**DP与机器学习**

Dwork 团队 2015 年提出应用差分隐私的想法可以解决机器学习的 over-fitting 问题，一步从隐私界跨到了 AI 界。她们的论文发表在了 2015 年的 Science 上：

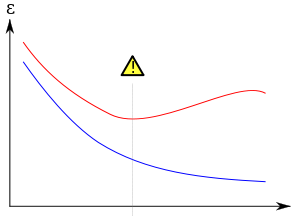
[The reusable holdout: Preserving validity in adaptive data analysis](http://science.sciencemag.org/content/349/6248/636)

**Overfitting（过拟合）：**

[**https://blog.csdn.net/Dream\_angel\_Z/article/details/48898817**](https://blog.csdn.net/Dream_angel_Z/article/details/48898817)

在统计学和机器学习中，overfitting一般在描述统计学模型随机误差或噪音时用到。它通常发生在模型过于复杂的情况下，如参数过多以致太适应当前数据而非一般情况等。overfitting会使得模型的预测性能变弱，并且增加数据的波动性。

当模型开始“memorize”训练数据而不是从训练数据中“learning”时(太适应训练数据)，overfitting就出现了



蓝色表示训练误差training error，红色表示validation error。当训练误差达到中间的那条垂直线的点时，模型应该是最优的，如果继续减少模型的训练误差（增加参数），这时就会发生过拟合，当增加的参数过多，就会产生过拟合。

*泛化能力（generalization ability）:机器学习算法对新鲜样本的适应能力。学习的目的是学到隐含在数据对背后的规律，对具有同一规律的学习集以外的数据，经过训练的网络也能给出合适的输出，该能力称为泛化能力*