CS 208 - Applied Privacy for Data Science Project Description

Jason Huang
Spring 2019 - Harvard University

Summary of Project Description and Plan

For this final project, a roughly 10-page report will be the ultimate deliverable along with a brief oral presentation. The focus will be on data that is under continual observation and examining privacy budget in for this type of data with references to composition theorems to understand how privacy loss compounds over time. Continuously generated data closely coincides with popular differential privacy applications for collecting distributed user data, and the project will therefore draw heavily upon local-DP concepts. In particular, the study will be grounded in practical analysis and attacks on local-DP, hopefully including commercial implementations like RAPPOR. Directions for future study would include connections to streaming algorithms and similar work on other commercial differential privacy instances.

1 Preamble and Motivation

Quantifying privacy loss is fundamental to privacy protection. Differential privacy provides such a means through a mathematical definition for privacy. In particular, a privacy loss parameter ϵ is defined for this purpose [5]. In this sense, the privacy budget is key to the goal of differential privacy as it is the mechanism by which release of sensitive information can be monitored and controlled. Usually, the privacy budget consists of a fixed global ϵ value, with each released statistic permanently consuming a portion of the budget.

While differential privacy originated with the centralized model where a single trusted curator is responsible for protecting the data, the local model has gained traction particularly in commercial applications for its distributed nature. In particular, it does not require a trusted curator and provides its privacy guarantees at the point of collection [3].

The focus of this project will be reconciling the critical budgeting concept of differential privacy with practical implementations that continuously connect data from users in a locally private manner. In particular, a large portion will be practical by simulating these concepts, backed by theoretical discussion of literature in this field and related fields.

2 Privacy for Continually Generated Data

Literature has developed on data with a temporal element, known interchangeably as continually observed or evolving data. These papers examine how privacy is affected over time and, most notably, how privacy can be weakened due to improper consideration of ϵ composition over time [1, 4, 6]. Some of these include examinations of local-DP system implementations in particular, which will also be a focus of this project, given the inherent nature of distributed user-generated data as the ideal practical scenario to involve time. Analysis of composition

over time will be undertaken in specific practical studies, as discussed in following sections. One of the papers highlights a differentially private application to the high-profile heavy hitters problem, for example.

A useful preceding paper conducting similar work is by Tang et al. on the shortcomings of Apple's differential privacy system. In particular, the section on *Report Generation and Privacy Budget Management over Time* [7]

A potential extension on this would be differentially private streaming algorithms. Streaming refers to a continuous "stream" of data to be processed. A common data structure used is a sketch, which retains useful summary information about the data in an efficient and compact manner. In this sense, streaming algorithms are very similar to what has been discussed so far, as streaming algorithms provide a summary much as differentially private mechanisms provide useful statistics, and new data is continuously being provided. Some previous work on differentially private streaming include: a Simons Institute lecture[1] and PeGaSus [2]. Depending on time and how comprehensive the rest of the project is, additional work and discussion will be provided on differentially private streaming.

3 Objectives for Analysis

As discussed in the motivation section, budgeting is critical to privacy protection provided by differential privacy. In the real world, there is often a temporal dimension how sensitive data, often user data, is generated and collected that needs to be seriously considered when evaluating the privacy guarantees that can be made using differential privacy. The main focus will therefore be evaluating privacy loss and utility for data collected over time.

Some key ideas to consider is whether the budget should be defined on a per-event basis or fixed time interval basis. The latter is a more reasonable and feasible approach, but in that case, a research question worth pursuing how would the sparsity or distribution of events across different time intervals affect privacy? If on the other hand, privacy loss is specified on for each event, then this may implicitly assume that the number of events is not protected. For example, if each emoji that a user uses is differentially private, then the number of emojis might then be leaked. A possibility would then be to set stricter constraints (i.e. an ϵ limit per event as well as per day, with the stricter in terms of privacy being selected). The utility will then be evaluated, since the privacy guarantees may be strengthened but likely at the cost of higher noise added.

Such analysis can be conducted through implementation of local-DP mechanisms and empirically evaluating privacy and utility dependent on certain parameters of budgeting across time. Simulation through code implementation of DP algorithms and corresponding attacks will be a major component and likely the primary component of the project. Certain currently existing systems, as will be discussed shortly, can be used for this purpose as well.

The practical elements of the project will be complemented by theoretical discussion that is centered on literature in the field of evolving and continually observed data. Composition theorems [5] will likely be a big focus in this area, but in the context of composition of privacy loss over time.

