

On the Privacy Risks of Deploying Recurrent Neural Networks in Machine Learning Models

Yunhao Yang*
yunhaoyang234@utexas.edu
University of Texas at Austin
USA

Parham Gohari*
pgohari@utexas.edu
University of Texas at Austin
USA

Ufuk Topcu
utopcu@utexas.edu
University of Texas at Austin
USA

ABSTRACT

We study the privacy implications of training recurrent neural networks (RNNs) with sensitive training datasets. Considering membership inference attacks (MIAs)—which aim to infer whether or not specific data records have been used in training a given machine learning model—we provide empirical evidence that a neural network’s architecture impacts its vulnerability to MIAs. In particular, we demonstrate that RNNs are subject to a higher attack accuracy than feed-forward neural network (FFNN) counterparts. Additionally, we study the effectiveness of two prominent mitigation methods for preempting MIAs, namely weight regularization and differential privacy. For the former, we empirically demonstrate that RNNs may only benefit from weight regularization marginally as opposed to FFNNs. For the latter, we find that enforcing differential privacy through either of the following two methods leads to a less favorable privacy-utility trade-off in RNNs: (i) adding Gaussian noise to the gradients calculated during training as a part of the so-called DP-SGD algorithm and (ii) adding Gaussian noise to the trainable parameters as a part of a post-training mechanism that we propose. As a result, RNNs can also be less amenable to mitigation methods, bringing us to the conclusion that the privacy risks pertaining to the recurrent architecture are higher than the feed-forward counterparts.

KEYWORDS

Differential Privacy, Recurrent Neural Networks, Membership Inference Attacks

1 INTRODUCTION

In the emerging applications of artificial intelligence, machine learning models are frequently trained with personal, proprietary, operational, confidential, or otherwise sensitive datasets, which raises privacy concerns. Even when these datasets are securely stored and safeguarded from unauthorized access, sharing the outputs of a machine learning model that has been trained with such sensitive data can lead to unintended information leakage [39, 47]. Hence, it is imperative to foresee and preempt the privacy risks of training machine learning models with sensitive datasets.

We study the privacy risks of machine learning models that are powered by recurrent neural networks (RNNs) and compare

them to their counterparts powered by feed-forward neural networks (FFNNs). As opposed to FFNNs, in which the nodes in every layer are only connected to subsequent-layer nodes, RNNs allow for backward connections in their architecture. RNNs are widely used in sequential machine learning tasks such as natural language processing [64], speech and handwriting recognition [20, 29, 50], deep reinforcement learning [28, 31], and semantic segmentation of video sequences [44]. While the privacy risks of neural networks—irrespective of their architecture—have been subject to an active line of research, an account of whether or not the architecture of neural networks affects their privacy risks remains unknown.

We consider *membership inference attacks (MIAs)* as the underlying privacy threat. In an MIA, an adversary is allowed to query the output of a neural network with a collection of data records, and must subsequently infer whether or not those data records belong to the neural network’s training dataset [25]. Successful instances of these attacks with minimal access to the neural network can have significant privacy ramifications for the individuals who populate the training datasets with their data. For example, consider a machine learning model that has been trained with the data of individuals with certain characteristics such as a particular ethnic origin, religion, medical condition, gender, or sexuality. In this case, a successful MIA that asserts—or refutes—the membership of an individual’s data may reveal those sensitive characteristics.

The main contributions of this paper are twofold: the first contribution concerns how RNNs and FFNNs compare in their vulnerability to MIAs, and the second contribution concerns defending neural networks against MIAs.

In the first contribution, we design and conduct a series of experiments to compare vulnerability to MIAs in three representative machine learning tasks, namely image classification, machine translation, and deep reinforcement learning. In order to study the impacts of network architecture on vulnerability to MIAs, we are mindful to separate other main factors that are known to impact vulnerability to MIAs such as overfitting [3, 51, 56, 66], number of trainable parameters [40], diversity of the training data [32], and number of prediction classes [58]. Taking all of these factors into account, we observe that the MIAs consistently achieve a higher attack accuracy against the RNN models.

In order to investigate the root causes of the observed higher vulnerability in RNNs, we further study the behavior of the two architectures when they are queried with members of their training datasets and unseen data. We observe that when the uncertainty of the two models’ predictions in terms of entropy is equal with respect to the validation dataset, the entropy with respect to the training data is lower in RNNs. Moreover, we demonstrate that the decisions of the MIAs resemble establishing a threshold for

*These authors contributed equally to this work

This work is licensed under the Creative Commons Attribution 4.0 International License. To view a copy of this license visit <https://creativecommons.org/licenses/by/4.0/> or send a letter to Creative Commons, PO Box 1866, Mountain View, CA 94042, USA.

Proceedings on Privacy Enhancing Technologies 2023(1), 68–84

© 2023 Copyright held by the owner/author(s).

<https://doi.org/10.56553/popets-2023-0005>



prediction entropy to distinguish member data from non-members. In such a threshold-based inference, a larger gap between the entropy of the predictions in training and validation—as observed in RNNs—increases attack accuracy. Moreover, we demonstrate that subsequent gradient updates in FFNNs can mask the membership of data used early in the history of training, whereas the MIAs remain relatively accurate even for such outdated data in RNNs.

In the second contribution, we shift the focus from vulnerability analysis to mitigation methods. A popular mitigation approach is to prevent overfitting as a root cause of vulnerability to MIAs—most prominently via weight regularization [51, 56]. While weight regularization has been shown to be oftentimes highly effective for FFNNs to preempt MIAs, in the experiments, we demonstrate that the RNN models benefit from regularization only marginally. As a result, RNNs may be not only more vulnerable to MIAs but also harder to be defended against them.

Methods that leverage the promise of differential privacy are known to be the most effective in defending neural networks against MIAs [25]. However, the protection afforded by these methods typically comes at the expense of a reduction in utility in terms of model performance [46]. These methods impose an error margin on the inference power of MIAs and the error can be balanced against utility loss by adjusting the level of differential privacy [66].

Existing methods that enforce differential privacy typically do so by obfuscating either of the following with noise: the objective function [67] or the gradients calculated during training [1, 37], or the model’s parameters post-training [6, 33, 63]. As opposed to post-training methods in which the privacy level can be easily modified by modifying the level of noise that is added to the model’s parameters, increasing the privacy level in the first two methods requires reversing training steps, which is challenging. As a result, post-training methods offer more flexibility in changing the privacy level. On the flip side, these methods may be less advantageous with respect to the privacy-utility trade-off that they face [1].

We compare RNNs and FFNNs in their utility loss due to differential privacy considering both approaches: the celebrated DP-SGD algorithm [1] which adds Gaussian noise to the gradients during training, and the Gaussian privacy module (GPM) which we introduce to add Gaussian noise to the trained parameters of a neural network post-training. For both methods, the experiment results indicate that adding the same level of noise degrades more utility in RNNs than FFNNs.

Although we develop the GPM solely to compare the utility loss of RNNs and FFNNs due to differential privacy, it may be of independent interest. We show that the GPM satisfies a relaxation of differential privacy called *random differential privacy* [22]. In noise-additive differential privacy mechanisms, the noise is typically calibrated with the extent to which a single record of the training dataset can change the model’s outcome, formally called *sensitivity*. Computing sensitivity analytically can be very challenging and one might have to resort to an upper bound for the sensitivity which can be too loose and subsequently cause too much noise to be added [6, 33, 63]. Alternatively, random differential privacy fixes a level of sensitivity with some confidence level and guarantees differential privacy for data records that give rise to that level of sensitivity.

We use the SENSITIVITYSAMPLER algorithm [48] to estimate the sensitivity of the models. We show that by utilizing these estimates,

we are able to achieve an acceptable privacy-utility trade-off for the models in the experiments: reducing the MIAs’ attack accuracy to roughly 50%—equivalent to random guessing—while trading off less than 10% utility. We further observe that the sensitivity estimates for the RNN and FFNN models in the experiments take similar values. As a result, adding the same level of noise to the two models using the DP-SGD algorithm and the proposed post-training mechanism, satisfies the same level of conventional and random differential privacy, respectively, yet it leads to more utility loss in RNNs than FFNNs. Since RNNs were consistently rendered more vulnerable to MIAs and more difficult to be defended, this paper provides strong empirical evidence that the privacy risks of RNNs are more severe than FFNNs.

2 PRELIMINARIES

In this section, we first review some background about the differences between RNNs and FFNNs. Then, we introduce the machine learning tasks that we consider in the experiments.

2.1 Recurrent vs. Feed-Forward Architecture

A neural network comprises a collection of nodes, each of which accepts an input and produces an output according to a fixed mapping called an activation function. The architecture of a neural network determines how the nodes of the networks are connected to one another. In a feed-forward architecture, the nodes can be stacked into an ordered sequence of layers from the network’s input to its output such that the output of each node only affects the nodes in the subsequent layers. Examples of FFNNs include multi-layer perceptrons (MLPs), convolutional neural networks (CNNs), and more sophisticated designs such as transformers [59].

In a recurrent architecture, the connections between the nodes may form a cycle. The backward connection between an RNN’s nodes can be unfolded into an infinite sequence of layers, each of which represents the node activations at different time steps. Therefore, an RNN’s output depends on the entire history of its inputs, which results in exhibiting a temporally dynamic behavior. Such features make RNNs suitable for processing sequential data such as sentences, videos, and audio [13].

FFNNs can also exhibit a temporally dynamic behavior through cascading MLPs or CNNs, or, more intelligently in transformers; however, the outputs in these methods only depend on a finite window in the history of inputs. Therefore, RNNs appear to be more expressive than FFNNs. On the other hand, it is easier to parallelize the training of FFNNs [17]. For example, generative pre-trained transformers [45] leverage parallelization to train natural-language processing models on very large datasets. Furthermore, making predictions based on the entire history of inputs may be unnecessary as theoretically shown in [55]. As a result, there has been an increasing interest—with many successful instances—in replacing RNNs with FFNNs [10, 17, 38, 59].

2.2 RNN Applications Considered

In the experiments, we consider three representative machine learning tasks: image classification, machine translation, and deep reinforcement learning. In the sequel, we briefly introduce each of the

tasks. Then, we state some of the possible privacy harms that MIAs may cause specific to these tasks.

In the image classification task, the model must label a given image using a fixed set of classes. The model’s output is a probability vector that determines its confidence in assigning each of the labels to the given image. CNNs are dominantly used in image classification [16, 19, 27]; however, RNNs may also be used to process images as a sequence of pixels [60].

In image classification tasks, the models may be trained with labeled image datasets that contain sensitive information. For example, consider a healthcare provider who fine-tunes a medical image classifier to predict the risk factors pertaining to a certain disease for a certain minority population. In this case, an MIA with access to an aggregated list of patient records can infer whether or not some of the data subjects belong to the considered minority group.

In the machine translation task, the model must map a sequence of words, syllables, or otherwise tokens from a fixed input dictionary to a target dictionary. Both RNN and FFNN solutions use an *encoder-decoder* framework. The first half of the model—the encoder—computes an encoding of the input sequence through multiple encoder layers. Subsequently, the second half of the model—the decoder—uses the encoding and generates an output sequence through multiple decoder layers. The output of the model is a sequence of probability vectors over the target dictionary words. The dictionaries are appended with start and end tokens to signal the start and completion of sentences, respectively.

Recurrent architectures such as bi-LSTM [65] use a network of long-short term memory (LSTM) units to construct both the encoder and the decoder networks and can process arbitrary-length sequences. Feed-forward architectures such as transformers [59] fix a window of sequence lengths allowed and construct the encoder and the decoder networks using FFNNs. Both of the above network architectures are widely used in machine translation; however, since the debut of transformers in 2017, they have outperformed RNN-based models [62].

As for the privacy risks that MIAs can pose to machine translation models, assume that some business analytics tool trains a model using internal meeting transcripts as training datasets. In this case, an MIA can infer whether or not a given sentence has been discussed in the meetings.

