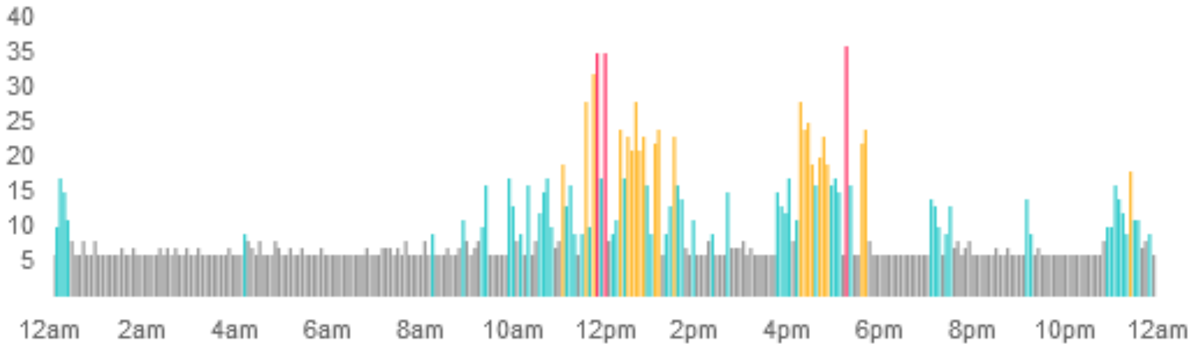
Pufferfish Privacy Mechanisms for Correlated Data

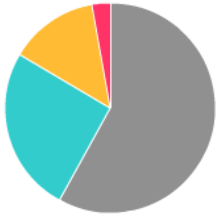
Shuang Song, Yizhen Wang, Kamalika Chaudhuri
University of California, San Diego

Sensitive Data with Correlation

- Data from social networks,
- eg. Spreading of flu

- Time series data,
- eg. Exercise per week





Why Does Correlation Make Privacy Protection Hard?

- $D = \{X_1, \ldots, X_n\},\ X_i = 1(\text{person } i \text{ has flu})$

- Goal:
  - Publish (approximately) # of people w/ flu
  - Prevent anyone from knowing if a specific person has flu or not
- Correlation makes privacy protection hard:
  - Knowing information about your social network → inferring information about you

Previous Solution 1

- Differential Privacy:
  - Hide the effect of single individual
- # of infected people + noise w/ std ~ 1
  - Assuming best case: everyone is independent

- There can be large connect groups and the disease can be highly contagious
- No enough protection!

Dwork, C., McSherry, F., Nissim, K., & Smith, A. Calibrating noise to sensitivity in private data analysis. In Theory of Cryptography Conference 2006

Previous Solution 2

- Group-Differential Privacy:
  - Hide the effect of the entire group
- # of infected people + noise w/ std ~Group_Size
  - Assuming worst case: complete correlation within group

- Group size can be large
- Poor utility!

The Hope for a Better Solution

DP: Everyone is independent

No enough protection!

?

Group-DP: Everyone is completely correlated

No enough utility!

- Observation: most real problems have low average correlation

Pufferfish Privacy

—— a framework with correlation taken into consideration

3 Components of Pufferfish Privacy:

1. Secrets S: set of information need to be protected
   - eg. Alice has flu, Bob was sleeping at 10am

2. Secret pair $Q \subseteq S \times S$: set of pairs of secrets need to be indistinguishable
   - eg. (Alice has flu, Alice is healthy), (Bob was sleeping at 10am, Bob was exercising at 10am)

3. Θ: a set of data distributions that plausibly generate the data (where correlation is captured)
   - eg. Flu is passed w.p. 0.2, Bob exercises only if he gets up before 8am

