2024 American Control Conference (ACC)
July 8-12, 2024. Toronto, Canada

Differential Privacy in Nonlinear Dynamical Systems with Tracking Performance Guarantees

Dhrubajit Chowdhury, Raman Goyal, and Shantanu Rane

Abstract— **We introduce a novel approach to make the tracking error of a class of nonlinear systems differentially private in addition to guaranteeing the tracking error performance. We use funnel control to make the tracking error evolve within a performance funnel that is pre-specified by the user. We make the performance funnel differentially private by adding a bounded continuous noise generated from an Ornstein-Uhlenbeck-type process. Since the funnel controller is a function of the performance funnel, the noise adds randomized perturbation to the control input. We show that, as a consequence of the differential privacy of the performance funnel, the tracking error is also differentially private. As a result, the tracking error is bounded by the noisy funnel boundary while maintaining privacy. We show a simulation result to demonstrate the framework.**

I. Introduction

The use of Cyber-Physical Systems (CPS) in our daily lives has been rapid recently due to the advancement in sensing and computational power. CPS finds widespread applications in various domains, including intelligent transportation systems, smart homes, and even the development of smart cities. However, these systems heavily rely on user-generated data to make informed decisions, thereby increasing the vulnerability of sensitive user information to potential exposure. To address the concern of protecting sensitive user data several privacy-preserving frameworks, namely, differential privacy, information-theoretic privacy, and privacy based on secure multiparty computation have been developed. See the survey paper [1] for a comprehensive overview of privacy algorithms.

A. Background on Differential Privacy

Differential privacy is a statistical notion of privacy that masks sensitive data using a mechanism that makes the output of the mechanism approximately unchanged if data belonging to any single user in the database is modified [2]. One of the main advantages of differential privacy is its protection from post-processing and it is not weakened even if an adversary knows the privacy mechanism used [3], [4]. Differential privacy is introduced using the "input perturbation" approach, which essentially means that noise is added to the system in either the input or output. However, adding noise to the system leads to a degradation in system performance both in static and dynamic cases [4]. In dynamical systems differential privacy makes the state trajectory of the system approximately indistinguishable [4] from other nearby state trajectories which the system could have produced.

Differential privacy was initially intended [3], [5] for protecting the information of individuals within static databases. It has since evolved to handle the privacy issues in control [2] and dynamical systems. Recent work on privacy in linear dynamical systems includes dynamic filters [4], differentially private linear quadratic (LQ) control [6], multi-agent formation control [7], and privacy-preserving consensus [8], [9]. However, unlike linear systems, the research in differential privacy in nonlinear systems is limited. In [10], [11], differential privacy was shown for incrementally input-to-state stable nonlinear systems without any performance guarantees.

B. Main Contribution

The main contributions of this paper are:

- We develop a new framework for making the tracking error of nonlinear systems differentially private using a funnel controller [12]. We add the privacy noise to the performance funnel to make it differentially private. Since the controller is an explicit function of the performance funnel [13], we indirectly add privacy noise to the control input of the system. See the extended version for a figure of the architecture [14].
- The privacy noise which is added to the performance funnel to make it differentially private is continuous and bounded. The performance funnel [13] belongs to a class of weak differentiable functions, therefore we cannot add privacy noise directly to the performance funnel as the noise is discontinuous in nature. The noise is filtered through an Ornstein-Uhlenbeck type process which makes it continuously differentiable and then it is added to the performance funnel. Please see the extended version [14] for detailed explanation.
- We use the funnel control algorithm developed in [13] for controlling the transient behavior of the tracking error for nonlinear systems with arbitrary relative degrees using high-gain observers. Since the tracking error evolves within the performance funnel we show using adjacency relationship that the tracking error becomes differentially private.

II. Tracking Using Funnel Control

A. Funnel Control

The concept underlying funnel control revolves around the use of a performance funnel to regulate the transient

D. Chowdhury, R. Goyal, and S. Rane are with Palo Alto Research Center - Part of SRI International, Palo Alto, CA, USA. {dhruba.chowdhury, raman.goyal, shantanu.rane}@sri.com,

behavior of tracking error. When the error approaches the funnel's boundary, the funnel gain is elevated, preventing the error from reaching the boundary. Fig. 1 provides a visual representation of a performance funnel $\mathcal{F}_\varphi$ and the error evolution within it. Let φ be a function of the following class: $\bar{\Phi}: = \{\varphi \in W^{1,\infty}(\mathbb{R}_{\geq 0}, \mathbb{R}_+) \mid \forall\ \tau \geq 0 :\ \varphi(\tau) > 0 \text{ and } \lim_{\tau\to\infty} \inf \varphi(\tau) > 0\}$ where $W^{1,\infty}(\mathbb{R}_{\geq 0}, \mathbb{R}_+)$ represents the class of weakly differentiable functions. The performance funnel is defined as :

$$\mathcal{F}_\varphi := \{(t, e) \in \mathbb{R}_{\geq 0} \times \mathbb{R} \mid \varphi(t)|e| < 1\} \tag{1}$$

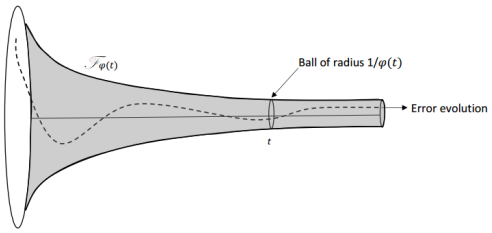

Fig. 1. Performance Funnel $\mathcal{F}_\varphi$

The reciprocal of the function $\varphi(t)$ determines the funnel boundary and the error $e(t)$ evolves within the funnel $\mathcal{F}_\varphi$. In this paper, we assume that the funnel is finite i.e., $\varphi(0) > 0$ and we define the funnel boundary as $\psi(t) = 1/\varphi(t)$.

