

Differentially Private Games via Payoff Perturbation

Yijun Chen, Guodong Shi

Abstract—In this paper, we study network games where players are involved in information aggregation processes subject to the differential privacy requirement for players’ payoff functions. We propose a Laplace linear-quadratic functional perturbation (LLQFP) mechanism, which perturbs players’ payoff functions with linear-quadratic functions whose coefficients are produced from truncated Laplace distributions. For monotone games, we show that the LLQFP mechanism maintains the concavity property of the perturbed payoff functions, and produces a perturbed NE whose distance from the original NE is bounded and adjustable by Laplace parameter tuning. We focus on linear-quadratic games, which is a fundamental type of network games with players’ payoffs being linear-quadratic functions, and derive explicit conditions on how the LLQFP mechanism ensures differential privacy with a given privacy budget. Lastly, numerical examples are provided for the verification of the advantages of the LLQFP mechanism.

I. INTRODUCTION

Games on networks has gained increased traction in recent years. It has been applied in a variety of fields such as online E-commerce in social networks [1], route planning in transportation networks [2], and resource allocations in wireless communication networks [3]. There are typically three information aggregation processes in games for players to achieve network-level goals: the distributed Nash equilibrium (NE) seeking [4]–[6], best-response dynamics [7]–[9], and no-regret learning [10]–[13].

What these frameworks have in common is that players need to share information with others in a dynamic process, such as their actions, payoff gradients, or payoffs, and then choose their actions for the next stage based on the information received and their own payoff functions. Clearly, players’ payoff functions are encoded in the shared information. However, players’ payoff functions are often sensitive and private [14]. As a result, players’ payoff functions are at risk of privacy leakage. Owing to differential privacy [15], [16], it is possible for players to share information and decide their actions over time to achieve the desired outcome while keeping their payoff functions from being compromised. Differentially private systems have been well studied in the sense that lots of privacy algorithms are designed for various tasks such as average consensus [17], [18], estimation and filtering [19], and convex optimization [20]–[22]. As for differentially private games, the works of [23], [24] have focused on privacy-preserving distributed Nash seeking strategy design for aggregated games.

Y. Chen and G. Shi are with the Australian Center for Field Robotics, The University of Sydney, NSW, Australia. (E-mail: yijun.chen@sydney.edu.au; guodong.shi@sydney.edu.au)

Problem of Interest In this paper, we consider a network game where players are interconnected through an interaction/communication network. Players are involved in information aggregation processes that requires them to share information to accomplish certain collective goal. The shared information that encodes the sensitive information of payoff functions is monitored by adversaries. As a result, we aim to protect the differential privacy of players’ payoff functions.

We are inspired by [22], [25]. We propose a Laplace linear-quadratic functional perturbation (LLQFP) mechanism, which perturbs players’ original payoff functions with linear-quadratic functional perturbation. The coefficients of those perturbation are generated by truncated Laplace distributions. The idea is to let players participate in certain information aggregation process using the perturbed payoff functions. If the LLQFP mechanism preserves differential privacy, then it also enforces differential privacy of information aggregation processes by the resilience to post-processing of differential privacy [16].

In the literature of differentially private information aggregation processes, a common approach is to add noises to players’ shared information [20], [21], [23], [24], [26]. For this approach, perturbation has to be designed in accordance with a diverse set of objectives during information aggregation processes. Moreover, perturbation has to be added at all time steps, and therefore the longer the operating time of information aggregation processes is, the more amount of perturbation is required to add. Functional perturbation is easier to implement since its design does not depend on specific tasks. In addition, functional perturbation only adds perturbation once to produce the perturbed payoff functions, regardless of the number of steps players participate in the following information aggregation processes.

Functional perturbation was also proposed by [22], [25]. They studied the distributed optimization problem subject to the requirement of differential privacy. Their work decomposed the objective functions into an infinite sequence of coefficients corresponding to the elements of a orthogonal basis in a separable Hilbert space, and added noises to the infinite coefficient sequence. Unfortunately, truncation is inevitable in practical implementations. Our work focuses on generalizing functional perturbation to the differentially private game setting. Instead of considering infinite expansion, we propose a mechanism that does not involve the decomposition of function space, but directly apply linear-quadratic functions as perturbation avoiding the truncation problem.

Contributions In this paper, we study network games

under the differential privacy requirement for players' payoff functions. We make the following contributions:

- We extend the notion of differential privacy to the network game setting, and propose a Laplace linear-quadratic functional perturbation (LLQFP) algorithm, which perturbs players' original payoff functions with linear-quadratic functional perturbation whose coefficients are generated according to truncated Laplace distributions.
- For monotone games, we show that the LLQFP algorithm maintains the concavity property of the perturbed payoff functions and yields a γ -accurate perturbed NE whose distance from the original NE is upper bounded by any prescribed constant γ .
- We investigate LQ games that players' payoff functions are parameterized. It serves as a tutorial example showing how Laplace parameters are selected to ensure certain differential privacy requirement.
- Experiments are conducted to verify the advantages of the LLQFP algorithm.

Organization The remainder of the paper is organized as follows. For privacy concerns about players' payoff functions in network games, we formalize our problem in Section II. In Section III, we propose the LLQFP algorithm. In Section IV, we consider monotone games, and show the advantages of the LLQFP algorithm. In Section V, we consider LQ games, and investigate Laplace parameter conditions that can guarantee certain different privacy requirement. Numerical examples are presented in Section VI. This paper ends with concluding remarks in Section VII.

II. PROBLEM FORMULATION

A. Network Games

Consider a network game with n players. The players are interconnected through an interaction/communication network. The interaction/communication network is associated with a graph $G(V, E)$, where $V := \{1, 2, \dots, n\}$ represents the nodes (players), and E defines the links (the interdependency among players). Each player $i \in V$ holds an action x_i from a compact convex action space $\mathcal{A}_i \subseteq \mathbb{R}$. The aggregated action profile of all players and the action profile excluding player i are denoted by $\mathbf{x} := [x_1, \dots, x_n]^\top$ and $\mathbf{x}_{-i} := [x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n]^\top$, respectively. Each player i then receives her payoffs determined by a payoff function, i.e., $u_i = f_i(x_i, \mathbf{x}_{-i})$, where the payoff function $f_i \in C^2(\mathcal{A})$ is twice continuously differentiable over $\mathcal{A} := \prod_{i \in V} \mathcal{A}_i$.

A common solution concept in game theory is called Nash equilibrium. It depicts an action profile under which no player may gain by simply modifying her action while others maintain theirs unaltered. We denote the NE by $\mathbf{x}^* := [x_1^*, \dots, x_n^*]^\top$.

Definition 1 (Nash equilibrium). *An action profile \mathbf{x}^* is said to be a pure-strategy NE of a game if $f_i(x_i^*, \mathbf{x}_{-i}^*) \geq f_i(x_i, \mathbf{x}_{-i}^*), \forall x_i \in \mathcal{A}_i, \forall i \in V$.*

Information Aggregation Processes In network games, there are many network-level information aggregation operations that require players to share dynamical states over a horizon $t \in \{0, 1, \dots, T\}$ to accomplish collective goals such as the distributed Nash seeking [4]–[6], best-response dynamics [7]–[9], and no-regret learning [10]–[13].

