



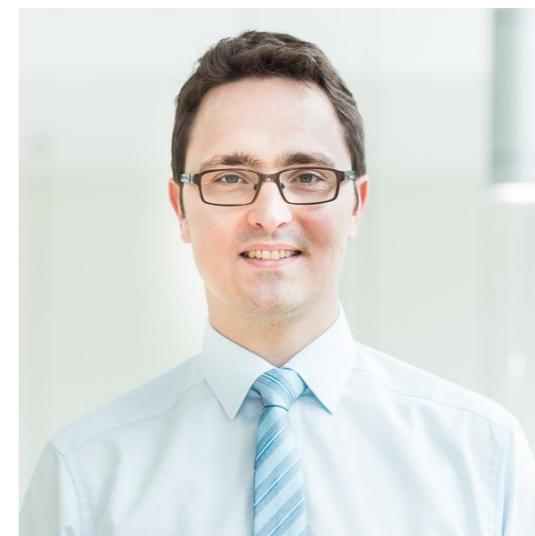
Private Set Generation with Discriminative Information



Dingfan Chen



Raouf Kerkouche

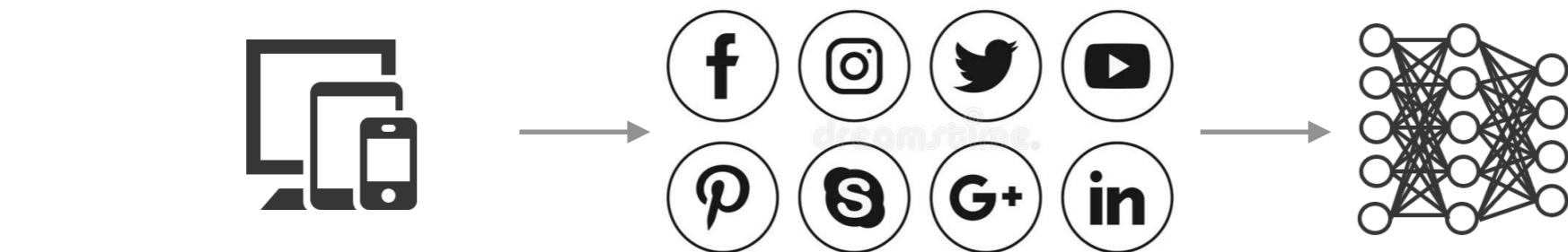


Mario Fritz

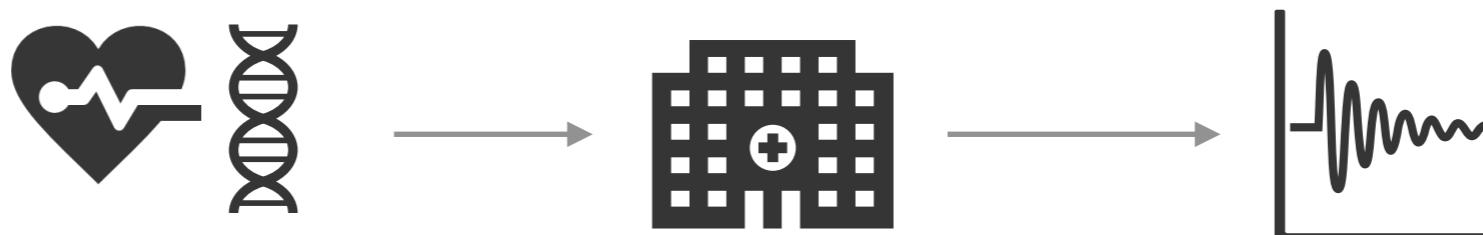
Data Privacy in ML:



- Sensitive data is **ubiquitous**



Mobile devices & Internet



Medical record



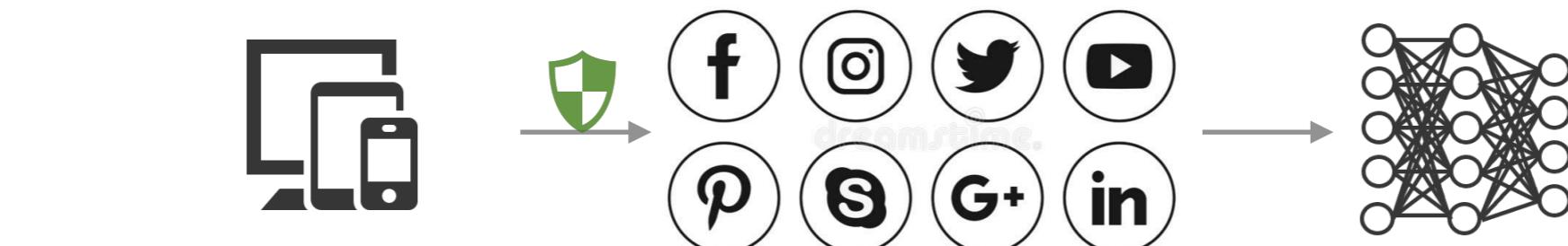
Demographic data

Data Privacy in ML:

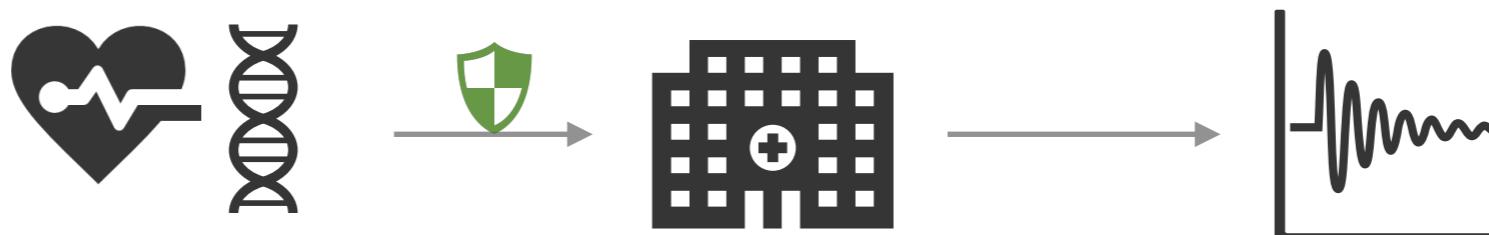


- Sensitive data is **ubiquitous**

Our task:
Data sanitization



Mobile devices & Internet



Medical record



Demographic data

Problem



- **Privacy-preserving data generation**
 - High-dimensional data → Deep Neural Network (NN)
 - Rigorous privacy guarantee → Differential Privacy (DP)
- **Existing approaches**

Problem



- Privacy-preserving data generation
 - High-dimensional data → Deep Neural Network (NN)
 - Rigorous privacy guarantee → Differential Privacy (DP)

• Existing approaches

The figure displays a grid of 10 academic papers, each representing a different approach to privacy-preserving data generation. The papers are arranged in two columns of five. Each paper includes its title, authors, abstract, and a small image of the document cover.

- PATE-GAN: Generating Synthetic Data with Differential Privacy Guarantees** (arXiv:2001.09700v1 [cs.LG] 27 Jan 2020) by James Jordan*, Mihai Mititelu, and Alain Rakotomamonjy. Published in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR) 2020.
- DP-CGAN : Differentially Private GANs** (arXiv:2006.08265v2 [cs.LG] 15 Mar 2021) by Reihaneh T. Takahashi, Michihiko Ueno, and Seng Pei Liew. Published in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR) 2021.
- GS-WGAN: A Gradient-Sanitized Approach for Learning Differentially Private Generators** (arXiv:2006.08265v2 [cs.LG] 15 Mar 2021) by Dingfan Chen¹, Alain Rakotomamonjy², and Frederik Harder³. Published in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR) 2021.
- DP-MERF: Differentially Private Mean Embeddings with Random Feature Aggregation** (arXiv:2007.09745 [cs.LG] 1 Nov 2021) by Yunhai Long^{1*}, Boxin Wang^{2*}, Kamil M. Etemadi³, Carl A. Gunzelmann⁴, and Alain Rakotomamonjy⁵. Published in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR) 2021.
- G-PATE: Scalable Differentially Private Aggregation via Generative Adversarial Training** (arXiv:submit/4007495 [cs.LG] 1 Nov 2021) by Alain Rakotomamonjy, Tianqi Chen¹, and Frederik Harder². Published in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR) 2022.
- Differentially Private Sliced Wasserstein Distance** (arXiv:submit/4007495 [cs.LG] 1 Nov 2021) by Tianqi Cao^{1,2}, Alex Beutel³, and Alain Rakotomamonjy⁴. Published in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR) 2022.
- Don't Train Me! Generating Differentially Private Synthetic Data via Sinkhorn Divergence Minimization** (arXiv:2106.04590v2 [cs.LG] 8 Mar 2022) by Boxin Wang¹, Mingjun Kim², and Jaewoo Lee³. Published in Proceedings of the AAAI Digital Library 2022.
- DataLens: Scalable Privacy Preserving Training via Gradient Compression and Aggregation** (arXiv:2106.04590v2 [cs.LG] 8 Mar 2022) by Lukas Ritschard¹, Lukas Ritschard¹, and Sven Schmid². Published in Proceedings of the AAAI Digital Library 2022.
- Differentially Private Normalizing Flows for Synthetic Data Generation** (arXiv:2106.04590v2 [cs.LG] 8 Mar 2022) by Jaewoo Lee¹, Mingjun Kim², and Seng Pei Liew³. Published in Proceedings of the AAAI Digital Library 2022.
- PEARL: DATA SYNTHESIS VIA PRIVATE EMBEDDINGS AND ADVERSARIAL RECONSTRUCTION LEARNING** (arXiv:2106.04590v2 [cs.LG] 8 Mar 2022) by Seng Pei Liew¹, Tsubasa Takahashi¹, Michihiko Ueno¹, and Takuishi Iwase². Published in Proceedings of the AAAI Digital Library 2022.

¹ Jordon, James, et al., "PATE-GAN: Generating synthetic data with differential privacy guarantees.", *ICLR*, 2018.

² Torkzadehmahani, Reihaneh et al., "Dp-cgan: Differentially private synthetic data and label generation.", *CVPR Workshops*, 2019.

³ Chen, Dingfan, et al., "Gs-wgan: A gradient-sanitized approach for learning differentially private generators.", *NeurIPS*, 2020.

⁴ Harder, Frederik, et al., "Dp-merf: Differentially private mean embeddings with randomfeatures for practical privacy-preserving data generation.", *AISTAT*, 2021.

⁵ Rakotomamonjy, Alain, et al., "Differentially private sliced wasserstein distance.", *ICML*, 2021.

⁶ Long, Yunhui, et al., "G-PATE: Scalable Differentially Private Data Generator via Private Aggregation of Teacher Discriminators.", *NeurIPS*, 2021.

⁷ Cao, Tianshi, et al., "Don't Generate Me: Training Differentially Private Generative Models with Sinkhorn Divergence.", *NeurIPS*, 2021.

⁸ Wang, Boxin et al., "DataLens: Scalable privacy preserving training via gradient compression and aggregation.", *CCS*, 2021.

⁹ Lee, Jaewoo, et al., "Differentially Private Normalizing Flows for Synthetic Tabular Data Generation.", *AAAI*, 2022.

¹⁰ Liew, Seng Pei, et al., "PEARL: Data Synthesis via Private Embeddings and Adversarial Reconstruction Learning.", *ICLR*, 2022.