B. Tracking Problem Definition

We consider the tracking problem for a single-input-single-output system, which is defined globally in the normal form [15] :

$$\dot{\xi}_i = \xi_{i+1},\ 1 \leq i \leq \rho - 1 \tag{2a}$$
$$\dot{\xi}_\rho = a(t, \xi) + b(\xi)u \tag{2b}$$
$$y_p = \xi_1 \tag{2c}$$

where $\xi = \text{col}(\xi_1, \xi_2, \ldots, \xi_\rho) \in R^\rho$, $u \in R$ and $y_p \in R$. The function b is locally Lipschitz; a is locally Lipschitz in ξ and piecewise continuous, bounded in t. We can also extend this class of systems to the special normal form see [16, Section 9.1].

Assumption 1: $b(\xi)$ is known and satisfies

$$b(\xi) \geq b_0 > 0, \quad \forall\ \xi \in R^\rho$$

Assumption 2: The reference signal $r(t)$ and its derivatives up to $r^{(\rho)}(t)$ are bounded for all $t \geq 0$ and the ρth derivative $r^{(\rho)}(t)$ is a piecewise continuous function of t.

We define $\mathcal{R} = \text{col}(r, r^{(1)}, \ldots, r^{(\rho-1)})$ and assume that $r(t)$ is available for control. Consider the following change of variables

$$\omega_1 = \xi_1 - r, \omega_2 = \varrho(\xi_2 - r^{(1)}), \ldots, \omega_\rho = \varrho^{\rho-1}(\xi_\rho - r^{(\rho-1)})$$

where $\varrho > 0$ is a scaling variable. The change of variables in matrix form is defined by $\xi = L^{-1}(\varrho)\omega_f + \mathcal{R}$, where $L(\varrho) = \text{diag}(1, \varrho, \varrho^2, \ldots, \varrho^{\rho-1})$, diag$(\cdot)$ represents a diagonal matrix, and $\omega_f = \text{col}(\omega_1, \ldots, \omega_\rho)$. The change of variables transforms system (2) into:

$$\varrho\dot{\omega}_i = \omega_{i+1}, \quad 1 \leq i \leq \rho - 1 \tag{3a}$$
$$\varrho\dot{\omega}_\rho = \varrho^\rho\{a(t, \xi) + b(\xi)u - r^{(\rho)}(t)\} \tag{3b}$$
$$e = \omega_1 \tag{3c}$$

where $e = y_p - r$ is the tracking error and $\xi = \text{col}\left(\omega_1 + r, \frac{\omega_2}{\varrho} + r^{(1)}, \ldots, \frac{\omega_\rho}{\varrho^{\rho-1}} + r^{(\rho-1)}\right)$.

Assumption 3: There exists a known continuous function $g_1(\cdot)$ such that

$$|\varrho^{\rho-1}a(t, L^{-1}(\varrho)\omega_f + \mathcal{R})| \leq g_1(||\omega_f||)$$

for $\varrho \in (0, \varrho_1)$, for some $\varrho_1 > 0$ and for all $t \geq 0$.
Assumption 3 is satisfied when a is globally Lipschitz in ξ. It is also satisfied if

$$|a| \leq g_2(|\xi_1|) + b_1|\xi_2|^{\rho-1} + b_2|\xi_3|^{\frac{\rho-1}{2}} + \ldots + b_{\rho-1}|\xi_\rho|$$

where g_2 is locally Lipschitz in ξ_1 and b_i for $i = 1, \ldots, \rho-1$ are positive constants.

C. Funnel Control by Synthesizing Virtual Output

Funnel control was used to evolve the tracking error e inside the performance funnel for known relative degree systems in [13], [17]. Here we present an abridged version of the main idea.

1) State Feedback Funnel Controller Design: We synthesize the virtual output from the system states as

$$s = \omega_1 + k_2\omega_2 + \ldots + k_\rho\omega_\rho \tag{4}$$

where k_2 to k_ρ are positive constants to be chosen. The relative degree of the system (3) with respect to s is one. By using feedback control we introduce a two-time scale structure to make $\omega_1, \omega_2, \ldots, \omega_{\rho-1}$ fast while making s slow. By choosing u as

$$u = \frac{1}{\varrho^\rho k_\rho b(\xi)}[-\omega_2 - k_2\omega_3 - \ldots - k_{\rho-1}\omega_\rho + \varrho v_f] \tag{5}$$

where v_f is an auxiliary input. The singularly perturbed system is given by

$$\varrho\dot{\omega} = F\omega + Hs \tag{6a}$$
$$\dot{s} = v_f + \varrho^{\rho-1}k_\rho\{a(t, \xi) - r^{(\rho)}(t)\} \tag{6b}$$

$$F = \begin{bmatrix} 0 & 1 & \ldots & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & & & & \vdots \\ 0 & \ldots & \ldots & 0 & 1 \\ -\frac{1}{k_\rho} & \ldots & \ldots & -\frac{k_{\rho-2}}{k_\rho} & -\frac{k_{\rho-1}}{k_\rho} \end{bmatrix}, H = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ \frac{1}{k_\rho} \end{bmatrix}$$

where $\omega = \text{col}(\omega_1, \ldots, \omega_{\rho-1})$, $F \in R^{\rho-1\times\rho-1}$, $H \in R^{\rho-1\times 1}$. The gains $k_2, k_3, \ldots, k_\rho$ are chosen such that the matrix F is Hurwitz, which is always possible. In (6), ω is the fast variable and s is the slow variable.

