Quantifying Differential Privacy Under Temporal Correlations

Yang Cao*#, Masatoshi Yoshikawa*, Yonghui Xiao#, Li Xiong#

* Kyoto University, Department of Social Informatics

Emory University, Department of Math and Computer Science

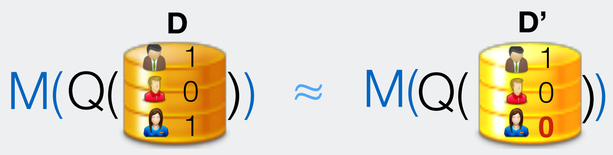
Abstract

- Differential Privacy (DP) has received increasing attention as a rigorous privacy framework.
- However, many existing studies assume that the data are independent.
- In this work, we investigated **how to satisfy DP on temporally correlated data** by finely analyzing, calculating and preventing the potential extra privacy loss under temporal correlations.

Problem

What is DP?

- ε-Differential Privacy (ε-DP) is a de facto **privacy definition** for Privacy Persevering Data Analysis.
  DP mechanism M guarantees that each record has slight effect (bounded by ε) on the output.



- Formally, M satisfies :

$$PL_0(\mathcal{M}) \triangleq \sup_{r, l_i, l_i'} \log \frac{\Pr(r \mid l_i, D_{\mathcal{K}})}{\Pr(r \mid l_i', D_{\mathcal{K}})} \leq \varepsilon$$

r output, i.e., M(Q(D))=r

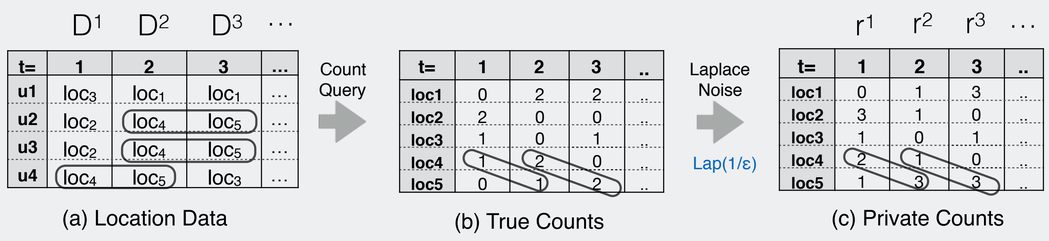
l_i, l_i', possible data of user i

$D_{\mathcal{K}}$ Knowledge of A_i

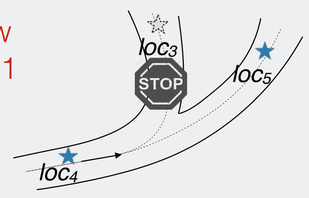
- ε is a metric of privacy leakage. ε ⬆️, privacy ⬇️.

What is the problem of DP under Temporal Correlation?

- Temporal correlations may degrade the privacy guarantee!



When attacker know
$Pr(l^t=loc_5 \mid l^{t-1}=loc_4)=1$
⬇️
2ε-DP at time 2



The question is,
when $Pr(l^t=loc_5 \mid l^{t-1}=loc_4)=0.2$ or 0.3
⬇️
?-DP at time 2

Solution

Analyzing the potential privacy loss

- Model temporal correlations using **Markov Chain**

e.g., user i : $loc_1 \rightarrow loc_3 \rightarrow loc_2 \rightarrow \ldots$

(a) Transition Matrix $\Pr(l_i^{t-1} \mid l_i^t)$

time t-1

time t	loc_1	loc_2	loc_3
loc_1	0.1	0.2	**0.7**
loc_2	0	0	1
loc_3	0.3	0.3	0.4

Backward Temporal Correlation P_i^B

(b) Transition Matrix $\Pr(l_i^t \mid l_i^{t-1})$

time t

time t-1	loc_1	loc_2	loc_3
loc_1	0.2	0.3	0.5
loc_2	0.1	0.1	0.8
loc_3	**0.6**	0.2	0.2

