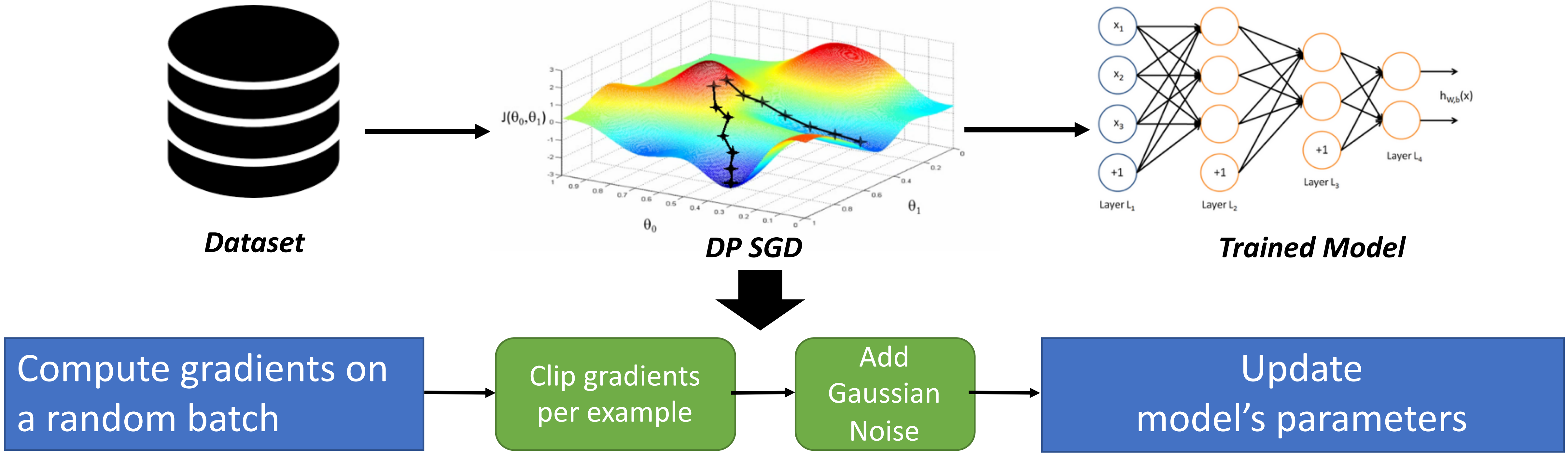
Differentially Private SGD

Adaptive selection of the norm bound for gradients clipping



Dataset

DP SGD

Trained Model

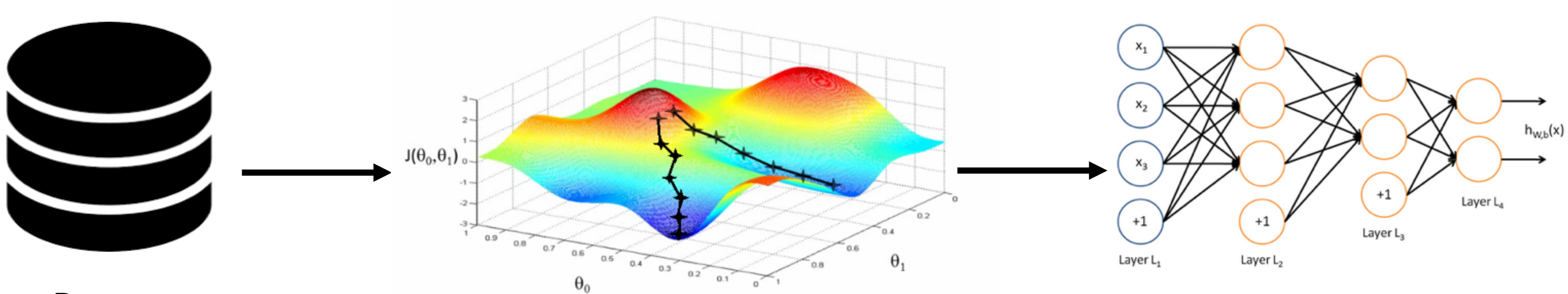
Compute gradients on a random batch

Clip gradients per example

Add Gaussian Noise

Update model's parameters

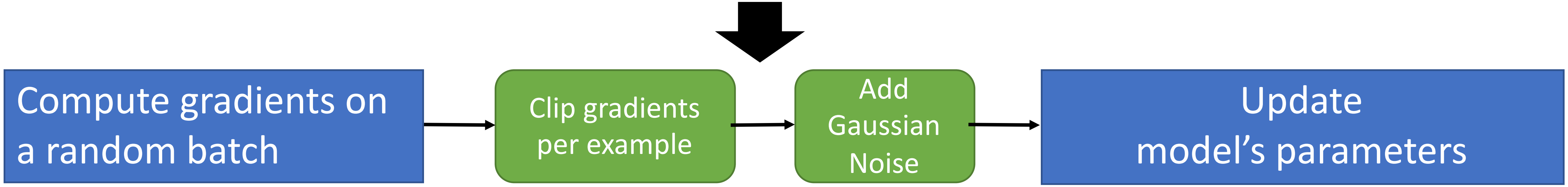
Differentially Private SGD



Dataset

DP SGD

Trained Model



Compute gradients on a random batch

Clip gradients per example

Add Gaussian Noise

Update model’s parameters

Adaptive selection of the norm bound for gradients clipping

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