This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TKDE.2020.3014246, IEEE Transactions on Knowledge and Data Engineering

More Than Privacy: Applying Differential Privacy in Key Areas of Artificial Intelligence

Tianqing Zhu, Dayong Ye, Wei Wang, Wanlei Zhou and Philip S. Yu*

Abstract—Artificial Intelligence (AI) has attracted a great deal of attention in recent years. However, alongside all its advancements, problems have also emerged, such as privacy violations, security issues and model fairness. Differential privacy, as a promising mathematical model, has several attractive properties that can help solve these problems, making it quite a valuable tool. For this reason, differential privacy has been broadly applied in AI but to date, no study has documented which differential privacy mechanisms can or have been leveraged to overcome its issues or the properties that make this possible. In this paper, we show that differential privacy can do more than just privacy preservation. It can also be used to improve security, stabilize learning, build fair models, and impose composition in selected areas of AI. With a focus on regular machine learning, distributed machine learning, deep learning, and multi-agent systems, the purpose of this article is to deliver a new view on many possibilities for improving AI performance with differential privacy techniques.

Index Terms—Differential Privacy, Artificial Intelligence, Machine Learning, Deep Learning, Multi-Agent Systems

1 Introduction

Artificial Intelligence (AI) is one of the most prevalent topics of research today across almost every scientific field. For example, multi-agent systems can be applied to distributed control systems [1], while distributed machine learning has been adopted by Google for mobile users [2]. However, as AI becomes more and more reliant on data, several new problems have emerged, such as privacy violations, security issues, model instability, model fairness and communication overheads. As just a few of the tactics used to derail AI, adversarial samples can fool machine learning models, leading to incorrect results. Multi-agent systems may receive false information from malicious agents. As a result, many researchers have been exploring new and existing security and privacy tools to tackle these new emerging problems. Differential privacy is one of these tools.

Differential privacy is a prevalent privacy preservation model which guarantees whether an individual's information is included in a dataset has little impact on the aggregate output. Fig. 1 illustrates a basic differential privacy framework using the following example. Consider two datasets that are almost identical but differ in only one record and that, access to the datasets is provided via a query function f. If we can find a mechanism that can query both datasets and obtain the same outputs, we can claim that differential privacy is satisfied. In that scenario, an adversary cannot associate the query outputs with either of the two neighbouring datasets, so the one different record is safe. Hence, the differential privacy guarantees that, even if an adversary knows all the other records in a dataset except for one unknown individual, they still cannot infer the information of that unknown record.

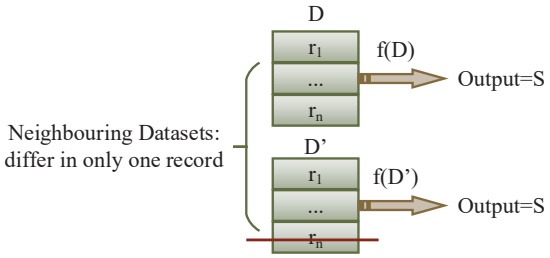


Fig. 1. Differential privacy

Interest in differential privacy mechanisms not only ranges from the privacy community to the AI community, it has also attracted the attention of many private companies, such as Apple[1], Uber[2] and Google [3].

The key idea of differential privacy is to introduce calibrated randomization to the aggregate output. When Dwork et al. [4] showed that applying differential privacy mechanisms to test data in machine learning could prevent over-fitting of learning algorithms, it launched a new direction beyond simple privacy preservation to one that solves emerging problems in AI [5]. We use two examples to illustrate how those new properties can be applied.

1.1 Examples

The first example pertains to machine learning. As shown in Fig. 2, machine learning suffers from several problems, including privacy violations, over-fitting and unfair models. Recent research has shown that differential privacy mechanisms have the potential to tackle those problems. First, to maintain fairness in a model, the training data can be re-sampled from the data universe using a differential privacy

Philip S. Yu is the corresponding author. Tianqing Zhu is with the School of Computer Science, China University of Geosciences, Wuhan, China; D. Ye, W. Wang and W. Zhou are with the Centre for Cyber Security and Privacy and the School of Computer Science, University of Technology, Sydney, Australia. Philip S. Yu is with the Department of Computer Science, University of Illinois at Chicago, USA. Email: Tianqing.e.zhu@gmail.com; {Dayong.Ye, Wei.Wang-3, Wanlei.Zhou}@uts.edu.au, psyu@cs.uic.edu

1. https://www.apple.com/au/privacy/approach-to-privacy/
2. https://www.usenix.org/node/208168

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TKDE.2020.3014246, IEEE Transactions on Knowledge and Data Engineering

mechanism [6]. Second, to preserve privacy, noise derived from a differential privacy mechanism can be added to the learning model [7]. Finally, calibrated noise can be applied to generate fresh testing data to increase stability and avoid over-fitting of the learning algorithm [4]. These successful applications of differential privacy show that learning problems can be solved by taking advantage of several properties of differential privacy, such as randomization, privacy preservation capability, and algorithm stability.

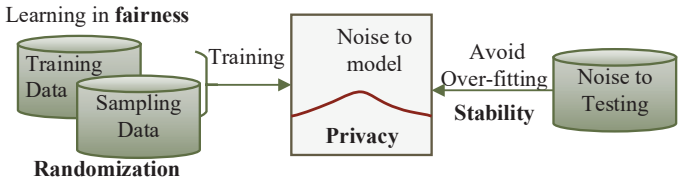


Fig. 2. Learning example

The second example comes from the realm of multi-agent systems, one of the traditional disciplines in AI. A multi-agent system is a computerized system composed of multiple interacting intelligent agents, such as sweeping robots as shown in Fig. 3. The faces are agents and the grid denotes the moving environment of all agents. An agent can make decisions over its direction of movement and can share that knowledge with other agents to help them make their decisions. The goal is for the robots to sweep all grids. Several problems exist in this multi-agent system. First, as each agent observes a different environment, it is difficult to share their knowledge. The randomizing mechanism in differential privacy can help to transfer the knowledge between agents. Second, communications between agents should be restricted to limit power consumption. Here, the privacy budget in differential privacy can help the system control to overall communications [8]. Third, when a malicious agent is present, like the agent in the red face, they may provide false knowledge. Differential privacy mechanisms can help improve the security level of communications by diminishing the impact of that agent.

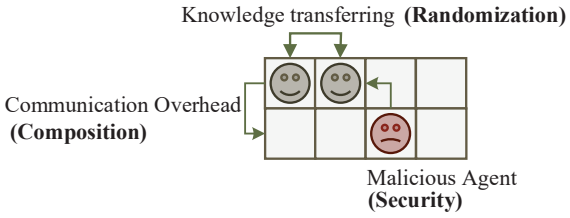


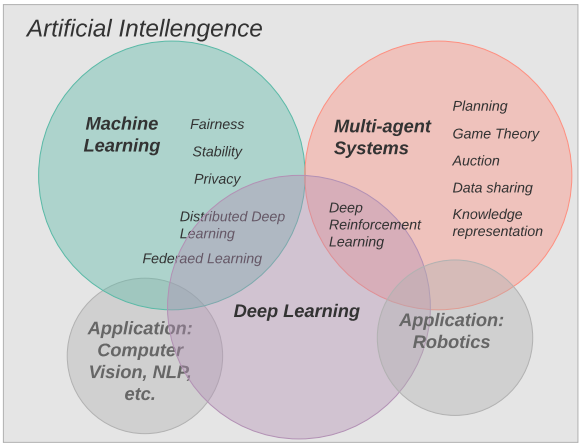
Fig. 3. Multi-agent example

Both these examples show how current research is applying differential privacy mechanisms to AI and how randomization can bring several new properties to AI.

1.2 AI areas

In AI, there are no strict area disciplines. Researchers and industries have built a birds-eye view of AI in all its diversity. Take the perspective of the Turing Test, for example. When programming a computer that needs to act like a human, the computer must have the following capabilities [9]: natural language processing so it can successfully communicate with a human; knowledge representation to store what it knows or hears; automated reasoning to use the stored information to answer questions and to draw new conclusions; machine learning to adapt to new circumstances and to detect and extrapolate patterns; computer vision to perceive objects; and robotics to manipulate objects.

Fig. 4. AI areas in the view of acting humanly



Based on this birds-eye view, we roughly categorize three major technical fields in AI: machine learning, deep learning and multi-agent system. Knowledge learning and automated reasoning can be processed by a multi-agent system; the other functions can be accomplished through machine learning and/or deep learning. In the view of the application, the AI area includes robotics, computer vision, natural language processing (NLP), etc.–see Fig 4.

Here, we note that although deep learning was originally a series of machine learning algorithms implemented in a neural network architecture, it has rapidly developed into a field of study in its own right with a huge number of novel perspectives and technologies, such as GANs [10], ResNets [11], etc. Therefore, we place deep learning in its own category.

The purpose of this paper is to document how the differential privacy mechanism can solve those new emerging problems in the technical fields: machine learning, deep learning and multi-agent systems. Applications such as robotics, NLP and computer vision have taken advantage of technologies such machine learning, deep learning and multi-agent system, so we have no reviewed these applications in dedicated sections.

1.3 Differential privacy in AI areas

Calibrated randomization benefits some AI algorithms. What follows is a summary of several properties derived from randomization.

- **Preserving privacy**. This is the original purpose of differential privacy. By hiding an individual in the aggregate information, differential privacy can preserve the privacy of participants in a dataset.
- **Stability**. Differential privacy mechanisms ensure that the probability of any outcome from a learning

algorithm is unchanged by modifying any individual record in the training data. This property establishes connections between a learning algorithm and its ability to be generalized.

- **Security**. Security relates to malicious participants in a system. Differential privacy mechanisms can reduce the impact of malicious participants in AI tasks. This property can guarantee security in AI systems.
- **Fairness**. In machine learning, a given algorithm is said to be fair, or to have fairness, if its results are independent of sensitive attributes, like race and gender. Differential privacy can help to maintain fairness in a learning model by re-sampling the training data from the universe.
- **Composition**. Differential privacy mechanisms can guarantee that any step that satisfies differential privacy can construct a new algorithm that also satisfies differential privacy. This property is referred to as composition and is controlled by the privacy budget. In AI, composition can be used to control the number of steps, communication loads, etc.

Table 1 shows the properties that have been explored to date for each of our three disciplines. In machine learning, differential privacy has been applied to private learning, stability and fairness. In deep learning, privacy is the major concern, but distributed deep learning and federated learning have also been investigated. In multi-agent systems, differential privacy has been used to guarantee privacy, provide security, and ensure composition. Utility shows the ultimate performance of the technology after adding differential privacy. Normally, privacy-preserving comes with a utility cost. However, if the differential privacy can contribute to stability, or security, the utility may increase, such as in federated learning or fairness.

Note, however, that blank cells do not mean we can not apply differential privacy mechanisms to those areas. As differential privacy has been proved to work well in many AI areas, in the future, more problems might be solved with the advantages of differential privacy.

The purpose of this paper is to highlight several possible avenues to integrate AI with differential privacy mechanisms, showing that differential privacy mechanisms have several attractive properties that make it quite valuable as a tool to AI beyond merely preserving privacy. The contributions of the paper are listed as follows:

- We have summarized several properties of differential privacy mechanisms.
- We have shown that these properties can improve diverse aspects of AI areas, including machine learning, deep learning and multi-agent systems.
- We explored new possibilities for taking advantage of differential privacy to bring new opportunities.

2 PRELIMINARY

2.1 Differential privacy

Consider a finite data universe $\mathcal{X}$. Let the variable r represent a record with d attributes sampled from the universe $\mathcal{X}$, a dataset D is an unordered set of n records from domain $\mathcal{X}$. Two datasets D and D' are neighbouring datasets if they differ in only one record. A query f is a function that maps a dataset D to an abstract range $\mathbb{R}$: $f : D \to \mathbb{R}$.

The target of differential privacy is to mask the differences between the results to query f between the neighbouring datasets to preserve privacy. The maximal difference is defined as the sensitivity Δf, which determines how much perturbation is required for a private-preserving answer. To achieve this goal, differential privacy provides a mechanism $\mathcal{M}$, which is a randomization algorithm that accesses the database and implements some functionalities. A formal definition of differential privacy follows.

Definition 1 (ϵ, δ-Differential Privacy [12]). *A randomized algorithm $\mathcal{M}$ gives ϵ-differential privacy for any pair of* neighbouring datasets *D and D', and, for every set of outcomes Ω, if $\mathcal{M}$ satisfies:*

$$Pr[\mathcal{M}(D) \in \Omega] \leq \exp(\epsilon) \cdot Pr[\mathcal{M}(D') \in \Omega] + \delta \qquad (1)$$

where Ω denotes the output range of the algorithm $\mathcal{M}$.

In Definition 1, the parameter ϵ is defined as the privacy budget, which controls the privacy guarantee level of mechanism $\mathcal{M}$. A smaller ϵ represents stronger privacy. If $\delta = 0$, the randomized mechanism $\mathcal{M}$ gives ϵ-differential privacy by its strictest definition. (ϵ, δ)-differential privacy provides freedom to violate strict ϵ-differential privacy for some low probability events.

Sensitivity is a parameter used in both mechanisms to determine how much randomization is required:

Definition 2 (Sensitivity). *For a query $f : D \to \mathbb{R}$, the sensitivity of f is defined as*

$$\Delta f = \max_{D,D'} ||f(D) - f(D')||_1 \qquad (2)$$

Two prevalent randomization mechanisms, Laplace and exponential, are used to satisfy the definition of differential privacy, but there are others, such as Gaussian mechanism. Each is explained next.

2.2 Randomization: Laplace mechanism

The Laplace mechanism is applied to numeric outputs [13]. The mechanism adds independent noise to the original answer, as shown in Definition 3.