[1] https://simons.berkeley.edu/sites/default/files/docs/1123/nikolovslides.pdf

4 RAPPOR

RAPPOR (randomized aggregatable privacy-preserving ordinal response) is an early differential private system implemented by Google for their software, particularly in the Chrome browser [9]. Many foundational differential privacy features are implemented, but the system predates much of the literature on differential privacy over time. As a result, there would be vulnerabilities expected in this sense.

Attacks have been successfully attempted on ostensibly secure data systems to demonstrate the necessity of differential privacy, as well as the shortcomings of historical privacy techniques. Some examples are membership attacks and reconstruction attacks. These can be attempted in the context of temporal data with local-DP. *The previously discussed analysis of local-DP for continuous data can be tested on this commercial differential privacy instance as the ideal goal for this project.*

Google has made the RAPPOR source code public[2], which makes detailed study possible. Other commercial instances of differential privacy include work by Apple [8] to incorporate private data collection into their operating systems. It would be preferable to work with other systems beyond RAPPOR such as Apple's, though these are not open-source and may be more difficult to work with for the purposes of this project.

Within the field of differentially privacy, RAPPOR is a comparatively high-profile and comprehensive early system, which makes it well-suited for testing the aforementioned objectives. However, if time or feasibility restraints prove to be a challenge, then a more straightforward evaluation of and attack on RAPPOR will be the project instead. *This will serve as a robust fallback plan in the case that desired results are not obtained.*

5 Timeline

- **Tue. April 9, 2019**: Project description due. This document is the project description that will be submitted, upon which work on the project will immediately commence. Begin with reading literature on differential privacy for continually observed data. Setup practical components by implementing basic local- and centralized-DP algorithms and studying RAPPOR system.

- **Tue. April 16, 2019**: Begin write-up of key ideas behind differentially privacy continually observed data. Begin implementation of analysis/attacks.

- **Tue. April 23, 2019**: Solid preliminary results are expected here. Depending on quality of results, either port previous work to RAPPOR or begin alternate analysis of RAPPOR. Finalize key concepts.

- **Tue. April 30, 2019**: Most key results expected by here. Tie the theoretical discussion and literature to these results and begin work on any follow-up exploration or technical analysis.

[2] https://github.com/google/rappor

- **Tue. May 7, 2019**: Complete core implementation. Focus on writeup and cleaning up practical components.
- **Fri. May 10, 2019**: Draft of final papers due. Complete entire implementation. Prepare brief oral presentation and make (likely minor) edits.
- **Mon. May 13, 2019 - Tue. May 14, 2019**: Project presentations. Based on feedback, make final additions and edits to paper.
- **Fri. May 17, 2019**: Revised final papers due. Solicit feedback and discuss possibility of extending the work in this project or pursuing other directions for differentially private research.

References

[1] Chan, T.-H. H., Shi, E., and Song, D. Private and continual release of statistics. *ACM Trans. Inf. Syst. Secur. 14*, 3 (Nov. 2011), 26:1–26:24.

[2] Chen, Y., Machanavajjhala, A., Hay, M., and Miklau, G. Pegasus: Data-adaptive differentially private stream processing. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (New York, NY, USA, 2017), CCS '17, ACM, pp. 1375–1388.

[3] Cormode, G., Jha, S., Kulkarni, T., Li, N., Srivastava, D., and Wang, T. Privacy at scale: Local differential privacy in practice. In *Proceedings of the 2018 International Conference on Management of Data* (New York, NY, USA, 2018), SIGMOD '18, ACM, pp. 1655–1658.

[4] Dwork, C., Naor, M., Pitassi, T., and Rothblum, G. N. Differential privacy under continual observation. In *Proceedings of the Forty-second ACM Symposium on Theory of Computing* (New York, NY, USA, 2010), STOC '10, ACM, pp. 715–724.

[5] Dwork, C., and Roth, A. The algorithmic foundations of differential privacy. *Found. Trends Theor. Comput. Sci. 9*, 3–4 (Aug. 2014), 211–407.

[6] Joseph, M., Roth, A., Ullman, J., and Waggoner, B. Local differential privacy for evolving data. *CoRR abs/1802.07128* (2018).

[7] Tang, J., Korolova, A., Bai, X., Wang, X., and Wang, X. Privacy loss in apple's implementation of differential privacy on macos 10.12. *CoRR abs/1709.02753* (2017).

[8] Team, D. P. Learning with privacy at scale. *Apple Machine Learning Journal 1* (2017).

[9] lfar Erlingsson, Pihur, V., and Korolova, A. Rappor: Randomized aggregatable privacy-preserving ordinal response. In *Proceedings of the 21st ACM Conference on Computer and Communications Security* (Scottsdale, Arizona, 2014).