Part I

Secret Sharing Schemes

Threshold Secret Sharing

Suppose a dealer knows a secret m and wants to share it among w players so that a minimum number of $t \leq w$ players must collaborate to reconstruct the secret m. Such a system is called (w, t)-threshold scheme.

Trivial schemes are:

- $t = 1$, in which the dealer gives m to all the players.
- $t = w$, in which all the players must cooperate (also called *secret splitting*).

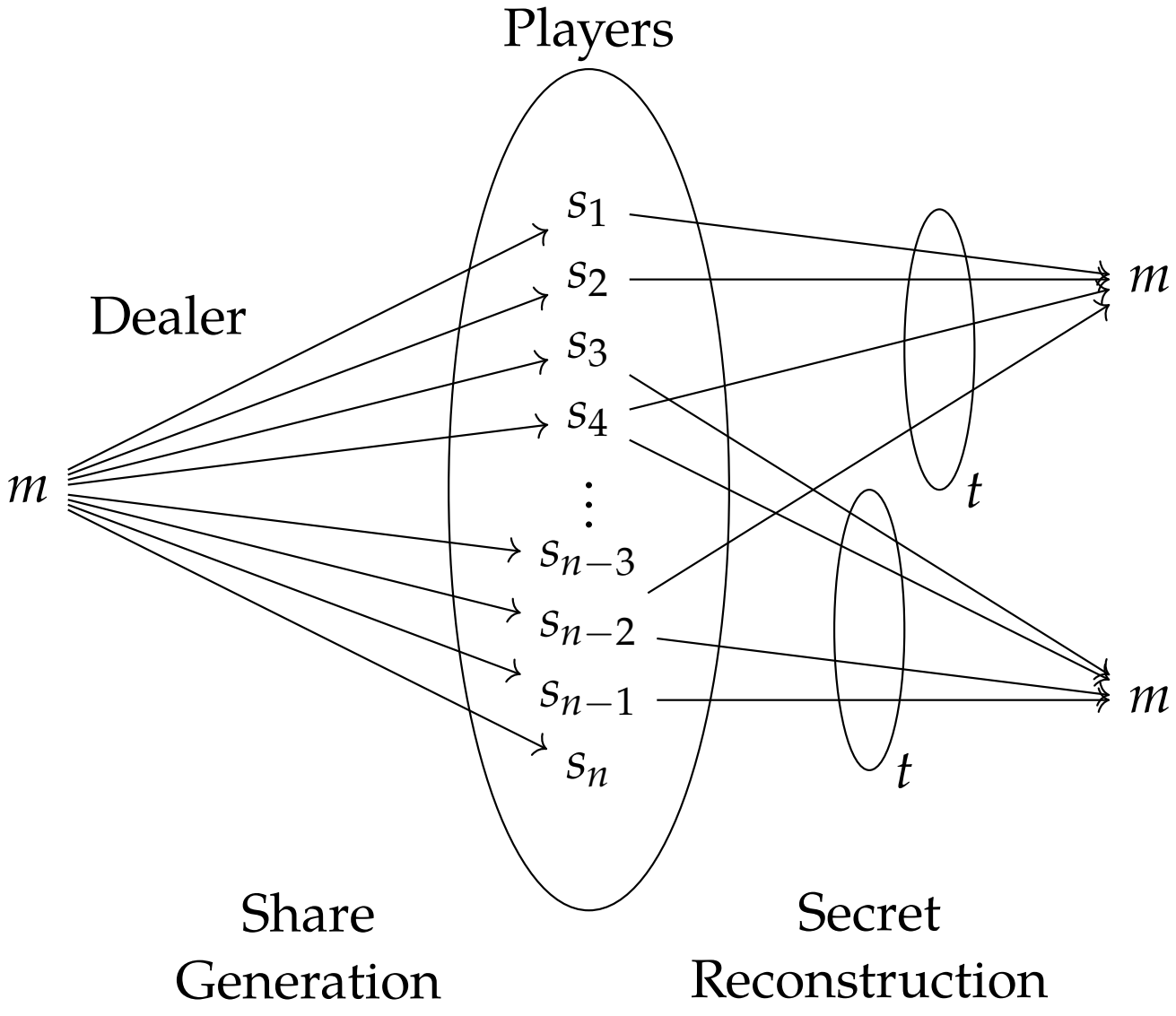
Primitives

Share Generation splits a secret m into n shares $s_1, \ldots, s_n$.

