PRIVACY-PRESERVING INDOOR LOCALIZATION

Raine Nieminen, Kimmo Järvinen

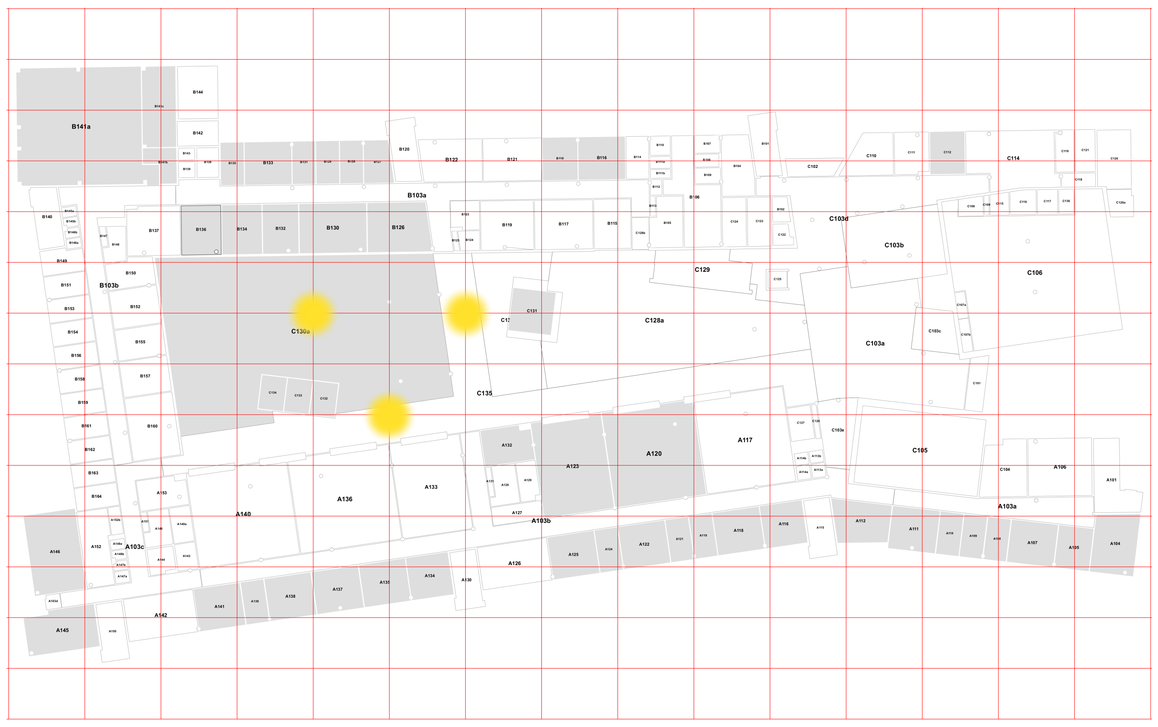
Department of Computer Science, University of Helsinki

FINGERPRINT-BASED INDOOR LOCALIZATION

⋆ An interest in indoor location-based services has been growing over the recent years (e.g., hotels, malls, . . .)

⋆ Global Navigation Satellite Systems (GNSS) are often unavailable indoors and different methods, such as fingerprint-based localization, need to be used instead

⋆ The service provider (SP) constructs a database $\mathfrak{D}$ by measuring received signal strengths (RSS) from access points (e.g., WiFi) at different reference locations



$$\mathfrak{D} = \begin{bmatrix} \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ (4,8,1) & 0 & 4 & 1 & 0 & 0 & 0 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ (6,8,1) & 0 & 2 & 0 & 0 & 4 & 4 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ (5,6,1) & 0 & 0 & 0 & 3 & 0 & 8 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{bmatrix}$$

⋆ A client measures RSS at its location and obtains a personal "fingerprint", e.g., $(0, 3, 1, 0, 3, 2, \dots)$

⋆ The SP's server compares the client's fingerprint to the database and returns the nearest location

PRIVACY CONCERNS

⋆ The server knows clients' locations, and therefore SP is able to track the clients

⋆ If the clients do the comparisons locally (i.e., $\mathfrak{D}$ is distributed), SP gives away its only asset

⋆ In privacy-preserving localization, we want to:

a) Preserve clients' location information private (i.e., the fingerprint)

b) Preserve SP's database $\mathfrak{D}$ private

PAILLIER ENCRYPTION

⋆ The clients' fingerprint can be encrypted with additively homomorphic encryption scheme denoted $E(\cdot)$