Finally, in the deep reinforcement learning task that we consider, an agent must learn how to navigate through an unknown map and reach a target state under partial state observations. At every state observation, the agent must compute a probability vector over the available actions, which is called a policy. Under partial state observations, the optimal policy may require memory [35] and RNNs can be integrated with deep reinforcement learning algorithms to capture long-term dependencies [7]. Both MLPs and LSTMs are commonly used in deep reinforcement learning algorithms such as soft actor critic [21], proximal policy optimization (PPO) [54], etc.

In deep reinforcement learning tasks, an MIA can infer whether or not specific locations have been used to train the agent. For example, a new owner of an autonomous vehicle may be able to infer whether or not the previous owner has visited certain locations, thereby violating the previous owner’s location privacy.

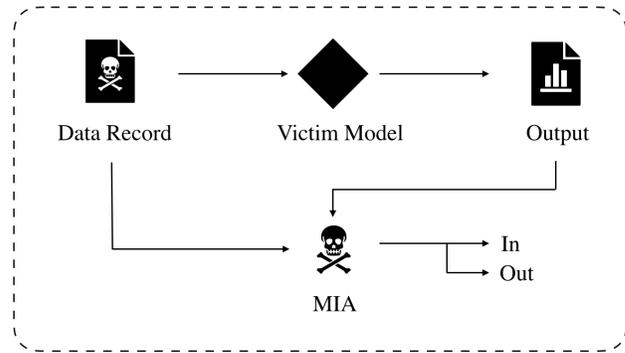


Figure 1: Schematic of the execution of an MIA.

3 METHODS

In this section, we describe the threat model that we consider for MIAs. Then, we lay out the methodology that we use to design the MIAs in the experiments and compare the MIA layouts with existing MIAs in the literature.

3.1 Threat Model and Assumptions

There exist two parties in the threat model that we consider: a victim and an attacker. The victim aims to train a neural network for a given machine learning task and a given training dataset. For example, the victim may train an image classifier using a dataset of labeled images. In order to train the neural network, the victim must choose a training algorithm alongside its hyperparameters, loss function, and neural network specifications—including the number of hidden layers, number of nodes per layer, architecture, activation functions, etc. Once the victim’s neural network is fully trained, the victim proceeds with generating predictions for outsider inquiries, i.e., the victim receives a data record and subsequently responds by publishing its predictions for the received data.

The attacker in the considered threat model conducts an MIA; that is, it submits an inquiry to the victim using some data record and must infer whether or not the data record belongs to the victim’s training dataset as depicted in Figure 1. MIAs are typically categorized into two groups: black-box and white-box attacks [25]. The former group assumes that the attacker can only access the input and the output of the victim’s neural network. White-box attackers may have access to the value of the weights and the output of the nodes anywhere in the victim’s neural network. Additionally, white-box attacks may also probe the victim’s loss function and its gradient for the queried data record.

In terms of the side-information that is available to the attacker, the survey in [25] assumes that a black-box MIA’s side-information is limited to the distribution of the training data—implying that the attacker can obtain a training dataset that is similar to that of the victim. The survey considers any additional assumption on the available side-information as an indicator of white-box attacking. However, such a distinction about side-information is not uniformly followed in the literature; for example, the work in [56] assumes that the attacker knows the training algorithm of the victim, and the MIAs in [49] are provided with side-information about the

victim’s training algorithm, hyperparameters, and the network specifications, yet both works consider their MIAs as black-box attacks. Access to the value of the loss function and its gradient is the key enabler that enhances the attack accuracy in white-box attacks as empirically demonstrated by [40]. We therefore draw the line between black-box and white-box attacks based on the access granted to the attacker and not the side-information.

We now state our assumptions on the attacker’s access limits and side-information. In terms of access limitations, we assume that the attacker has black-box access to the input and output layers of the victim’s neural network. The attacker is able to access the input layer via submitting an unlimited number of inquiries and is able to observe the output layer via evaluating the confidence scores with which the victim responds to an inquiry. In terms of the side-information that is available to the attacker, we assume that the attacker knows the victim’s task, training algorithm alongside its hyperparameters, and the network specifications.

The authors of [49] show that an optimal MIA—under mild assumptions on the distribution of the neural network’s parameters—utilizes the victim’s full confidence scores. Our goal in the experiments is to investigate whether or not the architecture of a neural network affects its vulnerability to MIAs. As a result, we assume full confidence-score observability in the threat model in an effort to maximize the accuracy of the MIAs and control the variables that have the potential of affecting the accuracy of MIAs besides architecture.

3.2 Designing MIAs

We follow the framework of *shadow models* [56] in designing the MIAs in this paper. Intuitively, a shadow model must mimic the victim’s behavior without having access to its training dataset. Following the assumption that the attacker knows the victim’s training data distribution, we assume that there exists a data source from which the attacker can obtain a similar training dataset to train a shadow model—see Figure 2. In order to increase accuracy, MIAs often obtain multiple training datasets from the data source and subsequently train multiple shadow models to better mimic the victim’s behavior.

For the image classification and machine translation tasks, we allocate two disjoint partitions of a large dataset to the victim and the attacker, separately. Analogously for the deep reinforcement learning task, we use two disjoint sets of environment maps for the victim and the attacker to train their models.

In the next step, the attacker splits its training dataset into two partitions. The first partition will be used to train the shadow models following the side-information that the attacker has regarding the victim’s training algorithm and network specifications. Once the shadow models are trained, the attacker is provided with a proxy to the victim’s neural network. The attacker knows which data records it has used to train the shadow models and it knows that the second partition has not been used to train any of the shadow models. Therefore, the attacker can train a binary classifier to distinguish between the outputs that correspond to member data and those corresponding to non-member data. The attacker can then use the binary classifier against the victim to execute the MIA as depicted in Figure 1.

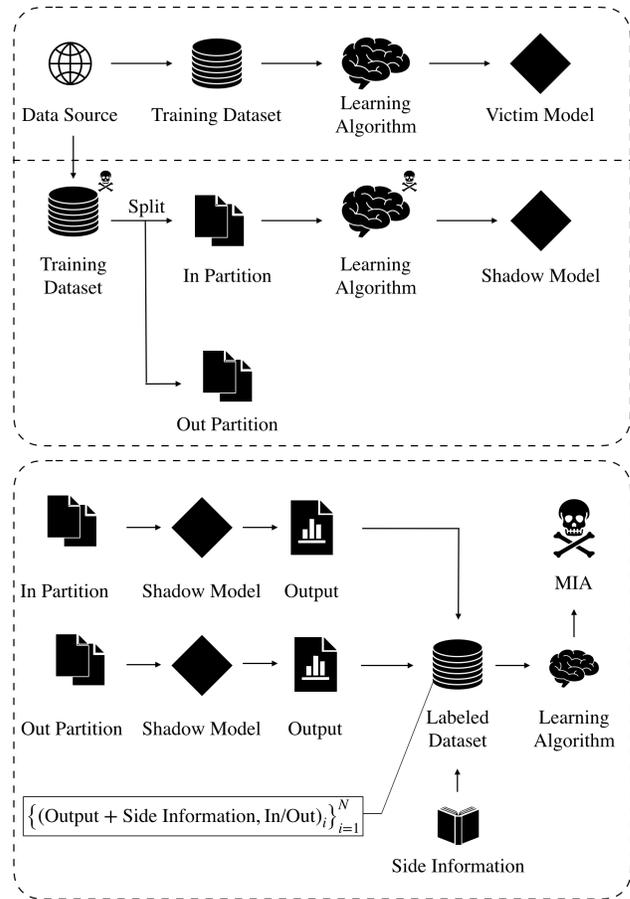


Figure 2: Top: a schematic of training shadow models. The skull above the shadow model’s training dataset and learning algorithm indicates that the two components may differ between the victim and the attacker’s side. Bottom: training the MIA using the output of the shadow model and side-information.

Shadow-model-based MIAs typically use a 3-tuple format for the entries of the binary classifier’s training dataset as shown in the bottom box in Figure 2. Each entry corresponds to a query that is made from a shadow model and the query may originate from either partition of the attacker’s training dataset. The first element contains the shadow model’s output, the second element indicates what the shadow model’s optimal output must have been, and the third element indicates whether the query was made using a member data record or a non-member data record.

For the first element, we use the shadow model’s full confidence score in vector format. If the shadow model’s output is a sequence of predictions—as the case in machine translation and deep reinforcement learning—we concatenate the confidence scores into one vector.

For the second element, we use the query’s corresponding label in the training dataset as a one-hot vector or a concatenation of a sequence of one-hot vectors—such labels are readily available in

the image classification and machine translation tasks. In the deep reinforcement learning task, such a labeled training dataset does not exist; we, therefore, train a “labeling agent” to generate these labels. The labeling agent simply learns a reward-maximizing policy in the environment in which a shadow model’s policy is queried. For each state observation at which the shadow model’s policy is queried, the labeling agent provides its policy as a reference label.

Once the binary classifier’s training dataset is fully populated, the attacker uses the first two elements as features and uses the third element as binary labels—member or non-member—and concludes the design of the MIA by training a binary classifier that distinguishes between member and non-member queries. The attacker then uses the trained binary classifier against the victim to execute the MIA as shown in Figure 1.

3.3 Connection with the Existing MIAs

We now state how the MIAs implemented in this paper compare with the existing MIAs in the literature. Regarding the image classification task, our MIA design is identical to the design in [56]. However, for the machine translation and deep reinforcement learning experiments, the existing MIAs have minor incompatibilities with this paper’s threat model which we address by modifying them.

The works in [24, 57] study developing MIAs specifically for machine translation models. However, neither of the two existing works assume full confidence-score observability because they both aim to design practical MIAs with minimal side-information assumptions. In particular, the authors of [57] develop an MIA that is intended to be used by individuals who wish to *audit* a natural language processing model—a process by which the individuals investigate whether or not their data has been used to train a natural language processing model. In this scenario, full confidence-score observability is not realistic and the authors feed a redacted list of the output word rankings to the MIAs, instead. We use the same MIA design as [57] except that we use full confidence scores instead of word rankings.

The authors of [24] use a similar design, but they take a further step towards developing practical MIAs and drop the assumption that the MIA knows the underlying distribution of the training data. However, the authors find that the resulting MIAs are not effective as their accuracy does not exceed random guessing by much.

We now review the existing MIAs in deep reinforcement learning tasks. The work in [41]—which we follow closely in our MIA design for deep reinforcement learning—is the first to consider a privacy attack against reinforcement learning agents that resembles MIAs. However, instead of modeling the MIA as a binary classifier, the privacy attack uses a multi-class classifier. As a result, the attacker must train a labeling agent for every possible environment map prior to the execution of the attack. By using a binary classifier, we train labeling agents only for the environment map with which the MIA is faced. In another work, the authors of [18] develop an MIA that infers the membership of a batch-constrained deep Q-learning agent’s roll-out trajectories stored in its replay buffer. We do not follow the above work’s methodology because we do not restrict the algorithm that is used to train the reinforcement learning agents.

4 VULNERABILITY TO PRIVACY THREATS

In this section, we report and analyze the results of a series of experiments by which we compare the vulnerability of RNNs and FFNNs to MIAs. In order to perform a meaningful comparison, we must control factors that affect vulnerability to MIAs other than network architecture. We review these vulnerability factors and discuss how we take them into account in our experimental setup. Finally, we report and analyze the numerical results.

4.1 Vulnerability Factors

Overfitting has been extensively studied as the main source of the vulnerability of machine learning models to MIAs [25]. Overfitting refers to the condition in which a machine learning model performs poorly when queried with data records outside its training dataset. There exist mounting empirical evidence that MIAs are more successful against models that overfit their training data [51, 56]. However, there also exist successful instances of MIAs used against models with relatively low overfitting [32]. In these instances, the underlying distribution of the training data as well as the size of the training datasets may leave some data records more vulnerable than others. By identifying such data records, MIAs may still maintain a high attack accuracy for models with low overfitting [25].

