$(t,w)$ Threshold schemes

- A master key $K$ (e.g. for a Certificate Authority) is very very sensitive to exposure or loss
  - exposure makes the whole system untrustable
  - loss makes system inaccessible
    - extra copies increases vulnerability
- Solution: split $K$ into $w$ shadows $K_1,...,K_w$ s.t.
  - with $t$ shadows, $K$ can be recovered
  - with fewer than $t$, $K$ can not be recovered
- Give the $w$ shadows to different users
  - exposure of fewer than $t$ shadows OK
  - loss of fewer than $w-t$ shadows OK
Shamir threshold scheme

- Use a random, secret, polynomial of degree \( t-1 \)
  
  \[ h(x) = (a_{t-1}x^{t-1} + \cdots + a_1x + a_0) \mod p \]
  
  - where \( a_0 = K, \ p > K, \ p > w, \ p \ \text{prime} \)

- \( K = h(0) \)
  
  \[ K_i = h(x_i) \text{ for } i \in [1, w], \ x_i \text{ distinct and not secret} \]

- Each pair \((x_i, K_i)\) is a point on the curve \( h(x) \)
  
  - \( t \) points uniquely determine a polynomial of degree \( t-1 \)
  
  - \( h(x) \) and thus \( K \) can be reconstructed by \( t \) shadows but not fewer
Shamir thresholds (cont)

• Given $t$ shadows $K_{i_1},..., K_{i_t}$, $h(x)$ is reconstructed
  e.g. by the Lagrange polynomial
  
  $$ h(x) = \sum_{s=1}^{t} K_{i_s} \prod_{j=1, j\neq s}^{t} \frac{(x-x_{i_j})}{(x_{i_s}-x_{i_j})} \mod p $$

• Since arithmetic is in $\mathbb{Z}_p$, division is by inverses
  mod $p$ and multiplication.

• Features:
  
  – More shadows: compute $h(x)$ for a new $x$
  – Retract shadows: use a new polynomial with same $K$
  – Users may have more than one shadow (president)

• Other threshold schemes exist.
Oblivious transfer

• A and B want to flip a coin by computer:
  – A picks two large primes $p,q$ and sends $n=pq$ to B
  – B picks a random $x<n$ s.t. $\gcd(x,n)=1$, and sends $a=x^2\mod n$ to A
  – A computes (by Chinese Remainder Remainder Theorem) four roots of $a$ and sends one randomly chosen to B
  • these are $x$, $n-x$, $y$, $y-n$, but A does not know $x$
  – If B receives $y$ or $y-n$ he can find $p$ and $q$ by computing $\gcd(x+y,n)=p$ or $q$. Otherwise he cannot.
  – B wins if he can factor $n$.

• Can be used in contract signing protocols.