DAMS: Meta-estimation of private sketch data structures for differentially private COVID-19 contact tracing

Praneeth Vepakomma , Subha Nawer Pushpita , Ramesh Raskar
MIT
Cambridge, MA 02139, USA
vepakom@mit.edu

Abstract

We propose an improved private count-mean-sketch data structure and show its applicability to differentially private contact tracing. Our proposed scheme (***D**iversifed* **A**veraging for **M**eta estimation of **S**ketches-DAMS) provides a better trade-off between true positive rates and false positive rates while maintaining differential privacy (a widely accepted formal standard for privacy). We show its relevance to the social good application of private digital contact tracing for COVID-19 and beyond. The scheme involves one way locally differentially private uploads from the infected client devices to a server that upon a post-processing obtains a private aggregated histogram of locations traversed by all the infected clients within a time period of interest. The private aggregated histogram is then downloaded by any querying client in order to compare it with its own data on-device, to determine whether it has come into close proximity of any infected client or not. We present empirical experiments that show a substantial improvement in performance for this particular application. We also prove theoretical variance-reduction guarantees of the estimates obtained through our scheme and verify these findings via experiments as well.

Introduction

Distributed applications involving multiple client entities often have stringent privacy requirements that are governed by legal regulations such as HIPAA (Mercuri 2004), GDPR (Goddard 2017) and PIPEDA (Austin 2005). Such requirements are also necessitated by individual preferences, ethical guidelines, national security interests and for seamlessly enabling partnerships in a rapidly globalizing society. One such societal application; that has recently come under the spotlight of privacy researchers given the global advent of the recent COVID-19 pandemic, is that of private digital contact tracing and exposure notification (Rivest et al. 2020; Tang 2020; Chan et al. 2020; Martin et al. 2020; Raskar et al. 2020; Fitzsimons et al. 2020; Hatke et al. 2020; Ahmed et al. 2020; Cho, Ippolito, and Yu 2020; Reichert, Brack, and Scheuermann 2020; Altuwaiyan, Hadian, and Liang 2018; Greiner et al. 2015). As shown in Figure 1, this refers to the problem of privately ascertaining whether a querying client has come into close proximity of an infected patient to privately notify the querying user with an obtained result. Currently cryptographic methods and differential privacy (Dwork, Roth, and others 2014; Dwork 2008;

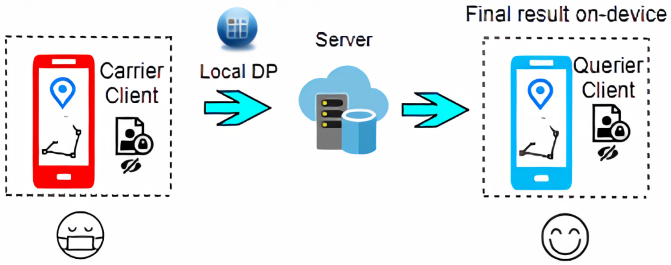

Figure 1: **Private contact tracing** refers to the problem of privately ascertaining whether a querying client has come into close proximity of any patient that is an infected carrier. Our proposed scheme involves a one-way upload of locally differentially private (local DP) informmation into the server that is downloaded by any client performing a contact tracing.

McSherry and Talwar 2007; Dwork and Smith 2010) are one of the widely accepted mathematical notions of formal privacy with varying levels of adoption for different applications. For example, the next U.S census (Abowd 2018; Abowd et al. 2019) is being privatized via differential privacy while several end to end encrypted messaging platforms are powered by cryptographic techniques. With respect to private digital contact tracing, several apps have recently been released and are are currently based on cryptographic schemes (Rivest et al. 2020; Chan et al. 2020; Beskorovajnov et al. 2020; Trieu et al. 2020; Singh et al. 2020; Berke et al. 2020; Chen and Hu 2020; Liu et al. 2020) such as secure multi-party computation (secure MPC), homomorphic encryption and public-key cryptosystems. In this paper, we propose one of the earliest solutions (to the best of our knowledge) for contact tracing that is instead based on differential privacy.

Works such as (Groce, Rindal, and Rosulek 2019) have shown that differentially private technologies can drastically reduce the computational and communication costs of large-scale systems compared to cryptographic technologies albeit at a weaker trade-off with privacy. A recent trend has been to build systems that depend on both differential privacy and cryptographic technologies at the same time (Wagh et al. 2020; Chowdhury et al. 2019) for better performance

guarantees. Thereby having a differentially private solution to contact tracing can have a downstream benefit from such efforts as well. All of our codebase will be made available as described in the ethics statement.

Contributions

1. We propose the first differentially private solution to COVID-19 contact tracing using sketching data structures.
2. We propose a new meta-estimator (DAMS) based on the private count-min sketch data structure and apply it to private digital contact tracing. We evaluate its performance over important baselines on multiple real-life trajectory datasets of human mobility with respect to the classification metrics of private digital contact tracing. We empirically show that our meta-estimator performs at a drastically higher true positive rate (TPR) with a relatively much lower false positive rate (FPR) in comparison to these baselines.
3. We theoretically show that our meta-estimator (Private DAMS) is unbiased, and has lower variance than that of private count-mean-sketch (PCMS).

Related work

We categorize works related to this paper into three categories of: *private digital contact tracing, local differential privacy and private sketching methods*.

Private digital contact tracing methods

There has been a rapid flurry of mobile apps released globally for digital contact tracing with varying levels of privacy protections. Within this space, a majority of deployed solutions or the ones that are undergoing rapid refinements are cryptography based as categorized in Table 1.

Differential privacy has been another popular approach for formal privacy. For example, it is being used to privatize the 2020 U.S census (Abowd 2018; Abowd et al. 2019) that is currently underway. There has not been much work at the intersection of differential privacy and contact tracing as yet, as shown in this table. DAMS for private contact tracing is instead based on differential privacy to help further the research on private digital contact tracing from a different viewpoint.

