Updates on Research and Collaborations

Matthew Hale
Department of Mechanical and Aerospace Engineering
University of Florida

Center of Excellence for Assured Autonomy in Contested Environments
Fall 2021 Review
November 9th, 2021
• Hybrid multi-agent optimization with Dawn Hustig-Schultz, Ricardo Sanfelice (UCSC)
  • “Exponentially Converging Distributed Gradient Descent with Intermittent
    Communication via Hybrid Methods” to appear at CDC ’21
  • Ricardo visited UF, made plans for next steps/journal version

• New privacy mechanism on the unit simplex with Parham Gohari, Bo Wu, Ufuk Topcu (UT-A)
  • P. Gohari, B. Wu, C. Hawkins, M. Hale and U. Topcu, "Differential Privacy on the Unit
    Simplex via the Dirichlet Mechanism," IEEE Transactions on Information Forensics and
  • Parham visited UF again, worked out basis for private policy synthesis in MDPs

• Resilient multi-agent control with Fred Zegers (UF & AFRL) and John Shea, Warren Dixon (UF)
    and Leader Tracking With Resilience to Byzantine Adversaries: A Reputation-Based
    Approach," IEEE Transactions on Control of Network Systems, vol. 8, no. 3, pp. 1417-
  • Discussions on incorporating privacy into event-triggered communication
Collaborations with Air Force Colleagues

• Applied optimization work to weapon-target assignment (WTA) problems
  • Kat and Kyle are full-time at UF REEF, collaborations continue

• Developed order-optimal algorithm for anomaly detection in multi-armed bandits with switching costs
  • With Ben Robinson and Beth Morrison at AFRL/RY
  • Publication forthcoming

• Engaging with AFRL every summer
  • William Warke was a Summer Scholar in 2018, 2019 at RW
  • I was a Summer Faculty Fellow at RW in 2020
  • Matthew Ubl was a Summer Scholar in 2021 at RY
  • William Warke applying to RW for 2022, Gabriel Behrendt applying to RV for 2022
Differential Privacy for Symbolic Systems with applications to Markov Chains

Bo Chen\textsuperscript{a}, Kevin Leahy\textsuperscript{b}, Austin Jones\textsuperscript{c}, Matthew Hale\textsuperscript{a}

Program Review for Center of Excellence on Assured Autonomy in Contested Environments

November 9\textsuperscript{th}

\textsuperscript{a}University of Florida, \textsuperscript{b}MIT Lincoln Laboratory, \textsuperscript{c}Arbor Biotechnologies.
Data driven systems create privacy threats

• Modern systems use more data than ever.

• In controls, sensitive information might be agents’ dynamics, control inputs, state trajectories, etc.

• Agents might reveal sensitive information while collaborating.

• In this talk, we focus on state trajectories for symbolic systems.
Strong data protections are difficult to get

• Simply making data anonymous does not work, e.g. Netflix was subject to a linkage attack.

• Takeaway: we don't know what else an adversary might know about us.

• Key question: how can we safeguard information against these threats in symbolic systems?
Solution? Differential Privacy!

- Formal definition of privacy from computer science literature.
- In short, randomize data to protect it. (Details later.)
- Immune to post-processing: $x$ is private implies $f(x)$ is private.
- No need to anticipate types of privacy attacks.
- Used by Google, Apple, Uber, and the 2020 Census.

We will design this!
New privacy notions are needed here

• Differential privacy is often implemented on numerical systems.
  • Numerical system: state trajectories can be represented by numbers.
  • For data $x$, we have a private data $\tilde{x} = x + z$, $z$ is Gaussian or Laplace noise.

Mike’s daily trajectory: (“Home”, “Office”, “Restaurant”, “Grocery”)

• How about symbolic systems?
Markov chain, a special symbolic system

• In this talk we focus on Markov chains.

• A Markov chain is a stochastic model describing a sequence of random variables $S_1, S_2 \ldots S_n$ such that
  \[
  \Pr[S_{t+1} | S_t, S_{t-1}, \ldots, S_1] = \Pr[S_{t+1} | S_t]
  \]

• States can be non-numerical.

Private outputs can’t be nonsense

• Goal for privacy of Markov chains: privatize sequence of states.[1]
• For a private sequence $w = s_1 s_2 ... s_n$ and any $t$, we must enforce $\Pr[s_{t+1} | s_t] > 0$

Differential Privacy on symbolic systems

- Goal of differential privacy: generate randomized outputs in order to “mask” differences between “similar” sequences.
- “Similar” sequences are defined by adjacency relationship.

**Definition 1 (Word Adjacency):** For a positive integer \( n \) and \( k \), the word adjacency relation between two words \( w_1, w_2 \) is \( Adj_{n,k} = \{ (w_1, w_2) | d(w_1, w_2) \leq k \} \).

**Definition 2 (Hamming Distance):** The Hamming distance between sequences \( w_1, w_2 \) denoted by \( d(w_1, w_2) \), is the minimum number of substitutions that can be applied to \( w_1 \) to convert it to \( w_2 \).
Definition 3 (Word Differential Privacy):
Let $\varepsilon > 0$. A randomized algorithm $M$ is $\varepsilon$-differential private if for all $S \subseteq \text{Range}(M)$ and for all word adjacent sequence $(w_1, w_2) \in \text{Adj}_{n,k}$ we have
$$\Pr[M(w_1) \in S] \leq \exp(\varepsilon) \Pr[M(w_2) \in S]$$

• Smaller epsilon implies stronger privacy.
• In literatures, $\varepsilon$ is ranging from $[0.01, 10]$.\footnote{2}

Differential Privacy on symbolic systems

• Goal of differential privacy: generate randomized outputs in order to “mask” differences between “similar” sequences.
• “Mask” means an adversary can not reliably tell if an output sequence is generated by an individual sequence or any adjacent sequence.