A theoretical account of the connection between overfitting and MIA accuracy remained unknown until the work in [66]. The said work characterizes overfitting by *average generalization error* defined as

$$R_{\text{gen}} = \mathbb{E}_{\substack{S \sim \mathcal{D}^n \\ z \sim \mathcal{D}}} [\ell_S(z)] - \mathbb{E}_{\substack{S \sim \mathcal{D}^n \\ z \sim S}} [\ell_S(z)], \quad (1)$$

where \mathcal{D} is the underlying distribution of the training data; S is the victim’s training dataset comprising n samples drawn from \mathcal{D} ; ℓ is a fixed loss function; and $\ell_S(\cdot)$ is the value of the model’s loss function after being trained with S .

Under the assumption that the victim’s loss function is bounded above and its value is accessible to the attacker, Yeom et al. establish that a higher average generalization error is a sufficient condition—but not necessary—for a higher attack accuracy [66]. The authors further provide empirical evidence that the sufficiency relationship holds when the assumptions are relaxed to black-box MIAs. Later, a theoretical account of the relationship between the generalization gap—training accuracy minus validation accuracy—and the accuracy of black-box MIAs was provided in [3].

In light of the established relationship between overfitting and attack accuracy, we are mindful to consider RNNs and FFNNs with similar training and validation performance levels. In order to control the effect of the size and the distribution of the victim’s training dataset on vulnerability to MIAs, we use the same training dataset for both of the RNN and FFNN models. As the vulnerability to MIAs may not be evenly distributed across a collection of data records [32], we evaluate the MIAs against the RNN and FFNN models using the same dataset. Finally, we consider RNNs and FFNNs whose number of parameters are close because it has been empirically demonstrated that a higher number of parameters increases vulnerability to MIAs [40].

4.2 Experimental Setup

We consider three representative machine learning tasks for the experiments of this section: image classification, machine translation, and deep reinforcement learning. In image classification, consistent with the threat model, we assume that there exists a data source that generates labeled image samples and use the CIFAR10 dataset [26] as 50,000 samples drawn from the data source. We split these samples evenly into two partitions: one used by the victim and the other used by the attacker for the training of the shadow models—we train 5 shadow models.

With the victim’s portion of the training samples, we separately train an FFNN model and an RNN model. The FFNN model is an instance of ResNet101 [23] implemented in the Keras library [9] and specified as follows: 101 convolutional layers followed by one max-pooling layer, one fully connected linear layer, and an output layer with softmax activation. For the RNN model, we use ResNet [60] implemented by PyTorch [43] under default parameters, which has the following specifications: 4 bi-directional LSTMs, 2 fully connected layers with ReLU activation, and an output layer with softmax activation. The former model contains 42,678,666 trainable parameters and the latter has 42,569,590 trainable parameters. Both models use the categorical cross-entropy loss function as their learning’s objective function and use the Adam optimizer. The learning rates used are 0.001 and 0.01 for the former and the latter model, respectively. The shadow model of the MIAs uses the same specifications as the victims for their training.

For the machine translation experiments, we choose a translation from French to English. Similar to image classification, we assume there exists a data source from which translated pairs of English and French sentences can be sampled. We take the Multi30K dataset [15] as 30,000 samples from the data source and split the samples evenly between the victim and the attacker.

For the RNN model, we use a bi-directional LSTM with a dot-product attention mechanism developed in [34]. For the FFNN model, we use the standard transformer network specified in [59]. The RNN model and the FFNN model have 3,213,191 and 3,225,714 trainable parameters, respectively. Both networks use the negative log-likelihood function as their learning algorithm’s loss function and use Adam optimizer with a learning rate of 0.001.

Finally, for the deep reinforcement learning task, we use the MiniGrid-MultiRoom-N4-v0 environment from the MiniGrid toolkit [8]. The victim’s goal is to train a deep reinforcement learning agent that can navigate its way through four rooms with closed doors and reach the green tile as shown in Figure 3. The victim is provided with a limited number of floor-maps for training and must generalize to unseen floor-maps. The attacker’s goal, on the other hand, is to infer the membership of floor-maps. In this experiment, the MiniGrid toolkit serves as the data source and the attacker is able to obtain an arbitrary number of floor-maps by feeding a randomly generated seed number to the toolkit’s simulator.

For the FFNN agent, we use an MLP network with 5,335 trainable parameters and the following specifications: the actor network has two hidden layers with dimension 74, and the critic network has 2 hidden layers with dimension 64. Both networks use a softmax output layer and tanh as their activation function. The RNN agent uses an MLP with some additional LSTM cells. The RNN

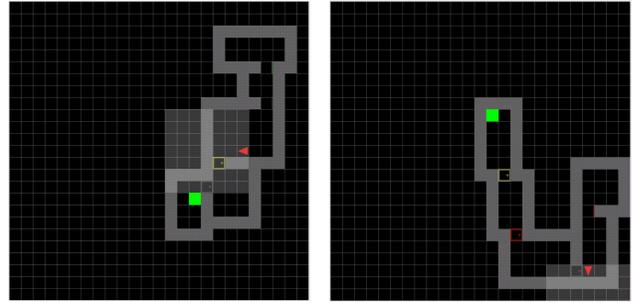


Figure 3: The MiniGrid-MultiRoom-N4-v0 environment. The agent (red triangle) must find the goal state (green square) while observing the highlighted box that surrounds it. The environment consists of multiple floor maps, two of which are shown above.

has 5,216 trainable parameters and its specifications are as follows: both the actor and the critic networks have 2 linear layers with hidden dimension 32, 4 single-directional LSTM cells, and a softmax output layer. We use the PPO algorithm [54] implemented by the RL-Starter-Files library [61] with default parameters to train the victim agents and their respective shadow models and labeling models.

4.3 Numerical Results

Following the experimental setup above, we train each of the described RNN and FFNN models for a range of epoch numbers and plot the training and validation performance of the models. For the image classification experiment, we use the percentage of the correct predictions—or prediction accuracy—as the performance measure; for machine translation, we measure performance using the bilingual evaluation understudy (BLEU) score [42], which captures how a model’s translation correlates to that of a human; and for deep reinforcement learning, we use the total episodic reward as the performance measure. The reward at time-step t is

$$r(t) = \begin{cases} 1 - \gamma \frac{t}{T}, & \text{goal reached,} \\ 0, & \text{otherwise,} \end{cases} \quad (2)$$

where T is the episode length—set to 200 in the experiments—and γ is the discount factor—set to 0.9.

At every epoch number tested, we train a separate MIA whose shadow models are trained for the same number of epochs as that of the victim. We evaluate the performance of the MIAs by measuring the percentage of correct inferences which we refer to as attack accuracy. In all instances, the MIAs’ validation datasets have an equal number of members and non-member records; hence, random guessing in this case achieves 50% attack accuracy.

In Figure 4, it can be observed that the attack accuracy against the RNN models is consistently higher than it is against FFNN models. In particular, The RNNs are more vulnerable before and after the performance level of the victims converges; however, the gap between the attack accuracy of the two MIAs narrows as the models train for higher epoch numbers.

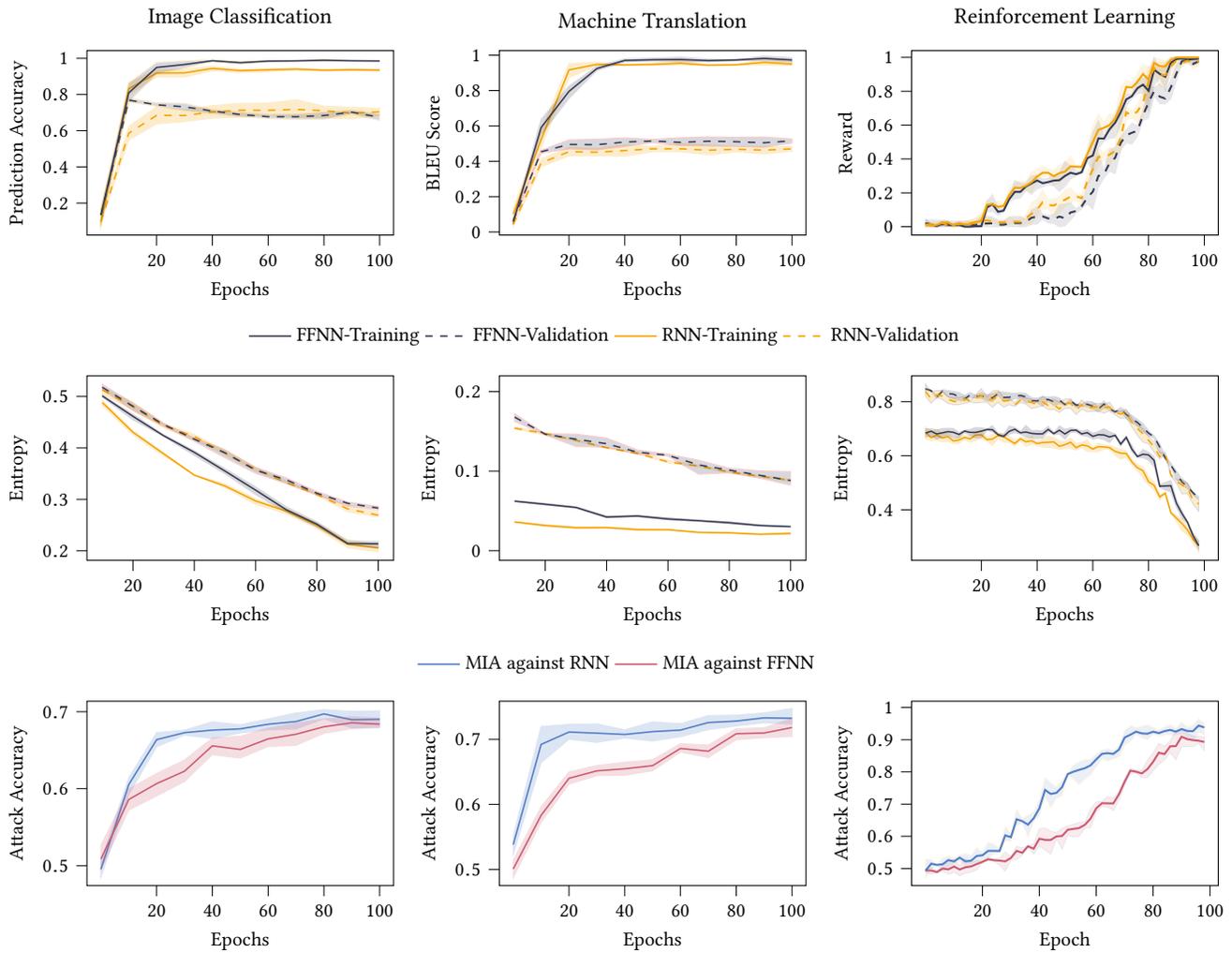


Figure 4: Comparing the vulnerability of RNNs and FFNNs to MIAs in three representative machine learning tasks: image classification (left), machine translation (center), and deep reinforcement learning (right). The first row plots training and validation performance vs. number of epochs; the second row plots the average prediction entropy vs. number of epochs; and the third row plots attack accuracy vs. number of epochs.

In the image classification experiment, the validation performance of the RNN and FFNN models are approximately equal. The FFNN model has a higher generalization gap than the RNN model upon convergence, and it has slightly more trainable parameters, yet surprisingly, the attack accuracy against the FFNN model is lower than the RNN model. In the machine translation experiment, the two models have approximately equal performance levels both in training and validation but the MIA against the RNN achieves a higher attack accuracy. Finally, in the deep reinforcement learning experiment, the two models appear to have a zero generalization gap upon convergence, yet the MIA against the RNN model is more accurate than it is against the FFNN model.