Local differential privacy

We employ the local differential privacy setting (Cormode et al. 2018; Cormode, Kulkarni, and Srivastava 2018; Joseph et al. 2019; Kairouz, Oh, and Viswanath 2014), where privacy is maintained locally at the client level. In this version, a privatized dataset is released from a client and a post-processing is applied remotely over this privatized dataset on a server or another client in order to complete analysis/model training/inference over that dataset. A weaker, yet relatively similar setting to local differential privacy is called 'non-interactive private data release' (Chanyaswad, Liu, and Mittal 2019; Smith, Thakurta, and Upadhyay 2017) . The key difference is that in local differential privacy, each data owner; for e.g. an individual iPhone user, privatizes his/her data before sending it out for any post-processing as against to non-interactive differential privacy that requires a trusted centralized unit who sees the original data (not the privatized version); for e.g. everyone's keyboard input data. Then, the trusted centralized unit privatizes the data before releasing them to the public.

Sketching methods

Sketching methods are popular for streaming data analysis, efficient information retrieval, and large scale machine learning. These techniques typically involve a dictionary of multiple hash functions used to hash the dataset into a table or data structure. In order to obtain the solution to any specific query such as frequency estimation, inner-product search or range estimation; a post-processing function corresponding to that particular query is applied on the data structure in order to efficiently obtain the result. Bloom filters (Broder and Mitzenmacher 2004) are one of the earliest such randomized data structures. Other examples of sketching methods (Indyk 2007; Braverman and Ostrovsky 2013; Andoni et al. 2009; Pilanci and Wainwright 2015) include Hadamard sketch (Team 2017), Broder's Sketch (Broder 2000), MinHash (Shrivastava and Li 2014; Ioffe 2010), AMS Sketch (Alon, Matias, and Szegedy 1999) and Count-Min-Sketch (Cormode and Garofalakis 2007; Cormode and Muthukrishnan 2005). Differential private versions of some of these skectching methods like (Team 2017; Erlingsson, Pihur, and Korolova 2014) exist. We modify this private count-mean-sketch data structure to obtain a better trade-off in terms of the true positive rate (TPR) and false positive rate (FPR) upon testing it on contact tracing usecases.

Preliminaries

Notation: The notation used in this paper is summarized for ease of reference in Table 2.

Definition 1 (ϵ-Local Randomizer (Dwork, Roth, and others 2014))**.** *Let $A : D \mapsto Y$ be a randomized algorithm mapping a data entry in data domain D to Y. The algorithm A is an ϵ-local randomizer if for all data entries $d, d' \in D$ and all outputs $y \in Y$, we have $-\epsilon \leq \ln\left(\frac{\Pr[A(d)=y]}{\Pr[A(d')=y]}\right) \leq \epsilon$.*

Definition 2 (Local Differential Privacy (Dwork, Roth, and others 2014; Team 2017))**.** *Let $A : D_n \mapsto Z$ be a randomized algorithm mapping a dataset with n records to some arbitrary range Z. The algorithm A is ϵ-local differentially private if it can be written as $A(d_1, \ldots, d_n) = \phi(A_1(d_1), \ldots, A_n(d_n))$ where each $A_i : D \mapsto Y$ is an ϵ- local randomizer for each $i \in [n]$ and $\phi : Y_n \mapsto Z$ is some post-processing function of the privatized records $A_1(d_1), \ldots, A_n(d_n)$. Note that the post-processing function does not have access to the raw data records.*

Private count-mean-sketch

The work in (Team 2017) provides a locally differentially private mechanism called private count mean sketch (PCMS) for privately releasing histograms. It is based on a non private version of this data structure (CMS) in (Cormode and Garofalakis 2007). PCMS has a client-side algorithm and a server-side algorithm. The client-side algorithm

	Cryptographic	Differential Privacy	Spatio-temporal differential privacy for correlated data (non i.i.d)	Differential Privacy for correlated data (non i.i.d)
Digital Contact Tracing	PACT, G.A.E.N, PrivateKit-SafePaths (now PathCheck), EpiOne, PPContactTracing, TraceSecure, BlueTrace, Blind Contact Tracing, DP3T, ConTraCorona, CovidSafe, StopCovid, CovidWatch, DESIRE, Pronto-C2	Private DAMS (Our Method)	None	None
Other applications	Extensive work	Extensive work	Geo-Indistinguishability, UD-LMDP/UC-LMDP, Planar Isotropic Mechanism, PANDA, δ-location set DP	Correlated Iteration Mechanism, PufferFish, LBS Queries Bayesian Differential Privacy, DDP

Table 1: We compare and categorize the proposed method within the current landscape of works on the private digital contact tracing problem. Green refers to solutions that are already deployed or in an advanced stage of development. Red refers to methods that are non-existant (referred by none), or not deployed within the context of private digital contact tracing. Pastel yellow, refers to our proposed method that is currently a prototype that has gone beyond the research stage as we plan to engineer it towards a controlled deployment, while we move on to create, adopt or build upon works currently in red for the contact tracing problem as part of future research. The red areas under other applications are very promising but need accelerated research for adopting them within the context of private digital contact tracing. The orange areas refer to differential privacy methods for non i.i.d spatio-temporal data that exist, but have not been adapted yet for contact tracing applications.

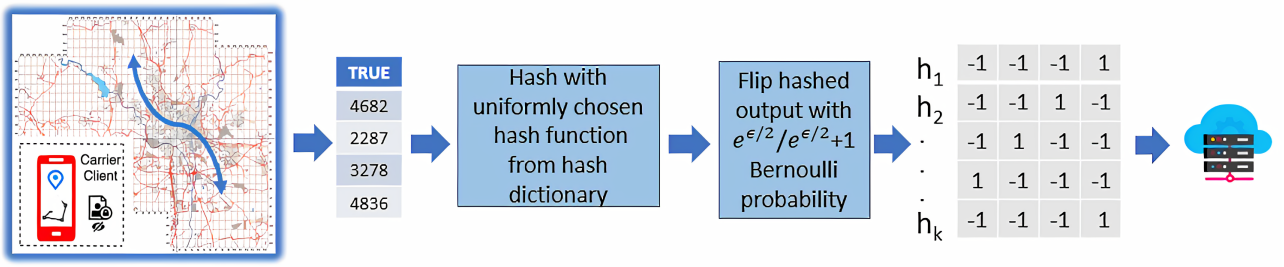

Figure 2: Sketch of the local DP scheme for standard private count-mean-sketch. Note that this the client side of the scheme that is prior to applying the server's post-processing function. We contrast this with our proposed meta-estimator in Figure 3.

