Machine Learning with Exponential Mechanism of Differential Privacy

Duo Li 2021215246
TBSI, Tsinghua University, China

Abstract

- Since 2018 Facebook data privacy scandal, privacy has once again become a dominant feature in peoples minds[1].
- The work on the preservation of privacy and machine learning is still in an infancy stage.
- Current research can not balance the data utility and privacy perfectly.

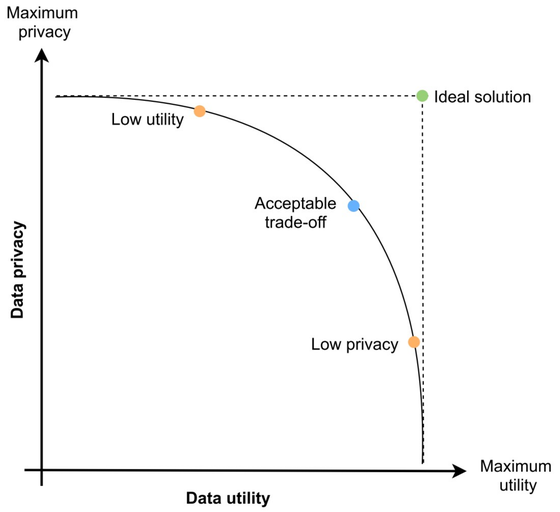

Figure1. Trade-off between privacy level and utility level of data. [2]

Method

Differential privacy

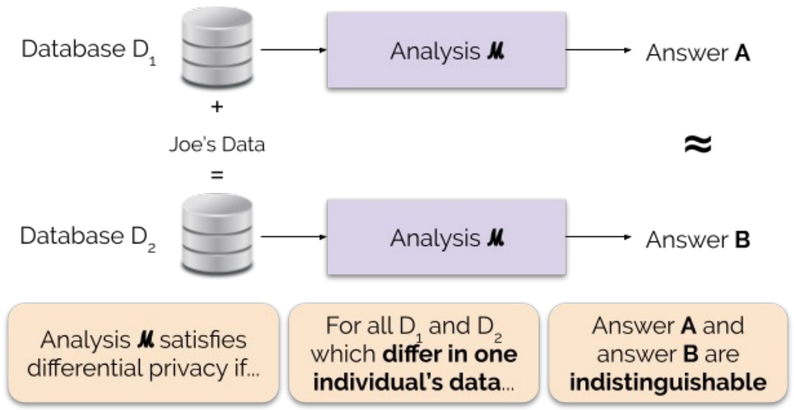

Figure 3. Informal Definition of Differential Privacy.

Proposed method

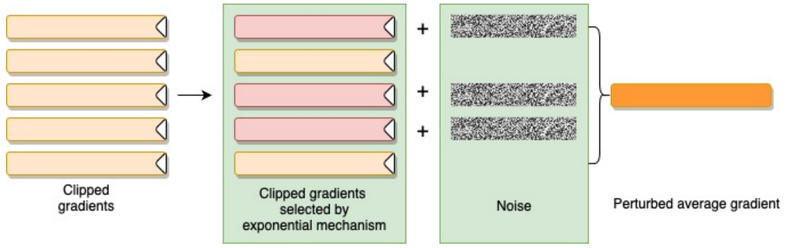

Figure 4. Workflow of our method.

Mechanisms

- Laplace mechanism will add noise , which is following Laplace distribution, to real-value numerical variables.

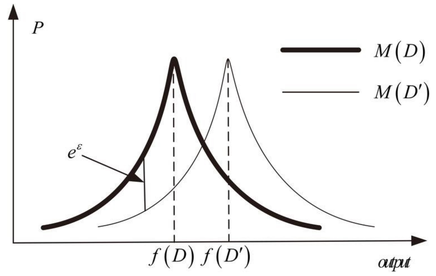

Figure 5. Illustration of laplace mechanism.

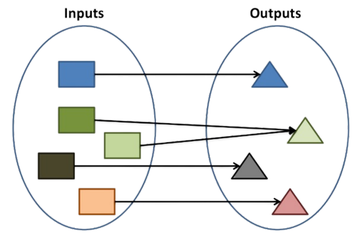

Figure 6. Illustration of exponential mechanism.