Definition 3 (Laplace mechanism). *For a function $f : D \to \mathcal{R}$ over a dataset D, the mechanism $\mathcal{M}$ in Eq. 3 provides ϵ-differential privacy.*

$$\mathcal{M}(D) = f(D) + Lap(\frac{\Delta f}{\epsilon}) \qquad (3)$$

2.3 Gaussian mechanism

Compared to a Laplace mechanism, a Gaussian mechanism adds noise that is sampled from a zero-mean isotropic Gaussian distribution. The noise Z is sampled $\sim \mathcal{N}(0, \sigma^2)$ to the L_2 sensitivity $\Delta f = \max_{D,D'} ||f(D) - f(D')||_2$ as follows:

TABLE 1
Properties of differential privacy in artificial intelligence

Selected AI areas		Privacy	Stability	Fairness	Security	Composition	Utility
Machine learning	Private learning	Yes				Yes	Decrease
	Stability in learning		Yes				Increase
	Fairness in learning			Yes			Increase
Deep learning	Deep Learning	Yes					Decrease
	Distributed deep learning	Yes				Yes	Decrease
	Federated learning	Yes		Yes		Yes	Decrease or Increase
Multi-agent system	Reinforcement learning	Yes			Yes	Yes	Increase
	Auction	Yes				Yes	Decrease
	Game theory					Yes	Decrease

Definition 4 (Gaussian mechanism). *For a function $f : D \to \mathcal{R}$ over a dataset D, the mechanism $\mathcal{M}$ in Eq. 4 provides ϵ, δ-differential privacy.*

$$\mathcal{M}(D) = f(D) + \sim \mathcal{N}(0, \sigma^2), \tag{4}$$

$\sigma = \Delta f \sqrt{2\log(1.25/\delta)/epsilon.}$

2.4 Exponential mechanism

Exponential mechanisms are used to randomize the results for non-numeric queries. They are paired with a score function $q(D, \phi)$ that evaluates the quality of an output ϕ. Defining a score function is application-dependent, so different applications lead to various score functions [14].

Definition 5 (Exponential mechanism). *Let $q(D, \phi)$ be a score function of dataset D that measures the quality of output $\phi \in \Phi$, Δq represents the sensitivity of ϕ. The exponential mechanism $\mathcal{M}$ satisfies ϵ-differential privacy if*

$$\mathcal{M}(D) = \left(return\ \phi\ \propto \exp(\frac{\epsilon q(D, \phi)}{2\Delta q}) \right). \tag{5}$$

2.5 Composition

Two privacy budget composition theorems are widely used in the design of differential privacy mechanisms: sequential composition [14] and parallel composition [15].

Theorem 1. Parallel Composition*: Suppose we have a set of privacy steps $\mathcal{M} = \{\mathcal{M}_1, ...\mathcal{M}_m\}$, if each $\mathcal{M}_i$ provides an ϵ_i privacy guarantee on a disjointed subset of the entire dataset, the parallel of $\mathcal{M}$ will provide* $\max\{\epsilon_1, ..., \epsilon_m\}$-differential privacy.

Parallel composition corresponds to cases where each $\mathcal{M}_i$ is applied to disjointed subsets of the dataset. The ultimate privacy guarantee only depends on the largest privacy budget.

Theorem 2. Sequential Composition*: Suppose a set of privacy steps $\mathcal{M} = \{\mathcal{M}_1, ...\mathcal{M}_m\}$ are sequentially performed on a dataset, and each $\mathcal{M}_i$ provides an ϵ privacy guarantee, $\mathcal{M}$ will provide* $(m \cdot \epsilon)$-differential privacy.

Sequential composition offers a privacy guarantee for a sequence of differentially private computations. When a series of randomized mechanisms are performed sequentially on a dataset, the privacy budgets are added up for each step.

3 Differential Privacy in Machine Learning

3.1 Private machine learning

Private machine learning aims to protect the individual's privacy in training data or learning models. Differential privacy has been considered to be one of the most important tools in private machine learning and has been heavily investigated in the past decade.

The essential mechanisms in differential privacy all work to extend current non-private machine learning algorithms into differentially private algorithms. These extensions can be realized by incorporating Laplace or exponential mechanisms into non-private learning algorithms directly [16], or by adding Laplace noise into the objective functions [7].

Starting with Kasiviswanathan et al.'s work [17], the line of research presenting the details of private learning process from privacy based on empirical risk minimization [18], [19], to prediction [20], [21], Bayesian inference [22], [23], [24] and the multi-armed bandit [25], [26].

Private machine learning is one of the most powerful models accepted in this field. To avoid redundancy, this paper will not dive into details of private machine learning. A number of survey papers have discussed this field [16], [27], [28], [29] thoroughly.

3.2 Differential privacy in learning stability

3.2.1 The overview of stability of learning

A stable learning algorithm is one in which the prediction does not change much when the training data is modified slightly. Bousquet et al. [30] have proved that stability is linked to the generalization error bound of the learning algorithm, indicating that a highly stable algorithm leads to a less over-fit result. However, increasing the stability of the algorithm is challenging when the size of the testing data is limited. This is because the validate data sometimes are reused and lead to an incorrect learning model. To preserve statistical learning validity, analysts should collect new data for a fresh testing set.

Differential privacy can be naturally linked to learning stability. The concept of differential privacy ensures that the probability of observing any outcome from an analysis is essentially unchanged by modifying any single record. Dwork et al. [4], [31] showed that differential privacy mechanisms can be used to develop adaptive data analysis algorithms with provable bounds for over-fitting, noting that certain stability notions are necessary and sufficient for generalization. Therefore, differential privacy is stronger than previ-

ous notions of stability and, in particular, possesses strong adaptive composition guarantees [32].

3.2.2 Differential privacy in learning stability

Dwork et al. [4] show that, by adding noise to generate fresh testing data, differential privacy mechanisms can achieve highly stable learning. For a dataset D, an analyst learns about the data by running a series of analyses f_i on the dataset. The choice of which analysis to run depends on the results from the earlier analyses. Specifically, the analyst first selects a statistic f_0 to query on D and observes a query result $y_1 = f_0(D)$. From the k^{th} analysis, the analyst selects a function f_k based on the query result $y_1, ..., ...y_{k-1}$. To improve the generalization capability of the adaptive scenario, noise is added in each analysis iteration. For example, $y_k = Lap(\frac{\Delta f}{\epsilon}) + f_{k-1}(D)$ [31].

This type of adaptive analysis can be linked to machine learning. The dataset D can be randomly partitioned into a training set D_t and a testing (holdout) set D_h. The analyst can access the training set D_t without restrictions but may only access D_h through a differentially private interface. The interface takes the testing and training sets as inputs and, for all functions given by the analyst, provides statistically valid estimates of each function's results.

For a sufficiently large testing set, the differential privacy interface guarantees that for function $f : D \rightarrow [0, 1]$, the mechanism will return a randomized value v_f. When v_f is compared to the query result y, we have $|v_f - y| \leq \tau$ with a probability of at least $1 - \beta$, where τ is the analyst's choice of error and β is the confidence parameter. The probability space is over the data elements in D_h and D_t and the randomness introduced by the interface. A multiplicative weight updating mechanism [33] could also be included in the interface to conserve the privacy budget.

3.2.3 Summary of stability of learning

The idea of adding randomization during data analysis to increase stability has been widely accepted. MacCoun et al. [34] believed: when deciding which results to report, the analyst interacts with a dataset that has been obfuscated through adding noise to observations, removing some data points, or switching data labels. The raw, uncorrupted, dataset is only used in computing the final reported values. Differential privacy mechanisms can follow the above rules to significantly improve learning stability.

3.3 Differential privacy in fairness

3.3.1 An overview of the fairness in learning

Fairness issues are prevalent in every facet of our lives including education, job application, the parole of prisoners and so on [35], [36], [37]. Instead of resolving fairness issues, modern AI techniques, however, can amplify social inequities and unfairness. For example, an automated hiring system may be more likely to recommend candidates from specific racial, gender or age groups [38], [39]. A search engine may amplify negative stereotypes by showing arrest-record ads in response to queries for names predominantly given to African-American babies but not for other names [40], [41]. Moreover, some software systems that are used to measure the risk of a person recommitting crime demonstrate a bias against African-Americans over Caucasians with the same profile [42], [43]. To address these fairness issues in machine learning, great effort has been placed on developing definitions of fairness [44], [45], [46] and algorithmic methods for assessing and mitigating undesirable bias in relation to these definitions [47], [48]. A typical idea is to make algorithms insensitive to one or multiple attributes of datasets, such as gender and race.

3.3.2 Applying differential privacy to improve fairness

Dwork et al. [49] classified individuals with the goal of preventing discrimination against a certain group while maintaining utility for the classifier. The key idea is to treat similar individuals similarly. To implement this idea, these researchers adopted the Lipschitz property, which requires that any two individuals, x and y, with a distance of $d(x, y) \in [0, 1]$ must map to the distributions $M(x)$ and $M(y)$, respectively, such that the statistical distance between $M(x)$ and $M(y)$ is at most $d(x, y)$ [50]. In other words, if the difference between x and y is $d(x, y)$, the difference of the classification outcomes of x and y is at most $d(x, y)$. A connection between differential privacy and the Lipschitz property has been theoretically established, in that a mapping satisfies differential privacy if, and only if, this mapping satisfies the Lipschitz property [49].

Zemel et al. [51] extended Dwork et al.'s [49] preliminary work by defining the metrics between individuals. They learned a restricted form of a distance function and formulated fairness as an optimization problem of finding the intermediate representation that best encodes the data. During the process, they preserved as much information about the individual's attributes as possible, while removing any information about membership with other protected subgroup. The goal was two-fold: first, the intermediate representation should preserve the data's original features as much as possible. Second, the encoded representation is randomized to hide whether or not the individual is from the protected group.

Both ideas take advantage of randomization in differential privacy. Considering an exponential mechanism with a carefully designed score function, the framework can sample fresh data from the universe to represent original data with the same statistical properties. However, the most challenging part of this framework is designing the score function. This is because differential privacy in fairness assumes that the similarity between individuals is given; however, estimating similarity between individuals in an entire feature universe is a tough problem. In other words, the evaluation of similarity between individuals is the key obstacle of model fairness, making score function design an obstinate problem. Therefore, differential privacy in model fairness needs further exploration.

Recently, researchers have attempted to adopt differential privacy to simultaneously achieve both fairness and privacy preservation [52], [53]. This research is motivated by settings where models are required to be non-discriminatory in terms of certain attributes, but these attributes may be sensitive and so must be protected while training the model [54]. Addressing fairness and privacy preservation simultaneously is challenging because they have different

aims [53], [55]. Fairness focuses on the group level and seeks to guarantee that the model's predictions for a protected group (such as female) are the same as the predictions made for an unprotected group. In comparison, privacy preservation focuses on the individual level. Privacy preservation guarantees that the output of a classification model is independent of whether any individual record is in or out of the training dataset. A typical solution to achieve fairness and privacy preservation simultaneously was proposed by Ding et al. [53]. Their solution is to add a different amount of differentially private noise based on different polynomial coefficients of the constrained objective function, where the coefficients relate to attributes in the training dataset. Therefore, privacy is preserved by adding noise to the objective function, and fairness is achieved by adjusting the amount of noise added to the different coefficients.

3.3.3 Summary of differential privacy in fairness

The best methods of similarity measurement and composition are open problems in fairness models. Further, differential privacy in fairness models has been directed toward classification problems. There are also some works on fairness in online settings such as online learning, bandit learning and reinforcement learning. However, how to use differential privacy mechanisms to benefit those online settings of fairness needs further investigation.

Composition fairness is also a big challenge. Here, fairness means that if each component in the algorithm satisfies the notion of fairness, the entire algorithm will satisfy the same [6]. This composition property is essential for machine learning, especially for online learning. Dwork et al. [56] explored this direction, finding that current methods seldom achieve this goal because classification decisions cannot be made independently, even by a fair classifier. Also, classifiers that satisfy group fairness properties may not compose well with other fair classifiers. Their results show that the signal provided by group fairness definitions under composition is not always reliable. Hence, further study is needed to figure out how to take advantage of differential privacy to ensure composition.

3.4 Summary of differential privacy in machine learning

Table 2 summarizes the papers that apply differential privacy to learning stability and fairness. From this summary, we can see that differential privacy can not only preserve privacy but also improve the stability and fairness in machine learning. The key idea of achieving stability is derived from allowing an analyst to access the testing set only in a differentially private manner. Likewise, the main idea of achieving fairness is also derived from randomly resampling fresh data from the data universe in a differentially private manner. The two examples show that the sampling from the data universe can improve the machine learning performance to some extent.

Even though differential privacy has been proven to guarantee privacy, stability and fairness in machine learning, there are still some open research issues. First, to preserve privacy, the utility of learning models is sacrificed to some extent. Thus, how to obtain an optimal trade-off between the privacy and the utility still needs further exploration. Second, current differentially private stable learning is suitable only for the learning models where loss functions do not have regularization. Differential privacy can provide additional generalization capability to the learning models who has limited regularization. Hence, improving generalization capability for regularized loss functions will be helpful. Third, the re-sampling in current fair learning is typically based on the exponential mechanism. Exponential mechanism requires the knowledge of the utility of each sample. This knowledge, however, may not be available or hardly be defined in some situations. Thus, new mechanisms are needed for today's fair learning.

Research on differential privacy in machine learning can be broadened to address other non-privacy issues. For example, differential privacy mechanisms may be able to generate new data samples based on existing ones by properly adding noise to the values of attributes in existing samples. These newly-generated samples may not be suitable for training data, but they can be used as testing data. Another example is that differential privacy mechanisms can be used for sampling. Sampling is an important step in deep reinforcement learning and batch learning. The small database mechanism may be a good tool for sampling in machine learning, as it can guarantee the desired accuracy while sampling only a small set of samples.

4 Differential Privacy in Deep Learning

Deep learning originated from regular neural networks but thanks to the availability of large volumes of data and advancements in computer hardware, implementing many-layered neural network models has become feasible, and these models significantly outperforms their predecessors. The latest deep learning algorithms have been successfully applied to many applications such as natural language processing, image processing, and speech and audio processing [57]. Differential privacy has been broadly used in deep learning to preserve data and model privacy. Thus, in this section, we mainly focus on analyzing the differential privacy in general deep neural networks, distributed deep learning [58] and federated learning [59].

4.1 Deep neural networks: attacks and defences

4.1.1 Privacy attacks in the deep neural networks

One of the most common privacy attacks is an inference attack where the adversary maliciously infers sensitive features and background information about a target individual from a trained model [60]. Typically, there are two types of inference attacks in deep learning.