Problem



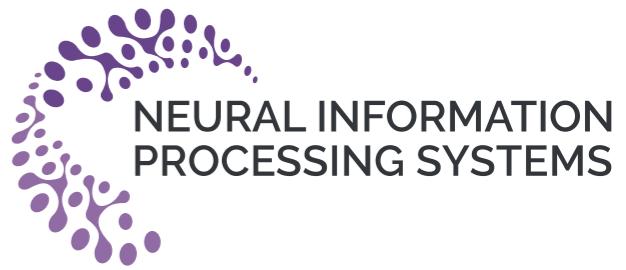
- **Privacy-preserving data generation**
 - High-dimensional data → Deep Neural Network (NN)
 - Rigorous privacy guarantee → Differential Privacy (DP)
- **Existing approaches**
 - Aim at fitting the complete data distribution
- **Our approach**

Problem



- **Privacy-preserving data generation**
 - High-dimensional data → Deep Neural Network (NN)
 - Rigorous privacy guarantee → Differential Privacy (DP)
- **Existing approaches**
 - Aim at fitting the complete data distribution
- **Our approach**
 - Target at common downstream tasks (e.g., classification)Generally easier

Problem



- **Privacy-preserving data generation**
 - High-dimensional data → Deep Neural Network (NN)
 - Rigorous privacy guarantee → Differential Privacy (DP)
- **Existing approaches**
 - Aim at fitting the complete data distribution
 - Optimize deep generative models
- **Our approach**
 - Target at common downstream tasks (e.g., classification)**Generally easier**

Problem



- **Privacy-preserving data generation**
 - High-dimensional data → Deep Neural Network (NN)
 - Rigorous privacy guarantee → Differential Privacy (DP)
- **Existing approaches**
 - Aim at fitting the complete data distribution
 - Optimize deep generative models
- **Our approach**
 - Target at common downstream tasks (e.g., classification)
 - Directly optimize a set of representative samples

Generally easier

Better convergence

Problem



- **Privacy-preserving data generation**
 - High-dimensional data → Deep Neural Network (NN)
 - Rigorous privacy guarantee → Differential Privacy (DP)
- **Existing approaches**
 - Aim at fitting the complete data distribution
 - Optimize deep generative models
 - Suboptimal utility: <85% for MNIST with $(\varepsilon, \delta)=(10, 10^{-5})$
- **Our approach**
 - Target at common downstream tasks (e.g., classification)
 - Directly optimize a set of representative samples

Generally easier

Better convergence

Problem



- **Privacy-preserving data generation**
 - High-dimensional data → Deep Neural Network (NN)
 - Rigorous privacy guarantee → Differential Privacy (DP)
- **Existing approaches**
 - Aim at fitting the complete data distribution
 - Optimize deep generative models
 - Suboptimal utility: <85% for MNIST with $(\varepsilon, \delta)=(10, 10^{-5})$
- **Our approach**
 - Target at common downstream tasks (e.g., classification)
 - Directly optimize a set of representative samples
 - ~10% downstream test accuracy improvement over SOTA

Generally easier

Better convergence

Useful samples

Approach

- **Target:**
 - Optimize for training downstream Neural Network classifier
- **Basic idea:**
 - Gradient-based **coreset generation**^{1,2}
 - DP stochastic gradient descent (DP-SGD)

¹ Zhao, Bo, et al., “Dataset condensation with gradient matching.”, *ICLR*, 2021.

² Zhao, Bo, et al., “Dataset condensation with differentiable siamese augmentation.”, *ICML*, 2021

Approach



- **Target:**
 - Optimize for training downstream Neural Network classifier
- **Basic idea:**
 - Gradient-based **coreset generation**^{1,2}
 - DP stochastic gradient descent (DP-SGD)

fake \mathcal{S}

real $x, y \sim P_{\mathcal{D}}$



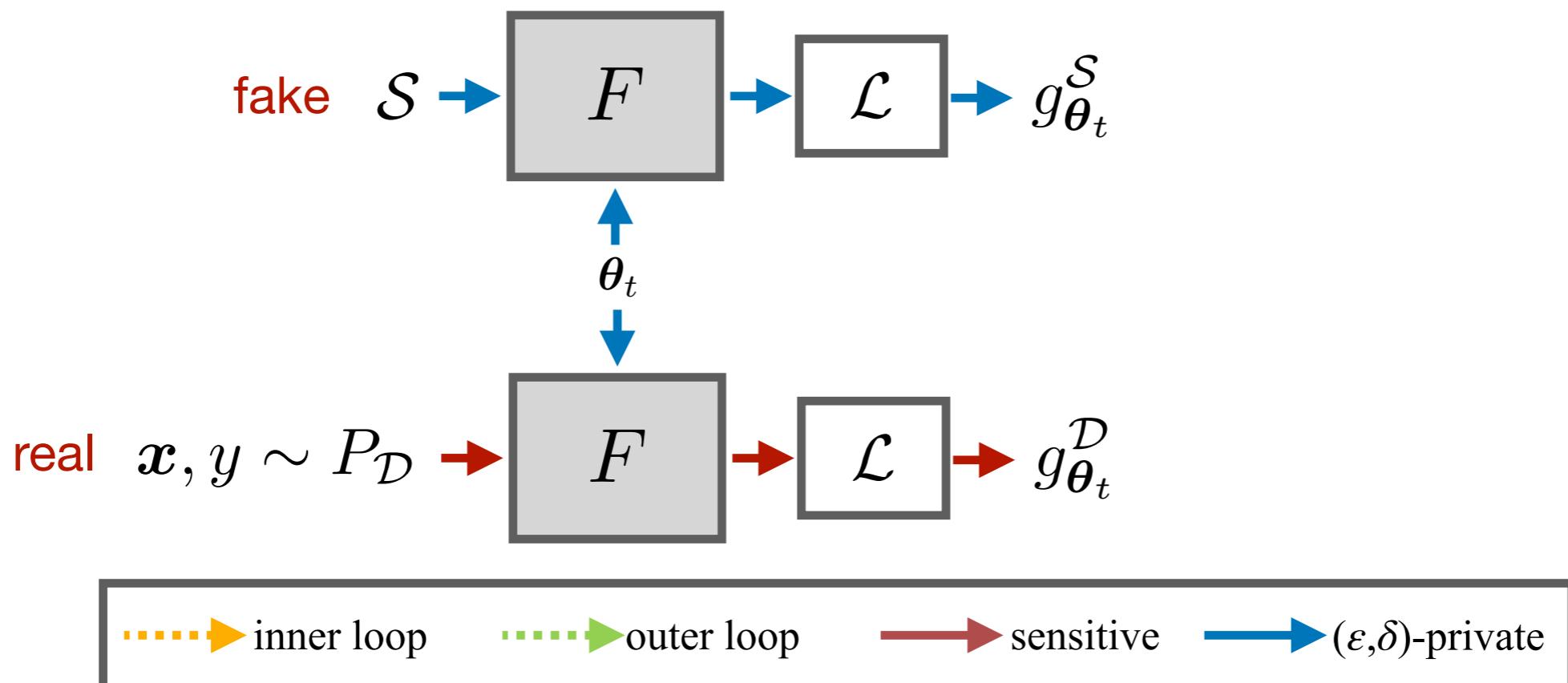
¹ Zhao, Bo, et al., “Dataset condensation with gradient matching.”, *ICLR*, 2021.

² Zhao, Bo, et al., “Dataset condensation with differentiable siamese augmentation.”, *ICML*, 2021

Approach



- **Target:**
 - Optimize for training downstream Neural Network classifier
- **Basic idea:**
 - Gradient-based **coreset generation**^{1,2}
 - DP stochastic gradient descent (DP-SGD)



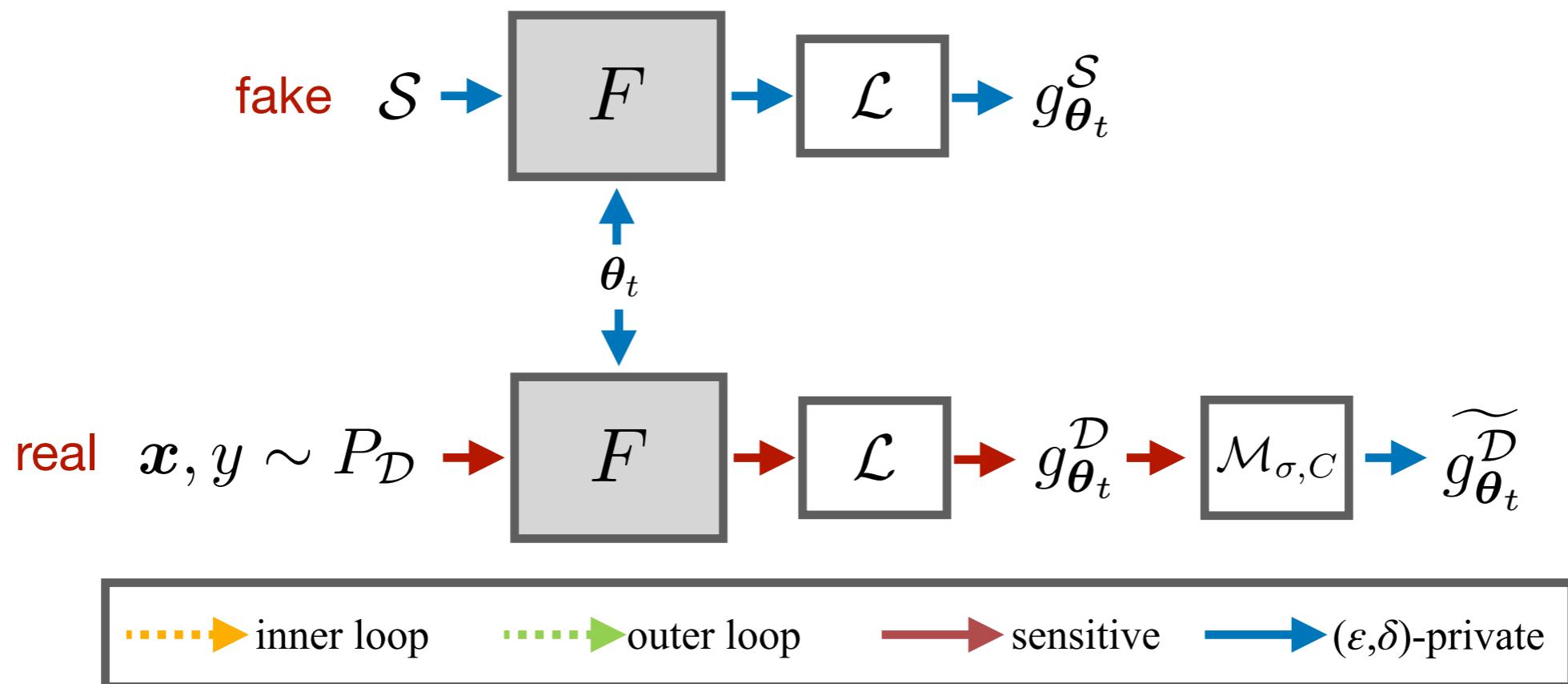
¹ Zhao, Bo, et al., "Dataset condensation with gradient matching.", *ICLR*, 2021.

