Hiding Among the Clones: A Simple and Nearly Optimal Analysis of Privacy Amplification by Shuffling

Vitaly Feldman
Apple

Audra McMillan
Apple

Kunal Talwar
Apple

Abstract

Recent work of Erlingsson et al. [9] demonstrates that random shuffling of input data amplifies differential privacy guarantees. Such amplification leads to substantially stronger privacy guarantees for systems in which data is contributed anonymously [5] and for the analysis of noisy stochastic gradient descent. We show that an ε_0-locally differentially private algorithm, under shuffling with n users, amplifies to a $(\Theta((1-e^{-\varepsilon_0})\sqrt{\frac{e^{\varepsilon_0}\log(1/\delta)}{n}}), \delta)$ central differential privacy guarantee. This significantly improves over previous work and achieves the asymptotically optimal dependence on ε_0. Our result is based on a new approach that is simpler than previous work and extends to approximate differential privacy with nearly the same guarantees. Our work also yields an empirical method to derive tighter bounds on the central ε and we show that it gets to within a small constant factor of the correct bound. As a simple corollary of our analysis we derive a better and simpler algorithm for frequency estimation in the shuffle model of privacy [6].

1 Introduction

In this work we consider privacy-preserving data analysis in the shuffle model of differential privacy. In this model, each user sends a locally differentially private report and these reports are then anonymized and randomly shuffled. This model was first proposed by Bittau et al. [5]. Erlingsson et al. [9] showed that random shuffling of inputs to local protocols amplifies the privacy guarantees and thus, when the collection of anonymized reports is viewed in the central model, the privacy guarantees are substantially stronger than the original local privacy guarantees. A similar result was shown for the binary randomized response by Cheu et al. [6] who also formalized the resulting model as the shuffling model of privacy.

The analysis in [9] relies on the privacy amplification by shuffling of the inputs to the local randomizers and holds even when local randomizers are chosen sequentially and adaptively. This allows one to analyze iterative algorithms such as noisy SGD run on a random permutation of data points, bridging a disconnect between the prior theoretical analyses and practice.

A key limitation of the amplification result in [9] is that it has suboptimal dependence on the local privacy parameter ε_0 when $\varepsilon_0 > 1$. Specifically, in this regime the resulting central privacy parameter is $\tilde{O}(e^{3\varepsilon_0}/\sqrt{n})$[1]. For the simpler setting in which the local randomizer is fixed (and, in particular, non-adaptive) Balle et al. [4] give a stronger bound of $\tilde{O}(e^{\varepsilon_0}/\sqrt{n})$ using a different proof approach. These results are in contrast to the binary randomized response for which the bound is just $\tilde{O}(e^{\varepsilon_0/2}/\sqrt{n})$ [6]. The regime where the local privacy guarantee $\varepsilon_0 > 1$ is commonly used in practice. Further, this regime naturally arises when the target central ε is greater than $1/\sqrt{n}$.

[1] The dependence on ε_0 was recently sharpened to $e^{2.5\varepsilon_0}$ in [3].

Preprint. Under review.

In this paper we give two new analyses of privacy amplification by shuffling. Specifically, we show that running a sequence of arbitrary ε_0-DP local randomizers on a uniformly random permutation of n data items, yields an (ε, δ)-DP algorithm, where

$$\varepsilon = \Theta\left((1 - e^{-\varepsilon_0})\frac{\sqrt{e^{\varepsilon_0}\log(1/\delta)}}{\sqrt{n}}\right).$$

When $\varepsilon_0 > 1$, this improves the dependence on ε_0 from $e^{2.5\varepsilon_0}$ to $e^{\varepsilon_0/2}$ matching the upper bound for the fixed binary randomized response [6]. The bound matches the existing bounds in the regime when $\varepsilon_0 < 1$ and is asymptotically optimal in both regimes.We then extend this analysis to approximately differentially private local randomizers with essentially the same guarantees. The best previous guarantee in this case has dependence of $e^{20\varepsilon_0}$ [3].

Importantly, our proof is also simpler than the rather delicate approaches in prior work [9, 4]. The proof reduces the problem of analyzing the shuffling privacy guarantee of an adaptive series of local algorithms to analyzing the shuffling privacy guarantee of a simple non-adaptive local algorithm on three inputs. Intuitively, we argue that given a single data point x, every other data point has some probability of sampling from the same output distribution as x. That is, each data point becomes a clone of x with some probability. For the $\varepsilon_0 > 1$ regime, the desired privacy guarantees then follow easily from the number of clones that x has to hide among being distributed as a binomial random variable. In the small ε_0-regime we also rely on the fact that a local randomizer on two inputs can be seen as the composition of binary randomized response with a post-processing step. The proof extends naturally to approximate differential privacy. In addition, it provides an efficient method for empirically computing an the amplification bound that is tighter than our theoretical statements.

