RANDOMIZED REQUANTIZATION WITH LOCAL DIFFERENTIAL PRIVACY

Sijie Xiong, Anand D. Sarwate, Narayan B. Mandayam

Rutgers, The State University of New Jersey

ABSTRACT

In this paper we study how individual sensors can compress their observations in a privacy-preserving manner. We propose a randomized requantization scheme that guarantees local differential privacy, a strong model for privacy in which individual data holders must mask their information before sending it to an untrusted third party. For our approach, the problem becomes an optimization over discrete memoryless channels between the sensor observations and their compressed version. We show that for a fixed compression ratio, finding privacy-optimal channel subject to a distortion constraint is a quasiconvex optimization problem that can be solved by the bisection method. Our results indicate interesting tradeoffs between the privacy risk, compression ratio, and utility, or distortion. For example, in the low distortion regime, we can halve the bit rate at little cost in distortion while maintaining the same privacy level. We illustrate our approach for a simple example of privatizing and recompressing lowpass signals and show that it yields better tradeoffs than existing approaches based on noise addition. Our approach may be useful in several privacy-sensitive monitoring applications envisioned for the Internet of Things (IoT).

***Index Terms*—** Local differential privacy, randomized requantization, quasiconvex optimization, IoT.

1. INTRODUCTION

The advent of large-scale data mining and Internet of Things (IoT) has highlighted the benefits and drawbacks of ubiquitous monitoring. For example, continuous data collection has been proposed for healthcare, transportation, energy management, environmental sensing, and industrial control in order to understand complex events such as disease outbreaks or traffic congestion, or creating more energy-efficient environmental control systems. Monitoring comes at a cost to privacy: users' contributed data may be shared in unexpected ways, causing privacy violations. From an engineering perspective, sensors must often be cheap and each sensor node may be resource constrained in terms of processing speed, memory and communication bandwidth. The goal of this work is to investigate tradeoffs between privacy, bandwidth, and fidelity in a monitoring model for future IoT systems.

In order to understand these tradeoffs, we adopt the differential privacy framework [1, 2] for quantifying privacy risk. Much of the existing work on differential privacy focuses on designing algorithms that trade off privacy and utility (usually accuracy) incurred by a trusted aggregator publishing functions of private data, such as summary statistics. This tradeoff appears because privacy is guaranteed by randomizing the output of the algorithm: the uncertainty caused by a "noisy" output guarantees privacy. However, in an IoT scenario, monitoring data has to be shared continuously (e.g. as time series) and the sensor may not trust the data aggregator. Rastogi and Nath [3] proposed an algorithm for sharing time series which applies Laplace perturbation algorithm (LPA) [4] to the first few Discrete Fourier Transform (DFT) coefficients of a data sequence; Fan and Xiong [5] used filtering and adaptive sampling techniques to privatize a single time series. In these approaches the goal is to compute an aggregate across the series, so the noise can decrease with the number of individuals [4]. Other approaches include making "events" private (rather than the data) [6, 7]. Zhou et al. [8] studied the problem of dimensionality reduction via a private linear transformation. In this paper we use the local privacy model [9]: each sensor shares a locally privatized version of their observation. Our goal is to understand how privacy-accuracy tradeoffs are affected by storage/bandwidth considerations.

In our system model, each sensor (or user) holds a sequence of real-valued data (e.g. time series) which needs to be privatized and compressed at the user level while maintaining a certain fidelity. We propose a novel privacy-preserving compression scheme – *randomized requantization*, and study the fundamental tradeoffs between privacy, compression and utility. We show that minimizing privacy risk under a distortion constraint at a fixed bitrate is a constrained quasiconvex optimization problem. We also show that in the context of Rastogi and Nath's problem [3], we can achieve a better distortion and network scalability by perturbing and quantizing in the transform domain.