² Zhao, Bo, et al., "Dataset condensation with differentiable siamese augmentation.", *ICML*, 2021

Approach



- **Target:**
 - Optimize for training downstream Neural Network classifier
- **Basic idea:**
 - Gradient-based **coreset generation**^{1,2}
 - DP stochastic gradient descent (DP-SGD)



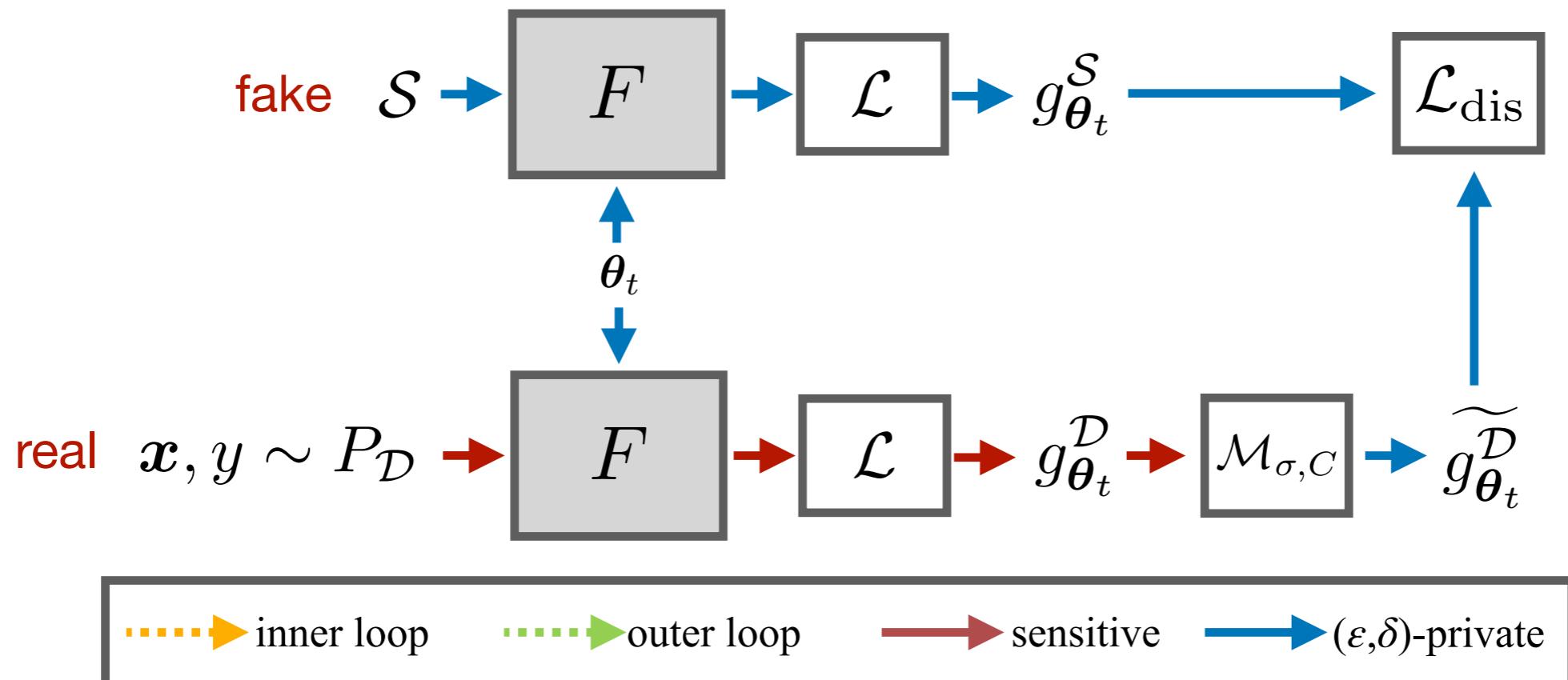
¹ Zhao, Bo, et al., “Dataset condensation with gradient matching.”, *ICLR*, 2021.

² Zhao, Bo, et al., “Dataset condensation with differentiable siamese augmentation.”, *ICML*, 2021

Approach



- **Target:**
 - Optimize for training downstream Neural Network classifier
- **Basic idea:**
 - Gradient-based **coreset generation**^{1,2}
 - DP stochastic gradient descent (DP-SGD)



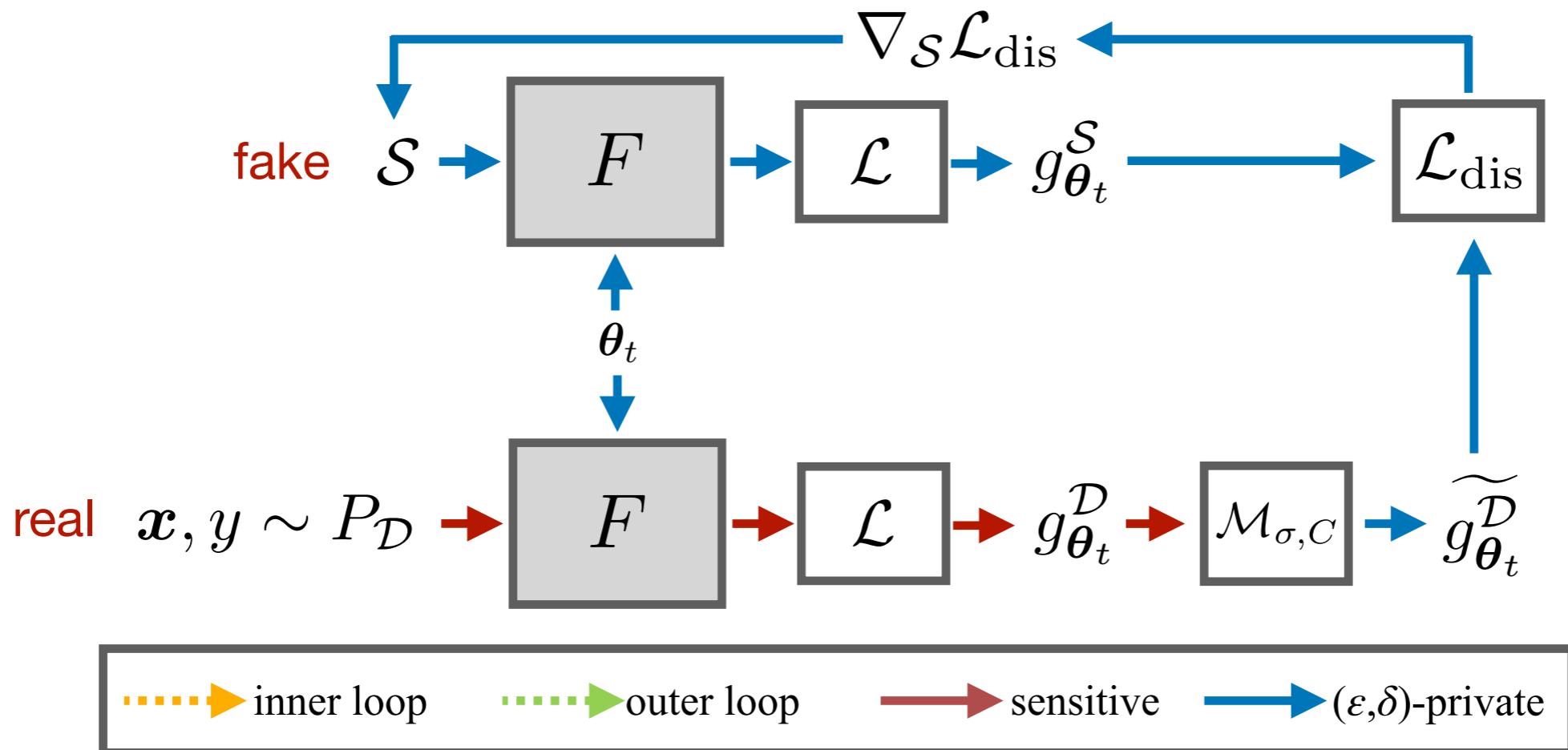
¹ Zhao, Bo, et al., “Dataset condensation with gradient matching.”, *ICLR*, 2021.

² Zhao, Bo, et al., “Dataset condensation with differentiable siamese augmentation.”, *ICML*, 2021

Approach



- **Target:**
 - Optimize for training downstream Neural Network classifier
- **Basic idea:**
 - Gradient-based **coreset generation**^{1,2}
 - DP stochastic gradient descent (DP-SGD)



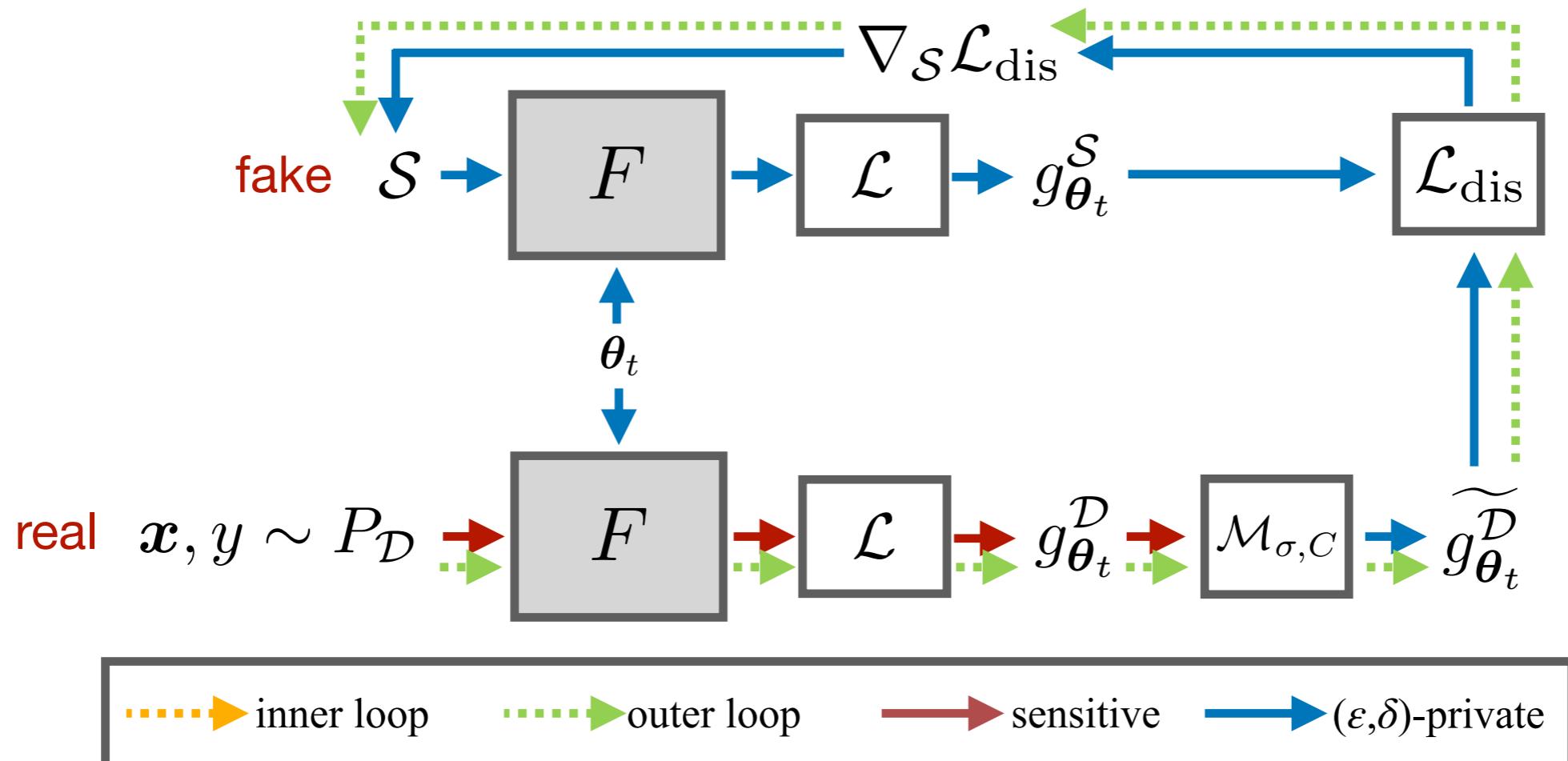
¹ Zhao, Bo, et al., "Dataset condensation with gradient matching.", *ICLR*, 2021.

