



UNIVERSIDAD
NACIONAL
DE COLOMBIA

SECRET SHARING

PROYECTO CRIPTOGRAFIA

**Thomas Molina Molina, Juan Jose Jimenez Maya, Juan Miguel Paez
Tatis, Catalina Metaute Gonzalez**

7 de marzo de 2025

INTRODUCCIÓN

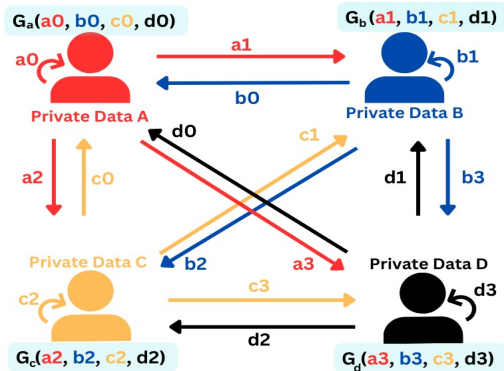
Este proyecto tiene como objetivo implementar un protocolo de comunicación seguro que permite a n partes calcular conjuntamente una función (en este caso, el producto de números privados) sin revelar sus datos individuales.

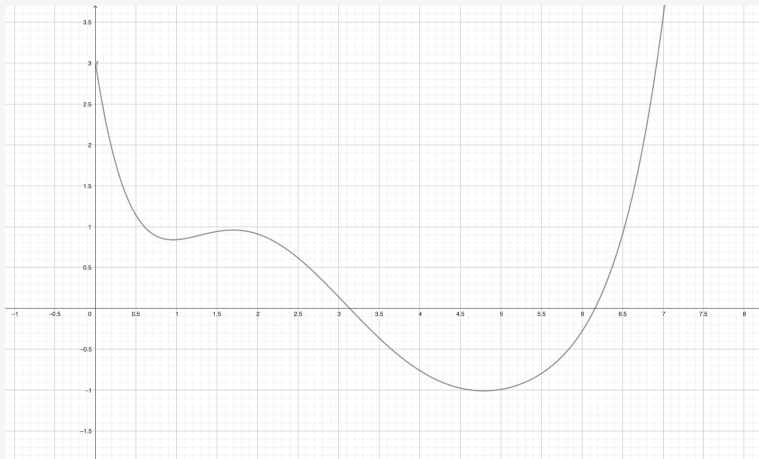
Las operaciones se realizan en un campo primo finito \mathbb{Z}_p , utilizando primos de Mersenne para optimizar la eficiencia de las operaciones modulares. El protocolo se basa en el esquema de Shamir Secret Sharing, donde cada parte genera y distribuye acciones (shares) de su dato privado, y posteriormente se reconstruye el secreto (el producto final) mediante interpolación de Lagrange.

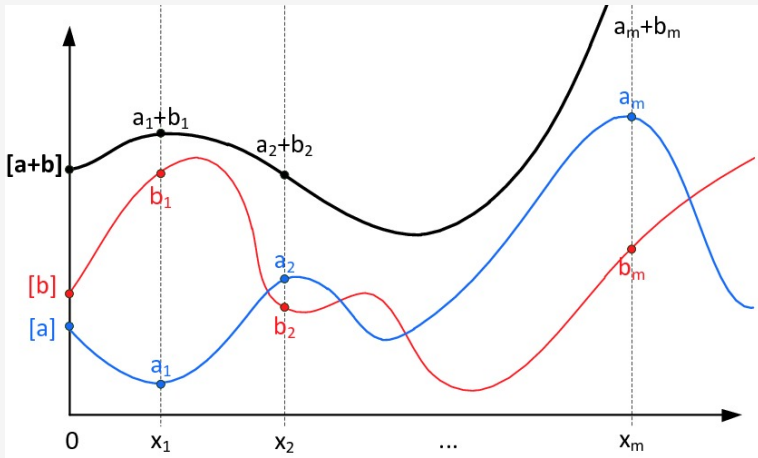
Además, se simula una red P2P para modelar la comunicación entre las partes, permitiendo la transmisión segura de las acciones.

Example: Secure Computation of $F(A, B, C, D)$

$$F(A, B, C, D) = f(G_a, G_b, G_c, G_d)$$







LAGRANGE INTERPOLATION

$$L_{n,k}(x) = \prod_{\substack{i=0 \\ i \neq k}}^n \frac{x - x_i}{x_k - x_i}$$

$$P_n(x) = \sum_{k=0}^n y_k L_{n,k}(x)$$

$$S_1 = 5 \quad S_2 = 6 \quad S_3 = 4 \quad \text{mod } 23$$

$$pol_1 = 5 + 3x \quad pol_2 = 6 + 4x \quad pol_3 = 4 + 3x$$

$$S_1 \quad S_2 \quad S_3$$

$$P_1 \quad 8 \quad 10 \quad 7 \quad P_1 = [8, 10, 7]$$

$$P_2 \quad 11 \quad 14 \quad 10 \quad P_2 = [11, 14, 10]$$

$$P_3 \quad 14 \quad 18 \quad 13 \quad P_3 = [14, 18, 13]$$

$S_1 \cdot S_2 \rightarrow$ multiplicaciones locales

$$MP_1 = 80 \text{ mod } 23 = 11$$

$$MP_2 = 16$$

$$MP_3 = 22$$

Polinomios para reducir grado

$$\left. \begin{array}{l} P_1 = 11 + 3x \Rightarrow [14, 17, 20] \Rightarrow [14, 21, 24] \\ P_2 = 16 + 5x \Rightarrow [21, 26, 31] \Rightarrow [17, 26, 26] \\ P_3 = 22 + 2x \Rightarrow [24, 26, 28] \Rightarrow [20, 31, 28] \end{array} \right\} \text{ Lagrange}$$

$$P_1 = 3 \quad P_2 = 22 \quad P_3 = 18 \quad \text{Asi,} \quad P_1 = [3, 7] \quad P_2 = [22, 10] \quad P_3 = [18, 13]$$

$$\text{Asi,} \quad S_1 \cdot S_2 = [3, 22, 18] \quad S_3 = [7, 10, 13]$$

$$\text{Hacemos } [S_1 \cdot S_2] \cdot S_3$$

Multiplicaciones locales

$$MP_1 = 21 \quad MP_2 = 13 \quad MP_3 = 4$$

$$\left. \begin{array}{l} P_1 = 21 + 3x \Rightarrow [24, 27, 30] \Rightarrow [24, 18, 6] \\ P_2 = 13 + 5x \Rightarrow [18, 23, 28] \Rightarrow [27, 23, 8] \\ P_3 = 4 + 2x \Rightarrow [6, 8, 10] \Rightarrow [30, 28, 10] \end{array} \right\} \text{Lagrange}$$

$$P_1 = 1 \quad P_2 = 20 \quad P_3 = 16$$

$$[S_1 \cdot S_2] \cdot S_3 = [1, 20, 16] \rightarrow \text{Lagrange}$$