2. PROBLEM SETTING

We consider a model in which each sensor observes a length-n sequence of data $X^n = (X_1, X_2, \cdots, X_n)$ and wishes to

S. Xiong and A.D. Sarwate are supported by NSF award CCF-1453432. N. Mandayam is supported in part by NSF award CNS-1423020.

share a private version $\hat{X}^n$ to a central aggregator. We assume that the sequence is already quantized to some discrete set of levels $\mathcal{X}$, so $X_i \in \mathcal{X}$. We are interested in *locally differentially private requantization* [9]: we would like to find a randomized mapping $Q : \mathcal{X} \to \hat{\mathcal{X}}$ where $\hat{\mathcal{X}} \subset \mathbb{R}$ is an output discrete set of points and $|\hat{\mathcal{X}}| \leq |\mathcal{X}|$. This requantization mapping can be thought of as a channel $Q(\hat{x}|x)$ (conditional probability distribution). Our goal is to pass X^n through this channel Q to release a privatized and compressed version $\hat{X}^n$. A channel Q is ε-locally differentially private[9, 10] if

$$\max_{(x,\tilde{x},\hat{x})\in\mathcal{X}\times\mathcal{X}\times\hat{\mathcal{X}}} \left\{ \frac{Q(\hat{x}|x)}{Q(\hat{x}|\tilde{x})} \right\} \leq e^{\varepsilon}. \tag{1}$$

Local differential privacy implies that the distribution of the output $\hat{x}$ reveals limited information about the input symbol x: for any other input $\tilde{x}$, the output under $\tilde{x}$ has a similar distribution to that under x. Small ε means greater indistinguishability and hence less privacy risk; it characterizes the false-alarm/missed-detection tradeoff for the hypothesis test in guessing x from $\hat{x}$ [11, 12].

As a concrete example to compare with Rastogi and Nath [3], consider the problem of compressing a lowpass signal. As noted by Papadimitriou et al. [13], compressing time series data requires that the signal class have a lower complexity: examples include signals which are sparse in some appropriately defined transform domain. Structured signal classes allow for less privacy-preserving noise and hence a huge utility improvement [3]. According to the *composition theorem* [14], if we guarantee ε-differential privacy in the Fourier domain, the resulting time series after inverse discrete Fourier transform (IDFT) will still be an ε-differentially private version of the original time series. Although we focus on privacy-preserving quantization of Fourier coefficients here, our model extends to other low-complexity signal classes.

For a given privacy level ε, define the set of channels which provides ε-local differential privacy by $\mathcal{Q}_{\text{LDP}}(\varepsilon) = \{Q(\hat{x}|x) : (1) \text{ holds}\}$. If the alphabet $\hat{\mathcal{X}}$ for each $\hat{X}_i$ is smaller than $\mathcal{X}$, then we can think of channel Q as both a privatization mechanism and a compression mechanism. That is, suppose each X_i is represented using R bits ($|\mathcal{X}| = 2^R$), and the corresponding $\hat{X}_i$ uses only $\hat{R}$ bits ($\hat{R} \leq R$, $|\hat{\mathcal{X}}| = 2^{\hat{R}}$), then we can define compression ratio ρ as

$$\rho = \frac{\hat{R}}{R} = \frac{\log_2|\hat{\mathcal{X}}|}{\log_2|\mathcal{X}|}. \tag{2}$$

Note that for a channel Q with predetermined size $|\mathcal{X}| \times |\hat{\mathcal{X}}|$, the compression ratio is also fixed.

A natural question is how to choose a particular $Q \in \mathcal{Q}_{\text{LDP}}(\varepsilon)$ to use. Due to utility requirement, we select a Q that yields a small distortion between input and output sequences with respect to a given distortion measure. Given a distortion function $d : \mathcal{X} \times \hat{\mathcal{X}} \to \mathbb{R}^+$ defined on a symbol-by-symbol basis, the distortion between two sequences X^n and $\hat{X}^n$ is the average of the per symbol distortions,

$$d(X^n, \hat{X}^n) = \frac{1}{n}\sum_{i=1}^{n} d(X_i, \hat{X}_i). \tag{3}$$

In order to minimize this average distortion, note that if X^n is drawn i.i.d. from a distribution P, the expected distortion $(X_i, \hat{X}_i) \sim P \times Q$ is

