An introdcution to Threshold PSI

Xinpeng Yang

July 15, 2023

Contents

What is threshold PSI

Threshold PSI is able to compute the elements that appear at least k times in n sets

Threshold PSI

There are n parties $P_1, \cdots, P_n$ where P_1 is the leader and $k \in [1, n-1]$ denotes the threshold.
Input: For each $i \in [n]$, P_i inputs a set X_i of size m.
Output: For each $x \in X_1$, let $q_x = |\{i : x \in X_i \text{ for } i \in \{2, \cdots, n\}\}|$,
Then, output $Y = \{x \in X_1 : q_x \geq k\}$ to P_1.

Simple approach

We can compute the result as follow

1. select subset $s \subseteq \{1, 2, \cdots, n\}$ and $|s| \geq k$
2. run multi-party PSI between X_j and get $X^s = \{x | x \in X_j, j \in s\}$
3. output $Y = \bigcap_{|s|>=k, s \subseteq [n]} X^s$

The computation cost is at least $C_n^k + C_n^{k+1} + \cdots + C_n^n$

inefficient and insecure !

Application

- Identifying High-Risk Individuals in the Spread of Disease
- Share ride
- Anonymous Voting and Consensus

Contents

Efficient Linear Multiparty PSI and Extensions to Circuit/Quorum PSI

CCS 21

Preliminaries

Circuit-based PSI

The problem of circuit PSI was introduced in the 2 party setting and enables parties P_1 and P_2, with their private input sets X and Y, respectively, to compute $f(X \cap Y)$, where f is any symmetric function

It allows to keep the intersection $X \cap Y$ secret from the parties while allowing to securely compute $f(X \cap Y)$

Applications: cardinality, set intersection sum and threshold cardinality/intersection

Contents

Practical Multi-Party Private Set Intersection Protocols

TIFS 22

Preliminaries

Bloom Filters

A Bloom Filter, $BF = (BF[0], \cdots, BF[j], \cdots, BF[m-1])$ encodes a set S of length at most n into m bit string
chosen k hash function $h_i : \{0,1\}* \longrightarrow [0, 1, \cdots, m-1]$
for every $x \in S$, set $BF(h_i(x)) = 1$ where $i = 1, 2, \cdots, k$, the other slot is $\mathbf{0}$

Inverted Bloom Filter

for $j \in 0, 1, \cdots, m-1$, set $IBF[j] = BF[j] + 1 \ mod\ 2$

Encrypted Bloom Filter

for $j \in 0, 1, \cdots, m-1$, $EBF[j] = Enc_{pk}(BF[j])$, where pk is a public key of a secret key sk

Preliminaries

Threshold Paillier PKE

- (t,n)-threshold version of the Paillier's scheme
- Additive Homomorphism
- At least t shares of decryption can reconstruct the plaintext

Preliminaries

Kerschbaum et al. Secure Comparison Protocol, SCP

Given only their encrypted values Enc(x_0) and Enc(x_1) as input. The output is a single encrypted bit Enc(b) and the encryption scheme is additive homomorphic (here is Paillier PKE)
In their protocol, $\mathbb{Z}_p$ is represented by the upper half of the range [0, p - 1] as negative, that is $[\lceil \frac{p}{2} \rceil, p - 1] \equiv [\lfloor -\frac{p}{2} \rfloor, -1]$

P_1 computes (a_1^1, a_2^1, a_3^1) = (Enc(1), Enc(0), Enc(c)) where

$$\text{Enc(c)} = (Enc(x_0)Enc(x_1))^{r_1}Enc(r_2) = Enc(r_1(x_0 - x_1) - r_2)$$

Preliminaries

For every party $P_i, 2 \leq i \leq t$, selects $r_2 < r_1$ and flips a coin $b_i \in \{0, 1\}$, sends (a_1^i, a_2^i, a_3^i) to P_{i+1} where

$$
\begin{aligned}
a_1^i &= a_{1+b}^{i-1}\, Enc(0) \\
a_2^i &= a_{2-b}^{i-1}\, Enc(0) \\
a_3^i &= (a_3^{i-1})^{r_1} Enc(r_2)
\end{aligned}
$$

All parties $P_i, 2 \leq i \leq t$, jointly decrypt a_t^3 to decide the result.

If $a_t^3 < 0$ then a_t^1 = Enc(1), that is $[\, x_0 \leq x_1]$ = 1, else a_t^1 = Enc(0).

Main method

Local EBFs generation

Each client $P_i, 1 \le i \le t-1$

1. Computes their Bloom filter of their private data set S_i , where $1 \le i \le t-1$
2. Computes their encrypted Bloom filter EBF_i by encrypting each element of $BFi[j]$ using pk
3. Forward their EBF_i to the server P_t

Result

Contents

Bibliography I

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Contents

End

Thanks for your listening.