Which one is generated by “bumper”?
We need two types of mechanisms

i) Offline Mechanism (batch privacy)
   • Privatize the whole sensitive sequence \( w = \sigma_1 \sigma_2 \ldots \sigma_n \) at once.

![Diagram of Bumper and Private Algorithm](diagram.png)

ii) Online Mechanism (real-time privacy)
   • Generate differentially private outputs but future states are unknown.

![Diagram of Private Algorithm and Bumper](diagram.png)

iii) For both
   • The private outputs of states are feasible.
   • Quantify tradeoffs between privacy and accuracy.
Construct offline mechanism

• Main idea: each feasible sequence can be selected based on Hamming distance.  
  \[ \text{Time complexity: } O(|S|^n). \]

• Challenge: We need to make sure this is efficient!

• Procedure of constructing offline mechanism.
  • Step 1: Select a Hamming distance \( l \).
  • Step 2: Select a private output from only sequences that have Hamming distance \( l \) to the input sequence.
Step 1: Select a Hamming distance

- For an input sequence $x$, Adjacency $Adj_{|x|,k}$, and privacy parameter $\varepsilon$, select a Hamming distance using the distribution

$$
\rho(l; |x|, k) = \frac{m_l \exp\left(-\frac{\varepsilon l}{2k}\right)}{\sum_{i=0}^{|x|} m_i \exp\left(-\frac{\varepsilon i}{2k}\right)}
$$

Length of sensitive input word

Number of possible sequences that are distance $i$ from input

For $|x| = 10, k = 1$

$\varepsilon = 1$

$\varepsilon = 2$

$\varepsilon = 3$

Length of sensitive input word

Number of possible sequences that are distance $i$ from input
Step 2: Select a private output

- Find sequences which are with a Hamming distance \( l \) efficiently.
- For a non-Markov symbolic system, we can do this using modified Hamming distance automaton. (Will make it Markov in next slide)

- **Takeaway:** This automaton is efficient and generate output sequence.

![Diagram](image)

Set of possible output characters which are independent with each other.

For an input “abc” and \( l=2 \)
Step 2: Select a private output

- Main idea: to extend to a Markov chain, we make synchronous product of the modified Hamming distance automaton and the Markov chain.

- The offline mechanism first selects a Hamming distance $l$, then selects an output sequence by running a product modified Hamming distance automaton.

Key Result: The offline mechanism is $\epsilon$-differentially private.
Concentration bounds

**Theorem 2 (differential privacy and concentration bounds):** For an input sequence $w_i$, let $w_o$ be an output sequence generated by the offline mechanism, then $w_o$ is $\varepsilon$-differentially private and the expectation and variance of distance is bounded by

$$\frac{n(N_{\text{min}} - 1)B_{\varepsilon,k}[(N_{\text{min}} - 1)B_{\varepsilon,k} + 1]^{n-1}}{\sum_{i=0}^{\sigma_i} m_i \exp\left(-\frac{\varepsilon i}{2k}\right)} \leq E[d(w_i, w_o)] \leq \frac{nN_{\text{max}}B_{\varepsilon,k} [N_{\text{max}}B_{\varepsilon,k} + 1]^{n-1}}{\sum_{i=0}^{\sigma_i} m_i \exp\left(-\frac{\varepsilon i}{2k}\right)}$$

$N_{\text{min}}, N_{\text{max}}$: min/max outdegree

$N_{\text{min}} = 2$, $N_{\text{max}} = 3$

Depends on $\varepsilon$ and $k$

Concentration bounds when $k=1$ and $n=10$. Lower bound

Weaker privacy
Online mechanism for Markov chains

• Main idea: each output state is generated based on the most recently generated private state.
Online mechanism for Markov chains

• For a sensitive input state $s_t$,
  • If $s_t$ is feasible from the most recently private state, then $\Pr[s_t]$ is set to $\tau$ and other states will have identical probability whose sum is $1 - \tau$.
  • If $s_t$ is not feasible then all feasible states will have identical probability whose sum is 1.
Online mechanism for Markov chains

**Theorem 2 (Online Mechanism is differentially private):** For a sensitive input sequence $w_o = s_1^0 s_2^0 ... s_n^0$ and an initial private state $s_0^0$, the online mechanism is word $\varepsilon$-differentially private if

$$\tau(s^0_t) = \frac{1}{(N(s^0_t) - 1) \exp \left(-\frac{\varepsilon}{k}\right) + 1}$$

the number of feasible states

![Graph showing correct probability vs. \(\varepsilon\) for different values of \(N\).](image)

The graph shows the correct probability for different values of \(\varepsilon\) and \(N\).

1. Bo Chen, Kevin Leahy, Austin Jones, Matthew Hale, "Differential Privacy for Symbolic Systems with applications to Markov Chains"
Experiment

• Example Markov chain is generated by the book “Green Eggs and Ham”.

• 50 unique words → 50 states in total.

• We generate differentially private versions of a sequence “I do so like green eggs and ham thank you thank you Sam I am”.

![Diagram of Markov chain](image-url)
Weaker privacy

This is random! We just got lucky!

Different starting word incurs different errors.

Future works

• Generalize to Partial Observable MDPs.
• Using this work on multi-agent reinforcement learning.
Thanks for listening!
Result for different conditions.

Sensitive input: I do so like green eggs and ham thank you thank you Sam I am