² Zhao, Bo, et al., "Dataset condensation with differentiable siamese augmentation.", *ICML*, 2021

Approach



- **Target:**
 - Optimize for training downstream Neural Network classifier
- **Basic idea:**
 - Gradient-based **coreset generation**^{1,2}
 - DP stochastic gradient descent (DP-SGD)

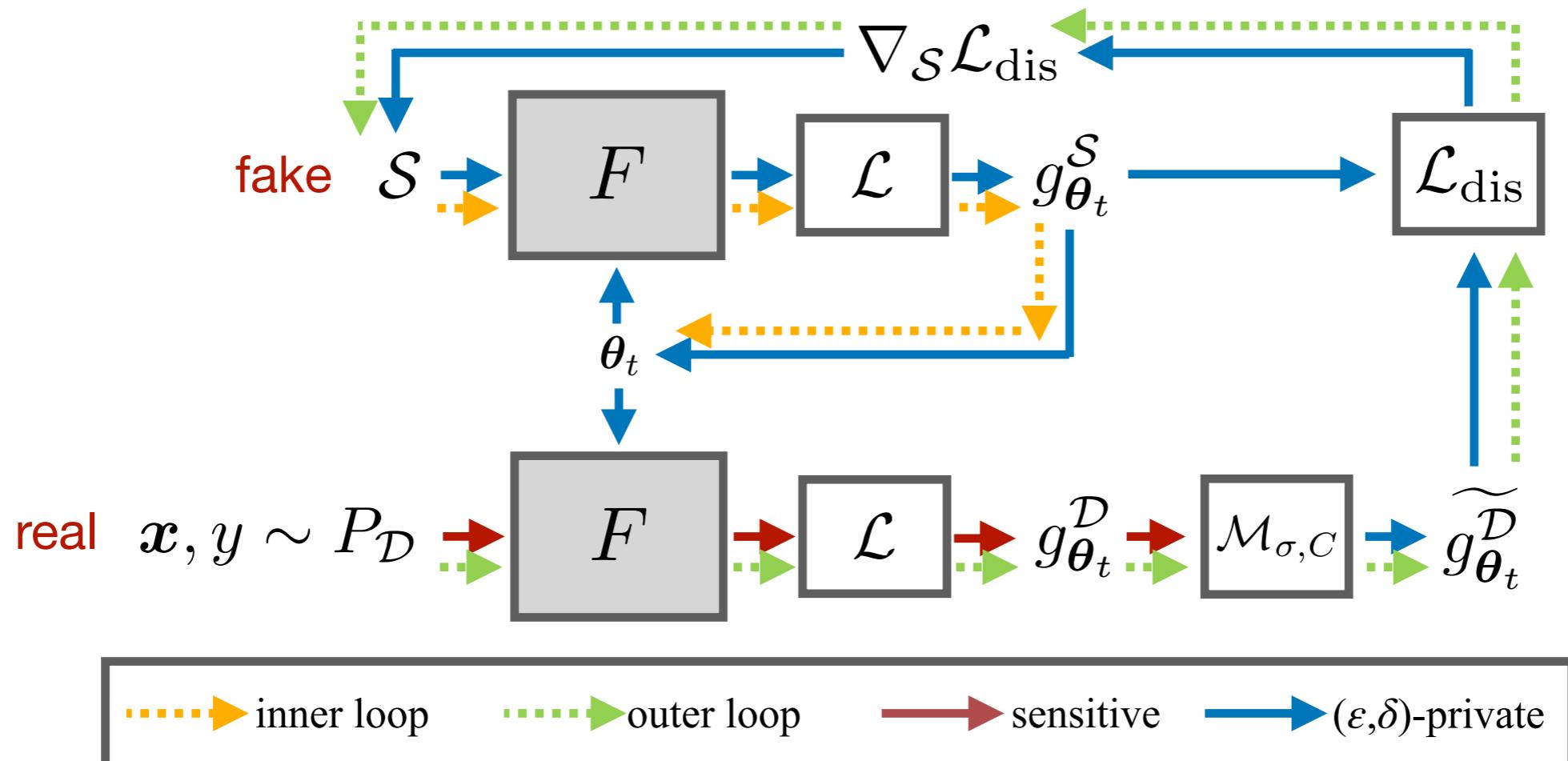


¹ Zhao, Bo, et al., “Dataset condensation with gradient matching.”, *ICLR*, 2021.

² Zhao, Bo, et al., “Dataset condensation with differentiable siamese augmentation.”, *ICML*, 2021

Approach

- **Target:**
 - Optimize for training downstream Neural Network classifier
- **Basic idea:**
 - Gradient-based **coreset generation**^{1,2}
 - DP stochastic gradient descent (DP-SGD)



¹ Zhao, Bo, et al., “Dataset condensation with gradient matching.”, *ICLR*, 2021.

² Zhao, Bo, et al., “Dataset condensation with differentiable siamese augmentation.”, *ICML*, 2021

Evaluation



- **Comparison to SOTA**
 - Utility for downstream classification task (train on fake; test on real)

Evaluation



- **Comparison to SOTA**
 - Utility for downstream classification task (train on synthetic; test on real)

	MNIST		FashionMNIST	
	$\varepsilon=1$	$\varepsilon=10$	$\varepsilon=1$	$\varepsilon=10$
DP-CGAN	-	52.5	-	50.2
G-PATE	58.8	80.9	58.1	69.3
DataLens	71.2	80.7	64.8	70.6
GS-WGAN	-	84.9	-	63.1
DP-Merf	72.7	85.7	61.2	72.4
DP-Sinkhorn	-	83.2	-	71.1
Ours (spc=20)	80.9	95.6	70.2	77.7

Evaluation



- **Comparison to SOTA**
 - Utility for downstream classification task (train on synthetic; test on real)

	MNIST		FashionMNIST	
	$\varepsilon=1$	$\varepsilon=10$	$\varepsilon=1$	$\varepsilon=10$
DP-CGAN	-	52.5	-	50.2
G-PATE	58.8	80.9	58.1	69.3
DataLens	71.2	80.7	64.8	70.6
GS-WGAN	-	84.9	-	63.1
DP-Merf	72.7	85.7	61.2	72.4
DP-Sinkhorn	-	83.2	-	71.1
Ours (spc=20)	80.9	95.6	70.2	77.7

Evaluation



- **Comparison to SOTA**
 - Generalization across model architecture

	MNIST						FashionMNIST					
	ConvNet	LeNet	AlexNet	VGG11	ResNet18	MLP	ConvNet	LeNet	AlexNet	VGG11	ResNet18	MLP
Real	99.6	99.2	99.5	99.6	99.7	98.3	93.5	88.9	91.5	93.8	94.5	86.9
DP-CGAN	50.2	52.6	52.1	54.7	51.8	54.3	50.2	52.6	52.1	54.7	51.8	54.3
GS-WGAN	84.9	83.2	80.5	87.9	89.3	74.7	54.7	62.7	55.1	57.3	58.9	65.4
DP-Merf	85.7	87.2	84.4	81.7	81.3	85.0	72.4	67.9	64.9	70.1	66.7	73.1
Ours (spc=10)	94.9	91.3	90.3	93.6	94.3	86.1	75.6	68.0	66.2	74.7	72.1	62.8
Ours (spc=20)	95.6	93.0	92.3	94.5	94.1	87.1	77.7	68.0	59.1	76.8	70.8	62.2

Evaluation

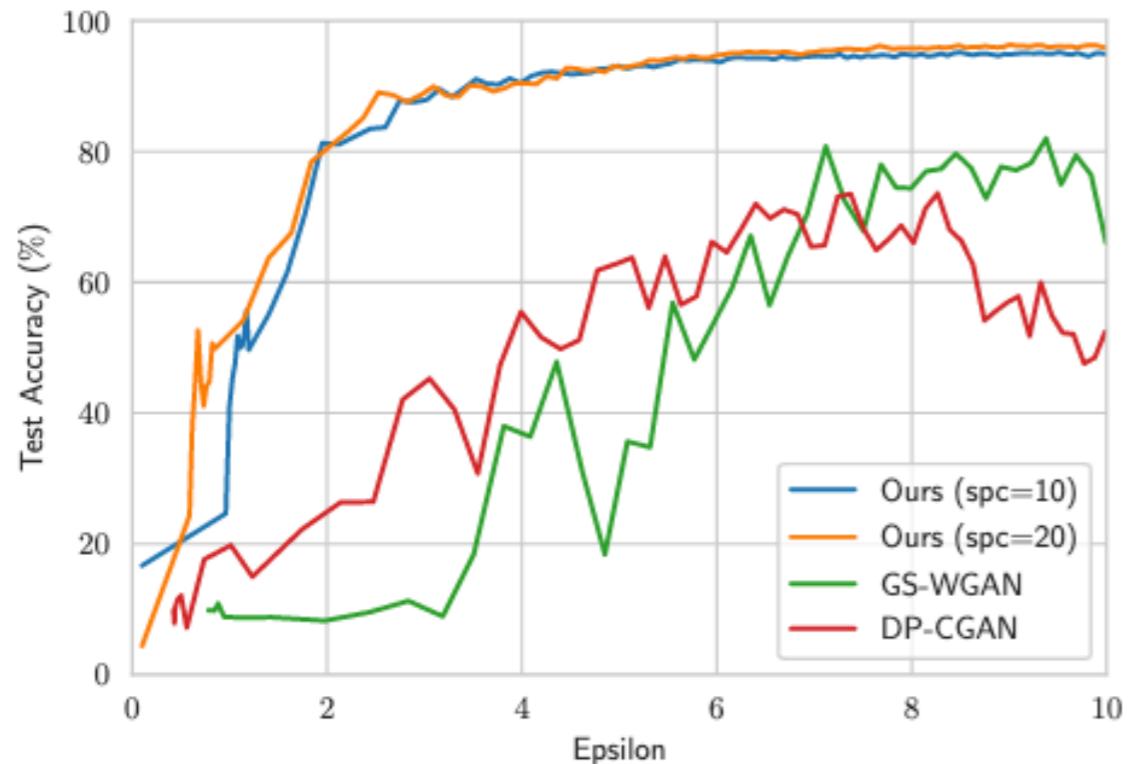


- **Comparison to SOTA**
 - Generalization across model architecture

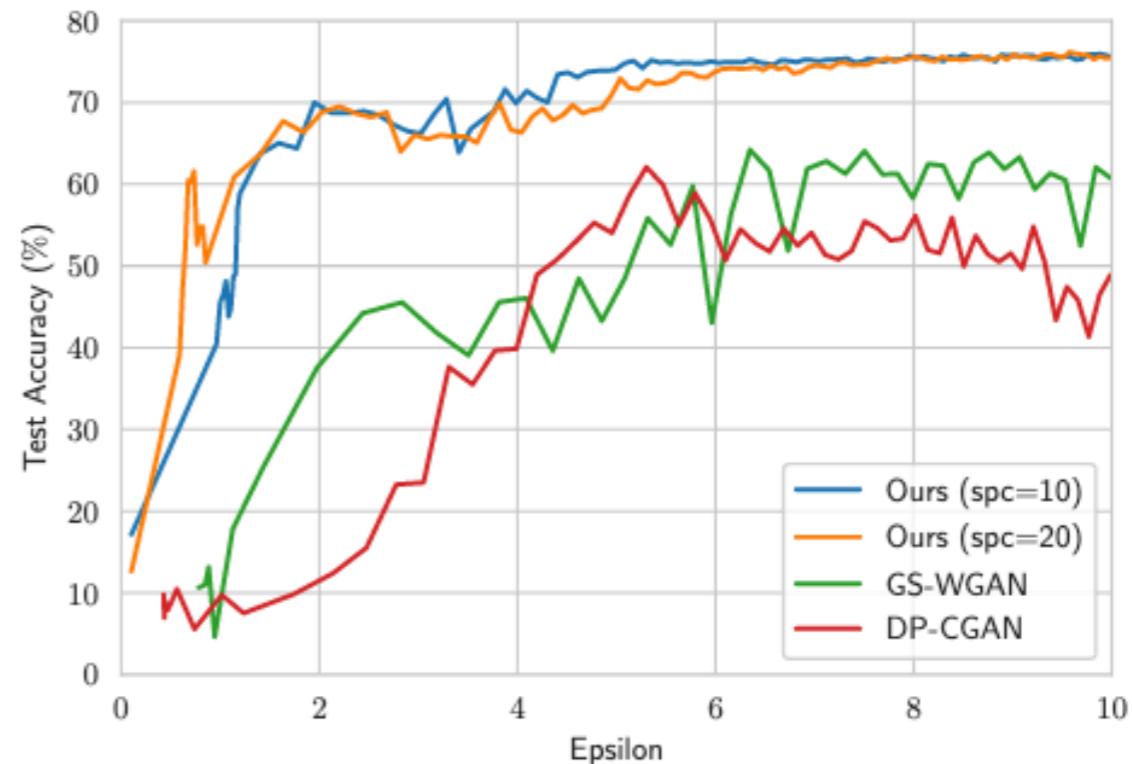
	MNIST						FashionMNIST					
	ConvNet	LeNet	AlexNet	VGG11	ResNet18	MLP	ConvNet	LeNet	AlexNet	VGG11	ResNet18	MLP
Real	99.6	99.2	99.5	99.6	99.7	98.3	93.5	88.9	91.5	93.8	94.5	86.9
DP-CGAN	50.2	52.6	52.1	54.7	51.8	54.3	50.2	52.6	52.1	54.7	51.8	54.3
GS-WGAN	84.9	83.2	80.5	87.9	89.3	74.7	54.7	62.7	55.1	57.3	58.9	65.4
DP-Merf	85.7	87.2	84.4	81.7	81.3	85.0	72.4	67.9	64.9	70.1	66.7	73.1
Ours (spc=10)	94.9	91.3	90.3	93.6	94.3	86.1	75.6	68.0	66.2	74.7	72.1	62.8
Ours (spc=20)	95.6	93.0	92.3	94.5	94.1	87.1	77.7	68.0	59.1	76.8	70.8	62.2