Prediction Entropy as a Vulnerability Factor: In order to further investigate the reasons behind the excessive vulnerability of RNNs to MIAs, we measure the uncertainty of the models’ outputs in terms of *average prediction entropy*, which we define as follows: let m be the number of prediction categories and $Y = \left\{ \left(y^{(i)}, p^{(i)} \right) \right\}_{i=1}^L$ be a sequence of L pairs of prediction outcomes and confidence scores, respectively. Then, the corresponding average prediction entropy is

$$H_{\text{APE}}(Y) = -\frac{1}{L} \sum_{i=1}^L \sum_{j=1}^m p_j^{(i)} \log \left(p_j^{(i)} \right). \quad (3)$$

We report the average prediction entropy of the RNN and the FFNN models in Figure 4. The results show that, while the prediction entropy of the two models is approximately equal over the

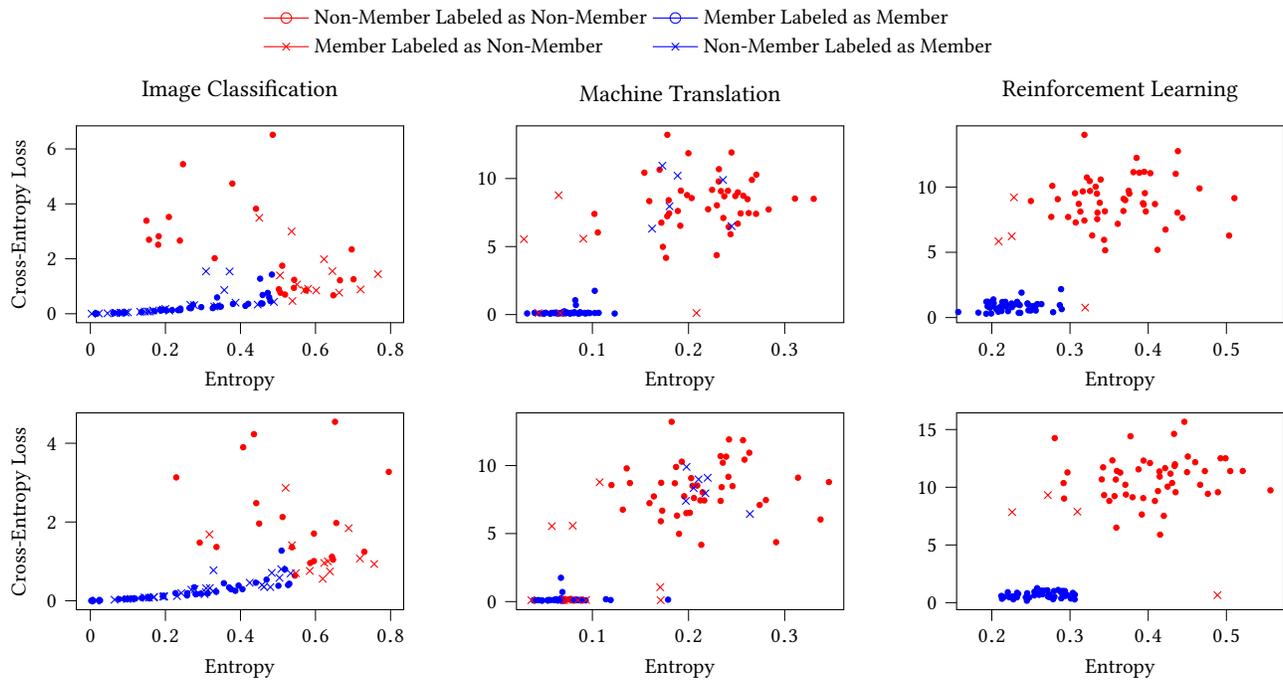


Figure 5: An illustration of the decision boundaries of MIAs with respect to cross-entropy loss and entropy of the confidence scores. The top row shows the results for RNNs and the bottom row shows the results for FFNNs.

validation dataset, their prediction entropy with respect to their training data differs noticeably—at least in the early stages of training. In the initial stages, the entropy gap between the validation and the training dataset in RNNs is larger than FFNNs. As the training prediction entropy of the FFNN model approaches that of the RNN model, the gap between the attack accuracy of the two MIAs narrows. As a result, the ability of RNNs to maintain a lower prediction entropy than FFNNs vis-à-vis member data records may render them more vulnerable to MIAs.

In the next experiment, we demonstrate that the MIAs are indeed sensitive to the entropy of the victim’s predictions. To illustrate this, for each inference made by the MIA, we measure the victim’s cross-entropy loss—as a performance measure—and we measure the prediction entropy of the victim. Then, we generate a scatter plot in which the y-axis represents cross-entropy and the x-axis measures prediction entropy. We use two colors to distinguish between member and non-member inferences made by the MIA and use a distinct marker to represent erroneous inferences. The results in Figure 5 suggest that the MIAs divide the scatter area into 4 quadrants and label data records with cross-entropy loss below a certain threshold and entropy below a certain threshold as member data.

Model Memorization as a Vulnerability Factor: In the last experiment, we demonstrate that the RNN and FFNN models also differ in the way they retain their performance with respect to member data post-training. If a model responds to a post-training query using member data with the same accuracy as it previously held while being trained with that member data, we say that the

model has *memorized* its training data. If the model’s accuracy for such a query decreases after training, we say that the model has *forgotten* the training data.

Model memorization, if not associated with overfitting, is favorable from a performance-maximizing perspective. For example, in the deep reinforcement learning experiment, both the RNN and the FFNN agents reach the goal state within roughly 35 time steps when validated in unseen floor maps. However, when the RNN agent is queried in a member floor map, it reaches the goal in approximately 20 time steps, whereas the FFNN agent still reaches the goal in 35 time steps. As a result, the RNN agent appears to memorize the floor maps whereas the FFNN agent seems to forget. We note that the reward function used in the training of the agents is relatively insensitive to the number of steps taken to reach the goal. Instead, it is more sensitive to whether or not the agent reaches the goal at all in an episode. In particular, a 75% increase in the number of steps from 20 to 35 decreases the total reward only by 7.42% according to (3). Hence, the RNN agent appears to memorize the floor maps even though it was not specifically incentivized by the reward system to do so.

From a privacy perspective, such discrepancies between a model’s performance with respect to seen and unseen data are harmful as they can be exploited by an adversary via MIAs. To illustrate this, we partition the training datasets into a collection of disjoint batches of data and assign an order to each batch arbitrarily at random. We then use these batches sequentially to train the RNN and FFNN models. Once the two models are trained, we report the accuracy of the MIAs with respect to the percentage of correct inferences

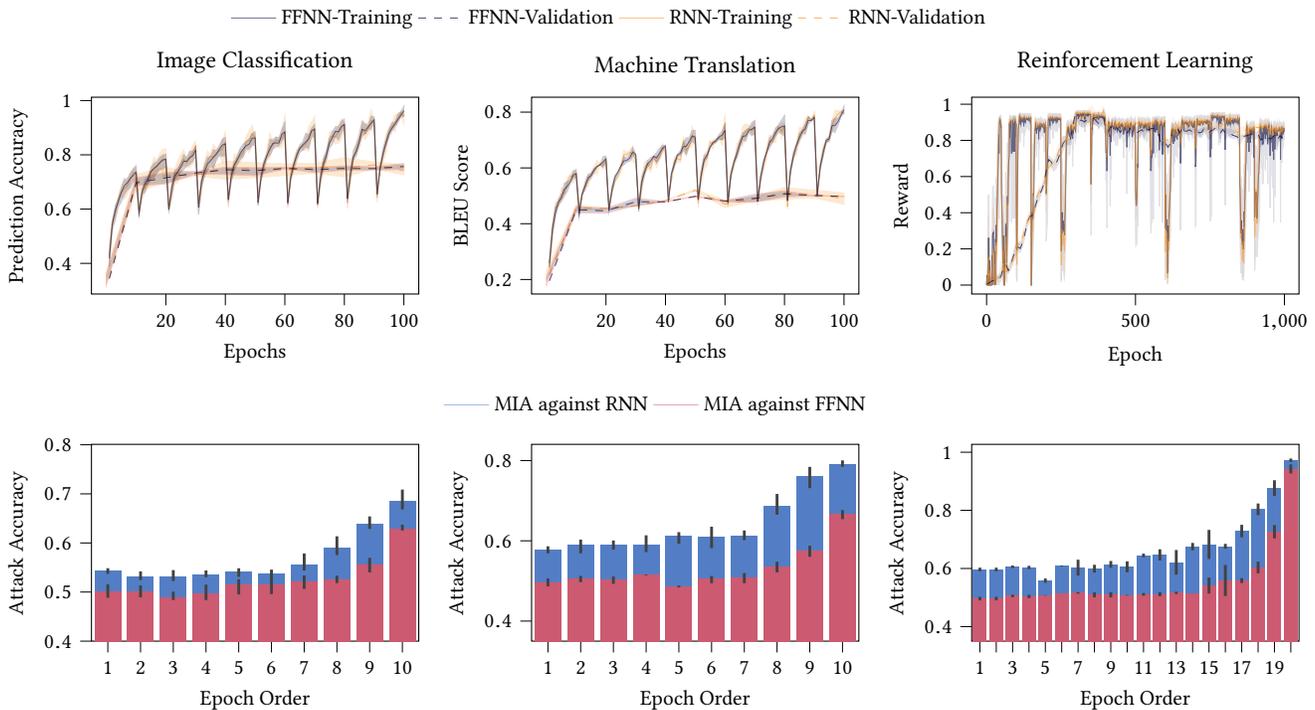


Figure 6: Comparing model memorization in RNNs and FFNNs. The top row plots the training and validation performance of the models when trained sequentially with a collection of ordered batches of training data. The saw-tooth pattern in the training performance is common in sequential training of machine learning models and is due to the catastrophic interference phenomenon [36]. The validation lines are smoothed out by measuring performance at the end of every 10 epochs. The bottom row plots the attack accuracy of the MIAs with respect to the individual epochs in the order in which they were introduced to the victims during training.

vis-à-vis each batch. The results in Figure 6 indicate that the MIAs’ accuracy for older batches of data in FFNNs quickly diminishes to 50%, whereas in RNNs, the MIAs maintain non-trivial accuracy even for the early batches of data. As a result, we posit that model memorization is another factor that renders RNNs more vulnerable to MIAs than FFNNs.

5 PREEMPTING PRIVACY THREATS

In this section, we shift the focus from studying vulnerability to studying defense methods against MIAs. We first briefly discuss regularization methods, then, we study methods that leverage the promise of differential privacy.

5.1 Defense via Regularization

We now investigate the effects of overtraining and regularization in the considered machine learning tasks. Increasing the training time of machine learning algorithms often results in overfitting. For example, the validation performance of the FFNN model in the image classification task decreases after training for 10 epochs in Figure 4, whereas its training performance keeps increasing. On the other hand, training machine learning models for an extended number of epochs may not always lead to overfitting. Such a phenomenon

in RNNs was first reported in [57] for natural language processing models which is consistent with our results in Figures 4.

Regularization methods such as ℓ_2 -regularization are effective in preventing overfitting and they have been shown to be effective in reducing the vulnerability of FFNN image-classification models to MIAs [51, 56]. However, regularization may add bias to the converging performance levels because they alter the objective function. In particular, these methods compute the ℓ_2 -norm of the node activations as a penalty term, which is subsequently multiplied with a regularization coefficient λ and added to the model’s loss function. In Figure 7, we observe that regularization affects the FFNN and RNN models in the image classification and machine translation experiments differently. In particular, the MIA accuracy in the FFNN models is highly sensitive to the regularization coefficient λ , whereas the MIA accuracy against RNN models is impacted by regularization only marginally.

