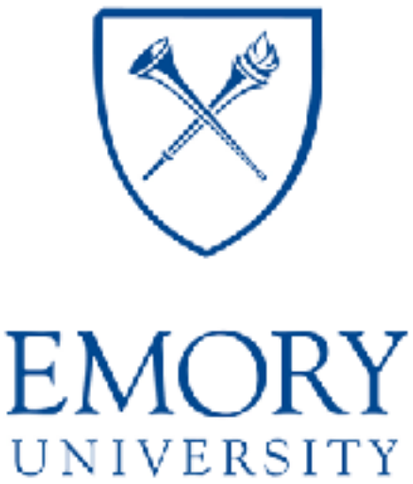
Quantifying Differential Privacy under Temporal Correlations

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

* Kyoto University

Emory University

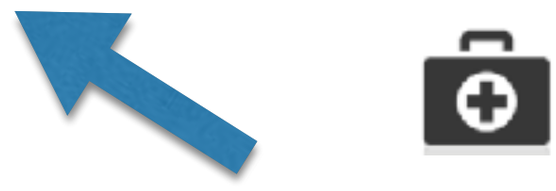


Outline

- What is Differential Privacy (DP)?
- What is Problem of DP under Temporal Correlations?
  - unexpected privacy loss
- How to solve this?
  - we **analyze**, **calculate** and **prevent** such privacy loss
- Experiments

Privacy Preserving Data Release

Company



Institute

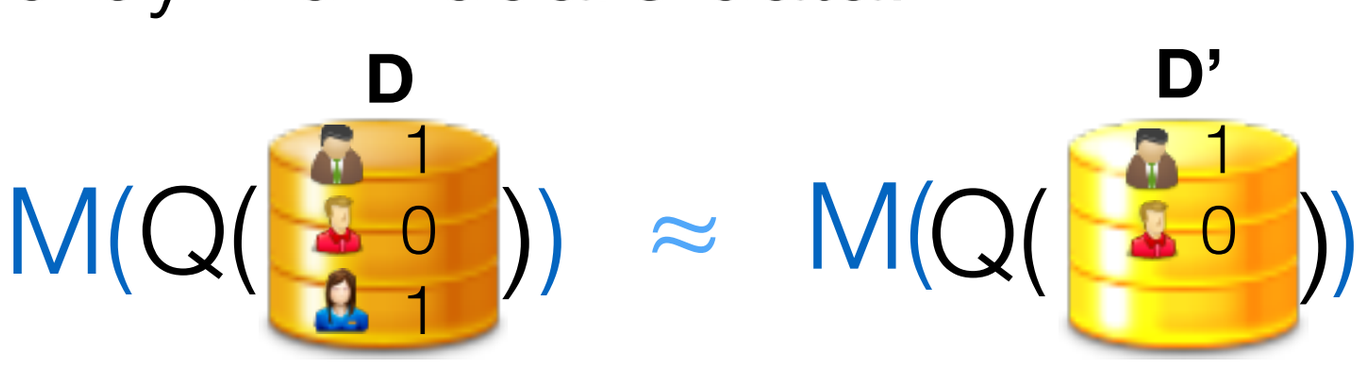
sensitive
database D

Public

Attacker

What is Differential Privacy

- Privacy: the right to be forgotten.
- DP: output of an algorithm should not be significantly affected by individual's data.



- Formally, M satisfies ε-DP if…

$$\log \frac{\Pr(M(Q(D)) = r)}{\Pr(M(Q(D')) = r)} \leq \varepsilon$$

ε ⬆️, privacy ⬇️.
e.g. **2ε**-DP means **more privacy loss** than **ε**-DP.

- e.g., Laplace mechanism: add Lap(1/ε) noise to Q(D)
- Sequential Composition. e.g., run **M** twice → **2ε**-DP

The Problem of DP under Temporal Correlation

- Our setting: *continuous data release with DP*

2ε-DP

ε-DP ~~ε-DP~~ ε-DP

r^1 r^2 r^3 …

D^1 D^2 D^3 …

t=	1	2	3	…
u1	loc_3	loc_1	loc_1	…
u2	loc_2	loc_4	loc_5	…
u3	loc_2	loc_4	loc_5	…
u4	loc_4	loc_5	loc_3	…

(a) Location Data

Count Query

t=	1	2	3	..
loc1	0	2	2	..
loc2	2	0	0	..
loc3	1	0	1	..
loc4	1	2	0	..
loc5	0	1	2	..

(b) True Counts

Laplace Noise

Lap(1/ε)

t=	1	2	3	..
loc1	0	1	3	..
loc2	3	1	0	..
loc3	1	0	1	..
loc4	2	1	0	..
loc5	1	3	3	..

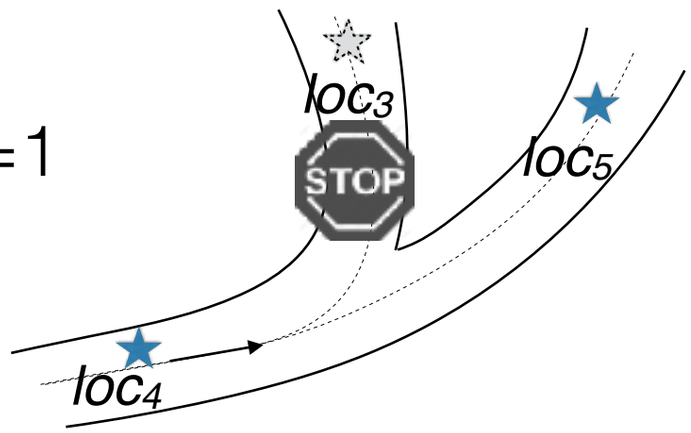
(c) Private Counts

- Temporal correlations degrade the privacy guarantee!

$Pr(l^t=loc_5 \mid l^{t-1}=loc_4)=1$

↓

2ε-DP at time 2



Road Network

$Pr(l^t=loc_5 \mid l^{t-1}=loc_4)=0.5$

↓

?-DP at time 2

Related work

- This scenario, ***continuous data release with DP,*** has been extensively studied for different issues:
  - high dimension[5][6][13],sliding window queries[7][8],infinite stream data[12], real-time publishing[11]
    - but none of them considered the effect of temporal correlations on privacy loss.
- Few works studied **potential privacy loss of DP on correlated** data, but no study investigated “DP under temporal correlations”.
  - Group DP[1][2] — not finely
  - Bayesian DP[4] ,Wasserstein Mechanism[16] — static database

Our contributions

We satisfy DP on temporally correlated data by …

- Analyzing Temporal Privacy Leakage (TPL).
  ⇒ the privacy loss may increase over time!