Evaluation

- Comparison to SOTA
 - Convergence rate



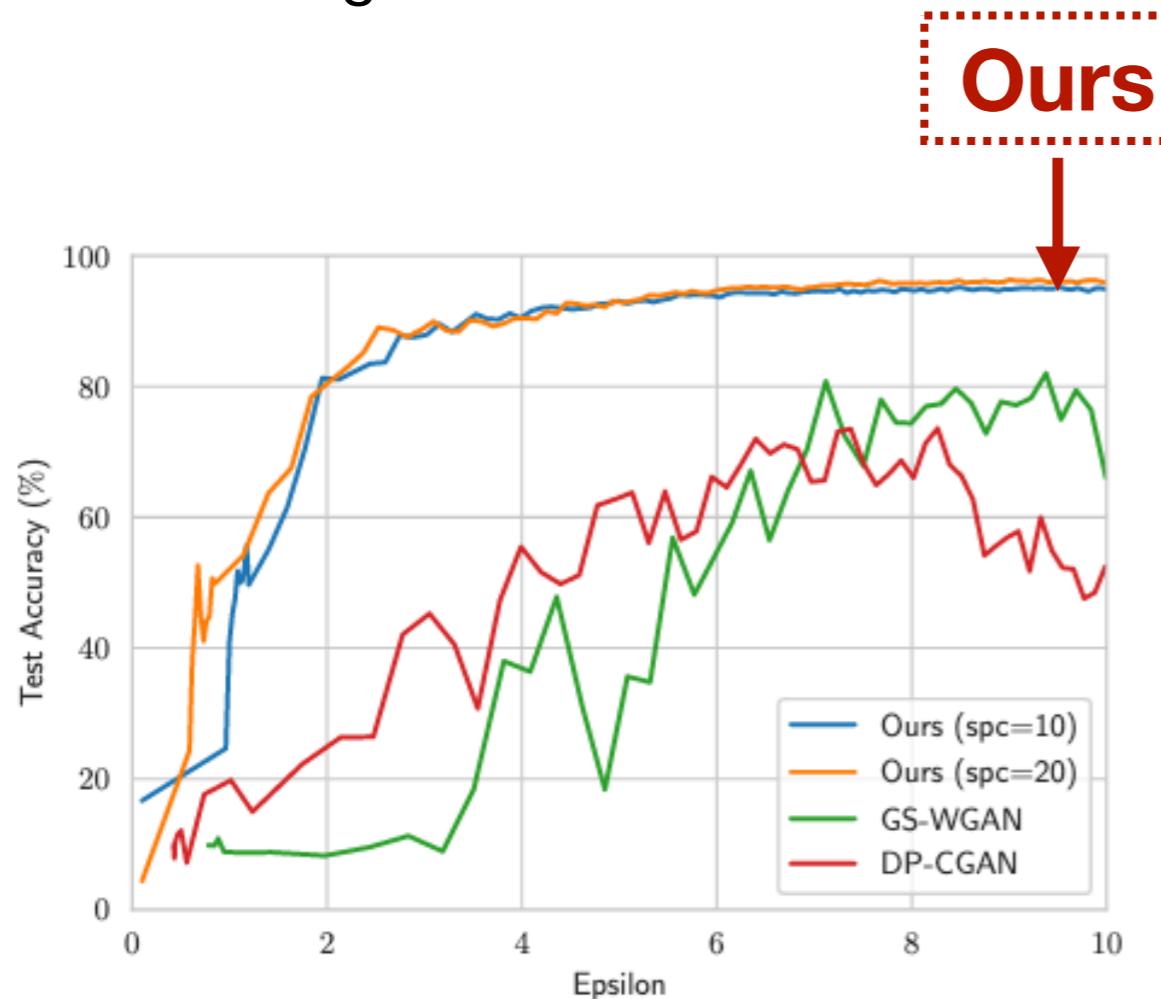
(a) MNIST



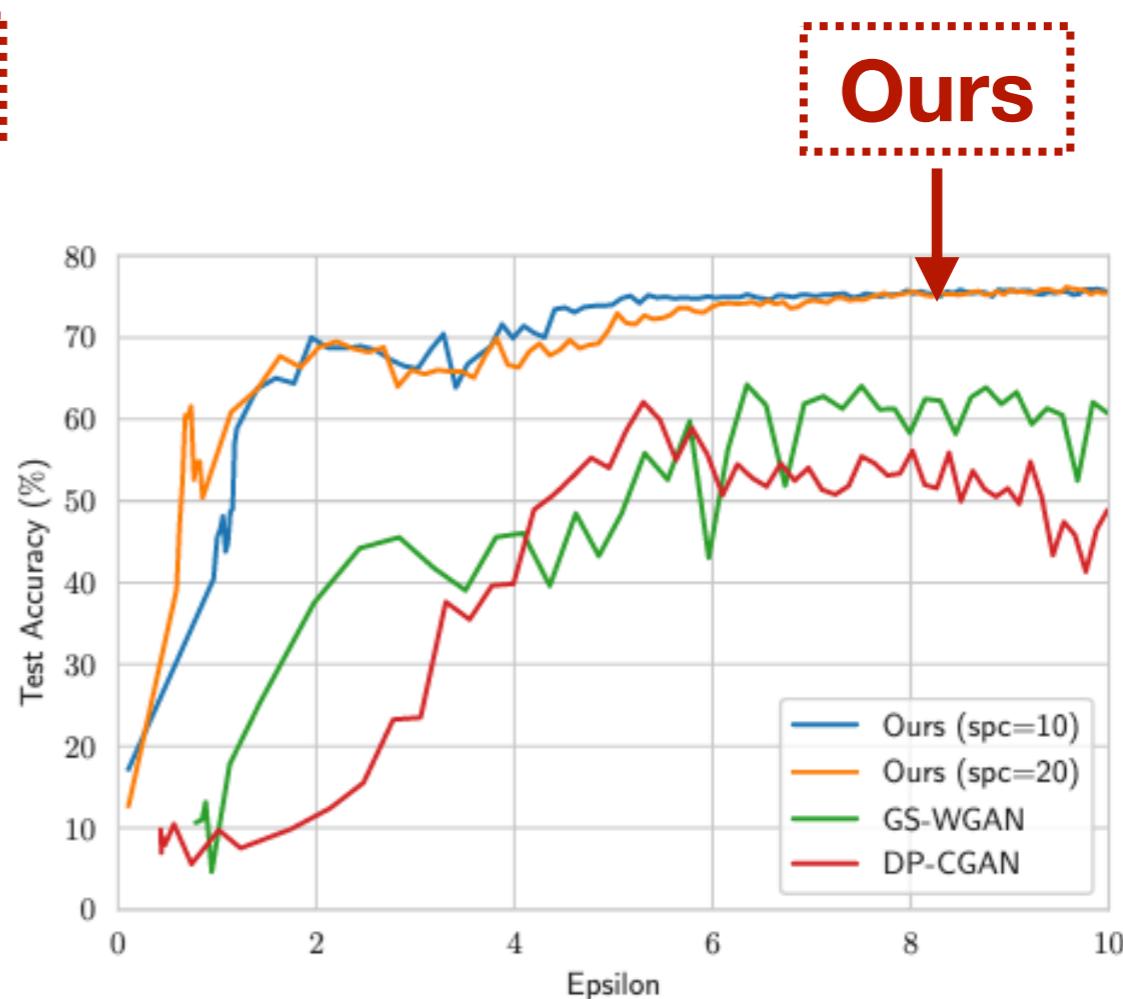
(b) FashionMNIST

Evaluation

- Comparison to SOTA
 - Convergence rate



(a) MNIST

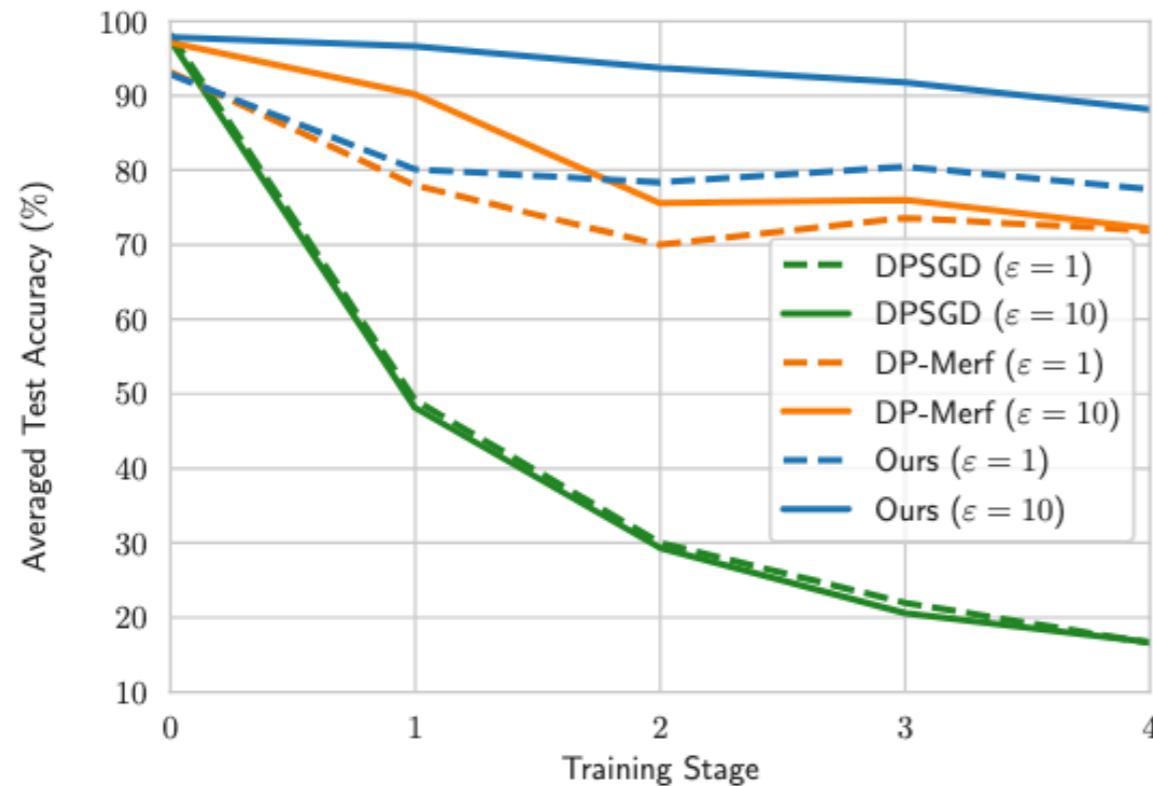


(b) FashionMNIST

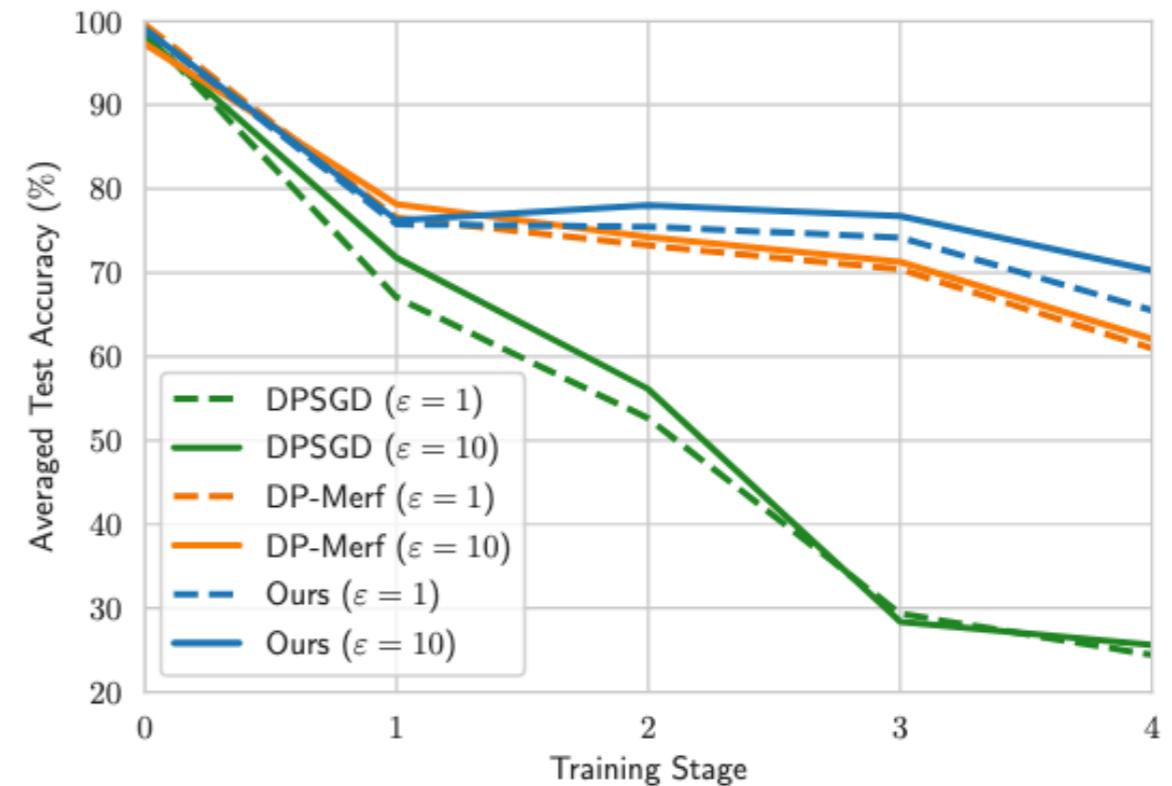
Evaluation



- **Application:** Continual learning with DP



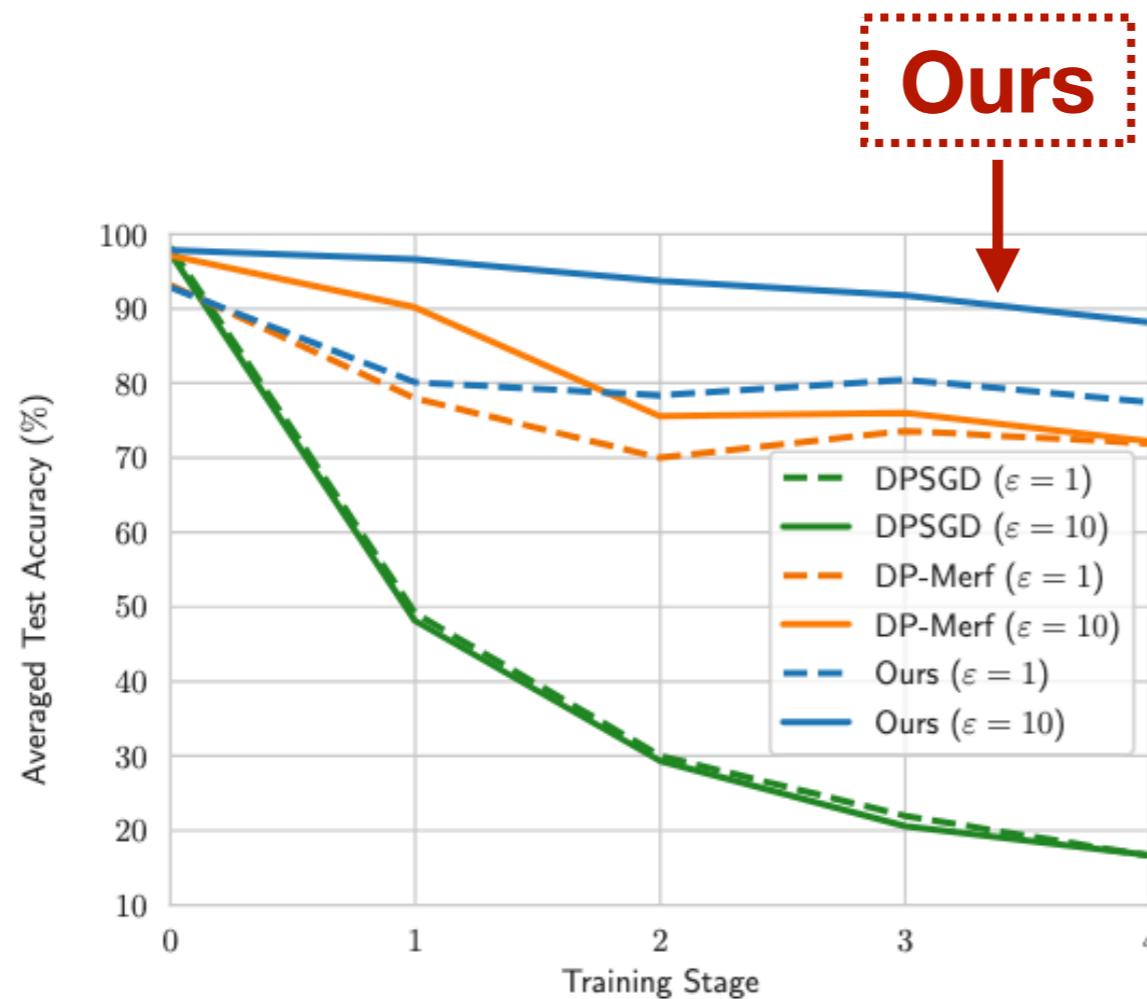
(a) SplitMNIST



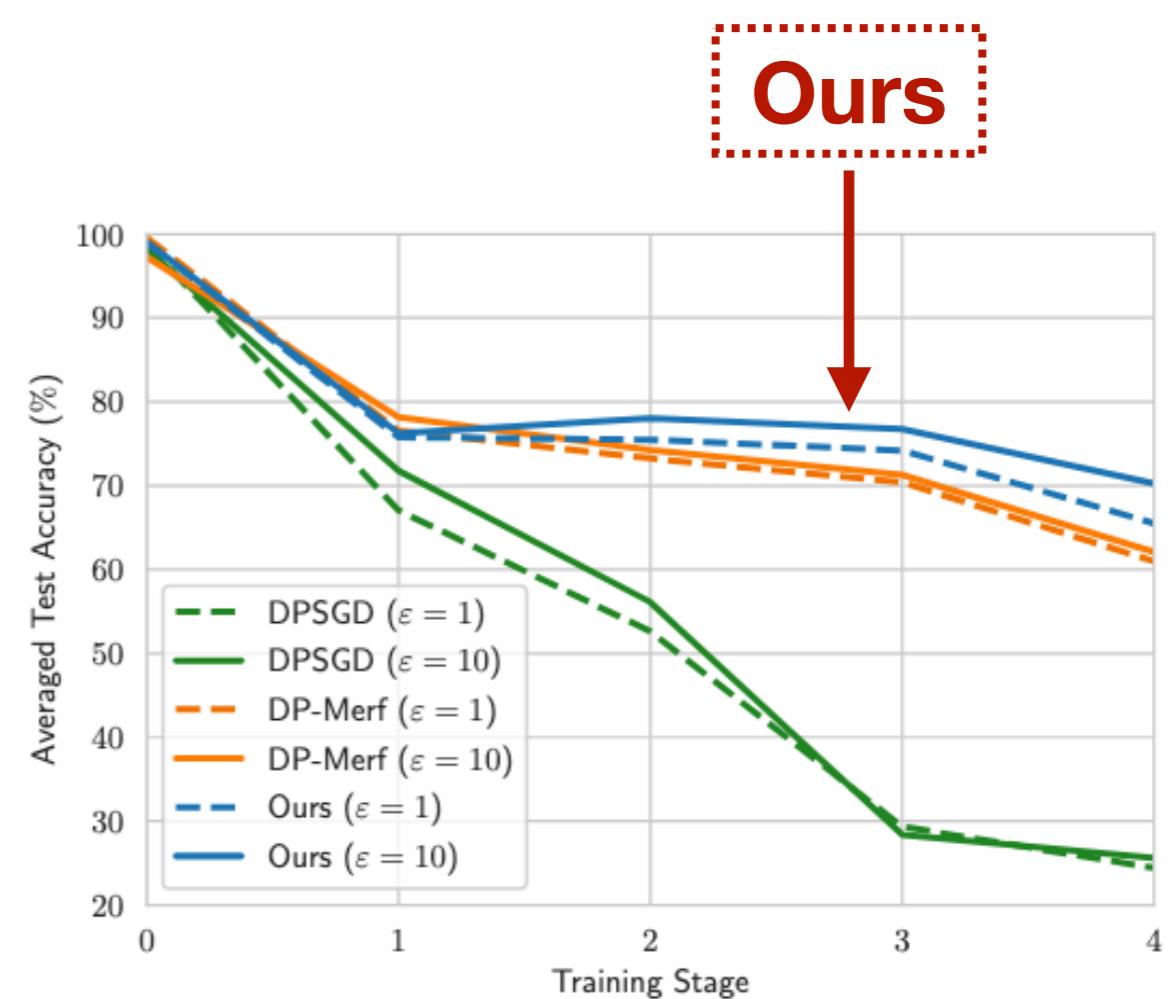
(b) SplitFashionMNIST

Evaluation

- **Application:** Continual learning with DP



(a) SplitMNIST



(b) SplitFashionMNIST

Discussion

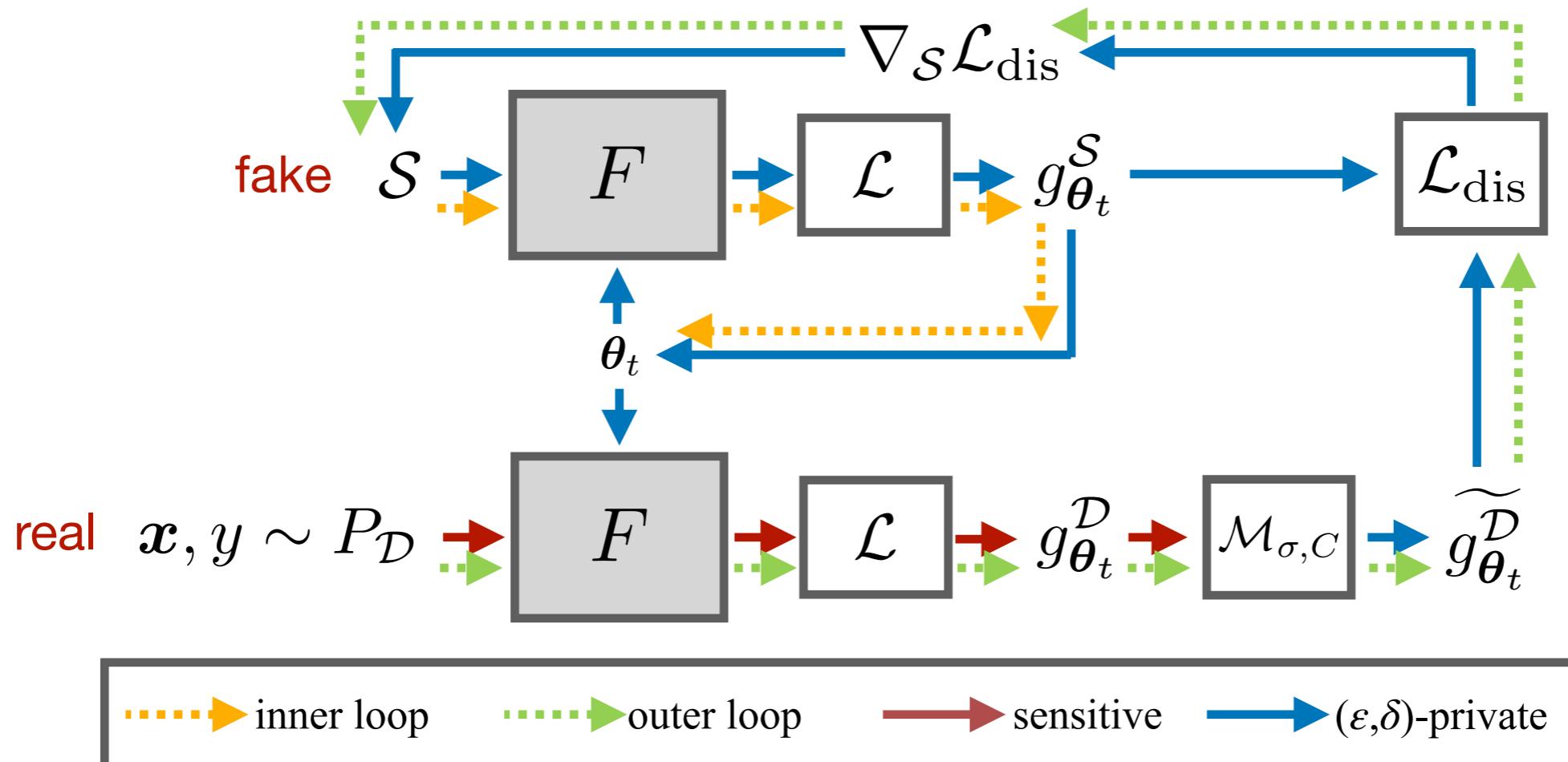


- **Are deep generative models the best option for this task?**

Discussion



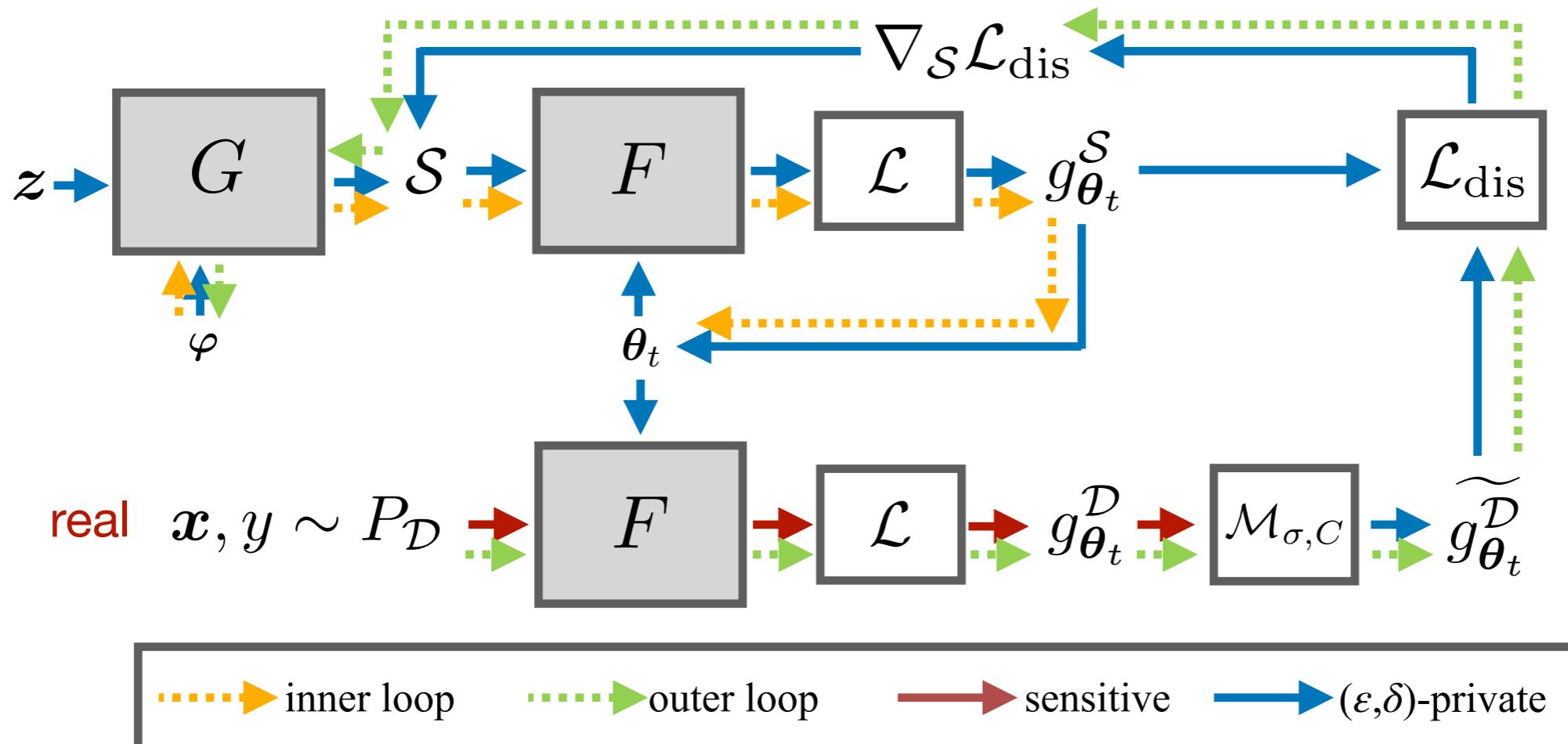
- Are deep generative models the best option for this task?



