An Algorithmic Framework For Differentially Private Data Analysis on Trusted Processors

Joshua Allen, Bolin Ding, Janardhan Kulkarni
Harsha Nori, Olga Ohrimenko and Sergey Yekhanin

Local vs. Global Differential Privacy (DP)

Local DP
\[ \Pr[\mathcal{A}(v) \in S] \leq e^\varepsilon \Pr[\mathcal{A}(v') \in S] \]

Global DP
\[ \Pr[\mathcal{A}(D_1) \in S] \leq e^\varepsilon \Pr[\mathcal{A}(D_2) \in S] + \delta \]

Information is Leaked via Side-Channels

External Memory

Memory access patterns to external memory compromise differential privacy guarantees

Trusted Execution Environment:
- containers for code and data
- isolated from the rest of the system (hypervisor, OS)
- data always encrypted in RAM
- remote attestation

Intel SGX

Differential Privacy with Trusted Processors

Differentially Private Data Analysis

secret keys

budget

noise

Query

Trusted Execution Environment:

Oblivious Differential Privacy

\[ \Pr[\mathcal{A}(D_1) \in (O, S)] \leq e^\varepsilon \Pr[\mathcal{A}(D_2) \in (O, S)] + \delta \]

where \( O \) is a subset of outputs and \( S \) is a subset of memory access patterns produced by \( \mathcal{A} \)

Oblivious Differentially Private Histogram Algorithm:

Histogram code

Bucket counters

Oblivious Shuffle

Dummies