For the deep reinforcement learning agents, we test a different method of regularization. It is common in deep reinforcement learning algorithms such as the PPO and trust-region policy optimization (TRPO) [53] to regularize the Kullback-Leibler divergence between the policy updates in order to increase model stability [30]. In the PPO algorithm, which we use to train the RNN and FFNN agents in the deep reinforcement learning experiment, a parameter called the

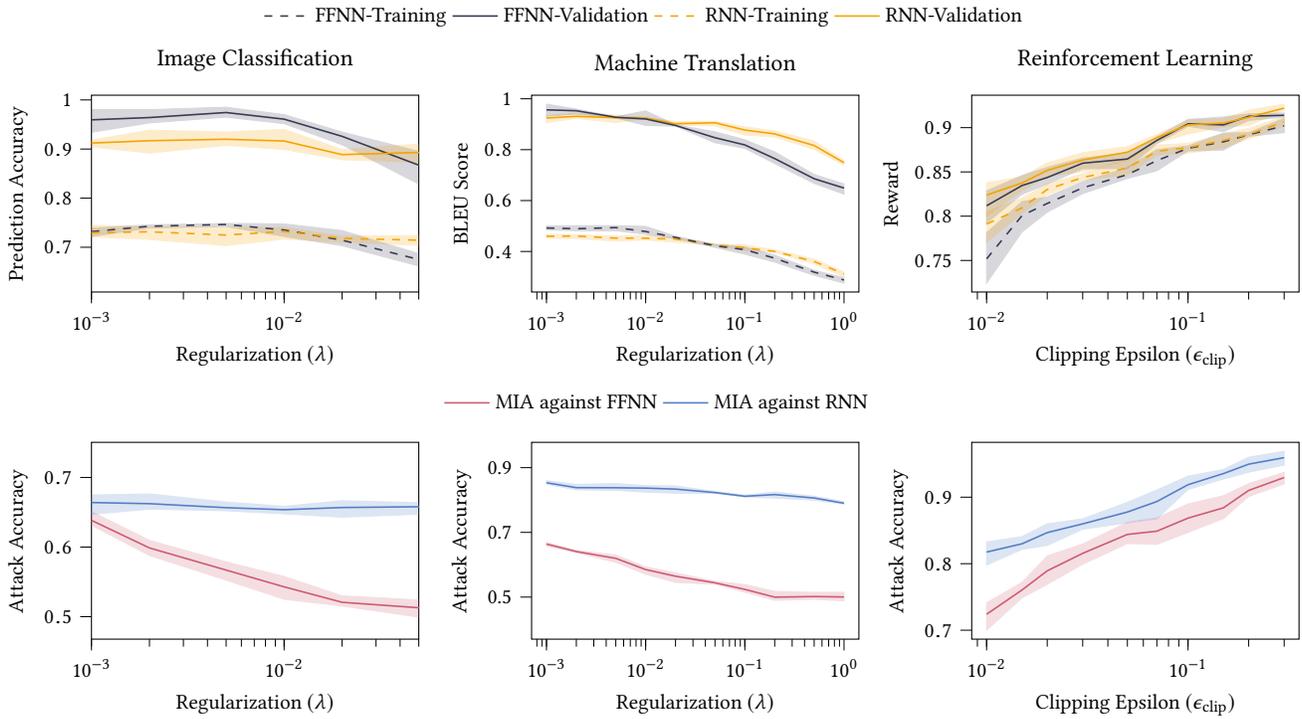


Figure 7: Effects of regularization on attack accuracy. From the left to the right column: image classification, machine translation, and deep reinforcement learning. The MIAs are trained separately for each regularization value tested and the shadow models use the same parameters as their victims.

clipping epsilon ϵ_{clip} controls the policy updates as follows: a small value of ϵ_{clip} prevents the agent from taking large gradient steps whereas a large epsilon does not restrict the agent as much. In this case, the validation performance of both the RNN and FFNN agents is sensitive to regularization. However, the RNN agent remains more vulnerable to the MIA than the FFNN agent, and its respective MIA accuracy is relatively less sensitive to regularization based on the corresponding line slopes.

5.2 Defense via Differential Privacy

Differential privacy is a characteristic of an algorithm and provides a quantitative definition of data privacy [14]. A differentially private algorithm makes it hard for any observer to link the algorithm’s outputs to the individual entries of the dataset that contributed to generating that output. It is best justified to use differential privacy when the purpose of the algorithm is to compute some aggregate information about a dataset whose entries contain sensitive information. For example, the US Census Bureau uses differential privacy to protect the data subjects in its publications [2]. Differential privacy is formally defined as follows:

DEFINITION 1. Let $f : \mathcal{D} \mapsto \mathcal{R}$ be a query function from an input domain \mathcal{D} to an output domain \mathcal{R} . Define two datasets D and D' —both in \mathcal{D} —adjacent if the number of the entries in which the two datasets hold different values is at most one. Let $(\Omega, \mathcal{F}, \mu)$ be a probability space and \mathcal{M} be a σ -algebra such that $(\mathcal{R}, \mathcal{M})$ is measurable. For a given $\epsilon \geq 0$ and $\delta \in [0, 1]$, a mechanism $M : \mathcal{R} \times \Omega \mapsto \mathcal{R}$ satisfies

(ϵ, δ) -differential privacy if, for all $R \subseteq \mathcal{R}$ and all adjacent D and D' ,

$$P[M(f(D)) \in R] \leq \exp(\epsilon) \cdot P[M(f(D')) \in R] + \delta. \quad (4)$$

If a mechanism satisfies (4) with $\delta = 0$, it satisfies pure ϵ -differential privacy. Intuitively, the parameter ϵ captures the strength of privacy protections and δ captures the probability that pure ϵ -differential privacy fails. Privacy failure could happen due to two reasons: either (4) holds for a larger ϵ or no finite ϵ ever satisfies pure differential privacy. It is customary to choose single-digit values for ϵ and choose δ to be $\mathcal{O}(|D|^{-1})$, where $|D|$ is the size of the dataset that we wish to protect [14]. However, in some applications, even large values for ϵ may still provide a strong privacy shield [4].

Differential privacy is immune to post-processing, meaning that post-hoc computations on the output of a differentially private mechanism do not affect the level of differential privacy. Subsequent queries from the output of a differentially private mechanism may weaken privacy, however. In general, the overall privacy level of a sequence of k queries from an (ϵ, δ) -differentially private mechanism results in $(k\epsilon, k\delta)$ -differential privacy according to the Composition Theorem [14]. The overall privacy level is often referred to as the *privacy budget*. In applications wherein multiple queries are made from some sensitive dataset, one must be mindful of the total privacy budget expended.

5.2.1 Enforcing Differential Privacy. The methods that we use in this section to enforce differential privacy utilize the Gaussian

Algorithm 2: SENSITIVITYSAMPLER

Input: training algorithm $\mathcal{A}_{\mathcal{H}}$ with hyperparameters \mathcal{H} , sample size n , data source DS, training dataset size N ,

Output: \bar{S}

for $i = 1$ **to** n **do**

for $j = 1$ **to** $N + 1$ **do**

$d_j \sim \text{DS}$; /* Sample from the data source*/

end

$D_1 \leftarrow \cup_{j=1}^N d_j$;

$D_2 \leftarrow \left(\cup_{j=1}^{N+1} d_j \right) \setminus \{d_N\}$;

$\theta \leftarrow \mathcal{A}_{\mathcal{H}}(D_1)$; /* Train Model 1*/

$\theta' \leftarrow \mathcal{A}_{\mathcal{H}}(D_2)$; /* Train Model 2*/

$\bar{S}^{(i)} \leftarrow \|\theta - \theta'\|_2$;

end

$\bar{S} \leftarrow \max_i \bar{S}^{(i)}$;

loss-function smoothing; that is, at every iteration i ,

$$\theta_{i+1} = \theta_i - \eta \frac{1}{|X_i|} \sum_{x \in X_i} \text{CL} \left(\mathbb{E}_{Z \sim \mathcal{N}(0, \sigma_s^2 \mathbf{I})} [g_x(\theta_i + Z)], C \right), \quad (9)$$

where σ_s^2 is the smoothing variance. Let the loss function ℓ be L -Lipschitz, m be the minibatch size, and $\beta = L/\sigma_s$. Then, after training for T iterations, it holds that

$$S(\mathcal{A}_{\mathcal{H}}) \leq 2 \frac{(1 + \eta\beta)^T - 1}{(m - 1)\beta} C. \quad (10)$$

PROOF. See Appendix A.1. \square

The established sensitivity bound established under the assumptions of Theorem 5.2 immediately implies the differential privacy of the GPM due to Theorem 5.1. However, the upper bound in (10) grows exponentially with the training horizon T . It is often the case that upper bounds for sensitivity are too loose and empirical measurements of the sensitivity take much smaller values. The SENSITIVITYSAMPLER algorithm [48] in combination with the notion of *random differential privacy* [22] addresses such an issue. The former is an algorithm that estimates sensitivity and the latter is a relaxation of (ϵ, δ) -differential privacy.

DEFINITION 3. *The mechanism M in Definition 1 satisfies (ϵ, δ) -random differential privacy with confidence $\gamma \in (0, 1)$ if, for all adjacent datasets D and D' drawn from a fixed data source DS,*

$$\mathbb{P}_{\substack{D \sim \text{DS} \\ D' \sim \text{DS}}} \left[\forall R \subset \mathcal{R}, \mathbb{P}_{y \sim M(f(D))} [y \in R] \leq \exp(\epsilon) \cdot \mathbb{P}_{y' \sim M(f(D'))} [y' \in R] + \delta \right] \geq 1 - \gamma. \quad (11)$$

Compared to (ϵ, δ) -differential privacy wherein δ captures the probability of privacy failure due to unlikely *outputs*, random differential privacy considers γ as the probability that (ϵ, δ) -differential privacy fails due to unlikely *input* datasets [48].

We use the SENSITIVITYSAMPLER algorithm in the context of training a neural network for machine learning as described in Algorithm 2. The algorithm repeatedly samples two adjacent training datasets from a fixed data source, invokes the training algorithm for both of the sampled training datasets, and estimates the sensitivity of the training algorithm based on the maximum 2-norm difference between the observed network parameters. The following theorem, which is an immediate result of Corollary 20 of [48], establishes the random differential privacy of the GPM.

THEOREM 5.3. *Fix a set of hyperparameters \mathcal{H} and training algorithm $\mathcal{A}_{\mathcal{H}}$. Let \bar{S} be the output of Algorithm 2 run with n samples. Further, let*

$$\rho = \exp \left(\frac{1}{2} W_{-1} \left(-\frac{1}{4n} \right) \right) \quad \text{and} \quad \gamma = \rho + \sqrt{\frac{\log(1/\rho)}{2n}}, \quad (12)$$

where W_{-1} is the Lambert W function defined as the inverse relation of the function $f(z) = z \exp(z)$. With σ the variance of the Gaussian mechanism in Algorithm 1, for all $\epsilon > 0$ and

$$\delta = \Phi \left(-\frac{\epsilon}{\mu} + \frac{\mu}{2} \right) - \exp(\epsilon) \Phi \left(-\frac{\epsilon}{\mu} - \frac{\mu}{2} \right), \quad (13)$$

where $\mu = \bar{S}/\sigma$, Algorithm 1 satisfies (ϵ, δ) -random differential privacy with confidence γ .

With the theoretical preliminaries set in this subsection, we now move on to the experiments.

5.2.2 *Experiments.* Similar to Section 4 in which we compared vulnerability to MIAs, we consider RNN and FFNN models in three representative machine learning tasks, namely image classification, machine translation, and deep reinforcement learning. However, for the machine translation task, we fine-tune a pre-trained model, BERT [11], with a subset of training samples from the WMT14 English-French training dataset [5] instead of training a model from scratch using the Multi30K dataset. WMT14 contains substantially more samples than Multi30K and is therefore more suitable for the SENSITIVITYSAMPLER algorithm.