Theorem 1: Consider the closed-loop system (6) obtained using the state feedback controller (5). Let k_2 to k_ρ be chosen

such that the matrix F is Hurwitz. Suppose Assumptions 1-3 are satisfied. Let $\varphi(t) \in \bar{\Phi}$ and suppose the initial states satisfy $(\omega(0), s(0)) \in \Lambda_0$, where Λ_0 is a compact set. Then the funnel controller,

$$v_f = -\frac{1}{\psi(t) - |s|}s \tag{7}$$

yields a closed-loop system such that the solution is bounded for all $t \geq 0$ and there exists $\varrho^* > 0$ such that for each $\varrho \in (0, \varrho^*]$, there exists $\kappa_s^* > 0$ such that

$$|e(t)| \leq \psi(t) - \kappa_s^*, \qquad \forall\ t \geq 0 \tag{8}$$

Proof: See [13]

2) Output Feedback Funnel Controller Design: The virtual output can be constructed by only measuring e using a high-gain observer to construct the estimates $\hat{\mathcal{E}} = \text{col}(\hat{e}_1, \hat{e}_2, \ldots, \hat{e}_\rho)$:

$$\dot{\hat{e}}_i = \hat{e}_{i+1} + \frac{\gamma_i}{\varsigma^i}(e - \hat{e}_1), \quad 1 \leq i \leq \rho - 1 \tag{9a}$$

$$\dot{\hat{e}}_\rho = a_0(\hat{\xi}) + b(\hat{\xi})\hat{u}_s + \frac{\gamma_\rho}{\varsigma^\rho}(e - \hat{e}_1) \tag{9b}$$

where ς is a small positive constant and $\gamma_1, \gamma_2, \ldots, \gamma_\rho$ are chosen such that the polynomial,

$$\tilde{g}^\rho + \gamma_1\tilde{g}^{\rho-1} + \ldots + \gamma_{\rho-1}\tilde{g} + \gamma_\rho \tag{10}$$

is Hurwitz, $a_0(\xi)$ serves as a nominal model for $a(t, \xi)$ and $\hat{\xi}_i = \hat{e}_i + r^{(i-1)}$. From the estimates $\hat{e}_1$ to $\hat{e}_\rho$ we have $\hat{\omega}_1 = \hat{e}_1$, $\hat{\omega}_2 = \varrho\hat{e}_2$, …, $\hat{\omega}_\rho = \varrho^{\rho-1}\hat{e}_\rho$. We saturate the estimates $\hat{\omega}_1, \ldots, \hat{\omega}_\rho$ outside the compact set Λ_f to overcome the peaking phenomenon of the observer [18]. The estimates are saturated as $\hat{\omega}_{is} = \bar{M}_i \text{sat}\left(\frac{\hat{\omega}_i}{\bar{M}_i}\right)$ where sat is the saturation function [18]. The estimate of the virtual output is saturated as,

$$\hat{s}_s = \hat{\omega}_{1s} + k_2\hat{\omega}_{2s} + k_3\hat{\omega}_{3s} + \ldots + k_\rho\hat{\omega}_{\rho s} \tag{11}$$

The funnel controller gain is given by $\hat{k}(t) = \dfrac{1}{\psi(t) - |\hat{s}_s|}$ and the funnel gain is saturated as $\hat{k}_s = \bar{M}_k \text{sat}\left(\dfrac{\hat{k}}{\bar{M}_k}\right)$.

See [13] on how to select the saturation levels $\bar{M}_1, \ldots, \bar{M}_\rho$ and $\bar{M}_k$. Using the estimates $(\hat{\omega}_1, \hat{\omega}_2, \ldots, \hat{\omega}_\rho)$, the output feedback control is given by,

$$\hat{u}_s = \frac{1}{\varrho^\rho k_\rho b(\hat{\xi})}[-\hat{\omega}_{2s} - \ldots - k_{\rho-1}\hat{\omega}_{\rho s} + \varrho\hat{v}_{fs}] \tag{12a}$$

$$\hat{v}_{fs} = -\hat{k}_s\hat{s}_s \tag{12b}$$

Theorem 2: Consider the plant (3), the observer (9), and the output feedback controller (12). Suppose all the assumptions of Theorem 1 are satisfied, γ_1 to γ_ρ are chosen such that the polynomial (10) is Hurwitz and $\hat{\mathcal{E}}(0) \in Y$ where Y is a compact subset of R^ρ. Then there exists $\varrho^{**} > 0$ and for each $\varrho \in (0, \varrho^{**})$, there is $\varsigma^* = \varsigma^*(\varrho) > 0$, such that for each $\varrho \in (0, \varrho^{**})$ and $\varsigma \in (0, \varsigma^*(\varrho))$ there exists $\kappa_o^* > 0$ such that

$$|e(t)| \leq \psi(t) - \kappa_o^*, \qquad \forall\ t \geq 0 \tag{13}$$

and the states $(\omega(t), s(t), \hat{\mathcal{E}})$ of the closed loop system are bounded for all $t \geq 0$.

Proof: See [13]

III. Differential Privacy Problem Setup

A. Adjacency Relation

We consider funnel boundary trajectories of the form $\psi(t) = (\psi(t_1), \psi(t_2), \ldots)$, where $\psi(t) \in \mathbb{R}$ and $0 < \psi(t) < \infty$ for all $t \geq 0$. We denote the set of all such sequences by $\psi \in \ell_1$. We will define our adjacency relation over ℓ_1.

Definition 1: (Adjacency for funnel boundary): We define the dataset Ψ and Ψ' where each element in the set is the tuple $\{-\psi(t_i), \psi(t_i)\}_{i=1}^n$ and $\{-\psi'(t_i), \psi'(t_i)\}_{i=1}^n$. The two trajectories $\psi, \psi' \in \ell_1$ are adjacent if

$$|\psi(t_i) - \psi'(t_i)| \leq \delta\psi, \quad \forall\ 1 \leq i \leq n \tag{14}$$

where $\delta\psi > 0$ is the adjacency parameter. The value of n is chosen based on some finite time $T_f > 0$ such that for all $t_i \in [0, T_f]$ the user requires differential privacy. We will write $\text{Adj}_{\delta\psi}(\psi, \psi^{'}) = 1$ if ψ and $\psi^{'}$ are adjacent which implies (14) holds, and $\text{Adj}_{\delta\psi}(\psi, \psi^{'}) = 0$, otherwise. The constant $\delta\psi$ is chosen based on the privacy requirement as the adjacency relation implies that a particular funnel boundary can be made approximately indistinguishable within distance $\delta\psi$ from all other funnel boundaries.

Definition 2: We define a query as

$$Q(d) = \psi \tag{15}$$

where $d \in \Psi$. The query implies that each time the query is called one funnel boundary is selected from the database.

