

# 绪论

局限：随机数

As I have said so many times, God doesn't play dice with the world.

- A. Einstein

那妇人道：“不好，不好！我这里有一方手帕，你顶在头上，遮了脸，撞个天婚，教我女儿从你跟前走过，你伸开手扯倒那个就把那个配了你罢。”

邓俊辉

deng@tsinghua.edu.cn

# 就地随机置乱

❖ 任给一个数组  $A[0, n)$ ，理想地将其中元素的次序**随机**打乱

❖ //[R. Fisher & F. Yates, 1938], [R. Durstenfeld, 1964], [D. E. Knuth, 1969]

```
void shuffle( int A[], int n )  
    { while ( 1 < n ) swap( A[ rand() % n ], A[ --n ] ); }
```



❖ 策略：自后向前，依次将各元素与随机选取的某一先驱（含自身）交换

❖ 的确可以**等概率**地生成所有  $n!$  种排列？