数据科学基础理论作业

曾文正 U201715853 自动化校际 1701

假设甲乙两人分别有一个N维实向量x，y（$N>2$），他们想计算两向量的内积$\langle x,y\rangle$，但不想让对方知道自己向量的信息，请设计一个机制来实现这个保证隐私的计算。

解：这里不考虑有第三方的存在，若想计算出两向量的内积又需要保密自己的信息，则需要加入一些不确定的、更高维的信息，然后利用向量分解和相互垂直的两向量内积为 0 的性质，推出一种可行的实现方法。

整个流程如下

（1） 甲告诉乙任意一个过自己向量 x 的平面α。

（2） 乙得知α后，计算出自己向量 y 在平面α上的投影$y_{/\!/}$，也即$y=y_{/\!/}+y_{\perp}$，其中$y_{/\!/}$在平面α内，而$y_{\perp}$垂直于平面α。

$$\begin{aligned} y_{/\!/} &= y - y_{\perp} \\ &= y - \|y\| \cdot \cos<y,n> \cdot n \\ &= y - (y \cdot n)n \end{aligned}$$

其中，n 为平面α的单位法向量。

（3） 乙把上一步计算得到的投影$y_{/\!/}$告诉甲，甲可以据此算出内积$\langle \boldsymbol{x},\boldsymbol{y}\rangle$

因为$y_{\perp}$垂直于平面α，且 x 在平面α内，故$x\perp y_{\perp}$，即$x\cdot y_{\perp}=0$

所以有：

$$\begin{aligned} x\cdot y &= x\cdot(y_{/\!/}+y_{\perp}) \\ &= x\cdot y_{/\!/}+0 \\ &= x\cdot y_{/\!/} \end{aligned}$$

（4） 甲通过计算得到内积$\langle \boldsymbol{x},\boldsymbol{y}\rangle$后将结果告诉乙，这样甲乙都知道了内积结果，计算完成。

下面来分析整个计算过程中双方各自的向量是否会泄露

（1） 乙知道的信息有 y、最终内积结果和过甲的向量 x 的一个平面α，一个平面无法推出 x,且这个平面中有无数个向量x'，满足$x'\cdot y_{/\!/}=x\cdot y$，因此即使知道内积结果也无法推出 x。因此乙无法根据已知信息推测出甲的向量 x。

（2） 甲知道的信息有 x、α、$y_{/\!/}$、内积结果，只知道 y 在α内的投影没法推出$y_{\perp}$，也推不出 y。因此甲也无法根据已知信息推测出乙的向量 y。

因此，整个计算过程中甲乙各自的信息不会泄露。