COMP20007 Design of Algorithms Semester 1 2016

Secret Sharing

Suppose you want to hide a secret s

- It might be a number or a string of bits
- Can you give *a,b* to two other people so that
  - Neither person alone has any information about s
    - *a or b* alone reveals nothing
  - But both people working together can find s
    - Some computation on *a, b* recovers s

  - Ans: give one person rand r.
  - Give the other person r XOR s (bitwise).
  - Recover s by computing r XOR (r XOR s)

  - Think of s as a number in range [0,n-1].
  - Give one person r in the range *** and n
  - Give the other person s + r mod n *** and n
  - Recover s by computing (s+r) – r mod n

Can you generalize?

- Can you give $a_1, a_2, \ldots, a_n$ to n other people so that
  - n-1 people have no information about s
  - But all n people working together can find s
    - Some computation on $a_1, a_2, \ldots, a_n$ recovers s
  - ?

A different generalization?

- Can you give $a_1, a_2, \ldots, a_n$ to n other people so that
  - One person alone has no information about s
  - But any 2 people working together can find s
    - Some computation on any pair (a_i, a_j) recovers s
  - ?

(Shamir or Blakeley) Secret sharing

- Give each person a point (i, ai+s) for fixed a
  - $i=1, \ldots, n$
  - One person alone has no information about x
  - But any 2 people working together can find x
    - Some computation on any pair (a_i, a_j) recovers x
  - ?