

# Consultation 8

10 December 2020 10:22

(3,5) - Shamir Threshold

$$f(x) = S + ax + bx^2 \pmod{p}$$

$$f(1) \rightarrow 1$$

$$f(2) \rightarrow 2$$

$$f(3) \rightarrow 3$$

$$f(4) \rightarrow 4$$

$$f(5) \rightarrow 4$$

$$A = \{\{1,2,3\}, \{1,4\}, \{2,4\}, \{3,4\}\}$$



Using a single instance of S + S

~~$$\begin{aligned} f(x) &= S_1 + ax + cx^2 \\ g(x) &= S_2 + bx + dx^3 \\ S &= S_1 \times S_2 \pmod{p} \end{aligned}$$~~

Not



$n, k, \lambda$   
3- (3, 4, 1) OA

$\lambda n^3 \times k$

$1 \cdot 3^3 \times 4$

27