Definition 3: (Query Sensitivity): The sensitivity of the query Q is given by

$$\Delta Q := \sup_{d, d' \,|\, \text{Adj}_{\delta\psi}(d, d') = 1} |Q(d) - Q(d^{'})|$$

The sensitivity captures the largest magnitude by which the output of the query can change across two adjacent databases.

Next, we define differential privacy for dynamic systems (see [4] for a formal construction).

Definition 4: (Differential privacy for funnel boundary/tracking error): Let $\epsilon > 0$ and $\delta \in (0, 1/2)$ be given. A mechanism $\mathcal{M}$ is (ϵ, δ)-differentially private if, for all adjacent $\psi, \psi' \in \ell_1$ or $e, e' \in \ell_1$, we have:

$$\mathbb{P}\left[\mathcal{M}\left(\psi\right) \in S\right] \leq \exp^{\epsilon}\mathbb{P}\left[\mathcal{M}\left(\psi'\right) \in S\right] + \delta \text{ for all } S \in \mathbb{R}.$$

$$\mathbb{P}\left[\mathcal{M}\left(e\right) \in S\right] \leq \exp^{\epsilon}\mathbb{P}\left[\mathcal{M}\left(e'\right) \in S\right] + \delta \text{ for all } S \in \mathbb{R}.$$

B. Univariate Bounded Gaussian Noise

A mechanism will add noise to the funnel boundary to make the funnel boundary differentially private. However, adding arbitrary noise to the funnel boundary can violate the assumptions of the funnel boundary. For example, if $\psi(t) + v(t) < 0$ for any $t \geq 0$, the funnel controller will fail to work. Therefore, in this section, we generate a bounded Gaussian noise. The bounded domain is given by $\mathcal{D} = [\alpha, \beta] \subset \mathbb{R}$,

where $\alpha = -c_1\psi_{\min}$, $\psi_{\min} = \inf_{t\geq 0} \psi(t)$, $0 < c_1 < 1$, and $\beta = -\alpha$ is chosen to make the probability density function symmetric. In general, β can be chosen as $\beta = c_2\psi_{\max}$, where $c_2 \geq 1$ and $\psi_{\max} = \sup_{t\geq 0} \psi(t)$.

Definition 5: (Univariate bounded Gaussian noise): Given $\mathcal{D} = [\alpha, \beta]$ where $(\alpha < \beta)$, both finite is a constrained domain. Then the probability density function of the univariate Gaussian noise is given by

$$p_B(v) = \begin{cases} \frac{1}{\sigma}\frac{\phi\left(\frac{v}{\sigma}\right)}{\Phi(\beta') - \Phi(\alpha')} & \text{if } v \in \mathcal{D}, \\ 0 & \text{otherwise,} \end{cases} \tag{16}$$

where the original Gaussian distribution is zero mean and σ variance, $\beta' = \frac{\beta}{\sigma}$, $\alpha' = \frac{\alpha}{\sigma}$ and

$$\phi(v) = \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{1}{2}v^2\right), \ \Phi(v) = \frac{1}{2}\left(1 + \text{erf}(v/\sqrt{2})\right)$$

We cannot sample noise from the distribution (16) and add it to the funnel boundary as it will make the performance funnel discontinuous. Therefore, we require the noise to be filtered before adding it to the funnel boundary which is discussed in the next section.

IV. Ornstein-Uhlenbeck Type Process

The bounded Gaussian noise is passed through a linear filter to produce a continuous noise which is added to the funnel boundary. We model this operation as an Ornstein–Uhlenbeck (OU) type process which is a stationary process [19]. It has the property that over time, the process tends to drift towards its mean function: such a process is called mean-reverting. We define the system as

$$\theta\frac{dy}{dt} = -y(t) + w(t) \tag{17a}$$

$$\frac{dw}{dt} = -\vartheta w(t) + v(t) \tag{17b}$$

where $0 < \theta << 1$, $\vartheta > 0$. The system (17) is represented by a singularly perturbed system where y is the fast variable and w is the slow variable.

A. Boundedness & Solutions of the Process

The solution of the decoupled equation (17b) is given by

$$w(t) = w_0 e^{-\vartheta t} + \int_0^t e^{-\vartheta(t-s)} v(s) ds \tag{18}$$

We choose the initial condition of the process as $w_0 = 0$ for simplicity. The solution can then be defined as

$$w(t) = \int_0^t e^{-\vartheta(t-s)} v(s) ds$$

The solution is an integral of a deterministic function with respect to a bounded Gaussian noise. From (16) we have $\alpha \leq v(t) \leq \beta$ which implies

$$\frac{\alpha}{\vartheta}(1 - e^{-\vartheta t}) \leq w(t) \leq \frac{\beta}{\vartheta}(1 - e^{-\vartheta t}), \ \forall\ t \geq 0 \tag{19}$$

Theorem 3: Let OU type process be defined by (17). Let $v(t)$ be the noise generated from the truncated Gaussian probability distribution (16). Then, there exists a time $T(\theta)$ such that for all $t \geq T(\theta)$ where $\lim_{\theta\to 0} T(\theta) = 0$

$$y(t) = w(t) + O(\theta), \quad t \geq T(\theta) \tag{20}$$

Proof: The quasi-steady-state of (17a) is obtained by setting $\theta = 0$, from which we have $y(t) = w(t)$. Next we define the variable $z(t) = y(t) - w(t)$ and by taking its derivative we have

$$\theta\dot{z} = -z - \theta[-\vartheta w(t) + v(t)] \tag{21}$$

By defining a Lyapunov function $V_z = (1/2)z^2$, and taking its derivative along (17), we have

$$\theta\dot{V}_z \leq -z^2 + \theta\bar{\Delta}|z|$$

where $|-\vartheta w(t) + v(t)| \leq \bar{\Delta}$, where the right-hand side is bounded since (17b) is Bounded-Input-Bounded-Output (BIBO) stable system. From which we have

$$\dot{V}_z \leq -\frac{z^2}{2\theta}, \quad \forall\ |z| \geq 2\theta\bar{\Delta}$$

It can be shown [18], that there exists a time $T(\theta)$, where $\lim_{\theta\to 0} T(\theta) = 0$ such that

$$|z(t)| \leq 2\theta\bar{\Delta}, \quad \forall\ t \geq T(\theta)$$

From which we can conclude that (20) follows.