Depth	k
Width	m
Hash Dictionaries	$\mathcal{H}_1, \mathcal{H}_2, \ldots, \mathcal{H}_p$
Hash Functions	$h_1, h_2, \ldots, h_k$
Privacy Parameter	ϵ
Dataset Size (# of records)	n
Dataset	$D_n = \{d_1, d_2, \ldots d_n\}$
Hash Output	$v \in \mathbb{R}^m$
Post-Processing Function	ϕ
Count Estimator	$\tilde{f}(d)$
Bernoulli Noise Vector	$b \in \{-1, +1, \}^m$
# of Clients	w
Histograms	$F_1, F_2 \ldots F_p$
Sketch Matrix	$\mathbf{M}$

Table 2: This is the notation used in this paper.

ensures the data that leaves the user's device is ϵ-local differentially private. In PCMS, a local differential privacy is achieved on a client via flipping the bits of any output v of hash function applied to a data record d with a Bernoulli noise vector $b \in \{-1, +1\}^m$, whose elements are picked with a probability of $\frac{e^{\epsilon/2}}{e^{\epsilon/2}+1}$. This noised output is stored in a matrix of dimension $k \times m$ called the sketch matrix. Here, m (referred as depth) is the dimension of the output of used hash functions and k is the number of hash functions. A post-processing is applied on this table at the server to obtain the private histogram as follows. As noised vectors arrive from various clients, the server adds the privatized vector to the vector at row j of a server side version of the sketch matrix $\mathbf{M}$, where j is the index of the hash function sampled by the device. The values of $\mathbf{M}$ are then scaled appropriately so that each row helps provide an unbiased estimator for the frequency of each element. To compute an estimate for any input $d \in D$, the server-side algorithm then averages the counts corresponding to each of the k hash functions in $\mathbf{M}$ for d.

Method

In this section we propose a meta-estimator as an improvement to the private count-mean-sketch data structure in order to achieve a better trade-off between the true positive rate and false positive rates when applied to the problem of private contact tracing. In addition, we show theoretical results that our meta-estimator provides a variance reduction

in comparison to the original private count-mean-sketch data structure based estimator and we substantiate this via empirical results as well. Before we describe the technical aspects of our proposed meta-estimator, we walk through a detailed example of any user's interaction with our proposed private contact tracing system.

Example roles of querying clients, infected clients and server in the proposed system

- **Infected clients:** Infected clients upload a locally differentially private version of their trajectories of movement to a centralized server. To be precise, all clients share an indexing to a spatial grid overlaid on the map. There are efficient ways to maintain such a global grid indexing using technologies like geohashes (for square grid cells) or H3 geospatial grid indexing (for hexagonal grid cells). Every trajectory is reprsented by an indexing corresponding to a discretized version of the trajectory to several grid-cells. The set of indexes corresponding to each category are privatized using our proposed meta-estimator, and shared with the server.
- **Server:** The server applies a post-processing function to obtain a locally differentially private histogram of counts of grid-cell indices traversed by all trajectories of a client within a chosen time window. It sums up all such private histograms obtained from each of the w infected clients to obtain a single private aggregated histogram.
- **Querier clients:** Any querier client would like to check if it came into contact with an infected client upto the resolution allowed by the grid-cells. It downloads the private aggregated histogram from the server onto its device and matches it with its own trajectory data and looks for counts beyond a threshold while also accounting for its own repeat visits.

Algorithm 1 DAMS

for Infected Clients $t \in [w]$ **do**
For each $r \in [p]$,
compute g_t^r = PrivateClientCMS($D_t, \epsilon_t, \mathcal{H}_r$) on-device.
Send sketches $g_t^1, g_t^2, \dots g_t^p$ **to Server**

ServerUpdate($g_t^1, g_t^2, \dots g_t^p$)**:**
for $t \in [w]$ **do**
Estimate histograms $F_t^1 = \phi(g_t^1), \dots F_t^p = \phi(g_t^p)$
Compute average histogram $F_t^\mu = \frac{\sum_{i=1}^p F_t^i}{p}$
Compute aggregate of average histograms
$F_{agg} = F_1^\mu + F_2^\mu + \dots F_w^\mu$
Send F_{agg} **to QuerierClient**

QueryClient Check:
Matches its data with non-zero counts in F_{agg} greater than a threshold for contact tracing result (excludes self-repeats).

Meta-estimator: Diversified averaging for meta-estimation of private sketches (DAMS)

We now describe our DAMS scheme that is also illustrated in Figure 3 The steps can be summarized as follows.

- **Step 1:** Every infected client generates p private sketches of their raw data, where each version (or run) differs in terms of the dictionary of hash functions $\mathcal{H}_i$ used. Each private sketch is done using the private count-mean-sketch estimator. These p private sketches per client are sent to the server. Note that in addition, we also divide the spatio-temporal region under study into serveral large zones; where each zone has its own hash dictionary that changes from run to run. This helps filter and quantize the data record down to a zone before using its hash dictionary.
- **Step 2:** The server applies its post-processing function on each of these private sketches to generate a private histogram. These p private histograms are averaged to get a final private histogram per client. Since there are w clients, a total of w private histograms are obtained at the server. The server now adds these w histograms to obtain one aggregated private histogram.
- **Step 3:** This aggregated histogram is downloaded by any querying client that would like to check if it has come into contact (close proximity) with an onfected client. The querying client checks if any of its movement trajectories match with the non-zero counts in the aggregated histogram beyond a threshold of counts after accounting for its own repeat visits. This helps the querying client obtain the final result of contact tracing on-device.

These steps are presented in the Algorithm 1 block presented above. Although we show empirically in the experimental section that our modified scheme tremendously improves the true positive rate of contact tracing while substantially reducing the false positive rate; it goes without saying that there is no free lunch. The trade-off of this increased utility happens at a reduction in privacy, precisely to an extent that we now describe. That said, we show that the constants that influence this utility-privacy trade-off are reasonably under control, in empirical experiments. In step 2 above, if every client releases each one of the p histograms with ϵ_i- differential privacy, then due to the sequential composition property (Dwork, Roth, and others 2014) of differential privacy, each averaged histogram from every client has $p\epsilon_i$- differential privacy. Similarly, due to the parallel composition property (Dwork, Roth, and others 2014) of differential privacy, the aggregated private histogram has $max(p\epsilon_i)$-differential privacy, $\forall i \in \{1, 2, \dots, w\}$. These are illustrated in Figure 3 as well.