Secret Reconstruction joins any t distinct shares into a secret m.

Security model is all-or-nothing. Any set of fewer than t shares gives no information on m.

Threshold Secret Sharing



1. Secret Sharing Schemes

- Secret Splitting
- Threshold Schemes
- Exercises

Secret Splitting

Secret Splitting is the easiest form of secret sharing. The secret m is divided among w parties and all of the shares are required to recover the secret.
Consider the case of two parties: Alice and Bob. The solution is simple:

- give Alice a random number r and
- give Bob $m - r$.

To recover the secret, Alice and Bob sum their shares.

There is a problem: it is impossible to choose r so that the Alice's and Bob's shares are uniformly distributed over all possible numbers.

Secret Splitting with two Parties

The solution is using modular arithmetic.

procedure SETUP
    Choose integer n larger than any possible secret
end procedure

procedure GENERATESHARE(m) ▷ m is the secret
    Choose r from $\mathbb{Z}_n$ uniformly at random
    Give Alice $s_A = r$
    Give Bob $s_B = m - r \bmod n$
end procedure

function RECONSTRUCTSECRET(s_A, s_B)
    return $s_A + s_B \bmod n$
end function

Secret Splitting

Secret splitting with two parties is the same as a One Time Pad. Alice receives the key and Bob receives the encrypted message. Proof of security is trivial: the key alone, or the encrypted message alone give no information.

Secret Splitting with Multiple Parties

The algorithm can be extended to any number of parties

procedure SETUP
  Choose integer n larger than any possible secret
  Let w be the number of players
end procedure
procedure GENERATESHARE(m) ▷ m is the secret
  Choose $r_1, r_2, \ldots, r_{w-1}$ randomly in $\mathbb{Z}_n$
  Give player i the share $s_i = r_i$, with $1 \leq i \leq w-1$
  Give player w the share $s_w := m - \sum_{i=1}^{w-1} r \bmod n$
end procedure
function RECONSTRUCTSECRET($s_1, \ldots, s_w$)
  return $\sum_{i=1}^{w} s_i \bmod n$
end function

