How to share a secret

A paper by Adi Shamir

Presentation by Prajna Puranik

Introduction

- Secret sharing involves:
  - Distributing a secret among a group
  - No individual holds any intelligible information about the secret
  - When a sufficient number of individuals combine their shares, secret reconstructed

- Shamir's secret sharing property: Information theoretic security
  - An adversary without enough shares cannot reconstruct the secret even with infinite time and computing capacity.

Objective of Shamir's paper

Show how to divide data D into *n* pieces in such a way that:

- D is easily reconstructable from any *k* pieces
- But complete knowledge of k - 1 pieces reveals absolutely no information about D

(k, n) threshold scheme

Goal: Divide data D into n pieces $D_1, D_2, \ldots D_n$ such that:

- Knowledge of any k or more D_i pieces makes D easily computable
- Knowledge of any k- 1 or fewer D_i pieces leaves D completely undetermined -> in the sense that all its possible values are equally likely

Such a scheme is called a (k, n) threshold scheme.

N = no of participants/number of pieces of secret

k= number of people that need to cooperate to get the secret

Need for (n,k) threshold scheme

Useful in management of cryptographic keys

- To protect data → encryption
- To protect encryption key ?
- Keeping the key in a single, well-guarded location → unreliable
- Possible solution → store multiple copies of the key at different locations → dangerous
- Best solution → (n,k) threshold scheme

Very robust key management scheme:

- Adversary cannot reconstruct the key even when security breaches expose k- 1 of the remaining k pieces.

Example

A company that digitally signs all its checks

- Each executive given a copy of the company's secret signature key → convenient but easy to misuse
- Cooperation of all the company's executives is needed to sign each check → Safe but inconvenient.
- Solution: Require at least three signatures per check
    - Easy to implement with a (3, n) threshold scheme.
    - Each executive is given a small magnetic card with one piece of the secret
    - Company's signature generating device accepts any 3 to generate a temporary copy of the actual signature
    - An unfaithful executive must have at least two accomplices in the company

Suitability of threshold scheme

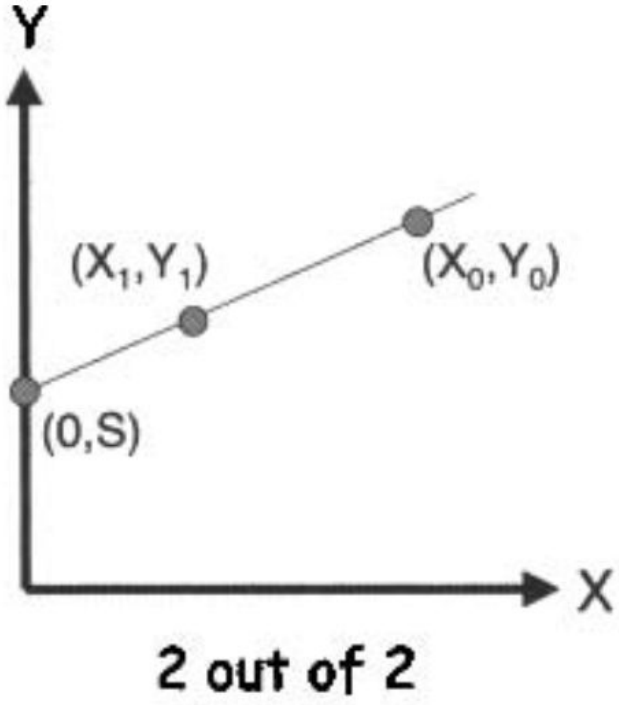
Threshold schemes are ideally suited to applications in which a group of mutually suspicious individuals with conflicting interests must cooperate.

Ideally we would like the cooperation to be based on mutual consent, but the veto power this mechanism gives to each member can paralyze the activities of the group.

By properly choosing the k and n parameters we can give any sufficiently large majority the authority to take some action while giving any sufficiently large minority the power to block it.

Mathematics behind secret sharing

- Suppose the secret S is a real number
- Alice and Bob want to share this secret
- Draw a line L in the plane through the point (0, S)
- Give Alice a point A = (X_0, Y_0) on L and give Bob another point B = (X_1, Y_1) on L
- Alice/Bob individually have no information about S since an infinite number of lines pass through a single point.
- Together A and B uniquely determine L
- Determining L => finding y-intercept, and hence the value S



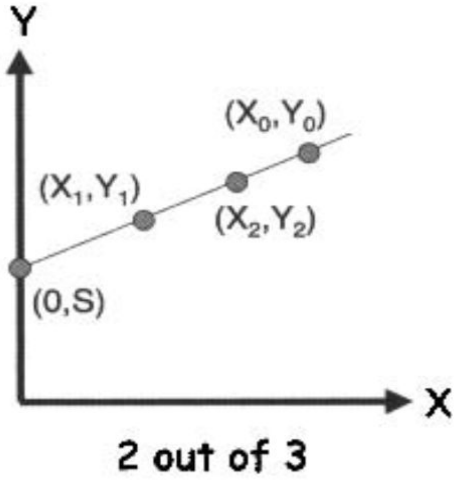
Line → polynomial of degree one → uniquely determined by two points

Parabola → polynomial of degree two → uniquely determined by three points.

