha^i\bmod p\quad(i=1,2,\cdots,n) \tag{7}$$

从而得到集合 $\beta=\{\beta_1,\beta_2,\cdots,\beta_k\}$. 在得到 α、β 之后,P_1 执行下面的程序,即

```
10  j=1;
20  i=1;
30  If α_j=β_i | T_{y_j} |=i;
40  i←i+1;
50  If i<m Goto 30;
60  j←j+1;
70  If j<n Goto 20;
80  End.
```

(6)公布最后的 $|T_{y_1}|,\cdots,|T_{y_m}|$,则 P_i 就可以根据 x_i 和 $|T_{y_1}|,\cdots,|T_{y_m}|$ 的情况知道自己的名次 $\pi(i)$. 如果 $H(P_i,x_i)=y_k$,那么 P_i 的名次就是第 $|T_{y_1}|+\cdots+|T_{y_{k-1}}|$ 名.

定理 1　计算保密排序的协议 1(记为 π)是保密的.

证明　根据保密性的定义,需要构造能够使式(1)成立的模拟器 S. 在本协议中有

$$v_1^{\pi}(x)=\{x_1,V_n(\alpha)\}=\{V_n(\alpha_1),\cdots,V_n(\alpha_m)\}$$

$$v_i^{\pi}(\bar{x})\{x_i,V_i(\alpha)\}=\{V_i(\alpha_1),\cdots,V_i(\alpha_m)\}\quad(i=2,\cdots,n)$$

$$f_i(\bar{x})=\{x_{\pi(1)},\cdots,x_{\pi(n)}\}$$

$$(x_{\alpha(1)}\geqslant\cdots\geqslant x_{\alpha(n)}),(i=1,\cdots,n)$$

据此构造 S 的模拟过程如下:①S 首先生成 n 个公钥/私钥对 $V_1/S_1,\cdots,V_n/S_n$,以用于在模拟协议执行过程中的各参加方所使用的密钥,同时 S 接受 $(x_i,f_i(\bar{x}))$作为输入,并根据 $f_i(\bar{x})$的值选择数据 $\bar{x}'=(x'_1,x'_2,\cdots,x'_n)$,使得 $f_i(\bar{x})=f_i(\bar{x}')$;② 以 $\bar{x}'$为基础,S 模拟协议的执行过程并在执行协议中将获得一个 P_i 获得的加密过的集合

$$V_i(\alpha')=\{V_i(\alpha'_1),\cdots,V_i(\alpha'_m)\}$$

且令

$$S(x_i,f_i(\bar{x}))=(x_i,V_i(\alpha'_1),\cdots,V_i(\alpha'_m))$$

因为 $\alpha=\{\alpha_1,\alpha_2,\cdots,\alpha_m\}$和 $\alpha'=\{\alpha'_1,\alpha'_2,\cdots,\alpha'_m\}$起初都是随机产生的,每一步的修改也都是将某个随机数模乘上一个确定的值再进行加密,其结果仍然是随机的,而随机数是不可区分的,所以

$$\{V_i(\alpha_1),\cdots,V_i(\alpha_m)\}\triangleq\{V_i(\alpha'_1),\cdots,V_i(\alpha'_m)\}$$

故

$$\{(S(x_i,f_i(\bar{x})),f(\bar{x})\}\overset{c}{\equiv}\{v_i^{\pi}(\bar{x}),o^{\pi}(\bar{x})\}$$

3　结　论

本文研究了一种新的多方保密计算问题:对集合元素进行保密排序的问题,并提出了基于离散对数假设的解决方案,且用模拟范例证明了方案的保密性. 因为目前尚未见到有关报导,直接用百万富翁解决方案仍不能解决保密排序的问题,所以也没有办法同有关的方案进行性能比较.

参考文献:

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

[2] GOLDWASSER S. Multi-party computations: past and present [C]// Proceedings of the 16th Annual ACM Symposium on Principles of Distributed Computing. New York: ACM Press, 1997:21-24.

[3] CRAMER R, DAMGAARDL I. Introduction to secure multi-party computations [EB/OL]. [2005-12-10]. http://homepages.cwi.nl/~cramer/.

[4] GOLDREICH O, MICALI S, WIGDERSON A. How

to play ANY mental game [C]// Proceedings of the 19th Annual ACM Conference on Theory of Computing. New York: ACM Press, 1987:218-229.

[5] GOLDREICH O. Foundations of cryptography: basic applications [M]. London: Cambridge University Press, 2004.

[6] DU W LENLIANG, Atallah M J. Secure multi-party computation problems and their applications: a review and open problems [C]// Proceedings of New Security Paradigms Workshop. New York: ACM Press, 2001: 13-22.

[7] SUSILO W, SAFAVI R, GYSIN M, et al. A new and efficient fail-stop signature scheme[J]. The Computer Journal, 2000, 43 (5):430-437.

[8] SCHNEIER B. Applied cryptography, protocol, algorithm and source code in C [M]. New York: John Wiley & Sons Inc., 1996.

(编辑 苗凌)