Differentially Private Language Generation and Identification in the Limit (Extended Abstract)

Anay Mehrotra ANAYMEHROTRA1@GMAIL.COM
Stanford University
Grigoris Velegkas GVELEGKAS@GOOGLE.COM
Google Research
Xifan Yu XIFAN.YU@YALE.EDU
Yale University
Felix Zhou FELIX.ZHOU@YALE.EDU
Yale University

Editors: Steve Hanneke and Tor Lattimore

Abstract

We initiate the study of language generation in the limit, a model recently introduced by Kleinberg and Mullainathan (2024), under the constraint of differential privacy. We consider the *continual release* model, where a generator must eventually output a stream of valid strings while protecting the privacy of the entire input sequence. Our first main result is that for countable collections of languages, privacy comes at no qualitative cost: we provide an ε-differentially-private algorithm that generates in the limit from *any* countable collection. This stands in contrast to many learning settings where privacy renders learnability impossible. However, privacy does impose a quantitative cost: there are finite collections of size k for which uniform private generation requires $\Omega(k/\varepsilon)$ samples, whereas just one sample suffices non-privately.

We then turn to the harder problem of language *identification* in the limit. Here, we show that privacy creates fundamental barriers. We prove that no ε-DP algorithm can identify a collection containing two languages with an infinite intersection and a finite set difference, a condition far stronger than the classical non-private characterization of identification. Next, we turn to the *stochastic* setting where the sample strings are sampled i.i.d. from a distribution (instead of being generated by an adversary). Here, we show that private identification is possible if and only if the collection is identifiable in the adversarial model. Together, our results establish new dimensions along which generation and identification differ and, for identification, a separation between adversarial and stochastic settings induced by privacy constraints.

Keywords: privacy, continual release, language generation in the limit, identification in the limit

1. Overview

We study *language generation in the limit* (Kleinberg and Mullainathan, 2024) under ε-DP in the *continual release* model (Dwork et al., 2010; Chan et al., 2011), requiring the entire stream of a generator $\mathcal{G}$'s outputs to be stable against changing any single input string from the adversary's enumeration of the target language K from a given collection $\mathcal{L}$. Our main results: **(i)** private generation is qualitatively free. There is an ε-DP algorithm that generates in the limit from *any* countable collection; **(ii)** uniform generation nonetheless has a privacy–utility gap, with tight sample complexity $d + \tilde{\Theta}(k/\varepsilon)$ in the size k and closure dimension d (versus $d + 1$ non-privately); and **(iii)** private identification is qualitatively much more challenging. There are collections that can be non-privately identified but not under ε-DP.

See Mehrotra et al. (2026) for the full version containing all statements and proofs.

Extended abstract. Full version appears as (Mehrotra et al., 2026).

References

T.-H. Hubert Chan, Elaine Shi, and Dawn Song. Private and continual release of statistics. *ACM Trans. Inf. Syst. Secur.*, 14(3):26:1–26:24, 2011. doi: 10.1145/2043621.2043626. URL https://doi.org/10.1145/2043621.2043626.

Cynthia Dwork, Moni Naor, Toniann Pitassi, and Guy N. Rothblum. Differential privacy under continual observation. In Leonard J. Schulman, editor, *Proceedings of the 42nd ACM Symposium on Theory of Computing, STOC 2010, Cambridge, Massachusetts, USA, 5-8 June 2010*, pages 715–724. ACM, 2010. doi: 10.1145/1806689.1806787. URL https://doi.org/10.1145/1806689.1806787.

Jon Kleinberg and Sendhil Mullainathan. Language generation in the limit. *Advances in Neural Information Processing Systems*, 37:66058–66079, 2024.

Anay Mehrotra, Grigoris Velegkas, Xifan Yu, and Felix Zhou. Differentially private language generation and identification in the limit. *arXiv preprint arXiv:2604.08504*, 2026.