Example 1 (Distributed Nash seeking [4]–[6]) At time t , each player i holds a dynamical state $\mathbf{y}_i(t)$ that typically consists of her action and her estimate of other players' actions. Then, each player i shares $\mathbf{y}_i(t)$ with other players via certain interaction/communication network. Next, each player i updates her dynamical state for $\mathbf{y}_i(t+1)$ based on the received players' dynamical states and her own payoff function f_i . The network-level objective is for (perhaps part of) the sequence $[\mathbf{y}_1(t); \dots; \mathbf{y}_n(t)], t = 0, 1, \dots$ to converge to a NE.

Example 2 (Best-response Dynamics [7]–[9]) At time t , each player i holds a dynamical state $\mathbf{y}_i(t)$ that represents her action. Then, each $\mathbf{y}_i(t)$ is observed by or communicated with other players. Next, each player i updates her state $\mathbf{y}_i(t+1)$ as the action that maximizes her payoff function given other players' current actions. Best-response dynamics is a behavioral model depicting how players strategically make decisions in a sequential manner. Sometimes, best-response dynamics converge to a NE.

Example 3 (No-regret Learning [10]–[13]) At time t , each player i holds a dynamical state $\mathbf{y}_i(t)$ that typically consists of her action and her estimate of other players' payoff gradients. Then, each player i shares $\mathbf{y}_i(t)$ with other players via certain interaction/communication network. Next, each player i updates her dynamical state upon the received players' dynamical states and her own payoff function f_i . The network-level objective of no-regret learning is for the sequence $\mathbf{y}_i(t), t = 0, 1, \dots$ to minimize the regret of player i as the cumulative loss compared with a plain/single action in hindsight.

B. Problem Definition

Differentially Private Information Aggregation Processes

From the above network-level information aggregation operations, it is clear that the $\mathbf{y}_i(t), i = 1, \dots, n, t = 0, 1, \dots, T$ encode the information of payoff functions. Those states $\mathbf{y}_i(t)$ are shared by player i with other players. However, players' payoff functions are often private and contains sensitive information [14]. As a result, payoff functions face privacy risk in the information aggregation processes.

Differential privacy has been a standard tool to protect an individual's data privacy in a system where aggregate information is publicly published, but individual information is privately withheld [16]. Specifically, to protect the differential privacy of players' payoff functions, the mapping from $\mathbf{f} := [f_1; \dots; f_n]$ to $\mathbf{Y} := [\mathbf{y}_1(0); \dots; \mathbf{y}_1(T); \dots; \mathbf{y}_n(0); \dots; \mathbf{y}_n(T)]$ should satisfy the following differential privacy condition.

Definition 2 (\mathcal{W} -adjacency [25]). *Given any normed vector space $(\mathcal{W}, \|\cdot\|_{\mathcal{W}})$, \mathbf{f} and \mathbf{f}' are said to be \mathcal{W} -adjacent if there exists $i_0 \in V$ such that*

$$f_i = f'_i, \quad i \neq i_0; \quad (1a)$$

$$f_{i_0} - f'_{i_0} \in \mathcal{W}. \quad (1b)$$

The normed vector space \mathcal{W} is a design choice that we specify later according to the class of payoff functions.

Definition 3 ((ϵ, δ) -differential privacy). *The mapping \mathcal{M} is said to preserve (ϵ, δ) -differential privacy if for any subset $\mathcal{M} \subseteq \text{range}(\mathcal{M})$,*

$$\mathbb{P}(\mathcal{M}(\mathbf{f}) \in \mathcal{M}) \leq e^\epsilon \mathbb{P}(\mathcal{M}(\mathbf{f}') \in \mathcal{M}) + \delta, \quad (2)$$

holds for any two \mathcal{W} -adjacent payoff functions \mathbf{f} and \mathbf{f}' .

C. Functional Perturbation

We propose a functional perturbation mechanism from \mathbf{f} to $\hat{\mathbf{f}}$ where certain perturbation is added to produce $\hat{\mathbf{f}}$, and then players use $\hat{\mathbf{f}}$ to participate in information aggregation processes. As a result, the privacy of players' payoff functions \mathbf{f} may be protected in the sense that Definition 3 may be satisfied. If the mapping from \mathbf{f} to $\hat{\mathbf{f}}$ preserves differential privacy, then differential privacy of the mapping from \mathbf{f} to \mathbf{Y} is also enforced by the immune to post-processing [16].

There are a few practical challenges in designing such a mechanism:

- Differential privacy of the functional perturbation mechanism from \mathbf{f} to $\hat{\mathbf{f}}$ should be provable.
- The basic regularity property of the game should be maintained. In particular, if \mathbf{f} are concave, $\hat{\mathbf{f}}$ should be also concave.
- The distance between the NE of the original game and the NE of the perturbed game should be upper bounded and adjustable by parameter tuning.

In this paper, we aim to develop a distributed algorithm to realize this functional perturbation mechanism that can address the above challenges.

III. THE PROPOSED ALGORITHM

The truncated Laplace distribution truncated by $[-a, a]$ with mean zero and scale parameter λ , denoted $\mathcal{L}_{tr}(a, \lambda)$, has probability density function

$$p(x; a, \lambda) = \begin{cases} B e^{-|x|/\lambda}, & \text{for } x \in [-a, a], \\ 0, & \text{otherwise,} \end{cases} \quad (3)$$

where $B = \frac{1}{2\lambda(1-e^{-a/\lambda})}$.

Denote the neighbors of player i by the set $N_i \subset V$. We sort the indices of player i 's neighbors in ascending order in the set $O_i := \{i_1, i_2, \dots, i_{|N_i|}\}$. For example, if player j is player i 's k th neighbor, then $i_k = j$.

Algorithm 1 Laplace Linear-quadratic Functional Perturbation Algorithm

Input: Laplace parameters a, λ ; payoff functions f_1, \dots, f_n ;
Output: perturbed payoff functions $\hat{f}_1, \dots, \hat{f}_n$

- 1: Each player $i \in V$ independently generates a sequence random numbers $\omega_{i,k}$, $k = 1, \dots, |N_i| + 2$, according to $\mathcal{L}_{tr}(a, \lambda)$ in (3).
- 2: Each player $i \in V$ computes

$$q_{ij} = \begin{cases} \frac{\omega_{i, (|N_i|+1)} + \frac{a(|N_i|+1)}{2}}{2}, & j = i, \\ \omega_{i,k}, & j = i_k, \\ 0, & \text{otherwise,} \end{cases} \quad (4a)$$

$$\beta_i = \omega_{i, (|N_i|+2)}. \quad (4b)$$

- 3: Each player $i \in V$ employs a perturbed payoff function based on $\mathbf{q}_i := [q_{i1}, \dots, q_{in}]^T$ and β_i :

$$\hat{f}_i(x_i, \mathbf{x}_{-i}) = f_i(x_i, \mathbf{x}_{-i}) - x_i \mathbf{q}_i^T \mathbf{x} - \beta_i x_i. \quad (5)$$

- 4: **return** $\hat{f}_1, \dots, \hat{f}_n$
-

A. LLQFP Algorithm

We next propose a Laplace linear-quadratic functional perturbation Algorithm in Algorithm 1.