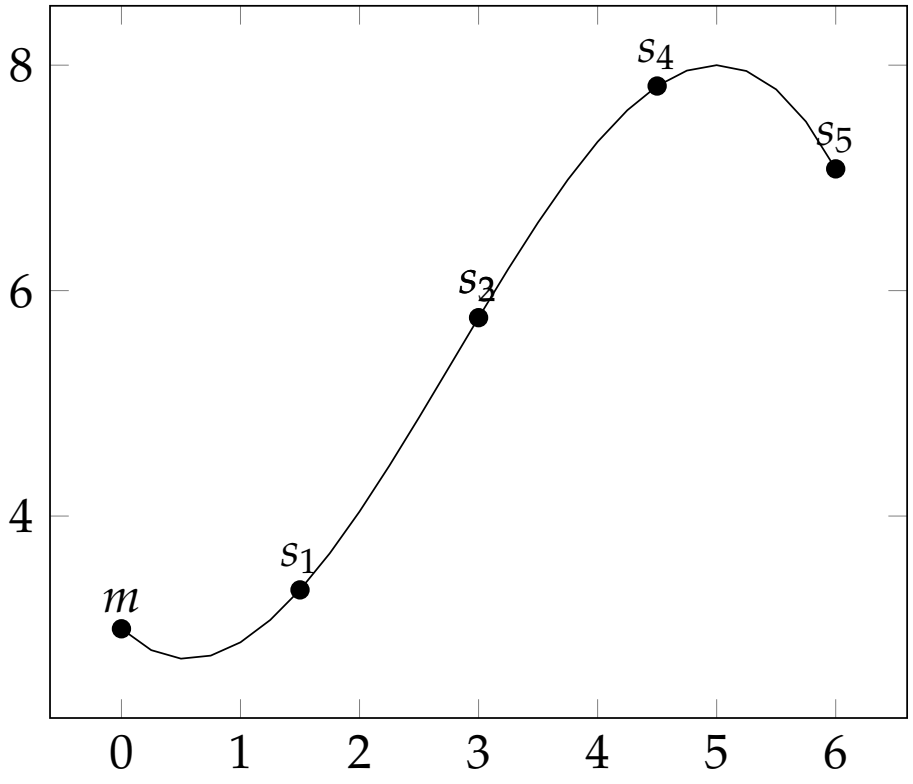
1. Secret Sharing Schemes

- Secret Splitting
- Threshold Schemes
- Exercises

Shamir Secret Sharing Scheme

Shamir's Scheme is a (w, t) scheme based on an extension of elementary algebra concepts, i.e. that at least 2 points are necessary to determine a line, 3 for a parabola, ...

$f(x)$ polynomial with degree $t - 1$



Shamir Secret Sharing

procedure SETUP

Choose a public prime number $p > w$ and larger than any possible secret.

Publish p

end procedure

procedure GENERATESHARE(m) ▷ m is the secret

Choose $r_1, r_2, \ldots, r_{t-1}$ randomly in $\mathbb{Z}_p$

Define the secret polynomial

$$s(x) = m + r_1 x + \cdots + r_{t-1} x^{t-1} \bmod p$$

Choose w distinct integers $x_1, \ldots, x_w$.

Give to player i the pair $(x_i, s(x_i))$ for $1 \leq i \leq w$.

end procedure

Shamir Secret Sharing

Secret Recovery

There are different algorithms with different complexity. The following algorithm is simple but has complexity $O(t^3)$.
We collect any t distinct shares $(x_1, y_1), \ldots, (x_t, y_t)$ and write a system of equations with unknowns $m, s_1, \ldots, s_{t-1}$.
Calling $s_0 = m$, we can write

$$\begin{pmatrix} 1 & x_1 & \ldots & x_1^{t-1} \\ 1 & x_2 & \ldots & x_2^{t-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_t & \ldots & x_t^{t-1} \end{pmatrix} \begin{pmatrix} s_0 \\ s_1 \\ \vdots \\ s_{t-1} \end{pmatrix} = \begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ y_{t-1} \end{pmatrix} \mod p$$

Solving for the s_i gives the secret polynomial.

Shamir Secret Sharing

Secret Recovery

We want to be sure that the system always has a one and only one solution.

A matrix in which the column are in a geometric progression is called a Vandermonde matrix. The determinant of a Vandermonde matrix is non-zero if and only if all the x_t are distinct mod p.
This happens if we choose t distinct shares.

If we have duplicate shares, the determinant is zero and the solution is not unique. However, for each possible value of m' of the secret, there is exactly one polynomial that fits the available shares plus $(0, m')$. Therefore, we claim that any set of fewer than t shares gives no information about m.

Dishonest parties

A dishonest party provides the other parties with false shares. There are some extensions of the secret sharing schemes dealing with such parties.

For the dishonest dealer, we have verifiable secret sharing, VSS. In VSS the dealer publishes a commitment to the secret polynomial. The players can verify that all the shares come from the same polynomial without disclosing the share.

For the dishonest player, we have robust secret sharing, RSS. In RSS, the secret can be reconstructed even if one or more players provide a false share.

Facts about Robust Secret Sharing

Shamir Secret Sharing can be made robust if reconstruction is done using the Berklekamp-Welch algorithm. For each false share it is necessary to have two additional correct shares. SSS is robust for any $t < w/3$, while no robust scheme exists for $t \geq w/2$. Various schemes exist for the intermediate cases.