$$\mathbb{E}_{P\times Q}[d(X^n, \hat{X}^n)] = \mathbb{E}_{P\times Q}[d(X, \hat{X})] \tag{4}$$

$$= \sum_{x_i,\hat{x}_i} P(x_i)Q(\hat{x}_i|x_i)d(x_i, \hat{x}_i). \tag{5}$$

To generalize this model, suppose X_i's are drawn i.i.d. from P which is unknown but known to be in the set of distributions $\mathcal{P}$. Then the set of channels which yield expected distortion no greater than a target δ is defined by

$$\mathcal{Q}_{\text{U}}(\delta) = \left\{ Q(\hat{x}|x) : \max_{P\in\mathcal{P}} \mathbb{E}_{P\times Q}[d(X, \hat{X})] \leq \delta \right\}. \tag{6}$$

Given $\mathcal{P}$, compression ratio ρ and distortion constraint δ, the optimal value of ε can be defined as

$$\varepsilon^*(\mathcal{P}, \rho, \delta) = \min\left\{\varepsilon : \mathcal{Q}_{\text{LDP}}(\varepsilon) \cap \mathcal{Q}_{\text{U}}(\delta) \neq \emptyset\right\}. \tag{7}$$

In the next section, we will show that finding the channel Q which yields the optimal value $\varepsilon^*(\mathcal{P}, \rho, \delta)$ can be formulated as a quasiconvex optimization problem, and can be solved using bisection method [15].

3. PRIVACY-COMPRESSION-UTILITY TRADEOFF

For a given compression ratio ρ and a distortion constraint δ, the optimal privacy level ε^* over $\mathcal{P}$ can be obtained according to equation (7). By varying the pair (ρ, δ), we will arrive at a privacy-compression-utility (ε-ρ-δ) tradeoff, which is of great importance since it can serve as a basis for practical design of privatization and compression mechanisms. However, two main challenges arise here: (i) how to find the optimal output alphabet $\hat{\mathcal{X}}$ without privacy violation and (ii) how to learn the optimal channel Q that achieves $\varepsilon^*(\mathcal{P}, \rho, \delta)$.

In general, (i) is challenging because the optimal set of reconstruction points depends on the private input data, which could violate the privacy requirement. For the purposes of this paper we assume that there is an auxiliary public data set from the same distribution which can be used to learn the quantization points using standard approaches (such as the Lloyd-Max algorithm [16, 17]). We defer a detailed investigation of (i) to the full version of this work.

Given a target output alphabet $\hat{\mathcal{X}}$, now the problem (ii) is how to find the optimal $(|\mathcal{X}| \times |\hat{\mathcal{X}}|)$-dimensional channel matrix Q that achieves $\varepsilon^*(\mathcal{P}, \rho, \delta)$. According to (7), this is

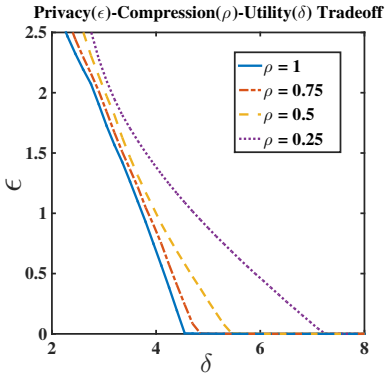


Fig. 1: Privacy-Compression-Utility Tradeoff

the same as minimizing ε over the set of channels $\mathcal{Q}_{\text{LDP}}(\varepsilon) \cap \mathcal{Q}_{\text{U}}(\delta)$. Consider instead the following program:

$$\underset{Q}{\text{minimize}} \quad \exp\left(\max_{(x,\tilde{x},\hat{x})\in\mathcal{X}\times\mathcal{X}\times\hat{\mathcal{X}}} \left\{\frac{Q(\hat{x}|x)}{Q(\hat{x}|\tilde{x})}\right\}\right) \tag{8}$$

$$\text{subject to} \quad \max_{P\in\mathcal{P}} \mathbb{E}_{P\times Q}[d(X,\hat{X})] \le \delta, \tag{9}$$

$$0 \preceq Q \preceq 1, \tag{10}$$

$$Q\cdot\hat{\mathbf{1}} = \mathbf{1}. \tag{11}$$

where $\hat{\mathbf{1}}$ and $\mathbf{1}$ are both all-ones column vectors with length-$|\hat{\mathcal{X}}|$ and $|\mathcal{X}|$ respectively. The objective function is simply minimizing e^{ε}, the worst-case ratio of pairs of conditionals.