Algorithm 1 perturbs the original payoff functions with linear-quadratic functional perturbation whose coefficients are generated according to (3). Each player i first generates $|N_i| + 2$ independent truncated Laplace noises, and then strategically inserts noises to her payoff function in a linear-quadratic perturbation form. Each \mathbf{q}_i in the perturbed payoff function is not a simple stack of $|N_i| + 1$ truncated Laplace noises, but depends on the network structure and the truncated bound a .

The work of [22], [25] also presented an analysis on the the mechanism of functional perturbation via Laplace noises under the problem setting of differentially private distributed convex optimization. The differences between theirs and ours are as follows:

- Their work was based on the assumption that the objective functions are twice continuously differentiable functions with bounded gradients and Hessians. But we are going to assume that the underlying game is a monotone game, which is common in the game literature [27]. As a result, investigating whether the basic properties of the game is maintained and characterizing the accuracy of NE after applying Algorithm 1 are different from their framework.
- Their work decomposed \mathbf{f} into its coefficients by the infinite expansion, and perturbed this infinite sequence by adding noise to all of its elements. As a result, truncation is inevitable in practical implementations. But we only consider linear-quadratic functional perturbation where the noise coefficients are related with the underlying interaction graph of the game. In a sense,

the network structure of the game may be maintained.

B. Positivity Guarantee

We now present a property of the coefficients generated according to $\mathcal{L}_{tr}(a, \lambda)$, which is necessary for the Theorems later.

Denote $\mathbf{d}_i = [q_{i1}, \dots, q_{i(i-1)}, 2q_{ii}, q_{i(i+1)}, \dots, q_{in}]^\top$ and $\mathbf{D} = [\mathbf{d}_1 \ \mathbf{d}_2 \ \dots \ \mathbf{d}_n]$. Also denote $\boldsymbol{\beta} = [\beta_1, \dots, \beta_n]^\top$.

Lemma 1. \mathbf{D}^\top is a positive semidefinite matrix.

Proof. We focus on the magnitude of the diagonal element in each row, and the sum of the magnitudes of all non-diagonal elements in that row. According to (4a), we have $|2q_{ii}| \in [a|N_i|, a(|N_i| + 2)]$ and $\sum_{i \neq j} |q_{ij}| \in [0, a|N_i|]$, $\forall i \in V$. Since $|2q_{ii}| \geq \sum_{i \neq j} |q_{ij}|$, \mathbf{D}^\top is diagonally dominant. A symmetric diagonally dominant real matrix with nonnegative diagonal entries is positive semidefinite. Hence, \mathbf{D}^\top is a positive semidefinite matrix. \square

IV. MONOTONE GAMES

In what follows, we look at a class of strongly monotone games, present its basic properties, and show the advantages of Algorithm 1.

For each $i \in V$, we denote the gradient of f_i with respect to x_i by $\nabla_{x_i} f_i := \frac{\partial f_i}{\partial x_i} \in \mathbb{R}$, and $\phi(\mathbf{x}) := [\nabla_{x_1} f_1, \dots, \nabla_{x_n} f_n]^\top \in \mathbb{R}^n$.

We impose the following assumption of a class of strongly monotone games.

Assumption 1 ([23]). For some $l_m > 0$ and for all $\mathbf{x}', \mathbf{x} \in \mathcal{A}$,

$$\sum_{i \in V} (\phi_i(\mathbf{x}) - \phi_i(\mathbf{x}'))(x_i - x'_i) \leq -l_m \|\mathbf{x} - \mathbf{x}'\|^2. \quad (6)$$

Assumption 1 implies that each player's original payoff function \mathbf{f} is strictly concave in x_i [27]. We introduce the definition of concavity preservation.

Definition 4 (Concavity preservation [25]). Let Assumption 1 hold. Algorithm 1 is said to be concavity-preserving if each \hat{f}_i is strictly concave in x_i for all $i \in V$.

A. Concavity Preservation

The following result proves that under Assumption 1, Algorithm 1 is concavity-preserving.

Theorem 1. Let Assumption 1 hold. Then, Algorithm 1 is concavity-preserving.

Proof. Under Assumption 1, each player i 's original payoff function is strictly concave in x_i . We consider $\mathbf{x} = [x_1, \dots, x_i, \dots, x_n]^\top$ and $\mathbf{x}' = [x_1, \dots, x'_i, \dots, x_n]^\top$ and obtain $(\phi_i(\mathbf{x}) - \phi_i(\mathbf{x}'))(x_i - x'_i) < 0$.

We then check the sign of $(\hat{\phi}_i(\mathbf{x}) - \hat{\phi}_i(\mathbf{x}'))(x_i - x'_i) = (\phi_i(\mathbf{x}) - \phi_i(\mathbf{x}'))(x_i - x'_i) - 2q_{ii}(x_i - x'_i)^2 < 0$, which complies with Definition 4. \square

The next result shows that under Assumption 1, both original game and perturbed game after Algorithm 1 admit a unique NE.

Theorem 2. Let Assumption 1 hold. Then,

(i) the original game with the payoff functions \mathbf{f} admits a unique NE.

(ii) after Algorithm 1, the perturbed game with the perturbed payoff functions $\hat{\mathbf{f}}$ admits a unique NE.

Proof. For (i), the class of strongly monotone games is a proper subclass of monotone games, first introduced in [27]. Instead of the stronger requirement in Assumption 1, the weaker assumption $\sum_{i \in V} c_i(\phi_i(\mathbf{x}) - \phi_i(\mathbf{x}'))(x_i - x'_i) < 0$ is imposed. Every monotone game admits a unique NE [27, Theorem 2]. Therefore, the original game under Assumption 1 also admits a unique NE.

For (ii), we are going to check whether the perturbed game is a monotone game by investigating whether the sign of $\sum_{i \in V} (\hat{\phi}_i(\mathbf{x}) - \hat{\phi}_i(\mathbf{x}'))(x_i - x'_i) < 0$, $\forall \mathbf{x}', \mathbf{x} \in \mathcal{A}, \mathbf{x}' \neq \mathbf{x}$. It is straightforward that

$$\begin{aligned} & \sum_{i \in V} (\hat{\phi}_i(\mathbf{x}) - \hat{\phi}_i(\mathbf{x}'))(x_i - x'_i) \\ &= \sum_{i \in V} (\phi_i(\mathbf{x}) - \phi_i(\mathbf{x}'))(x_i - x'_i) - \sum_{i \in V} 2q_{ii}(x_i - x'_i)^2 < 0. \end{aligned}$$

We draw the conclusion that the perturbed game is a monotone game, therefore admitting a unique NE. \square

B. γ -accurate Nash equilibrium

According to Theorem 2, when Assumption 1 holds, both original game and perturbed game admit a unique NE. We denote the original NE of the original game by \mathbf{x}^* and the perturbed NE of the perturbed game by $\hat{\mathbf{x}}^*$.

