Cheater Identification
In
Secret Sharing Scheme

By

Sarvajeet Haldar (510816031)

Sounit Ghosh (510816004)

Suman Mahato (510816044)

Secret:

- A highly sensitive data meant to be kept unknown
- E.g. encryption keys, missile launch codes, numbered bank accounts etc.

Secret Sharing:

- Breaking a secret into multiple shares
- Distributing the shares among multiple parties
- A subclass of these parties can reconstruct the secret
- Thus there is no single point of failure that can lead to its loss

Shamir's Secret Sharing:

- An old cryptography algorithm invented by the Israeli cryptographer **Adi Shamir(1979)**
- Split a secret **S** in **n** parts
- Any **k**-out-of-**n** pieces can reconstruct the original secret **S**
- But with any **k-1** pieces no information is exposed about **S**
- This is conventionally called a **(n, k)** threshold scheme

Implementation:

- Any **k** points can define a polynomial of **k-1** degree.
- Given two points you can define a line equation, given 3 points you can define a parabola equation and so on and so forth.

Creating shares:

- To split a secret **S** into **n** shares, such that

-any combination of <= **L** shares can't learn **S**

-any combination of >=**L** shares learns **S**

- We construct a degree-**L** polynomial **f** such that **f(0) = S**

- And compute,

$$\text{share}_1 = \mathbf{f(1)}$$
$$\text{share}_2 = \mathbf{f(2)}$$
$$\ldots\ldots$$
$$\ldots\ldots$$
$$\text{share}_n = \mathbf{f(n)}$$

Reconstructing the secret:

- First we need to recreate the polynomial using the **Lagrange Polynomial Interpolation(1795)**

Example:

- Let the shares be **f(5)=3, f(7)=2, f(12)=6, f(30)=15**
- Then $\partial_i(x) = \prod \frac{x-j}{i-j}$ for $j \in C$, $j != i$ where $C = \{5,7,12,30\}$
- Now we can reconstruct the polynomial by computing,

  $f(x) = 3\,\partial_5(x) + 2\partial_7(x) + 6\partial_{12}(x) + 15\partial_{30}(x)$

- And to get the secret we just need to compute **f(0)**

Output (Creating Shares)

<<< Shamir's Secret Sharing Scheme >>>

Enter 1 to generate shares from a secret
Enter 2 to find the secret from keys

Enter your value: 1
Default Prime no.(p) for restricting finite fields: 15485867

To change p enter a large prime else enter 0 :0

Enter the no. of shares(n) to be generated such that n<p :6

Enter the minimum no. of shares(k) required to reconstruct the secret:3

<<< Publicly known values are >>>
No. of shares : 6
Threshold no. of shares : 3
Prime p: 15485867

Enter the secret(s) to be divide into shares such that s<p :1024
Evaluating the polynomial at 0: 1024.0
The list of shares are: [(1, 7280850.0), (2, 6466022.0), (3, 13042407.0), (4, 11524138.0), (5, 1911215.0), (6, 15175372.0)]

Output (Reconstructing the Secret)

<<< Shamir's Secret Sharing Scheme >>>

Enter 1 to generate shares from a secret
Enter 2 to find the secret from keys

Enter your value: 2
Default Prime no.(p) for restricting finite fields: 15485867

To change p enter a large prime else enter 0 :0

Enter the no. of keys(max 20) :3
Key 1>>
Enter the x value of the key:1

Enter the y value of the key:7280850
Key 2>>
Enter the x value of the key:2

Enter the y value of the key:6466022
Key 3>>
Enter the x value of the key:3

Enter the y value of the key:13042407
The secret is: 1024.0

Cheater in Shamir's scheme:

- Vicious participants release forged shares in secret reconstruction
- Once these outside cheaters gather enough shares by depriving other participants, they can reconstruct the secret exclusively
- **Tompa & Woll (1979)** showed such a type of cheating

Explanation:

Let **n=5**, **k=3**, **S= 2** & the polynomial is $f(x) = 2x^2 - 3x + 2$

- Shares:

$Sh_1 = 1$, $Sh_2 = 4$, $Sh_3 = 11$

$Sh_4 = 22$, $Sh_5 = 37$

- Let **shares 1, 2 and 3** are selected for secret reconstruction
- Let **participant 1** wants to cheat
- It chooses a polynomial **h(x)** such that **h(0) = 2** and $\mathbf{h(i_j) = 0}$ for **j = 2…k** and constructs a polynomial using interpolation
- i.e. $h(x) = \frac{1}{3}(x^2 - 5x + 6)$
- And submits $d_1 = Sh_1 + h(1) = 1 + \frac{2}{3} = \frac{5}{3}$ as its share
- Now constructed polynomial is:

$$f'(x) = \frac{x^2 - 5x + 6}{2} \times \frac{5}{3} - (x^2 - 4x + 3) \times 4 + \frac{x^2 - 3x + 2}{2} \times 11$$

and

$$f'(0) = 4$$

- Thus **participant 1** can easily get the secret, **S = 4-2 = 2**

Cheater Detection:

- A lot of schemes have been proposed by different eminent scientists
- But some of them are really effective and their implementation is computationally favourable
- We have chosen :

Feldman’s Scheme

- It is based on **commitment** property
- Where each participant can verify whether their shares are generated from same polynomial **(Dealer Verification)**
- And the **combiner** can detect the cheater if exists

Implementation of Feldman's Scheme

Let us take an example where,

- Secret: **S**
- Participants: **n**,
- Threshold value: **k**
- Prime number: **q**
- **g** is the generator of a cyclic group which is hard to detect from (**g**^{i} mod **q**)

- Constructed polynomial is $f(x) = S + a_1 x + a_2 x^2 + ... + a_{k-1} x^{k-1} \bmod q$
- Dealer computes the commitment as

and makes them public.

$$c_0 = g^S \bmod q$$
$$c_1 = g^{a_1} \bmod q$$
$$..$$
$$c_{k-1} = g^{a_{k-1}} \bmod q$$

Dealer Verification

- Any one can verify whether the share is generated from same polynomial or not by using the following derivation.

$$g^{sh_i} = \left(c_0 . c_1^{i} . c_2^{i^2} \ldots\ldots c_{k-1}^{i^{k-1}}\right) \bmod q$$

$$as$$

$$\left(c_0 . c_1^{i} . c_2^{i^2} \ldots\ldots c_{k-1}^{i^{k-1}}\right) \bmod q$$

$$\Rightarrow \left(g^{s} . (g^{a_1})^{i} . (g^{a_2})^{i^2} \ldots\ldots (g^{a_{k-1}})^{i^{k-1}}\right) \bmod q$$

$$\Rightarrow g^{\left(S + a_1 . i + a_2 . i^2 + \ldots + a_{k-1} . i^{k-1}\right) \bmod q}$$

$$\Rightarrow g^{f(i) \bmod q}$$

- But publishing **g**^{s} leaks information about the secret

Output (Generating cyclic group)

