Privacy of Real-Time Pricing in Smart Grid

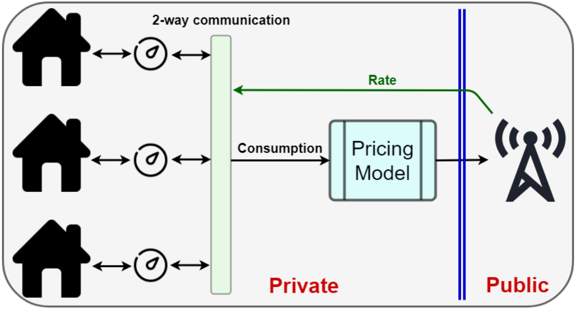
Mahrokh Ghoddousi[⋆], Dominik Fay[†],
Christos Dimitrikakis[†], Maryam Kamgarpour[⋆]

[⋆]Automatic Control Laboratory, ETH Zürich
[†]Computer Science and Engineering faculty, Chalmers University of Technology

CDC, December 12th, 2019

Motivations

Real-time pricing (RTP): Assigning an electricity rate based on the consumption in discrete time intervals



+: Customers' load shift

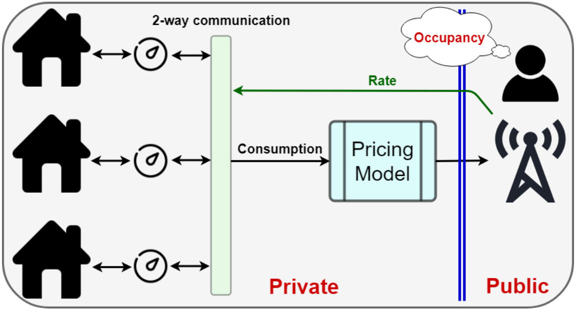
$\Longrightarrow$ save costs and flatten demand curve

−: Public rate broadcasting

$\Longrightarrow$ may leak information about *individuals' occupancy*

Motivations

Real-time pricing (RTP): Assigning an electricity rate based on the consumption in discrete time intervals



+: Customers' load shift

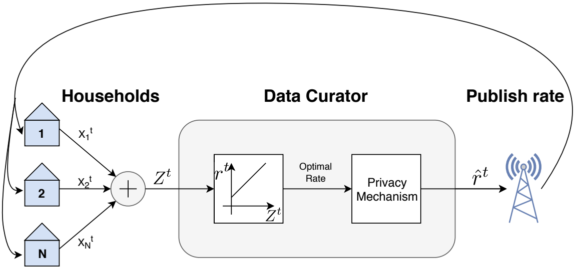
$\implies$ save costs and flatten demand curve

−: Public rate broadcasting

$\implies$ may leak information about *individuals' occupancy*

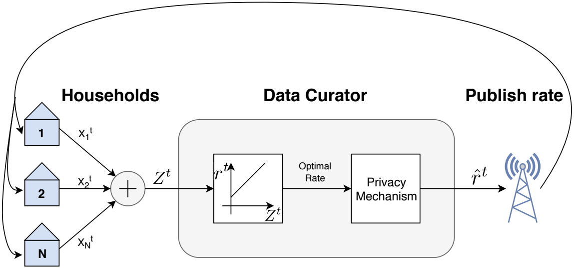
Table of Content

Problem Setup: Households' Side



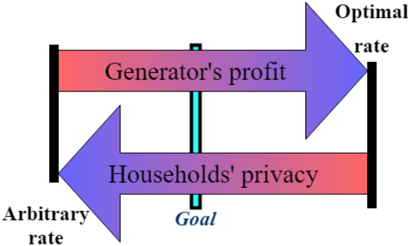
- Published rates before time step t: $\{\hat{r}^{t'} : 1 \leq t' < t\}$
- Household i consumes X_i^t
  - depending on the previous rates and its' occupancy S^t
  - independent from others
  - consumption is protected
  - $X_i^t \sim f(X_i^t | S_i^t, \hat{r}^{t'})$ is common knowledge
  - if house i is occupied $X_i^t \leq u_i$; else $X_i^t \leq u'_i$