We now introduce the definition of γ -accurate NE.

Definition 5 (γ -accurate NE). Let Assumption 1 hold. The perturbed NE $\hat{\mathbf{x}}^*$ is said to be γ -accurate if $\|\mathbf{x}^* - \hat{\mathbf{x}}^*\| \leq \gamma$.

In the following result, we derive an upper bound for the distance between the original NE and the perturbed NE after Algorithm 1.

Theorem 3. Let Assumption 1 hold. Further suppose that the original NE and perturbed NE are both interior points in the action space \mathcal{A} . Then, the perturbed NE is γ -accurate with

$$\gamma = \frac{\sqrt{na} + \sqrt{\sum_{i \in V} (4|N_i|^2 + 5|N_i| + 4)a} \|\mathbf{x}^*\|}{l_m} \quad (7)$$

Proof. By taking the derivative of (5) w.r.t. x_i and rewriting it in the vector form, we obtain

$$\hat{\phi}(\mathbf{x}) = \phi(\mathbf{x}) - \mathbf{D}^\top \mathbf{x} - \boldsymbol{\beta}. \quad (8)$$

We now turn to the original NE and perturbed NE, whose existence and uniqueness are guaranteed by Theorem 2. Moreover, in Theorem 3, we further impose the assumption of interior NE. Substituting $\hat{\mathbf{x}}^*$ into Eq. (8), we have $\phi(\hat{\mathbf{x}}^*) = \hat{\phi}(\hat{\mathbf{x}}^*) + \mathbf{D}^\top \hat{\mathbf{x}}^* + \boldsymbol{\beta}$. The first-order condition for the interior NE is that $\phi(\mathbf{x}^*) = 0$ and $\hat{\phi}(\hat{\mathbf{x}}^*) = 0$. Then, it yields

$[\phi(\mathbf{x}^*) - \phi(\hat{\mathbf{x}}^*)] - \mathbf{D}^\top(\mathbf{x}^* - \hat{\mathbf{x}}^*) = -\beta - \mathbf{D}^\top \mathbf{x}^*$. Multiplying by $(\mathbf{x}^* - \hat{\mathbf{x}}^*)^\top$, we observe that

$$\begin{aligned} & -(\mathbf{x}^* - \hat{\mathbf{x}}^*)^\top (\beta + \mathbf{D}^\top \mathbf{x}^*) \\ &= (\mathbf{x}^* - \hat{\mathbf{x}}^*)^\top [\phi(\mathbf{x}^*) - \phi(\hat{\mathbf{x}}^*)] - (\mathbf{x}^* - \hat{\mathbf{x}}^*)^\top \mathbf{D}^\top (\mathbf{x}^* - \hat{\mathbf{x}}^*) \\ &\stackrel{(a)}{\leq} (\mathbf{x}^* - \hat{\mathbf{x}}^*)^\top [\phi(\mathbf{x}^*) - \phi(\hat{\mathbf{x}}^*)] \\ &\stackrel{(b)}{\leq} -l_m \|\mathbf{x}^* - \hat{\mathbf{x}}^*\|^2. \end{aligned}$$

The inequality (a) holds because \mathbf{D}^\top is designed to be a positive semidefinite matrix (See Lemma 1). The inequality (b) is exactly from Eq. (6). Thus there holds $(\mathbf{x}^* - \hat{\mathbf{x}}^*)^\top (\beta + \mathbf{D}^\top \mathbf{x}^*) \geq l_m \|\mathbf{x}^* - \hat{\mathbf{x}}^*\|^2 > 0$.

Further considering the Cauchy–Schwarz inequality, we finally obtain a bound on the distance

$$\begin{aligned} & \|\mathbf{x}^* - \hat{\mathbf{x}}^*\| && (9a) \\ & \leq \frac{\|\beta\| + \|\mathbf{D}\| \|\mathbf{x}^*\|}{l_m} && (9b) \\ & \leq \frac{\sqrt{na} + \sqrt{\sum_{i \in \mathcal{V}} (4|N_i|^2 + 5|N_i| + 4)a} \|\mathbf{x}^*\|}{l_m}. && (9c) \end{aligned}$$

The proof is now completed. \square

Remark 1. *The upper bound (9c) is very conservative because it considers the worst-case scenario in which all $q_{ij}, \beta_i, \forall i, j \in \mathcal{V}$ take their maximum values. In comparison, the upper bound (9b) is a relatively small bound, which is more likely to happen with high probability in realization.*

V. LINEAR-QUADRATIC GAMES

A practical challenge of Algorithm 1 is how to select the Laplace parameters a and λ that can ensure certain differential privacy requirement. The selection depends on the class of payoff functions and the design choice of \mathcal{W} -adjacency. In this section, we analyze a benchmark game whose payoff functions are in the linear-quadratic form.

Denote the adjacency matrix of the interaction/communication network by $\mathbf{G} \in \mathbb{R}^{n \times n}$, with each entry $g_{ij} \in \mathbb{R}$ denoting whether player $j \in \mathcal{V}$ is linked to player $i \in \mathcal{V}$ and also indicating the linkage intensity.

We now impose the assumption of linear-quadratic games.

Assumption 2. *The payoff functions of a linear-quadratic game are set as*

$$f_i(x_i, \mathbf{x}_{-i}) = -\frac{1}{2}x_i^2 + b_i x_i + \sum_{j \in \mathcal{V}} g_{ij} x_i x_j, \quad \forall i \in \mathcal{V}, \quad (10)$$

where $b_i \in \mathbb{R}^{\geq 0}$ represents the marginal benefit of player i .

Since each player i 's payoff functions is now parameterized by the parameters g_{ij} and b_i . Hence, it is reasonable to specify \mathcal{W} -adjacency on these parameters. For example, we specify a definition of μ -adjacency for LQ games.

Definition 6 (μ -adjacency). *Consider linear-quadratic payoff functions \mathbf{f} and \mathbf{f}' . They are said to be μ -adjacent if there*

exists $i_0 \in \mathcal{V}$ such that

$$g_{i1} = g'_{i1}, \dots, g_{in} = g'_{in}, b_i = b'_i, \quad i \neq i_0; \quad (11a)$$

$$\max\{g_{i_0 1} - g'_{i_0 1}, \dots, g_{i_0 n} - g'_{i_0 n}, b_{i_0} - b'_{i_0}\} \leq \mu. \quad (11b)$$

In what follows, we first present how the Laplace parameters a and λ are selected to guarantee (ϵ, δ) -differential privacy for one-dimensional truncated Laplace mechanism, and then generalize this result to differential private LQ games.