Variance reduction guarantees and important baselines

We now compare the variance under the following three scenarios

- **Scenario I** The scenario of using $\epsilon = p\epsilon'$ with the algorithm being run once with one set of hash functions. This is equivalent to the privacy level obtained when the same set of hash functions are used across p runs of the algorithm on the same dataset due to the sequential composition property (Dwork, Roth, and others 2014) of differential privacy. This is an important baseline to compare against in order to confirm that changing the hash function dictionary across multiple runs (# of runs = p), is a better

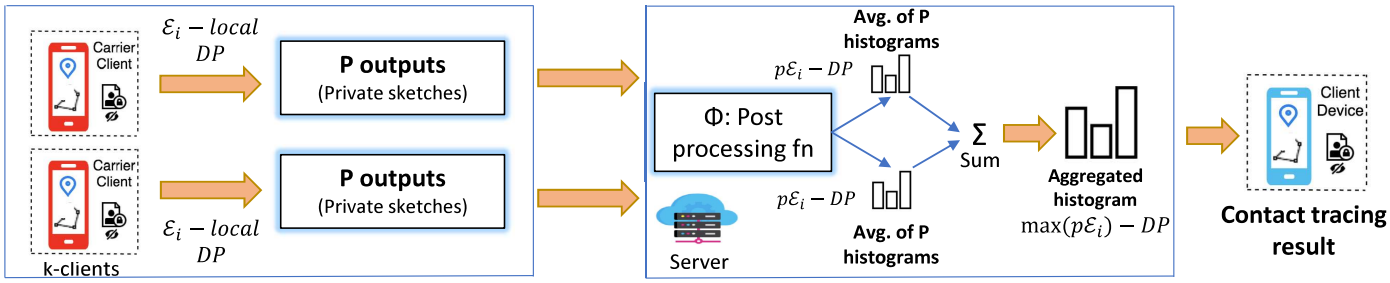

Figure 3: Illustration of our proposed meta-estimation scheme where each infected client device performs p sketches of its data using the private count-mean-sketch data structure, where each sketch is performed with a completely different dictionary of hash functions. The p intermediate result obtained from each client is said to the server, where they are post-processed to obtain p private histograms that are averaged to finally obtain one histogram per client. These are all aggregated to obtain one single histogram that is shared with the querying user for matching with its own data on-device to get the result of contact tracing.

option than performing one single run with one hash function dictionary; yet with an equivalent level of privacy. We would like to note that, even when $p = 1$, there is a difference in hash dictionaries used across different zones that the region of interest is divided into; as explained in Step 1 of our method in the previous section.

- **Scenario II** The scenario of using $\epsilon = \epsilon'$, while the algorithm is run q times using a ***same*** dictionary of hash functions in each of the run as part of the private count-mean-sketch algorithm. The final result is obtained as the average of the estimate counts. This is an important baseline to compare against in order to confirm that changing the hash function dictionary across each of the p runs, is a better option than keeping them same across the p runs.
- **Scenario III** The scenario of using $\epsilon = \epsilon'$, while the algorithm is run q times using a ***different*** dictionary of hash functions in each of the run as part of the private count-mean-sketch algorithm. The final result is obtained as the average of the estimated counts. We refer to this option as our proposed private DAMS estimator.

Theorem 1. *Private DAMS estimator in scenario III has a lower variance than the estimator in scenario I when $\epsilon > 2$.*

Proof. $\tilde{f}(d)$ is the estimated frequency of data element d and its variance in the standard differentially private count-mean-sketch scheme is given by (Team 2017).

$$\text{Var}\,[\tilde{f}(d)] = n(c_\epsilon^2 - 1)/4 + \frac{n - f(d)}{m}\left(1 - \frac{1}{m} - \frac{1}{k} + \frac{1}{km}\right) + \left(\frac{1}{km} - \frac{1}{km^2}\right)\left(\sum_{d^* \neq d} f(d^*)^2\right) \tag{1}$$

Here $f(d^*) \in D$ is the original frequency of the element d^* and D is the dataset, n is the number of data points, k is the depth of the CMS-data structure, m is the width and $c_\epsilon = \frac{e^{\epsilon/2}+1}{e^{\epsilon/2}-1}$.

We now show the variance of the count estimator obtained in each of the above estimators. In scenario I, we have the following expression for the vaiance upto a constant C that is independent of ϵ.

$$\text{Var}\,[\tilde{f}(d)] = n(c_{p\epsilon'}^2 - 1)/4 + \frac{n - f(d)}{m}\left(1 - \frac{1}{m} - \frac{1}{k} + \frac{1}{km}\right) + \left(\frac{1}{km} - \frac{1}{km^2}\right)\left(\sum_{d^* \neq d} f(d^*)^2\right) = n(c_{p\epsilon'}^2 - 1)/4 + C \tag{2}$$

In scenario III, now since all the hash functions across the p runs are three-wise independent, we have $\text{Var}\,\tilde{f}(d) = \frac{\text{Var}\,[\tilde{f}_1(d)] + \text{Var}\,[\tilde{f}_2(d)] + \ldots + \text{Var}\,[\tilde{f}_p(d)]}{p^2}$ where $\text{Var}\,\tilde{f}_i(d)$ is the variance of an individual run. But since we use the same k, n, m across runs although the hash function dictionaries are the same, we have $\text{Var}\,\tilde{f}(d) = n(c_{\epsilon'}^2 - 1)/4 + C$ Note that there is a reduction from $1/p^2$ to $1/p$ due to equality of variances. To complete the proof, we would need to show that, $\frac{1}{p}\left[n(c_{p\epsilon'}^2 - 1)/4 + C\right] \leq n(c_{p\epsilon'}^2 - 1)/4 + C$. Substituting $c_\epsilon = \frac{e^{\epsilon/2}+1}{e^{\epsilon/2}-1} = 1 + \frac{2}{e^{\epsilon/2}-1}$, we would need to show that

$$\frac{1}{p}\left[\frac{n}{4}\left[1 + \frac{2}{e^{\epsilon/2} - 1}\right]^2 + C\right] \leq \frac{n}{4}\left[1 + \frac{2}{e^{p\epsilon/2} - 1}\right]^2 + C.$$