The first type is a membership inference attack. The aim here is to infer whether or not a given record is in the present training dataset [61]. Membership inference attacks can be either black-box or white-box. Black-box means that an attacker can query a target model but does not know any other details about that model, such as its structure [62]. In comparison, white-box means that an attacker has full access to a target model along with some auxiliary information [63]. The attack model is based on the observation that machine learning models often behave differently on training data versus the data they "see" for the first time.

TABLE 2
Summary of differential privacy in machine learning

Papers	Research areas	Techniques used	Research aims	Advantages	Disadvantages
Dwork et al. [4], [31]	Stable learning	Laplace mechanism	Improve stability	Improve stability with little overhead	Limited access to testing dataset
Dwork et al. [49]	Fairness in learning	Concept of differential privacy	Improve fairness	Not only enforce fairness but also detect unfairness	An available similarity metric is assumed a prerequisite
Zemel et al. [51]	Fairness in learning	Concept of differential privacy	Improve fairness	Simultaneously encode and obfuscate data	Representation dependent
Xu et al. [52]	Fairness in learning	Laplace mechanism	Improve fairness and preserve privacy	Achieve both fairness and privacy	For logistic regression only
Jagielski et al. [54]	Fairness in learning	Laplace mechanism	Improve fairness and preserve privacy	Achieve both fairness and privacy	Need large dataset
Ding et al. [53]	Fairness in learning	Functional mechanism	Improve fairness and preserve privacy	Achieve both fairness and privacy	For logistic regression only

The second type of attack is an attribute inference attack. The aim of an attribute inference attack is to learn hidden sensitive attributes of a test input given access to the model and information about the non-sensitive attributes [64]. Fredrikson [64] describes a typical attribute inference attack method, which attempts to maximize the posterior probability estimate of the sensitive attributes based on the values of non-sensitive attributes.

4.1.2 Differential privacy in deep neural networks

Some of the properties of differential privacy are naturally resistant to membership and attribute inference attacks. An intuitive way to resist inference attacks is to properly add differentially private noise to the values of the sensitive attributes before using the dataset to train a model. In a typical deep learning algorithm, there are four places to add noise, as shown in Figure 5. The first place is the training dataset, where the noise is derived from an input perturbation mechanism. This operation occurs before the training starts and is usually done to resist attribute inference attacks.

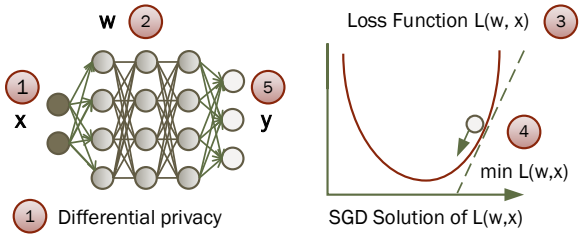


Fig. 5. Differential privacy in deep learning

The second place is the loss function, which yields an objective perturbation mechanism. This operation occurs during training and is usually done to resist membership inference attacks.

The third place is the gradients at each iteration, i.e., a gradient perturbation mechanism. Gradients are computed using the loss function to do partial-derivative against the weights of the deep neural network. Likewise, this operation occurs during training and is usually done to resist membership inference attacks.

The fourth place is the weights of the deep neural network, constituting the learned model, called an output perturbation mechanism. This operation happens once training is complete. The operation is easy to implement and can resist both membership and attribute inference attacks. However, directly adding noise to the model may significantly harm its utility, even if the parameter values in differential privacy have been carefully adjusted.

Of these four places, adding noise to the gradients is the most common method. However, because the gradient norm may be unbounded in deep learning, a bound must be imposed before applying gradient perturbation. A typical way is to manually clip the gradient at each iteration [65]. Such a clipping can also provide a sensitivity bound with differential privacy. Table 3 summarizes the properties of the mentioned attacks and their defence strategies.

From Table 3, we can see that adding noise to a dataset can defend against attribute inference attacks. Since the aim of attribute inference attacks is to infer the values of sensitive attributes, directly adding noise to these values is the most straightforward and efficient method of protecting them. However, this method may significantly affect the utility of the learned model, because it is heavily dependent on the values of the attributes in the training dataset, and using a dataset with modified attribute values to learn a model is similar to using a "wrong" dataset.

By comparison, adding noise to the loss function or gradient only slightly affects the utility of the learned model. This is because the noise is added during the training process and the model can be corrected by taking the noise into account. Adding noise to the loss function or gradient can resist membership inference attacks, which can be guaranteed by the properties of differential privacy. However, adding noise to the loss function or gradient does not offer much resistance to attribute inference attacks. As mentioned before, a typical attribute inference attack needs two pieces of information: 1) the underlying distribution of the training dataset; and 2) the values of non-sensitive attributes. These two pieces of information are not modified when adding noise to the loss function or gradient.

Finally, adding noise to the weights or classes of a neural network can resist both membership and attribute inference attacks. This is because adding noise to the weights will modify the learned model and both of these types of attacks need to access the learned model to launch an attack. The downside is that adding noise to a learned model after training may drastically affect its utility, and retraining the model will not correct the problem as noise simply needs to be added again. Noise could be added to the weights in each iteration of training. However, this method might

TABLE 3
Attacks and defense in deep learning

Noise	Membership inference attack	Attribute inference attack	Privacy guarantee	Performance impact
Dataset [66]		✓	very strong	high
Loss function [67]	✓		strong	low
Gradient [65], [68], [69]	✓		strong	low
Weights [70], [71]	✓	✓	very strong	very high
Classes [72], [73], [74]	✓	✓	very strong	low

affect convergence, since the output of the algorithm is computed based on the weights. Hence, if noise is added to each weight, the total amount of noise might become large enough to make the loss never convergent. Adding noise to the classes has the similar disadvantage for the same reason.

4.2 Differential privacy in distributed deep learning

4.2.1 Overview of distributed deep learning

Conventional deep learning is limited to a single-machine system, where the system has all the data and carries out the learning independently. Distributed deep learning techniques, however, accelerate the learning process. Two main approaches are applied in distributed deep learning: data parallelism and model parallelism [58]. In data parallelism, a central model is replicated by a server and distributed to all the clients. Each client then trains the model based on her own data. After a certain period of time, each client summarizes an update on top of the model and shares the update to the server. The server then synchronizes the updates from all the clients and improves the central model. In model parallelism, all the data are processed with one model. The training of the model is split between multiple computing nodes, with each computes only a subset of the model. As data parallelism can intrinsically protect the data privacy of clients, most research on distributed deep learning focuses on data parallelism.

4.2.2 Differential privacy in distributed deep learning

As mentioned in the previous subsection, differentially private noise can be added to five places in a deep neural network. The following review is divided into methods based on adding noise.

Adding noise to input datasets. Heikkila et al. [66] proposed a general approach for privacy-preserving learning in distributed settings. Their approach combines secure multi-party communication with differentially private Bayesian learning methods so as to achieve distributed differentially private Bayesian learning. In their approach, each client i adds a Gaussian noise to her data and divides them and the noise into shares. Each share is then sent to a server. In this way, the sum of the shares discloses the real value, but separately they are just random noise.

Adding noise to loss functions. Zhao et al. [67] proposed a privacy-preserving collaborative deep learning system that allows users to collaboratively build a collective learning model while only sharing the model parameters, not the data. To preserve the private information embodied in the parameters, a functional mechanism, which is an extended version of the Laplace mechanism, was developed to perturb the objective function of the neural network.

Adding noise to gradients. Shokri and Shmatikov [68] designed a system that allows participants to independently train on their own datasets and share small subsets of their models' key parameters during training. Thus, participants can jointly learn an accurate neural network model without sharing their datasets, and can also benefit from the models of others to improve their learning accuracy while still maintaining privacy.

Abadi et al. [65] developed a differentially private stochastic gradient descent algorithm for distributed deep learning. At each iteration during the learning, Gaussian noise is added to the clipped gradient to preserve privacy in the model. In addition, their algorithm also involves a privacy accountant and a moment accountant. The privacy accountant computes the overall privacy cost during the training, while the moment accountant keeps track of a bound on the moments of the privacy loss random variable.

Cheng et al. [69] developed a privacy-preserving algorithm for distributed learning based on a leader-follower framework, where the leaders guide the followers in the right direction to improve their learning speed. For efficiency, communication is limited to leader-follower pairs. To preserve the privacy of leaders, Gaussian noise is added to the gradients of the leaders' learning models.

Adding noise to weights. Jayaraman et al. [70] applied differential privacy with both output perturbation and gradient perturbation in a distributed learning setting. With the output perturbation, each data owner combines their local model with a secure computation and adds Laplace noise to the aggregated model estimator before revealing the model. With the gradient perturbation, the data owners collaboratively train a global model using an iterative learning algorithm, where, at each iteration, each data owner aggregates their local gradient within a secure computation and adds Gaussian noise to the aggregated gradient before revealing the gradient update.

Phan et al. [71] proposed a heterogeneous Gaussian mechanism to preserve privacy in deep neural networks. Unlike a regular Gaussian mechanism, this heterogeneous Gaussian mechanism can arbitrarily redistribute noise from the first hidden layer and the gradient of the model to achieve an ideal trade-off between model utility and privacy loss. To obtain the property of arbitrary redistribution, a noise redistribution vector is introduced to change the variance of the Gaussian distribution. Further, it can be guaranteed that, by adapting the values of the elements in the noise redistribution vector, more noise can be added to the more vulnerable components of the model to improve robustness and flexibility.

Adding noise to output classes. Papernot et al. [72] de-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TKDE.2020.3014246, IEEE Transactions on Knowledge and Data Engineering

veloped a model called Private Aggregation of Teacher Ensembles (PATE) which has been successfully applied to generative adversarial nets (GAN) for privacy guarantees [75]. PATE consists 1) an ensemble of n teacher models; 2) an aggregation mechanism; and 3) a student model. Each teacher model is trained independently on a subset of private data. To protect the privacy of data labels, Laplace noise is added to the output classes, i.e., the teacher votes. Last, the student model is trained through knowledge transfer from the teacher ensemble with the public data and privacy-preserving labels. Later, Papernot et al. [73] improved the PATE model to make it applicable to large-scale tasks and real-world datasets. Zhao [74] also improved the PATE model by extending it to the distributed deep learning paradigm. Each distributed entity uses deep learning to train a teacher network on private and labeled data. The teachers then transfer the knowledge to the student network at the aggregator level in a differentially-private manner by adding Gaussian noise to the predicted output classes of the teacher networks. This transfer uses non-sensitive and unlabeled data for training.

4.2.3 Summary of differential privacy in distributed deep learning

Although a number of privacy-preserving methods have been proposed for distributed deep learning, there are still some challenging issues that have not yet been properly addressed. The first issue is synchronization. If data parallelism has too many training modules, it has to decrease the learning rate to ensure a smooth training procedure. Similarly, if model parallelism has too many segmentations, the output from the nodes will reduce training efficiency [58]. Differential privacy offers potential for solving this issue. Technically, the challenge is a coordination problem, where modules or nodes collaboratively perform a task, but each has a privacy constraint. This coordination problem can be modeled as a multi-player cooperative game, and differential privacy has been proven as effective for achieving equilibria in this game [76].

The second issue is collusion. Most of the existing methods assume non-collusion between multiple computation parties. This assumption, however, may fail in some situations. For example, multiple service providers may collude to obtain a user's private information. Joint differential privacy may be able to address this issue, as it has been proven to successfully protect any individual user's privacy even if all the other users collude against that user [77].

The third issue is privacy policies. Most existing methods rely on privacy policies that specify which data can be used by which users according to what rules. However, there is no guarantee that all the users will strictly follow the privacy policies. Differential privacy may be available to deal with this issue, as differential privacy can guarantee users will truthfully report their types and faithfully follow the recommendations given by the privacy policies.

4.3 Differential privacy in federated learning

4.3.1 Overview of federated learning

Federated learning enables individual users to collaboratively learn a shared prediction model while keeping all the training data on the users' local devices. Federated learning was first proposed by Google in 2017 as an additional approach to the standard centralised machine learning approaches [78], and has been applied to several real-world applications [79].

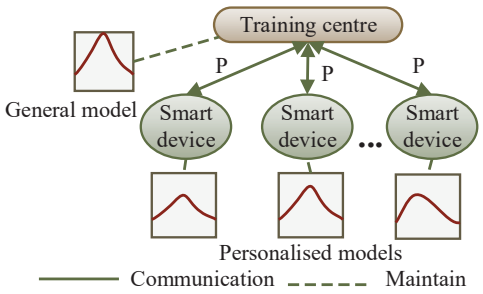


Fig. 6. Federated Learning Framework

Fig. 6 shows the structure of a simple federated learning framework. First, the training centre distributes a general learning model, trained on general data, to all the smart devices in the network. This model is used for general purposes, such as image processing. In a learning iteration, each user downloads a shared model from the training centre to their local device. Then, they improve the downloaded model by learning from their own local data. Once complete, the changes to each user's local model are summarized as a small update, which is sent to the training centre through a secure communication channel. Once the cloud server receives all the updates, the shared model is improved wholesale. During the above learning process, each user's data remain on their own device and is never shared with either the training centre or another user.

However, although private user data cannot be directly obtained by others, it may be indirectly leaked through the updates. For example, the updates of the parameters in an optimization algorithm, such as stochastic gradient descent [80], may leak important data information when exposed together with data structures [81]. Differential privacy can, however, resolve this problem, as explained next.

4.3.2 Applying differential privacy in federated learning

Although no training data is transferred from mobile devices to the cloud centre in federated learning, simply keeping data locally does not provide a strong enough privacy guarantee when conventional learning methods are used. For example, adversaries can use differential attacks to discover what data was used during training through the parameters of the learning model [2]. To protect against these types of attacks, several algorithms that incorporate differential privacy have been proposed that ensure a learned model does not reveal whether the data from a mobile device was used during training [82].

Adversaries can also interfere with the messages exchanged between communicating parties, or they can collude among communicating parties during training to attack the accuracy of the learning outcomes. To ensure the resulting federated learning model maintains acceptable prediction accuracy, approaches using both differential privacy mechanisms and secure multiparty computation

frameworks have been created, providing formal data privacy guarantees [83].