In the first experiment, we use the DP-SGD algorithm to enforce differential privacy using a range of values for noise variance. Then, we measure the cost of privacy in terms of utility loss, which we formally define as follows:

DEFINITION 4. *Let \mathbb{M} be an evaluation metric that takes as input a set of predictions Y alongside their ground-truth labels Y_{GT} , and returns a numerical value that indicates the quality of the predictions. Then, the utility loss is*

$$\mathcal{L}_{util} = 1 - \frac{\mathbb{M}(\hat{Y}, Y_{GT})}{\mathbb{M}(Y, Y_{GT})}.$$

We now report the results. The top row of Figure 8 indicates that the RNN models consistently trade-off more utility than the FFNN models at every noise variance tested. The same level of noise translates to the same level of (ϵ, δ) -differential privacy in DP-SGD; as a result, enforcing the same level of (ϵ, δ) -differential privacy is more costly in RNNs than FFNNs with respect to utility loss.

A similar observation can be made when the GPM enforces random differential privacy for the RNN and FFNN models. In this experiment, we fine-tune the hyperparameters of the training algorithms such that: (i) the two models achieve similar validation

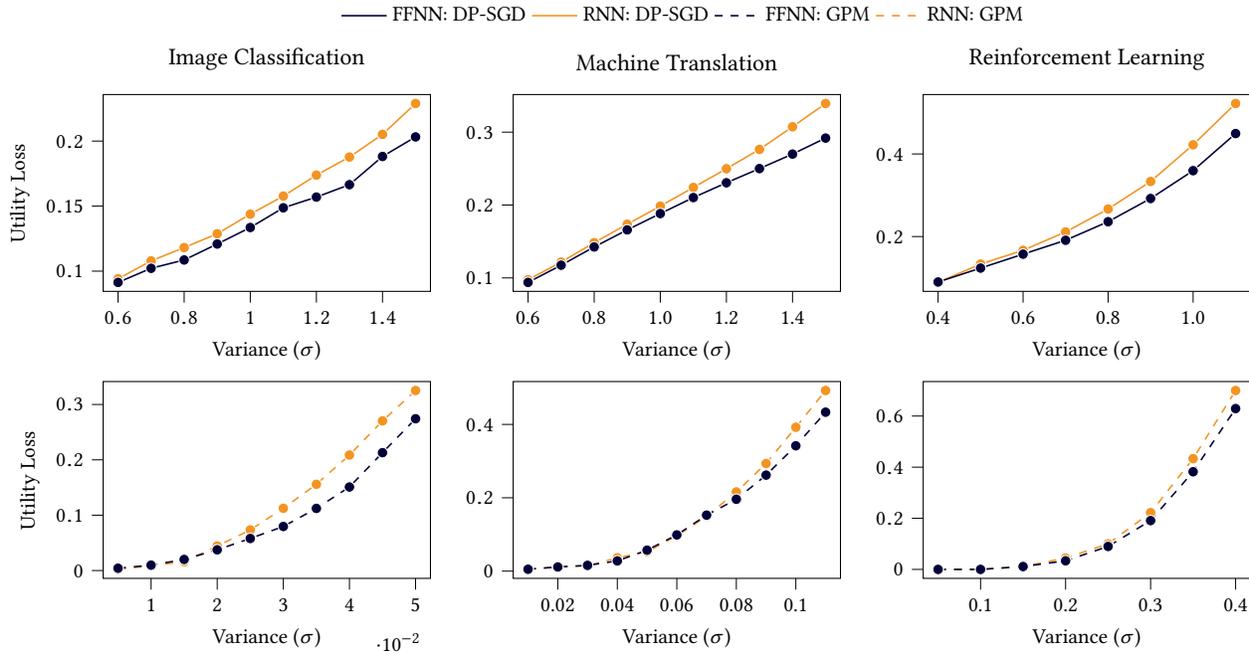


Figure 8: The privacy-utility trade-off of DP-SGD and GPM. The top row corresponds to the utility loss caused by DP-SGD and the second row corresponds to the utility loss caused by the GPM. The RNNs consistently trade off more utility than FFNNs for both DP-SGD and GPM.

performance levels before the GPM is deployed and (ii) Algorithm 2 estimates the same level of sensitivity for the two models as reported in Table 1. We refer to these estimates as *empirical sensitivity*. The empirical sensitivities in Table 1 correspond to $n = 500$ samples which translates to confidence $\gamma < 0.08$ established by (12) in Theorem 5.3.

Table 1: Empirical sensitivity estimated by Algorithm 2.

Task	\bar{S}_{RNN}	\bar{S}_{FFNN}
Image Classification	0.013209	0.013518
Machine Translation	0.11678	0.11845
Reinforcement Learning	0.093682	0.093429

In Figure 8, where we plot utility loss vs. noise variance, it can be observed that deploying the GPM consistently trades off more utility in RNNs than FFNNs. The results in Figure 8 also illustrate that the RNNs trade-off more utility for the same level of random differential privacy because the sensitivities of the two models are approximately equal.

6 CONCLUSION

In this work, we provided empirical evidence that MIAs can achieve higher accuracy when they attack RNNs compared with their FFNN counterparts. We showed that RNNs maintain a larger entropy gap between the predictions corresponding to member data and those corresponding to unseen data as a key vulnerability factor that is more elevated in RNNs than FFNNs. We also found that RNNs

memorize their training data in a way that an MIA can maintain a non-trivial attack accuracy over the entire history of their training, whereas the corresponding attack accuracy for the FFNNs quickly drops to 50% as we move back in the training history.

In the second part of the study, we considered two prominent mitigation methods: weight regularization and differential privacy. Then, we showed that regularization was less effective in protecting RNNs compared to FFNNs. Moreover, we showed that enforcing differential privacy in RNNs can be more costly than FFNNs in terms of the privacy-utility trade-off.

We conclude this paper with the observation that the privacy risks of deploying RNNs in machine learning are higher than FFNNs with the same level of performance. Alongside the existing computational drawbacks of training RNNs, our results provide further incentives to replace RNNs with FFNNs.

ACKNOWLEDGMENTS

This research was supported in part by the Office of Naval Research (ONR) under Grant N00014-21-1-2502 and in part by the Air Force Research Laboratory (AFRL) under Grant FA9550-19-1-0169.

REFERENCES

- [1] Martin Abadi, Andy Chu, Ian Goodfellow, H Brendan McMahan, Ilya Mironov, Kunal Talwar, and Li Zhang. 2016. Deep learning with differential privacy. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*. ACM, New York, NY, USA, 308–318.
- [2] John M Abowd. 2018. The US Census Bureau adopts differential privacy. In *Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*. ACM, New York, NY, USA, 2867–2867.