- Calculating TPL
  ⇒ Linear-Fractional Programing

  Simplex Algorithm: $O(2^n)$

  Our Algorithm: $O(n^2)$

- Preventing TPL
  ⇒ by carefully calibrating ε at each time point

Analyzing TPL

Model Attacker → **Define TPL** → **Find structure of TPL**

- Model temporal correlations using **Markov Chain**

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

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

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 $\Pr(l_i^t | l_i^{t-1})$

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

Analyzing TPL

Model Attacker → **Define TPL** → **Find structure of TPL**

- DP can protect against the attacker with knowledge of all tuples except the one of victim + Temporal Correlation ?

D

t=	1
u1	? loc_3
u2	loc_2
u3	loc_2
u4	loc_4

l_i

D_K

$A_i(D_{\mathcal{K}})$

$A_i^{\mathcal{T}}(D_{\mathcal{K}}, P_i^B, P_i^F)$

(i) $A_i^{\mathrm{T}}(D_{\mathrm{K}}, P_i^B, \varnothing)$

(ii) $A_i^{\mathrm{T}}(D_{\mathrm{K}}, \varnothing, P_i^F)$

(iii) $A_i^{\mathrm{T}}(D_{\mathrm{K}}, P_i^B, P_i^F)$

Analyzing TPL

Model Attacker → **Define TPL** → **Find structure of TPL**

- Recall the definition of DP:

$$PL_0(\mathcal{M}) \overset{\text{def}}{=\!=} \max_{\forall A_i, i \in \boldsymbol{U}} PL_0(A_i, \mathcal{M}) = \sup_{\boldsymbol{r}, D, D'} \log \frac{\Pr(\boldsymbol{r}|D)}{\Pr(\boldsymbol{r}|D')}$$

if $PL_0(\mathcal{M}) \leq \varepsilon$, then $\mathcal{M}$ satisfies ε-DP.

- Definition of TPL:

$$TPL(A_i^{\mathcal{T}}, \mathcal{M}^t) \overset{\text{def}}{=\!=} \sup_{l^t, l_i^{t\prime}, \boldsymbol{r}^1, \ldots, \boldsymbol{r}^T} \log \frac{\Pr(\boldsymbol{r}^1, \ldots, \boldsymbol{r}^T | l_i^t, D_{\mathcal{K}}^t)}{\Pr(\boldsymbol{r}^1, \ldots, \boldsymbol{r}^T | l_i^{t\prime}, D_{\mathcal{K}}^t)}. \quad (2)$$

$$TPL(\mathcal{M}^t) \overset{\text{def}}{=\!=} \max_{\forall A_i^{\mathcal{T}}, i \in \boldsymbol{U}} TPL(A_i^{\mathcal{T}}, \mathcal{M}^t) \quad (3)$$

$$= \sup_{D^t, D^{t\prime}, \boldsymbol{r}^1, \ldots, \boldsymbol{r}^T} \log \frac{\Pr(\boldsymbol{r}^1, \ldots, \boldsymbol{r}^T | D^t)}{\Pr(\boldsymbol{r}^1, \ldots, \boldsymbol{r}^T | D^{t\prime})}. \quad (4)$$

Analyzing TPL

Model Attacker → **Define TPL** → **Find structure of TPL**

- Definition of TPL:

$$TPL(A_i^{\mathcal{T}}, \mathcal{M}^t) \overset{\text{def}}{=\!=} \sup_{l^t, l_i^{t\prime}, \boldsymbol{r}^1, \ldots, \boldsymbol{r}^T} \log \frac{\Pr(\boldsymbol{r}^1, \ldots, \boldsymbol{r}^T | l_i^t, D_{\mathcal{K}}^t)}{\Pr(\boldsymbol{r}^1, \ldots, \boldsymbol{r}^T | l_i^{t\prime}, D_{\mathcal{K}}^t)}. \quad (2)$$

$$TPL(\mathcal{M}^t) \overset{\text{def}}{=\!=} \max_{\forall A_i^{\mathcal{T}}, i \in \boldsymbol{U}} TPL(A_i^{\mathcal{T}}, \mathcal{M}^t) \quad (3)$$

$$= \sup_{D^t, D^{t\prime}, r^1, \ldots, r^T} \log \frac{\Pr(\boldsymbol{r}^1, \ldots, \boldsymbol{r}^T | D^t)}{\Pr(\boldsymbol{r}^1, \ldots, \boldsymbol{r}^T | D^{t\prime})}. \quad (4)$$

- If no temporal correlation… **TPL = PL_0**

$$\text{Eqn(2)} = \underbrace{\log \frac{\Pr(r^1 | l_i^t, D_k{}^t)}{\Pr(r^1 | l_i^{t'}, D_k{}^t)}}_{0} + \ldots + \underbrace{\log \frac{\Pr(r^t | l_i^t, D_k{}^t)}{\Pr(r^t | l_i^{t'}, D_k{}^t)}}_{PL_0} + \ldots + \underbrace{\log \frac{\Pr(r^T | l_i^t, D_k{}^t)}{\Pr(r^T | l_i^{t'}, D_k{}^t)}}_{0}$$

Analyzing TPL

Model Attacker → **Define TPL** → **Find structure of TPL**

- Definition of TPL:

$$TPL(A_i^{\mathcal{T}}, \mathcal{M}^t) \overset{\text{def}}{=\!=} \sup_{l^t, l_i^{t\prime}, \boldsymbol{r}^1, \ldots, \boldsymbol{r}^T} \log \frac{\Pr(\boldsymbol{r}^1, \ldots, \boldsymbol{r}^T | l_i^t, D_{\mathcal{K}}^t)}{\Pr(\boldsymbol{r}^1, \ldots, \boldsymbol{r}^T | l_i^{t\prime}, D_{\mathcal{K}}^t)}. \quad (2)$$

$$TPL(\mathcal{M}^t) \overset{\text{def}}{=\!=} \max_{\forall A_i^{\mathcal{T}}, i \in \boldsymbol{U}} TPL(A_i^{\mathcal{T}}, \mathcal{M}^t) \quad (3)$$

$$= \sup_{D^t, D^{t\prime}, \boldsymbol{r}^1, \ldots, \boldsymbol{r}^T} \log \frac{\Pr(\boldsymbol{r}^1, \ldots, \boldsymbol{r}^T | D^t)}{\Pr(\boldsymbol{r}^1, \ldots, \boldsymbol{r}^T | D^{t\prime})}. \quad (4)$$