Forward Temporal Correlation P_i^F

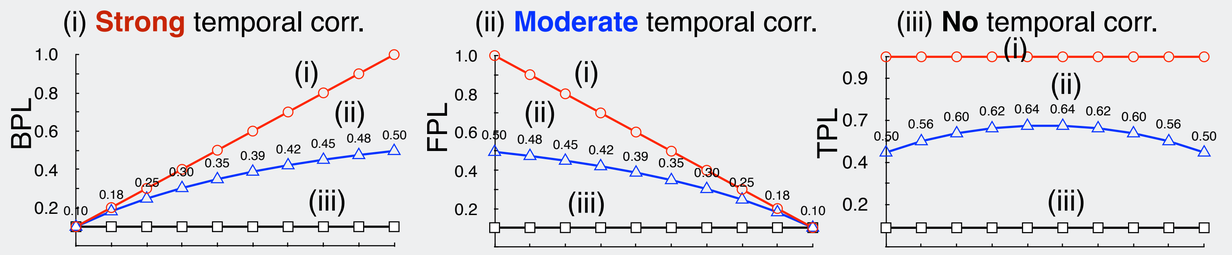
- The Temporal Privacy Leakage (TPL) includes FPL & BPL

$$TPL(\mathcal{M}^t) \triangleq \underbrace{\sup \log \frac{\Pr(r^1,\ldots,r^t \mid l_i^t, D_{\mathcal{K}}^t)}{\Pr(r^1,\ldots,r^t \mid l_i^{t'}, D_{\mathcal{K}}^t)}}_{BPL(\mathcal{M}^t)} + \underbrace{\sup \log \frac{\Pr(r^t,\ldots,r^T \mid l_i^t, D_{\mathcal{K}}^t)}{\Pr(r^t,\ldots,r^T \mid l_i^{t'}, D_{\mathcal{K}}^t)}}_{FPL(\mathcal{M}^t)} - PL_0(\mathcal{M}^t)$$

Solution (cont')

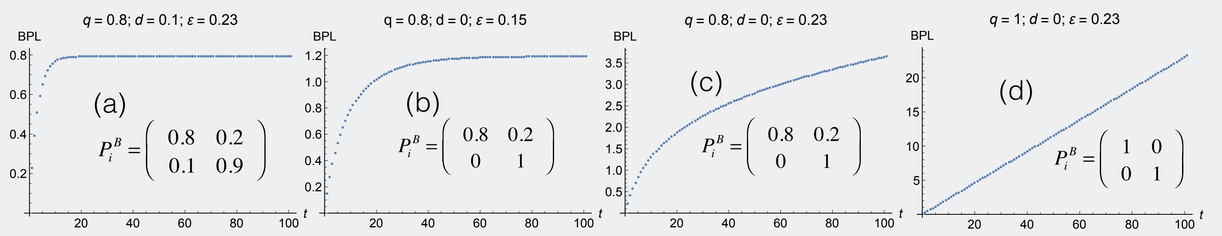
Calculating the privacy loss

- The calculation of BPL/FPL is to solve Linear-Fractional Program
- Traditionally, it takes $O(2^n)$ time complexity, our algorithm $O(n^2)$

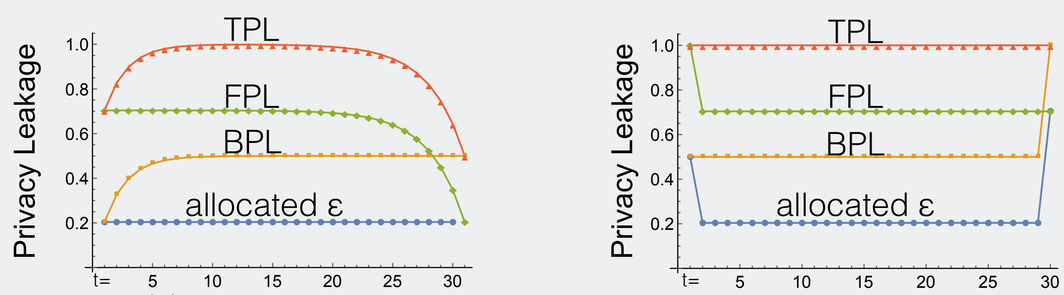


Preventing the extra privacy loss

- Given P_i^F/P_i^B, is there a **limit** of the increase of BPL/FPL?