- [3] Jason W Bentley, Daniel Gibney, Gary Hoppenworth, and Sumit Kumar Jha. 2020. Quantifying Membership Inference Vulnerability via Generalization Gap and Other Model Metrics.
- [4] Abhishek Bhowmick, John Duchi, Julien Freudiger, Gaurav Kapoor, and Ryan Rogers. 2018. Protection against reconstruction and its applications in private federated learning.
- [5] Ondrej Bojar, Christian Buck, Christian Federmann, Barry Haddow, Philipp Koehn, Johannes Leveling, Christof Monz, Pavel Pecina, Matt Post, Herve Saint-Amand, Radu Soricut, Lucia Specia, and Ales Tamchyna. 2014. Findings of the 2014 Workshop on Statistical Machine Translation.
- [6] Kamalika Chaudhuri, Claire Monteleoni, and Anand D Sarwate. 2011. Differentially private empirical risk minimization. *Journal of Machine Learning Research* 12, 3 (2011), 1069–1109.
- [7] Clare Chen, Vincent Ying, and Dillon Laird. 2016. Deep q-learning with recurrent neural networks. *Stanford Cs229 Course Report* 4 (2016), 3.
- [8] Maxime Chevalier-Boisvert, Lucas Willems, and Suman Pal. 2018. Minimalistic Gridworld Environment for OpenAI Gym. <https://github.com/maximecb/gym-minigrid>.
- [9] François Chollet et al. 2015. Keras. <https://keras.io>.
- [10] Yann N Dauphin, Angela Fan, Michael Auli, and David Grangier. 2017. Language modeling with gated convolutional networks. In *International conference on machine learning*. PMLR, MIT Press, Cambridge, MA, USA, 933–941.
- [11] Jacob Devlin, Ming-Wei Chang, Kenton Lee, and Kristina Toutanova. 2019. BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding. In *Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Volume 1 (Long and Short Papers)*. Association for Computational Linguistics, Minneapolis, Minnesota, 4171–4186.
- [12] Jinshuo Dong, Aaron Roth, and Weijie J Su. 2019. Gaussian differential privacy.
- [13] Samuel Dupond. 2019. A thorough review on the current advance of neural network structures. *Annual Reviews in Control* 14 (2019), 200–230.
- [14] Cynthia Dwork and Aaron Roth. 2014. The Algorithmic Foundations of Differential Privacy. *Found. Trends Theor. Comput. Sci.* 9, 3–4 (Aug. 2014), 211–407.
- [15] Desmond Elliott, Stella Frank, Khalil Sima'an, and Lucia Specia. 2016. Multi30K: Multilingual English-German Image Descriptions. <https://doi.org/10.18653/v1/w16-3210>
- [16] Paul Gavrikov and Janis Keuper. 2022. CNN Filter DB: An Empirical Investigation of Trained Convolutional Filters.
- [17] Jonas Gehring, Michael Auli, David Grangier, Denis Yarats, and Yann N Dauphin. 2017. Convolutional sequence to sequence learning. In *International Conference on Machine Learning*. PMLR, MIT Press, Cambridge, MA, USA, 1243–1252.
- [18] Maziar Gomrokchi, Susan Amin, Hossein Aboutaleb, Alexander Wong, and Doina Precup. 2021. Where Did You Learn That From? Surprising Effectiveness of Membership Inference Attacks Against Temporally Correlated Data in Deep Reinforcement Learning.
- [19] Benjamin Graham. 2014. Spatially-sparse convolutional neural networks.
- [20] Alex Graves, Marcus Liwicki, Santiago Fernández, Roman Bertolami, Horst Bunke, and Jürgen Schmidhuber. 2008. A novel connectionist system for unconstrained handwriting recognition. *IEEE transactions on pattern analysis and machine intelligence* 31, 5 (2008), 855–868.
- [21] Tuomas Haarnoja, Aurick Zhou, Kristian Hartikainen, George Tucker, Sehoon Ha, Jie Tan, Vikash Kumar, Henry Zhu, Abhishek Gupta, Pieter Abbeel, et al. 2018. Soft actor-critic algorithms and applications.
- [22] Robert Hall, Larry Wasserman, and Alessandro Rinaldo. 2013. Random Differential Privacy. *Journal of Privacy and Confidentiality* 4, 2 (Mar. 2013). <https://doi.org/10.29012/jpc.v4i2.621>
- [23] Kaiming He, X. Zhang, Shaoqing Ren, and Jian Sun. 2016. Deep Residual Learning for Image Recognition. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, Vol. 1. IEEE, Piscataway, NJ, USA, 770–778.
- [24] Sorami Hisamoto, Matt Post, and Kevin Duh. 2020. Membership Inference Attacks on Sequence-to-Sequence Models: Is My Data In Your Machine Translation System? *Transactions of the Association for Computational Linguistics* 8 (01 2020), 49–63. https://doi.org/10.1162/tacl_a_00299 arXiv:https://direct.mit.edu/tacl/article-pdf/doi/10.1162/tacl_a_00299/1923547/tacl_a_00299.pdf
- [25] Hongsheng Hu, Zoran Salcic, Gillian Dobbie, and Xuyun Zhang. 2021. Membership Inference Attacks on Machine Learning: A Survey.
- [26] Alex Krizhevsky, Geoffrey Hinton, et al. 2009. Learning multiple layers of features from tiny images.
- [27] Alex Krizhevsky, Ilya Sutskever, and Geoffrey E. Hinton. 2012. ImageNet classification with deep convolutional neural networks. *Commun. ACM* 60 (2012), 84–90.
- [28] Xiujun Li, Lihong Li, Jianfeng Gao, Xiaodong He, Jianshu Chen, Li Deng, and Ji He. 2015. Recurrent Reinforcement Learning: A Hybrid Approach. arXiv:1509.03044 [cs.LG]
- [29] Xiangang Li and Xihong Wu. 2015. Constructing long short-term memory based deep recurrent neural networks for large vocabulary speech recognition. In *2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, Piscataway, NJ, USA, 4520–4524.
- [30] Boyi Liu, Qi Cai, Zhuoran Yang, and Zhaoran Wang. 2019. Neural proximal/trust region policy optimization attains globally optimal policy.
- [31] Fangyu Liu, Shuaipeng Li, Liqiang Zhang, Chenghu Zhou, Rongtian Ye, Yuebin Wang, and Jiwen Lu. 2017. 3DCNN-DQN-RNN: A Deep Reinforcement Learning Framework for Semantic Parsing of Large-Scale 3D Point Clouds. In *Proceedings of the IEEE international conference on computer vision*. IEEE, Piscataway, NJ, USA.
- [32] Yunhui Long, Vincent Bindschaedler, Lei Wang, Diyu Bu, Xiaofeng Wang, Haixu Tang, Carl A Gunter, and Kai Chen. 2018. Understanding membership inferences on well-generalized learning models.
- [33] Zhigang Lu, Hassan Jameel Asghar, Mohamed Ali Kaafar, Darren Webb, and Peter Dickinson. 2022. A Differentially Private Framework for Deep Learning with Convexified Loss Functions.
- [34] Minh-Thang Luong, Hieu Pham, and Christopher D. Manning. 2015. Effective Approaches to Attention-based Neural Machine Translation. arXiv:1508.04025 [cs.CL]
- [35] Christopher David Lusen. 2001. *Finite memory policies for partially observable Markov decision processes*. University of Kentucky, Lexington, KY, USA.
- [36] Michael McCloskey and Neal J Cohen. 1989. Catastrophic interference in connectionist networks: The sequential learning problem. In *Psychology of learning and motivation*. Vol. 24. Elsevier, Amsterdam, Netherlands, 109–165.
- [37] H. Brendan McMahan, Daniel Ramage, Kunal Talwar, and Li Zhang. 2018. Learning Differentially Private Recurrent Language Models. <https://openreview.net/forum?id=Bj0hF1Zob>
- [38] John Miller and Moritz Hardt. 2019. Stable Recurrent Models. <https://openreview.net/forum?id=Hygxb2CqKm>
- [39] Fatemehsadat Mireshghallah, Mohammadkazem Taram, Praneeth Vepakomma, Abhishek Singh, Ramesh Raskar, and Hadi Esmaeilzadeh. 2020. Privacy in deep learning: A survey.
- [40] Milad Nasr, Reza Shokri, and Amir Houmansadr. 2019. Comprehensive privacy analysis of deep learning: Passive and active white-box inference attacks against centralized and federated learning. In *2019 IEEE symposium on security and privacy (SP)*. IEEE, Piscataway, NJ, USA, 739–753.
- [41] Xinlei Pan, Weiyao Wang, Xiaoshuai Zhang, Bo Li, Jinfeng Yi, and Dawn Song. 2019. How you act tells a lot: Privacy-leaking attack on deep reinforcement learning. In *Proceedings of the 18th International Conference on Autonomous Agents and MultiAgent Systems*. IEEE, Piscataway, NJ, USA, 368–376.
- [42] Kishore Papineni, Salim Roukos, Todd Ward, and Wei-Jing Zhu. 2002. Bleu: a Method for Automatic Evaluation of Machine Translation. In *Proceedings of the 40th Annual Meeting of the Association for Computational Linguistics*. Association for Computational Linguistics, Philadelphia, Pennsylvania, USA, 311–318. <https://doi.org/10.3115/1073083.1073135>
- [43] Adam Paszke, Sam Gross, Francisco Massa, Adam Lerer, James Bradbury, Gregory Chanan, Trevor Killeen, Zeming Lin, Natalia Gimelshein, Luca Antiga, Alban Desmaison, Andreas Köpf, Edward Yang, Zach DeVito, Martin Raison, Alykhan Tejani, Sasank Chilamkurthy, Benoit Steiner, Lu Fang, Junjie Bai, and Soumith Chintala. 2019. PyTorch: An Imperative Style, High-Performance Deep Learning Library. arXiv:1912.01703 [cs.LG]
- [44] Andreas Pfeuffer, Karina Schulz, and Klaus Dietmayer. 2019. Semantic Segmentation of Video Sequences with Convolutional LSTMs. *2019 IEEE Intelligent Vehicles Symposium (IV)* 1 (2019), 1441–1447.
- [45] Alec Radford, Karthik Narasimhan, Tim Salimans, and Ilya Sutskever. 2018. Improving language understanding by generative pre-training.
- [46] Md Atiqur Rahman, Tanzila Rahman, Robert Laganière, Noman Mohammed, and Yang Wang. 2018. Membership Inference Attack against Differentially Private Deep Learning Model. *Trans. Data Priv* 11, 1 (2018), 61–79.
- [47] Maria Rigaki and Sebastian Garcia. 2020. A survey of privacy attacks in machine learning.
- [48] Benjamin IP Rubinstein and Francesco Aldà. 2017. Pain-free random differential privacy with sensitivity sampling. In *International Conference on Machine Learning*. PMLR, MIT Press, Cambridge, MA, USA, 2950–2959.
- [49] Alexandre Sablayrolles, Matthijs Douze, Cordelia Schmid, Yann Ollivier, and Hervé Jégou. 2019. White-box vs Black-box: Bayes Optimal Strategies for Membership Inference. In *ICML*. MIT Press, Cambridge, MA, USA.
- [50] Hasim Sak, Andrew W Senior, and Françoise Beaufays. 2014. Long short-term memory recurrent neural network architectures for large scale acoustic modeling.
- [51] Ahmed Salem, Yang Zhang, Mathias Humbert, Pascal Berrang, Mario Fritz, and Michael Backes. 2018. ML-leaks: Model and data independent membership inference attacks and defenses on machine learning models.
- [52] Kevin Scaman, Ludovic Dos Santos, Merwan Barlier, and Igor Colin. 2020. A simple and efficient smoothing method for faster optimization and local exploration. *Advances in Neural Information Processing Systems* 33 (2020), 6503–6513.
- [53] John Schulman, Sergey Levine, Pieter Abbeel, Michael Jordan, and Philipp Moritz. 2015. Trust region policy optimization. In *International conference on machine learning*. PMLR, MIT Press, Cambridge, MA, USA, 1889–1897.
- [54] John Schulman, Filip Wolski, Prafulla Dhariwal, Alec Radford, and Oleg Klimov. 2017. Proximal Policy Optimization Algorithms. arXiv:1707.06347 [cs.LG]

- [55] Vatsal Sharan, Sham Kakade, Percy Liang, and Gregory Valiant. 2018. Prediction with a Short Memory. In *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing* (Los Angeles, CA, USA) (STOC 2018). Association for Computing Machinery, New York, NY, USA, 1074–1087. <https://doi.org/10.1145/3188745.3188954>
- [56] Reza Shokri, Marco Stronati, Congzheng Song, and Vitaly Shmatikov. 2017. Membership Inference Attacks Against Machine Learning Models. *2017 IEEE Symposium on Security and Privacy (SP)* 1 (May 2017). <https://doi.org/10.1109/sp.2017.41>
- [57] Congzheng Song and Vitaly Shmatikov. 2019. Auditing data provenance in text-generation models. In *Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*. ACM, New York, NY, USA, 196–206.
- [58] Stacey Truex, Ling Liu, Mehmet Emre Guroy, Lei Yu, and Wenqi Wei. 2019. Demystifying membership inference attacks in machine learning as a service. *IEEE Transactions on Services Computing* 14, 6 (2019), 2073–2089.
- [59] Ashish Vaswani, Noam Shazeer, Niki Parmar, Jakob Uszkoreit, Llion Jones, Aidan N Gomez, Łukasz Kaiser, and Illia Polosukhin. 2017. Attention is all you need. , 5998–6008 pages.
- [60] Francesco Visin, Kyle Kastner, Kyunghyun Cho, Matteo Matteucci, Aaron Courville, and Yoshua Bengio. 2015. ReNet: A Recurrent Neural Network Based Alternative to Convolutional Networks. arXiv:1505.00393 [cs.CV]
- [61] Lucas Willems. 2018. RL-Starter-Files. <https://github.com/lcswillems/rl-starter-files>.
- [62] Thomas Wolf, Lysandre Debut, Victor Sanh, Julien Chaumond, Clement Delangue, Anthony Moi, Pierric Cistac, Tim Rault, Remi Louf, Morgan Funtowicz, Joe Davison, Sam Shleifer, Patrick von Platen, Clara Ma, Yacine Jernite, Julien Plu, Canwen Xu, Teven Le Scao, Sylvain Gugger, Mariama Drame, Quentin Lhoest, and Alexander Rush. 2020. Transformers: State-of-the-Art Natural Language Processing. In *Proceedings of the 2020 Conference on Empirical Methods in Natural Language Processing: System Demonstrations*. Association for Computational Linguistics, Online, 38–45. <https://doi.org/10.18653/v1/2020.emnlp-demos.6>
- [63] Xi Wu, Fengang Li, Arun Kumar, Kamalika Chaudhuri, Somesh Jha, and Jeffrey Naughton. 2017. Bolt-on differential privacy for scalable stochastic gradient descent-based analytics. In *Proceedings of the 2017 ACM International Conference on Management of Data*. ACM, New York, NY, USA, 1307–1322.
- [64] Yonghui Wu, Mike Schuster, Zhifeng Chen, Quoc V Le, Mohammad Norouzi, Wolfgang Macherey, Maxim Krikun, Yuan Cao, Qin Gao, Klaus Macherey, et al. 2016. Google’s neural machine translation system: Bridging the gap between human and machine translation.
- [65] Yonghui Wu, Mike Schuster, Zhifeng Chen, Quoc V Le, Mohammad Norouzi, Wolfgang Macherey, Maxim Krikun, Yuan Cao, Qin Gao, Klaus Macherey, et al. 2016. Google’s neural machine translation system: Bridging the gap between human and machine translation.
- [66] Samuel Yeom, Irene Giacomelli, Matt Fredrikson, and Somesh Jha. 2018. Privacy Risk in Machine Learning: Analyzing the Connection to Overfitting. *2018 IEEE 31st Computer Security Foundations Symposium (CSF)* 1 (2018), 268–282.
- [67] Jun Zhang, Zhenjie Zhang, Xiaokui Xiao, Yin Yang, and Marianne Winslett. 2012. Functional mechanism: regression analysis under differential privacy.

