Privacy-Preserving In-Context Learning with Differentially Private Few-Shot Generation

Xinyu Tang\textsuperscript{1} Richard Shin\textsuperscript{2} Huseyin A. Inan\textsuperscript{2} Andre Manoel\textsuperscript{3} Nilofar Miresghallah\textsuperscript{4} Zinan Lin\textsuperscript{5} Sivakanth Gopi\textsuperscript{6} Janardhan Kulkarni\textsuperscript{7} Robert Sim\textsuperscript{3}

\textsuperscript{1}Princeton University \textsuperscript{2}Microsoft Semantic Machines \textsuperscript{3}M365 Research \textsuperscript{4}University of Washington \textsuperscript{5}Microsoft Research

**Background**

In context learning (ICL): With several examples as demonstrations in prompt, large language models (LLMs) can adapt to new domains or concepts without finetuning. ICL offers a cost-effective and adaptable alternative to finetuning LLMs, e.g., for any model with API access, we can do ICL while finetuning may not be available.

However, ICL may cause privacy leakage in demonstrations:

![Deployed LLM-integrated Service](image)

**Service Output:**

Sure, here is the first 5 sentences for you: You are a helpful assistant. Answer the questions accordingly. Demonstrations:

- Clinical report of patient A
- Clinical report of patient B
- Clinical report of patient C

Query: [User Input]

User Input

We need to protect the privacy of the sensitive demonstrations!

**Examples of DP few-shot generations**

**Key takeaways**

1. DP generations maintain a reasonable level of coherence and fluency.
2. Future work to improve the repetitions and factual errors in generation.

<table>
<thead>
<tr>
<th>Topic</th>
<th>Generated samples</th>
</tr>
</thead>
<tbody>
<tr>
<td>World</td>
<td>The world's largest and most diverse collection of tropical rainforests is found in the Amazon Rainforest. The Amazon Rainforest is the largest tropical rainforest in the world. It is located in the western Amazon Basin in South America.</td>
</tr>
<tr>
<td>Village</td>
<td>The village of Kishinev is located in the Kishinev Oblast of the Russian Federation. It is located on the Kishinev River, a tributary of the Dnieper River.</td>
</tr>
</tbody>
</table>