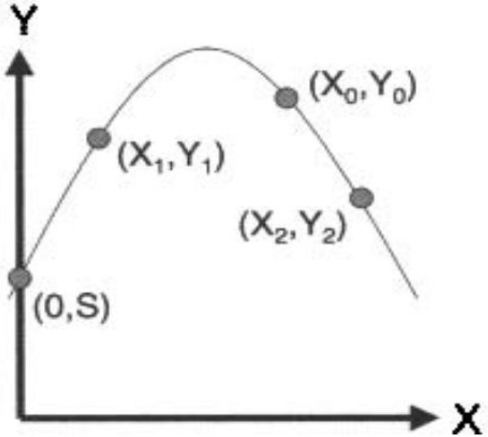
=> a polynomial of degree m - 1 is uniquely determined by m points

For example:

- Only one line can be drawn between two points
- Only one possible parabola crosses through the same three points
- Only one cubic curve passes through the same four points



2 out of 3



3 out of 3

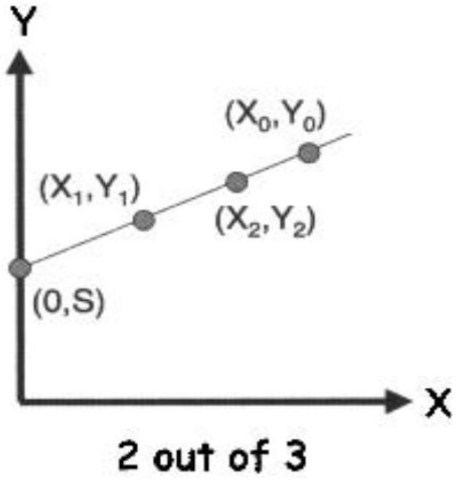
Polynomial interpolation

A polynomial of degree m - 1 is uniquely determined by m points

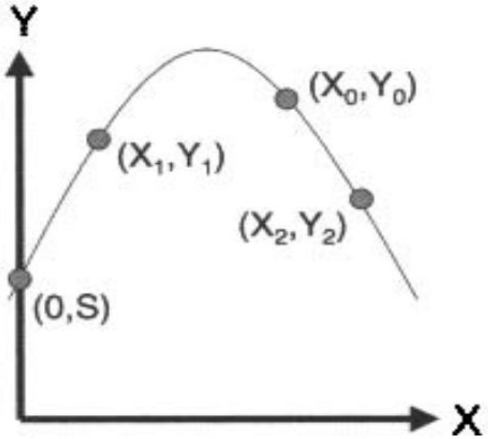
This fact allows us to construct an **m out of n** secret sharing scheme for any m <= n

- n is the number of participants
- any m of which can cooperate to recover the secret.

Given k points in the 2-dimensional plane (x_1,y_1) ..... (x_k, Y_k) with distinct x_i , there is one and only one polynomial q(x) of degree k - 1 such that $q(x_i) = y_i$ for all i



2 out of 3



3 out of 3

Polynomial interpolation for secret sharing

- If n = number of shares and k = threshold
- Choose polynomial P with degree k-1
- Encode our secret as a coefficient of P
- Evaluating P at n points
- Given data = D, we need to divide it into D_i pieces
- Steps:
    - Select a random k-1 degree polynomial $q(x) = a_0 + a_1(x) + a_2(x^2)+....+a_{k-1}(x^{k-1})$ in which $a_0 = D$
    - Evaluate: $D_1 = q(1)$ ....$D_i = q(i)$ ..... $D_n = q(n)$
- Given any subset of k of these D_i values, we can find the coefficients of q(x) by interpolation, and then evaluate D=q(0).
- Knowledge of just k- 1 of these values does not suffice in order to calculate D.

