Suppose an organization has a strict privacy policy regarding secret data sharing and wishes to further reduce the amount of information that would otherwise be divulged by an inside attacker.

Assume the organization has Dep. A and Dep. B that each own sensitive sets, SA andSB respectively, containing comparable elements. Also assume entities Alice and Bob, in Dep. A and Dep. B respectively, can only query each other’s sets using elements that exist in their own set. Assume the goal of an inside attacker, *Evil Bob*, is to divulge the maximal amount of **any** secret information with minimal interaction. Note that since Evil Bob is an insider, it is assumed he can decrypt communications with Alice securely. Then consider the case where the valid request is made to compute the intersection of the sets between Alice and Evil Bob:

Case 1 (**Evil** **Bob Requests**):

Evil Bob is an active inside attacker and can choose the set SA to attack by requesting the intersection.

Case 1.1 (**Private Evil Bob**):

Alice sends SA to Evil Bob to compute the intersection privately. Evil Bob then divulges the larger set of secret information SA andSB.

Case 1.2 (**Private Alice**):

Bob sends SB to Alice to compute the intersection privately who then returns it to Evil Bob. Evil Bob can only divulge SB at most instead of SA andSB

Case 2 (**Alice Requests**):

Evil Bob is a passive inside attacker and cannot choose the set SA to attack. The request is instead made by Alice.

Case 2.1 (**Private Alice**):

Bob sends SB to Alice to compute the intersection privately who then returns it to Evil Bob. Evil Bob can only divulge SB at most instead of SA andSB.

Case 2.2 (**Private Evil Bob**):

Alice sends SA to Evil Bob to compute the intersection privately. Evil Bob divulges the larger set of secret information SA andSB.

There are several important takeaways here, namely that it is naively assumed we know who the inside attacker is. If we consider that Alice is equally likely to be an inside attacker, we see that Case 1 and Case 2 are identical. Therefore it wouldn’t matter if only one party could request or if the intersection was computed by a third party. **This means that in all cases an inside attacker can divulge the maximal amount of any secret information with minimal interaction**.

To solve this problem, we use Private Set intersection where Alice and Evil Bob compute the hash of each element and exchange the set of hashes. Then since the information of non-matching hashes are confidential (iff the space of set elements are large) Evil Bob or Evil Alice cannot divulge information not already in their set.