Geyer et al. [2] incorporated differential privacy mechanisms into federated learning to ensure that whether an individual client participates in the training cannot be identified. This approach protects the entire data of an individual client. To achieve this aim, in each communication round, a subset of the total clients is randomly selected. Then, the difference between the central model and each of the selected client's local model is calculated, and Gaussian noise is added to the difference.

Shi et al. [84] investigated a distributed private data analysis setting, where multiple mutually distrustful users co-exist and each of them has private data. There is also an untrusted data aggregator in the setting who wishes to compute aggregate statistics over these users. The authors adopted computational differential privacy to develop a protocol, which can output meaningful statistics with a small total error even when some of the users fail to respond. Also, the protocol can guarantee the privacy of honest users, even when a portion of the users are compromised and colluding.

Agarwal et al. [85] combined two aspects of distributed optimization in federated learning: 1) quantization to reduce the total communication cost; and 2) adding Gaussian noise to the gradient before sending the result to the central aggregator to preserve the privacy of each client.

4.3.3 Summary of differential privacy in federated learning

The main advantage of the federated leaning model is that none of the training data needs be transferred to the cloud centre which satisfies the basic privacy concerns of mobile device users can be satisfied. However, federated learning has some unique challenges, mainly in the following three respects:

- Issues related to attacks on various vulnerabilities of the federated learning model and the countermeasures to defend against these attacks. For example, adversaries can use differential attacks to determine which mobile users have been included in the learning process [86]; messages can be tampered with; and adversaries can use model poisoning attacks to cause the model to misclassify a set of chosen inputs with high confidence [87], [88].
- Issues related to the learning algorithms, such as the requirements of accuracy, scalability, efficiency, fault-tolerance, etc. [78], [89].
- Issues related to the structure of the federated learning system, including its communication efficiency, the computational and power limitation of the mobile devices, the reliability of the mobile devices and communication system, etc. [86]. This issue can potentially be tackled through the composition property of differential privacy by fixing the privacy budget and forcing all communications to consume that budget.

To effectively use federated learning in various applications, we first need to overcome the challenges related to attacks, the system structures, and the learning algorithms. Therefore, intensive research addressing these challenges will be required in the near future. The second future development will be to explore the power and benefits of federated learning for both new and existing applications, especially now that mobile devices are ubiquitous. The third future development will be the automation of tools that use federated learning and the emergence of companies providing such services to meet the various needs of business and individual customers.

4.4 Summary of differential privacy in deep learning

Table 4 summarizes the papers that apply differential privacy to distributed deep learning and federated learning. In this summary, we can see that most of these papers make use of the Gaussian mechanism. This is because the probability density function of the Gaussian distribution is differentiable, and this property is necessary for calculating the gradient of a learning model. The Laplace mechanism does not have this property, so that it was seldom to be applied in deep learning.

It is worth pointing out that simply using differential privacy mechanisms during a learning process may not provide enough security to protect the privacy of a learning model or the training data. This is because an adversary, who is pretending to be an honest participant, can use a GAN [10] to generate prototypical samples of a victim's private training dataset, and because the generated samples have the same distribution as the victim's training dataset, the adversary can bypass the protection of differential privacy [90]. A potential solution against this security issue is to use local differential privacy. Unlike regular differential privacy which takes into account all users' data in a dataset, local differential privacy add randomization on single user's data [91]. Thus, local differential privacy has a finer granularity and stronger privacy guarantee. Even if an adversary has the access to the personal responses of an individual user in the dataset, the adversary is still unable to learn accurate information about the user's personal data.

Moreover, there are two urgent research problems which need further investigation. The first direction is model inversion attack and its defense [92], [93]. Model inversion attacks aim to infer the training data from a target model's predictions. To implement model inversion attacks, a popular method is to train a second model called attack model [93]. The attack model takes the target model's predictions as input and outputs reconstructed data which are expected to be very similar to the training data of the target model. Most of existing defense methods focus only on membership inference attacks so that their effectiveness on model inversion attacks is still unclear. A potential defense method against model inversion attacks is to adopt differential privacy to modify the target model's predictions. The major reason of the success of model inversion attacks is owning to the redundant information contained in the target model's predictions. Thereby, if this redundant information can be destroyed, the attacks can be effectively defended.

The second direction is the client accuracy in federated learning. In regular federated learning, the server takes the updates from all clients equally, aiming to minimize an aggregate loss function in general. However, minimizing an aggregate loss function cannot guarantee the accuracy of

TABLE 4
Summary of differential privacy in deep learning

Papers	Research areas	Techniques used	Research aims	Advantages	Disadvantages
Papernot et al. [72]	Deep learning	Laplace mechanism	Preserve privacy	Independent of learning algorithms	Suitable only for small-scale tasks
Papernot et al. [73]	Deep learning	Gaussian mechanism	Preserve privacy	Suitable for large-scale tasks	Need two aggregators
Shokri et al. [68]	Distributed deep learning	Sparse vector technique	Preserve privacy	Preserve the privacy of participants without sacrificing the accuracy of resulting models	Vulnerable to Generative Adversarial Network -based attacks [90]
Abadi et al. [65]	Distributed deep learning	Gaussian mechanism	Preserve privacy	Preserve the privacy of deep neural networks with non-convex objectives	Effective in a limited number of deep neural networks
Heikkila et al. [66]	Distributed deep learning	Gaussian mechanism	Preserve privacy	Achieve DP in distributed settings	Sacrifice learning performance
Cheng et al. [69]	Distributed deep learning	Gaussian mechanism	Preserve privacy	Low differential privacy budget and high learning accuracy	High communication overhead
Zhao [74]	Distributed deep learning	Gaussian mechanism	Preserve privacy	Use the teacher-student paradigm to improve learning performance	High communication overhead
Jayaraman et al. [70]	Distributed deep learning	Zero-concentrated DP mechanism	Preserve privacy	Both output and gradient are protected with reduced noise	Data owners' utility cannot be maximized
Zhao et al. [67]	Distributed deep learning	Exponential and Laplace mechanism	Preserve privacy and improve stability	Preserve the privacy of collective deep learning systems with the existence of unreliable participants	Accuracy is less than the centralized methods
Phan et al. [71]	Distributed deep learning	Gaussian mechanism	Preserve privacy	Achieve tight robustness bound	Model accuracy is sacrificed
Geyer et al. [2]	Federated learning	Gaussian mechanism	Preserve privacy	Balance tradeoff between privacy loss and model performance	Model performance depends on the number of clients
Shi et al. [84]	Federated learning	Concept of differential privacy	Preserve privacy	No P2P communication and fault tolerance	Focus only on multi-input functions
Agarwal et al. [85]	Federated learning	Gaussian and binomial mechanisms	Preserve privacy	Achieve both communication efficiency and differential privacy	The analysis of binomial mechanism may not be tight

individual clients in the federated network [94], [95], which is unfair to the clients. To improve the learning accuracy of the clients, Li et al. [95] introduce an aggregate re-weighted loss function in federated learning, where different clients are allocated different weights. A limitation in this type of method is that the server still need to send all the clients the same model update. This limitation could be overcome by enabling the server to send different model updates to different clients according to each client's requirements. The server could use joint differential privacy [76] to differentiate the model updates in federated learning.

5 Differential Privacy in Multi-Agent Systems

A multi-agent system is a loosely coupled group of agents, such as sensor networks [96], power systems [97] and cloud computing [98], interacting with one another to solve complex domain problems [99], [100]. An agent is an intelligent entity that can perceive its environment and act upon the environment through actuators. Currently, multi-agent systems face challenges with privacy violation, security issues and communication overhead.

In Mcsherry et al.'s early work [14], differential privacy mechanisms were applied to auctions to diminish the impact of untrusted participants. In multi-agent systems, differential privacy mechanisms can also avoid malicious agents through a similar mechanism. There is an increasing trend to apply differential privacy techniques to multi-agent systems so as to preserve the agents' privacy [101] or improve the agents' performance [102]. This section focuses on some key sub-areas of multi-agent systems, including multi-agent learning, auction, and game theory.

5.1 Differential privacy in multi-agent reinforcement learning

Multi-agent learning is generally based on the reinforcement learning [103]. Normally, an agent learns proper behavior through the interactions with their environment and other agents in a trial-and-error manner. Every time an agent performs an action, they receive a reward which tells them how good that action was for accomplishing the given goal. Importantly, agents can and do change their strategy to get or better rewards. Therefore, the aim of the agent is to maximize its long-term expected reward by taking sequential actions.

For example, Figure 7 shows a set of sweeper robots (the agents with smiling or crying faces) who are collecting rubbish from a grid (the red diamonds). When a robot plans to move to the corner of the grid, it may try to move to the right first. However, if it bumps into the wall, it receives a very low reward; thus, the robot learns that moving to the right from its current location is not a good idea.

Standard multi-agent learning approaches may need a large number of interactions between agents and an environment to learn proper behaviors [104]. Therefore, to improve agent learning performance, agent advising was proposed, where agents are allowed to ask for advice from each other [105]. For example, the robot in position $(1, 1)$ in Fig. 7 can ask its neighbor in $(2, 2)$ for advice and may obtain the knowledge that it cannot move to the left from its current location.

Existing agent advising approaches, however, suffer from malicious agents who may provide false advice to hinder the performance of the system, and heavy communi-

cation overheads [106], [107] because agents are allowed to broadcast to all their neighboring agents for advice [106], [107]. For example, in Figure 7, the malicious robot (the crying face) may provide false information to the other robots so that the rubbish is not collected in time.

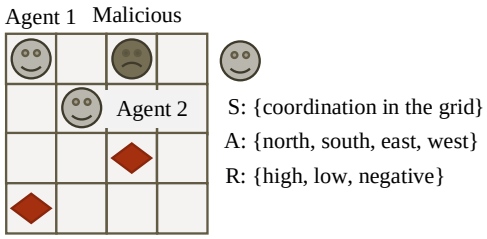


Fig. 7. A multi-agent learning example

5.1.1 Differential privacy to improve the security of the reinforcement learning

Differential privacy mechanisms can provide a security guarantee that a malicious agent being in or out of a multi-agent system has little impact on the utility of other agents. As the probability of selecting neighbors to ask for advice is based on the reward history provided by neighbors, exponential or Laplace mechanisms can be applied to this step to diminish the impact of malicious agents on security purpose. Moreover, the composition of the privacy budget can naturally control the communication overhead, namely by limiting the amount of advice allowed throughout the whole system.

Ye et al. [8] proposed a differentially private framework to deal with malicious agents and communication overhead problems. Using Fig. 7 as an example, suppose each agent in the grid environment wants to move to the corner and has the moving knowledge that can be shared with others.

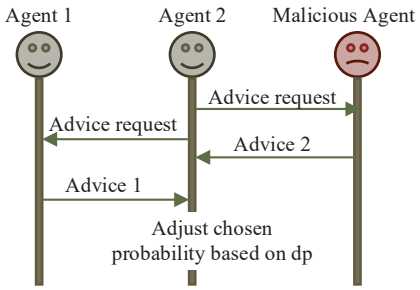


Fig. 8. Differentially private multi-agent system

Fig. 8 illustrates the process of agent interaction in this example. Agent 2 send out an advice request to its neighbors. Agent 1 and the malicious agent would give advice to agent 2. Agent 1's advice will include the best action in agent 2's state according to agent 1's knowledge. However, the malicious agent will always give false advice. After receiving advice from both neighbors, agent 2 performs a differentially private adviser selection algorithm, which applies an exponential mechanism to adjust the chosen probabilities. Because the malicious agent always provides false advice, the exponential mechanism may filter its advice with a high probability. So that the impact of the malicious agent will be diminished. The system will stop communicating when the privacy budget is used up, so that the privacy budget can be used to control the communication overhead.

5.1.2 Summary of differential privacy in reinforcement learning

Differential privacy technology has been proven to improve the performance of agent learning in addition to its use as a privacy-preservation tool. Compared to the benchmark broadcast-based approach, the differential privacy approach achieves a better performance (normally evaluated by the total reward of the system and the convergence rate) with less communication overhead when malicious agents are present. However, further exploration of differential privacy technique in new environments, such as a dynamic or an uncertain environment, would be worthwhile.

5.2 Differential privacy in auction

Auction-based approaches are effective in multi-agent systems for task and resource allocation [108]. Normally, there are three parties in an auction, including a seller, an auctioneer and a group of buyers. The auctioneer presents the item and receives bids from the buyers following a pre-established bidding convention. This convention determines the sequence of bids as well as the way to decide the winner and the price. The current privacy-preserving mechanisms are mainly based on cryptography and multi-party secure computation. However, there may still be privacy leaks if one infers their sensitive information from the auction's outcomes. Differential privacy techniques can help to combat this issue [109]. The current differentially private auction mechanisms are mostly designed for spectrum allocation in wireless communication. Radio spectrum is a scarce resource and thus, the allocation of it needs to be managed carefully. However, communication also comes with a high desirability for security, resulting in several private spectrum auction mechanisms.

Zhu et al. [110] proposed a differentially private spectrum auction mechanism with approximate revenue maximization. Their mechanism consists of three steps. First, the auctioneer partitions the bidders into groups and subgroups. Second, the auctioneer initializes the set of prices and calculates the probability distribution over these prices using the exponential mechanism. Finally, based on the probability distribution, the auctioneer randomly selects a price as the auction payment, and the corresponding bidders are pronounced the winners.

Zhu and Shin [111] alternative achieves strategy-proofness and is polynomially tractable. The mechanism performs an auction in four steps. The auctioneer first partitions bidders into groups. The auctioneer then creates virtual channels for bidders based on their geographical locations and a conflict graph. Next, the auctioneer computes the probability of selecting each bidder as the winner. Finally, the auctioneer selects the winner based on an exponential mechanism and determines the payment for the winner.

Wu et al. [112] developed a differentially private auction mechanism which guarantees bid privacy and achieves approximate revenue maximization. In their mechanism, the

auctioneer first groups bidders based on their conflict graph, and next determines the price for winners in each group using an exponential mechanism. Finally, the auctioneer selects the winner based on sorted group revenues.