Problem Setup: Provider's Side



- Total consumption: $Z^t = \sum_{i=1}^{N} X_i^t$
- Elec. generation cost: $J(Z^t) = \frac{\alpha}{2}(Z^t)^2 + \beta Z^t + \gamma$ [Glover, et al., 2012]
- Generator's profit of selling Z^t at rate r^t is $r^t Z^t - J(Z^t)$
- Optimal rate: $r^t = \alpha Z^t + \beta$
  - an aggregate function of individuals' consumption
  - publishing r^t imposes privacy risk to households [Dwork, et al., 2014]

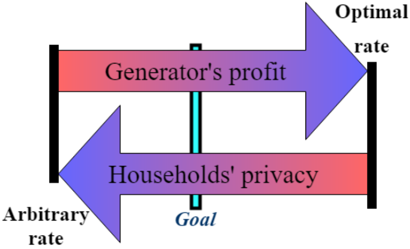
Problem Statement



Goal

- Publish dynamic electricity rates close to the optimal ones
- Prevent anyone from knowing if a specific house is occupied or not at anytime

Problem Statement



Goal

- Publish dynamic electricity rates close to the optimal ones
- Prevent anyone from knowing if a specific house is occupied or not at anytime

Further Challenges

C1) Publish continual rates $r^1, \cdots, r^T$ over T time steps

C2) The occupancy states are time-correlated

C3) The rates have to be computed and published in real time

C4) sensitive data (occupancy) $\neq$ dataset (power consumption)

Further Challenges

C1) Publish continual rates $r^1, \cdots, r^T$ over T time steps

[Cao, et al., 2017]

C2) The occupancy states are time-correlated

[Kessler, et al., 2015]

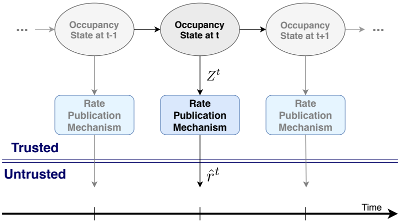
C3) The rates have to be computed and published in real time

C4) sensitive data (occupancy) $\neq$ dataset (power consumption)

This paper: Blowfish privacy

Modeling Correlations

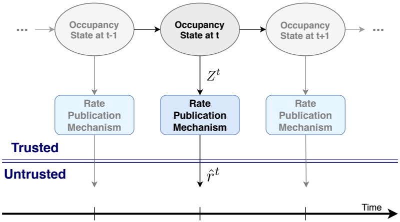
- Continuous Density Hidden Markov Model
  - how do people change their occupancy? [Kleiminger, et al., 2013]
  - how does the occupancy affect consumption?



- States: occupancy of all households
  - transition matrix: how people change their occupancy
- Observations: released rates
  - random variable depending on the state

Modeling Correlations

- Continuous Density Hidden Markov Model
  - how do people change their occupancy? [Kleiminger, et al., 2013]
  - how does the occupancy affect consumption?



- States: occupancy of all households
  - transition matrix: how people change their occupancy
- Observations: released rates
  - random variable depending on the state

Adversarial Model

Adversary

Every third party who wishes to increase her chance of guessing the occupancy state of a single participant

- Has access to the rates
- Considers an occupancy model
- *Prior/Posterior* probability distribution: *Before/After* observing the rate at t
- Obtain info observing continual rates $\Longrightarrow$ impossible states

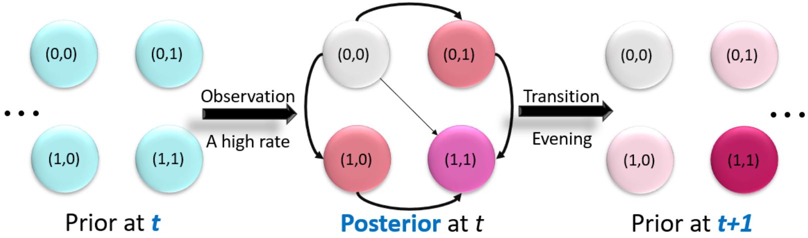


Table of Content

Differential Privacy

- **Aim:** hide the effect of single individuals on a published aggregate statistic (query)

Laplace Mechanism

Query answer $+$ Laplace noise with std $\propto$ sensitivity

The maximum amount each person can change the query answer $\Longrightarrow$ sensitivity of a query

