Encuentra tu *perfect match*

Maribel González
mariaisabel.gonzalez@uc3m.es

12 de febrero de 2026

1. Intersección Privada de Conjuntos (Private Set Intersection, PSI)

La *Intersección Privada de Conjuntos* (Private Set Intersection, PSI) es una primitiva criptográfica que permite a dos o más partes computar la intersección de conjuntos de datos privados sin revelar información adicional sobre los elementos fuera de dicha intersección. Formalmente, podemos describir el problema genérico que se aborda de la siguiente forma: sean dos partes, A y B, con conjuntos privados X y Y, respectivamente. Un protocolo de PSI permite que ambas partes obtengan el conjunto $X \cap Y$, garantizando:

- Que ninguna parte aprende información sobre elementos del otro conjunto fuera de la intersección.
- Que la única información revelada es la salida autorizada por el protocolo.

Los protocolos de PSI son cruciales en múltiples aplicaciones, como en la comparación privada de bases de datos sensibles, la detección colaborativa de fraudes o la realización de análisis de datos procedentes de diferentes fuentes gestionadas por entidades que no confían unas en otras. A la hora de analizar la seguridad de protocolos de PSI se contemplan distintos modelos adversariales:

- **Honesto-pero-curioso (semi-honesto):** las partes siguen el protocolo pero tratan de extraer información adicional de los mensajes vistos.
- **Malicioso:** las partes pueden desviarse arbitrariamente del protocolo.

A menudo, según el contexto de aplicación, hay variantes de PSI que pueden utilizarse para resolver problemas concretos, las más conocidas son:

- **PSI cardinalidad (PSI-CA):** solo se revela la cardinalidad $|X \cap Y|$.
- **PSI con salida asimétrica:** solo una de las dos partes obtiene el resultado.
- **PSI multipartito:** participan más de dos partes.

En la literatura hay muchas soluciones para conseguir implementar protocolos PSI relativamente eficientes y flexibles, puedes ver algunos en este tutorial.

2. El Reto

Los diseñadores de una App para encontrar amigos asocian a cada usuario un conjunto de atributos que describen sus gustos y características principales. El objetivo de los diseñadores de la App es implementar un protocolo para conseguir las siguientes funcionalidades:

- **A. Identificación de usuarios afines**: Cada usuario A puede fijar un umbral k de modo que si habla con un usuario B determinado, solo recibirá el identificador personal del mismo (hará *match*) si B comparte con A, al menos, k atributos. El protocolo no debe revelar a A ninguna otra información acerca de un usuario del sistema con el que se comunique a través de la aplicación; solo si éste comparte al menos k atributos con él (en cuyo caso, la aplicación le permite obtener el identificador personal de ese usuario para seguir comunicándose con él).

- **B. Sesiones de tres usuarios:** Si tres usuarios A, B y C quieren comprobar si son suficientemente afines, pueden ejecutar una sesión conjunta hablando de manera anónima y tras esa sesión recibirán, respectivamente, los identificadores necesarios para establecer contacto entre ellos, si y solo si la intersección entre cualesquiera 2 de ellos contiene al menos tantos atributos como la mitad del número de atributos de cualquiera de ellos y la intersección entre los tres es, al menos, un quinto de ese valor. En símbolos: Si A tiene un conjunto de atributos X, B un conjunto Y y C un conjunto Z, se requiere que

$$min(|X \cap Y|, |X \cap Z|, |Y \cap Z|) \geq \frac{1}{2} max(|X|, |Y|, |Z|)$$

y

$$|X \cap Y \cap Z| \geq \frac{1}{5} max(|X|, |Y|, |Z|)$$

Las soluciones al reto pueden utilizar un protocolo PSI de entre los descritos en este tutorial, directamente o modificado de modo que se minimice el número de mensajes que los usuarios han de enviarse y las rondas de comunicación necesarias para completar el proceso.