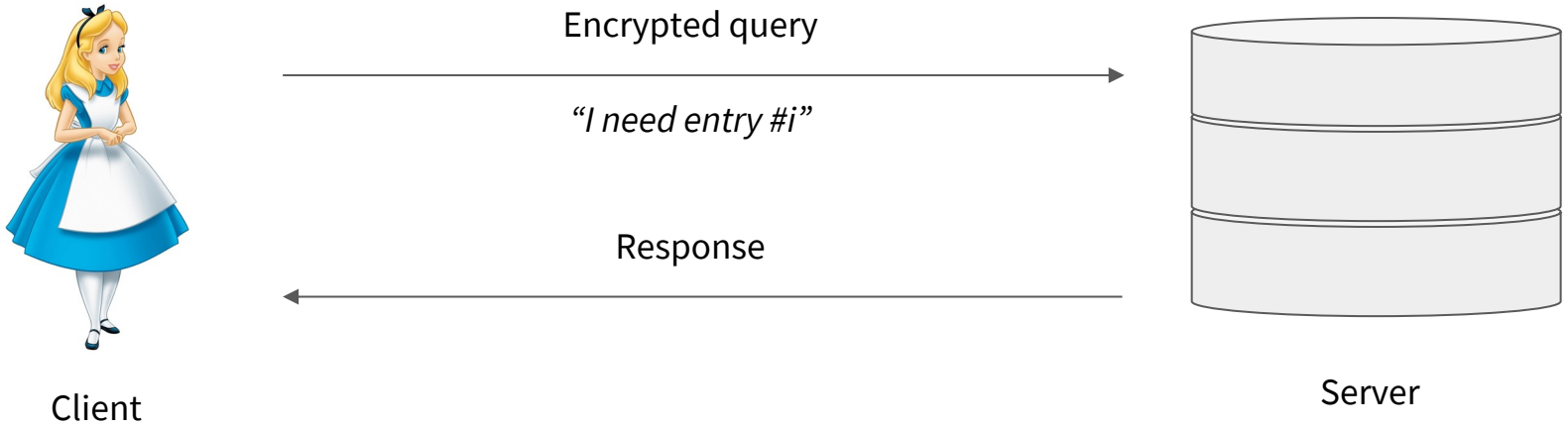
Friday Live Exercises

Homomorphic Encryption

Private Information Retrieval



Client Privacy:
Server does not know which *i* Alice asked for.

Private Information Retrieval

Client

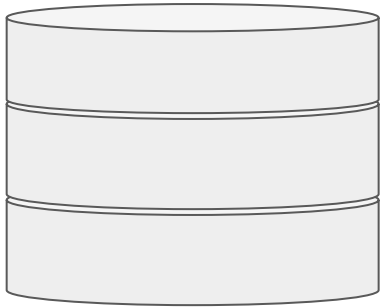
q = Query(i)

q

r = Response(q)

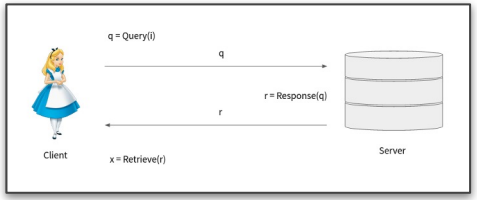
r

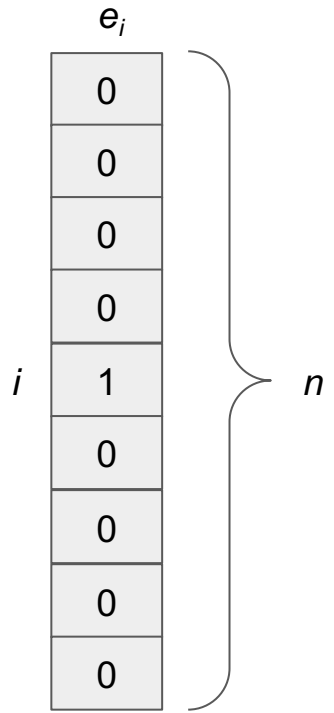
x = Retrieve(r)



Server

Attempt I





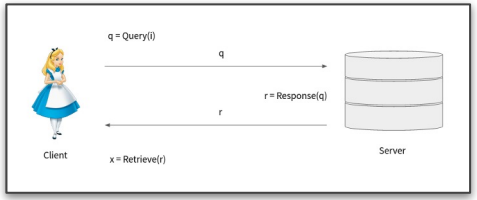
How to use FHE and the indicator vector e_i to implement the protocol?

q = Query(i)

r = Response(q)

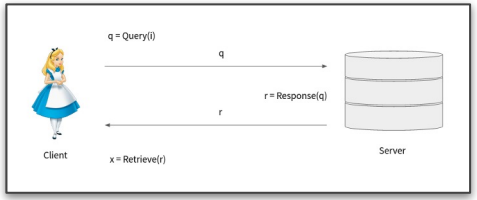
x = Retrieve(r)

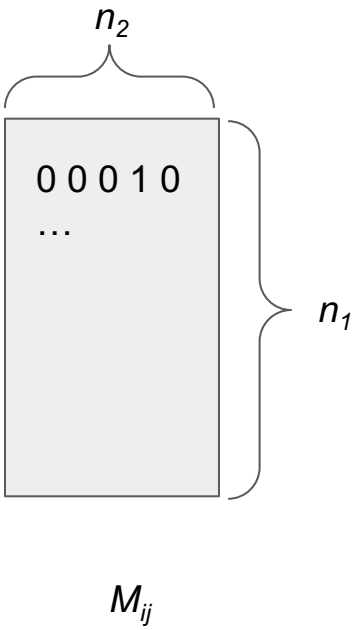
Attempt I. Analysis



1. What is the threat model (e.g., honest, honest-but-curious, malicious server)
2. What is the computation and communication cost of the system in terms of *n* (database size) and *m* (record size)?
3. What is the multiplicative depth?

Attempt II. Sublinear communication





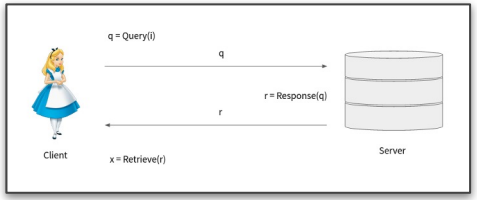
How to use FHE and the indicator matrix M_{ij} to implement the protocol?

q = Query(i)

r = Response(q)

x = Retrieve(r)

Attempt II. Analysis



1. What is the threat model (e.g., honest, honest-but-curious, malicious server)
2. What is the computation and communication cost of the system in terms of *n* (database size) and *m* (record size)?
3. What is the multiplicative depth?

Server privacy

Do the protocols achieve server privacy? (The client only learns information about the requested record)

1. Honest-but-curious client
2. Malicious client