- Answering a query on correlated datasets makes privacy protection harder
  - knowing occupancy at a previous time step $\Longrightarrow$ inferring information about the current occupancy
  - RTP sens. in T time steps $= T\times$ RTP sens. in 1 time step

Differential Privacy

- **Aim:** hide the effect of single individuals on a published aggregate statistic (query)

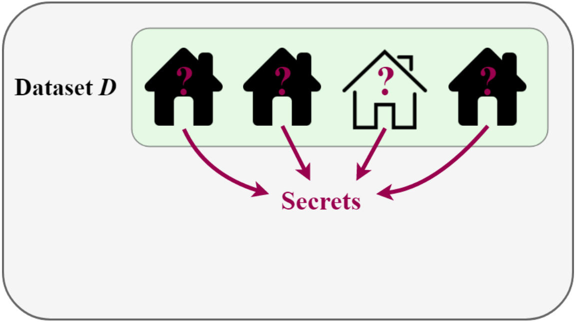
Laplace Mechanism

Query answer $+$ Laplace noise with std $\propto$ sensitivity

The maximum amount each person can change the query answer $\Longrightarrow$ sensitivity of a query

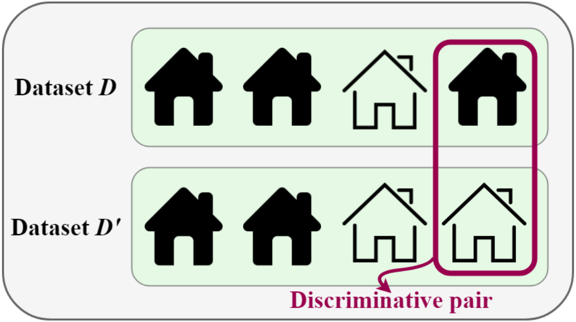
- Answering a query on correlated datasets makes privacy protection harder
  - knowing occupancy at a previous time step $\Longrightarrow$ inferring information about the current occupancy
  - RTP sens. in T time steps $= T\times$ RTP sens. in 1 time step

Blowfish Privacy: Elements (1)



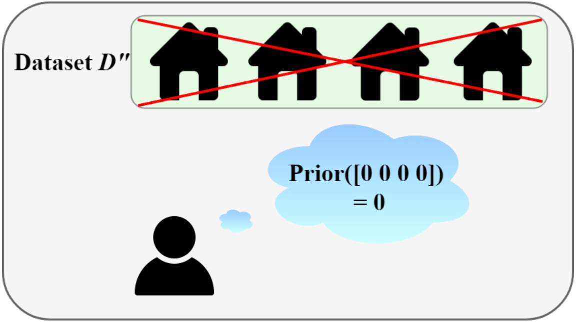
- **Secrets:** information to protect
- **Discriminative pairs:** indistinguishable to the adversary

Blowfish Privacy: Elements (1)



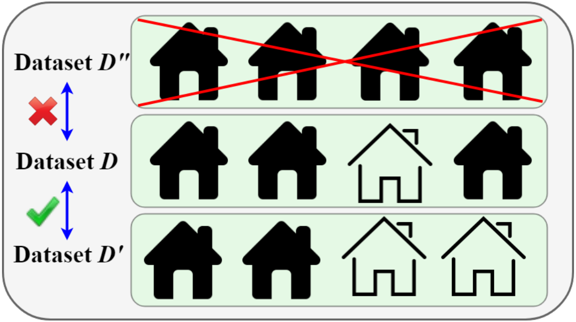
- **Secrets:** information to protect
- **Discriminative pairs:** indistinguishable to the adversary

Blowfish Privacy: Elements (2)



- **Constraints:** publicly known information about the data
  - *ex:* impossible states
  - restrict the universe of datasets to the compatible ones

Blowfish Privacy: Neighbors



Blowfish neighbors

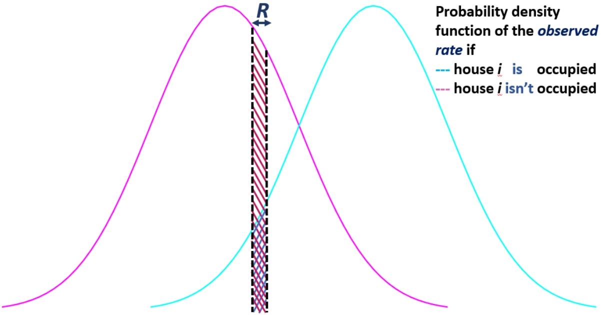
A pair of datasets s.t.