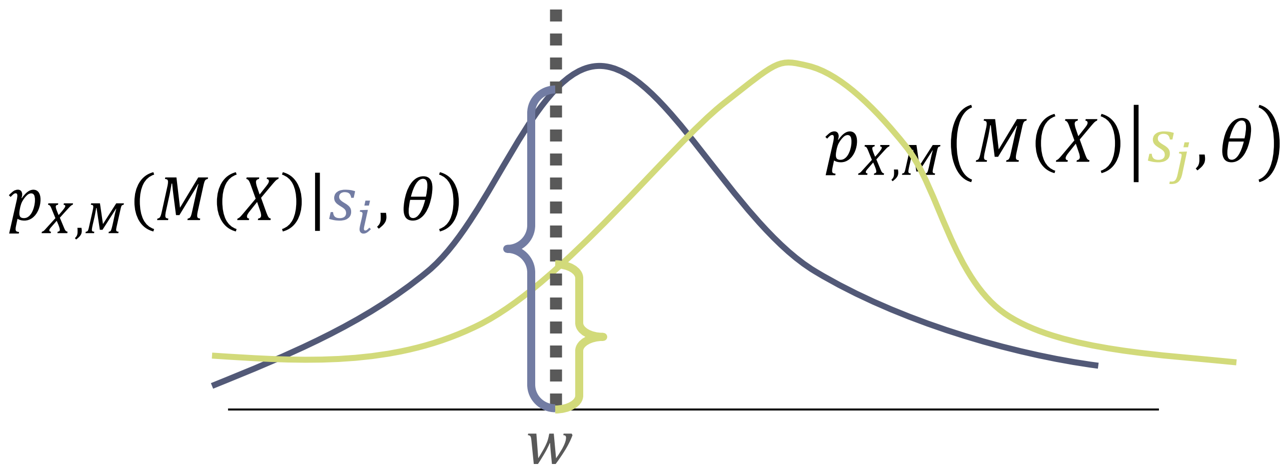
ϵ-Pufferfish Privacy

- A privacy mechanism M is ϵ-Pufferfish private with Pufferfish parameters (S, Q, Θ) if $\forall w \in \text{Range}(M), \forall (s_i, s_j) \in Q, \forall \theta \in \Theta$ with $X \sim \theta$

$$e^{-\epsilon} \leq \frac{p_{X,M}(M(X) = w | s_i, \theta)}{p_{X,M}(M(X) = w | s_j, \theta)} \leq e^{\epsilon}$$

when $P(s_i|\theta) \neq 0$, $P(s_j|\theta) \neq 0$.

  - ϵ measures privacy level: smaller ϵ → more privacy.



Pufferfish Privacy

- Allows correlation
- Generalizes differential privacy
  - DP is a special case where Θ contains all independent distributions

How to achieve Pufferfish privacy?

Algorithms for Pufferfish Privacy

- Algorithms for special Pufferfish instantiations: [KM12, HMD12]

- Our contribution:
  - Wasserstein Mechanism (completely general)
  - Markov Quilt Mechanism (Bayesian network)

- Concurrent work: [GK17]

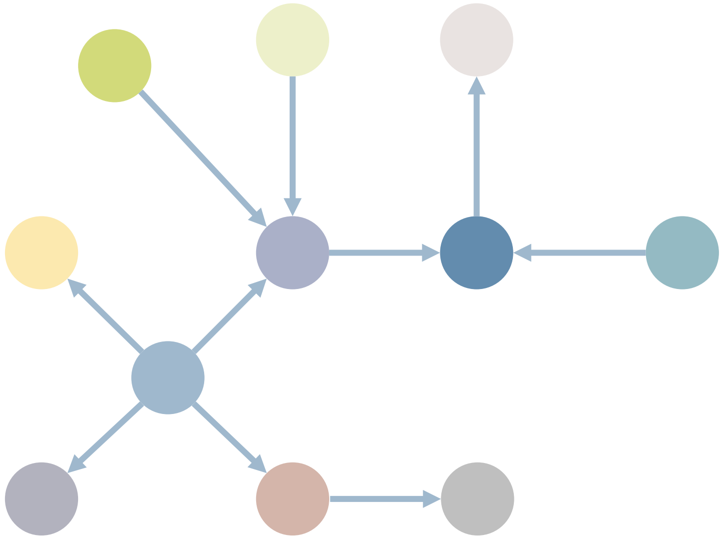
[HMD12] He, X., Machanavajjhala, A., & Ding, B. Blowfish privacy: Tuning privacy-utility trade-offs using policies. SIGMOD 2014
[GK17] Ghosh, A., & Kleinberg, R. Inferential Privacy Guarantees for Differentially Private Mechanisms. ITCS 2017

Outline

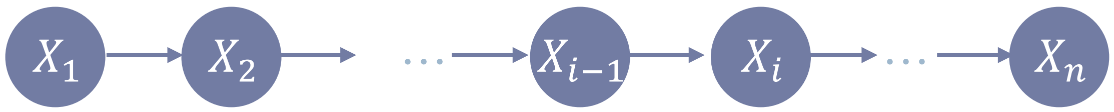
- Pufferfish privacy definition
- Our algorithms:
  - Wasserstein Mechanism (Please come to our poster for detail ☺)
  - Markov Quilt Mechanism
- Experimental results

Markov Quilt Mechanism (MQM)

- Bayesian network:
  - $X = \{X_1, \dots, X_n\}$ + DAG $G = (X, E)$
  - E represents parent-child relationship



