安全计算协议

姚期智
加利福尼亚大学伯克利分校
翻译：李晓峰 (cy_lxf@163.com)
译文来自于经典文献翻译项目 https://gitee.com/uisu/InfSecClaT
译者单位：北京联合大学智慧城市学院

2021 年 12 月 14 日

摘要

此文是对姚期智老师 Protocols for secure computations 文章的翻译。

1 引言

2 安全计算的统一视图

3 确定性计算

3.1 百万富翁问题的解决方案

3.2 一般性问题的模型

Alice 有个秘密数 i，Bob 有个秘密数 j，假设 Alice 有一个公共单向函数 E_a，其逆函数是 D_a，逆函数只有 Alice 知道，对于 Bob 同样有函数 E_b, D_b，假设 E_a, E_b 相互独立并且是从 Q_N 中随机选取，Q_N 是 N 比特整数的 1-1 满射函数集合，下面我们精确地描述 Alice 和 Bob 如何通过协议 Λ 计算 $f(i,j)$。

Alice 和 Bob 交替给对方发送字符串。

Bob 每次发送完成，Alice 检查她所拥有的信息：

1、字符串序列 $\alpha_1, \alpha_2, \ldots, \alpha_t$

2、这些字符串之间的关系，比如 $E_b(\alpha_3) = \alpha_9$,α_8 有奇数个 1.
3、根据 Alice 和 Bob 至此已经传输过的比特，协议说明 Alice 如何计算隐私字符串 $\alpha_{t+1}, \alpha_{t+2}, \ldots, \alpha_s$, 此处每一个新的字符串 $\alpha_u, u \in \{t+1, \ldots, s\}$ 都是以前字符串的函数，或者说新字符串都是这样的形式 $E_a(y), E_b(y)$ 或 $D_a(y)$，此处 y 是 Alice 已经获得的字符串。A 随机选择使用哪个函数，例如，Alice 投币决定使用 $E(4)$ 或者计算 $\alpha_2 + 3\alpha_8$。
4、Alice 计算完后，她将发一个字符串给 Bob，选择发送哪个字符串也是随机的。

Bob 收到字符串后，他也按 Alice 的方法计算一些字符串，并且根据协议发送一个字符串。

Alice 和 Bob 达成一致，当收到一个特殊的字符时，协议执行结束，这时，协议有一条指令，就是每个参与者都秘密计算函数 f 的值，最后，在协议中，我们要求 Bob 和 Alice 计算 E 和 D 的数量受 $O(N^k)$ 的限制，此处 k 是一个事先选择好的整数。

隐私限制 (Privacy Constraint)

设 $\epsilon, \delta > 0$, $f(i,j)$ 函数值为 0 或 1，假定初始时所有 (i,j) 取值可能性都是一样的，并且假定 Bob 和 Alice 根据协议忠实第计算，最后 Alice 原则上可以根据她计算的函数值 v 和她拥有的字符串，计算 j 值的概率分布 $p_i(j)$. 一个协议如果满足以下条件，我们就说此协议满足 (ϵ, δ) 隐私限制：
1.$p_i(j) = \frac{1}{\|G_i\|}(1 + O(\epsilon)), j \in G_i$, 此处 G_i 是使 $f(i,j) = v$ 等式成立的所有 j 组成的集合，如果 $j \notin G_i$，则 $p_i(j) = 0$.
2. 如果 Alice 之后尝试执行更多计算计算 E 和 D，但计算的次数不超过 $O(N^k)$ 次, 那么她会以至少 $1-\delta$ 的概率仍然得到 j 上的上述概率分布。
3. 对于 Bob 也有以上同样要求.

Theorem 1 *对于任何 $\epsilon, \delta > 0$ 和任何函数 f, 存在一个用于计算 f 的协议满足 (ϵ, δ) 隐私限制。*

3.3 增加的需求

复杂性 (complexity)

文章中给出的百万富翁算法并不实用，因为决定 i,j 范围的 n 如果很大，那么传输的比特也会很多，因为传输的比特数与 n 是一个正比关系，那么一个有意思的问题就出现了：

对于满足 (ϵ, δ) 隐私限制的用于计算 f 的任一协议来说，所学传输的最小比特数是多少？

可以想象，在没有因私限制时，有一些函数很容易计算，但是当有额外的隐私限制时，就变得很不容易。幸运的是，我们可以证明事实并非如此。假设 Λ 是一个协议，当使用此协议时，Alice 和 Bob 之间传输的最大比特数记为 $T(\Lambda)$.

Theorem 2 设 $1 > \epsilon, \delta > 0$,*f(i,j)* 是一个 *0-1* 函数，如果 f 可以被一个规模为 *C(f)* 的布尔电路计算，那么这里就有一个计算 f 的协议 Λ 满足 (ϵ, δ) 隐私限制，并且 $T(\Lambda) = O(C(f) \log \frac{1}{\epsilon\delta})$.

事实上,如果 f 可以被一个图灵机在时间 S 内计算,那么这个协议可以被实现，以至于 Alice 和 Bob 都有图灵机算法来执行这个协议在 $O(S \log(\frac{1}{\epsilon\delta}))$.

相互怀疑的参与者 (Mutually-Suspecting Participants)

3.4 应用

4 概率计算

5 m 方情况的一般化描述

6 什么不能做