A. One-dimensional Truncated Laplace Mechanism

The work of [29]–[31] investigated how the Laplace parameters are chosen to meet the differential privacy criterion in the one-dimensional case. As presented in (9c), Algorithm 1 leads to a biased perturbed NE. As a result, a stringent analysis is required to determine the lower bounds of the Laplace parameters that can produce a less biased perturbed NE. Compared with [29], the following result relaxes the requirement for the Laplace parameters to guarantee the differential privacy, and gives the tight lower bounds for a and λ in the one-dimensional case.

We consider one-dimensional truncated perturbation mechanism. Let D be the space of datasets of interest. Suppose there is a query as a function $y : D \rightarrow \mathbb{R}$. Given D , a randomized mapping \mathcal{K} will release the one-dimensional response $\mathcal{K}(D)$ that is the summation of the true query answer $y \in \mathbb{R}$ and a random noise $\eta \in [-a, a]$ following $\mathcal{L}_{tr}(a, \lambda)$, $\mathcal{K}(D) = y(D) + \eta$. The sensitivity of one-dimensional true query is then given by $\Delta y = \max_{D_1, D_2 \in D} |y(D_1) - y(D_2)|$. The randomized mapping \mathcal{K} gives (ϵ, δ) -differential privacy if for any two datasets $D_1, D_2 \in D$ differing in at most one element, and all $\mathcal{K} \subseteq \text{range}(\mathcal{K})$, there holds

$$\mathbb{P}(\mathcal{K}(D_1) \in \mathcal{K}) \leq e^\epsilon \mathbb{P}(\mathcal{K}(D_2) \in \mathcal{K}) + \delta. \quad (12)$$

Lemma 2. *Given the privacy parameters $0 < \delta < \frac{1}{2}, \epsilon > 0$, the randomized mapping \mathcal{K} preserves (ϵ, δ) -differential privacy if*

$$\lambda \geq \frac{\Delta y}{\epsilon - \ln(1 - \delta)}, \quad (13a)$$

$$a \geq \max \left\{ \Delta y, \lambda \ln \left(\frac{e^{\frac{\Delta y}{\lambda}} - 1}{2\delta} + 1 \right) \right\}. \quad (13b)$$

Proof. We are seeking to show that for any $D_1, D_2 \in D$ differing in at most one element, for any subset $\mathcal{K} \subseteq \text{range}(\mathcal{K})$, Eq. (12) is satisfied.

Without loss of generality, we let $y(D_1) \leq y(D_2)$. Given $\mathcal{K} \subseteq \text{range}(\mathcal{K})$, there are 5 cases to consider, each of which should render Eq. (12) to be satisfied.

1. $\mathcal{K} \subseteq (-\infty, -a + y(D_1))$: It is true that $0 \leq e^\epsilon \cdot 0 + \delta$.
2. $\mathcal{K} \subseteq [-a + y(D_1), -a + y(D_2)]$: First, since $\delta < \frac{1}{2}$, it is impossible to find the configuration for a and λ that can make Eq. (12) valid when $a \leq \Delta y$. Second, we now consider $y(D_2) - y(D_1) \leq \Delta y < a$. For any D_1 and D_2 differing in at most one element, to satisfy Eq. (12),

we are going to show that the probability mass in the interval $[-a + y(D_1), -a + y(D_2)]$ does not exceed δ :

$$\begin{aligned} \int_{\mathcal{X}} Be^{-\frac{|y-y(D_1)|}{\lambda}} dy &= B\lambda(e^{-\frac{-a+y(D_2)-y(D_1)}{\lambda}} - e^{-\frac{-a}{\lambda}}) \\ &\leq B\lambda(e^{-\frac{-a+\Delta}{\lambda}} - e^{-\frac{-a}{\lambda}}) \leq \delta. \end{aligned}$$

The first inequality holds because $e^{-\frac{-a+y(D_2)-y(D_1)}{\lambda}}$ increases when $y(D_2)-y(D_1)$ increases, while the second inequality comes from the condition (13b).

3. $\mathcal{X} \subseteq [-a + y(D_2), a + y(D_1)]$: Equation (12) can be written as $\int_{\mathcal{X}} Be^{-\frac{|y-y(D_1)|}{\lambda}} dy \leq e^\epsilon \int_{\mathcal{X}} Be^{-\frac{|y-y(D_2)|}{\lambda}} dy + \delta$. Using triangle inequality $|y-y(D_2)| \leq |y-y(D_1)| + |y(D_1)-y(D_2)|$ and combining the condition (13a), it is sufficient to show that $\int_{\mathcal{X}} Be^{-\frac{|y-y(D_1)|}{\lambda}} dy \leq e^\epsilon \int_{\mathcal{X}} Be^{-\frac{|y-y(D_1)|}{\lambda}} dy + \delta$, or further, $1 \leq e^\epsilon + \delta \leq e^\epsilon + \frac{\delta}{\int_{\mathcal{X}} Be^{-\frac{|y-y(D_1)|}{\lambda}} dy}$.
4. $\mathcal{X} \subseteq [a + y(D_1), a + y(D_2)]$: It is true that $0 \leq e^\epsilon \int_{\mathcal{X}} Be^{-\frac{|y-y(D_2)|}{\lambda}} dy + \delta$.
5. $\mathcal{X} \subseteq [a + y(D_2), \infty]$: It is valid that $0 \leq e^\epsilon \cdot 0 + \delta$.

In all, under conditions (13a) and (13b), the randomized mapping \mathcal{X} preserves (ϵ, δ) -differential privacy. \square

B. Differentially Private LQ Games

In what follows, Laplace parameter conditions are given to ensure certain differential privacy requirement for LQ games.

Stack the non-zero elements q_{ij} into $\mathbf{q} \in \mathbb{R}^m$ with $m = n + \sum_{i \in V} |N_i|$. Also stack g_{ij} into $\mathbf{g} \in \mathbb{R}^m$ such that each element in \mathbf{g} is matched with the corresponding element in \mathbf{q} . In particular, if the k th element of \mathbf{q} is q_{ij} , then the k th element of \mathbf{g} is g_{ij} . The dimension of $\begin{bmatrix} \mathbf{g} \\ \mathbf{b} \end{bmatrix}$ is $l = 2n + \sum_{i \in V} |N_i|$. Further define $p = 1 + \max_{i \in V} |N_i|$.

Theorem 4. Consider a LQ game. Then given any $\epsilon, \delta, \mu > 0$, the mapping $\widehat{\mathcal{M}}(\mathbf{g}, \mathbf{b}) = \begin{bmatrix} \mathbf{g} - \mathbf{q} \\ \mathbf{b} - \beta \end{bmatrix}$ achieves $(p\epsilon, p\delta)$ -differential privacy under μ -adjacency if

$$\lambda \geq \frac{\mu}{\epsilon - \ln(1 - \delta)}, \quad (14a)$$

$$a \geq \max \left\{ \mu, \lambda \ln \left(\frac{e^{\frac{\mu}{\lambda}} - 1}{2\delta} + 1 \right) \right\}. \quad (14b)$$

Proof. Consider two μ -adjacent linear-quadratic payoff functions \mathbf{f} and \mathbf{f}' that are uniquely determined by the pairs (\mathbf{g}, \mathbf{b}) and $(\mathbf{g}', \mathbf{b}')$, respectively.

