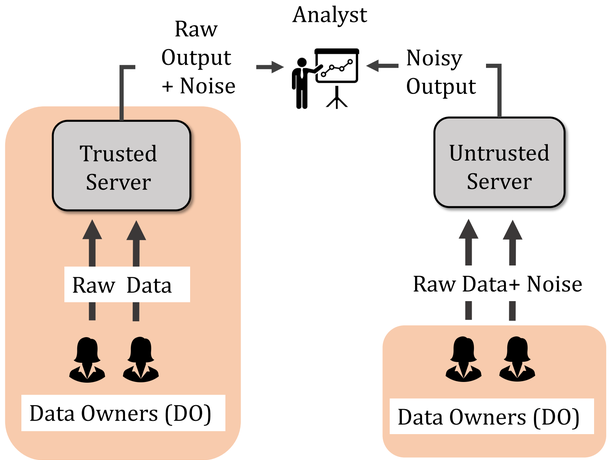
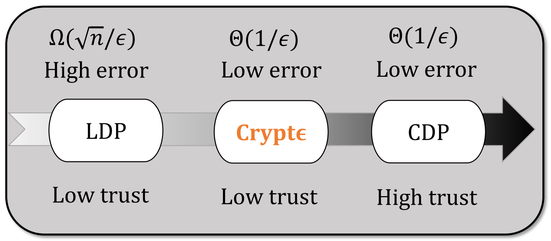
# 1. Problem Statement

- **Differential privacy (DP)** is currently the de facto standard for achieving data privacy

**Central DP (CDP)** **Local DP (LDP)**

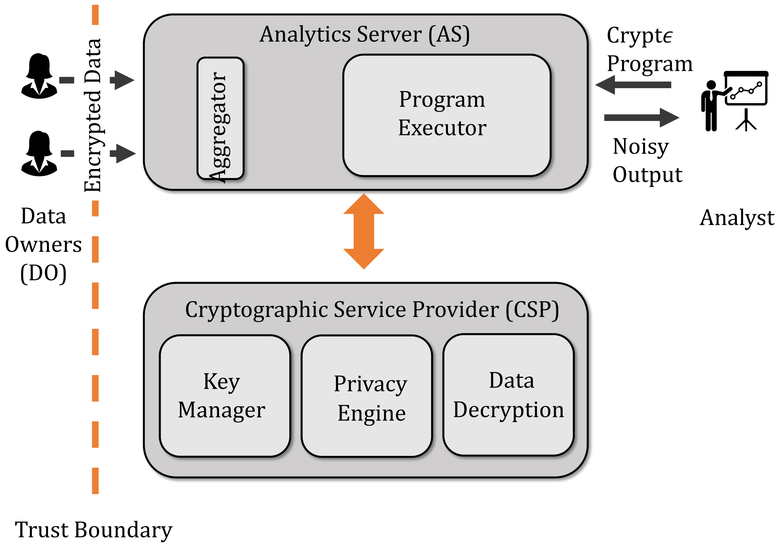



**Crypte** achieves the best of both worlds via **cryptographic primitives**

- Linear Homomorphic Encryption
- Garbled Circuits

# 2. Crypte Overview

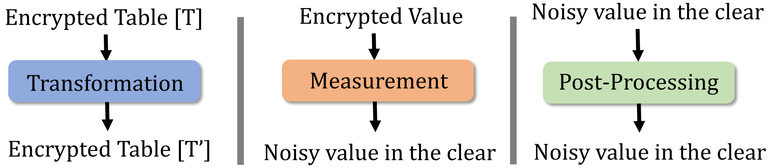



**Two-Server Model**

- **Analytics Server (AS)**: Stores encrypted data from DOs and executes DP programs on it
- **Crypto Service Provider (CSP)**: Manages the cryptographic primitives and collaborates with AS to generate outputs

# 3. Crypte Programming Framework

Crypte supports 3 types of operators




# 4. DP Index Optimization

**Program**: Output the marginal over attributes $Age(A)$ and $Gender(G)$ for Canadian employees

- Without optimization – compute over entire dataset
- Index on $Nation$ – compute only on a subset of rows
- Construct a noisy index since true index violates DP

**No Optimization**

Project $\pi_{A,G,N}$ $\{n\}$

Filter $\sigma_{N=Ca}$ $\{n\}$

CrossProduct $\times_{A,G}$ $\{n\}$

GroupBy $\gamma^{count}_{A\times G}$ $\{n\}$

Laplace $Lap$

$\{n\}$

| A | G | N |
|---|---|---|
| [30] | [M] | [Ca] |
| [47] | [F] | [N2] |
| [43] | [M] | [N5] |
| ... | ... | ... |
| [31] | [M] | [Ca] |

**DP Index Optimization**

Project $\pi_{A,G,N}$ $\{n\}$

Filter $\sigma_{N=Ca}$ $\{n'\}$

CrossProduct $\times_{A,G}$ $\{n'\}$

GroupBy $\gamma^{count}_{A\times G}$ $\{n'\}$

Laplace $Lap$

$\{n'\}$

| A | G | N |
|---|---|---|
| [30] | [M] | [Ca] |
| [43] | [M] | [Ca] |
| [31] | [M] | [Ca] |
| ... | ... | ... |
| [43] | [M] | [N5] |

# 5. Evaluation Highlights

UCI Adult Dataset: ~33K records, 4 attributes

- Crypte achieves same order of magnitude of error as CDP
- Proposed optimizations improve performance by **41-5667X**
- A large class of programs run in **3.5 hrs** for **1M** records