- If with temporal correlation…**TPL = ?**

Hard to quantify Eqn(2)…

$$\text{Eqn(2)} = \underbrace{\log \frac{\Pr(r^1 | l_i^t, D_k^t)}{\Pr(r^1 | l_i^{t\prime}, D_k^t)}}_{?} + \ldots + \underbrace{\log \frac{\Pr(r^t | l_i^t, D_k^t)}{\Pr(r^t | l_i^{t\prime}, D_k^t)}}_{PL_0} + \ldots + \underbrace{\log \frac{\Pr(r^T | l_i^t, D_k^t)}{\Pr(r^T | l_i^{t\prime}, D_k^t)}}_{?}$$

Analyzing TPL

Model Attacker → **Define TPL** → **Find structure of TPL**

$$\text{Eqn.(2)} = \sup_{l^t, l_i^{t\prime}, \boldsymbol{r}^1, \ldots, \boldsymbol{r}^T} \log \frac{\Pr(\boldsymbol{r}^1 | l_i^t, D_{\mathcal{K}}^t)}{\Pr(\boldsymbol{r}^1 | l_i^t, D_{\mathcal{K}}^t)} * \cdots * \frac{\Pr(\boldsymbol{r}^T | l_i^t, D_{\mathcal{K}}^t)}{\Pr(\boldsymbol{r}^T | l_i^t, D_{\mathcal{K}}^t)}$$

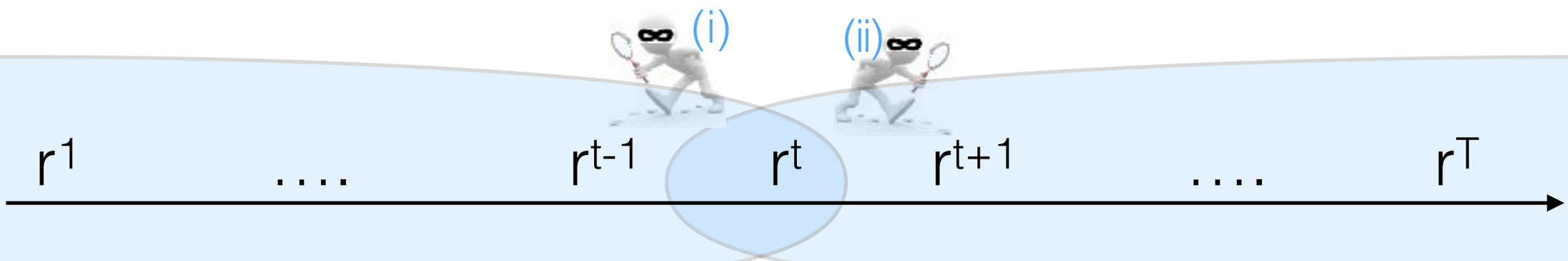
$$= \underbrace{\sup_{\substack{\boldsymbol{r}^1, \ldots, \boldsymbol{r}^t, \\ l_i, l_i'}} \log \frac{\Pr(\boldsymbol{r}^1, \ldots, \boldsymbol{r}^t | l_i^t, D_{\mathcal{K}}^t)}{\Pr(\boldsymbol{r}^1, \ldots, \boldsymbol{r}^t | l_i^t, D_{\mathcal{K}}^t)}}_{\text{(i) } A_i^{\mathrm{T}}(D_{\mathrm{K}}, P_i^B, \varnothing)} + \underbrace{\sup_{\substack{\boldsymbol{r}^t, \ldots, \boldsymbol{r}^T, \\ l_i, l_i'}} \log \frac{\Pr(\boldsymbol{r}^t, \ldots, \boldsymbol{r}^T | l_i^t, D_{\mathcal{K}}^t)}{\Pr(\boldsymbol{r}^t, \ldots, \boldsymbol{r}^T | l_i^t, D_{\mathcal{K}}^t)}}_{\text{(ii) } A_i^{\mathrm{T}}(D_{\mathrm{K}}, \varnothing, P_i^F)}$$

backward privacy leakage (BPL) | forward privacy leakage (FPL)

$$- \underbrace{\sup_{\boldsymbol{r}^t, l_i, l_i'} \log \frac{\Pr(\boldsymbol{r}^t | l_i^t, D_{\mathcal{K}}^t)}{\Pr(\boldsymbol{r}^t | l_i^t, D_{\mathcal{K}}^t)}}_{PL_0(A_i^{\mathcal{T}}, \mathcal{M}^t)} \tag{5}$$

(iii) $A_i^{\mathrm{T}}(D_{\mathrm{K}}, P_i^B, P_i^F)$

$$\Rightarrow \quad TPL(A_i^{\mathcal{T}}, \mathcal{M}^t) = BPL(A_i^{\mathcal{T}}, \mathcal{M}^t) + FPL(A_i^{\mathcal{T}}, \mathcal{M}^t) - PL_0(A_i^{\mathcal{T}}, \mathcal{M}^t). \tag{10}$$



Analyzing TPL

BPL

Model Attacker → **Define TPL** → **Find structure of TPL**

$$BPL(A_i^{\mathcal{T}}, \mathcal{M}^t) \overset{\text{def}}{=\!=} \sup_{l_i^t, l_i^{t\prime}, \boldsymbol{r}^1, \ldots, \boldsymbol{r}^t} \log \frac{\Pr(\boldsymbol{r}^1, \ldots, \boldsymbol{r}^t | l_i^t, D_{\mathcal{K}}^t)}{\Pr(\boldsymbol{r}^1, \ldots, \boldsymbol{r}^t | l_i^{t\prime}, D_{\mathcal{K}}^t)}. \quad (6)$$