Privacy amplification with the optimal dependence on ε_0 allows us to design algorithms that achieve optimal trade off between privacy and utility in the central model while also achieving some level of local differential privacy guarantees. We show an example of such an algorithm for frequency estimation / histograms in Section 2.1. For a given level of accuracy, this algorithm simultaneously achieves optimal central as well as local differential privacy bounds. This algorithm also enjoys low communication, and improves on the best bounds in the shuffle model of privacy [12].

1.1 Background and Related Work

Differential privacy is a measure of stability of a randomized algorithm. It ensures that the distribution on outputs changes slowly with changes in the input, in particular so that changes to a single individual's data are hidden. The measure of closeness of output distributions is (ε, δ)-indistinguishability. Two random variables P and Q are (ε, δ)-*indistinguishable* if for all events E,

$$e^{-\varepsilon}\Pr(Q \in E) - \delta \leq \Pr(P \in E) \leq e^{\varepsilon}\Pr(Q \in E) + \delta.$$

We will be concerned in this paper with both local and central differential privacy. In the local model, formally introduced in [13], each individual randomizes their data before sending it to the data curator. This means that individuals are not required to trust the curator. Due to this minimal trust model, most industrial deployments of differential privacy leverage local differential privacy [10, 2, 7].

Definition 1.1 (Local Differential Privacy)**.** An algorithm $\mathcal{A} : \mathcal{D} \to \mathcal{O}$ is (ε, δ)-*locally differentially private* if for all pairs $x, x' \in \mathcal{D}$, $\mathcal{A}(x)$ and $\mathcal{A}(x')$ are (ε, δ)-indistinguishable.

In the central model, introduced in [8], individuals send their data directly to the curator. The central curator is then trusted to perform queries on the data whose output does not disclose too much about the individual's data. While this model requires a higher level of trust than the local model, it is possible to design significantly more accurate mechanisms. We say that two databases are neighbouring if they differ on the data of a single individual.

Definition 1.2 (Central Differential Privacy)**.** An algorithm $\mathcal{A} : \mathcal{D}^n \to \mathcal{O}$ is (ε, δ)-*differentially private* if for all neighbouring databases X and X', $\mathcal{A}(X)$ and $\mathcal{A}(X')$ are (ε, δ)-indistinguishable.

In both models, if $\delta = 0$ then we will refer to an algorithm as ε-differentially private. Further, we will occasionally refer to $\delta = 0$ as pure differential private and $\delta > 0$ as approximate differential privacy.

The shuffle model provides a bridge between the local and central models of differential privacy. As in the local model, individuals randomize their data before transmitting to the central curator. The curator then anonymizes the local reports (by applying a random permutation). The anonymization of local reports to improve privacy was proposed in [5], who designed and implemented a principled systems architecture for shuffling. The intuition was formalised in [9, 6]. [9] showed that for general local DP mechanisms, when viewed in the central model, the anonymized local reports enjoy a much high privacy guarantee than the local guarantee might suggest. The optimal dependence on ε_0 for binary algorithms was given by [6]. The privacy amplification by shuffling bounds were further improved [4, 14, 3] to include tighter analyses for specific algorithms [4, 3], and amplification for (ϵ, δ)-DP local algorithms [3].

2 Improved Guarantees for Privacy Amplification by Shuffling

In this section we present our main technical theorem, an improved upper bound on the central privacy guarantee in the shuffle model. Given $a, b \in [n]$, let $\tau_{a,b}$ be the transposition that swaps a and b.

