

Topics

- Introduction
- Cloaking-based Solution
- **Transformation-based Solution**
- Private Information Retrieval-based Solution



Preliminary

- We observed that *one-way function* can be an ideal mechanism to preserve users' privacy.
- A one-way function is easy to compute but difficult to invert, meaning that some algorithms can compute the function in polynomial time while no probabilistic polynomial-time algorithm can compute an inverse image of the function with better than negligible probability.



Preliminary (Cont.)

- The applied transformation function has to allow fast computation of its preimage with special information, called *trapdoor*.
- In mathematical terms, if f is a trapdoor function there exists some secret information y , such that given $f(x)$ and y it is easy to compute x .
- Multiplication of two large prime numbers.



Space Encryption

- A *space-filling curve* is a continuous curve, which passes through every point of a closed space.
- The important property of these curves is that they retain the proximity and neighboring aspects of the indexed data.
- The paper investigates the applicability of space-filling curves as **ciphers** for preserving location privacy of mobile users.

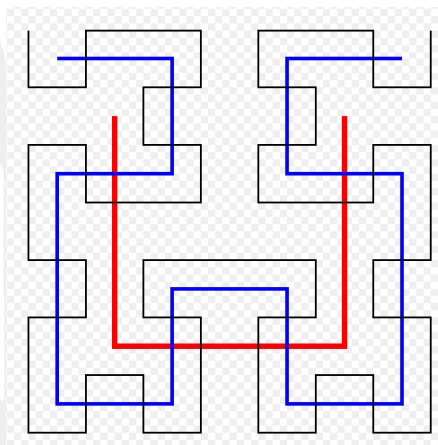


Space Encryption (Cont.)

- A user applies space-filling curves to encrypt the locations of spatial objects in a 2-D space before sending requests to service providers.
- Since the user knows the curve parameters (i.e., [the curve order and orientation](#)), the query results returned from the service provider can be decrypted with the corresponding curve order and orientation as the trapdoor.



Space Encryption (Cont.)



Space Encryption (Cont.)

- For a two dimensional space, we define H_o^m as the m^{th} order Hilbert curve with the o^{th} orientation.
- We can formalize the relationship as $V_H = H_o^m(x, y)$ where x and y are the coordinates of a 2-D space point.

5	6	9	10
4	7	8 ^[B]	11
3	2 ^[A]	13	12 ^[D]
0 ^[A]	1	14	15



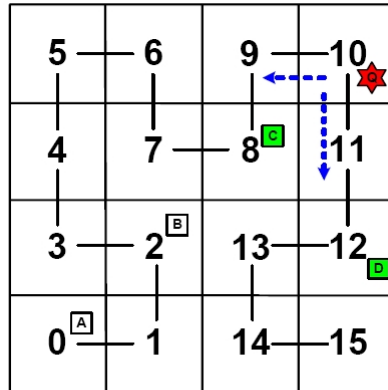
Query Evaluation – Range Query

5	6	9	10
4	7	8 ^[C]	11
3	2 ^[B]	13	12 ^[D]
0 ^[A]	1	14	15

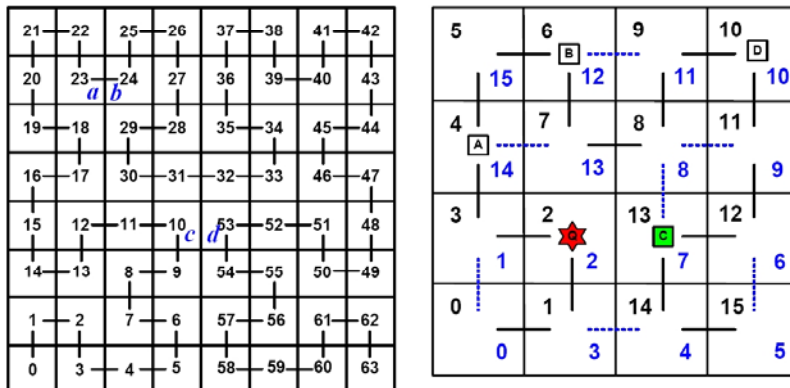
A dashed rectangle highlights a range query area covering points 7, 8, 2, and 13.
 Point 0 is labeled 'A', point 2 is labeled 'B', point 8 is labeled 'C', and point 12 is labeled 'D'.
 An upward arrow labeled 'a' is shown below point 1, and a downward arrow labeled 'b' is shown below point 13.
 A rightward arrow labeled 'R' is shown below point 14.



