CatioCrypto 2025: Multi-Party Computation

26-27 Septiembre 2025

Autor Emanuel Nicolás Herrador
Speaker Eduardo Soria-Vázquez

1 Introducción

Algunos ejemplos acerca de qué se ocupa la criptografía son:

- *Verifiable Computation*: Demostrar que se ha ejecutado un programa, sin que quien lo verifique tenga que re-ejecutarlo.
- *Zero-Knowledge Proofs*: Similar a VC, pero quien demuestra hacer el cálculo pueden mantener algunos datos ocultos.
- *Secret Sharing*: Fragmentar un secreto entre varias entidades, de tal forma que solo pueda reconstruirse si ciertos subconjuntos de ellas acuerdan hacerlo.
- *Multi-Party Computation* (MPC): Calcular sobre datos "sin verlos", de forma distribuida.
- Otros: privacidad diferencial (DP), recuperación privada de información (PIR), cifrado totalmente homomórfico (FHE), cifrado funcional (FE), time-lock puzzles, blockchaings, criptomonedas, ...

2 Multi-Party Computation

2.1 Protocolo MPC

Un protocolo MPC consta de n entidades que desconfían las unas de las otras y de modo que cada una pueda aportar un valor P_i secreto. La idea/objetivo es calcular un función f aplicada a estos valores en conjunto pero sin mostrarlos a otra de las entidades.

Una forma de resolverlo sin MPC es con una tercera parte de confianza, pero el problema es que no siempre existe. Lo que vuelve difícil a MPC es la presencia de un adversario que participa y corrompe a ciertas entidades para coordinar su ataque:

- Corrupción pasiva: las entidades corruptas hacen lo que deben pero comparten información entre ellas para tratar de aprender más cosas sobre las demás entidades
- Corrupción activa: las entidades corruptas pueden actuar de forma arbitraria para sabotear los objetivos de seguridad

El objetivo es lograr todas las propiedades que lograríamos con una tercera parte de confianza pero sin ella.

2.2 Primitivas

Algunas de las prmitivas usadas por MPC son:

- Garbled Circuits
- Secret Sharing
- Oblivious Transfer
- Homomorphic Encryption

2.2.1 Secret Sharing (compartición de secretos)

Definición 2.1 (Esquema de compartición de secretos)**.** Sea $\mathbb{F}$ un cuerpo finito y $n, t \in \mathbb{Z} : 0 \leq t < n$. Sean las entidades $P_1, \ldots, P_n$ y un compartidor en posesión de un secreto $s \in \mathbb{F}$. Un esquema (n, t)-umbral de compartición de secretos consta de las siguientes fases:

1. Fase de compartición: El Compartidor fragmenta s en n partes $s_1, \ldots, s_n \in \mathbb{F}$ y la entidad P_i recibe su parte $s_i \in \mathbb{F}$
2. Fase de reconstrucción: Al menos $t + 1$ entidades envían su parte a quien quieran que reconstruya s.

Y tal que satisface las siguientes propiedades:

- t-privacidad: Cualquier conjunto de a lo sumo t partes no revela ninguna información sobre el secreto $s \in \mathbb{F}$
- $(t + 1)$-reconstrucción: Cualquier conjunto de $t + 1$ partes determina de forma única el secreto $s \in \mathbb{F}$

Definición 2.2 (Esquema lineal de compartición de secretos)**.** Decimos que el esquema es *lineal* si además satisface que $\forall s, t \in \mathbb{F}$ compartidos como $(s_1, \ldots, s_n), (t_1, \ldots, t_n) \in \mathbb{F}^n$, tenemos que $(s_1 + t_1, \ldots, s_n + t_n)$ es una compartición de $s + t \in \mathbb{F}$.

Nota. Abusaremos notación y nos restringiremos a esquemas de compartición de secretos que sean sobre un cuerpo finito $\mathbb{F}$, umbrales y lineales (sobre $\mathbb{F}$). Además, usaremos la notación definida como $[s] := (s; s_1, \ldots, s_n)$, de modo que $[s] + [t] = [s + t]$.

Compartición de secretos aditiva Sea $F_p := (\mathbb{Z}/p\mathbb{Z}, +, \cdot)$, $\mathbb{Z}/p\mathbb{Z} = (0, \ldots, p-1)$, p nro. primo, el esquema es:

1. Fase de compartición:
   (a) Compartidor escoge de forma uniformemente aleatoria $s_1, \ldots, s_n \in \mathbb{F}_p : s_1 + \cdots + s_n = s$.
   (b) Compartidor envía la parte s_i a P_i
2. Fase de reconstrucción:
   (a) Cada P_i envía s_i a la entidad que quieren que reconstruya el secreto
   (b) Dicha entidad calcula $s = s_1 + \cdots + s_n$

Nota. Notar que el umbral t debe ser $n - 1$ para que sea reconstruible teniendo todos los pedacitos de secretos. El hecho de que no sea reconstruible con $n - 1$ entidades se reduce al OTP porque si tenemos $s_1, \ldots, s_{n-1} \in \mathbb{F}_p$ elegidos uniformemente aleatorios, entonces $s_n = s - (s_1 + \cdots + s_{n-1})$ es también uniformemente aleatorio.