Chen et al. [109] designed a differentially private double spectrum auction mechanism. Their mechanism is a uniform price auction mechanism, where all sellers are paid with a selling clearing price and all buyers groups are charged with a buying clearing price. They apply an exponential mechanism twice, once to select a selling clearance price and again to select a buying clearance price.

In addition to spectrum allocation, differentially private auction mechanisms have also been developed for resource allocation in cloud computing. Xu et al. [113] proposed a differentially private auction mechanism for trading cloud resources, which preserves the privacy of individual bidding information and achieves strategy-proofness. Their mechanism iteratively progresses through a set of rounds, where each round consists of four steps. The auctioneer first uses the exponential mechanism to compute the probability distribution over the set of current bids. Next, the auctioneer randomly selects a bid from the set as the winner in the current round. The auctioneer then creates a payment scheme for the winner. Finally, the winner is removed from the set.

5.2.1 Summary of differential privacy in auctions

Although differential privacy in auctions has been widely accepted, these approaches typically assume a seller or an auctioneer can directly interact with all potential buyers. This assumption, however, may not be applicable to some real situations, where sellers and buyers are organized in a network, e.g., social networks [114], [115]. Auctions in social networks introduce new challenging privacy issues.

The first issue is the bidding propagation. In a social network, a bid from a buyer cannot be sent directly to the seller but has to be propagated by other agents to the seller. These intermediate agents may be potential buyers and are thus competitive to that buyer. Therefore, the bid value of that buyer is private and cannot be disclosed to others. An intuitive way to protect the privacy of that buyer is to add Laplace noise to the bid value. However, this does not stop the problem of a seller receiving a fake bid and making a wrong decision.

The second issue is social relationships. During bid propagation, a trajectory forms which indicates who is engaged in the propagation. By investigating this trajectory, the seller may learn things about the buyer's social relationships.

5.3 Differential privacy in game theory

Game theory is a mathematical model used to study the strategic interaction among multiple agents or players [116]. Game theory has been broadly studied and applied in various domains, e.g., economic science [117], social science [116] and computer science [118]. Most of these studies, however, overlook the privacy of agents, the malicious agents or the stability of the game playing process. To tackle these issues, differential privacy techniques have been introduced into game theory [119], [120], [121].

Differential privacy-based game theory research can be roughly classified into two categories: 1) using differential privacy to improve the performance of game theory, e.g., stability and equilibrium, and 2) applying differential privacy to preserve the privacy of agents in games.

5.3.1 Differential privacy to improve the performance

Kearns et al. [76] developed a differentially private recommender mechanism for incomplete information games. Thanks to differential privacy techniques, their mechanism achieves equilibria of complete information games even with a large number of players and any player's action only slightly affects the payoffs for other players. Their mechanism offers a proxy that can recommend actions to players. Players are free to decide whether to opt in to the proxy, but if players do opt in, they must truthfully report their types. In addition to satisfy the game-theoretic properties, the mechanism also guarantees player privacy, namely that no group of players can learn much about the type of any player outside the group.

Rogers and Roth [122] improved the performance and defense of malicious users by expanding on Kearns et al.'s work [76] to allow players to falsely report their types even if the players opt in to the proxy. They theoretically show that by using differential privacy to form an approximate Bayes-Nash equilibrium, players have to truthfully report their types and faithfully follow the recommendations.

Pai et al. [102] improved game performance as well. They studied infinitely repeating games of imperfect monitoring with a large number of players, where players observe noisy results, generated by differential privacy mechanisms, about the play in the last round. The authors find that, theoretically, folk theorem equilibria may not exist in such settings, which concern all the Nash equilibria of an infinitely repeated game. Based on this finding, they yield antifolk theorems [123], where restrictions are imposed on the information pattern of repeated games such that individual deviators cannot be identified [124].

Lykouris et al. [125] increased game stability by analyzing the efficiency of repeated games in dynamically changing environments and population sizes. They draw a strong connection between differential privacy and the high efficiency of learning outcomes in repeated games with frequent change. Here, differential privacy is used as a tool to find solutions that are close to optimal and robust to environmental changes.

Han et al. [126] developed an approximately truthful mechanism to defend against malicious users in an application to manage the charging schedules of electric vehicles. To ensure users to truthfully report their specifications, their mechanism takes advantage of joint differential privacy which can limit the sensitivity of the scheduling process to changes in user specifications. Therefore, any individual user cannot benefit from misreporting his specification, which results in truthful reports.

5.3.2 Applying differential privacy to preserve the privacy

Hsu et al. [127] modelled the private query-release problem in differential privacy as a two-player zero-sum game between a data player and a query player. Each element of the data universe for the data player is interpreted as an action. The data player's mixed strategy is a distribution over her databases. The query player has two actions for each query.

The two actions are used to penalize the data player, when the approximate answer to a query is too high or too low. An offline mechanism, based on the Laplace mechanism, is then developed to achieve the private equilibrium of the game.

Zhang et al. [77] developed a general mobile traffic offloading system. They used the Gale-Shapley algorithm [128] to optimize the offloading station allocation plan for mobile phone users. In this algorithm, to protect users' location privacy, they proposed two differentially private mechanisms based on a binary mechanism [129]. The first mechanism is able to protect the location of privacy of any individual user when all the other users are colluding against this user, but the administrator is trusted. The second mechanism is stronger than the first mechanism because it assumes that even the administrator is untrusted.

Zhou et al. [130] adopted an aggregation game to model spectrum sharing in large-scale and dynamic networks, where a set of users compete for a set of channels. They then applied differential privacy techniques to guarantee the truthfulness and privacy of the users. Specifically, they use a Laplace mechanism to add noise to the cost threshold and users' costs to protect this information. Moreover, they use an exponential mechanism to decide the mixed strategy aggregative contention probability distribution for each user so as to preserve the privacy of users' utility functions.

5.3.3 Summary of differential privacy in game theory

The current research on differential privacy in game theory has mainly focused on static environments. These same issues in dynamic environments are generally still open. Of the little research that does consider dynamic environments [125], only changes in population are considered while overlooking changes in other areas, such as the strategies available to each agent or the utility of each of those strategies. Studying game theory with changing available strategies is a challenging issue, as these types of changes may result in no equilibria between agents. This is because no matter which strategy is taken by an agent, other agents may always have strategies to defeat that agent. In other words, other agents are incentivized to unilaterally change their strategies. However, since differential privacy can be used to force agents to report truthfully, it may also be used to force agents to reach equilibria.

5.4 Summary of multi-agent systems

Table 5 summarizes the papers that apply differential privacy to multi-agent systems. In this summary, three important facts are involved. First, some of these papers use differential privacy not to preserve the privacy of agents but for other aims, e.g., avoiding malicious agents and improving agents' performance. This implies that the differential privacy technique is able to achieve other research aims besides privacy preservation. In keeping with this spirit, more potential applications of differential privacy are worthy of research. Second, by using differential privacy, the common disadvantage is that only approximate optimal results can be achieved. Thus, more efficient differential privacy mechanisms need to be developed.

Third, most of these papers involve agent interaction; and differential privacy is adopted to guarantee the privacy of interaction information. Therefore, other multi-agent research, which involves agent interaction, may also enjoy the benefits of differential privacy and deserves further investigation. For example, multi-agent negotiation enables multiple agents to alternatively provide offers to reach agreements on given events or goods [131]. However, offers may explicitly or implicitly contain agents' sensitive information, e.g., commercial secrets, which should be protected. Another example is multi-agent resource allocation. To allocate resources fairly, agents have to reveal their preference over different types of resources to others [132]. The preference, however, might be what the agents incline to hide. In summary, differential privacy has a great potential to solve diverse problems in multi-agent system.

6 Future Research Directions

6.1 Private transfer learning

In addition to introducing differential privacy into standalone machine learning, differentially private transfer learning has also been investigated [133], [134]. Transfer learning aims to transfer knowledge from source domains to improve learning performance in target domains [134]. It is typically used to handle the situation that data are not stored in one place but distributed over a set of collaborative data centers [135], [136]. For example, transfer learning can be used in speech recognition to transfer the knowledge of connectionist temporal classification model to the target attention-based model to overcome the problem of limited speech resource in the target domain [137]. Transfer learning can also be used in recommendation systems to address the data-sparsity issue by enabling knowledge to be transferred among recommendation systems [138]. Instead of transferring raw data, the intermediate computation results are transferred from source domains to target domains. However, even the intermediate results are potentially vulnerable to privacy-breach [139], which is the motivation of privacy-preserving transfer learning.

6.2 Deep reinforcement learning

Deep reinforcement learning is a combination of reinforcement learning and deep learning [140], and could be used to solve a wide range of complex decision-making problems that were previously beyond the capability of regular reinforcement learning. The learning process of deep reinforcement learning is similar to regular reinforcement learning in that both are based on trial-and-error. However, unlike regular reinforcement learning which may use a reward value table (Q-table) to store learned knowledge, deep reinforcement learning uses a deep Q-network instead. One of the advantages of using a deep Q-network is that deep reinforcement learning can take high-dimensional and continuous states as inputs, which is close to unfeasible with regular reinforcement learning.

Differential privacy in deep reinforcement learning has not been researched thoroughly. Wang and Hegde [141] applied differential privacy to deep reinforcement learning to protect the value function approximator by adding Gaussian to the objective function, but their work still focuses on the "deep learning" aspects of the approach

TABLE 5
Summary of differential privacy in multi-agent systems

Papers	Research areas	Techniques used	Research aims	Advantages	Disadvantages
Ye et al. [8]	Multi-agent learning	Laplace mechanism	Avoid malicious agents	Avoid malicious agents with low communication and computation overhead	Malicious agents cannot be identified
Zhu et al. [110]	Auction in spectrum	Exponential mechanism	Preserve privacy	Guarantee both the truthfulness of bidders' valuations and their privacy	Only approximate revenue maximization
Zhu and Shin [111]	Auction in spectrum	Exponential mechanism	Preserve privacy	Preserve the privacy of both bidders and the auctioneer together	Only near optimal revenue achieved
Wu et al. [112]	Auction	Exponential mechanism	Preserve privacy	Guarantee both bid privacy and fairness	Only approximate revenue maximization
Chen et al. [109]	Auction in spectrum	Exponential mechanism	Preserve privacy	Preserve the privacy of bidders in double spectrum auctions	Only approximate social welfare maximization
Xu et al. [113]	Auction in cloud computing	Exponential mechanism	Preserve privacy	Preserve the privacy of consumers in cloud environments	Only approximate truthfulness and revenue maximization guarantees
Hsu et al. [127]	Game theory in databases	Laplace mechanism	Preserve privacy	Preserve the privacy of both individuals and analysts of database systems	Achieve only nearly optimal error rates
Kearns et al. [76]	Game theory	Concept of differential privacy	Preserve privacy and Improve performance	Implement equilibria of complete information games in settings of incomplete information	The type of a player is still possible to be revealed
Rogers and Roth [122]	Game theory	Concept of differential privacy	Preserve privacy and avoid malicious agents	Implement equilibria of complete information games in settings of incomplete information even if players are lying	The type of a player is still possible to be revealed
Zhang et al. [77]	Game theory in mobile communication	Binary mechanism	Preserve privacy	Preserve each user's location privacy even if other users collude	The system administrator is required to be honest or semi-honest
Zhou et al. [130]	Game theory in spectrum sharing	Laplace and exponential mechanisms	Preserve privacy	Guarantee both truthfulness and privacy of users	Achieve only approximate Nash equilibrium
Pai et al. [102]	Game theory	Concept of differential privacy	Improve performance	Quantify limit results for repeated games	Achieve only approximate equilibria
Lykouris et al. [125]	Game theory	Concept of differential privacy	Improve stability	Connect differential privacy with learning efficiency in dynamic games	The solution is approximate optimal
Han et al. [126]	Game theory in electric vehicles	Laplace mechanism	Avoid malicious agents	Reduce the incentive of user misreporting	Achieve only approximate truthfulness

rather than the "reinforcement learning" parts. Compared to standard reinforcement learning and deep learning, deep reinforcement learning has some unique features. First, the training samples are collected during learning rather than pre-assembled before learning. Second, the training samples may not be independent but rather highly correlated. Third, the training samples are not usually labelled. Thus, to avoid overfitting with deep reinforcement learning, experience replay is required, which means randomly selecting a set of samples for training in each iteration. As discussed in the previous sections, differential privacy can improve the stability of learning. Therefore, it may be interesting to research whether introducing differential privacy into deep reinforcement learning can help to avoid overfitting.

6.3 Meta-learning

Meta-learning, also known as 'learning to learn', is a learning methodology that systematically observes how different machine learning approaches perform on a wide range of learning tasks and then learning from these observations [142], [143], [144]. In meta-learning, the goal of the trained model is to quickly learn a new task from a small amount of new data. Also, the trained model should be able to learn on a number of different tasks [145], [146], but this opens the risk of breaching the privacy of the different task owners [147].

Recently, Li et al. [147] introduced differential privacy into meta-learning to preserve the privacy of task owners. Specifically, they use a certified (ϵ, δ)-differential privacy stochastic gradient descent [148] with each task, which guarantees that the contribution of each task owner carries global differential privacy guarantees with respect to the meta-learner. However, to guarantee global differential privacy, the number of tasks has to be known beforehand. This is hard to know in some situations, such as online meta-learning where tasks are revealed one after the other in a dynamic manner [149]. Therefore, it would be worthwhile developing a new differential privacy-based algorithm to preserve the privacy of task owners in online meta-learning,

6.4 Generative adversarial networks

Generative adversarial networks (GANs) [10] are a framework for producing a generative model by way of a two-player minimax game. One player is the generator who attempts to generate realistic data samples by transforming noisy samples drawn from a distribution using a transformation function with learned weights. The other player is the discriminator who attempts to distinguish between synthetic data samples created by the generator.