- both satisfy the constraints
- differ in only 1 discriminative pair

Blowfish Privacy: Definition

Blowfish privacy

Given $\epsilon \in \mathbb{R}_+$, discriminative pairs $\mathcal{S}^t_{pairs}$, and a set of constraints Q^t, a mechanism $\mathcal{A} : U \rightarrow \mathbb{R}$ is $(\epsilon, \mathcal{S}^t_{pairs}, Q^t)$-*Blowfish private* if for all Blowfish neighbors D^t, $\hat{D}^t$ and every set of outputs $R \subseteq Range(\mathcal{A})$, $Pr[\mathcal{A}(D^t) \in R] \leq e^{\epsilon} Pr[\mathcal{A}(\hat{D}^t) \in R]$



Proposed Mechanism

- *Recall 1:* Constraints determine the *possible* datasets
- *Recall 2:* States with *0 prior* probability are impossible

Constraint: Having non-zero prior

- Intuition: The adversary concludes that states with 0 prior will not happen $\implies$ protecting them is pointless

Algorithm sketch:

Assuming a model θ, at each time step:

1. Calculate the prior
2. Find all Blowfish neighbors
3. Form a set of houses that differ between neighbors ($\kappa^{t,\theta}$)
4. Find the sensitivity of the optimal rate to the houses in the set ($\lambda^{t,\theta} \leftarrow \alpha \times \max_{h \in \kappa^{t,\theta}} u_h$)
5. Add Laplace noise with std $= \lambda^{t,\theta}/\epsilon$

Proposed Mechanism

- *Recall 1:* Constraints determine the *possible* datasets
- *Recall 2:* States with *0 prior* probability are impossible

Constraint: Having non-zero prior

- Intuition: The adversary concludes that states with 0 prior will not happen $\implies$ protecting them is pointless

Algorithm sketch:

Assuming a model θ, at each time step:

1. Calculate the prior
2. Find all Blowfish neighbors
3. Form a set of houses that differ between neighbors $(\kappa^{t,\theta})$
4. Find the sensitivity of the optimal rate to the houses in the set $(\lambda^{t,\theta} \leftarrow \alpha \times \max_{h \in \kappa^{t,\theta}} u_h)$
5. Add Laplace noise with std $= \lambda^{t,\theta}/\epsilon$

Privacy Guarantees

Theorem 1

The proposed rate publication mechanism preserves $(\epsilon, \mathcal{S}^t_{pairs}, Q^t)$-Blowfish privacy at each time step

Main ideas of the proof:

1. Derive the probability of observing a rate in range R
2. For all neighbors, find the noise std ensuring privacy
3. Use the greatest deviation to keep all neighbors approx. indistinguishable

Theorem 2

The mechanism is $(\epsilon T, \mathcal{S}_{pairs}, Q)$-Blowfish private observing T rates where $\mathcal{S}_{pairs} = (\mathcal{S}^1_{pairs}, \cdots, \mathcal{S}^T_{pairs})$ and $Q = (Q^1, \cdots, Q^T)$

Privacy Guarantees

Theorem 1

The proposed rate publication mechanism preserves $(\epsilon, \mathcal{S}^t_{pairs}, Q^t)$-Blowfish privacy at each time step

Main ideas of the proof:

1. Derive the probability of observing a rate in range R
2. For all neighbors, find the noise std ensuring privacy
3. Use the greatest deviation to keep all neighbors approx. indistinguishable

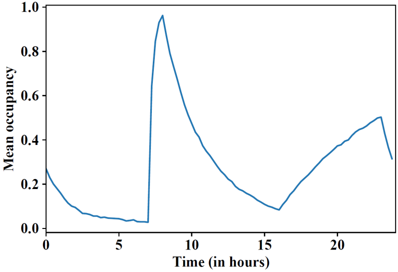
Theorem 2

The mechanism is $(\epsilon T, \mathcal{S}_{pairs}, Q)$-Blowfish private observing T rates where $\mathcal{S}_{pairs} = (\mathcal{S}^1_{pairs}, \cdots, \mathcal{S}^T_{pairs})$ and $Q = (Q^1, \cdots, Q^T))$