Discussion



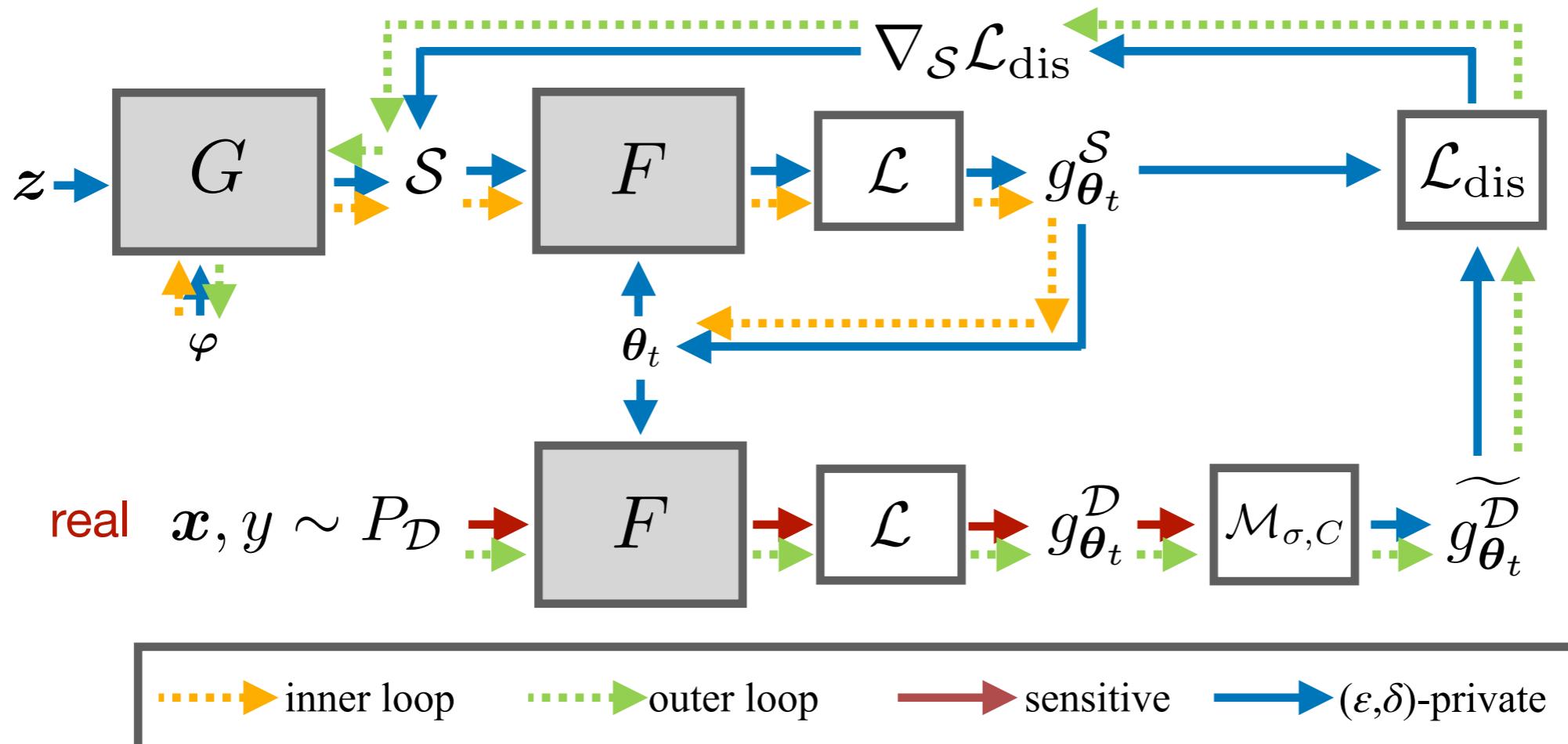
- Are deep generative models the best option for this task?



Discussion



- Are deep generative models the best option for this task?



Discussion



- **Are deep generative models the best option for this task?**

Discussion



- Are deep generative models the best option for this task?

Most probably not!

Discussion



- Are deep generative models the best option for this task?

- Deep generative models result in:

- Better visual quality

- Sub-optimal downstream utility

Most probably not!

0	0 0 0 0 0 0 0 0 0 0
1	1 1 1 1 1 1 1 1 1 1
2	2 2 2 2 2 2 2 2 2 2
3	3 3 3 3 3 3 3 3 3 3
4	4 4 4 4 4 4 4 4 4 4
5	5 5 5 5 5 5 5 5 5 5
6	6 6 6 6 6 6 6 6 6 6
7	7 7 7 7 7 7 7 7 7 7
8	8 8 8 8 8 8 8 8 8 8
9	9 9 9 9 9 9 9 9 9 9

0	0 0 0 0 0 0 0 0 0 0
1	1 1 1 1 1 1 1 1 1 1