B. Probability Density Function of the OU type Process

We first discuss the probability density functions of $w(t)$, and $y(t)$ when the input noise is sampled from a Gaussian distribution. The variables $w(t)$, and $y(t)$ will have steady-state probability density functions as the process (17b) is stationary [19] since $\vartheta > 0$. Next we define the following lemma.

Lemma 1: Let v_G be the input to the OU type process (17), where v_G is sampled from a Gaussian distribution $v_G \sim \mathcal{N}(0, \sigma_G^2)$ with probability density function $p_G(v_G) = \frac{1}{\sigma_G}\phi\left(\frac{v_G}{\sigma_G}\right)$. Then, the steady-state probability density function of y up to an order of $O(\theta)$ for all $t \geq \bar{T}_{ss} > 0$ is given by

$$p_{ss}(y) = \frac{1}{\sigma_G'}\phi\left(\frac{v}{\sigma_G'}\right) \tag{22}$$

where p_{ss} is the steady-state probability density function of y, $\sigma_G' = \sigma_G/(\sqrt{2\vartheta})$ and the mechanism $\mathcal{M} = Q(d) + y(t)$, where $d \in \Psi$, makes the funnel boundary (ϵ, δ)-differentially private with $\sigma_G' \geq \Delta Q \delta\psi\kappa(\delta_G, \epsilon_G)$, where $\kappa(\delta_G, \epsilon_G) = \frac{1}{2\epsilon_G}\left(K_{\delta_G} + \sqrt{K_{\delta_G}^2 + 2\epsilon_G}\right)$, with $K_\delta := \mathcal{Q}^{-1}(\delta_G)$, $\mathcal{Q}$ representing the Gaussian tail integral.

Proof: When v_G is sampled from a Gaussian distribution we can rewrite (17b) as

$$dw = \vartheta(\mu - w(t))dt + \sigma_G' dq$$

where q is a Wiener process [19]. We can use Ito's integral [19] to show that conditional expectation and variance when $w(0) = w_0 = 0$ are

$$E[w(t)] = E\left[\int_0^t e^{-\vartheta(t-s)} dq(s)\right] = \mu(1 - e^{-\vartheta t}) = 0$$

since $\mu = 0$, and

$$\text{Var}[w(t)] = E\left[\left(\sigma_G' \int_0^t e^{-\vartheta(t-s)} dq(s)\right)^2\right] = {\sigma_G'}^2(1-e^{-2\vartheta t}).$$

It can be shown that the probability distribution using the Fokker-Planck representation [19] is given by

$$p(w,t) = \frac{1}{\sqrt{2\pi(1-e^{-2\vartheta t})}\sigma_G'} \exp\left[\frac{y^2}{{\sigma_G'}^2(1-e^{-2\vartheta t})}\right]$$

Then, for all $t \geq \bar{T}_{ss} > 0$, the steady-state probability distribution up to an error of $O(\theta)$ is given by (22) using Theorem 3. Using the steady-state probability (22), adjacency definition (14) and query sensitivity (16), it can be shown [5] that the mechanism $\mathcal{M} = Q(d) + y(t)$, where $d \in \Psi$, makes the funnel boundary (ϵ, δ)-differentially private with $\sigma_G' \geq \Delta Q \delta\psi \kappa(\delta_G, \epsilon_G)$, where $\kappa(\delta_G, \epsilon_G) = \frac{1}{2\epsilon_G}\left(K_{\delta_G} + \sqrt{K_{\delta_G}^2 + 2\epsilon_G}\right)$.

When the process (17b) is driven by an input noise sampled from a truncated Gaussian probability distribution, the output $y(t)$ will also have a steady-state probability density function. This follows since the process (17b) is stationary. In this case, we denote the steady-state probability density function of y as $p_{OU}(y)$ for all $t \geq T_{ss} > 0$.

Remark 1: For our problem, we cannot use Gaussian noise as the input to the OU type process as it might violate the funnel controller assumptions. Since we use truncated Gaussian noise as an input to the OU type process the probability density function $p_{OU}(y)$ is not infinite support compared to $p_{ss}(y)$. But we conjecture that the shape of $p_{OU}(y)$ will be similar to the shape of $p_{ss}(y)$.

Theorem 4: Let OU type process be defined by (17). Let $v(t)$ be the noise generated from the truncated Gaussian probability distribution (16). Then for all $t \geq T_{ss} > 0$,

- *$p_{OU}(y)$ is continuous*
- *$p_{OU}(y)$ is bounded*
- *$p_{OU}(y \geq \beta/\vartheta) = p_{OU}(y \leq \alpha/\vartheta) = 0$*

Proof: We perform our analysis when the probability density function $p_{OU}(y)$ reaches steady-state for $t \geq T_{ss} > 0$. The probability density function $p_{OU}(y)$ is continuous since the random variable y is continuous as it is the output of the OU type process (17).

The boundedness of the probability density function comes from the boundedness of the noise $v(t)$ which limits the range of $w(t)$ to (19). Finally, the upper and lower bounds of $w(t)$ are reached when $v(t) = \beta, \forall\ t \geq 0$ or $v(t) = \alpha, \forall\ t \geq 0$. The probability of sampling the bounds are as follows

$$P(w = \alpha) = \int_\alpha^\alpha p_B(v)dv = \int_0^0 p_B(v)dv = 0$$

$$P(w = \beta) = \int_\beta^\beta p_B(v)dv = \int_0^0 p_B(v)dv = 0$$

From which we can conclude that $p_{OU}(y = \beta/\vartheta) = p_{OU}(y = \alpha/\vartheta) = 0$. For $t \geq T_{ss} > 0$, the maximum and minimum value of $w(t)$ is β/ϑ and α/ϑ from which we can conclude that $p_{OU}(y \geq \beta/\vartheta) = p_{OU}(y \leq \alpha/\vartheta) = 0$.

