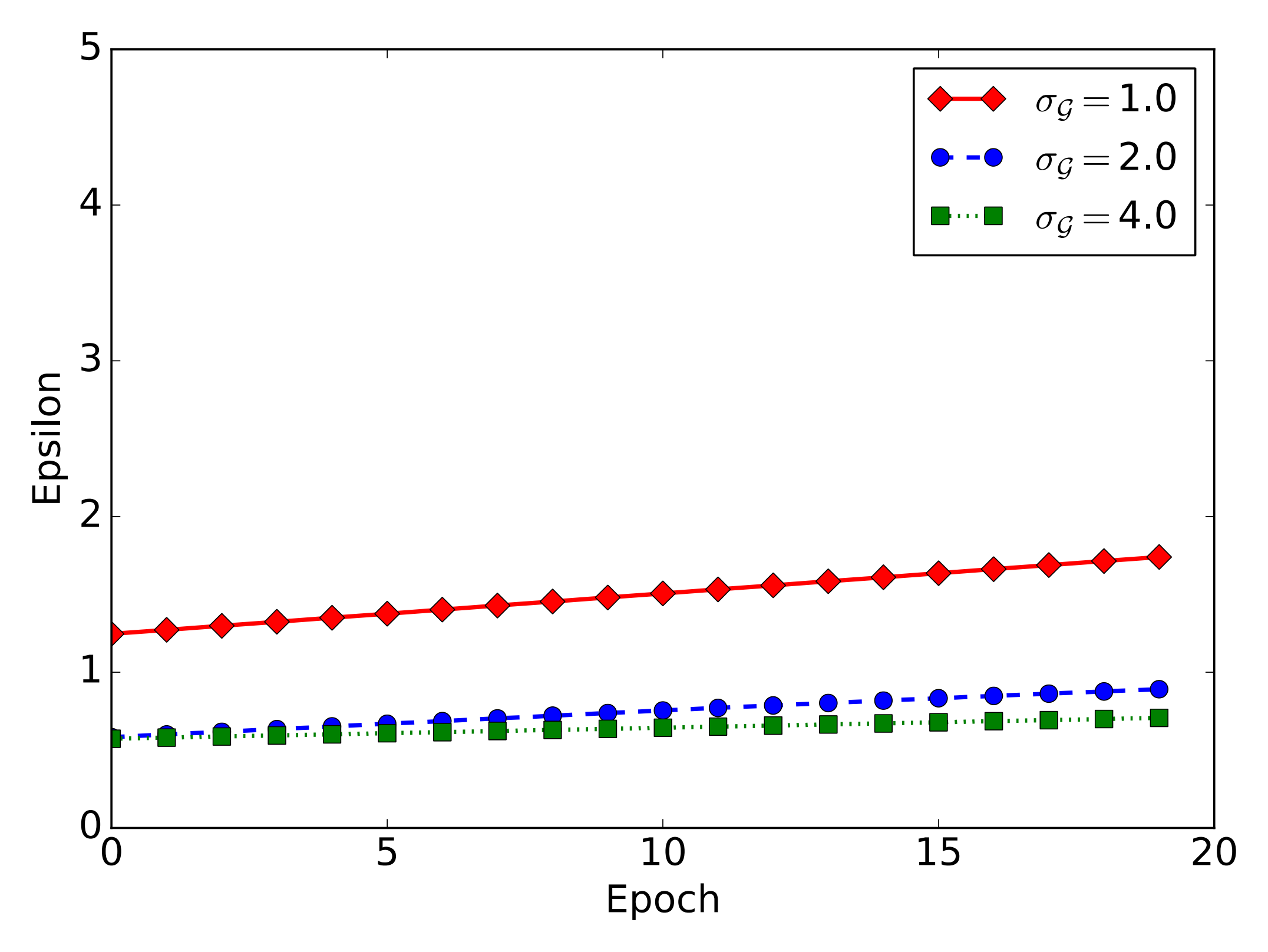
