Secure Distance Computation Using Homomorphic Encryption

Alagu Valliappan  aav5705@rit.edu
Advisor:  Dr. Peizhao Hu  ph@cs.rit.edu

INTRODUCTION
Geosocial applications are very popular, utilizing the powerful localization techniques of the mobile devices for various social networking opportunities. In the trade off between exposing location co-ordinates and utilizing the power of geolocation, we compromise privacy even to the applications that only need nearby information. This project is intended to securely compute the distance of encrypted location information using Homomorphic Encryption (HE).

HOMOMORPHIC ENCRYPTION
Cryptographic technique that allows arbitrary functions to be computed on encrypted data. It holds the property that applying any operation on the encrypted data will produce the same result as applying the same operation on plaintext and then encrypting it.

- Fully Homomorphic Encryption (FHE)
- Somewhat Homomorphic Encryption (SWHE)

SCENARIO
Bob wants to know if Alice is nearby without sharing precise location coordinates with the service provider or each other.

SOMETHOW HOMOMORPHIC ENCRYPTION SCHEME
- FV2012: A cryptographic scheme based on the Ring-LWE assumption which states that, if \( s \) and \( a \) are uniformly sampled from \( \mathbb{R} \), and \( e \) from \( \mathcal{X} \) such that \( b_i = a_i \cdot s + e_i \), then the pairs \((a_i, b_i)\) are computationally indistinguishable from \((b'_i, b''_i)\), where \( b'_i \) are uniformly sampled from \( \mathbb{R} \).
- For secret key \( s \) and scale invariant \( \Delta \in \mathbb{Q}/\mathbb{T} \), the basic HE operations are defined as:

\[
\text{PublicKeyGeneration:} \quad \text{ct} = \left( \left[ - \left( a \cdot s + e \right) \right]_q, a \right)
\]

\[
\text{Encrypt:} \quad \text{ct} = \left( \left[ p_u \cdot u + e_1 + \Delta \cdot m \right]_q, \left[ p_i \cdot u + e_2 \right]_q \right)
\]

\[
\text{Decrypt(s, ct)}: \quad \frac{\text{ct}}{q} - \left[ c_0 + c_1 \cdot s \right]_q
\]

- This scheme supports addition and multiplication operations that are used to construct functions required for the distance computation techniques.

TECHNIQUES

EUCLIDEAN DISTANCE
Computation of exact point-to-point distance between two encrypted co-ordinates using HE Native Operations.

- The user can infer the circular bounding area of the possible locations of the other user and then use the process of elimination or multiple queries to obtain exact location along the circumference.
- The error grows with increase in distance.

GEOHASHING
Computation of nearby distance based on a spatial cloaking concept.

- Maps every location to a reduced dimension and assigns a quad key to every geolocation.
- The closer the points, the longer the matching prefix of quad key which is then mapped to the bounding box returned as the result.
- The quad key is converted to a binary polynomial and encrypted using the scheme with the errors are sampled from the gaussian noise.
- The prefix matching is formulated as a string matching problem and solved by applying XNOR on the encrypted polynomials resulting in the common prefix.
- Provides only the maximum distance between the coordinates based on the bounding box.

RESULTS
Raspberry Pi, Odroid-XU3 and Amazon EC2 were used to test and the results are summarized below.

SCENARIO
Bob wants to know if Alice is nearby without sharing precise location coordinates with the service provider or each other.

CONCLUSION
Among the two approaches prototyped, geohashing was better suited for preserving privacy. The underlying Ring-LWE problem determines the security. Future work includes improving the speed of geohashing and supporting multiple key encryption.

REFERENCES