

1. Membership Inference

Given $f(\text{data})$, infer $x \in \text{data}(\text{e.g., } f \text{ is a aggregation})$

[HSR+08, WLM+09] for generic data

[Pyrgelis et al., NDDS'18] for *mobility* data

Membership inference is a very active research area, not
only in machine learning



Well-understood problem (beside leakage)

Use it to establish wrongdoing

Or to assess protection, e.g., with differentially private noise

MEMBERSHIP INFERENCE

DOES NOT COME FROM ML



Given $f(\text{data})$, infer if $x \in \text{data}$ (e.g., f is aggregation)

[HSR+08, WLW+09] for **genomic** data

[Pyrgelis et al., NDSS'18] for **mobility** data

Use it to establish wrongdoing

Or to assess protection, e.g., with differentially private noise

2. Inferring Class Representatives

