Experimental Evaluation

Numerically compute privacy guarantees (privacy budget)

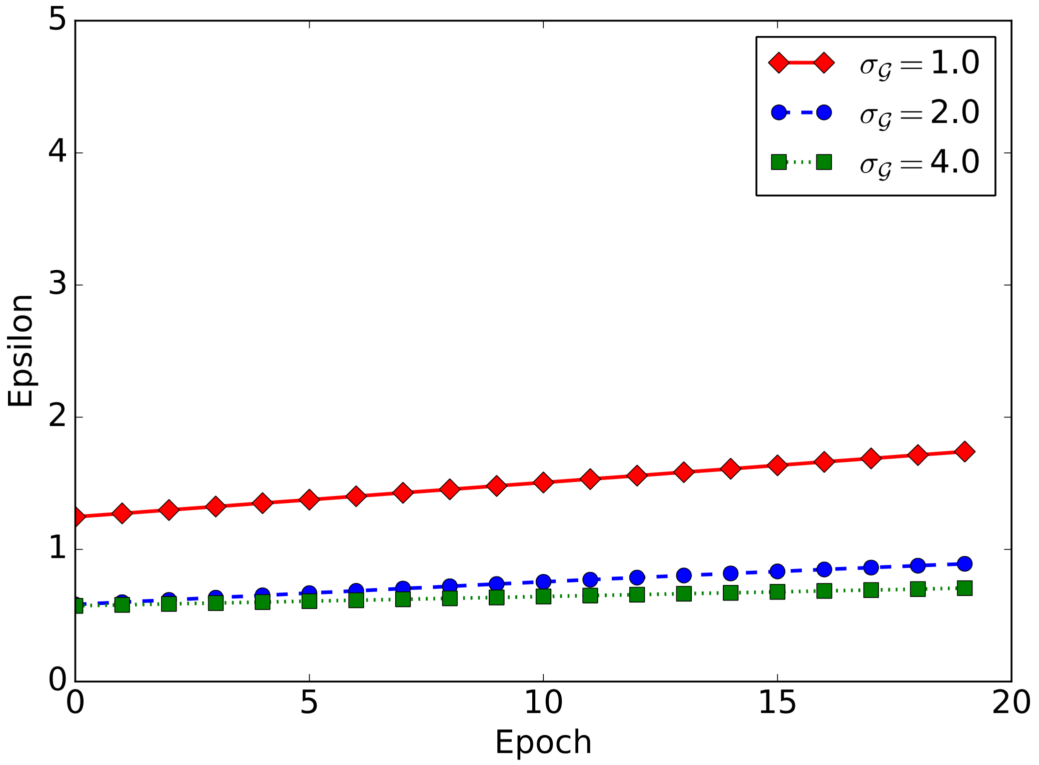
Test on two Generative NN Models:

- Restricted Boltzmann Machines (RBM) [200 hidden neurons]
- Variational Auto-Encoder (VAE) [200 hidden neurons, 2d latent space]

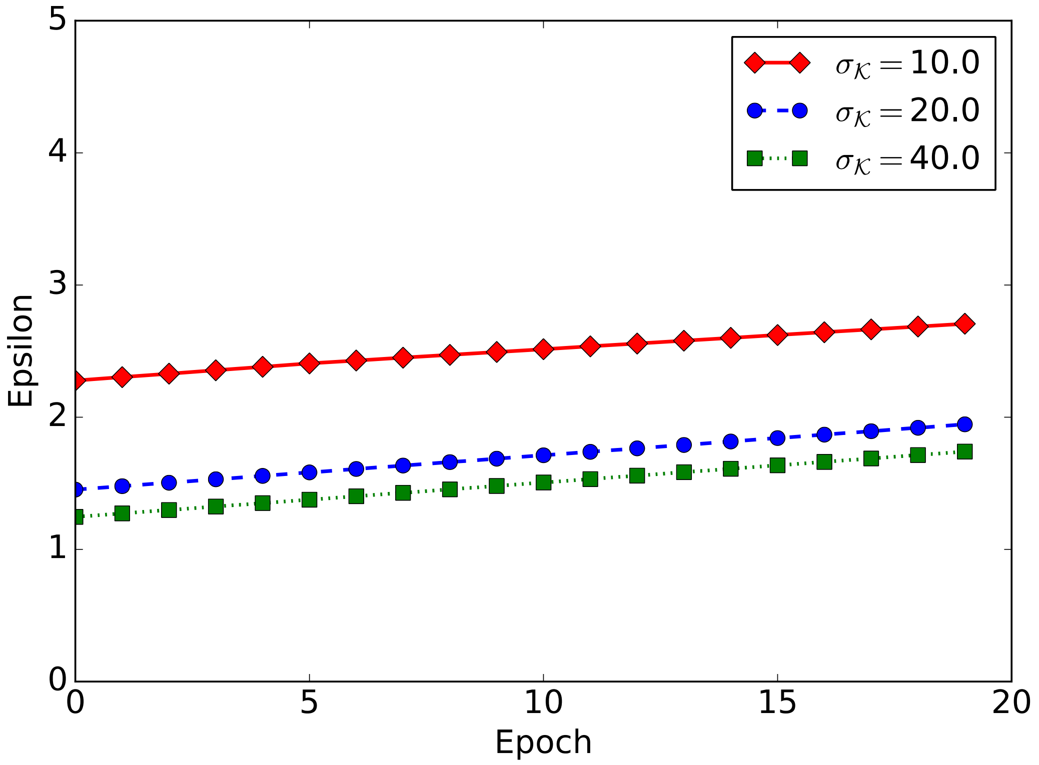
Evaluate quality of generated samples (digits) on MNIST

Use Case: Counting Queries on synthetic data

Privacy guarantees



SGD noise



Clustering noise