Admin:

Project one-pager due today

Today:

Shamir's secret-sharing

Reading:

Shamir paper (1979)

Smart Chapter 19
Key management

Start with "secret sharing" (threshold cryptography).

- Assume Alice has a secret $s$, (e.g. a key)
- She wants to protect $s$ as follows:
  
  She has $n$ friends $A_1, A_2, \ldots, A_n$
  
  She picks a "threshold" $t$, $1 \leq t \leq n$.
  
  She wants to give each friend $A_i,$
  
  a "share" $s_i$ of $s$, so that
  
  - any $t$ or more friends can reconstruct $s$
  - any set of $< t$ friends can not.

Easy cases:

- $t = 1$: $s_i = s$
- $t = n$: $s_1, s_2, \ldots, s_{n-1}$ random
  
  $s_n$ chosen so that
  
  $s = s_1 \oplus s_2 \oplus \cdots \oplus s_n$

What about $1 < t < n$?

Also see bitcoin "multisig" as motivation
Shamir's method ("How to Share a Secret", 1979)

Idea: 2 points determine a line
3 points determine a quadratic
... 
$t$ points determine a degree $(t-1)$ curve

Let $f(x) = a_{t-1} x^{t-1} + a_{t-2} x^{t-2} + ... + a_1 x + a_0$

There are $t$ coefficients. Let's work modulo prime $p$.

We can have $t$ points: $(x_i, y_i)$ for $1 \leq i \leq t$

They determine coefficients, and vice versa.

**Polynomial Evaluation**

\[ \{(x_i, y_i)\} \rightarrow (a_{t-1}, a_{t-2}, ..., a_1, a_0) \]

**Polynomial Interpolation**

Pt/Value pairs \rightarrow Coefficients

To share secret $s$ (here $0 \leq s < p$):

Let $y_0 = a_0 = s$

Pick $a_1, a_2, ..., a_{t-1}$ at random from $\mathbb{Z}_p$

Let share $s_i = (i, y_i)$ where $y_i = f(i)$, $1 \leq i \leq n$.

Evaluation is easy.
Interpolation

Given \((x_i, y_i)\) \(1 \leq i \leq t\) (wlog)

Then \(f(x) = \sum_{i=1}^{t} f(x) \cdot y_i\)

where \(f_i(x) = \begin{cases} 1 & \text{at } x = x_i \\ 0 & \text{for } x = x_j, j \neq i, 1 \leq j \leq t \end{cases}\)

Furthermore:

\[ f_i(x) = \frac{\prod_{j \neq i} (x - x_j)}{\prod_{j \neq i} (x_i - x_j)} \]

This is a polynomial of degree \(t-1\).
So \(f\) also has degree \(t-1\).

Evaluating \(f(0)\) to get \(s\) simplifies to

\[ s = f(0) = \sum_{i=1}^{t} y_i \cdot \frac{\prod_{j \neq i} (-x_j)}{\prod_{j \neq i} (x_i - x_j)} \]

Theorem: Secret sharing with Shamir’s method is information-theoretically secure. Adversary with \(< t\) shares has no information about \(s\).

Proof: A degree \(t-1\) curve can go through any point \((0, s)\)

as well as any given \(d \notin t\) pts \((x_i, y_i)\), if \(d < t\).

Refs: Reed-Solomon codes, erasure codes, error correction, information dispersal (Rabin).