Table of Content

Simulating the Occupancy States

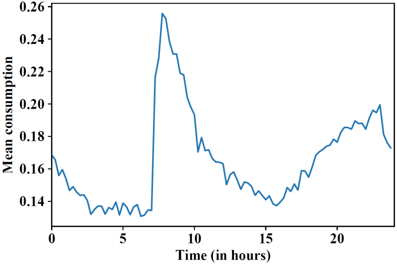
- 4 transition matrices for the morning, noon, evening, and night
- Difference between individuals' habits $\implies$ perturb the matrices by adding Gaussian noise for each household



- Simulations for 15-min intervals over a day

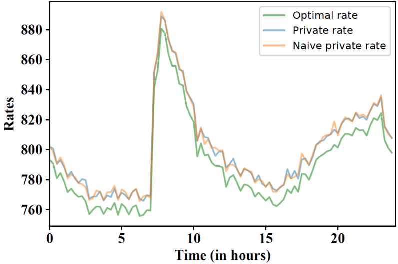
Simulating the Consumption

- house i consumption $X_i^t \sim U(0, u_i)$
  - $\max$ empty house consumption $u_i \sim U(0, 0.5)$
  - $\max$ occupied house consumption $u_i \sim U(0, 1)$



Results

- Naive mechanism: doesn't model occupancy $\implies$ doesn't remove any states



- Evaluation measure: deviation from the optimal rates

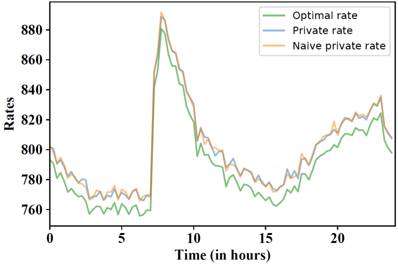
$$E := \frac{1}{T}\sqrt{\sum_{t=1}^{T}((\hat{r}^t - r^t)/r^t)^2}$$

- $E_{Naive} = 1.149e-3$ *vs.* $E_{Blowfish} = 1.089e-3$

$$\implies 5.5\%\textbf{decrease}$$

Results

- Naive mechanism: doesn't model occupancy $\Longrightarrow$ doesn't remove any states



- Evaluation measure: deviation from the optimal rates

$$E := \frac{1}{T}\sqrt{\sum_{t=1}^{T}((\hat{r}^t - r^t)/r^t)^2}$$

- $E_{Naive} = 1.149e-3$ vs. $E_{Blowfish} = 1.089e-3$

$\Longrightarrow$ **5.5%decrease**

Table of Content

Conclusions

- Introduce an occupancy model
  - how people change their occupancy
  - what is the relationship between the occupancy and the released rate
  - how can an adversary infer information accessing the rates

- Improving the naive mechanism:
  - if there is enough evidence that a state is not possible, remove it from the set of protected states

Conclusions

- Introduce an occupancy model
  - how people change their occupancy
  - what is the relationship between the occupancy and the released rate
  - how can an adversary infer information accessing the rates

- Improving the naive mechanism:
  - if there is enough evidence that a state is not possible, remove it from the set of protected states

Future Work

- Less noise at each time step
  - studying states with small prior probabilities rather than the 0 ones
- Reduce linear privacy degradation with time horizon
  - find *far* time steps $\implies$ almost independent [Song, et al., 2017]
    rate at t doesn't reveal info about a far time step

Thank you for your attention!

Updating Prior and Posterior

- **Notation:** Assuming a model θ

  $P^{t|t-1,\theta}$ is prior at t
  $P^{t|t,\theta}$ is posterior at t
  $i \in \{1, \cdots, m\}$ shows the number of the state
  $\mathbf{A}^{t,\theta}$ is the transition matrix

- **Updating equations:** By Bayesian inference,

$$P^{t|t-1,\theta} = P^{t-1|t-1,\theta} \times \mathbf{A}^{t,\theta}$$

$$P_i^{t|t,\theta} = \frac{P_i^{t|t-1,\theta} \times Pr[\hat{r}^t|M^i]}{\sum_{j=1}^m P_j^{t|t-1,\theta} \times Pr[\hat{r}^t|M^j]}$$