V. Differential Privacy of Funnel Boundary and Tracking Error

A. Funnel Boundary Differential Privacy

Theorem 5: Let $v(t)$ be the noise generated from the probability density function (16) which is filtered through the OU type process (17) with the output as $y(t)$ and the steady-state probability density function as $p_{OU}(y)$. Then, the mechanism $\mathcal{M} = Q(d) + y(t)$, where $d \in \Psi$, makes the funnel boundary (ϵ, δ)-differentially private with respect to $\text{Adj}_{\delta\psi}$ in ψ where

$$\epsilon \leq \epsilon_U, \quad \delta \leq \delta_U \tag{23}$$

for all $t \in [\bar{T}, T_f]$ where ϵ_U, and δ_U are the upper bounds of ϵ and δ, $\bar{T} = \max\{T(\theta), T_{ss}\}$ and $T_f > \bar{T} > 0$.

Proof: We use the results in [20] to find the upper bounds of ϵ and δ. We perform our analysis when the probability density function of $w(t)$ is in steady-state and (20) holds. Therefore, our analysis is between the time period $t \in [\bar{T}, T_f]$ where $\bar{T} = \max\{T(\theta), T_{ss}\}$ and $T_f > \bar{T} > 0$. For $t_i \in [\bar{T}, T_f]$, we define the dataset $\bar{\Psi}$ and $\bar{\Psi}'$ where each element in the set is the tuple $\{-\psi(t_i), \psi(t_i)\}_{i=n_1}^{n_2}$ as $\{-\psi'(t_i), \psi'(t_i)\}_{i=n_1}^{n_2}$ where n_1 and n_2 can be determined from $\bar{T}$, and T_f. During this time period we have

$$|\psi(t_i) - \psi'(t_i)| \leq \delta\psi', \quad \forall\ n_1 \leq i \leq n_2 \tag{24}$$

where $\delta\psi' > 0$ is the adjacency parameter in this time period. The steady-state probability density function of $p_{OU}(y)$ is represented by Fig. 2. Following [20, Theorem 3.6], we define $\Theta_0 = [-M, M]$ and $\Theta_1 = (-\infty, -M] \cup [M, \infty)$ such that

$$\epsilon \leq \ln\left[\sup_{\delta\in[-\delta\psi',\delta\psi'],y\in\Theta_0} \frac{p_{OU}(y-\delta)}{p_{OU}(y)}\right] \tag{25a}$$

$$\delta \leq 2\oint_{\Theta_1} p_{OU}(y)dy = S1 + S2 \tag{25b}$$

Let $c_b = \sup_{\delta\in[-\delta\psi',\delta\psi'],y\in\Theta_0} \frac{p_{OU}(y-\delta)}{p_{OU}(y)}$. The supremum can be written as

$$\frac{\max_{\delta\in[-\delta\psi',\delta\psi'],y\in\Theta_0} p_{OU}(y-\delta)}{\min_{y\in\Theta_0} p_{OU}(y)}$$

The above holds because the probability density function of $p_{OU}(y)$ is continuous and defined in a closed and compact interval. We consider two cases:

Case I: $\delta\psi' < M$: In this case c_b will depend on $\delta\psi'$ and M as we have $c_b = \frac{p_{OU}(M - \delta\psi')}{p_{OU}(M)}$

Case II: $\delta\psi' \geq M$: In this case c_b will depend on M as we

have $c_b = \dfrac{p_{OU}(0)}{p_{OU}(M)}$

Taking $\epsilon_U = \ln(c_b)$, we arrive at the inequality.

From Fig. 2, the term δ_U is bounded since the probability density function $p_{OU}(y)$ is bounded and

$$2\oint_{\Theta_1} p_{OU}(y)dy = S1 + S2$$

Remark 2: The upper bounds ϵ_U, and δ_U depend on the choice of M, the noise bounds α, β, and the OU process parameter ϑ. These values can be tuned by the user to based on the requirement of differential privacy for the problem.

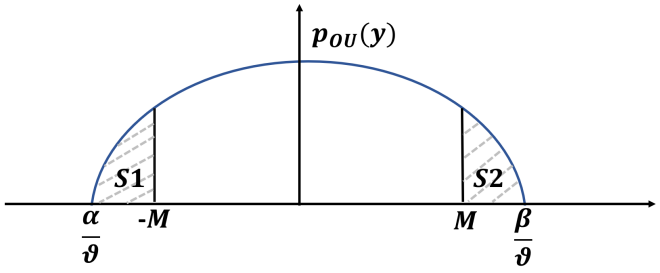

Fig. 2. Probability density function of OU type process

B. Tracking Error Differential Privacy for State and Output feedback Funnel Controller

Theorem 6: Let Theorem 1 and 5 hold and the state feedback funnel controller be defined by (5) and (7). Let the mechanism $\mathcal{M} : Q(d) + y$ where y is generated from the probability distribution (16) and the OU type process (17) makes the funnel boundary (ϵ, δ) differentially private. Then, the tracking error e obtained using the state feedback funnel controller is (ϵ, δ) differentially private for all $t \in [\bar{T}, T_f]$ where time $T_f > \bar{T} > 0$.

Proof: We define the datasets E and E' as the set $\{e(t_i)\}_{i=1}^n$, and $\{e'(t_i)\}_{i=1}^n$ where e and e' correspond to the tracking error of the system (2) obtained using the state feedback funnel controller with funnel boundary $\psi(t_i)$ and $\psi'(t_i)$ from Definition 1. From (8), we have

$$-\psi(t_i) < e(t_i) < \psi(t_i), \quad \text{and} \quad -\psi'(t_i) < e'(t_i) < \psi'(t_i) \tag{26}$$

for $i = 1, \ldots, n$. From the above inequalities, we can conclude that the datasets E and E' are in the interior of the datasets Ψ and Ψ'. Using (26)