- Analyze BPL

Backward *temporal correlations*

Eqn(6)=

$$\sup_{\substack{l_i^t, l_i^{t\prime}, \\ \boldsymbol{r}^1, \ldots, \boldsymbol{r}^{t-1}}} \log \frac{\sum_{l_i^{t-1}} \underbrace{\Pr(\boldsymbol{r}^1, \ldots, \boldsymbol{r}^{t-1} | l_i^{t-1}, D_{\mathcal{K}}^{t-1})}_{(i) BPL(A_i^{\mathcal{T}}, \mathcal{M}^{t-1})} \underbrace{\Pr(l_i^{t-1} | l_i^t)}_{(ii) P_i^B}}{\sum_{l_i^{t-1\prime}} \Pr(\boldsymbol{r}^1, \ldots, \boldsymbol{r}^{t-1} | l_i^{t-1\prime}, D_{\mathcal{K}}^{t-1}) \Pr(l_i^{t-1\prime} | l_i^{t\prime})}$$

$$+ \sup_{l_i^t, l_i^{t\prime}, \boldsymbol{r}^t} \log \underbrace{\frac{\Pr(\boldsymbol{r}^t | l_i^t, D_{\mathcal{K}}^t)}{\Pr(\boldsymbol{r}^t | l_i^{t\prime}, D_{\mathcal{K}}^t)}}_{(iii) PL_0(A_i^{\mathcal{T}}, \mathcal{M}^t)}. \quad (12)$$

Backward privacy loss function.
how to calculate it?

$$\Rightarrow \quad BPL(A_i^{\mathcal{T}}, \mathcal{M}^t) = \mathcal{L}^B\big(BPL(A_i^{\mathcal{T}}, \mathcal{M}^{t-1})\big) + PL_0(A_i, \mathcal{M}^t) \quad (13)$$

Analyzing TPL

FPL

Model Attacker → **Define TPL** → **Find structure of TPL**

$$FPL(A_i^{\mathcal{T}}, \mathcal{M}^t) \overset{\text{def}}{=\!=} \sup_{l_i^t, l_i^{t\prime}, \boldsymbol{r}^t, \ldots, \boldsymbol{r}^T} \log \frac{\Pr(\boldsymbol{r}^t, \ldots, \boldsymbol{r}^T | l_i^t, D_{\mathcal{K}}^t)}{\Pr(\boldsymbol{r}^t, \ldots, \boldsymbol{r}^T | l_i^{t\prime}, D_{\mathcal{K}}^t)}. \quad (8)$$

- Analyze FPL

Forward *temporal correlations*

$$\sup_{\substack{l_i^t, l_i^{t\prime}, \\ \boldsymbol{r}^{t+1}, \ldots, \boldsymbol{r}^T}} \log \frac{\sum_{l_i^{t+1}} \underbrace{\Pr(\boldsymbol{r}^{t+1}, \ldots, \boldsymbol{r}^T | l_i^{t+1}, D_{\mathcal{K}}^{t+1})}_{(i)FPL(A_i^{\mathcal{T}}, \mathcal{M}^{t+1})} \underbrace{\Pr(l_i^{t+1} | l_i^t)}_{(ii)P_i^F}}{\sum_{l_i^{t+1\prime}} \Pr(\boldsymbol{r}^{t+1}, \ldots, \boldsymbol{r}^T | l_i^{t+1\prime}, D_{\mathcal{K}}^{t+1}) \Pr(l_i^{t+1\prime} | l_i^{t\prime})}$$

$$+ \sup_{l_i^t, l_i^{t\prime}, \boldsymbol{r}^t} \log \underbrace{\frac{\Pr(\boldsymbol{r}^t | l_i^t, D_{\mathcal{K}}^t)}{\Pr(\boldsymbol{r}^t | l_i^{t\prime}, D_{\mathcal{K}}^t)}}_{(iii)PL_0(A_i^{\mathcal{T}}, \mathcal{M}^t)}.$$

Forward *privacy loss function.*
how to calculate it?

$$\Rightarrow \quad FPL(A_i^{\mathcal{T}}, \mathcal{M}^t) = \mathcal{L}^F\left(FPL(A_i^{\mathcal{T}}, \mathcal{M}^{t+1})\right) + PL_0(A_i, \mathcal{M}^t) \quad (15)$$

Calculating BPL & FPL

Privacy Quantification → Upper bound

- We convert the problem of BPL/FPL calculation to **finding an optimal solution of a linear-fractional programming problem.**

$$\mathcal{L}^B\left(BPL(A_i^{\mathcal{T}}, \mathcal{M}^{t-1})\right) = \sup_{\boldsymbol{q},\boldsymbol{d}\in P_i^B} \log \frac{q_1 x_1 + \cdots + q_n x_n}{d_1 x_1 + \cdots + d_n x_n}$$

$$= \sup_{\boldsymbol{q},\boldsymbol{d}\in P_i^B} \log \frac{\boldsymbol{qx}}{\boldsymbol{dx}}$$

$$\text{maximize} \quad \frac{\boldsymbol{qx}}{\boldsymbol{dx}} \tag{18}$$

$$\text{subject to} \quad e^{-\alpha_{t-1}^B} \leq \frac{x_j}{x_k} \leq e^{\alpha_{t-1}^B}, \tag{19}$$