For $\epsilon' > 2$, we have c_ϵ is approximately ≤ 4 and therefore $\frac{1}{p}\left[\frac{n}{4}\left[1 + \frac{2}{e^{\epsilon/2}-1}\right]^2 + C\right] \leq \frac{1}{p}[4n + C]$. Upon substituting the same into the r.h.s of the inequality we get $\frac{1}{p}[4n + C] \leq \frac{n}{4} + C$ that can be trivially satisfied by choosing values of p that satisfy this inequality. □

Lemma 1. *Private DAMS estimator is unbiased.*

Proof. $\mathbb{E}\,\tilde{f}(d) = \frac{\mathbb{E}[\tilde{f}_1(d)] + \mathbb{E}[\tilde{f}_2(d)] + \ldots + \mathbb{E}[\tilde{f}_p(d)]}{p}$ where $\mathbb{E}\,\tilde{f}_i(d)$ is the expectation of an individual run. Each of the individual estimators in the numerator is unbiased as the differentially private count-mean-sketch estimator that was used is unbiased (Team 2017). Therefore the private DAMS estimator is unbiased. □

Theorem 2. *The variance of the estimator of private DAMS in scenario III is less than the variance of the estimator in scenario II.*

Proof. In scenario II, without loss of generality, when $p = 2$ we have $\text{Var}\,\tilde{f}(d) = \frac{\sum_i \text{Var}\,[\tilde{f}_i(d)]}{p^2} + 2\sum_{ij} \text{Cov}(\tilde{f}_i(d), \tilde{f}_j(d))$ where $\text{Var}\,\tilde{f}_i(d)$ is the variance of an individual run and $\text{Cov}(\tilde{f}_i(d), \tilde{f}_j(d))$ is the covariance. Since, we use 3-wise independent hash functions (Team 2017) as suggested in the standard differentially private count-mean-sketch estimator in (Team 2017), the covariance when $i \neq j$ is $\frac{1}{m} - \frac{1}{m^2}$ while it is 0, when $i = j$. Now, $\frac{1}{m} - \frac{1}{m^2}$ is always positive for non-zero integer values of m. Therefore all the covariances show positive correlation in this case and the sum of covariances is of the order

$$q(\frac{1}{m} - \frac{1}{m^2})(2p - 1)$$

. Therefore, the variance of scenario III is always lesser than scenario II. Without loss of generality, this holds when $p > 2$ as well. □

Experiments

Microsoft GeoLife GPS Trajectory Dataset

This GPS trajectory dataset (Zheng et al. 2008; 2010; 2009) is a massive dataset that was collected in (Microsoft Research Asia) Geolife project by 178 users in a period of over four years (from April 2007 to October 2011). A GPS trajectory of this dataset is represented by a sequence of time-stamped points, each of which contains the information of latitude, longitude and altitude. This dataset contains 17621 trajectories with a total distance of 1,251,654 kilometers and a total duration of 48,203 hours. A subset of this dataset was used for a detailed evaluation with 50 trajectories labeled as infected patient trajectories and one was labeled as a querier trajectory. Each trajectory was of length 720. Therefore $51 \times 720 = 36720$ datapoints were used to be processed through our private DAMS data structure.

GoTrack GPS trajectories dataset

This dataset is available on the UCI repository and we use a formatted subset of the dataset where querier trajectories intersect with some infected patient trajectories in 336 co-ordinates among 1123 co-ordinates and unlike the above experiment, the trajectory length of each participant is not the same in this dataset.

Empirical evaluation

Private DAMS Vs. PCMS: We compare our approach of private DAMS with $p = 1$, where each zone has a different hash dictionary Vs. with the standard private count-mean-sketch (PCMS-1 as in scenario I) with $p = 1$ as shown in Figures 4 and 7. In PCMS, each zone has the same dictionary. The comparison is in terms of the important metrics of true positive rates (TPR), false positive rates (FPR), F1 score and MCC score of contact tracing received at querier client, with respect to the ground truth of intersections. Note that the x-axis refers to the different values of ϵ considered between 2.5 to 7, with increasing values of 0.5. That said, it is important to note that all the $\epsilon's$ reported on the x-axis are the corresponding values obtained after accounting for the sequential and parallel composition laws of differential privacy in our scheme as described in Figure 3.

Effectiveness of $p > 1$ in DAMS: We also compare our approach private DAMS with $p = 5$ (DAMS-5) and $p = 10$ (DAMS-10) against scenario - II for $p = 5$ (CMS-5) and $p = 10$ (CMS-10) runs. These results are shown in Figures 5,6,8 and 9. We observe a greater TPR in each of the DAMS results in comparison to the CMS results as desired. Similarly we observe a lower FPR in each of the DAMS results in comparison to the CMS results as desired.

Variance reduction with DAMS: In addition, we observe that the variance across the obtained FPR's are significantly lower in the DAMS results in comparison to the CMS results although the change in variances in case of the TPR's is not as significant. We note that the denominator in computing the FPR's is way larger than that of the denominator in computing TPR over this dataset. Therefore the overall variance reduction is significant. In Figure 10, we compare the effect of increasing p over our proposed DAMS scheme. We note that the TPR increases wuth increasing p, although the increase begins to flatten out with larger p's. That said with increasing p, the FPR's mildly increase in the DAMS scheme as shown in Figure 13. Note that regardless of this effect, the TPR's and FPR's of DAMS outperforms CMS for all three p's that were tried, as in for $p = 1, p = 5$ and $p = 10$.

Data imbalance As the datasets are highly imbalanced (and so is the usecase of contact tracing), in terms of having a much smaller number of intersections as against the number of non-intersections between the trajectories of querier clients and infected clients, we therefore also compare the different versions of DAMS and CMS in terms of F1 scores and MCC scores, that are better suited for such settings. These results are presented in Figures 11, 12, 14 and 15.

Future research

As part of suggested future work, we give credence to the non i.i.d (non independent and identically distributed) nature of the problem in contact tracing as our proposed solution could be further improved using differential privacy primitives that are well-suited for dependent/correlated data. These notions of modified differential privacy for non i.i.d data (Chatzikokolakis, Palamidessi, and Stronati 2015; Liu, Chakraborty, and Mittal 2016; Andrés et al. 2013) are currently at an early stage of the research horizon. We believe that first investigating the digital private contact tracing problem through the lens of differental privacy under the relatively simpler assumption of i.i.d data is beneficial to carry forward the learnings obtained into the more stringent settings of non i.i.d data as shown in the Table 1 in red. Other location based COVID-19 privacy projects such as (Research 2020) by Facebook, also assume i.i.d'ness to support solutions with simplistic assumptions at first.