A APPENDIX

A.1 Proof of Theorem 5.2

THEOREM A.1. *With \mathcal{H} a fixed set of hyperparameters, including a fixed initialization and a fixed seed for generating random numbers, let $\mathcal{A}_{\mathcal{H}}$ be an SGD algorithm modified with gradient clipping and loss-function smoothing; that is, at every iteration i ,*

$$\theta_{i+1} = \theta_i - \eta \frac{1}{|X_i|} \sum_{x \in X_i} \text{CL} \left(\mathbb{E}_{Z \sim \mathcal{N}(0, \sigma_s^2)} [g_x(\theta_i + Z)], C \right), \quad (14)$$

where σ_s^2 is the smoothing variance. Let the loss function ℓ be L -Lipschitz, m be the minibatch size, and $\beta = L/\sigma_s$. Then, after training for T iterations, it holds that

$$S(\mathcal{A}_{\mathcal{H}}) \leq 2 \frac{(1 + \eta\beta)^T - 1}{(m - 1)\beta} C. \quad (15)$$

PROOF. Let $\bar{\ell}(\theta_i, x) = \mathbb{E}_{Z \sim \mathcal{N}(0, \sigma_s^2)} [\ell(\theta_i + Z, x)]$. Such an operation is known as randomized smoothing which transforms the L -Lipschitz loss function ℓ into L/σ_s -smooth $\bar{\ell}$ [52]; that is,

$$\left\| \frac{\partial \bar{\ell}(\theta, x)}{\partial \theta} \Big|_{\theta=a} - \frac{\partial \bar{\ell}(\theta, x)}{\partial \theta} \Big|_{\theta=b} \right\| \leq \frac{L}{\sigma_s} \|a - b\|. \quad (16)$$

We also have that

$$\frac{\partial \bar{\ell}(\theta, x)}{\partial \theta} \Big|_{\theta=\theta_i} = \mathbb{E}_{Z \sim \mathcal{N}(0, \sigma_s^2)} [g_x(\theta_i + Z)]. \quad (17)$$

Considering SGD’s update rule with clipped gradients and randomized smoothing, we have that, for two adjacent datasets D and D' and their respective minibatches at stage 0, X_0 and X'_0 ,

$$\theta_1 = \theta_0 - \eta \frac{1}{|X_0|} \sum_{x \in X_0} \text{CL} \left(\frac{\partial \bar{\ell}(\theta, x)}{\partial \theta} \Big|_{\theta_0}, C \right) \quad (18)$$

and

$$\theta'_1 = \theta_0 - \eta \frac{1}{|X'_0|} \sum_{x' \in X'_0} \text{CL} \left(\frac{\partial \bar{\ell}(\theta, x')}{\partial \theta} \Big|_{\theta_0}, C \right). \quad (19)$$

The two minibatches can only differ in one data record and fixing the random seeds ensures that the same data indices will be chosen for both X_0 and X'_0 . As a result,

$$\begin{aligned} \|\theta_1 - \theta'_1\| &= \\ \eta \left\| \sum_{x \in X_0 \setminus X'_0} \text{CL} \left(\frac{\partial \bar{\ell}(\theta, x)}{\partial \theta} \Big|_{\theta_0}, C \right) - \sum_{x' \in X'_0 \setminus X_0} \text{CL} \left(\frac{\partial \bar{\ell}(\theta, x')}{\partial \theta} \Big|_{\theta_0}, C \right) \right\| & \\ \leq 2\eta \frac{C}{m}. & \quad (20) \end{aligned}$$

For the next SGD update, we write

$$\theta_2 = \theta_1 - \eta \frac{1}{|X_1|} \sum_{x \in X_1} \text{CL} \left(\frac{\partial \bar{\ell}(\theta, x)}{\partial \theta} \Big|_{\theta_1}, C \right) \quad (21)$$

and

$$\theta'_2 = \theta'_1 - \eta \frac{1}{|X'_1|} \sum_{x' \in X'_1} \text{CL} \left(\frac{\partial \bar{\ell}(\theta, x')}{\partial \theta} \Big|_{\theta'_1}, C \right). \quad (22)$$

Due to the smoothness of $\bar{\ell}$, we have that

$$\left\| \text{CL} \left(\frac{\partial \bar{\ell}(\theta, x)}{\partial \theta} \Big|_{\theta=a}, C \right) - \text{CL} \left(\frac{\partial \bar{\ell}(\theta, x)}{\partial \theta} \Big|_{\theta=b}, C \right) \right\| \leq \min \left(2C, \frac{L}{\sigma_s} \|a - b\| \right). \quad (23)$$

With $\beta = \frac{L}{\sigma_s}$, we can write

$$\|\theta_2 - \theta'_2\| \leq \|\theta_1 - \theta'_1\| + \eta \left(1 - \frac{1}{m} \right) \|\theta_1 - \theta'_1\| \beta + 2\eta \frac{C}{m}. \quad (24)$$

The reason that (24) holds is that X_1 and X'_1 are obtained from two adjacent datasets and because of the fixed-seed assumption, they hold equal entries except for one; for the equal entries, the second term on the right-hand side of (24) can be used and for the non-equal entry, the third term can be used as an upper bound. Analogously, for every stage $i \geq 2$, we have

$$\|\theta_i - \theta'_i\| \leq 2\eta \frac{C}{m} + \left[1 + \eta \left(1 - \frac{1}{m} \right) \beta \right] \|\theta_{i-1} - \theta'_{i-1}\|, \quad (25)$$

or

$$\|\theta_i - \theta'_i\| \leq 2 \frac{(1 + \eta\beta)^i - 1}{(m-1)\beta} C, \quad (26)$$

which concludes the proof. \square

A.2 Reproducibility Information

In this section, we state the hyperparameters that we used in the experiments.

MIA on the reinforcement learning agent: We use the PPO algorithm to train the agents, for which we use the default parameters set by the RL-Starter-Files toolbox unless stated below. The feed-forward agent uses an MLP with two hidden layers, each of which consists of 74 neurons. The RNN agent uses the MLP architecture that consists of two 32-neurons layers with 4 additional LSTM units. The first layer is activated by tanh functions and the last layer is activated by a softmax function. We train the agents for a total of 204,800 iterations on seeds 1 to 16 for both agents. We use the default clipping epsilon 0.2 while training.

For the implementation of the MIA, we use an MLP with 5 ReLU-activated hidden layers and 1 LSTM unit. We use 6400 in trajectories and 6400 out trajectories to generate the binary classifier's training dataset. We train the binary classifier using the Adam optimizer and the cross-entropy loss function for 15 epochs, each of which consists of 100 gradient updates. We use the Keras library [9] to train the binary classifier with a learning rate of 0.001 and default parameters unless stated above.

MIA on the machine translation model: We use an LSTM encoder-decoder network with dot product attention mechanism [34] to construct the sequence-to-sequence model. We use the Multi30K dataset [15] which consists of 30,000 sentence pairs for training and 1,000 pairs for testing. We use 5,000 sentence pairs to train the shadow model and a negative likelihood loss to update gradients. The shadow model is trained for 20 epochs, with a word-embedding dimension of 150, a hidden dimension of 200, a learning rate of 0.001, and a dropout rate of 0.2. We use PyTorch [43] to implement and train the victim model with default parameters unless specified above. Once the shadow model is fine-tuned, we use 2,000

output sequences to populate the training dataset of the MIA's binary classifier. In the training procedure, we set the max norm of the gradients to 10 and clip the gradients with norms above the threshold.

We use a transformer as the FFNN structure. The transformer architecture is identical to the model from 'attention is all your need', trained with default parameters.

The binary classifier consists of 1 LSTM unit, two linear layers, a ReLU-activated layer, and a softmax layer. We implement the MIA classifier using PyTorch and train it using the cross-entropy loss function for 20 epochs with the default parameters.

MIA on the image classification model: We use ResNet101 [23] implemented in the Keras library [9] as the FFNN model for image classification. ResNet101 consists of 101 convolutional layers followed by one max-pooling layer, one fully connected linear layer, and an output layer with softmax activation.

We use ReNet [60] implemented by PyTorch [43] under default parameters as the RNN model for image classification. ReNet consists of 4 bi-directional LSTMs, 2 fully connected layers with ReLU activation, and an output layer with softmax activation. We train both models using the categorical cross-entropy loss function as their learning objective function and use the Adam optimizer. The learning rates used are 0.001 and 0.01 for ResNet101 and ReNet, respectively.

We use the image classification dataset Cifar10 which consists of 50,000 training records and 10,000 testing records. We train the target model and shadow model using 10,000 training records and a categorical cross-entropy loss is used to update the gradient. We clip the gradients whose norm is greater than 10.

For the implementation of the MIA, we use an MLP with 5 ReLU-activated hidden layers. We train the classifier using 20,000 probability pairs with half labeled 'in'. We use the Keras library [9] to train the binary classifier with a learning rate of 0.001 and default parameters unless stated above.

A.3 Privacy Level vs. Noise Variance

Figure 9 shows the private budget ϵ at each noise level σ . Together with Figure 8, we observe that the proposed GPM can achieve a high privacy level ($\epsilon < 5$) with a utility loss less than 10%. DP-SGD can also achieve a reasonable privacy level ($\epsilon < 10$) with a utility loss lower than 15%.

To obtain the results, we run the DP experiments following the specifications stated in Table 2.

Table 2: Experiment Specifications.

Task	train size $ D $	\bar{S}_{RNN}	\bar{S}_{FFNN}	δ	clip norm	batch	epoch
IC	10000	0.013209	0.013518	1e-4	10	128	50
RL	6400(32)	0.093682	0.093429	1e-4	10	128	100
NMT	5000	0.11678	0.11845	1e-4	10	128	50

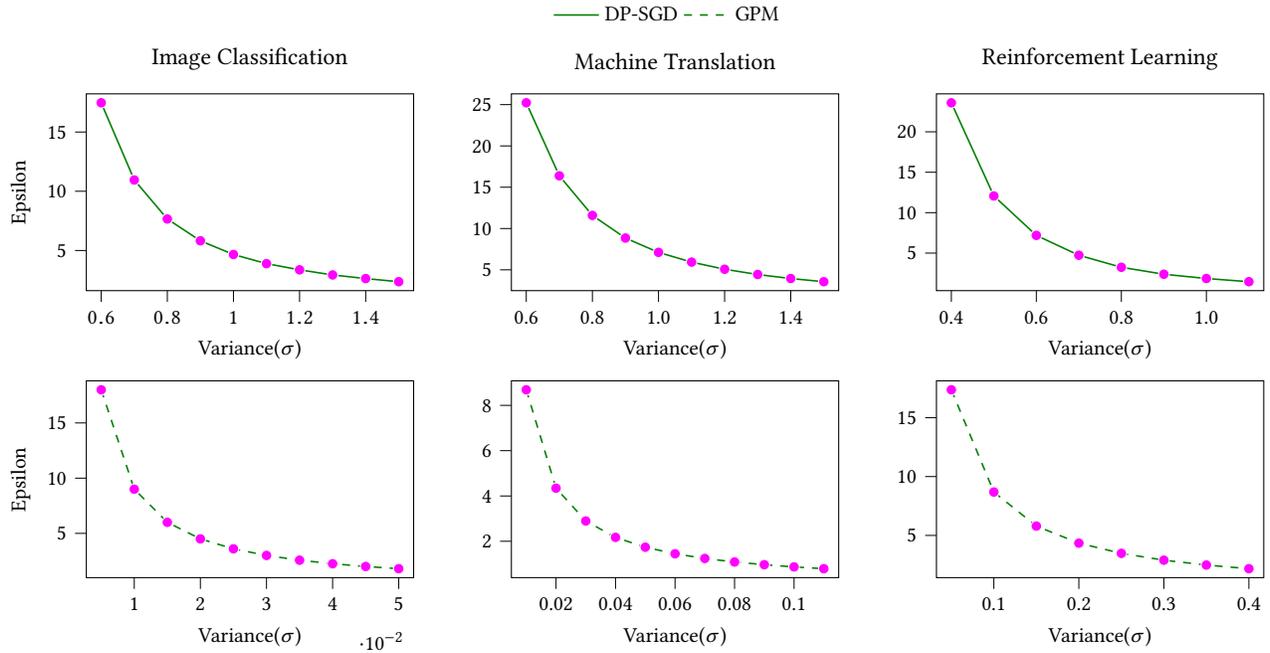


Figure 9: privacy budget ϵ at each Gaussian noise level. The first row shows the privacy level of DP-SGD and the second row shows the privacy level of proposed GPM.