The GAN framework is one of the most successful learning models and has been applied to applications such as imitating expert policies [150] and domain transfer [151]. More

recently, GANs have been extended to accommodate multiple generators and discriminators so as to address more complex problems. Like other learning models, GAN frameworks also suffer from the risk of information leaks. More specifically, the generator model estimates the underlying distribution of a dataset and randomly generates realistic samples, which means the generator, through the power of deep neural networks, remembers training samples. Now, when the GAN model is applied to a private or sensitive dataset, the privacy of the dataset may be leaked. To deal with this problem, Xu et al. proposed a GAN-obfuscator [152], i.e., a differentially private GAN framework, where carefully designed Gaussian noise is added to the gradients of learning models during the learning procedure. By using the GAN-obfuscator, an unlimited amount of synthetic data can be generated for arbitrary tasks without disclosing the privacy of training data. However, although the framework can guarantee the privacy of training data, there is only one generator and one discriminator in this framework. Therefore, a useful direction of future research might be to extend these principles to multiple generators and discriminators to address more complex problems.

6.5 Multi-agent systems

6.5.1 Multi-agent advising learning

When an agent is in an unfamiliar state during a multi-agent learning process, it may ask for advice from another agent [106]. These two agents then form a teacher-student relationship. The teacher agent offers advice to the student agent about which action should be taken. Existing research is based on a common assumption that the teacher agent can offer advice only if it has visited the same state as the student agent's current state. But this assumption might be relaxed by using differential privacy technique.

The property of differential privacy can be borrowed to address the advice problem. Two similar states are interpreted as two neighbouring datasets. The advice generated from the states is interpreted as the query result yielded from datasets. Since two results from neighbouring datasets can be considered approximately identical, two pieces of advice generated from two similar states can also be considered approximately identical. This property can thus guarantee that advice created in a state can still be used in another similar state. Hence, this may be an interesting way to improve agent learning performance.

6.5.2 Multi-agent transfer learning

When agents transfer knowledge between each other to improve learning performance, a key problem discussed is that privacy needs to be preserved [107]. Existing methods are typically based on homomorphic cryptosystems [153], [154], [155]. However, homomorphic cryptosystems have a high computation overhead and, therefore, may not be very efficient in resource-constrained systems, e.g., wireless sensor networks. Differential privacy, with its light computation overhead, therefore, could be a good alternative in these situations.

6.5.3 Multi-agent reasoning

Reasoning is an ability that enables an agent to use known facts to deduce new knowledge. It has been widely employed to address various real-world problems. For example, knowledge graph-based reasoning can be used in speech recognition to parse speech contents into logical propositions [156], and case-based reasoning can be adopted to address the data-sparsity issue in recommendation systems by filling in the vacant ratings of the user-item matrix [157]. A typical reasoning method is based on the Belief, Desire and Intention (BDI) model [158]. An agent's beliefs correspond to information the agent has about the world.

Reasoning is a powerful tool in AI especially when it is combined with deep neural networks. For example, Mao et al. [159] has recently proposed a neuro-symbolic concept learner which combines symbolic reasoning with deep learning. Their model can learn visual concepts, words and semantic parsing of sentences without explicit supervision on any of them. As reasoning requires querying known facts which may contain private information, privacy preservation becomes an issue in reasoning process. Tao et al. [160] propose a privacy-preserving reasoning framework. Their idea is to hide the truthful answer from a querying agent by providing the answer "Unknown" to a query. Then, the querying agent cannot distinguish between the case that the query is being protected and the case that the query cannot be inferred from the known facts. However, simply hiding truthful answers may seriously hinder the utility of querying results. Differential privacy, with its theoretical guarantee of utility of querying results, may be a promising technique for privacy-preserving reasoning.

Recently, there have been great efforts to combine differential privacy with reasoning [161], [162], [163]. These works, however, aim to take advantage of reasoning to prove differential privacy guarantees of programs, instead of using differential privacy to guarantee privacy-preserving reasoning. Therefore, a potential direction of future research may be introducing differential privacy into reasoning process to guarantee the privacy of known facts.

6.6 Combination of machine learning, deep learning and multi-agent systems

A novel research area by combining machine learning, deep learning and multi-agent systems is the multi-agent deep reinforcement learning (MADRL) [164]. In MADRL, multi-agent system technique is used to coordinate the behaviors of agents; machine learning technique is responsible for guiding the learning process of agents; and deep learning is employed by agents to learn efficient strategies.

One of the current research directions along MADRL is the action advising [165], [166], [167]. Action advising in regular multi-agent reinforcement learning allows a teacher agent to offer only an action as advice to a student agent in a concerned state. By comparison, action advising in MADRL usually allows a student agent to query a teacher agent's knowledge base to receive action suggestions [167]. However, as the number of states in MADRL is very large, an agent's knowledge base may contain the agent's very rich private information that should be protected. Privacy-

preservation in MADRL is still an open research problem which may be addressed by using differential privacy.

7 Conclusion

In this paper, we investigated the use of differential privacy in selected areas of AI. We described the critical issues facing AI and the basic concepts of differential privacy, highlighting how differential privacy can be applied to solving some of these problems. We discussed the strengths and limitations of the current studies in each of these areas and also pointed out the potential research areas of AI where the benefits of differential privacy remain untapped. In addition to the three areas of focus in this article – machine learning, deep learning and multi-agent learning – there are many other interesting areas of research in AI that have also leveraged differential privacy, such as natural language processing, computer vision, robotics, etc. Surveying differential privacy in these areas is something we intend to do in future work.

References

[1] X. Ge, Q.-L. Han, D. Ding, X.-M. Zhang, and B. Ning, "A survey on recent advances in distributed sampled-data cooperative control of multi-agent systems," *Neurocomputing*, vol. 275, pp. 1684–1701, 2018.

[2] R. C. Geyer, T. Klein, and M. Nabi, "Differentially Private Federated Learning: A Client Level Perspective," in *Proc. of NIPS Workshop on Machine Learning on the Phone and other Consumer Devices*, 2017.

[3] Úlfar Erlingsson, V. Pihur, and A. Korolova, "Rappor: Randomized aggregatable privacy-preserving ordinal response," in *Proceedings of the 21st ACM Conference on Computer and Communications Security*, Scottsdale, Arizona, 2014.

[4] C. Dwork, V. Feldman, M. Hardt, T. Pitassi, O. Reingold, and A. Roth, "The reusable holdout: Preserving validity in adaptive data analysis," *Science*, vol. 349, no. 6248, pp. 636–638, 2015.

[5] T. Zhu and P. S. Yu, "Applying differential privacy mechanism in artificial intelligence," in *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, 2019, pp. 1601–1609.

[6] A. Chouldechova and A. Roth, "The frontiers of fairness in machine learning," *CoRR*, vol. abs/1810.08810, 2018.

[7] K. Chaudhuri, C. Monteleoni, and A. D. Sarwate, "Differentially private empirical risk minimization," *Journal of Machine Learning Research*, vol. 12, pp. 1069–1109, 2011.

[8] D. Ye, T. Zhu, W. Zhou, and P. S. Yu, "Differentially Private Malicious Agent Avoidance in Multiagent Advising Learning," *IEEE Transactions on Cybernetics*, p. DOI: 10.1109/TCYB.2019.2906574, 2019.

[9] S. Russell and P. Norvig, "Artificial intelligence: a modern approach," 2002.

[10] I. J. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio, "Generative Adversarial Nets," in *Proc. of NIPS*, 2014, pp. 2672–2680.

[11] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in *2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2016, pp. 770–778.

[12] C. Dwork, "Differential privacy," in *ICALP'06: Proceedings of the 33rd international conference on Automata, Languages and Programming*. Berlin, Heidelberg: Springer-Verlag, 2006, pp. 1–12.

[13] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *TCC'06: Proceedings of the Third conference on Theory of Cryptography*. Berlin, Heidelberg: Springer-Verlag, 2006, pp. 265–284.

[14] F. McSherry and K. Talwar, "Mechanism design via differential privacy," in *48th Annual IEEE Symposium on Foundations of Computer Science (FOCS'07)*, Oct 2007, pp. 94–103.

[15] F. McSherry, "Privacy integrated queries: an extensible platform for privacy-preserving data analysis," *Commun. ACM*, vol. 53, no. 9, pp. 89–97, 2010.

[16] T. Zhu, G. Li, W. Zhou, and P. S. Yu, "Differentially private data publishing and analysis: A survey," *IEEE Transactions on Knowledge and Data Engineering*, vol. 29, no. 8, pp. 1619–1638, Aug 2017.

[17] S. P. Kasiviswanathan, H. K. Lee, K. Nissim, S. Raskhodnikova, and A. Smith, "What can we learn privately?" in *2008 49th Annual IEEE Symposium on Foundations of Computer Science*, 2008, pp. 531–540.

[18] K. Chaudhuri, C. Monteleoni, and A. D. Sarwate, "Differentially Private Empirical Risk Minimization," *Journal of Machine Learning Research*, vol. 12, pp. 1069–1109, 2011.

[19] D. Wang, M. Ye, and J. Xu, "Differentially Private Empirical Risk Minimization Revisited: Faster and More General," in *Proc. of NIPS*, 2017.

[20] C. Dwork and V. Feldman, "Privacy-preserving Prediction," in *Proc. of COLT*, 2018.

[21] Y. Dagan and V. Feldman, "PAC learning with stable and private predictions," https://arxiv.org/pdf/1911.10541.pdf, 2019.

[22] J. Foulds, J. Geumlek, M. Welling, and K. Chaudhuri, "On the Theory and Practice of Privacy-Preserving Bayesian Data Analysis," in *Proc. of UAI*, 2016, pp. 192–201.

[23] G. Bernstein and D. R. Sheldon, "Differentially Private Bayesian Inference for Exponential Families," in *Proc. of NIPS*, 2018.

[24] G. Bernstein and D. Sheldon, "Differentially Private Bayesian Linear Regression," in *Proc. of NIPS*, 2019.

[25] A. C. Y. Tossou and C. Dimitrakakis, "Algorithms for Differentially Private Multi-Armed Bandits," in *Proc. of AAAI*, 2016, pp. 2087–2093.

[26] A. C. Tossou and C. Dimitrakakis, "Achieving Privacy in the Adversarial Multi-Armed Bandit," in *Proc. of AAAI*, 2017, pp. 2653–2659.

[27] P. Mohassel and Y. Zhang, "SecureML: A System for Scalable Privacy-Preserving Machine Learning," in *IEEE Symposium on Security and Privacy*, 2017, pp. 19–38.

[28] M. Al-Rubaie and J. M. Chang, "Privacy-Preserving Machine Learning: Threats and Solutions," *IEEE Security & Privacy Magazine*, vol. 17, no. 2, pp. 49–58, 2019.

[29] B. Jayaraman and D. Evans, "Evaluating Differentially Private Machine Learning in Practice," in *Proc. of the 28th USENIX Security Symposium*, 2019, pp. 1895–1912.

[30] O. Bousquet and A. Elisseeff, "Stability and generalization," *Journal of machine learning research*, vol. 2, no. Mar, pp. 499–526, 2002.

[31] C. Dwork, V. Feldman, M. Hardt, T. Pitassi, O. Reingold, and A. L. Roth, "Preserving statistical validity in adaptive data analysis," in *Proceedings of the Forty-seventh Annual ACM Symposium on Theory of Computing*, ser. STOC '15. New York, NY, USA: ACM, 2015, pp. 117–126.

[32] M. Hardt and J. Ullman, "Preventing false discovery in interactive data analysis is hard," in *Proceedings of the 2014 IEEE 55th Annual Symposium on Foundations of Computer Science*, ser. FOCS '14. Washington, DC, USA: IEEE Computer Society, 2014, pp. 454–463.

[33] M. Hardt, K. Ligett, and F. Mcsherry, "A simple and practical algorithm for differentially private data release," in *Advances in Neural Information Processing Systems 25*, F. Pereira, C. J. C. Burges, L. Bottou, and K. Q. Weinberger, Eds. Curran Associates, Inc., 2012, pp. 2339–2347.

[34] R. MacCoun and S. Perlmutter, "Blind analysis: Hide results to seek the truth," *Nature*, vol. 526, pp. 187–189, 10 2015.

[35] R. Binns, "Fairness in Machine Learning: Lessons from Political Philosophy," *Proceedings of Machine Learning Research*, vol. 81, pp. 1–11, 2018.

[36] K. Holstein, J. W. Vaughan, H. D. III, M. Dudik, and H. Wallach, "Improving Fairness in Machine Learning Systems: What Do Industry Practitioners Need," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 2019, pp. Paper600:1–16.

[37] T. Zhang, T. Zhu, J. Li, M. Han, W. Zhou, and P. Yu, "Fairness in Semi-supervised Learning: Unlabeled Data Help to Reduce Discrimination," *IEEE Transactions on Knowledge and Data Engineering*, p. DOI: 10.1109/TKDE.2020.3002567, 2020.

[38] S. Wachter-Boettcher, "AI Recruiting Tools Do Not Eliminate Bias," https://time.com/4993431/ai-recruiting-tools-do-not-eliminate-bias/, 2017.

[39] V. Giang, "The Potential Hidden Bias in Automated Hiring Systems," https://www.fastcompany.com/40566971/the-potential-hidden-bias-in-automated-hiring-systems, 2018.

[40] BBC, "Google Searches Expose Racial Bias, Says Study of Names," https://www.bbc.com/news/technology-21322183, 2013.

[41] S. U. Nobel, *Algorithms of Oppression: How Search Engines Reinforce Racism*. NYU Press, 2018.

[42] J. Angwin, J. Larson, S. Mattu, and L. Kirchner, "Machine Bias," https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing, May 2016.

[43] N. Mehrabi, F. Morstatter, N. Saxena, K. Lerman, and A. Galstyan, "A Survey on Bias and Fairness in Machine Learning," https://arxiv.org/abs/1908.09635, 2019.

[44] R. Zemel, Y. Wu, K. Swersky, T. Pitassi, and C. Dwork, "Learning Fair Representation," in *Proc. of ICML*, 2013.

[45] M. Hardt, E. Price, and N. Srebro, "Equality of Opportunity in Supervised Learning," in *Proc. of NIPS*, 2016, pp. 3315–3323.

[46] C. Dwork and C. Ilvento, "Fairness under Composition," in *Proc. of ITCS*, 2019, pp. 33:1–20.

[47] M. Kusner, J. Loftus, C. Russell, and R. Silva, "Counterfactual Fairness," in *Proc. of NIPS*, 2017, pp. 4066–3076.