$$|e(t_i) - e'(t_i)| < |\psi(t_i) - \psi'(t_i)|, \quad 1 \le i \le n$$

Using (14) we have

$$|e(t_i) - e'(t_i)| < \delta\psi, \quad 1 \le i \le n \tag{27}$$

From Theorem 5, the funnel boundary is (ϵ, δ) differentially private for all $t \in [\bar{T}, T_f]$. For $t_i \in [\bar{T}, T_f]$, we define datasets $\bar{E}$, $\bar{E}'$ as the set $\{e(t_i)\}_{i=n_1}^{n_2}$, and $\{e'(t_i)\}_{i=n_1}^{n_2}$ where n_1 and n_2 can be determined from $\bar{T}$, and T_f. Using the above inequalities and (24) we have

$$|e(t_i) - e'(t_i)| < \delta\psi', \quad n_1 \le i \le n_2 \tag{28}$$

Moreover,

$$-\psi(t_i) < e(t_i) < \psi(t_i), \quad \text{and} \quad -\psi'(t_i) < e'(t_i) < \psi'(t_i) \tag{29}$$

for $i = n_1, \ldots, n_2$. Therefore, we can conclude that the datasets $\bar{E}$, and $\bar{E}'$ are in the interior of the dataset $\bar{\Psi}$ and $\bar{\Psi}'$ for all $t \in [\bar{T}, T_f]$ and satisfies the adjacency relationship (24). Therefore, the following holds [4]

$$\mathbb{P}\left[\mathcal{M}\left(e\right) \in S\right] \le \exp^{\epsilon} \mathbb{P}\left[\mathcal{M}\left(e'\right) \in S\right] + \delta \text{ for all } S \in \mathbb{R}.$$
$$\mathbb{P}\left[\mathcal{M}\left(e'\right) \in S\right] \le \exp^{\epsilon} \mathbb{P}\left[\mathcal{M}\left(e\right) \in S\right] + \delta \text{ for all } S \in \mathbb{R}.$$

Using the above we conclude differential privacy of the tracking error.

Next we prove the tracking error differential privacy for the output feedback funnel controller.

Theorem 7: Let Theorem 2 and 5 hold and the state feedback funnel controller be defined by (12) and the mechanism $\mathcal{M} : Q(d) + y(t)$ where y is generated from the probability distribution (16) and the OU type process (17) makes the funnel boundary (ϵ, δ). Then, the tracking error is (ϵ, δ) differentially private for all $t \in [\bar{T}, T_f]$ for some finite time $T_f > \bar{T} > 0$.

Proof: The proof can be done by repeating the steps of Theorem 6 and using the relation (13).

VI. Simulation Results

We consider a second-order nonlinear system

$$\dot{\xi}_1 = \xi_2, \quad \dot{\xi}_2 = -\xi_1 + \xi_1^3 + u \tag{30}$$

The reference signal is generated from the output of the following exosystem [21]

$$\dot{\xi}_{r1} = \xi_{r1}, \quad \dot{\xi}_{r2} = 2(1 - \xi_{r1}^2)\xi_{r2} - \xi_{r1} \tag{31}$$

where $r(t) = \xi_{r1}$. The performance funnel is chosen as

$$\psi(t) = (2\pi - \psi_{ss})e^{-t/2} + \psi_{ss} + y(t)$$

where ψ_{ss} is the steady-state bound and $y(t)$ is the output of the Ornstein Uhlenbeck process. We transform the system into the error coordinates and choose the virtual output as $s = \omega_1 + k_2\omega_2$ where $\omega_1 = \xi_1 - r$, $\omega_2 = \varrho(\xi_2 - \dot{r})$ and $e = \omega_1$. The output feedback funnel controller is given by

$$u = \frac{1}{\varrho^2 k_2}\left[\frac{1}{k_2}\left(\hat{s}_s - \hat{\omega}_{1s}\right) + \varrho\hat{v}_{fs}\right], \hat{k}(t) = \frac{1}{\psi(t) - |\hat{s}_s(t)|} \tag{32a}$$

$$\hat{k}_s(t) = \bar{M}_k \text{sat}\left(\frac{\hat{k}}{\bar{M}_k}\right), \hat{v}_{fs} = -\hat{k}_s(t)\hat{s}_s(t) \tag{32b}$$

where $M_k = 5$ and the estimates are given by the high-gain observer

$$\dot{\hat{e}}_1 = \hat{e}_2 + \frac{\gamma_1}{\varsigma}(e - \hat{e}_1), \quad \dot{\hat{e}}_2 = \frac{\gamma_2}{\varsigma^2}(e - \hat{e}_1) \tag{33}$$

The estimates $\hat{\omega}_1 = \hat{e}_1$ and $\hat{\omega}_2 = \varrho\hat{e}_2$ are saturated with the saturation levels ± 1 and ± 3. The saturation levels are chosen from simulations to see the maximal values that the state trajectories would take when using the state feedback

