UNIVERSIDAD
NACIONAL
DE COLOMBIA

Secret Sharing

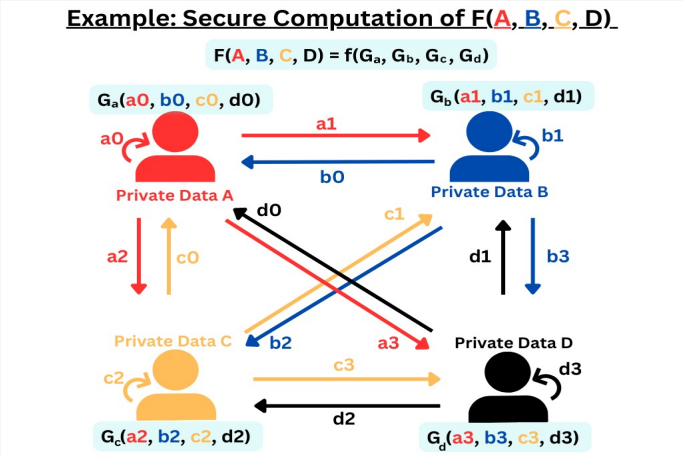
Proyecto Criptografia

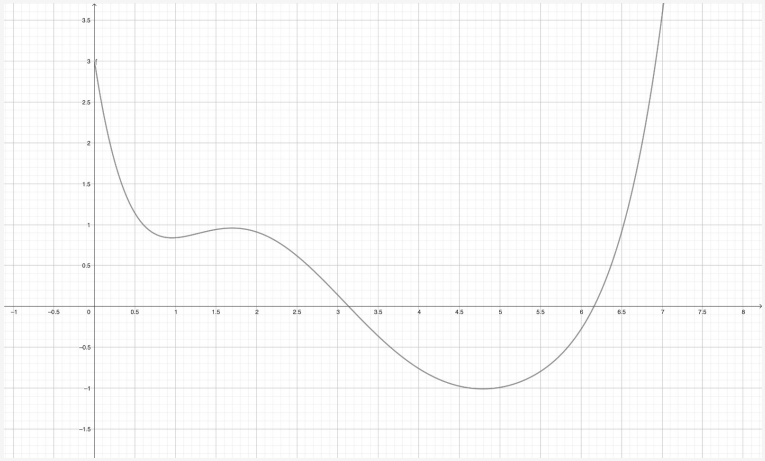
Thomas Molina Molina, Juan Jose Jimenez Maya, Juan Miguel Paez Tatis, Catalina Metaute Gonzalez

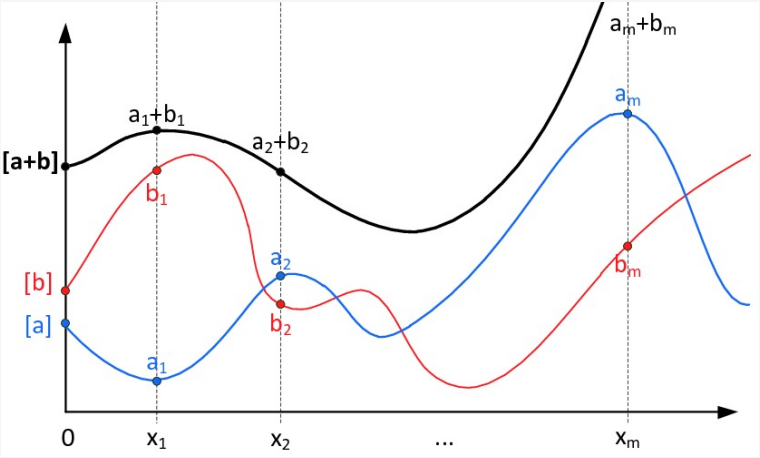
7 de marzo de 2025

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 Zp, 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 utiliza 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(Ga, Gb, Gc, Gd)
Ga(a0, b0, c0, d0)
Gb(a1, b1, c1, d1)
a0
a1
b1
b0
Private Data A
Private Data B
d0
c1
a2
c0
d1
b3
Private Data C
b2
a3
Private Data D
c2
c3
d3
d2
Gc(a2, b2, c2, d2)
Gd(a3, b3, c3, d3)


3.5
3
2.5
2
1.5
1
0.5
−0.5
−1
−1.5
−1
−0.5
0
0.5
1
1.5
2
2.5
3
3.5
4
4.5
5
5.5
6
6.5
7
7.5
8


[a+b]
[b]
[a]
a_1+b_1
a_2+b_2
a_m+b_m
b_1
a_2
b_2
a_1
a_m
b_m
0
x_1
x_2
...
x_m

Lagrange Interpolation

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

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

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

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

	S_1	S_2	S_3	
P_1	8	10	7	$P_1 = [8, 10, 7]$
P_2	11	14	10	$P_2 = [11, 14, 10]$
P_3	14	18	13	$P_3 = [14, 18, 13]$

$S_1 \cdot S_2 \rightarrow$ multiplicaciones locales

$MP_1 = 80 \mod 23 = 11$

$MP_2 = 16$

$MP_3 = 22$

Polinomios para reducir grado

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

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

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

Hacemos $[S_1 \cdot S_2] \cdot S_3$

Multiplicaciones locales

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

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

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

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