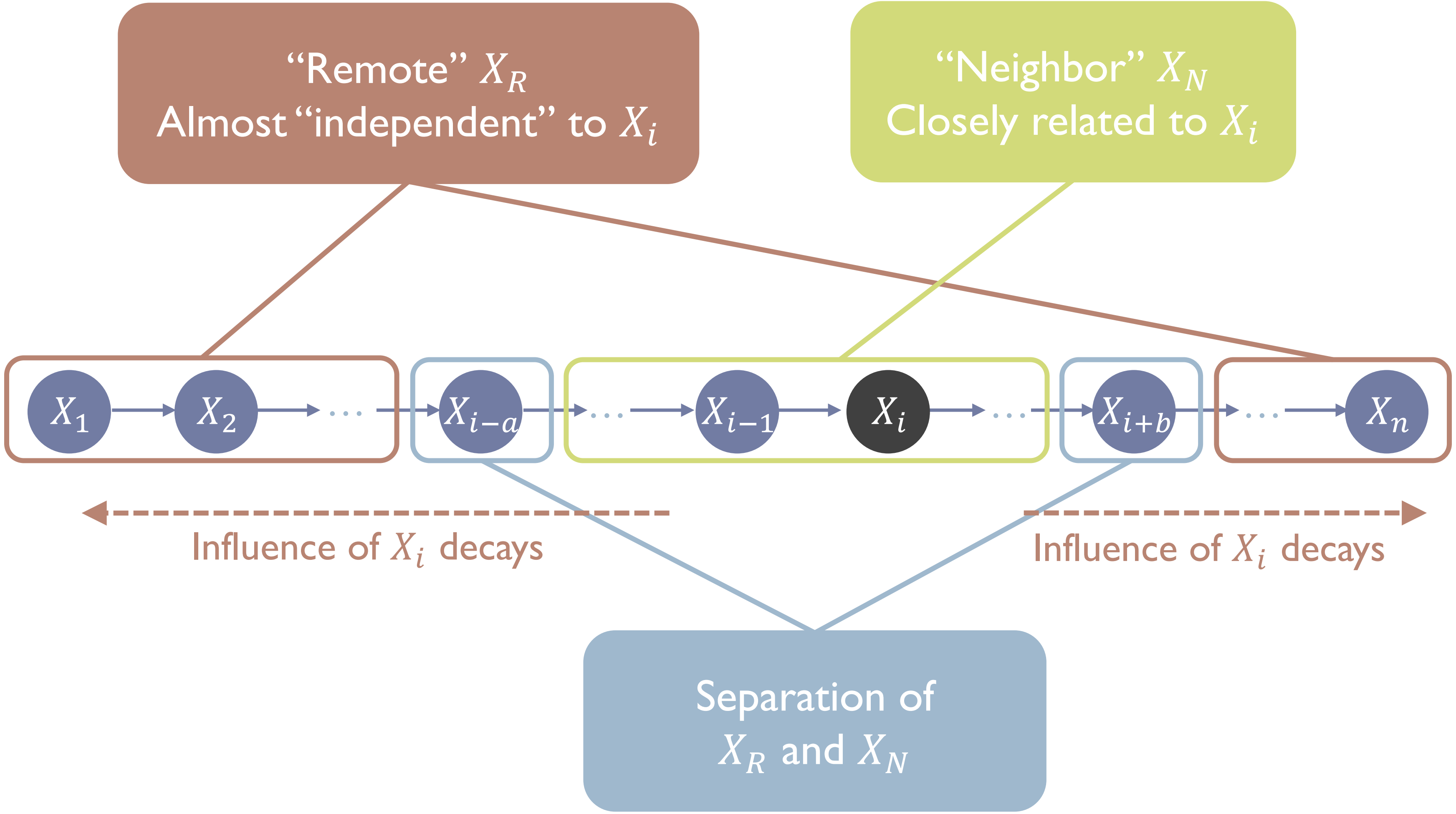
MQM on Markov Chain



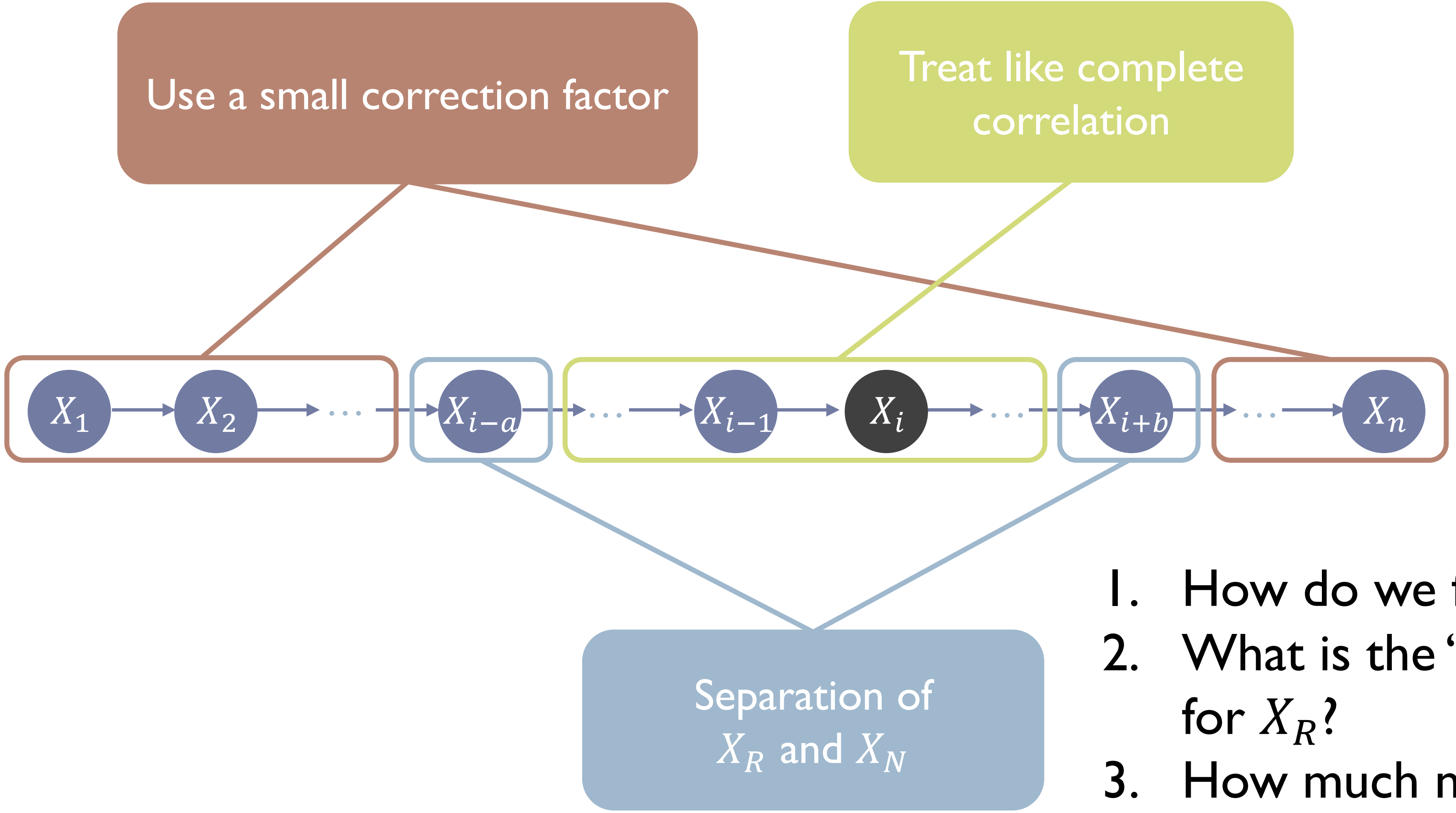
- Θ: Markov Chains $\{X_1, \ldots, X_n\}, X_i \in [K]$
- $S = \{X_i = s : i \in [n], s \in [K]\}$
- $Q = \{(X_i = s, X_i = t) : i \in [n], s, t \in [K], s \neq t\}$