Denote $\mathbf{v} = [\mathbf{g}^\top \ \mathbf{b}^\top]^\top \in \mathbb{R}^l$ and $\mathbf{v}' = [\mathbf{g}'^\top \ \mathbf{b}'^\top]^\top \in \mathbb{R}^l$. Also define $V_{\text{perturbed}} = \{1, 2, \dots, l\}$. Due to μ -adjacency, there exists $i_0 \in V$ such that the conditions (11a) and (11b) hold. We denote by V_{diff} the indices of b_{i_0} and $g_{i_0j}, j \in N_{i_0} \cup \{i_0\}$, in \mathbf{v} . The conditions (11a) and (11b) indicate that 1) \mathbf{v} and \mathbf{v}' differ in at most $|N_{i_0}| + 1$ elements; 2) and for any $i \in V_{\text{diff}}$, we have $|v_i - v'_i| \leq \mu$.

Note that each $v_i, i \in V_{\text{diff}}$, is independent of any other $v_j, j \in V_{\text{perturbed}} \neq i$. We decompose $\widehat{\mathcal{M}}$ and further notice that each component $\widehat{\mathcal{M}}_i(v_i), i \in V_{\text{diff}}$, can be viewed as a randomization of v_i . We then apply Lemma 2 with $\Delta y = \mu$.

It is therefore straightforward that when the conditions (14a) and (14b) are satisfied, each component $\widehat{\mathcal{M}}_i(v_i), i \in V_{\text{diff}}$, preserves (ϵ, δ) -differential privacy.

We now examine the probability $\mathbb{P}(\widehat{\mathcal{M}}(\mathbf{v}) \in \widehat{\mathcal{M}}) = \prod_{i \in V_{\text{perturbed}}} \mathbb{P}(\widehat{\mathcal{M}}_i(v_i) \in \widehat{\mathcal{M}}_i)$. There are at most $|N_{i_0}| + 1$ different elements indexed in V_{diff} between \mathbf{v} and \mathbf{v}' , while the remaining elements indexed in the set $V_{\text{same}} := (V_{\text{perturbed}} - V_{\text{diff}})$ are the same. Also, combining the fact that each component $\widehat{\mathcal{M}}_i(v_i), i \in V_{\text{diff}}$, is (ϵ, δ) -differentially private, as a consequence, we can substitute

$$\begin{aligned} &\prod_{i \in V_{\text{perturbed}}} \mathbb{P}(\widehat{\mathcal{M}}_i(v_i) \in \widehat{\mathcal{M}}_i) \\ &= \prod_{i \in V_{\text{same}}} \mathbb{P}(\widehat{\mathcal{M}}_i(v_i) \in \widehat{\mathcal{M}}_i) \prod_{i \in V_{\text{diff}}} \mathbb{P}(\widehat{\mathcal{M}}_i(v_i) \in \widehat{\mathcal{M}}_i) \\ &\leq \prod_{i \in V_{\text{same}}} \mathbb{P}(\widehat{\mathcal{M}}_i(v'_i) \in \widehat{\mathcal{M}}_i) \prod_{i \in V_{\text{diff}}} (e^\epsilon \mathbb{P}(\widehat{\mathcal{M}}_i(v'_i) \in \widehat{\mathcal{M}}_i) + \delta) \end{aligned}$$

If we focus on the second product term and look at the additive contribution of each of the δ terms, of which there are $|N_{i_0}| + 1$, we notice that they are only ever multiplied by probabilities that are at most one. Therefore, each contributes at most an additive δ :

$$\begin{aligned} &\prod_{i \in V_{\text{diff}}} (e^\epsilon \mathbb{P}(\widehat{\mathcal{M}}_i(v'_i) \in \widehat{\mathcal{M}}_i) + \delta) \\ &\leq e^{(|N_{i_0}|+1)\epsilon} \prod_{i \in V_{\text{diff}}} \mathbb{P}(\widehat{\mathcal{M}}_i(v'_i) \in \widehat{\mathcal{M}}_i) + (|N_{i_0}| + 1)\delta \end{aligned}$$

Then, we have

$$\begin{aligned} &\prod_{i \in V_{\text{perturbed}}} \mathbb{P}(\widehat{\mathcal{M}}_i(v_i) \in \widehat{\mathcal{M}}_i) \\ &\leq e^{(|N_{i_0}|+1)\epsilon} \mathbb{P}(\widehat{\mathcal{M}}(\mathbf{v}') \in \widehat{\mathcal{M}}) + (|N_{i_0}| + 1)\delta. \end{aligned}$$

Note that i_0 can be any $i \in V$. Therefore, $\widehat{\mathcal{M}}$ releases $(p\epsilon, p\delta)$ -differential privacy with $p = 1 + \max_{i \in V} |N_i|$. \square

Remark 2. Note that the privacy guarantee depends in a crucial way on how the notion of adjacency is defined. Although we only prove the differential privacy from \mathbf{f} to $\hat{\mathbf{f}}$ for LQ games with μ -adjacency in Definition 6, it serves as a tutorial example and can be applied to other monotone games as long as players' payoff functions are explicitly given.

VI. NUMERICAL EXAMPLES

Consider a LQ game with 10 players. Players are arranged in a ring lattice with each player connected to $|N_i| = 4, \forall i \in V$, neighbors. (Thus, $p = 5$.) Each linkage intensity is set as 0.08. The action space considered is relatively large, $\mathbf{x}_i \in [0, 100], \forall i \in V$, to ensure interior original NE and perturbed NE. According to [28], the original NE is calculated by $\mathbf{x}^* = (\mathbf{I} - \mathbf{G})^{-1}\mathbf{b}$.

Experiment 1 (Validation of Theorems). We consider $\mu = 0.01$ and choose two parameter configurations

$$\epsilon_1 = \ln 2, \quad \delta_1 = 0.05, \quad a_1 = 0.034, \quad \lambda_1 = 0.013; \quad (S1)$$

$$\epsilon_2 = 3 \ln 2, \quad \delta_2 = 0.15, \quad a_2 = 0.015, \quad \lambda_2 = 0.0045, \quad (S2)$$

where $a_1, a_2, \lambda_1, \lambda_2$ are selected upon Theorem 4 to guarantee differential privacy.

Under each parameter configuration, we conduct 500 executions, in each of which we apply Algorithm 1. Each perturbed NE is calculated by $\hat{\mathbf{x}}^* = (\mathbf{I} - \mathbf{G} + \mathbf{D})^{-1}(\mathbf{b} - \beta)$. We then compute $\|\mathbf{x}^* - \hat{\mathbf{x}}^*\|$, and γ according to (9b).