2	2 2 2 2 2 2 2 2 2 2
3	3 3 3 3 3 3 3 3 3 3
4	4 4 4 4 4 4 4 4 4 4
5	5 5 5 5 5 5 5 5 5 5
6	6 6 6 6 6 6 6 6 6 6
7	7 7 7 7 7 7 7 7 7 7
8	8 8 8 8 8 8 8 8 8 8
9	9 9 9 9 9 9 9 9 9 9

0	0 0 0 0 0 0 0 0 0 0
1	1 1 1 1 1 1 1 1 1 1
2	2 2 2 2 2 2 2 2 2 2
3	3 3 3 3 3 3 3 3 3 3
4	4 4 4 4 4 4 4 4 4 4
5	5 5 5 5 5 5 5 5 5 5
6	6 6 6 6 6 6 6 6 6 6
7	7 7 7 7 7 7 7 7 7 7
8	8 8 8 8 8 8 8 8 8 8
9	9 9 9 9 9 9 9 9 9 9

0	0 0 0 0 0 0 0 0 0 0
1	1 1 1 1 1 1 1 1 1 1
2	2 2 2 2 2 2 2 2 2 2
3	3 3 3 3 3 3 3 3 3 3
4	4 4 4 4 4 4 4 4 4 4
5	5 5 5 5 5 5 5 5 5 5
6	6 6 6 6 6 6 6 6 6 6
7	7 7 7 7 7 7 7 7 7 7
8	8 8 8 8 8 8 8 8 8 8
9	9 9 9 9 9 9 9 9 9 9

0	0 0 0 0 0 0 0 0 0 0
1	1 1 1 1 1 1 1 1 1 1
2	2 2 2 2 2 2 2 2 2 2
3	3 3 3 3 3 3 3 3 3 3
4	4 4 4 4 4 4 4 4 4 4
5	5 5 5 5 5 5 5 5 5 5
6	6 6 6 6 6 6 6 6 6 6
7	7 7 7 7 7 7 7 7 7 7
8	8 8 8 8 8 8 8 8 8 8
9	9 9 9 9 9 9 9 9 9 9