Algorithm Details

Algorithm 1 Rate Publication Mechanism

Input: privacy parameter ϵ, time horizon T, rate function parameters (α, β), consumption bound for each household u_i, set of data generating models Θ

Output: Published rates $\hat{r}^1, \cdots, \hat{r}^T$

At each time step $t \in \{1, \cdots, T\}$:
for $\theta = (\mathbf{A}^{t,\theta}, \Pi^{\theta}) \in \Theta$ **do**
  initialize: $P^{1|0,\theta} \leftarrow \Pi^{\theta}$ ▷ Prior at step 1
  $P^{t|t-1,\theta} \leftarrow P^{t-1|t-1,\theta}\mathbf{A}^{t,\theta}$ ▷ Calculate prior
  $\mu^{t,\theta} \leftarrow \{M^i | P_i^{t|t-1,\theta} \neq 0\}$ ▷ Non-zero prior states
  $\nu^{t,\theta} \leftarrow \{(M^i, M^j) \in \mu^{t,\theta} \times \mu^{t,\theta} \mid ||M^i - M^j||_1 = 1\}$
  $\kappa^{t,\theta} \leftarrow \{$*Entries that differ between pairs in* $\nu^{t,\theta}\}$
  $\lambda^{t,\theta} \leftarrow \alpha \times \max_{h \in \kappa^{t,\theta}} u_h$
end for
$\lambda^t \leftarrow \max_{\theta \in \Theta} \lambda^{t,\theta}$ ▷ Maximum over all models
$r^t \leftarrow \alpha \sum_{i=1}^{N} X_i^t + \beta$ ▷ Optimal rate
$N^t \sim Lap(\lambda^t / \epsilon)$ ▷ Noise to be added
$\hat{r}^t \leftarrow r^t + N^t$ ▷ Noisy rate
return $\hat{r}^t$ ▷ Publish rate
Derive $P^{t|t,\theta}$ $\forall \theta \in \Theta$ by Equation (3)
Go to time step *t+1*

Proof of Theorem 1 (1)

Theorem 1

The proposed rate publication mechanism preserves $(\epsilon, \mathcal{S}^t_{pairs}, Q^t)$-Blowfish privacy at each time step

- Blowfish neighbors M^l and M^k with $M^l_1 = 1$, $M^k_1 = 0$, and $M^l_{2:N} = M^k_{2:N}$
- Probability of observing a rate of w at time t conditioned on the state S^t

$$Pr[\hat{r}^t{=}w|S^t{=}M^l]{=}\int\cdots\int\frac{\epsilon}{2\lambda_1^{t,\theta}}\prod_{\ell=1}^{N} f(X^t_\ell|S^t_\ell{=}M^l_\ell, \hat{r}^{t-1})$$
$$\times exp(-\epsilon|w-\alpha\sum_{i=1}^{N} X^t_i - \beta|/\lambda_1^{t,\theta})d_{X^t_1}\cdots d_{X^t_N} \qquad (1)$$

Proof of Theorem 1 (2)

- Let $g := (w - \alpha(\sum_{i=2}^{N} X_i^t + \frac{u_1}{2}) - \beta)/\alpha$

$$e^{\frac{-\epsilon\alpha}{\lambda_1^{t,\theta}}(|g| + |X_1^t - \frac{u_1}{2}|)} \leq e^{\frac{-\epsilon\alpha}{\lambda_1^{t,\theta}}|g - (X_1^t - \frac{u_1}{2})|} \leq e^{\frac{-\alpha\epsilon}{\lambda_1^{t,\theta}}(|g| - |X_1^t - \frac{u_1}{2}|)}$$