In Fig. 1, we plot the comparison of γ and $\|\mathbf{x}^* - \hat{\mathbf{x}}^*\|$ between two parameter configurations (S1) and (S2). The result of Fig. 1 is consistent with Theorem 3 that the distance between the original NE and the perturbed NE is bounded by γ while preserving differential privacy. \square

Experiment 2 (Benchmark with Existing Methods). Based on Experiment 1, we further plot each player's original NE and distribution of the perturbed NE under two parameter configurations (S1) and (S2) among 500 executions.

The result of Fig. 2 shows that most perturbed NE under (S1) and (S2) are located to the left of the original NE. The parameter configuration (S2) has a weaker requirement for differential privacy. The perturbed NE under (S2) are closer to the original NE, implying that one has to sacrifice the differential privacy of payoff functions for the accuracy of NE.

To further show the relevance among the accuracy of NE, the privacy requirement ϵ and the Laplace parameter a , we fix $\delta = 0$ and plot $\|\mathbf{x}^* - \hat{\mathbf{x}}^*\|/\|\mathbf{x}^*\|$ versus ϵ and a each for 50 executions in Fig. 3. Roughly speaking, it shows that as ϵ decreases (stricter privacy), the Laplace parameter a increases and thus the accuracy of NE decreases.

Compared with existing methods of state/communication perturbation [20], [23], [32], we both show the tradeoff between the accuracy of the optimal points/NE and the privacy of objective functions/payoff functions. However, they prove that $\lim_{k \rightarrow \infty} \mathbb{E}(\|\mathbf{x}(k) - \mathbf{x}^*\|^2)$ has an upper bound depending on convergence rate and privacy level. According to the structure of their privacy algorithm, they might produce an asymptotically unbiased perturbed NE. Unlike those results, Algorithm 1 always produces a biased perturbed NE. It arises from $\mathbb{E}(q_{ii}) > 0, \forall i \in \mathbf{V}$ that are necessary to ensure the concavity of the perturbed payoff function. However, they

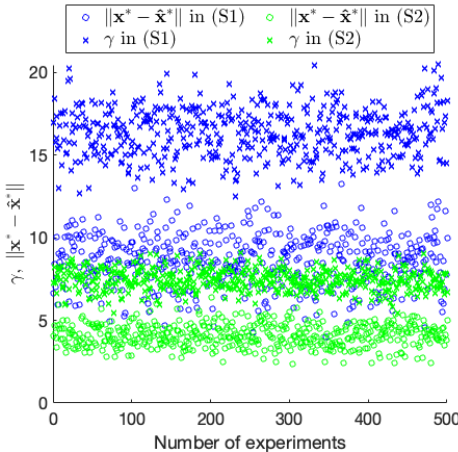


Fig. 1: The comparison of γ and $\|\mathbf{x}^* - \hat{\mathbf{x}}^*\|$ between two parameter configurations (S1) and (S2).

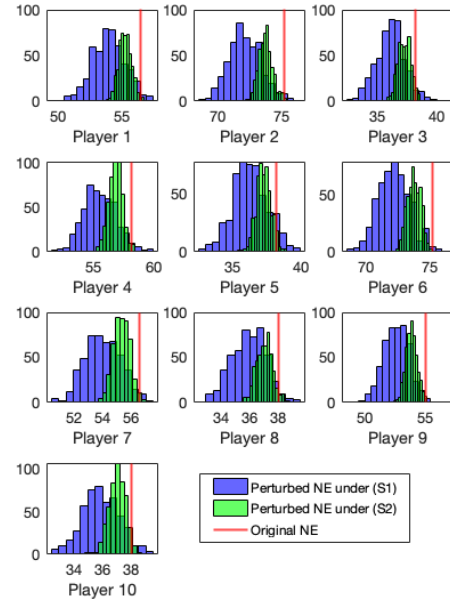


Fig. 2: The original NE and the distribution of the perturbed NE under the parameter configurations (S1) and (S2). The y-axis represents the number of times that player i 's perturbed NE action occurred within the intervals set by the x-axis among 500 executions.

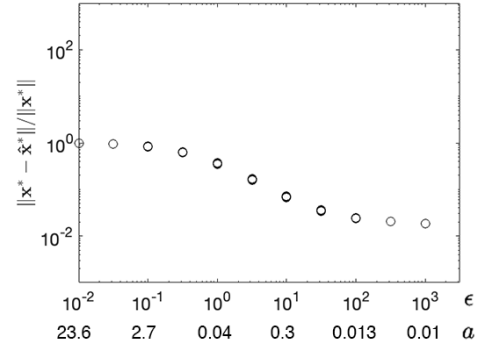


Fig. 3: The plot of $\|\mathbf{x}^* - \hat{\mathbf{x}}^*\|/\|\mathbf{x}^*\|$ versus ϵ and a each for 50 executions.

have to add perturbation to communications at all time steps. For example, in [32], it takes roughly 4000 steps to reach a close distance from \mathbf{x}^* , in each of which perturbation is added to players' state. In contrast, we only add perturbation to the original payoff functions once, after which the computation of the distributed NE is deterministic. The number of linear-quadratic perturbation coefficients (non-zero $q_{ij}, \beta_i, \forall i, j \in \mathbf{V}$) generated by Algorithm 1 is only 60, which is far less than theirs. \square

Experiment 3 (Tradeoff between Privacy and Payoffs). Upon Experiment 1, we further compute the players' payoffs at the original NE and the perturbed NE under two parameter configurations, $\mathbf{f}(\mathbf{x}^*)$ and $\mathbf{f}(\hat{\mathbf{x}}^*)$, and plot them in Fig. 4.

From the result of Fig. 4, it is not surprising that players' payoffs at the perturbed NE under (S1) and (S2) are always lower than those at the original NE. Players' payoffs at the perturbed under (S1) are lower than those at the perturbed

NE under (S2). It indicates that the sacrifice of the accuracy of NE for payoff functions' privacy leads to the decline of players' payoffs. \square

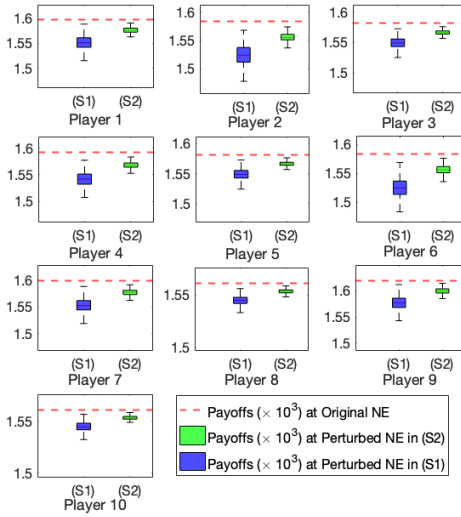


Fig. 4: Players' payoffs at the original NE, the perturbed NE in (S1), and the perturbed NE in (S2). The y-axis represents the value of player i 's payoffs.