(a) MNIST (w/o prior)

0	0 0 0 0 0 0 0 0 0 0
1	1 1 1 1 1 1 1 1 1 1
2	2 2 2 2 2 2 2 2 2 2
3	3 3 3 3 3 3 3 3 3 3
4	4 4 4 4 4 4 4 4 4 4
5	5 5 5 5 5 5 5 5 5 5
6	6 6 6 6 6 6 6 6 6 6
7	7 7 7 7 7 7 7 7 7 7
8	8 8 8 8 8 8 8 8 8 8
9	9 9 9 9 9 9 9 9 9 9

0	0 0 0 0 0 0 0 0 0 0
1	1 1 1 1 1 1 1 1 1 1
2	2 2 2 2 2 2 2 2 2 2
3	3 3 3 3 3 3 3 3 3 3
4	4 4 4 4 4 4 4 4 4 4
5	5 5 5 5 5 5 5 5 5 5
6	6 6 6 6 6 6 6 6 6 6
7	7 7 7 7 7 7 7 7 7 7
8	8 8 8 8 8 8 8 8 8 8
9	9 9 9 9 9 9 9 9 9 9

0	0 0 0 0 0 0 0 0 0 0
1	1 1 1 1 1 1 1 1 1 1
2	2 2 2 2 2 2 2 2 2 2
3	3 3 3 3 3 3 3 3 3 3
4	4 4 4 4 4 4 4 4 4 4
5	5 5 5 5 5 5 5 5 5 5
6	6 6 6 6 6 6 6 6 6 6
7	7 7 7 7 7 7 7 7 7 7
8	8 8 8 8 8 8 8 8 8 8
9	9 9 9 9 9 9 9 9 9 9

0	0 0 0 0 0 0 0 0 0 0
1	1 1 1 1 1 1 1 1 1 1
2	2 2 2 2 2 2 2 2 2 2
3	3 3 3 3 3 3 3 3 3 3
4	4 4 4 4 4 4 4 4 4 4
5	5 5 5 5 5 5 5 5 5 5
6	6 6 6 6 6 6 6 6 6 6
7	7 7 7 7 7 7 7 7 7 7
8	8 8 8 8 8 8 8 8 8 8
9	9 9 9 9 9 9 9 9 9 9

(c) MNIST (with prior)

0	0 0 0 0 0 0 0 0 0 0
1	1 1 1 1 1 1 1 1 1 1
2	2 2 2 2 2 2 2 2 2 2
3	3 3 3 3 3 3 3 3 3 3
4	4 4 4 4 4 4 4 4 4 4
5	5 5 5 5 5 5 5 5 5 5
6	6 6 6 6 6 6 6 6 6 6
7	7 7 7 7 7 7 7 7 7 7
8	8 8 8 8 8 8 8 8 8 8
9	9 9 9 9 9 9 9 9 9 9

0	0 0 0 0 0 0 0 0 0 0
1	1 1 1 1 1 1 1 1 1 1
2	2 2 2 2 2 2 2 2 2 2
3	3 3 3 3 3 3 3 3 3 3
4	4 4 4 4 4 4 4 4 4 4
5	5 5 5 5 5 5 5 5 5 5
6	6 6 6 6 6 6 6 6 6 6
7	7 7 7 7 7 7 7 7 7 7
8	8 8 8 8 8 8 8 8 8 8
9	9 9 9 9 9 9 9 9 9 9

0	0 0 0 0 0 0 0 0 0 0
1	1 1 1 1 1 1 1 1 1 1
2	2 2 2 2 2 2 2 2 2 2
3	3 3 3 3 3 3 3 3 3 3
4	4 4 4 4 4 4 4 4 4 4
5	5 5 5 5 5 5 5 5 5 5
6	6 6 6 6 6 6 6 6 6 6
7	7 7 7 7 7 7 7 7 7 7
8	8 8 8 8 8 8 8 8 8 8
9	9 9 9 9 9 9 9 9 9 9

0	0 0 0 0 0 0 0 0 0 0
1	1 1 1 1 1 1 1 1 1 1
2	2 2 2 2 2 2 2 2 2 2
3	3 3 3 3 3 3 3 3 3 3
4	4 4 4 4 4 4 4 4 4 4
5	5 5 5 5 5 5 5 5 5 5
6	6 6 6 6 6 6 6 6 6 6
7	7 7 7 7 7 7 7 7 7 7
8	8 8 8 8 8 8 8 8 8 8
9	9 9 9 9 9 9 9 9 9 9

(d) FashionMNIST (with prior)

Discussion



- Are deep generative models the best option for this task?

- Deep generative models result in:

- Better visual quality 

- Sub-optimal downstream utility 

Most probably not!



(a) MNIST (w/o prior)



(b) FashionMNIST (w/o prior)



(c) MNIST (with prior)



(d) FashionMNIST (with prior)

with generative model

Discussion



- **Are deep generative models the best option for this task?**

- Deep generative models result in:

- Better visual quality
- Slow convergence

Most probably not!

Discussion

- Are deep generative models the best option for this task?

- Deep generative models result in:

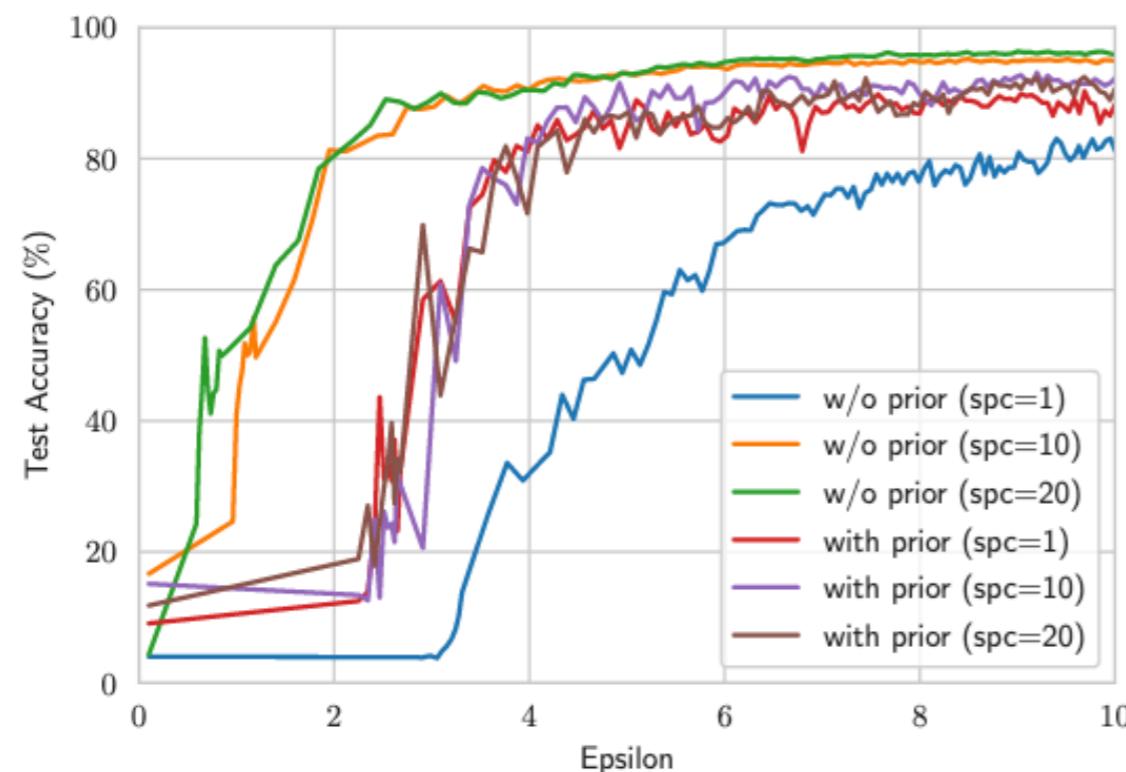
- Better visual quality



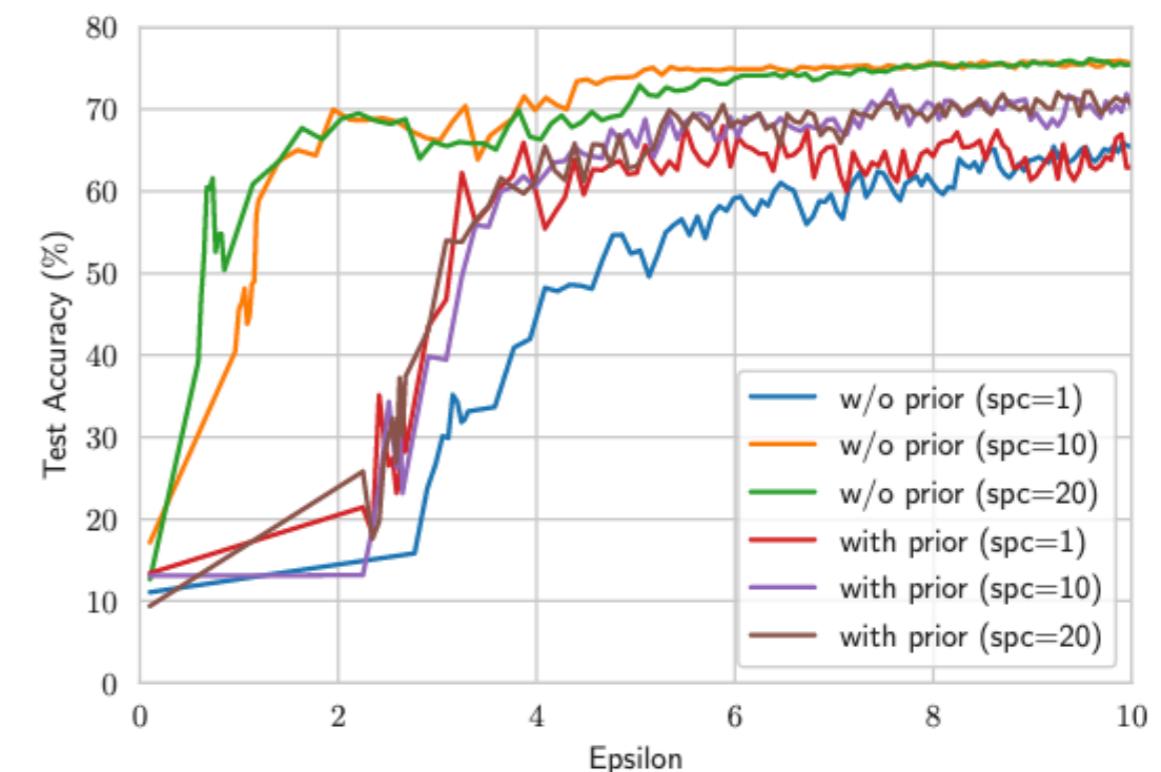
- Slow convergence



Most probably not!



(a) MNIST



(b) FashionMNIST

Discussion



- Are deep generative models the best option for this task?

- Deep generative models result in:

- Better visual quality
- Slow convergence
- Sub-optimal downstream utility

Most probably not!

	MNIST			FashionMNIST		
	1	10	20	1	10	20
w/o prior	81.4	94.9	95.6	66.7	75.6	77.7
with prior	88.2	92.2	90.6	63.0	70.2	70.7

Discussion



- Are deep generative models the best option for this task?

- Deep generative models result in:

- Better visual quality
- Slow convergence
- Sub-optimal downstream utility

Most probably not!

	MNIST			FashionMNIST		
	1	10	20	1	10	20
w/o prior	81.4	94.9	95.6	66.7	75.6	77.7
with prior	88.2	92.2	90.6	63.0	70.2	70.7

with generative model

More details in the paper

Private Set Generation with Discriminative Information

Dingfan Chen

Raouf Kerkouche

Mario Fritz

Source code available on Github:

<https://github.com/DingfanChen/Private-Set>

Contact:

Dingfan Chen, dingfan.chen@cispa.de