Blockchain and Privacy

2022

6/01

!

- Implementation (k,m) threshold scheme (slide 373)

K=3, m=5, D=148, P=997 ($P > \max(D, m)$)

$$g(x) = 148 + \underbrace{59}x + \underbrace{340}x^2$$

RANDOM

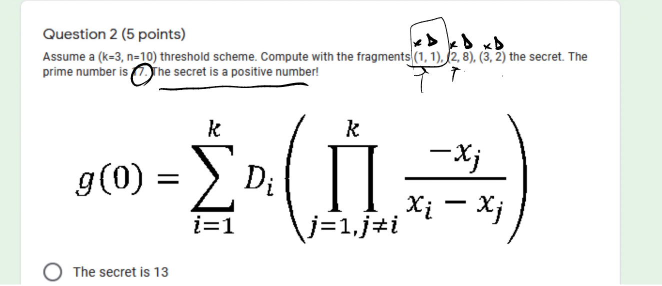
$D_1 = g(1) \bmod p$

$D_2 = g(2) \bmod p$

⋮

$D_5 = g(5) \bmod p$

- Distribute $\{i, D_i\}$ to each of k person
- How many of k people are needed to rebuild g(0) and so D?



Question 2 (5 points)

Assume a (k=3, n=10) threshold scheme. Compute with the fragments (1, 1), (2, 8), (3, 2) the secret. The prime number is 17. The secret is a positive number!

$$g(0) = \sum_{i=1}^{k} D_i \left(\prod_{j=1, j \neq i}^{k} \frac{-x_j}{x_i - x_j} \right)$$

○ The secret is 13

$$1\left(\overbrace{\frac{-2}{1-2} \cdot \frac{-3}{1-3}}^{3}\right) + 8\left(\overbrace{\frac{-1}{2-1} \cdot \frac{+3}{2-3}}^{-3}\right) + 2\left(\overbrace{\frac{-1}{\underbrace{3-1}_{2}} \cdot \frac{-2}{\underbrace{3-2}_{1}}}^{1}\right) \Rightarrow g(0) = -19$$

$g(0) \bmod p$

$+19 \bmod = 2$

$$g(0) = 1\left(\frac{-2}{\underbrace{1-2}_{-1}} \cdot \frac{-3}{\underbrace{1-3}_{-2}}\right) + 8\left(\frac{-1}{\underbrace{2-1}_{1}} \cdot \frac{-3}{\underbrace{2-3}_{-1}}\right) + 2\left(\overbrace{\frac{-1}{\underbrace{3-1}_{2}} \cdot \frac{2}{\underbrace{3-2}_{1}}}^{1}\right)$$

$$= 3 - 24 + 2 = -19$$

$g(0) \bmod 17 = \boxed{2}$ X