# Secret-Sharing Schemes

Jim Royer

*Introduction to Cryptography*

October 16, 2018



## References

- *Secret Sharing* on Wikipedia,
  https://en.wikipedia.org/wiki/Secret_sharing
  *(The graphics on the last page come from this article.)*
- *Secret-Sharing Schemes: A Survey* by Amos Beimel,
  https://www.cs.bgu.ac.il/~beimel/Papers/Survey.pdf



## Secret Splitting

### Problem

- I want to send Alice and Bob a message $m \in \mathbb{Z}_n$.
- But I want to be sure that the only way Alice and Bob can read $m$ is if they both agree to unlock the message.

### Solution: Split the Message

Pick $r \overset{\text{ran}}{\in} \mathbb{Z}_n$.
Send Alice $r$.
Send Bob $(m - r) \bmod n$.

- Why does this work?
- How can we generalize this to $k$ people?



## Shamir's Threshold Scheme, I

### Problem

Suppose $1 < t \leq k$. *("t" for threshold.)*
We want to split a secret $m \in \mathbb{Z}_n$ among $k$ people so that:

- If any $t$ of them agree to open the secret, they can.
- *But*, if only $t' < t$ of then agree, they cannot.
- *(Think secret bank account numbers, launch codes, etc.)*

### The Shamir Threshold Scheme: Basic Ideas

- $t$ points determine a $(t - 1)$-degree polynomial $s$.
- Distribute points $(x, s(x))$ where $x \neq 0$.
- Make $s(0) = m$.

## Shamir's Scheme, II

- Setup
  Pick a prime $p$ larger than any possible message.
- Encoding the Message
  Choose $s_1, \dots, s_{t-1} \overset{\text{ran}}{\in} \mathbb{Z}_p$ with $s_{t-1} \neq 0$.
  Set $s(x) =_{\text{def}} m + s_1 x + s_2 x^2 + \cdots + s_{t-1} x^{t-1} \pmod p$.
- Distributing the Secret
  Pick distinct $x_1, \dots, x_k \overset{\text{ran}}{\in} \mathbb{Z}_p^*$.
  For $i = 1, 2, \dots, k$:
  Send the $i^{th}$ person $(x_i, y_i)$, where $y_i = s(x_i)$.
- Unlocking the Secret
  - $t$ folks get together with shared info: $(x_1, y_1), \dots, (x_t, y_t)$.
  - $t$ points uniquely determine a $(t-1)$-degree polynomial.
  - Q: But how do you reconstruct the polynomial?



## Unlocking the Secret, Version 1

Q: How do you reconstruct the polynomial from the shared information $(x_1, y_1), \dots, (x_t, y_t)$?

- We know that, for each $j = 1, \dots, t$:
  $y_j = m + s_1 \cdot x_j^1 + s_2 \cdot x_j^2 + \cdots + s_{t-1} \cdot x_j^{t-1} \pmod p$.
- So we solve the following for $m, s_1, \dots, s_{t-1}$:

$$\begin{pmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{t-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{t-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_t & x_t^2 & \dots & x_t^{t-1} \end{pmatrix} \begin{pmatrix} m \\ s_1 \\ \vdots \\ s_{t-1} \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_t \end{pmatrix}$$

The above is the Vandermonde matrix, $V$.
Fact: $\det V = \prod_{1 \le i < j \le t} (x_j - x_i)$.
$\therefore$ $\det V \equiv 0 \pmod p$ iff $x_i = x_j$ for some $i \neq j$.



## Unlocking the Secret, Version 2

Q: How do you reconstruct the polynomial from the shared information $(x_1, y_1), \dots, (x_t, y_t)$?

- For each $i \in \{1, \dots, t\}$, let:

$$X_i =_{\text{def}} \{1, \dots, t\} - \{i\}. \qquad \ell_i(x) =_{\text{def}} \prod_{j \in X_i} \left( \frac{x - x_j}{x_i - x_j} \right) \bmod p.$$

- Note: $\ell_i(x_i) = 1$.
- Note: $\ell_i(x_j) = 0$ when $i \neq j$.

### The Lagrange Interpolation Polynomial

$$q(x) = \sum_{i=1}^{t} y_i \cdot \ell_i(x) \qquad \leftarrow \textit{degree } t-1$$

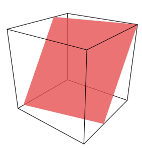
- Note $q(x_i) = y_i$ for $i = 1, \dots, t$. *(Why?)*

$$\therefore\ s(x) = q(x) \text{ and } m = \sum_{i=1}^{t} y_i \prod_{j \in X_i} \left( \frac{-x_j}{x_i - x_j} \right) \pmod p.$$

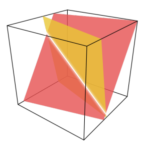


## Blakley's Secret-Sharing Scheme

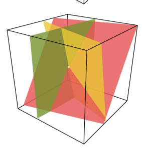
$k$ participants, $t$ to unlock.



- Basic Ideas for $t = 3$
  - Go 3D.
  - Give each person a plane such that any three planes share only a single point $= (M, y, z)$.



- Setup
  - $p$, a prime
  - $x_0 \leftarrow$ the secret ($\in \mathbb{Z}_p$)
  - $Q \leftarrow (x_0, y_0, z_0)$ where $y_0, z_0 \overset{\text{ran}}{\in} \mathbb{Z}_p$.



- For Each Person
  - Choose $a, b \overset{\text{ran}}{\in} \mathbb{Z}_p$
  - Compute $c \equiv z_0 - a \cdot x_0 - b \cdot y_0 \pmod p$
    $z = a \cdot x + b \cdot y + c$ is a plane.
- For $t > 3$, Go to $t$-Dimensions.