Theorem 2.1. *For a domain $\mathcal{D}$, let $\mathcal{A}_{\mathrm{ldp}}^{(i)} : \mathcal{S}^{(1)} \times \cdots \times \mathcal{S}^{(i-1)} \times \mathcal{D} \to \mathcal{S}^{(i)}$ for $i \in [n]$ (where $\mathcal{S}^{(i)}$ is the range space of $\mathcal{A}_{\mathrm{ldp}}^{(i)}$) be a sequence of algorithms such that $\mathcal{A}_{\mathrm{ldp}}^{(i)}$ is ε_0-DP for all values of auxiliary inputs $\mathcal{S}^{(1)} \times \cdots \times \mathcal{S}^{(i-1)}$. Let $\mathcal{A}_{\mathrm{s}} : \mathcal{D}^n \to \mathcal{S}^{(1)} \times \cdots \times \mathcal{S}^{(n)}$ be the algorithm that given a dataset $x_{1:n} \in \mathcal{D}^n$, samples $a \in [n]$ uniformly at random, then sequentially computes $z_i = \mathcal{A}_{\mathrm{ldp}}^{(i)}(z_{1:i-1}, x_{\tau_{1,a}(i)})$ for $i \in [n]$ and outputs $z_{1:n}$. Let X and X' be neighbouring databases such that $x_1 \neq x_1'$. Then for any $\delta \in [0, 1]$ such that $\varepsilon_0 \leq \log(\frac{n}{16 \log(2/\delta)})$, $\mathcal{A}_{\mathrm{s}}(X)$ is (ε, δ)-indistinguishable from $\mathcal{A}_{\mathrm{s}}(X')$, where*

$$\varepsilon \leq \log\left(1 + (1 - e^{-2\varepsilon_0})\left(\frac{8\sqrt{e^{\varepsilon_0}\log(4/\delta)}}{\sqrt{n}} + \frac{8e^{\varepsilon_0}}{n}\right)\right) \tag{1}$$

Due to space constraints, the proof of Theorem 2.1 has been omitted. In addition to the theoretical upper bound on the central epsilon given in Theorem 2.1, our proof also gives us an efficient method for empirically computing a tighter upper bound. We will demonstrate this empirical approach in Section 3.

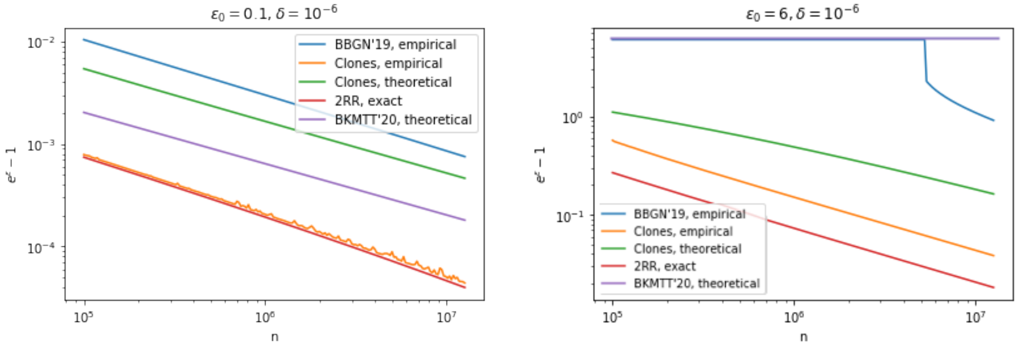
Since a transposition is sufficient to amplify the privacy guarantee of a single individual, a random permutation is sufficient to amplify the overall privacy guarantee. This gives us a privacy amplification by shuffling result. For brevity, we state our corollary for more general case of approximately differentially private local algorithms. An analysis of privacy amplification by shuffling of (ε, δ)-DP local randomizers was first given in [3] who achieved a central ε of order $\Theta(\frac{e^{30\varepsilon_0}}{n} + \frac{e^{20\varepsilon_0}\sqrt{\log(1/\delta)}}{\sqrt{n}})$ in the high ε_0 regime, which we improve significantly.The proof of Proposition 2.2 is a slight variation on the proof of Theorem 2.1. The main additional technique required is a conversion of an (ε, δ)-local DP mechanism to a ε-DP mechanism that has almost the same output distributions.

