姚氏百万富翁问题的原始协议

作者: 张志强 , 发表于 2019-03-09 , 共 1956 字 , 共阅读 1789 次

系列：机器统治世界
查看该系列所有文章

机器统治世界，其中一个重要的部分便是安全计算。而这一领域的开创性工作便是姚期智先生的「姚氏百万富翁问题」。相关的工作发表于 1982 年 FOCS 上的的《Protocols for secure computations》。

这个问题和文章我很早就听说过，但一直没看过。直到最近思考 机器统治世界 的问题时，才阅读了这篇论文。简单描述如下。

1、百万富翁问题

两个百万富翁，想知道谁的钱更多，但都不想让对方知道自己有多少钱。

2、姚的原始协议

Yao 在论文《Protocols for secure computations》里给了一个非常精妙的答案。

假设富翁甲的钱数为 a，富翁乙的钱数为 b，均满足 $1 \leq a, b \leq N$。乙有一个公钥私钥密码对 (E, C)，将公钥 E 发给甲，自己保留私钥 C。

第一步：

甲 取一个随机数 r，计算并发送 $x = E(r) - a$。

第二步：

乙收到 $x = E(r) - a$ 后，由于并不清楚 a 的值，只能枚举 $E(r) \in X = \{x+1, x+2, \cdots, x+N\}$。然后解密集合 X 里的所有数据：

$$R = \{C(x+1), C(x+2), \cdots, C(x+N)\} \tag{1}$$

乙知道 R 里面有一个是甲选择的 r，但不知道具体是哪个。

第三步：

乙取一个质数 p，将集合 R 里的数据改成：

$$R_p = \{C(x+i) \mod p \mid 1 \le i \le N\} \tag{2}$$

第四步：

保留 R_p 的前 b 项，后面的项增加 1，和 p 一起发送给乙。

最终甲收到的 N 个数分别为：

$$R_p^b = \{\delta_{i,b} + C(E(r) - a + i) \mod p \mid 1 \le i \le N\} \tag{3}$$

其中 $\delta_{i,b} = 1 \text{ if } i > b \text{ else } 0$。

第五步：

甲检查收到的第 a 个数，如果恰好等于 r，表示乙的 b 大于等于自己的 a。否则表示乙的 b 小于自己的 a。但甲无法获知准确的 b。

这里的第三步是关键，也是协议的神来之笔。缺少这一步，乙的 b 将被暴露，甲只需要解析：

$$\{E(\delta_{i,b} + C(E(r) - a + i)) \mid 1 \le i \le N\} \tag{4}$$

由于 $\forall y, E(C(y)) = y$，甲只需要将上面的序列和 $\{E(r) - a + i \mid 1 \le i \le N\}$ 比较即可知道 b 的大小。

一些中文参考资料：

- 密码学协议举例（四）：秘密数字的比较，对每一步都举了例子。
- 姚期智百万富翁问题的 python 演示 。

3、协议的缺陷

论文里的协议非常简单，因而优美。但一个很大的不足是它的复杂度是指数级别的，即在计算过程中需要传递指数级别的信息。注意，这里的指数级是相对于 $\log(N)$ 而言的，因为两个富翁的钱数可以用 $\log(N)$ 长度的数来表示。

姚先生的这篇论文的引用数超过 4000，无数人做了更进一步的工作。其中有一些多项式复杂度的协议（更准确地说，平方级复杂度）。不过思路更复杂，等有时间再写一下。

另外还有一个问题是协议是非对称的。在操作之后，富翁甲可以知道自己的钱和富翁乙的钱谁更多（但不知道富翁乙的具体钱数），但富翁乙一无所知。

Q. E. D.

0