$$0 < x_j < 1 \text{ and } 0 < x_k < 1, \tag{20}$$

$$\text{where } x_j, x_k \in \boldsymbol{x},\ j, k \in [1, n].$$

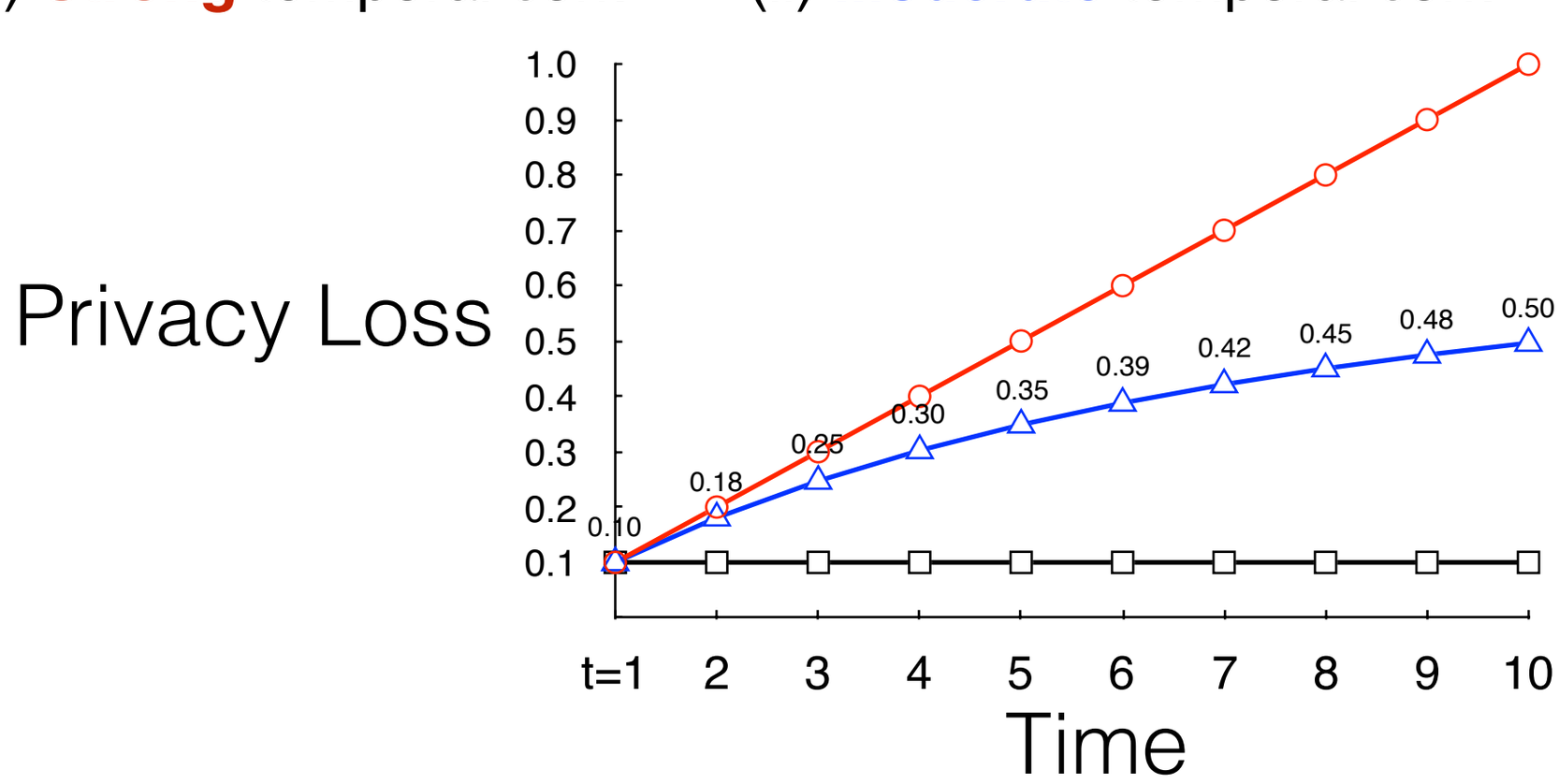
- This problem can be solved by simplex algorithm in $O(2^n)$.
- We designed a $O(n^2)$ algorithm for quantifying BPL/FPL.

Calculating BPL & FPL

Privacy Quantification → Upper bound

- Example of **BPL** under different temporal corr.

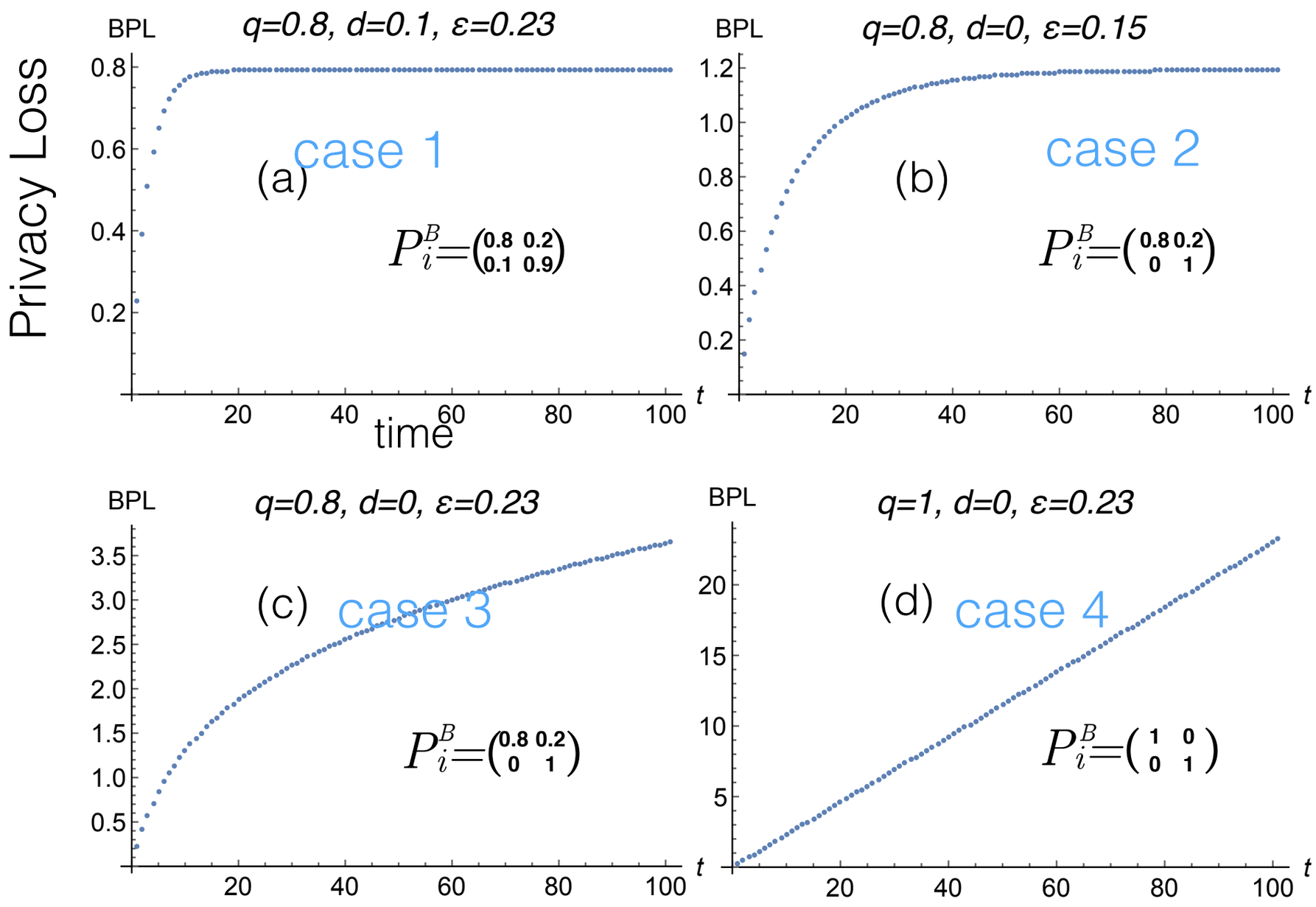
(i) **Strong** temporal corr. (ii) **Moderate** temporal corr. (iii) **No** temporal corr.