- f: 1-Lipschitz function
  - E.g. count
  - Extend to any Lipschitz function

Markov Quilt Mechanism Intuition



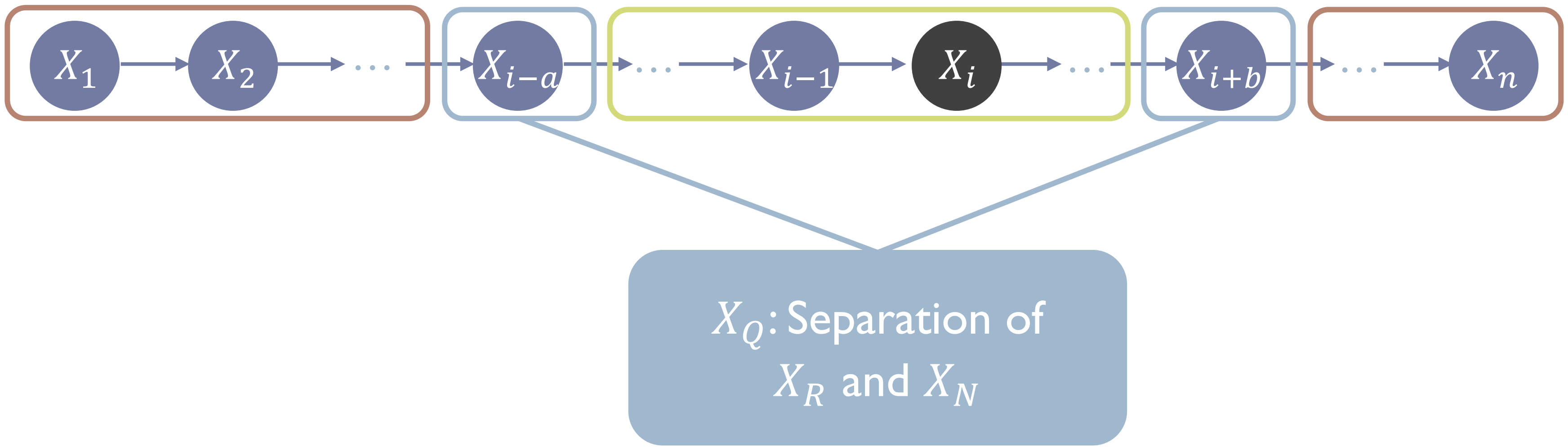
Markov Quilt Mechanism Intuition



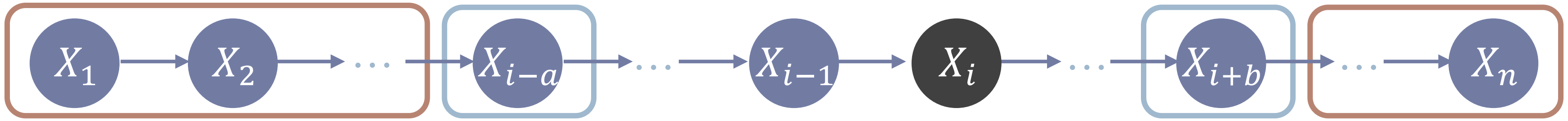
1. How do we formalize "separation"?
2. What is the "small correction factor" for X_R?
3. How much noise to add for X_N?

1. Formalizing "Separation"

- Markov Quilt X_Q for X_i:
  - Deleting X_Q breaks graph into X_N and X_R, $X_i \in X_N$
  - Given X_Q, X_i and X_R are independent



2. “Small Correction Factor” for Remote



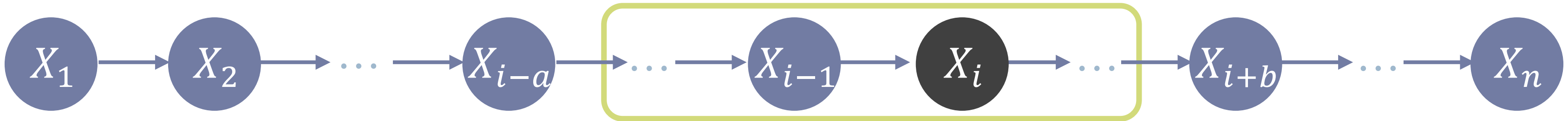
- Max-influence of X_i on any set X_A under Θ:

$$e(X_A|X_i) = \max_{s,t,x_A,\theta} \log \frac{P(X_A = x_A|X_i = s, \theta)}{P(X_A = x_A|X_i = t, \theta)}$$

  - Lower max-influence → less correlated

- Correction term for $X_R \cup X_Q$: $e\left(X_R \cup X_Q \middle| X_i\right) = e(X_Q|X_i)$

3. Noise for Neighbor



- $\epsilon - e(X_Q | X_i)$ budget left
- Treat as worst case:
  - Group-DP: X_N changes as a group
  - 1-Lipschitz function changes by at most $|X_N|$
- Final std of noise:

$$\frac{|X_N|}{\epsilon - e(X_Q | X_i)}$$

Putting Together Everything

- Repeat for all X_i:
  - Repeat for all X_Qs
  - $\text{noise}(X_i) = \min_{X_Q} \frac{|X_N|}{\epsilon - e(X_Q|X_i)}$
- $\text{noise}(D) = \max_{i \in [n]} \text{noise}(X_i)$
- Output $f(D)$ + Noise w/ std $\sim\text{noise}(D)$

- Theorem: MQM guarantees ϵ-Pufferfish privacy.

Outline

- Pufferfish privacy definition
- Our algorithms:
  - Wasserstein Mechanism
  - Markov Quilt Mechanism
- Experimental results