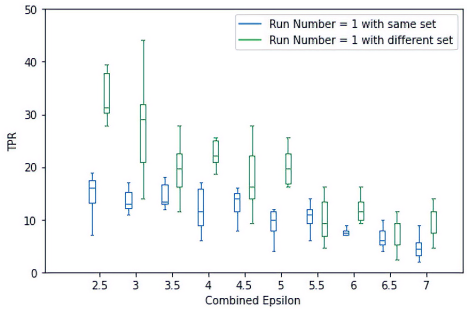

Figure 4: GeoLife GPS: TPR of DAMS Vs. PCMS for $p = 1$

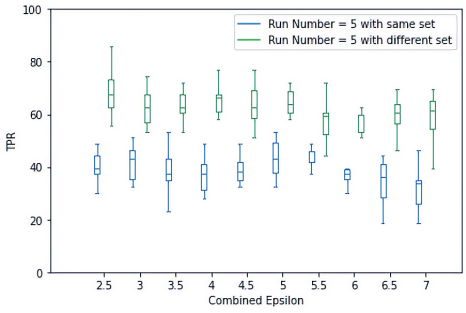

Figure 5: GeoLife GPS: TPR of DAMS Vs. PCMS for $p = 5$

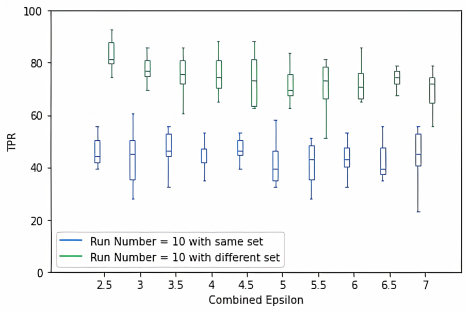

Figure 6: GeoLife GPS: TPR of DAMS Vs. PCMS for $p = 10$

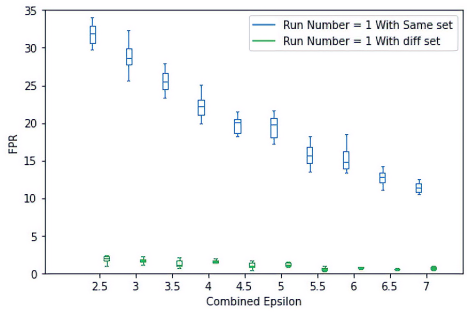

Figure 7: GeoTrack GPS: FPR of DAMS Vs. PCMS for $p = 1$

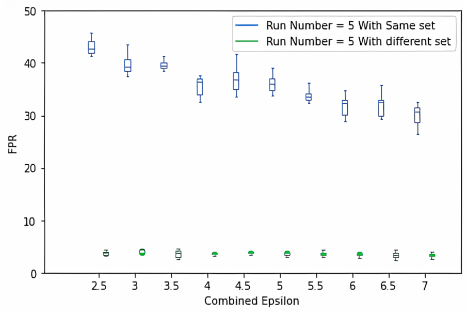

Figure 8: GeoTrack GPS: FPR of DAMS Vs. PCMS for $p = 5$

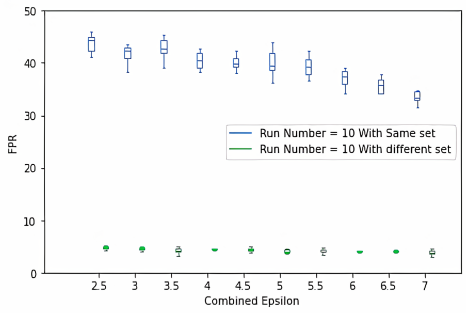

Figure 9: GeoTrack GPS: FPR of DAMS Vs. PCMS for $p = 10$

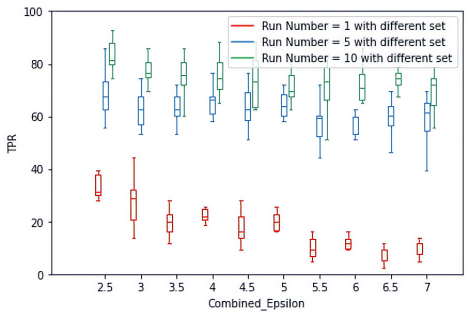

Figure 10: GeoLife GPS: TPR trend in DAMS for $p = 1, 5$ and 10

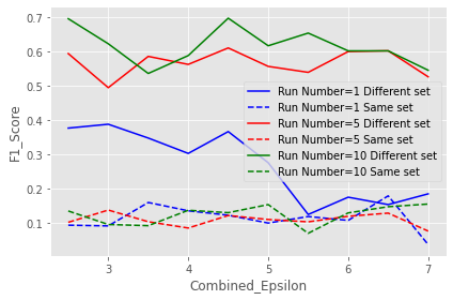

Figure 11: GeoLife GPS: F1 score across DAMS and PCMS for $p = 1, 5$ and 10

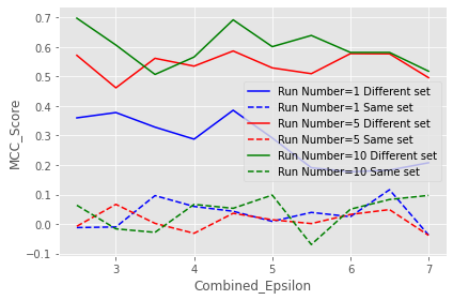

Figure 12: GeoLife GPS: MCC score across DAMS and PCMS for $p = 1, 5$ and 10

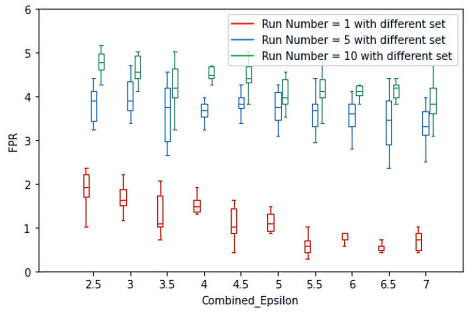

Figure 13: GeoTrack GPS: FPR trend in DAMS for $p = 1, 5$ and 10

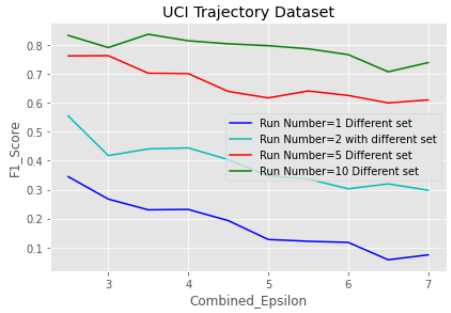

Figure 14: GeoTrack GPS: F1 score across DAMS and PCMS for $p = 1, 5$ and 10

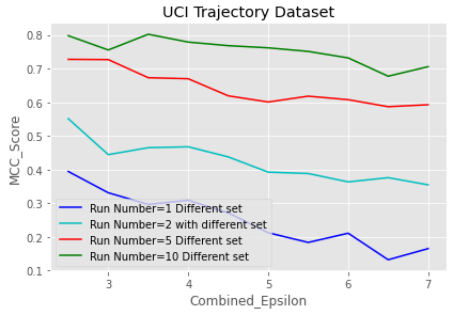

Figure 15: GeoTrack GPS: MCC score across DAMS and PCMS for $p = 1, 5$ and 10

References

Abowd, J.; Ashmead, R.; Simson, G.; Kifer, D.; Leclerc, P.; Machanavajjhala, A.; and Sexton, W. 2019. Census top-down: Differentially private data, incremental schemas, and consistency with public knowledge. Technical report, Technical Report. US Census Bureau.

Abowd, J. M. 2018. The us census bureau adopts differential privacy. In *Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*, 2867–2867.

Ahmed, N.; Michelin, R. A.; Xue, W.; Ruj, S.; Malaney, R.; Kanhere, S. S.; Seneviratne, A.; Hu, W.; Janicke, H.; and Jha, S. K. 2020. A survey of covid-19 contact tracing apps. *IEEE Access* 8:134577–134601.

Alon, N.; Matias, Y.; and Szegedy, M. 1999. The space complexity of approximating the frequency moments. *Journal of Computer and system sciences* 58(1):137–147.

Altuwaiyan, T.; Hadian, M.; and Liang, X. 2018. Epic: efficient privacy-preserving contact tracing for infection detection. In *2018 IEEE International Conference on Communications (ICC)*, 1–6. IEEE.

Andoni, A.; Do Ba, K.; Indyk, P.; and Woodruff, D. 2009. Efficient sketches for earth-mover distance, with applications. In *2009 50th Annual IEEE Symposium on Foundations of Computer Science*, 324–330. IEEE.

Andrés, M. E.; Bordenabe, N. E.; Chatzikokolakis, K.; and Palamidessi, C. 2013. Geo-indistinguishability: Differential privacy for location-based systems. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, 901–914.

Austin, L. M. 2005. Is consent the foundation of fair information practices? canadas experience under pipeda. *SSRN Electronic Journal*.