[48] A. Agarwal, A. Beygelzimer, M. Dudik, J. Langford, and H. Wallach, "A Reductions Approach to Fair Classification," in *Proc. of ICML*, 2018.

[49] C. Dwork, M. Hardt, T. Pitassi, O. Reingold, and R. Zemel, "Fairness through Awareness," in *Proc. of ITSC*, 2012, pp. 214–226.

[50] K. Dixit, M. Jha, S. Raskhodnikova, and A. Thakurta, "Testing the lipschitz property over product distributions with applications to data privacy," in *Theory of Cryptography Conference*. Springer, 2013, pp. 418–436.

[51] R. Zemel, Y. Wu, K. Swersky, T. Pitassi, and C. Dwork, "Learning fair representations," in *ICML*, vol. 28, no. 3, 17–19 Jun 2013, pp. 325–333.

[52] D. Xu, S. Yuan, and X. Wu, "Achieving Differential Privacy and Fairness in Logistic Regression," in *Proc. of WWW*, 2019, pp. 594–599.

[53] J. Ding, X. Zhang, X. Li, J. Wang, R. Yu, and M. Pan, "Differentially Private and Fair Classification via Calibrated Functional Mechanism," in *Proc. of AAAI*, 2020.

[54] M. Jagielski and et al., "Differentially Private Fair Learning," in *Proc. of ICML*, 2019.

[55] R. Cummings, V. Gupta, D. Kimpara, and J. Morgenstern, "On the Compatibility of Privacy and Fairness," in *Proc. of the 27th Conference on User Modeling, Adaptation and Personalization*, 2019, pp. 309–315.

[56] C. Dwork and C. Ilvento, "Fairness under composition," *CoRR*, vol. abs/1806.06122, 2018.

[57] S. Dargan, M. Kumar, M. R. Ayyagari, and G. Kumar, "A Survey of Deep Learning and Its Applications: A New Paradigm to Machine Learning," *Archives of Computational Methods in Engineering*, pp. DOI:https://doi.org/10.1007/s11 831–019–09 344–w, 2019.

[58] S. Pouyanfar, S. Sadiq, Y. Yan, H. Tian, Y. Tao, M. P. Reyes, M. Shyu, S. Chen, and S. S. Iyengar, "A Survey on Deep Learning: Algorithms, Techniques, and Applications," *ACM Computing Surveys*, vol. 51, no. 5, pp. 92:1–36, 2018.

[59] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated Machine Learning: Concept and Applications," *ACM Transactions on Intelligent Systems and Technology*, vol. 10, no. 2, pp. 12:1–19, 2019.

[60] M. Gong, K. Pan, Y. Xie, A. K. Qin, and Z. Tang, "Preserving differential privacy in deep neural networks with relevance-based adaptive noise imposition," *Neural Networks*, vol. 125, pp. 131–141, 2020.

[61] M. Nasr, R. Shokri, and A. Houmansadr, "Comprehensive Privacy Analysis of Deep Learning: Passive and Active White-box Inference Attacks against Centralized and Federated Learning," in *S & P*, 2019, pp. 739–753.

[62] R. Shokri, M. Stronati, C. Song, and V. Shmatikov, "Membership Inference Attacks Against Machine Learning Models," in *Proc. of IEEE Symposium on Security and Privacy*, 2017, pp. 3–18.

[63] S. Yeom, I. Giacomelli, M. Fredrikson, and S. Jha, "Privacy Risk in Machine Learning: Analyzing the Connection to Overfitting," in *Proc. of IEEE 31st Computer Security Foundations Symposium*, 2018, pp. 268–282.

[64] M. Fredrikson, E. Lantz, S. Jha, S. Lin, D. Page, and T. Ristenpart, "Privacy in Pharmacogenetics: An End-to-End Case Study of Personalized Warfarin Dosing," in *Proc. of the 23rd USENIX Security Symposium*, 2014, pp. 17–32.

[65] M. Abadi, A. Chu, and I. Goodfellow, "Deep Learning with Differential Privacy," in *Proc. of CCS*, 2016, pp. 308–318.

[66] M. Heikkila, E. Lagerspetz, S. Kaski, K. Shimizu, S. Tarkoma, and A. Honkela, "Differentially Private Bayesian Learning on Distributed Data," in *Proc. of NIPS*, 2017.

[67] L. Zhao, Q. Wang, Q. Zou, Y. Zhang, and Y. Chen, "Privacy-Preserving Collaborative Deep Learning with Unreliable Participants," *IEEE Transactions on Information Forensics and Security*, p. DOI: 10.1109/TIFS.2019.2939713, 2019.

[68] R. Shokri and V. Shmatikov, "Privacy-Preserving Deep Learning," in *Proc. of CCS*, 2015, pp. 1310–1321.

[69] H. Cheng, P. Yu, H. Hu, F. Yan, S. Li, H. Li, and Y. Chen, "LEASGD: an Efficient and Privacy-Preserving Decentralized Algorithm for Distributed Learning," in *Proc. of NIPS Workshop on Privacy Preserving Machine Learning*, 2018.

[70] B. Jayaraman, L. Wang, D. Evans, and Q. Gu, "Distributed Learning without Distress: Privacy-Preserving Empirical Risk Minimization," in *Proc. of NIPS*, 2018.

[71] N. Phan, M. N. Vu, Y. Liu, R. Jin, D. Dou, X. Wu, and M. T. Thai, "Heterogeneous Gaussian Mechanism: Preserving Differential Privacy in Deep Learning with Provable Robustness," in *Proc. of IJCAI*, 2019, pp. 4753–4759.

[72] N. Papernot, M. Abadi, U. Erlingsson, I. Goodfellow, and K. Talwar, "Semi-supervised knowledge transfer for deep learning from private training data," in *Proc. of ICLR*, 2017.

[73] N. Papernot, S. Song, I. Mironov, A. Raghunathan, K. Talwar, and U. Erlingsson, "Scalable Private Learning with PATE," in *Proc. of ICLR*, 2018.

[74] J. Zhao, "Distributed Deep Learning under Differential Privacy with the Teacher-Student Paradigm," in *Proc. of the Workshops of AAAI*, 2018, pp. 404–407.

[75] J. Jordon, J. Yoon, and M. van der Schaar, "PATE-GAN: Generating Synthetic Data with Differential Privacy Guarantees," in *Proc. of ICLR*, 2019.

[76] M. Kearns, M. M. Pai, A. Roth, and J. Ullman, "Mechanism Design in Large Games: Incentives and Privacy," in *Proc. of ITCS*, 2014, pp. 403–410.

[77] Y. Zhang, Y. Mao, and S. Zhong, "Joint Differentially Private Gale-Shapley Mechanisms for Location Privacy Protection in Mobile Traffic Offloading Systems," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 10, pp. 2738–2749, 2016.

[78] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-Efficient Learning of Deep Networks from Decentralized Data," in *AISTATS*, vol. 54. PMLR, 20–22 Apr 2017, pp. 1273–1282.

[79] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: Concept and applications," *ACM Trans. Intell. Syst. Technol.*, vol. 10, no. 2, Jan. 2019. [Online]. Available: https://doi.org/10.1145/3298981

[80] H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Federated Learning of Deep Networks using Model Averaging," arXiv:1602.05629, Tech. Rep., 2017.

[81] L. T. Phong, Y. Aono, T. Hayashi, L. Wang, and S. Moriai, "Privacy-preserving Deep Learning via Additively Homomorphic Encryption," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 5, pp. 1333–1345, 2018.

[82] R. C. Geyer, T. Klein, and M. Nabi, "Differentially private federated learning: A client level perspective," *CoRR*, vol. abs/1712.07557, 2017.

[83] S. Truex, N. Baracaldo, A. Anwar, T. Steinke, H. Ludwig, and R. Zhang, "A hybrid approach to privacy-preserving federated learning," *CoRR*, vol. abs/1812.03224, 2018.

[84] E. Shi, T. H. H. Chan, E. Rieffel, and D. Song, "Distributed Private Data Analysis: Lower Bounds and Practical Constructions," *ACM Transactions on Algorithms*, vol. 13, no. 4, pp. 50:1–38, 2017.

[85] N. Agarwal, A. T. Suresh, F. Yu, S. Kumar, and H. B. McMahan, "cpSGD: Communication-Efficient and Differentially-Private Distributed SGD," in *Proc. of NIPS*, 2018.

[86] V. Smith, C.-K. Chiang, M. Sanjabi, and A. S. Talwalkar, "Federated multi-task learning," in *Advances in Neural Information Processing Systems*, 2017, pp. 4424–4434.

[87] A. N. Bhagoji, S. Chakraborty, P. Mittal, and S. Calo, "Analyzing federated learning through an adversarial lens," *arXiv preprint arXiv:1811.12470*, 2018.

[88] A. N. Bhagoji, S. Chakraborty, P. Mittal, and S. Calo, "Analyzing federated learning through an adversarial lens," in *Proceedings of the 36th International Conference on Machine Learning*, ser. Proceedings of Machine Learning Research, K. Chaudhuri and R. Salakhutdinov, Eds., vol. 97. Long Beach, California, USA: PMLR, 09–15 Jun 2019, pp. 634–643.

[89] J. Konecný, H. B. McMahan, F. X. Yu, P. Richtárik, A. T. Suresh, and D. Bacon, "Federated learning: Strategies for improving communication efficiency," *CoRR*, vol. abs/1610.05492, 2016.

[90] B. Hitaj, G. Ateniese, and F. Perez-Cruz, "Deep Models under the GAN: Information Leakage from Collaborative Deep Learning," in *Proc. of CCS*, 2017, pp. 603–618.

[91] U. Erlingsson, V. Pihur, and A. Korolova, "RAPPOR: Randomized Aggregatable Privacy-Preserving Ordinal Response," in *Proc. of CCS*, 2014.

[92] M. Fredrikson, S. Jha, and T. Ristenpart, "Model Inversion Attacks That Exploit Confidence Information and Basic Countermeasures," in *Proc. of CCS*, 2015, pp. 1322–1333.

[93] Z. Yang, J. Zhang, E. Chang, and Z. Liang, "Neural Network Inversion in Adversarial Setting via Background Knowledge Alignment," in *Proc. of CCS*, 2019, pp. 225–240.

[94] M. Mohri, G. Sivek, and A. T. Suresh, "Agnostic Federated Learning," in *Proc. of ICML*, 2019.

[95] T. Li, M. Sanjabi, A. Beirami, and V. Smith, "Fair Resource Allocation in Federated Learning," in *Proc. of ICLR*, 2020.

[96] D. Ye and M. Zhang, "A Self-Adaptive Sleep/Wake-Up Scheduling Approach for Wireless Sensor Networks," *IEEE Transactions on Cybernetics*, vol. 48, pp. 979–992, 2018.

[97] D. Ye, M. Zhang, and D. Sutanto, "A hybrid multiagent framework with Q-learning for power grid systems restoration," *IEEE Transactions on Power Systems*, vol. 26, pp. 2434–2441, 2011.

[98] D. Ye, Q. He, Y. Wang, and Y. Yang, "An Agent-Based Integrated Self-Evolving Service Composition Approach in Networked Environments," *IEEE Transactions on Services Computing*, vol. 12, pp. 880–895, 2019.

[99] M. Wooldridge and N. R. Jennings, "Intelligent agents: theory and practice," *The Knowledge Engineering Review*, pp. 115–152, 1995.

[100] D. Ye, M. Zhang, and A. V. Vasilakos, "A Survey of Self-Organization Mechanisms in Multiagent Systems," *IEEE Transactions on Systems, Man and Cybernetics: Systems*, vol. 47, no. 3, pp. 441–461, 2017.

[101] F. Fioretto and P. V. Hentenryck, "Privacy-Preserving Federated Data Sharing," in *Proc. of AAMAS*, 2019, pp. 638–646.

[102] M. M. Pai, A. Roth, and J. Ullman, "An Antifolk Theorem for Large Repeated Games," *ACM Transactions on Economics and Computation*, vol. 5, no. 2, pp. 10: 1–20, 2016.

[103] K. Tuyls and G. Weiss, "Multiagent Learning: Basics, Challenges, and Prospects," *AI Magazine*, vol. 33, no. 3, pp. 41–52, 2012.

[104] L. Busoniu, R. Babuska, and B. D. Schutter, "A Comprehensive Survey of Multiagent Reinforcement Learning," *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews*, vol. 38, no. 2, pp. 156–172, 2008.

[105] F. L. da Silva, M. E. Taylor, and A. H. R. Costa, "Autonomously Reusing Knowledge in Multiagent Reinforcement Learning," in *Proc. of IJCAI 2018*, Sweden, July 2018, pp. 5487–5493.

[106] F. L. da Silva, R. Glatt, and A. H. R. Costa, "Simultaneously Learning and Advising in Multiagent Reinforcement Learning," in *AAMAS 2017*, Brazil, May 2017, pp. 1100–1108.

[107] F. L. D. Silva and A. H. R. Costa, "A Survey on Transfer Learning for Multiagent Reinforcement Learning Systems," *Journal of Artificial Intelligence Research*, vol. 64, pp. 645–703, 2019.

[108] S. Parsons, J. A. Rodriguez-Aguilar, and M. Klein, "Auctions and bidding: A guide for computer scientists," *ACM Computing Surveys*, vol. 43, no. 2, pp. 10:1–66, 2011.

[109] Z. Chen, T. Ni, H. Zhong, S. Zhang, and J. Cui, "Differentially Private Double Spectrum Auction with Approximate Social Welfare Maximization," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 11, pp. 2805–2818, 2019.

[110] R. Zhu, Z. Li, F. Wu, K. G. Shin, and G. Chen, "Differentially Private Spectrum Auction with Approximate Revenue Maximization," in *Proc. of MobiHoc*, 2014, pp. 185–194.

[111] R. Zhu and K. G. Shin, "Differentially Private and Strategy-Proof Spectrum Auction with Approximate Revenue Maximization," in *Proc. of INFOCOM*, 2015, pp. 918–926.

[112] C. Wu, Z. Wei, F. Wu, G. Chen, and S. Tang, "Designing Differentially Private Spectrum Auction Mechanisms," *Wireless Networks*, vol. 22, no. 1, pp. 105–117, 2016.