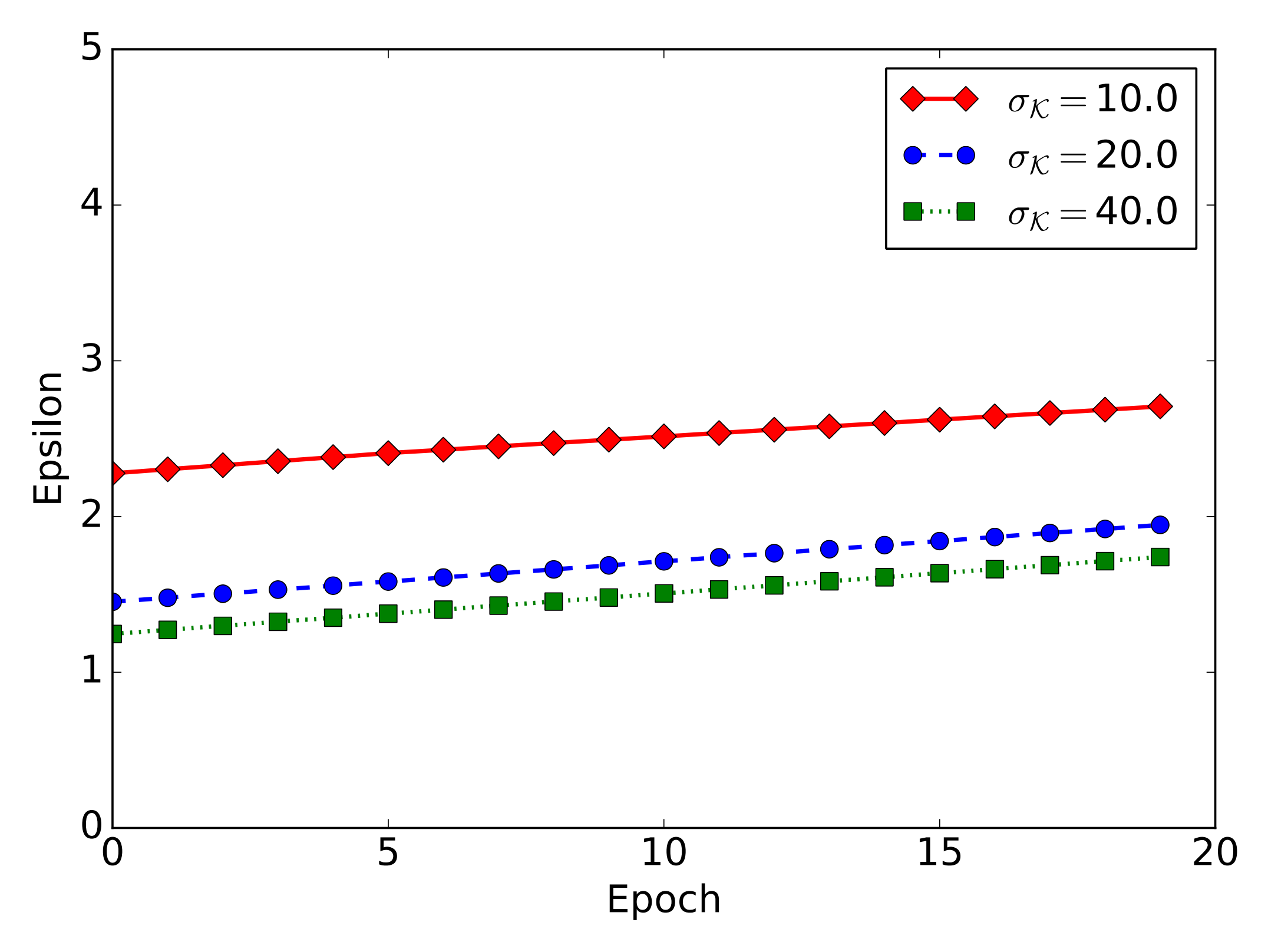
Privacy guarantees