$$\Rightarrow \quad TPL(A_i^{\mathcal{T}}, \mathcal{M}^t) = BPL(A_i^{\mathcal{T}}, \mathcal{M}^t) + FPL(A_i^{\mathcal{T}}, \mathcal{M}^t) - PL_0(A_i^{\mathcal{T}}, \mathcal{M}^t). \qquad (10)$$

Calculating BPL & FPL

Privacy Quantification → Upper bound

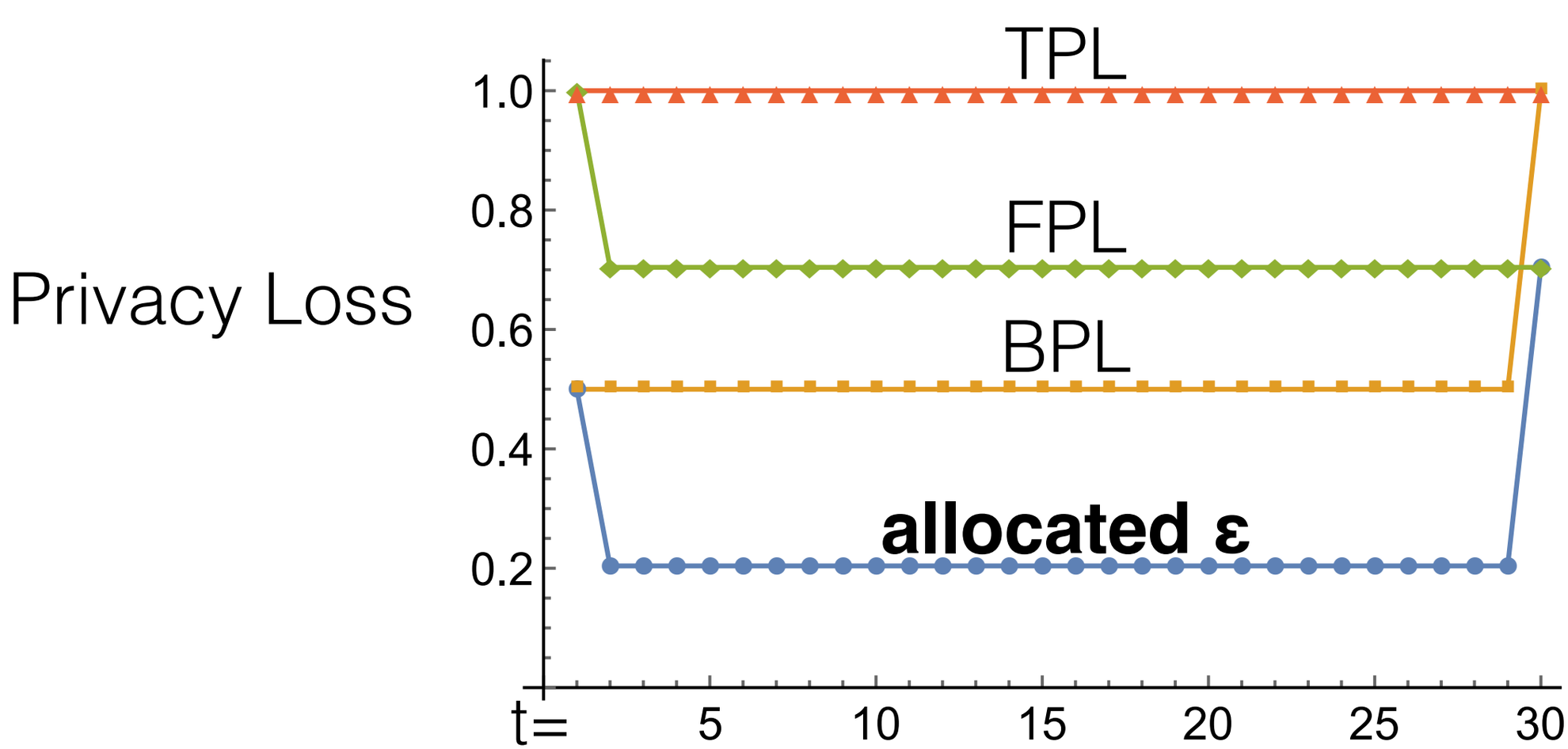


Refer to **Theorem 5** in our paper

Preventing BPL & FPL

by Quantification → **by Upper Bound**

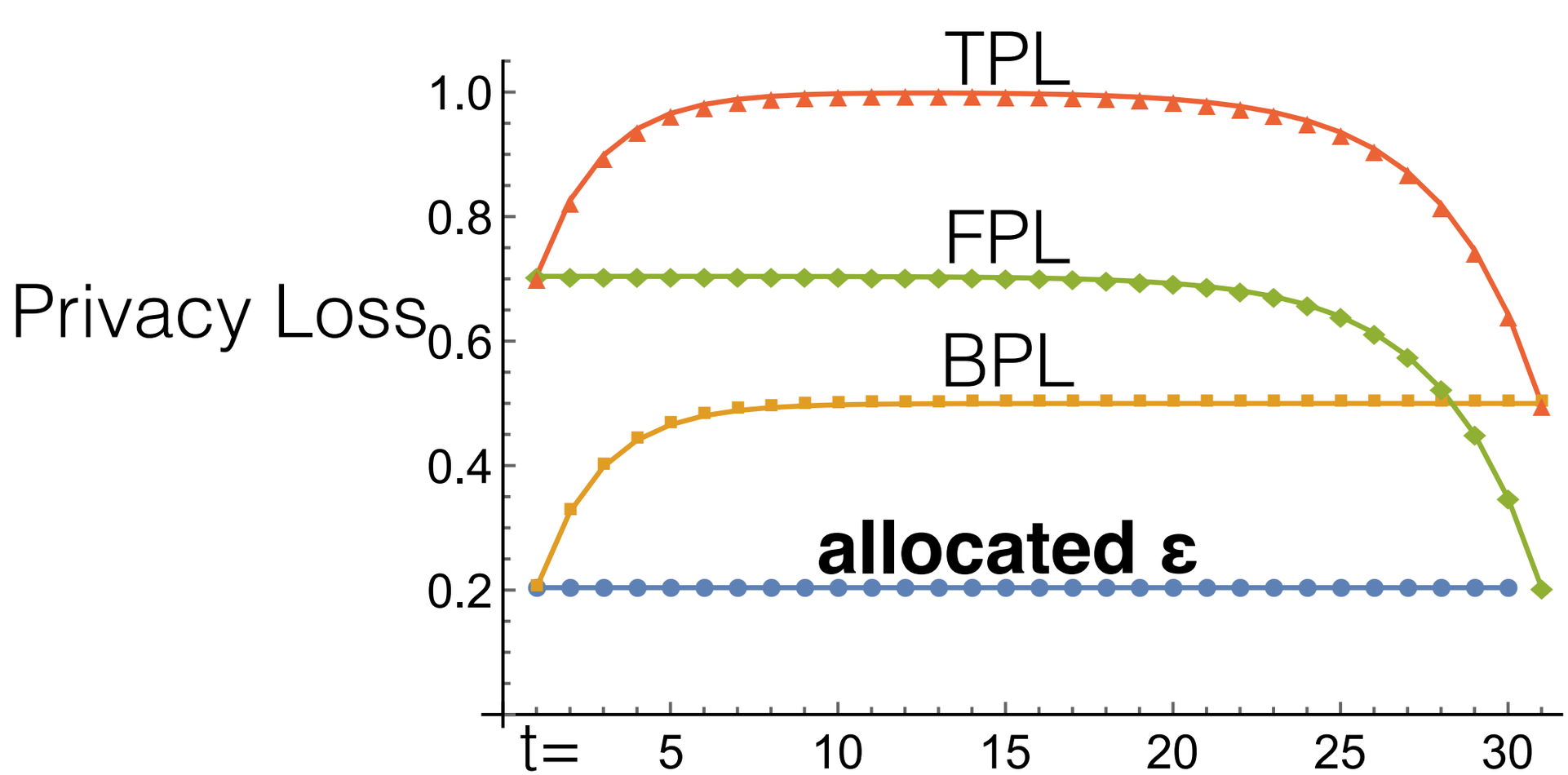
- If T is known, we can assign proper ε at each t,
  to make sure that TPL always equal to a specific value.



Preventing BPL & FPL

by Quantification → **by Upper Bound**

- If T is unknown, we can assign proper ε at each t, to make sure that TPL never exceeds a specific value.



Experiments

- Goals
  - (1) Runtime of privacy quantification algorithm
  - (2) Impact of temporal correlations on privacy