[113] J. Xu, B. Palanisamy, Y. Tang, and S. D. M. Kumar, "PADS: Privacy-Preserving Auction Design for Allocating Dynamically Priced Cloud Resources," in *Proc. of IEEE 3rd International Conference on Collaboration and Internet Computing*, 2017, pp. 87–96.

[114] B. Li, D. Hao, D. Zhao, and T. Zhou, "Mechanism Design in Social Networks," in *Proc. of AAAI*, 2017, pp. 586–592.

[115] D. Zhao, B. Li, J. Xu, D. Hao, and N. R. Jennings, "Selling Multiple Items via Social Networks," in *Proc. of AAMAS*, 2018, pp. 68–76.

[116] G. Bonanno, *Game Theory*, 2nd ed. CreateSpace Independent Publishing Platform, 2018.

[117] A. Acquisti, C. Taylor, and L. Wagman, "The Economics of Privacy," *Journal of Economic Literature*, vol. 54, no. 2, pp. 442–492, 2016.

[118] S. N. Durlauf and L. E. Blume, *Game Theory*. Springer, 2010, ch. Computer Science and Game Theory, pp. 48–65.

[119] A. Roth, "Differential Privacy, Equilibrium, and Efficient Allocation of Resources," in *Proc. of IEEE 51st Annual Allerton Conference*, 2013, pp. 1593–1597.

[120] M. M. Pai and A. Roth, "Privacy and Mechanism Design," *ACM SIGecom Exchanges*, vol. 12, no. 1, pp. 8–29, 2013.

[121] I. Wanger and D. Eckhoff, "Technical Privacy Metrics: a Systematic Survey," *ACM Computing Surveys*, vol. 51, no. 3, pp. 57: 1–45, 2018.

[122] R. Rogers and A. Roth, "Asymptotically Truthful Equilibrium Selection in Large Congestion Games," in *Proc. of ACM EC*, 2014, pp. 771–781.

[123] M. M. Pai, A. Roth, and J. Ullman, "An antifolk theorem for large repeated games," *ACM Trans. Econ. Comput.*, vol. 5, no. 2, Oct. 2016.

[124] J. Masso, "More on The 'Anti-Folk Theorem'," *Journal of Mathematical Economics*, vol. 18, pp. 281–290, 1989.

[125] T. Lykouris, V. Syrgkanis, and E. Tardos, "Learning and Efficiency in Games with Dynamic Population," in *Proc. of ACM-SIAM SODA*, 2016, pp. 120–129.

[126] S. Han, U. Topcu, and G. J. Pappas, "An Approximately Truthful Mechanism for Electric Vehicle Charging via Joint Differential Privacy," in *Proc. of AACC*, 2015, pp. 2469–2475.

[127] J. Hsu, A. Roth, and J. Ullman, "Differential Privacy for the Analyst via Private Equilibrium Computation," in *Proc. of STOC*, 2013, pp. 341–350.

[128] D. Gale and L. S. Shapley, "College admissions and the stability of marriage," *The American Mathematical Monthly*, vol. 69, no. 1, pp. 9–15, 1962.

[129] T. H. H. Chan, E. Shi, and D. Song, "Private and Continual Release of Statistics," *ACM Transactions on Information and System Security*, vol. 14, no. 3, pp. 26: 1–23, 2011.

[130] P. Zhou, W. Wei, K. Bian, D. O. Wu, Y. Hu, and Q. Wang, "Private and Truthful Aggregative Game for Large-Scale Spectrum Sharing," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 2, pp. 463–477, 2017.

[131] Y. Dimopoulos, J.-G. Mailly, and P. Moraitis, "Argumentation-based Negotiation with Incomplete Opponent Profiles," in *Proc. of AAMAS*, 2019, pp. 1252–1260.

[132] A. Beynier, S. Bouveret, M. Lemaitre, N. Maudet, S. Rey, and P. Shams, "Efficiency, Sequenceability and Deal-Optimality in Fair Division of Indivisible Goods," in *Proc. of AAMAS*, 2019, pp. 900–908.

[133] L. Xie, I. M. Baytas, K. Lin, and J. Zhou, "Privacy-Preserving Distributed Multi-Task Learning with Asynchronous Updates," in *Proc. of KDD*, 2017, pp. 1195–1204.

[134] Y. Wang, Q. Gu, and D. Brown, "Differentially Private Hypothesis Transfer Learning," in *Proc. of ECML/PKDD*, 2018, pp. 811–826.

[135] N. LeTien, A. Habrard, and M. Sebban, "Differentially Private Optimal Transport: Application to Domain Adaptation," in *Proc. of IJCAI*, 2019, pp. 2852–2858.

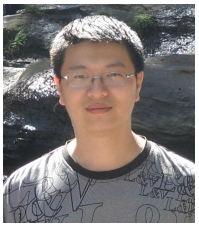
[136] Q. Yao, X. Guo, J. Kwok, W. Tu, Y. Chen, W. Dai, and Q. Yang, "Privacy-preserving Stacking with Application to Cross-organizational Diabetes Prediction," in *Proc. of IJCAI*, 2019, pp. 4114–4120.

[137] C. Qin, D. Qu, and L. Zhang, "Towards end-to-end speech recognition with transfer learning," *EURASIP Journal on Audio, Speech, and Music Processing*, vol. 18, pp. 18:1–9, 2018.

[138] L. Zhao, S. J. Pan, E. W. Xiang, E. Zhong, Z. Lu, and Q. Yang, "Active Transfer Learning for Cross-System Recommendation," in *Proc. of AAAI*, 2013, pp. 1205–1211.
[139] R. Wang, Y. F. Li, X. Wang, H. Tang, and X. Zhou, "Learning Your Identity and Disease from Research Papers: Information Leaks in Genome Wide Association Study," in *Proc. of CCS*, 2009, pp. 534–544.
[140] V. Francois-Lavet, P. Henderson, R. Islam, M. G. Bellemare, and J. Pineau, "An Introduction to Deep Reinforcement Learning," *Foundations and Trends in Machine Learning*, vol. 11, no. 3-4, 2018.
[141] B. Wang and N. Hegde, "Privacy-preserving Q-Learning with Functional Noise in Continuous Spaces," in *Proc. of NIPS*, 2019.
[142] R. Vilalta and Y. Drissi, "A Perspective View and Survey of Meta-Learning," *Artificial Intelligence Review*, vol. 18, pp. 77–95, 2002.
[143] C. Lemke, M. Budka, and B. Gabrys, "Metalearning: A Survey of Trends and Technologies," *Artificial Intelligence Review*, vol. 44, pp. 117–130, 2015.
[144] J. Vanschoren, *Automated Machine Learning*. Springer, 2019, ch. Meta-Learning, pp. 35–61.
[145] C. Finn, P. Abbeel, and S. Levine, "Model-Agnostic Meta-Learning for Fast Adaptation of Deep Networks," in *Proc. of ICML*, 2017.
[146] A. Nichol, J. Achiam, and J. Schulman, "On First-Order Meta-Learning Algorithms," https://arxiv.org/abs/1803.02999, 2018.
[147] J. Li, M. Khodak, S. Caldas, and A. Talwalkar, "Differentially Private Meta-Learning," in *Proc. of ICLR*, 2020.
[148] R. Bassily, V. Feldman, K. Talwar, and A. Thakurta, "Private Stochastic Convex Optimization with Optimal Rates," in *Proc. of NIPS*, 2019.
[149] C. Finn, A. Rajeswaran, S. Kakade, and S. Levine, "Online Meta-Learning," in *Proc. of ICML*, 2019.
[150] J. Ho and S. Ermon, "Generative adversarial imitation learning," in *Proc. of NIPS*, 2016, pp. 4565–4573.
[151] D. Yoo, N. Kim, S. Park, A. S. Paek, and I. S. Kweon, "Pixel-Level Domain Transfer," in *Proc. of ECCV*, 2016.
[152] C. Xu, J. Ren, D. Zhang, Y. Zhang, Z. Qin, and K. Ren, "GANobfuscator: Mitigating Information Leakage under GAN via Differential Privacy," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 9, pp. 2358–2371, 2019.
[153] J. Sakuma, S. Kobayashi, and R. N. Wright, "Privacy-Preserving Reinforcement Learning," in *Proc. of ICML*, 2008.
[154] F. Wu, S. Zilberstein, and X. Chen, "Privacy-Preserving Policy Iteration for Decentralized POMDPs," in *Proc. of AAAI*, 2018, pp. 4759–4766.
[155] X. Liu, R. Deng, K.-K. R. Choo, and Y. Yang, "Privacy-Preserving Reinforcement Learning Design for Patient-Centric Dynamic Treatment Regimes," *IEEE Transactions on Emerging Topics in Computing*, 2019.
[156] M. Zhou, N. Duan, S. Liu, and H.-Y. Shum, "Progress in Neural NLP: Modeling, Learning, and Reasoning," *Engineering*, vol. 6, pp. 275–290, 2020.
[157] A. A. Tawfik, H. Alhoori, C. W. Keene, C. Bailey, and M. Hogan, "Using a Recommendation System to Support Problem Solving and Case-Based Reasoning Retrieval," *Technology, Knowledge and Learning*, vol. 23, pp. 177–187, 2017.
[158] M. D'Inverno, M. Luck, M. Georgeff, D. Kinny, and M. Wooldridge, "The dMARS Architecture: A Specification of the Distributed Multi-Agent Reasoning System," *Autonomous Agents and Multi-Agent Systems*, vol. 9, pp. 5–53, 2004.
[159] J. Mao, C. Gan, P. Kohli, J. B. Tenenbaum, and J. Wu, "The Neuro-Symbolic Concept Learner: Interpreting Scenes, Words, and Sentences from Natural Supervision," in *Proc. of ICLR*, 2019.
[160] J. Tao, G. Slutzki, and V. Honavar, "A Conceptual Framework for Secrecy-preserving Reasoning in Knowledge Bases," *ACM Transactions on Computational Logic*, vol. 16, no. 1, pp. 3:1–32, 2014.
[161] G. Barthe, B. Kopf, F. Olmedo, and S. Zanella-Beguelin, "Probabilistic Relational Reasoning for Differential Privacy," *ACM Transactions on Programming Languages and Systems*, vol. 35, no. 3, pp. 9:1–49, 2013.
[162] G. Barthe, N. Fong, M. Gaboardi, B. Gregoire, J. Hsu, and P.-Y. Strub, "Advanced Probabilistic Coupling for Differential Privacy," in *Proc. of CCS*, 2016, pp. 55–67.
[163] H. Zhang, E. Roth, A. Haeberlen, B. C. Pierce, and A. Roth, "Fuzzi: A Three-Level Logic for Differential Privacy," in *Proc. of ACM Program. Lang.*, 2019, pp. 93:1–28.
[164] P. Hernandez-Leal, B. Kartal, and M. E. Taylor, "A survey and critique of multiagent deep reinforcement learning," *Autonomous Agents and Multi-Agent Systems*, vol. 3, pp. 750–797, 2019.
[165] E. Ilhan, J. Gow, and D. Perez-Liebana, "Teaching on a Budget in Multi-Agent Deep Reinforcement Learning," in *Proc. of IEEE Conference on Games*, 2019.
[166] S. Omidshafiei, D.-K. Kim, M. Liu, G. Tesauro, M. Riemer, C. Amato, M. Campbell, and J. P. How, "Learning to Teach in Cooperative Multiagent Reinforcement Learning," in *Proc. of AAAI*, 2019, pp. 6128–6136.
[167] F. L. D. Silva, P. Hernandez-Leal, B. Kartal, and M. E. Taylor, "Uncertainty-Aware Action Advising for Deep Reinforcement Learning Agents," in *Proc. of AAAI*, 2020.

Tianqing Zhu received her B.Eng. degree and her M.Eng. degree from Wuhan University, Wuhan, China, in 2000 and 2004, respectively. She also holds a PhD in computer science from Deakin University, Australia (2014). She is currently a professor in China University Geosciences, Wuhan, China. Prior to that, she was a Lecturer with the School of Information Technology, Deakin University, from 2014 to 2018. Her research interests include privacy-preserving, data mining, and cyber security.

Dayong Ye received his MSc and PhD degrees both from University of Wollongong, Australia, in 2009 and 2013, respectively. Now, he is a research fellow of Cyber-security at University of Technology, Sydney, Australia. His research interests focus on differential privacy, privacy preserving, and multi-agent systems.



Wei Wang is a postdoc in the School of Computer Science, Faculty of Engineering and Information Technology, at the University of Technology Sydney, Australia. He is a member of the Centre for Cyber Security and Privacy. His research interests include decision support, artificial intelligence, data visualization and privacy. He has published papers in journals such as Decision Support Systems and IEEE Transactions on Systems, Man, and Cybernetics.

Wanlei Zhou received the B.Eng and M.Eng degrees from Harbin Institute of Technology, Harbin, China in 1982 and 1984, respectively, and the PhD degree from The Australian National University, Canberra, Australia, in 1991, all in Computer Science and Engineering. He is currently the Head of school of Computer Science in University of Technology Sydney (UTS). Before joining UTS, Professor Zhou held the positions of Alfred Deakin Professor, Chair of Information Technology, and Associate Dean (International Research Engagement) of Faculty of Science, Engineering and Built Environment, Deakin University. His research interests include security and privacy, bioinformatics, and e-learning.

Philip S. Yu Philip S. Yu received the B.S. Degree in E.E. from National Taiwan University, the M.S. and Ph.D. degrees in E.E. from Stanford University. He is a Distinguished Professor in Computer Science at the University of Illinois at Chicago and also holds the Wexler Chair in Information Technology. Dr. Yu is the recipient of ACM SIGKDD 2016 Innovation Award for his influential research and scientific contributions on mining, fusion and anonymization of big data, the IEEE Computer Society's 2013 Technical Achievement Award for "pioneering and fundamentally innovative contributions to the scalable indexing, querying, searching, mining and anonymization of big data". He was the Editor-in-Chiefs of ACM Transactions on Knowledge Discovery from Data (2011-2017) and IEEE Transactions on Knowledge and Data Engineering (2001-2004).