(Triangle inequality)

$$\Rightarrow e^{\frac{-\epsilon\alpha}{\lambda_1^{t,\theta}}(|g| + \frac{u_1}{2})} \leq e^{\frac{-\epsilon\alpha}{\lambda_1^{t,\theta}}|g - (X_1^t - \frac{u_1}{2})|} \leq e^{\frac{-\alpha\epsilon}{\lambda_1^{t,\theta}}(|g| - \frac{u_1}{2})} \qquad (2)$$

$$(X_1^t \in [0, u_1])$$

- Substitute (2) in (1)

$$\int \cdots \int e^{\frac{-\epsilon\alpha}{\lambda_1^{t,\theta}}(g + \frac{u_1}{2})} \prod_{\ell=1}^{N} f(X_\ell^t | S_\ell^t = M_\ell^l, \hat{r}^{t-1}) d_{X_1^t} \cdots d_{X_N^t}$$

$$\leq \frac{2\lambda_1^{t,\theta}}{\epsilon} Pr[\hat{r}^t = w | S^t = M^l] \leq$$

$$\int \cdots \int e^{\frac{-\epsilon\alpha}{\lambda_1^{t,\theta}}(g - \frac{u_1}{2})} \prod_{\ell=1}^{N} f(X_\ell^t | S_\ell^t = M_\ell^l, \hat{r}^{t-1}) d_{X_1^t} \cdots d_{X_N^t}$$

Proof of Theorem 1 (3)

- Remove the inner integral by integrating over X_1^t, yielding *1*

$$\int\cdots\int e^{\frac{-\epsilon\alpha}{\lambda_1^{t,\theta}}(g+\frac{u_1}{2})}\prod_{\ell=2}^{N} f(X_\ell^t|S_\ell^t{=}M_\ell^l,\hat{r}^{t-1})d_{X_2^t}\cdots d_{X_N^t}$$
$$\leq \frac{2\lambda_1^{t,\theta}}{\epsilon}Pr[\hat{r}^t = w|S^t = M^l] \leq$$
$$\int\cdots\int e^{\frac{-\epsilon\alpha}{\lambda_1^{t,\theta}}(g-\frac{u_1}{2})}\prod_{\ell=2}^{N} f(X_\ell^t|S_\ell^t{=}M_\ell^l,\hat{r}^{t-1})d_{X_2^t}\cdots d_{X_N^t}$$

- Repeat for $\hat{S}^t$ and divide the inequalities

$$e^{\frac{-\epsilon\alpha}{\lambda_1^{t,\theta}}u_1} \leq \frac{Pr[\hat{r}^t = w|S^t = M^l]}{Pr[\hat{r}^t = w|\hat{S}^t = M^k]} \leq e^{\frac{\epsilon\alpha}{\lambda_1^{t,\theta}}u_1} \qquad (3)$$

- Keeping data of user *1* private $\implies \lambda_1^{t,\theta} \geq \alpha u_1$

Proof of Theorem 1 (4)

Corollary

If two neighbor datasets have different occupancy state for house i, adding noise sampled from $Lap(\lambda_i^{t,\theta}/\epsilon)$ with $\lambda_1^{t,\theta} \geq \alpha u_i$ suffices

$\implies \lambda^{t,\theta} = \alpha . \max_{h \in \kappa^{t,\theta}} u_h$ ensures all secret pairs are secured from disclosure given model θ

Proof of Theorem 2

Theorem 2

The mechanism is $(\epsilon T, \mathcal{S}_{pairs}, Q)$-Blowfish private observing T rates where $\mathcal{S}_{pairs} = (\mathcal{S}^1_{pairs}, \cdots, \mathcal{S}^T_{pairs})$ and $Q = (Q^1, \cdots, Q^T))$

- Rates $\hat{r} = (\hat{r}^1, \cdots, \hat{r}^T)$
- $S = (S^1, \cdots, S^T)$ and $\hat{S} = (\hat{S}^1, \cdots, \hat{S}^T)$ are Blowfish neighbors $\forall t \in \{1, \cdots, T\}$
- probability of being at states S and observing rates $\hat{r}$

$$Pr[S, \hat{r}] = \pi_{S^1} \prod_{t=2}^{T} Pr[S^t|S^{t-1}] \prod_{t=1}^{T} Pr[\hat{r}^t|S^t]$$

$$= Pr[S] \prod_{t=1}^{T} Pr[\hat{r}^t|S^t] \leq Pr[S] \prod_{t=1}^{T} e^{\epsilon} Pr[\hat{r}^t|\hat{S}^t]$$

($(\epsilon, \mathcal{S}^t_{pairs}, Q^t)$-Blowfish privacy at each time step)

$$Pr[\hat{r}|S]/Pr[\hat{r}|\hat{S}] \leq exp(\epsilon T)$$