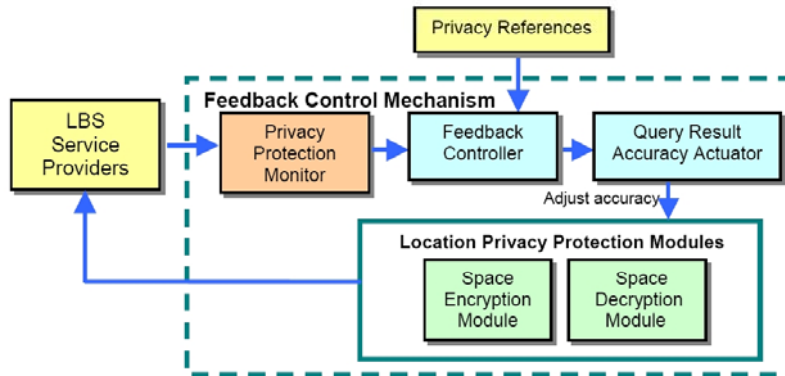
Query Evaluation - *k*NN



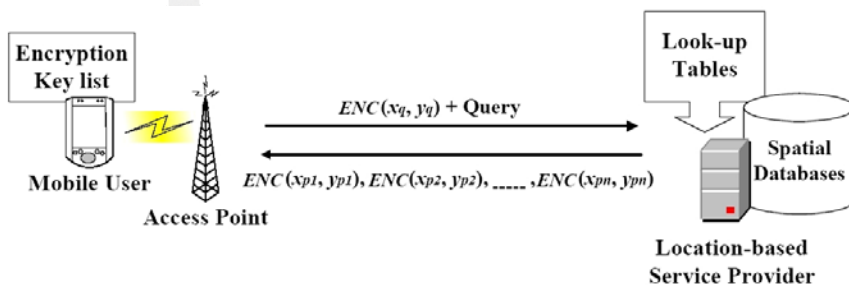
Improving query processing accuracy



Tradeoff Modeling



System Architecture



System Architecture (Cont.)

- The number of encryption keys to be stored in a client?
- The relationship between encryption key number and location privacy.
- Encryption key updating frequency.



Topics

- Introduction
- Cloaking-based Solution
- Transformation-based Solution
- **Private Information Retrieval-based Solution**



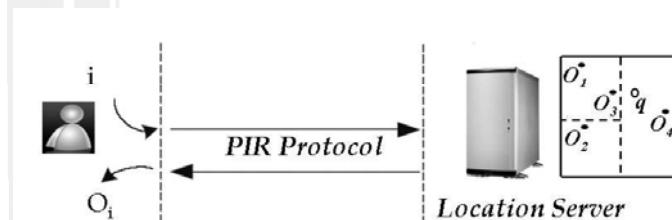
Private Information Retrieval (PIR)

- A user needs to gain access to a specific record of a database but does not want to reveal **the record in which s/he is interested**.
- A PIR protocol allows a user to retrieve the i^{th} record from a database of size n stored at an untrusted server, without revealing i to the server.
- Theoretical PIR and practical PIR.

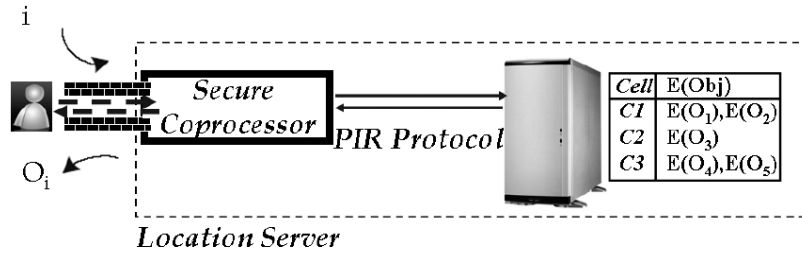


Theoretical PIR

- The client and server follow a secure two-party computation which allows the client to privately retrieve the i^{th} bit from a bit string of size n owned by the server.



Practical PIR



Practical PIR (Cont.)