Berke, A.; Bakker, M.; Vepakomma, P.; Raskar, R.; Larson, K.; and Pentland, A. 2020. Assessing disease exposure risk with location histories and protecting privacy: A cryptographic approach in response to a global pandemic. *arXiv preprint arXiv:2003.14412*.

Beskorovajnov, W.; Dörre, F.; Hartung, G.; Koch, A.; Müller-Quade, J.; and Strufe, T. 2020. Contra corona: Contact tracing against the coronavirus by bridging the centralized-decentralized divide for stronger privacy. *IACR Cryptol. ePrint Arch.* 2020:505.

Braverman, V., and Ostrovsky, R. 2013. Generalizing the layering method of indyk and woodruff: Recursive sketches for frequency-based vectors on streams. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*. Springer. 58–70.

Broder, A., and Mitzenmacher, M. 2004. Network applications of bloom filters: A survey. *Internet mathematics* 1(4):485–509.

Broder, A. Z. 2000. Identifying and filtering near-duplicate documents. In *Annual Symposium on Combinatorial Pattern Matching*, 1–10. Springer.

Chan, J.; Gollakota, S.; Horvitz, E.; Jaeger, J.; Kakade, S.; Kohno, T.; Langford, J.; Larson, J.; Singanamalla, S.; Sunshine, J.; et al. 2020. Pact: Privacy sensitive protocols and mechanisms for mobile contact tracing. *arXiv preprint arXiv:2004.03544*.

Chanyaswad, T.; Liu, C.; and Mittal, P. 2019. Rongauss: Enhancing utility in non-interactive private data release. *Proceedings on Privacy Enhancing Technologies* 2019(1):26–46.

Chatzikokolakis, K.; Palamidessi, C.; and Stronati, M. 2015. Location privacy via geo-indistinguishability. *ACM SIGLOG News* 2(3):46–69.

Chen, B.-R., and Hu, Y.-C. 2020. Blindsignedid: Mitigate denial-of-service attacks on digital contact tracing. *arXiv preprint arXiv:2008.09351*.

Cho, H.; Ippolito, D.; and Yu, Y. W. 2020. Contact tracing mobile apps for covid-19: Privacy considerations and related trade-offs. *arXiv preprint arXiv:2003.11511*.

Chowdhury, A. R.; Wang, C.; He, X.; Machanavajjhala, A.; and Jha, S. 2019. Cryptepsilon: Crypto-assisted differential privacy on untrusted servers. *arXiv preprint arXiv:1902.07756*.

Cormode, G., and Garofalakis, M. 2007. Sketching probabilistic data streams. In *Proceedings of the 2007 ACM SIGMOD international conference on Management of data*, 281–292.

Cormode, G., and Muthukrishnan, S. 2005. An improved data stream summary: the count-min sketch and its applications. *Journal of Algorithms* 55(1):58–75.

Cormode, G.; Jha, S.; Kulkarni, T.; Li, N.; Srivastava, D.; and Wang, T. 2018. Privacy at scale: Local differential privacy in practice. In *Proceedings of the 2018 International Conference on Management of Data*, 1655–1658.

Cormode, G.; Kulkarni, T.; and Srivastava, D. 2018. Marginal release under local differential privacy. In *Proceedings of the 2018 International Conference on Management of Data*, 131–146.

Dwork, C., and Smith, A. 2010. Differential privacy for statistics: What we know and what we want to learn. *Journal of Privacy and Confidentiality* 1(2).

