Privacy Preserving Smart Metering
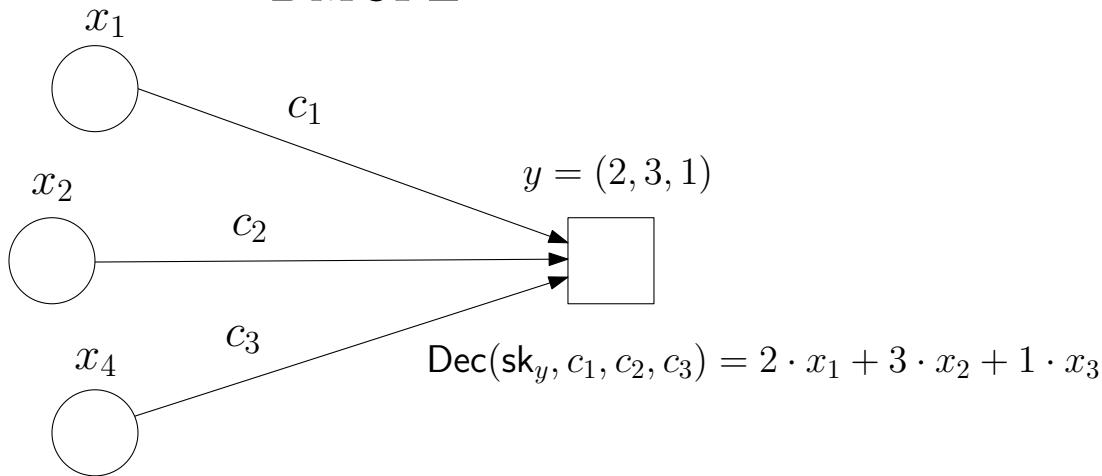
Johannes Ernst

2021-01-15
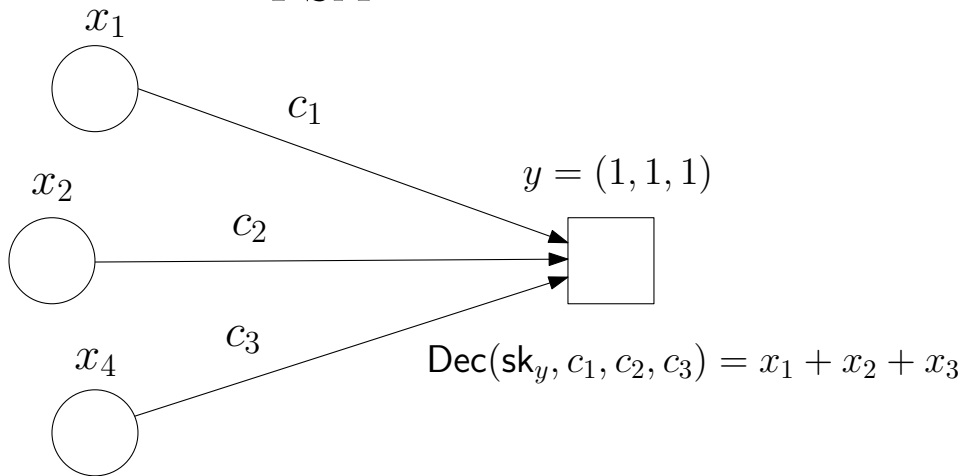
Smart Meter

DMCFE

x_1

c_1

x_2

c_2

$y = (2, 3, 1)$

x_4

c_3

$\mathsf{Dec}(\mathsf{sk}_y, c_1, c_2, c_3) = 2 \cdot x_1 + 3 \cdot x_2 + 1 \cdot x_3$

PSA

x_1

c_1

x_2

c_2

$y = (1, 1, 1)$

x_4

c_3

$\mathsf{Dec}(\mathsf{sk}_y, c_1, c_2, c_3) = x_1 + x_2 + x_3$
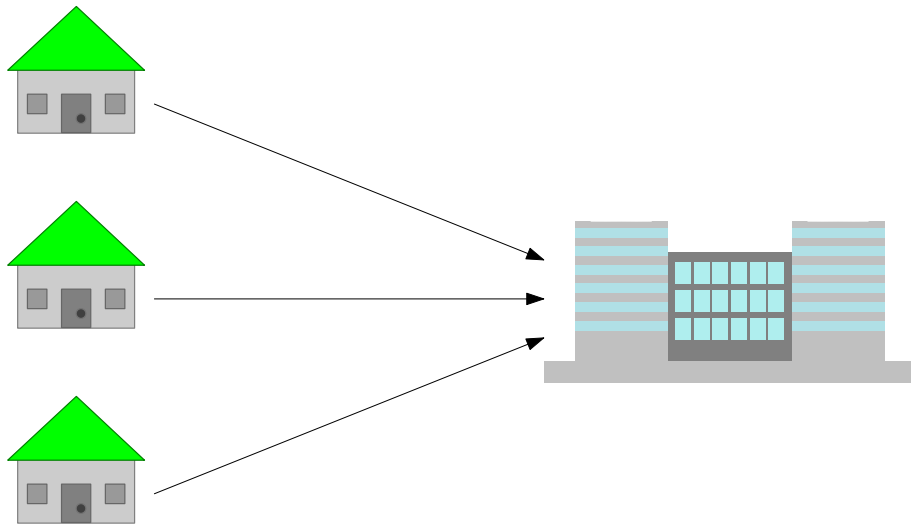
Results

- decentralized setup is very slow for both PSA and DMCFE
- decryption in PSA faster than in DMCFE, but not as much as expected

Other Use Cases

- Heatmaps
- Federated Learning