Seal: Secure Engine for AnaLytics From Secure Similarity Search to Secure Data Analytics

CNS-1514526, Feifei Li, lifeifei@cs.utah.edu, Huijia Rachel Lin, rachel.lin@cs.ucsb.edu, Jeff Phillips, jeffp@cs.utah.edu

THE UNIVERSITY OF UTAH   **UCSB**

Challenge:

- Design and implement SEAL --- a secure and efficient engine for performing a wide range of analytic tasks over private data

Solution:

- Design secure similarity search as the basis

- Support secure analytics by decomposing complex analytic tasks into similarity searches and other simple queries like range queries

Scientific Impact:

- Supporting data analytics over private data is an important security goal on its own and will be essential for a more secure and trustworthy cloud.

Broader Impact:

- SEAL helps build a more secure cloud, which benefits the society at large.

- Implementation of SEAL will be open-sourced, which helps technology transfer.

Our results: $\sqrt{N}$ is the tradeoff between partition size and client storage cost.

$$G_1 = \{p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8, p_{10}\}$$
$$G_2 = \{p_5, p_6, p_7, p_8, p_{10}, p_9, p_{11}, p_{12}, p_{13}, p_{14}, p_{15}, p_{16}\}$$

Voronoi Diagram Based Partitioning

$E(i) = 100...010...$