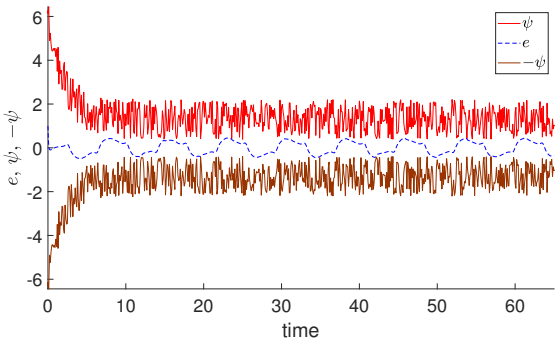

Fig. 3. Tracking error evolution inside performance funnel

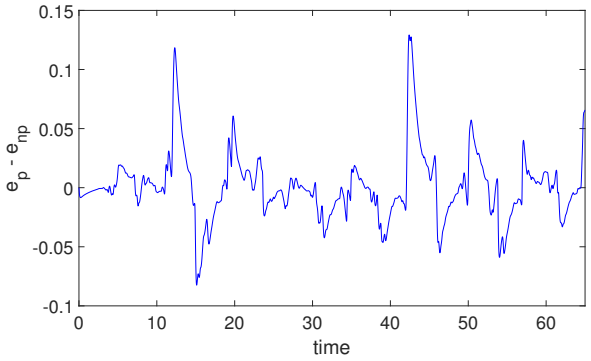

Fig. 4. Difference in tracking error in the presence privacy signal

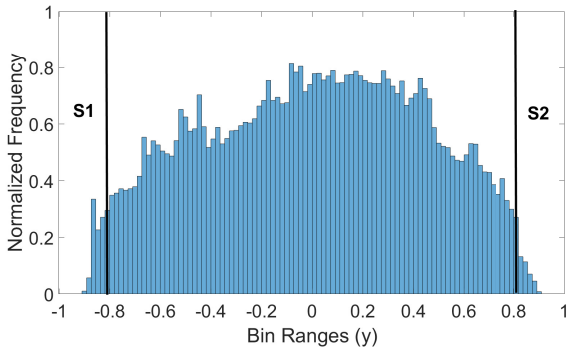

Fig. 5. Histogram of y with area divisions for ϵ, δ calculation

controller. The simulation is carried out with $\xi_1(0) = 2, \xi_2(0) = 0$, $\xi_{r1}(0) = 1, \xi_{r2}(0) = 1$, $k_2 = 7.5$, $\varrho = 0.01$, $\varsigma = 0.001$, $\gamma_1 = 2$, $\gamma_2 = 1$, $\psi_{ss} = 1.3$, $\alpha = -0.9$, $\beta = 0.9$, $\delta\psi = 0.5$, $\mu = 0$, $\sigma = 1$.

Fig. 3 shows the evolution of e within the performance funnel under the output feedback controller (32). Fig. 4 shows the difference between the tracking errors in the presence and absence of privacy signals. Fig. 5 shows the histogram of the output of the OU type process y. In the figure, for the choice of $M = 0.8$, the areas $S1$, $S2$ are shown for the calculation of ϵ, and δ which is calculated as $\epsilon \leq 1.0001, \quad \text{and} \quad \delta \leq 0.0397$.

VII. Conclusion

In this paper, we presented a new framework for introducing differential privacy in the tracking error of nonlinear systems. The initial funnel control problem is formulated for nonlinear systems with arbitrary relative degrees using high-gain observers using the idea of the virtual output. We then make the performance funnel differentially private by adding a continuous bounded noise which is the output of an Ornstein-Uhlenbeck type process. We provide bounds of ϵ and δ using the results of [20] and show that the tracking error is differentially private using the differential privacy of the performance funnel.

References

[1] M. U. Hassan, M. H. Rehmani, and J. Chen, "Differential privacy techniques for cyber physical systems: a survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 746–789, 2019.

[2] S. Han and G. J. Pappas, "Privacy in control and dynamical systems," *Annual Review of Control, Robotics, and Autonomous Systems*, vol. 1, pp. 309–332, 2018.

[3] C. Dwork, A. Roth *et al.*, "The algorithmic foundations of differential privacy," *Foundations and Trends® in Theoretical Computer Science*, vol. 9, no. 3–4, pp. 211–407, 2014.

[4] J. Le Ny and G. J. Pappas, "Differentially private filtering," *IEEE Transactions on Automatic Control*, vol. 59, no. 2, pp. 341–354, 2013.

[5] C. Dwork, "Differential privacy: A survey of results," in *International conference on theory and applications of models of computation*. Springer, 2008, pp. 1–19.

[6] K. Yazdani, A. Jones, K. Leahy, and M. Hale, "Differentially private lq control," *IEEE Transactions on Automatic Control*, vol. 68, no. 2, pp. 1061–1068, 2022.

[7] C. Hawkins and M. Hale, "Differentially private formation control: Privacy and network co-design," *arXiv preprint arXiv:2205.13406*, 2022.

[8] Y. Mo and R. M. Murray, "Privacy preserving average consensus," *IEEE Transactions on Automatic Control*, vol. 62, no. 2, pp. 753–765, 2016.

[9] Z. Huang, S. Mitra, and G. Dullerud, "Differentially private iterative synchronous consensus," in *Proceedings of the 2012 ACM workshop on Privacy in the electronic society*, 2012, pp. 81–90.

[10] Y. Kawano and M. Cao, "Differential privacy and qualitative privacy analysis for nonlinear dynamical systems," *IFAC-PapersOnLine*, vol. 51, no. 23, pp. 52–57, 2018.

[11] Y. Kawano and M. Cao, "Design of privacy-preserving dynamic controllers," *IEEE Transactions on Automatic Control*, vol. 65, no. 9, pp. 3863–3878, 2020.

[12] A. Ilchmann, E. P. Ryan, and C. J. Sangwin, "Tracking with prescribed transient behaviour," *ESAIM: Control, Optimisation and Calculus of Variations*, vol. 7, pp. 471–493, 2002.

[13] D. Chowdhury and H. K. Khalil, "Funnel control for nonlinear systems with arbitrary relative degree using high-gain observers," *Automatica*, vol. 105, pp. 107–116, 2019.

[14] D. Chowdhury, R. Goyal, and S. Rane, "Differential privacy in nonlinear dynamical systems with tracking performance guarantees," *arXiv preprint cs.SY, arXiv:2403.08181*, 2024.

[15] H. K. Khalil, *Nonlinear Systems*. Upper Saddle River, NJ: Prentice hall, 2002, vol. 3.

[16] A. Isidori, *Nonlinear control systems: an introduction*. Springer, 1985.

[17] D. Chowdhury and H. K. Khalil, "Funnel control of higher relative degree systems," in *2017 American Control Conference (ACC)*. IEEE, 2017, pp. 598–603.

[18] H. K. Khalil, *High-gain observers in nonlinear feedback control*. SIAM, 2017.

[19] H. Risken and J. Eberly, "The fokker-planck equation, methods of solution and applications," *Journal of the Optical Society of America B Optical Physics*, vol. 2, no. 3, p. 508, 1985.

[20] J. He, L. Cai, and X. Guan, "Differential private noise adding mechanism and its application on consensus algorithm," *IEEE Transactions on Signal Processing*, vol. 68, pp. 4069–4082, 2020.

[21] D. Chowdhury and H. K. Khalil, "Practical synchronization in networks of nonlinear heterogeneous agents with application to power systems," *IEEE Transactions on Automatic Control*, vol. 66, no. 1, pp. 184–198, 2020.