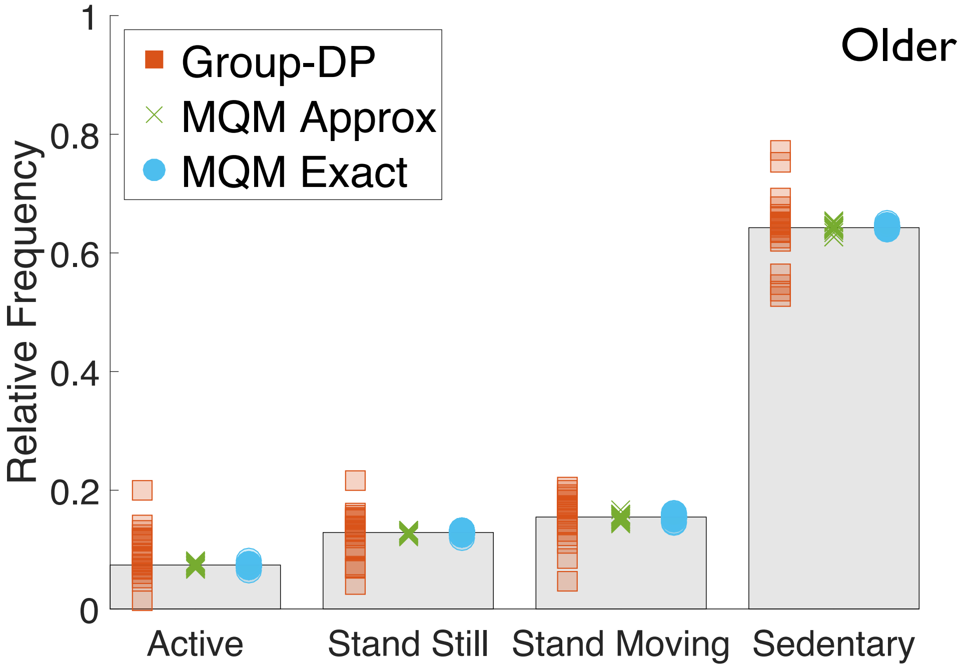
Experiments: Privacy-Utility Trade-off

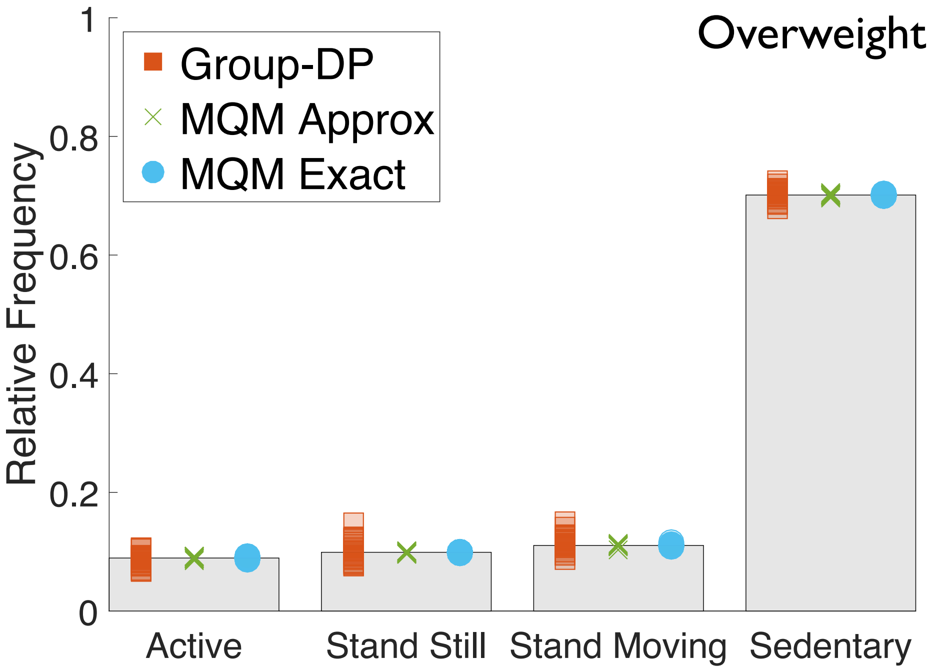
- Data: Markov chains
- Query function f: histogram of states
- Compare four algorithms:
  - Group-DP
  - [GK17]
  - MQM-Approx
  - MQM-Exact