⋆ Squared Euclidean distance is computed on the server:

$$E\left(\sum v^2\right) \cdot \prod E\left(-2f\right)^v \cdot E\left(\sum f^2\right)$$

where f is client's RSS value and v is entry from $\mathfrak{D}$

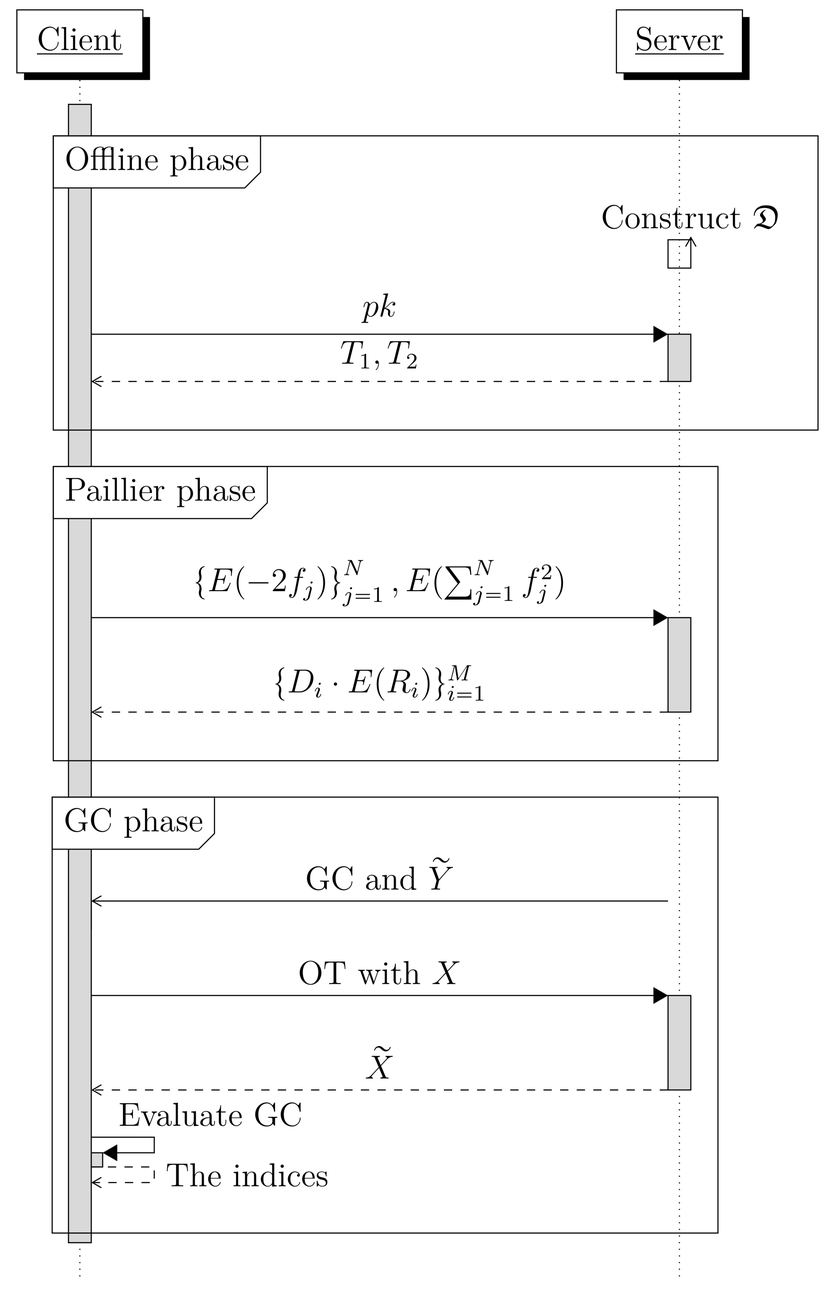
GARBLED CIRCUITS

⋆ The distances reveal $\mathfrak{D}$ to the client after multiple queries, and thus they need to be masked

⋆ Multi-party computation technique based on Garbled circuits (GC) is used to:

1. Remove the mask from the distances
2. Sort and return the index of the smallest distance

SYSTEM OVERVIEW



▷ Paillier cryptosystem increases computational overhead

▷ Garbled circuits increase communication overhead

▷ Security relies on well-studied protocols (Paillier, GC)

▷ MPC operations stay simple and scheme is practical

Contact: {raine.nieminen, kimmo.u.jarvinen}@helsinki.fi