5
4
3
2
1
0
Epsilon
0
5
10
15
20
Epoch
$\sigma_{\mathcal{G}} = 1.0$
$\sigma_{\mathcal{G}} = 2.0$
$\sigma_{\mathcal{G}} = 4.0$


5
4
3
2
1
0
Epsilon
0
5
10
15
20
Epoch
$\sigma_{\mathcal{K}} = 10.0$
$\sigma_{\mathcal{K}} = 20.0$
$\sigma_{\mathcal{K}} = 40.0$

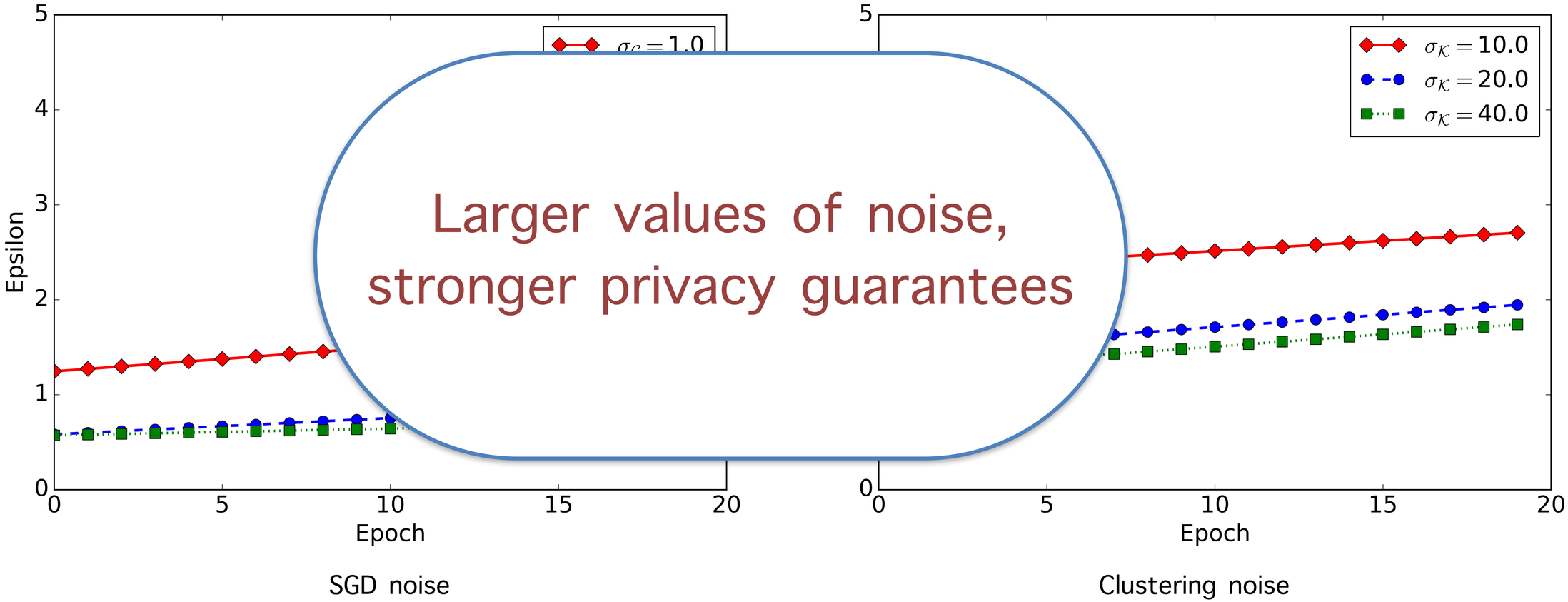