1. Secret Sharing Schemes

- Secret Splitting
- Threshold Schemes
- Exercises

Exercise

Suppose you have a secret, the number 5. You want to design a system in which each of four users A, B, C, and D have a share of the secret. The collaboration of two parties is necessary to compute the secret, while each single party cannot. Describe the system and tell the numeric value of each share.

Solution

We need a $(2, 4)$-threshold sharing scheme. Choose a prime p larger than the number of parties (4) and than the secret (5). We choose $p = 7$.
Define the first degree random polynomial

$$s(x) \equiv 5 + 2x \pmod 7$$

Then the shares are:

$$A \leftarrow s(1) = 0 \qquad B \leftarrow s(2) = 2$$
$$C \leftarrow s(3) = 4 \qquad D \leftarrow s(4) = 6$$

Exercise

We have prepared a $(2, 30)$-Shamir's threshold scheme working mod 101. Two of the shares are $(1, 13)$ and $(3, 12)$. Another person has the share $(2, *)$, where the second number is unreadable. What is the value of $*$?

Solution

We need to recover the polynomial $s(x)$.

$$\begin{pmatrix} 1 & 1 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} m \\ s_1 \end{pmatrix} \equiv \begin{pmatrix} 13 \\ 12 \end{pmatrix} \pmod{101}$$

Then

$$\begin{pmatrix} m \\ s_1 \end{pmatrix} \equiv 2^{-1} \begin{pmatrix} 3 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 13 \\ 12 \end{pmatrix} \equiv \begin{pmatrix} 64 \\ 50 \end{pmatrix} \pmod{101}$$

The polynomial is $s(x) \equiv 64 + 50x$.

Therefore the missing share is $s(2) = 63$.

Exercise

In a Shamir scheme, the secret is the constant term in a polynomial with degree 4 mod 1093. Suppose that three persons have the shares $(2, 197)$, $(4, 874)$, and $(13, 547)$.
What are the possible values for the secret?

Solution

The secret could be any element of $\mathbb{Z}_{1093}$. In fact, for any secret m, there exists a fourth degree polynomial that fits the data.

Exercise

A key distribution scheme uses a $(2, 20)$-threshold scheme for distributing to 20 participants the combination for a safe.

1. What is the minimum number of participants necessary for opening the safe if one of them wants to cheat giving a random number?
2. If it is possibile to try a single combination (in case of error the safe blocks and cannot be opened any longer), how many participants are necessary to open the safe?

Solution

1. At least two good shares; thus three participants.

Solution

1. At least two good shares; thus three participants.
2. With three participants there are three different polynomials. With four participants there are two correct polynomials and two wrong polynomials.

Exercise

A military office consists of a general, two colonels, and five employees that control a missile. For launching the missile it is necessary to have the approval of the general.
Otherwise, it is necessary the approval of the two colonels, or of the five employees, or of a single colonel plus three employees.
Describe how theese constraints can be met by using a secret sharing scheme.
(Hint: try distributing the shares in a Shamir scheme (10,30))

Solution

role	shares
general	10
colonel	5
employee	2

Total shares = 30

group	shares
general	10
2 colonels	10
5 employees	10
1 colonel plus 3 employees	11
1 colonel plus 2 employees	9

Exercise

Consider a situation in which three governments A, B, and C are hostile to one another, yet they fear the common threat by the Antartica government. Each government sends a delegation of 10 members to an international summit to discuss the threat of Antartica penguins to the world security. They decide that, if the birds become too turbolent, they will attack.
Using a secret sharing scheme, describe how the launch code can be divided so that it is necessary the collaboration of three members of delegation A, four members of delegation B, and two members of delegation C to recover the code.

Solution

Since all three delegations are necessary, we split the secret in three parts with a splitting technique.

Then, we divide each part into shares using an appropriate threshold scheme: (10,3) for A, (10,4) for B, and (10,2) for C.