Example

Secret S = 1954 with 4 (n) shares and a threshold of 3 (k)

1) Randomly choose k - 1 positive integers = 2 positive integers

   Assume 2 positive integers are 43 and 12

2) Build a polynomial of the form $q(x) = a_0 + a_1(x) + a_2(x^2)+....+a_{k-1}(x^{k-1})$ where a_0 is the secret

   We get polynomial $q(x) = a_0 + a_1(x) + a_2(x^2)$ where a_1 and a_2 are our randomly chosen integers.

Resulting polynomial: $y = 1954 + 43x + 12x^2$

3) Use this formula to create 4 points (shares) that we give to each participant

Share 1

$y = 1954 + 43*1 + (12*1)^2$

$y = 2009$

Point 1 = (1, 2009)

Share 2

$y = 1954 + 43*2 + (12*2)^2$

$y = 2088$

Point 2 = (2, 2088)

Share 3

$y = 1954 + 43*3 + (12*3)^2$

$y = 2191$

Point 3 = (3, 2191)

Share 4

$y = 1954 + 43*4 + (12*4)^2$

$y = 2318$

Point 4 = (4, 2318)

One share is given to one participant

K = 3 so choose polynomial of degree 2 => parabola

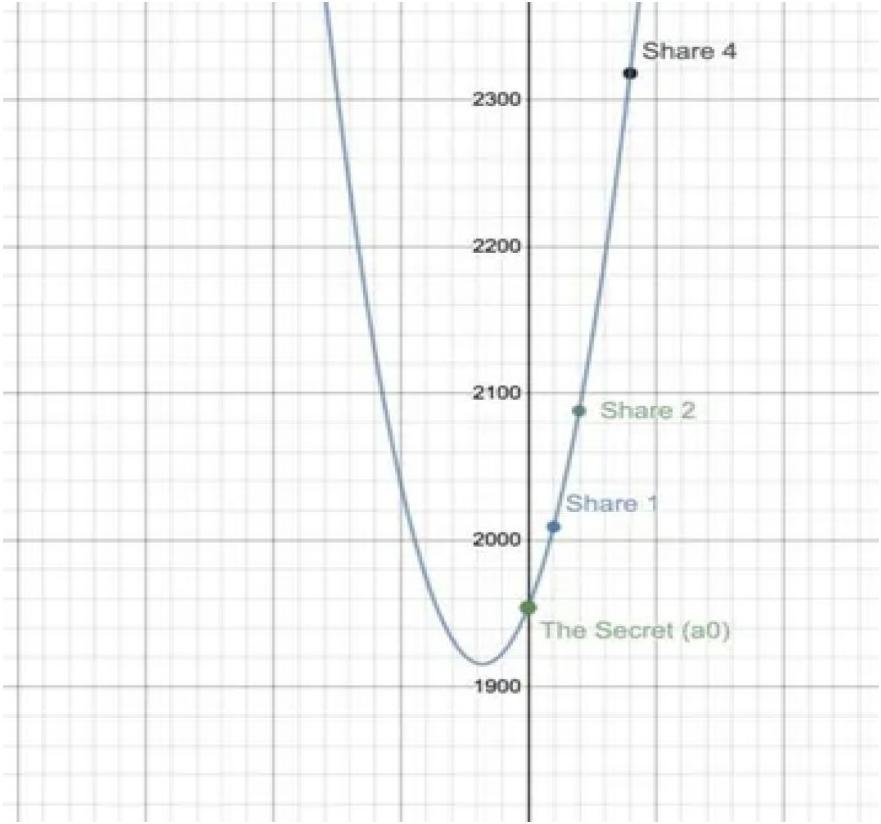
If we use three points, we can draw a parabola and calculate a_0 (the secret).

Let's assume we have control of shares 1, 2, and 4.

Step 1 - Plot the points (shares) that we control

Step 2 - Draw the corresponding parabola

Step 3 - Find the point where x=0. It's y value is the secret



Advantages of shamir secret sharing

- The size of each piece does not exceed the size of the original data
- When k is kept fixed, D_i pieces can be dynamically added or deleted without affecting the other D_i pieces
- It is easy to change the D_i pieces without changing the original data
    - All we need is a new polynomial q(x) with the same free term.
    - A frequent change of this type can greatly enhance security
- Allows a hierarchical scheme → number of pieces needed to determine D depends on their importance
        - A company's president can have 3 shares
        - Each vice-president two shares
        - Each executive has one share
        - (3, n) threshold scheme enables checks to be signed either by any three executives, or by any two executives one of whom is a vice-president, or by the president alone.

Thank you!

Primary paper: Shamir, Adi (1979), "How to share a secret", Communications of the ACM, 22 (11): 612–613, doi:10.1145/359168.359176

Reference: https://blog.boot.dev/cryptography/shamirs-secret-sharing/