Dwork, C.; Roth, A.; et al. 2014. The algorithmic foundations of differential privacy. *Foundations and Trends in Theoretical Computer Science* 9(3-4):211–407.

Dwork, C. 2008. Differential privacy: A survey of results. In *International conference on theory and applications of models of computation*, 1–19. Springer.

Erlingsson, Ú.; Pihur, V.; and Korolova, A. 2014. Rappor: Randomized aggregatable privacy-preserving ordinal response. In *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security*, 1054–1067.

Fitzsimons, J. K.; Mantri, A.; Pisarczyk, R.; Rainforth, T.; and Zhao, Z. 2020. A note on blind contact tracing at scale with applications to the covid-19 pandemic. *arXiv preprint arXiv:2004.05116*.

Goddard, M. 2017. The eu general data protection regulation (gdpr): European regulation that has a global impact. *International Journal of Market Research* 59(6):703–705.

Greiner, A. L.; Angelo, K. M.; McCollum, A. M.; Mirkovic, K.; Arthur, R.; and Angulo, F. J. 2015. Addressing contact tracing challenges—critical to halting ebola virus disease transmission. *International Journal of Infectious Diseases* 41:53–55.

Groce, A.; Rindal, P.; and Rosulek, M. 2019. Cheaper private set intersection via differentially private leakage. *Proceedings on Privacy Enhancing Technologies* 2019(3):6–25.

Hatke, G. F.; Montanari, M.; Appadwedula, S.; Wentz, M.; Meklenburg, J.; Ivers, L.; Watson, J.; and Fiore, P. 2020. Using bluetooth low energy (ble) signal strength estimation to facilitate contact tracing for covid-19. *arXiv preprint arXiv:2006.15711*.

Indyk, P. 2007. Sketching, streaming and sublinear-space algorithms. *Graduate course notes, available at* 33:617.

Ioffe, S. 2010. Improved consistent sampling, weighted minhash and l1 sketching. In *2010 IEEE International Conference on Data Mining*, 246–255. IEEE.

Joseph, M.; Mao, J.; Neel, S.; and Roth, A. 2019. The role of interactivity in local differential privacy. In *2019 IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS)*, 94–105. IEEE.

Kairouz, P.; Oh, S.; and Viswanath, P. 2014. Extremal mechanisms for local differential privacy. In *Advances in neural information processing systems*, 2879–2887.

Liu, X.; Trieu, N.; Kornaropoulos, E. M.; and Song, D. 2020. Beetrace: A unified platform for secure contact tracing that breaks data silos. *arXiv preprint arXiv:2007.02285*.

Liu, C.; Chakraborty, S.; and Mittal, P. 2016. Dependence makes you vulnberable: Differential privacy under dependent tuples. In *NDSS*, volume 16, 21–24.

Martin, T.; Karopoulos, G.; Hernández-Ramos, J. L.; Kambourakis, G.; and Fovino, I. N. 2020. Demystifying covid-19 digital contact tracing: A survey on frameworks and mobile apps. *arXiv preprint arXiv:2007.11687*.

McSherry, F., and Talwar, K. 2007. Mechanism design via differential privacy. In *48th Annual IEEE Symposium on Foundations of Computer Science (FOCS'07)*, 94–103. IEEE.

Mercuri, R. T. 2004. The hipaa-potamus in health care data security. *Communications of the ACM* 47(7):25–28.

Pilanci, M., and Wainwright, M. J. 2015. Randomized sketches of convex programs with sharp guarantees. *IEEE Transactions on Information Theory* 61(9):5096–5115.

Raskar, R.; Schunemann, I.; Barbar, R.; Vilcans, K.; Gray, J.; Vepakomma, P.; Kapa, S.; Nuzzo, A.; Gupta, R.; Berke, A.; et al. 2020. Apps gone rogue: Maintaining personal privacy in an epidemic. *arXiv preprint arXiv:2003.08567*.

Reichert, L.; Brack, S.; and Scheuermann, B. 2020. A survey of automatic contact tracing approaches. *Cryptol. ePrint Arch., IACR, Bellevue, WA, USA, Tech. Rep* 672:2020.

Research, F. 2020. Protecting privacy in facebook mobility data during the covid-19 response. In *Blog*.

Rivest, R. L.; Weitzner, D.; Ivers, L.; Soibelman, I.; and Zissman, M. 2020. Pact: Private automated contact tracing.

Shrivastava, A., and Li, P. 2014. In defense of minhash over simhash. In *Artificial Intelligence and Statistics*, 886–894.

Singh, P.; Singh, A.; Cojocaru, G.; Vepakomma, P.; and Raskar, R. 2020. Ppcontacttracing: A privacy-preserving contact tracing protocol for covid-19 pandemic. *arXiv preprint arXiv:2008.06648*.

Smith, A.; Thakurta, A.; and Upadhyay, J. 2017. Is interaction necessary for distributed private learning? In *2017 IEEE Symposium on Security and Privacy (SP)*, 58–77. IEEE.

Tang, Q. 2020. Privacy-preserving contact tracing: current solutions and open questions. *arXiv preprint arXiv:2004.06818*.

Team, D. P. 2017. Learning with privacy at scale. In *https://machinelearning.apple.com/*.

Trieu, N.; Shehata, K.; Saxena, P.; Shokri, R.; and Song, D. 2020. Epione: Lightweight contact tracing with strong privacy. *arXiv preprint arXiv:2004.13293*.

Wagh, S.; He, X.; Machanavajjhala, A.; and Mittal, P. 2020. Dp-cryptography: Marrying differential privacy and cryptography in emerging applications. *arXiv preprint arXiv:2004.08887*.

Zheng, Y.; Li, Q.; Chen, Y.; Xie, X.; and Ma, W.-Y. 2008. Understanding mobility based on gps data. In *Proceedings of the 10th international conference on Ubiquitous computing*, 312–321.

Zheng, Y.; Zhang, L.; Xie, X.; and Ma, W.-Y. 2009. Mining interesting locations and travel sequences from gps trajectories. In *Proceedings of the 18th international conference on World wide web*, 791–800.

Zheng, Y.; Xie, X.; Ma, W.-Y.; et al. 2010. Geolife: A collaborative social networking service among user, location and trajectory. *IEEE Data Eng. Bull.* 33(2):32–39.