Review: Querying Encrypted Databases

- Suppose the following table shows the partition and identification functions of attributes A and B from two tables RA and RB respectively. For simplicity, we denote a translated condition of the form (IdA=a ∧ IdB=b) as (a, b) where a and b are identification values of A and B partitions respectively.

A-Partitions	Identification (IdA)	B-Partitions	Identification (IdB)
[0, 100]	4	[0,200]	6
(100, 200]	8	(200, 400]	8
(200, 300]	9		
(300, 400]	3		

- What is the condition at the server if the query has the join condition “A = B” ?
- What about “A < B” ?
- An alternative scheme is to transmit RA and RB to the client, and leave to the client to perform the join. Since both the above cases have fewer than 8 combinations, pushing the processing of these join operations to the server will definitely result in superior performance (in terms of transmission cost) as compared to the naïve scheme. True or False.

Review: Querying Encrypted Databases

A-Partitions	Identification (IdA)	B-Partitions	Identification (IdB)
[0, 100]	4	[0,200]	6
(100, 200]	8	(200, 400]	8
(200, 300]	9		
(300, 400]	3		

- What is the condition at the server if the query has the join condition “A = B” ?

$$(4, 6) \vee (8, 6) \vee (9, 8) \vee (3, 8)$$

- What about “A < B” ?

$$(4, 6) \vee (4, 8) \vee (8, 6) \vee (8, 8) \vee (9, 8) \vee (3, 8)$$

Review: Querying Encrypted Databases

A-Partitions	Identification (IdA)	B-Partitions	Identification (IdB)
[0, 100]	4	[0,200]	6
(100, 200]	8	(200, 400]	8
(200, 300]	9		
(300, 400]	3		

- An alternative scheme is to transmit RA and RB to the client, and leave to the client to perform the join. Since both the above cases have fewer than 8 combinations, pushing the processing of these join operations to the server will definitely result in superior performance (in terms of transmission cost) as compared to the naïve scheme. True or False.

  False. This is because we need to compute the cross product of the matching buckets. This size may be larger than the RA+RB.