VII. CONCLUSION

In this work, we investigated network games in which players participated in information aggregation processes under the differential privacy requirement for players' payoff functions. The LLQFP mechanism was proposed. We turned to monotone games, demonstrating that the LLQFP mechanism preserved the concavity property and generated a bounded perturbed NE which was controllable by Laplace parameter tuning. We also looked at LQ games as a pedagogical example to explain, given what Laplace parameter conditions, differential privacy of the LLQFP mechanism could be ensured. Finally, numerical examples were presented to demonstrate the benefits of the LLQFP mechanism.

REFERENCES

- [1] Y. Leng, Y. Chen, X. Dong, J. Wu, and G. Shi, "Privacy risks of social interaction structure: Network learning in quadratic games," *Available at SSRN 3875878*, 2021.
- [2] L. Bianco, M. Caramia, S. Giordani, and V. Piccialli, "A game-theoretic approach for regulating hazmat transportation," *Transportation Science*, vol. 50, no. 2, pp. 424–438, 2016.
- [3] D. Niyato and E. Hossain, "Competitive pricing for spectrum sharing in cognitive radio networks: Dynamic game, inefficiency of nash equilibrium, and collusion," *IEEE journal on selected areas in communications*, vol. 26, no. 1, pp. 192–202, 2008.
- [4] F. Salehisadaghiani and L. Pavel, "Distributed nash equilibrium seeking: A gossip-based algorithm," *Automatica*, vol. 72, pp. 209–216, 2016.
- [5] F. Parise, B. Gentile, S. Grammatico, and J. Lygeros, "Network aggregative games: Distributed convergence to nash equilibria," in *2015 54th IEEE Conference on Decision and Control (CDC)*. IEEE, 2015, pp. 2295–2300.
- [6] M. Ye and G. Hu, "Distributed nash equilibrium seeking by a consensus based approach," *IEEE Transactions on Automatic Control*, vol. 62, no. 9, pp. 4811–4818, 2017.
- [7] E. Hopkins, "A note on best response dynamics," *Games and Economic Behavior*, vol. 29, no. 1-2, pp. 138–150, 1999.
- [8] A. Matsui, "Best response dynamics and socially stable strategies," *Journal of Economic Theory*, vol. 57, no. 2, pp. 343–362, 1992.

- [9] N. Nisan, M. Schapira, G. Valiant, and A. Zohar, "Best-response mechanisms," in *ICS*. Citeseer, 2011, pp. 155–165.
- [10] T. Lin, Z. Zhou, W. Ba, and J. Zhang, "Optimal no-regret learning in strongly monotone games with bandit feedback," *arXiv preprint arXiv:2112.02856*, 2021.
- [11] M. Bravo, D. Leslie, and P. Mertikopoulos, "Bandit learning in concave n-person games," in *Proceedings of the 32nd International Conference on Neural Information Processing Systems*, ser. NIPS'18. Curran Associates Inc., 2018, p. 5666–5676.
- [12] Z. Zhou, P. Mertikopoulos, S. Athey, N. Bambos, P. W. Glynn, and Y. Ye, "Learning in games with lossy feedback," *Advances in Neural Information Processing Systems*, vol. 31, 2018.
- [13] G. J. Gordon, A. Greenwald, and C. Marks, "No-regret learning in convex games," in *Proceedings of the 25th international conference on Machine learning*, 2008, pp. 360–367.
- [14] J. C. Harsanyi, "Morality and the theory of rational behavior," *Social research*, pp. 623–656, 1977.
- [15] C. Dwork, "Differential privacy: A survey of results," in *International conference on theory and applications of models of computation*. Springer, 2008, pp. 1–19.
- [16] C. Dwork, A. Roth et al., "The algorithmic foundations of differential privacy," *Found. Trends Theor. Comput. Sci.*, vol. 9, no. 3-4, pp. 211–407, 2014.
- [17] 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.
- [18] E. Nozari, P. Tallapragada, and J. Cortés, "Differentially private average consensus: Obstructions, trade-offs, and optimal algorithm design," *Automatica*, vol. 81, pp. 221–231, 2017.
- [19] J. Le Ny and G. J. Pappas, "Differentially private filtering," *IEEE Transactions on Automatic Control*, vol. 59, no. 2, pp. 341–354, 2013.
- [20] S. Han, U. Topcu, and G. J. Pappas, "Differentially private distributed constrained optimization," *IEEE Transactions on Automatic Control*, vol. 62, no. 1, pp. 50–64, 2016.
- [21] Z. Huang, S. Mitra, and N. Vaidya, "Differentially private distributed optimization," in *Proceedings of the 2015 international conference on distributed computing and networking*, 2015, pp. 1–10.
- [22] E. Nozari, P. Tallapragada, and J. Cortés, "Differentially private distributed convex optimization via functional perturbation," *IEEE Transactions on Control of Network Systems*, vol. 5, no. 1, pp. 395–408, 2018.
- [23] M. Ye, G. Hu, L. Xie, and S. Xu, "Differentially private distributed nash equilibrium seeking for aggregative games," *IEEE Transactions on Automatic Control*, vol. 67, no. 5, pp. 2451–2458, 2021.
- [24] M. Shakarami, C. De Persis, and N. Monshizadeh, "Distributed dynamics for aggregative games: Robustness and privacy guarantees," *International Journal of Robust and Nonlinear Control*, vol. 32, no. 9, pp. 5048–5069, 2022.
- [25] J. Cortés, G. E. Dullerud, S. Han, J. Le Ny, S. Mitra, and G. J. Pappas, "Differential privacy in control and network systems," in *2016 IEEE 55th Conference on Decision and Control (CDC)*. IEEE, 2016, pp. 4252–4272.
- [26] C. Zhang, M. Ahmad, and Y. Wang, "Admm based privacy-preserving decentralized optimization," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 3, pp. 565–580, 2018.
- [27] J. B. Rosen, "Existence and uniqueness of equilibrium points for concave n-person games," *Econometrica: Journal of the Econometric Society*, pp. 520–534, 1965.
- [28] C. Ballester, A. Calvó-Armengol, and Y. Zenou, "Who's who in networks. wanted: The key player," *Econometrica*, vol. 74, no. 5, pp. 1403–1417, 2006.
- [29] Q. Geng, W. Ding, R. Guo, and S. Kumar, "Tight analysis of privacy and utility tradeoff in approximate differential privacy," in *International Conference on Artificial Intelligence and Statistics*. PMLR, 2020, pp. 89–99.
- [30] W. L. Croft, J.-R. Sack, and W. Shi, "Differential privacy via a truncated and normalized laplace mechanism," *arXiv preprint arXiv:1911.00602*, 2019.
- [31] N. Holohan, S. Antonatos, S. Braghin, and P. Mac Aonghusa, "The bounded laplace mechanism in differential privacy," *arXiv preprint arXiv:1808.10410*, 2018.
- [32] T. Ding, S. Zhu, J. He, C. Chen, and X. Guan, "Differentially private distributed optimization via state and direction perturbation in multiagent systems," *IEEE Transactions on Automatic Control*, vol. 67, no. 2, pp. 722–737, 2021.