- Synthetic datasets
  - Generate transition matrix randomly.
  - Generate the strongest temporal correlation $P_i=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$
  - Uniformize the strongest temporal correlation by Laplace smoothing:

$$\hat{p_{jk}} = \frac{p_{jk} + s}{\sum_{u=1}^{n} (p_{ju} + s)} \qquad (25)$$

A smaller **s** results in a stronger temporal correlation.

e.g., s=0 $P_i=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$

e.g., s=0.1 $P_i=\begin{pmatrix}0.92 & 0.08\\ 0.08 & 0.92\end{pmatrix}$

e.g., s=0.5 $P_i=\begin{pmatrix}0.75 & 0.25\\ 0.25 & 0.75\end{pmatrix}$

Runtime Evaluation

- **lp_solve** and **Gurobi** are two well-known software for solving optimization problems (e.g., Linear-Fractional Program in our setting)

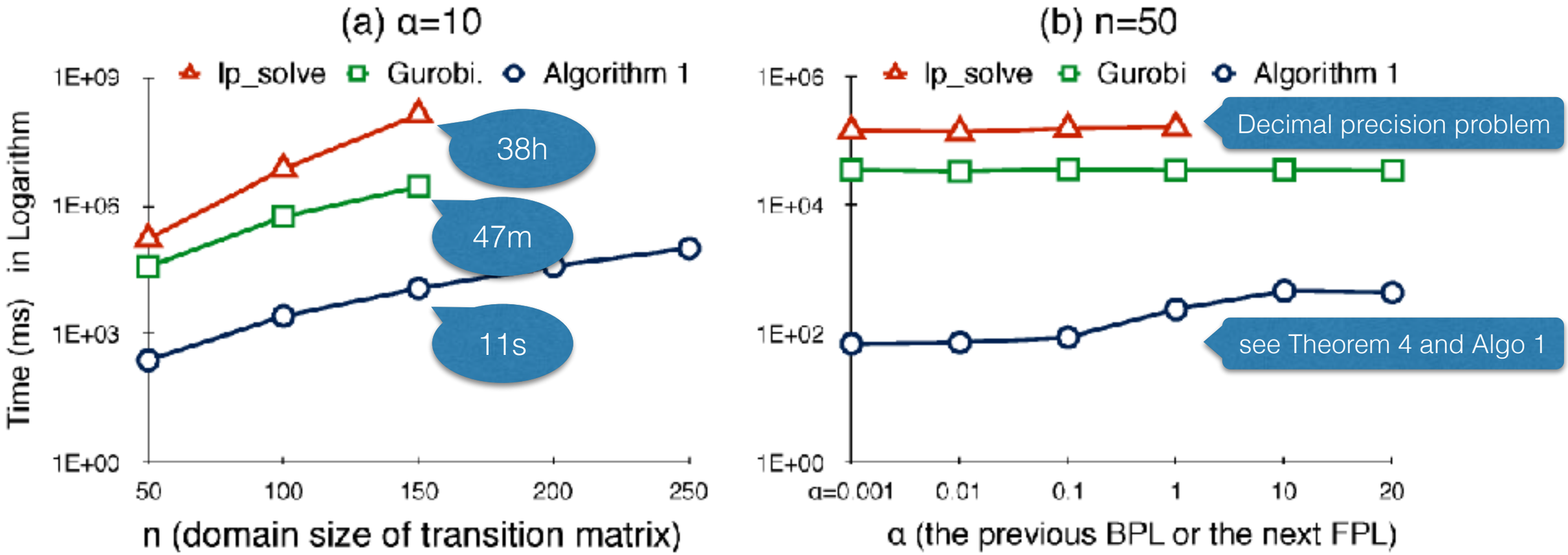


Fig. 5: Runtime of Privacy Quantification Algorithms.

