Some useful properties for ML

Post-processing Theorem

If $M(D)$ is ϵ-private, and f is any function, then $f(M(D))$ is ϵ-private.

Composition Theorem

If $M_1, \ldots, M_k$ are ϵ-private, then $M(D) \equiv \left(M_1(D), \ldots, M_k(D)\right)$ is $(k * \epsilon)$-private

Modularity

We can design algorithms as we normally would. Just access the data using differentially private subroutines, and keep track of our “privacy budget”

36

Some useful properties for ML

Post-processing Theorem

If $M(D)$ is ϵ-private, and f is any function, then $f(M(D))$ is ϵ-private.

Composition Theorem

If $M_1, \ldots, M_k$ are ϵ-private, then $M(D) \equiv \left(M_1(D), \ldots, M_k(D)\right)$ is $(k * \epsilon)$-private

Modularity

We can design algorithms as we normally would. Just access the data using differentially private subroutines, and keep track of our "privacy budget"

A Simple Proposal [ICDM'17]

Dataset D
Private Kernel K-means
Cluster 1
Cluster 2
Cluster k
Private Generative NN 1
Private Generative NN 2
Private Generative NN k
θ_1
θ_2
θ_k
Data Reconstruction
Synthetic Dataset