<<< Feldman's Verifiable Secret Sharing Scheme >>>

<<< Choosing primes >>>

q is the prime, q = 127

r = 4

p is prime, p = 509

<<< Generating cyclic group >>>

Z_p* =

[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194, 195, 196, 197, 198, 199, 200, 201, 202, 203, 204, 205, 206, 207, 208, 209, 210, 211, 212, 213, 214, 215, 216, 217, 218, 219, 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236, 237, 238, 239, 240, 241, 242, 243, 244, 245, 246, 247, 248, 249, 250, 251, 252, 253, 254, 255, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 267, 268, 269, 270, 271, 272, 273, 274, 275, 276, 277, 278, 279, 280, 281, 282, 283, 284, 285, 286, 287, 288, 289, 290, 291, 292, 293, 294, 295, 296, 297, 298, 299, 300, 301, 302, 303, 304, 305, 306, 307, 308, 309, 310, 311, 312, 313, 314, 315, 316, 317, 318, 319, 320, 321, 322, 323, 324, 325, 326, 327, 328, 329, 330, 331, 332, 333, 334, 335, 336, 337, 338, 339, 340, 341, 342, 343, 344, 345, 346, 347, 348, 349, 350, 351, 352, 353, 354, 355, 356, 357, 358, 359, 360, 361, 362, 363, 364, 365, 366, 367, 368, 369, 370, 371, 372, 373, 374, 375, 376, 377, 378, 379, 380, 381, 382, 383, 384, 385, 386, 387, 388, 389, 390, 391, 392, 393, 394, 395, 396, 397, 398, 399, 400, 401, 402, 403, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417, 418, 419, 420, 421, 422, 423, 424, 425, 426, 427, 428, 429, 430, 431, 432, 433, 434, 435, 436, 437, 438, 439, 440, 441, 442, 443, 444, 445, 446, 447, 448, 449, 450, 451, 452, 453, 454, 455, 456, 457, 458, 459, 460, 461, 462, 463, 464, 465, 466, 467, 468, 469, 470, 471, 472, 473, 474, 475, 476, 477, 478, 479, 480, 481, 482, 483, 484, 485, 486, 487, 488, 489, 490, 491, 492, 493, 494, 495, 496, 497, 498, 499, 500, 501, 502, 503, 504, 505, 506, 507, 508]

G =

[1, 14, 16, 17, 20, 21, 23, 24, 25, 30, 36, 38, 43, 44, 45, 54, 55, 57, 62, 66, 67, 81, 82, 91, 93, 97, 99, 103, 104, 107, 113, 116, 121, 122, 123, 127, 130, 137, 145, 148, 156, 167, 174, 179, 181, 183, 185, 195, 196, 199, 211, 222, 224, 234, 238, 239, 241, 245, 247, 251, 256, 261, 272, 278, 280, 281, 284, 286, 289, 292, 293, 294, 302, 319, 320, 322, 329, 332, 333, 336, 337, 340, 350, 351, 355, 356, 357, 359, 365, 368, 371, 376, 383, 384, 389, 391, 394, 400, 403, 404, 407, 408, 409, 413, 415, 417, 420, 424, 425, 426, 429, 436, 438, 439, 441, 445, 453, 460, 470, 472, 480, 483, 498, 500, 503, 504, 505]

Order of G is 127. This must be equal to q.

g = 123

G is the cyclic group which is generated by g

Let the secret polynomial be: 84 + 75x + 50x^2

(Secret polynomial coefficients taken from the group Z_q)

Output (Computing & Verifying Shares)

<<< Computing shares and verifying them >>>

i = 1
Share: f(1) = 82
Commitment: g^f(1) = 500
Verification: (g^a0)*((g^a1)^i)*((g^a2)^(i^2)) = 500

i = 2
Share: f(2) = 53
Commitment: g^f(2) = 409
Verification: (g^a0)*((g^a1)^i)*((g^a2)^(i^2)) = 409

i = 3
Share: f(3) = 124
Commitment: g^f(3) = 55
Verification: (g^a0)*((g^a1)^i)*((g^a2)^(i^2)) = 55

i = 4
Share: f(4) = 41
Commitment: g^f(4) = 394
Verification: (g^a0)*((g^a1)^i)*((g^a2)^(i^2)) = 394

i = 5
Share: f(5) = 58
Commitment: g^f(5) = 25
Verification: (g^a0)*((g^a1)^i)*((g^a2)^(i^2)) = 25

i = 6
Share: f(6) = 48
Commitment: g^f(6) = 400
Verification: (g^a0)*((g^a1)^i)*((g^a2)^(i^2)) = 400

The list of shares are: [82, 53, 124, 41, 58, 48]

Output (Reconstructing the Secret)

<<< Reconstructing the secret >>>

Share of P_1 is 82

i= 1

j= 2

j= 3

delta = 3.0

Share of P_2 is 53

i= 2

j= 1

j= 3

delta = 124.0

Share of P_3 is 124

i= 3

j= 1

j= 2

delta = 1.0

The secret is: 84.0

Thank You !