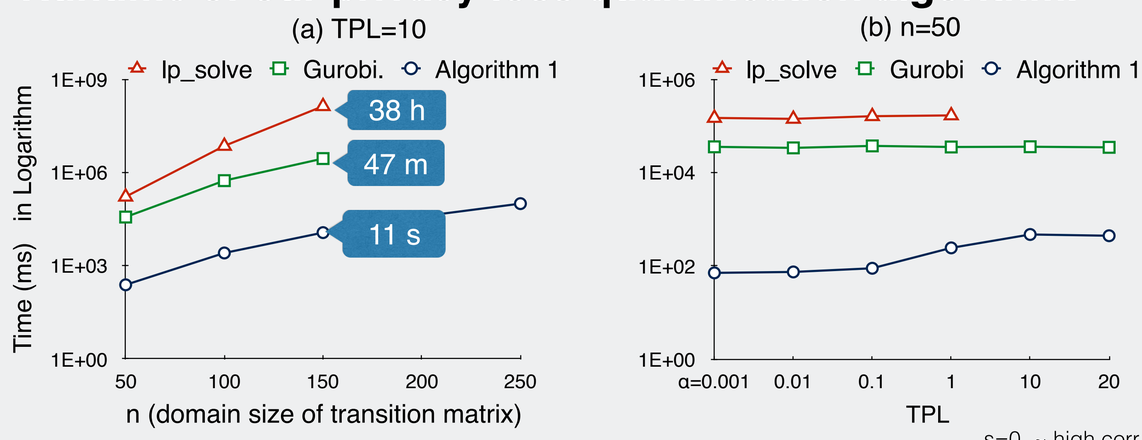


- Two strategies for preventing extra privacy loss of DP:



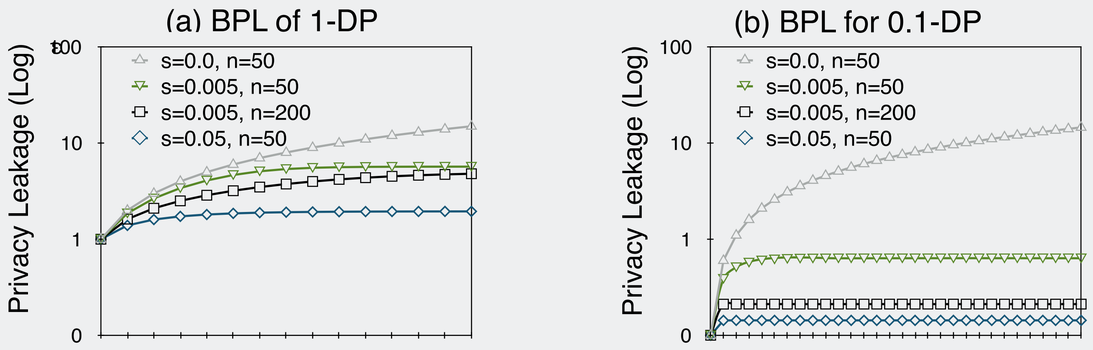
Experiments

Runtime of our privacy loss quantification algorithm.



Impact of temporal correlations on privacy loss

s=0 ~ high corr.
s=0.005 ~ mediate corr.
s=0.05 ~ low corr.



Conclusions

- Temporal correlations may result in extra privacy loss of DP.
- Such unexpected privacy loss may increase over time.
- We prevent this undesired privacy loss by allocating proper ε.

Application

- Convert a traditional DP mechanism into one prevent against TPL under temporal correlations.

Extensions

- How to learn appropriate temporal correlations?
- How to model/quantify DP under other types of correlations?
- Is there a better way to prevent TPL (e.g., utilize temporal corr.)?

Source Code:https://github.com/brahms2013/TPL

Kyoto University & Emory University

This work was supported by JSPS KAKENHI Grant Numbers 16K12437 and 15H02705, JSPS Core-to-Core Program (A. Advanced Research Networks), the National Institute of Health (NIH) under award number R01GM114612, the Patient-Centered Outcomes Research Institute (PCORI) under contract ME-1310-07058, and the National Science Foundation under award CNS-1618932.