Proposition 2.2. *For a domain $\mathcal{D}$, let $\mathcal{A}_{\mathrm{ldp}}^{(i)} : \mathcal{S}^{(1)} \times \cdots \times \mathcal{S}^{(i-1)} \times \mathcal{D} \to \mathcal{S}^{(i)}$ for $i \in [n]$ (where $\mathcal{S}^{(i)}$ is the range space of $\mathcal{A}_{\mathrm{ldp}}^{(i)}$) be a sequence of algorithms such that $\mathcal{A}_{\mathrm{ldp}}^{(i)}$ is $(\varepsilon_0, \delta_0)$-DP for all values of auxiliary inputs $\mathcal{S}^{(1)} \times \cdots \times \mathcal{S}^{(i-1)}$. Let $\mathcal{A}_{\mathrm{s}} : \mathcal{D}^n \to \mathcal{S}^{(1)} \times \cdots \times \mathcal{S}^{(n)}$ be the algorithm that given a dataset $x_{1:n} \in \mathcal{D}^n$, samples a uniformly random permutation π, then sequentially computes $z_i = \mathcal{A}_{\mathrm{ldp}}^{(i)}(z_{1:i-1}, x_{\pi(i)})$ for $i \in [n]$ and outputs $z_{1:n}$. Then for any $\delta \in [0, 1]$ such that $\varepsilon_0 \leq \log(\frac{n}{16\log(2/\delta)})$, $\mathcal{A}_{\mathrm{s}}$ is $(\varepsilon, \delta + (e^{\varepsilon} + 1)(1 + e^{-\varepsilon_0})n\delta_0)$-DP, where ε is as in Equation (1).*

2.1 Frequency Estimation

In this section we show how our amplification result can be used to obtain an algorithm for histogram estimation in the shuffle model with optimal error in the central model and low communication. Let $x_1, \cdots, x_n$ be n values from $[k]$. The problem of Frequency Estimation is to estimate for each $j \in [k]$, the value $n_j = |\{i \in [n] : x_i = j\}|$, given the data set $X = \{x_1, \cdots, x_n\}$. For simplicity, we will consider the relative frequency $p_j = n_j/n$. The optimal solution to this problem under central differential privacy is well-understood [8]. There exists an ε-DP algorithm in the central model of differential privacy that outputs an estimate $\hat{p}$ such that with high probability

$$\max_{i \in [k]} |p(i) - \hat{p}(i)| = \Theta\left(\frac{\min\{\log k, \log(1/\delta)\}}{\epsilon n}\right).$$



(a) Comparison of central ε for fixed $\varepsilon_0 = 0.1$ and $\delta = 10^{-6}$ and n ranging between 10^5 and 10^7.

(b) Comparison of central ε for fixed $\varepsilon_0 = 6$ and $\delta = 10^{-6}$ and n ranging between 10^5 and 10^7.

Figure 1: Comparison of new privacy amplification by shuffling bounds given in this work to bounds given in [4] and [6].

This error is known to be optimal in the central model [15, Theorem 5.14].

Frequency estimation in the local model is also well studied. Recently [1] gave an efficient, low communication ($\log k$ communication) ε_0-local DP algorithm that outputs an estimate $\hat{p}$ such that (for large ϵ_0) with high probability, $\max_{i\in[k]} |p(i) - \hat{p}(i)| = O\left(\frac{\sqrt{\log k}}{\sqrt{e^{\varepsilon_0} n}}\right)$. Prior work on frequency estimation in the shuffle model has been unable to properly leverage the results in the local model since the dependence on ε_0 was too large. Indeed, [6] and [11] give algorithms that achieve the right central privacy-utility trade-offs, but these algorithms are complex, have either a polynomial communication or polynomial computation complexity, and require multiple rounds of communication. Using our optimal amplification by shuffling results, we are able to leverage the local DP result of [1] to immediately obtain a low communication, single round algorithm in the shuffle model whose error (up to logarithmic factors) matches the optimal error in the central model, as well as the local model.

For a local randomizer $\mathcal{A}_{\text{ldp}}$, let $\mathcal{A}_{\text{s}}(\mathcal{A}_{\text{ldp}})$ be the algorithm that given a data set $x_{1:n} \in \mathcal{D}^n$, samples a uniform random permutation π over $[n]$, then outputs $(\mathcal{A}_{\text{ldp}}(x_{\pi(1)}), \cdots, \mathcal{A}_{\text{ldp}}(x_{\pi(n)}))$.

Theorem 2.3. *There exists a local randomizer $\mathcal{A}_{\text{ldp}}$ with communication complexity $O(\log k)$ such that $\mathcal{A}_{\text{s}}(\mathcal{A}_{\text{ldp}})$ satisfies (ε, δ)-DP and there exists an algorithm f such that if $\hat{p} = f \circ \mathcal{A}_{\text{s}}(\mathcal{A}_{\text{ldp}})$ then with high probability*

$$\max_{i\in[k]} |p(i) - \hat{p}(i)| = O\left(\frac{\sqrt{\log k \log(1/\delta)}}{\epsilon n}\right).$$

Note that the fact that Theorem 2.3 obtains obtains the optimal central model error up to logarithmic error implies that Proposition 2.2 must be tight up to logarithmic factors.