- Exponential Mechanism returns a value exactly in the dataset with a probability affected by the parameter of the differential privacy.

Results

Model	Parameters	Error
SGD	[1.012 1.990]	0.00093
DP-SGD	[0.924 1.266]	2.90315
Ours	[0.818 1.275]	2.973019

Introduction

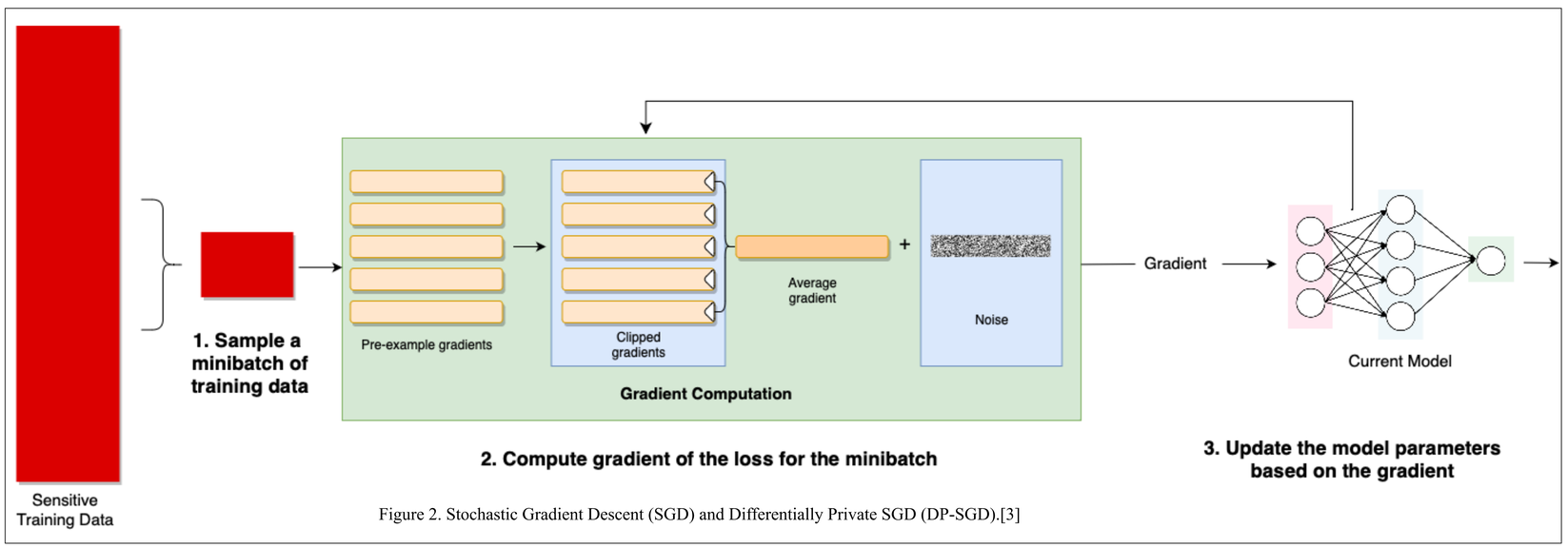

Figure 2. Stochastic Gradient Descent (SGD) and Differentially Private SGD (DP-SGD).[3]

Conclusion

- Compared to traditional machine leaning methods, our method and DP-SGD perform unstable because of privacy concerns.
- Our method proposed a new approach to combine exponential mechanism and laplace mechanism to reduce the expense of privacy budget.

References

[1] Liu, Bo, et al. "When machine learning meets privacy: A survey and outlook." *ACM Computing Surveys (CSUR)* 54.2 (2021): 1-36.
[2]Carvalho, Tânia, et al. "Survey on Privacy-Preserving Techniques for Data Publishing." *arXiv preprint arXiv:2201.08120* (2022).
[3] Abadi, Martin, et al. "Deep learning with differential privacy." *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*. 2016.