Clustering noise

SGD noise

41

Larger values of noise, stronger privacy guarantees

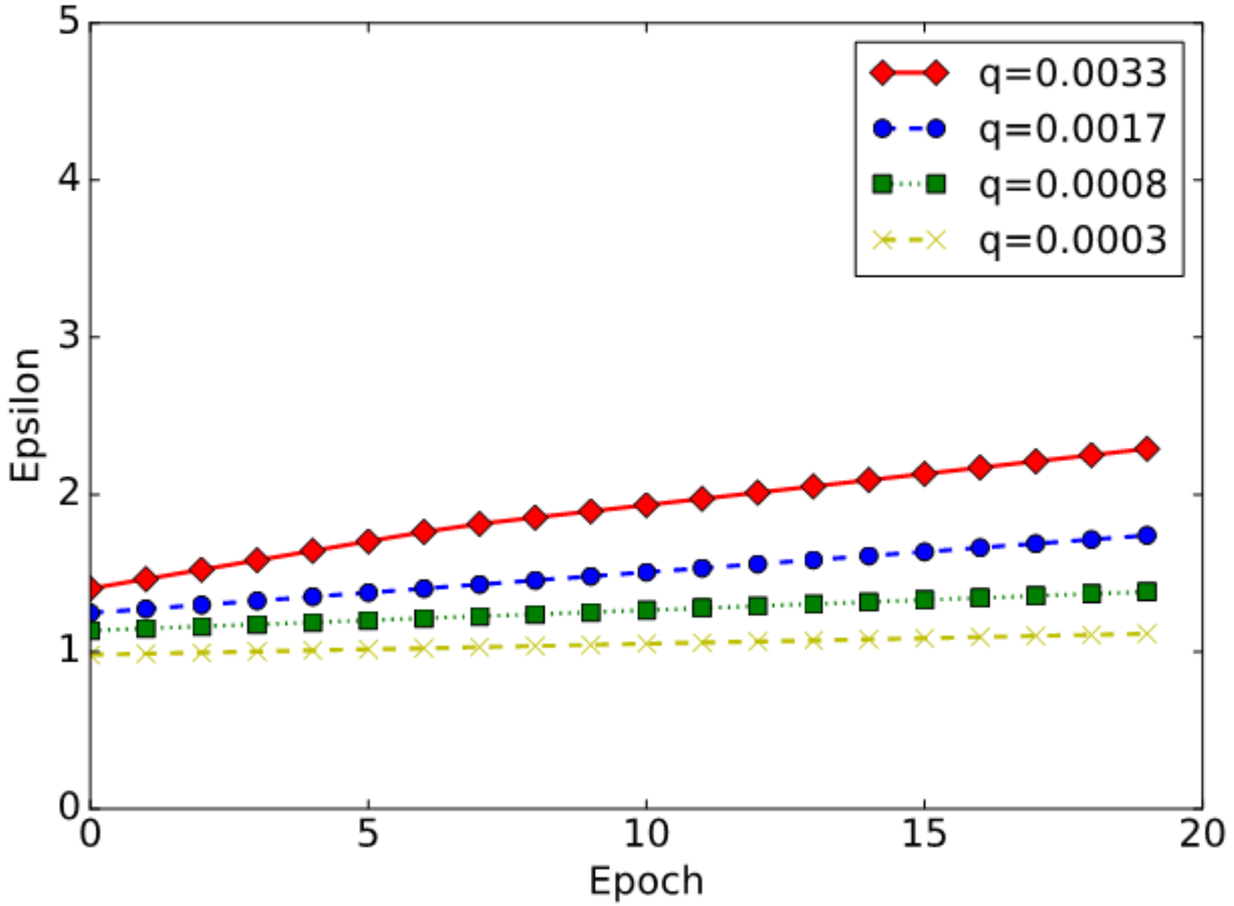
Privacy guarantees



SGD noise

Clustering noise

Privacy guarantees



Sampling probability

$$q = \frac{batch\ size}{|\ Dataset\ |}$$