3 Numerical Results

In this section, we provide numerical evaluations of the privacy amplification bound given in Proposition 2.2 with $\delta_0 = 0$. `Clones, theoretical` is the bound presented in Proposition 2.2 with $\delta_0 = 0$, while `Clones, empirical` is a numerical computation of this bound. In Figure 1, `BBGN'19` is the privacy amplification bound for general algorithm given by [4][2], `BKMTT'20` is the bound proven in [3] and `2RR, exact` is an exact computation of the shuffling privacy guarantee of randomized response, which appeared in [6]. We do not compare to [9] since empirically it is outperformed by [4] in most parameter regimes. We can see in both figures that `Clones, empirical` is tighter than previous general bounds in both regimes, and `Clones, theoretical` is tighter for large ε_0.

[2] `BBGN'19` curves were produced using open source code released by [4].

References

[1] Jayadev Acharya, Ziteng Sun, and Huanyu Zhang. Hadamard response: Estimating distributions privately, efficiently, and with little communication. volume 89 of *Proceedings of Machine Learning Research*, pages 1120–1129. PMLR, 16–18 Apr 2019.

[2] Apple's Differential Privacy Team. Learning with privacy at scale. *Apple Machine Learning Journal*, 1(9), 2017.

[3] B. Balle, Peter Kairouz, H. McMahan, Om Thakkar, and Abhradeep Thakurta. Privacy amplification via random check-ins. *ArXiv*, abs/2007.06605, 2020.

[4] Borja Balle, James Bell, Adrià Gascón, and Kobbi Nissim. The privacy blanket of the shuffle model. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology – CRYPTO 2019*, pages 638–667, Cham, 2019. Springer International Publishing.

[5] Andrea Bittau, Úlfar Erlingsson, Petros Maniatis, Ilya Mironov, Ananth Raghunathan, David Lie, Mitch Rudominer, Ushasree Kode, Julien Tinnes, and Bernhard Seefeld. Prochlo: Strong privacy for analytics in the crowd. In *Proceedings of the 26th Symposium on Operating Systems Principles*, SOSP '17, page 441–459, New York, NY, USA, 2017. Association for Computing Machinery.

[6] Albert Cheu, Adam Smith, Jonathan Ullman, David Zeber, and Maxim Zhilyaev. Distributed differential privacy via shuffling. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2019*, pages 375–403, Cham, 2019. Springer International Publishing.

[7] Bolin Ding, Janardhan Kulkarni, and Sergey Yekhanin. Collecting telemetry data privately. In *Proceedings of the 31st International Conference on Neural Information Processing Systems*, NIPS'17, page 3574–3583, Red Hook, NY, USA, 2017. Curran Associates Inc.

[8] Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith. Calibrating noise to sensitivity in private data analysis. In Shai Halevi and Tal Rabin, editors, *Theory of Cryptography*, pages 265–284, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg.

[9] Úlfar Erlingsson, Vitaly Feldman, Ilya Mironov, Ananth Raghunathan, Kunal Talwar, and Abhradeep Thakurta. Amplification by shuffling: From local to central differential privacy via anonymity. In *Proceedings of the Thirtieth Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '19, page 2468–2479, USA, 2019. Society for Industrial and Applied Mathematics.

[10] Úlfar Erlingsson, Vasyl Pihur, and Aleksandra Korolova. Rappor: Randomized aggregatable privacy-preserving ordinal response. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, CCS '14, page 1054–1067, New York, NY, USA, 2014. Association for Computing Machinery.

[11] Badih Ghazi, Noah Golowich, R. Kumar, R. Pagh, and A. Velingker. On the power of multiple anonymous messages. *IACR Cryptol. ePrint Arch.*, 2019:1382, 2019.

[12] Badih Ghazi, Rasmus Pagh, and Ameya Velingker. Scalable and differentially private distributed aggregation in the shuffled model, 2019.

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

[14] Úlfar Erlingsson, Vitaly Feldman, Ilya Mironov, Ananth Raghunathan, Shuang Song, Kunal Talwar, and Abhradeep Thakurta. Encode, shuffle, analyze privacy revisited: Formalizations and empirical evaluation, 2020.

[15] Salil Vadhan. *The Complexity of Differential Privacy*, pages 347–450. 04 2017.