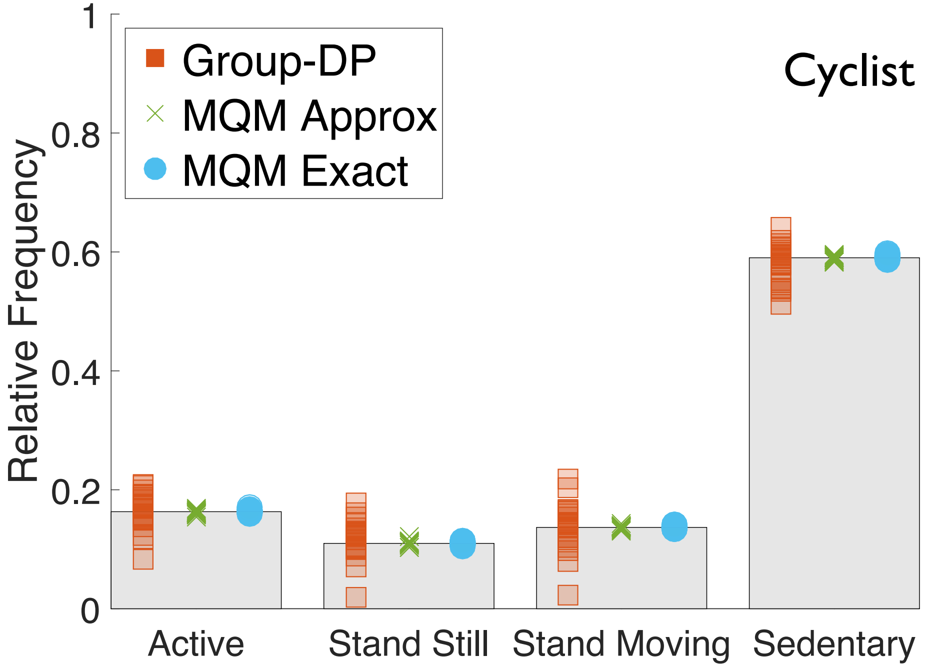
On Physical Activity Data

- 36 overweight subjects, 16 older subjects, 40 cyclists
- ~ every 12 s, ~7 days during daytime (7 chains each of length ~3000)
- 4 states: active, standing still, standing moving, sedentary
- Q: {(activity a at time t, activity b at time t)}
- Θ: obtained from data

- Aggregate histograms over each group of subjects





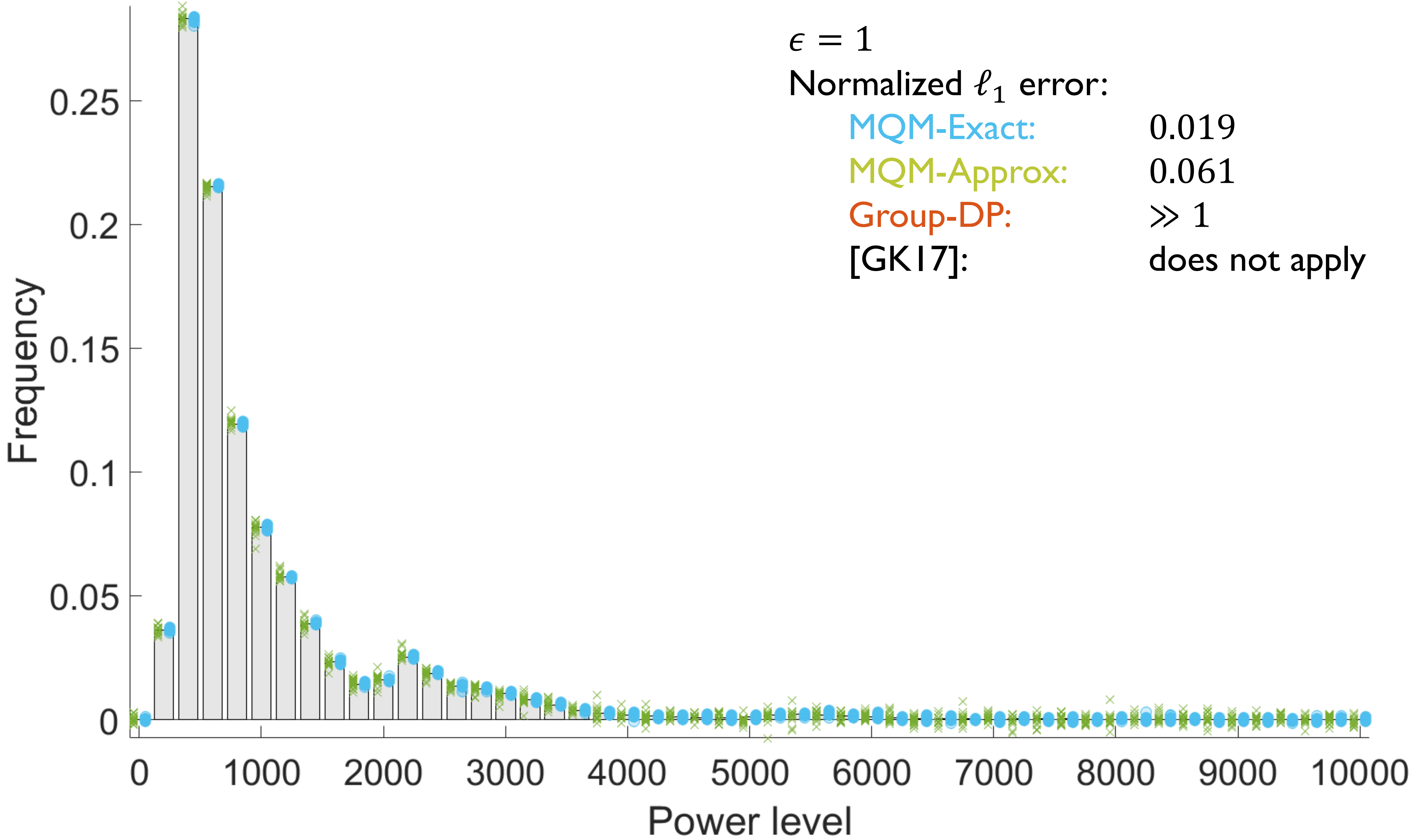


- $\epsilon = 1$
- Four algorithms:
  - MQM-Exact
  - MQM-Approx
  - Group-DP
  - [GK17]: does not apply

On Electricity Power Data

- Electricity power meter reading (Watt) in a single household in the greater Vancouver area, BC, Canada
- Every 1 min, ~2 years (1 chain of length ~1,000,000)
- Divided into 200:200:10000W (51 states)
- Q: {(power level a at time t, power level b at time t)}
- Θ: obtained from data

Makonin, S., Ellert, B., Bajić, I.V., & Popowich, F. (2016). Electricity, water, and natural gas consumption of a residential house in Canada from 2012 to 2014. Scientific data, 3.