Impact of Temporal Corr. on Privacy Leakage

- temporal correlation ⬆️ (s ⬇️), privacy leakage ⬆️
- ε significantly delayed the growth of privacy leakage
- value domain n ⬆️, privacy leakage ⬇️

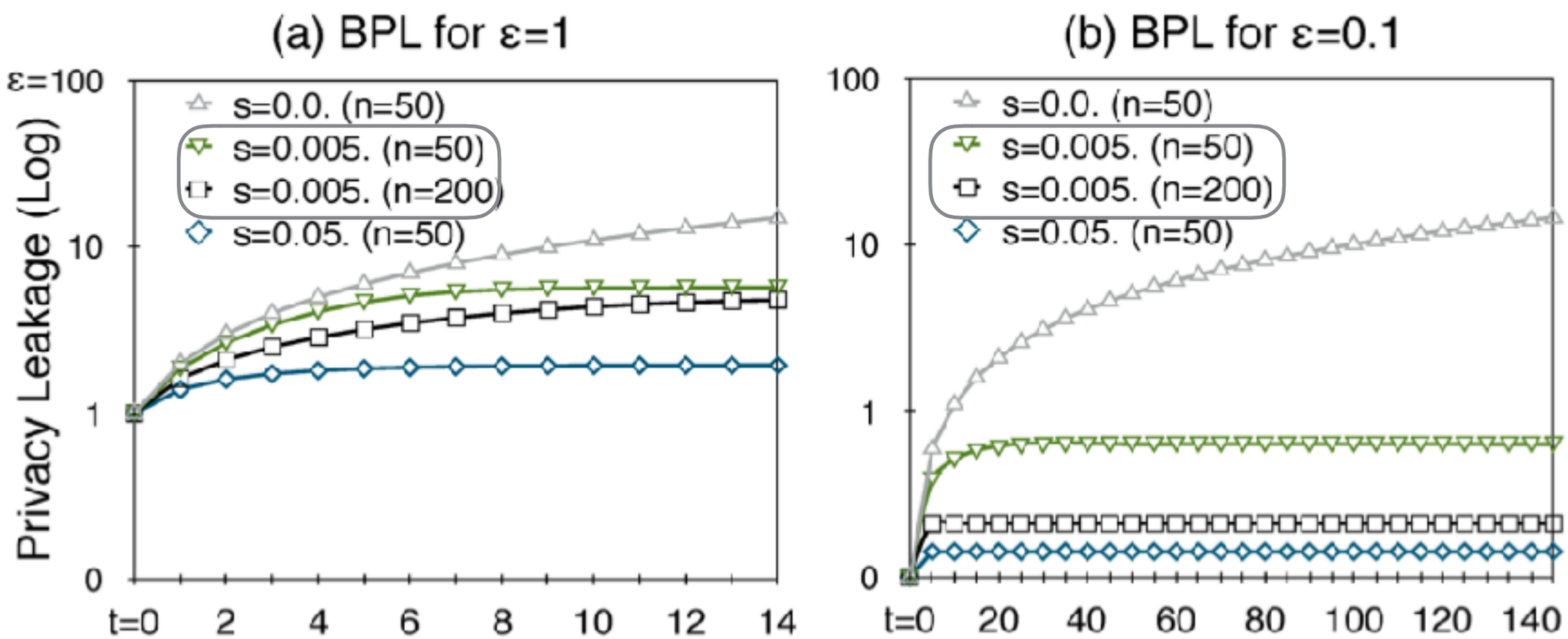


Fig. 6: Evaluation of BPL.

Future work

- **Applications**

- Convert a traditional DP mechanism into one prevent against TPL under temporal correlations.
- Using our new sequential composition theorem, to Design complicated algorithms against TPL

- **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.)?

References

1. C. Dwork, F. McSherry, K. Nissim, and A. Smith. Calibrating noise to sensitivity in private data analysis. In S. Halevi and T. Rabin, editors, Lecture Notes in Computer Science, volume 3876, pages 265–284, 2006.
2. R. Chen, B. C. Fung, P. S. Yu, and B. C. Desai. Correlated network data publication via differential privacy. VLDBJ, 23(4):653–676, 2014.
3. C. Liu, S. Chakraborty, and P. Mittal. Dependence makes you vulnerable: Differential privacy under dependent tuples. In NDSS, 2016.
4. B. Yang, I. Sato, and H. Nakagawa. Bayesian differential privacy on correlated data. In SIGMOD, pages 747–762, 2015.
5. G. Acs and C. Castelluccia. A case study: Privacy preserving release of spatio-temporal density in paris. In KDD, pages 1679–1688, 2014.
6. J. Bolot, N. Fawaz, S. Muthukrishnan, A. Nikolov, and N. Taft. Private decayed predicate sums on streams. In ICDT, pages 284–295, 2013.
7. T.-H. H. Chan, M. Li, E. Shi, and W. Xu. Differentially private continual monitoring of heavy hitters from distributed streams. In PETS, pages 140–159, 2012.
8. T.-H. H. Chan, E. Shi, and D. Song. Private and continual release of statistics. ACM Trans. Inf. Syst. Secur., 14(3):26:1–26:24, 2011.
9. C. Dwork. Differential privacy in new settings. In SODA, pages 174– 183, 2010.
10. C. Dwork, M. Naor, T. Pitassi, and G. N. Rothblum. Differential privacy under continual observation. In STOC, pages 715–724, 2010.
11. L. Fan, L. Xiong, and V. Sunderam. FAST: differentially private real-time aggregate monitor with filtering and adaptive sampling. In SIGMOD, pages 1065–1068, 2013.
12. G. Kellaris, S. Papadopoulos, X. Xiao, and D. Papadias. Differentially private event sequences over infinite streams. PVLDB, 7(12):1155– 1166, 2014.
13. Y. Xiao, J. Gardner, and L. Xiong. DPCube: releasing differentially private data cubes for health information. In ICDE, pages 1305–1308, 2012.
14. C. Dwork and A. Roth. The Algorithmic Foundations of Differential Privacy, volume 9. 2013.
15. F. D. McSherry. Privacy integrated queries: an extensible platform for privacy-preserving data analysis. In Proceedings of the 2009 ACM SIGMOD, pages 19–30, 2009.

Thank you!

Calculating BPL & FPL

Privacy Quantification → Upper bound

- Example of BPL/FPL/TPL under different temporal corr.

(i) **Strong** temporal corr. (ii) **Moderate** temporal corr. (iii) **No** temporal corr.