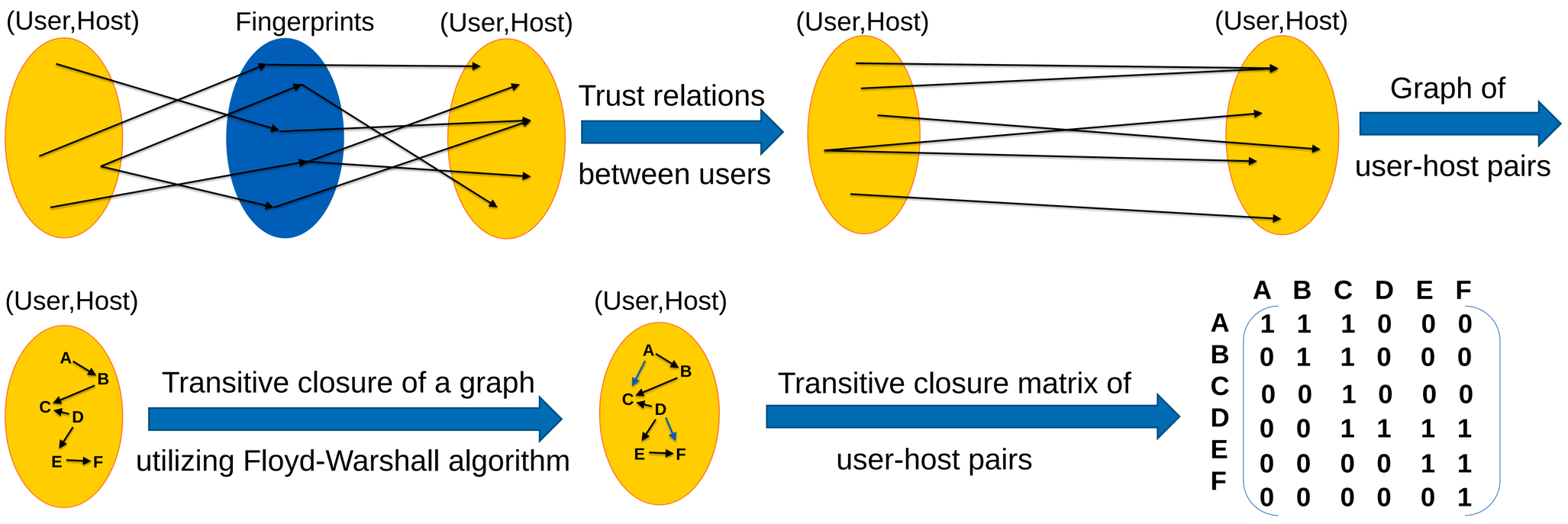
Cloud-Assisted Security Services (CloSer)
Department of Computer Science, University of Helsinki

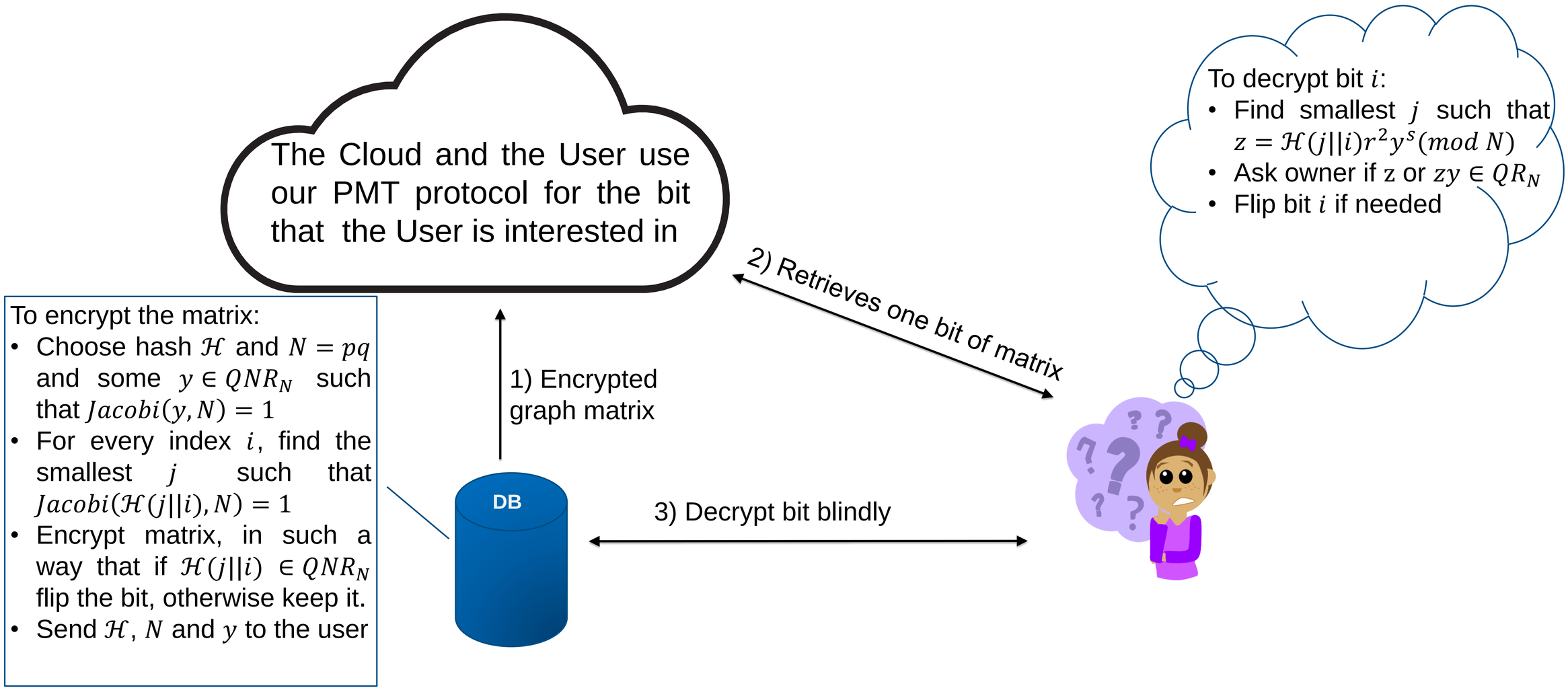
Sara Ramezanian, Tommi Meskanen and Valtteri Niemi

Private Graph Search

- **Introduction**: A Private Graph Search protocol enables users to query the graph to find if there is a path from node A to node B without revealing their queries. Users are also prevented from learning anything else about the graph.
- **Protocol:** The database owner holds two lists of triplets: (sourceuser, sourcehost, fingerprint) and (fingerprint, sourceuser, sourcehost). These define **trust relations** between users on different hosts. This database can be illustrated as a directed graph.



- **Queries on Transitive Closure:** We store the encrypted matrix in a cloud that is not allowed to know what bit is queried. There are three parties in this protocol: Owner of the graph, the User and the Cloud.



- **Conclusion:** We use Goldwasser-Micali and Paillier homomorphic encryption schemes in our protocol. After executing the protocol, user obtains the value of just one bit in the matrix. Cloud does not learn the graph nor the user's query, and the graph owner does not learn the nodes that the user is interested in.

Ramezanian, S., Meskanen, T., Naderpour, M., Niemi, V. "Private Membership Test Protocol with Low Communication Complexity" . In NSS 2017.
Meskanen, T., Liu, J., Ramezanian, S., & Niemi, V. (2015, August). Private membership test for bloom filters. In *Trustcom/BigDataSE/ISPA*

HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

ssh communications security

Tekes