**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维实向量，（），他们想计算两向量的内积，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。
2. 乙得知后，计算出自己向量y在平面上的投影,也即,其中在平面内，而垂直于平面。



其中，n为平面的单位法向量。

1. 乙把上一步计算得到的投影告诉甲，甲可以据此算出内积

因为垂直于平面，且x在平面内，故，即

所以有： 

1. 甲通过计算得到内积后将结果告诉乙，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，一个平面无法推出x,且这个平面中有无数个向量，满足，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、、、内积结果，只知道y在内的投影没法推出，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。