$\epsilon = 1$
Normalized ℓ_1 error:
MQM-Exact: 0.019
MQM-Approx: 0.061
Group-DP: $\gg 1$
[GK17]: does not apply
Frequency
0.25
0.2
0.15
0.1
0.05
0
0
1000
2000
3000
4000
5000
6000
7000
8000
9000
10000
Power level

Running Time

- Running time in second:

	Overweight	Older	Cyclist	Power Data
MQM-Approx	0.0028	0.0060	0.0064	0.0567
MQM-Exact	0.6299	1.2786	1.5186	282.2273

- Use MQM-Approx when
  - State space is large
  - Enough data to mitigate the effect of the approximation

Summary

- Privacy definition:
  - Pufferfish privacy framework

- Our contributions:
  - Wasserstein Mechanism for general Pufferfish instantiations
  - Markov Quilt Mechanism for Bayesian network
  - Experimental results

Questions?

Wasserstein Mechanism

- How sensitive is the query function wrt to secret pair (s_i, s_j)?
- $p(f(X)|s_i, \theta)$ vs. $p\left(f(X)\middle|s_j, \theta\right)$
  - Need a right distance measurement for distributions

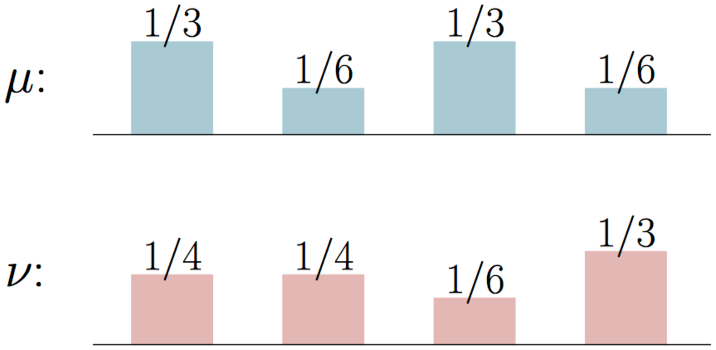
Wasserstein distance

∞-Wasserstein Distance

- Two random variables $X \sim \mu, Y \sim \nu$

$$W_\infty(\mu, \nu) = \inf_{\gamma \in \Gamma(\mu,\nu)} \max_{(x,y) \in A_\gamma} |x - y|$$

  - $\Gamma(\mu, \nu)$: all possible joint distributions of X, Y
  - A_γ: the support of $\gamma \in \Gamma(\mu, \nu)$
- The minimum "effort" needed to convert μ to ν.



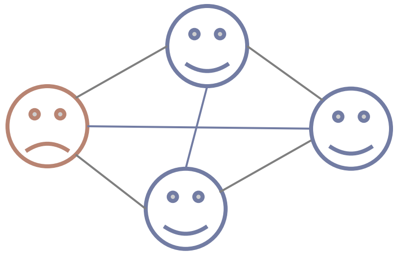
$$W_\infty(\mu, \nu) = 1$$

Wasserstein Mechanism

- Given any query function f,
  - For any secret pair $(s_i, s_j) \in Q$, any $\theta \in \Theta$:
    - $\mu_{i,\theta} = p(f(X)|s_i, \theta), \mu_{j,\theta} = p\big(f(X)\big|s_j, \theta\big)$
    - $W_{i,j,\theta} = W_\infty(\mu_{i,\theta}, \mu_{j,\theta})$
  - $W = \sup_{s_i, s_j, \theta} W_{i,j,\theta}$
  - $M(D) = f(D) + \mathrm{Lap}(W/\epsilon)$

- Theorem: Wasserstein Mechanism guarantees ϵ-Pufferfish privacy

Always Better than Group-DP



- N: # of infected people

	N = 0	N = 1	N = 2	N = 3	N = 4
$P(N\|X_i = 0)$	0.2	0.225	0.5	0.075	0
$P(N\|X_i = 1)$	0	0.075	0.5	0.225	0.2

- Wasserstein Mechanism: noise w/ sd ~ 2
- Group-DP: noise w/ sd ~ 4

- Wasserstein Mechanism always no worse than Group-DP