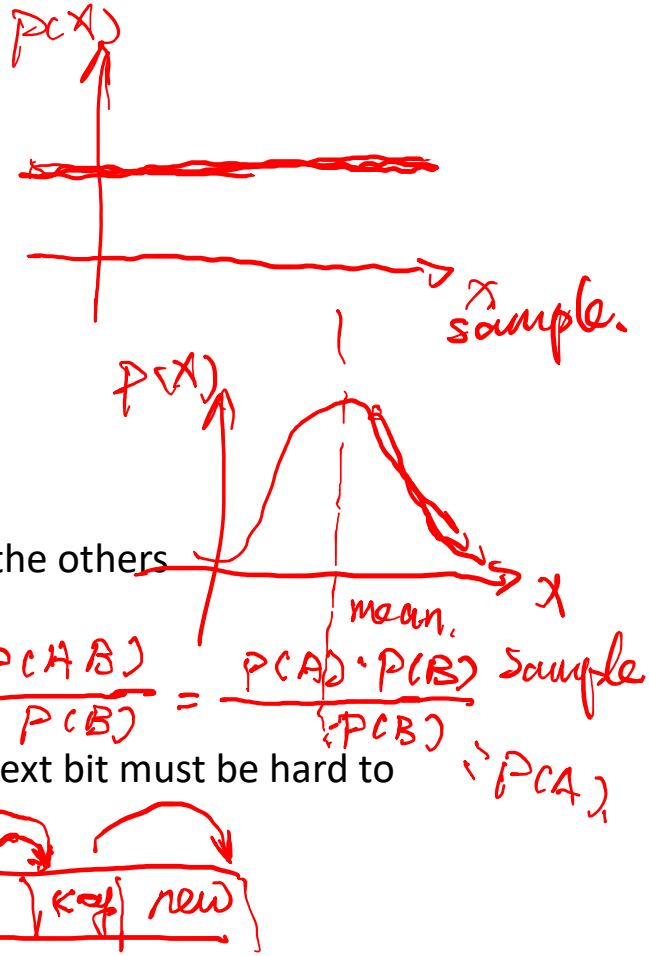
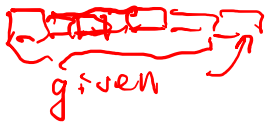
Properties of Random Numbers

- Randomness
  - Uniformity
    - distribution of bits in the sequence should be uniform
  - Independence
    - no one subsequence in the sequence can be inferred from the others
- Unpredictable
  - satisfies the "next-bit test“
    - given consecutive sequence of bits output (but not seed), next bit must be hard to predict



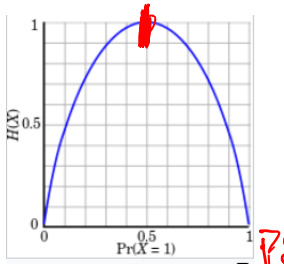


Entropy

- A measure of uncertainty
  - In other words, a measure of how unpredictable the outcomes are
  - High entropy = unpredictable outcomes = desirable in cryptography
  - The uniform distribution has the highest entropy (every outcome equally likely, e.g. fair coin toss)
  - Usually measured in bits (so 3 bits of entropy = uniform, random distribution over 8 values)

$$H = -\sum_i p_i \log_2 (p_i)$$

Entropy of an information source



Random data source

8 value

Value		max
1	→ 1/8	1/8
2	→ 0	1/8
3	→ 1/16	1/8
4	→ 1/4	1/8
5	→ 1/8	1/8
6	→ 3/16	1/8
7	→ 1/16	1/8
8	→ 3/16	1/8

given S1 — S2

8 value

$\frac{\#\,8}{\#\sum_{i=1}^{8}}$

$H = -\sum_i P_i \cdot \log_2 P_i$

$= -\left[\frac{1}{8}\cdot\log_2\frac{1}{8} + 0 + \frac{1}{16}\cdot\log_2\frac{1}{16} + \cdots + \frac{3}{16}\log_2\frac{3}{16}\right]$

$= -\left[-\frac{1}{8}\cdot 3 + 0 - \frac{1}{16}\cdot 4 - \frac{3}{4} - \frac{3}{8} - 0.45 - \frac{4}{16} - 0.45\right]$

$= 2.234$

$H = -\left[\frac{1}{8}\cdot\log_2\frac{1}{8}\right]\cdot 8$

$= -\left[\frac{1}{8}(-3)\right]\cdot 8 = 3$

uniform

$\max_{P_i} -\sum_i P_i \log_2 P_i$

$\sum_{i=1}^{n} P_i = 1$

Lagrange multiplier

$y = -\sum_i P_i \log_2 P_i + \lambda\left[\sum_{i=1}^{n} P_i - 1\right]$

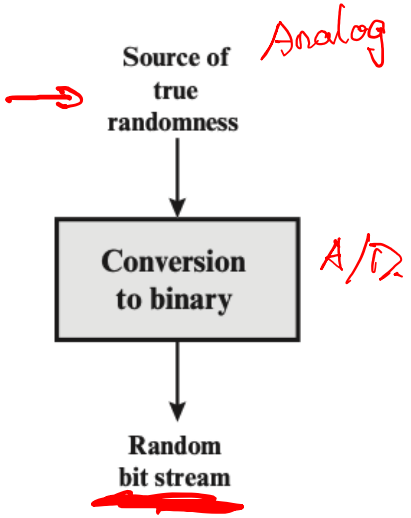
$\frac{\partial y}{\partial P_i} = \cdots = 0$

$\lambda =$

$P_i = \frac{1}{n}$

True random numbers generators

- Several sources of randomness – natural sources of randomness
  - decay times of radioactive materials
  - electrical noise from a resistor or semiconductor
  - radio channel or audible noise
  - keyboard timings
  - disk electrical activity
  - mouse movements
  - Physical unclonable function (PUF)
- Some are better than others



(a) TRNG