Our main analytical result is to show that the program above is quasiconvex.

Theorem 1. *The program in* (8)-(11) *is a constrained quasi-convex optimization problem.*

Proof. We first show that the constraints (9)-(11) on the channel Q form a convex feasible set. Note that (10) and (11) suggest the channel matrix Q to be right stochastic, which can be easily shown to be a convex set since any convex combination between two right stochastic matrices is still right stochastic, i.e. for any Q_1, Q_2 satisfying (10) and (11), $(\theta Q_1 + (1-\theta)Q_2)\cdot\hat{\mathbf{1}} = \theta Q_1\cdot\hat{\mathbf{1}} + (1-\theta)Q_2\cdot\hat{\mathbf{1}} = \mathbf{1}, \forall\theta\in[0,1]$. Also, based on (5), constraint (9) can be expressed as

$$\max_{P\in\mathcal{P}} \sum_{(x_i,\hat{x}_i)\in\mathcal{X}\times\hat{\mathcal{X}}} P(x_i)Q(\hat{x}_i|x_i)d(x_i,\hat{x}_i) \le \delta. \tag{12}$$

Equivalently we can write this as

$$\sum_{(x_i,\hat{x}_i)\in\mathcal{X}\times\hat{\mathcal{X}}} P(x_i)Q(\hat{x}_i|x_i)d(x_i,\hat{x}_i) \le \delta, \quad \forall P\in\mathcal{P}, \tag{13}$$

the intersection of a set of halfspaces in $[0,1]^{|\mathcal{X}|\times|\hat{\mathcal{X}}|}$. Therefore, the feasible set of Q is convex.

We next show that the objective function in (8) is quasi-convex. Given $\mathcal{Q}_{\text{LDP}}(\varepsilon)$, we can minimize e^{ε} by minimizing the left-hand side of (1) over $Q\in\mathcal{Q}_{\text{LDP}}(\varepsilon)$. This is convex as a function of $Q(\hat{x}|x)/Q(\hat{x}|\tilde{x})$, since point-wise maximum preserves convexity [15]. However, this doesn't lead to convexity in terms of Q. A single Q actually yields $|\mathcal{X}|\times|\mathcal{X}|\times|\hat{\mathcal{X}}|$ individual ratios $Q(\hat{x}|x)/Q(\hat{x}|\tilde{x})$. If we think of this as a mapping from Q to a higher-dimensional array $\hat{Q}$:

$$\hat{Q}(i,j,s) = \frac{Q(i,s)}{Q(j,s)} = \frac{I(i,:)\cdot Q\cdot\hat{I}(:,s)}{I(j,:)\cdot Q\cdot\hat{I}(:,s)}, \tag{14}$$

where I and $\hat{I}$ are identity matrices of size $|\mathcal{X}|$ and $|\hat{\mathcal{X}}|$ respectively, and $1\le i,j\le|\mathcal{X}|$, $1\le s\le|\hat{\mathcal{X}}|$. Then our objective function is the same as

$$e^{\varepsilon} = \max\hat{Q}. \tag{15}$$

To show its quasiconvexity, we need to show all the sublevel sets $\mathcal{S}_\alpha = \{Q\in\text{dom}\, e^{\varepsilon} | \, e^{\varepsilon}\le\alpha, \forall\alpha\in\mathbb{R}\}$ are convex, which is trivial since $e^{\varepsilon}\le\alpha$ is equivalent to $(I(i,:)-\alpha I(j,:))\cdot Q\cdot\hat{I}(:,s)\le 0$ and hence is a (convex) halfspace. □

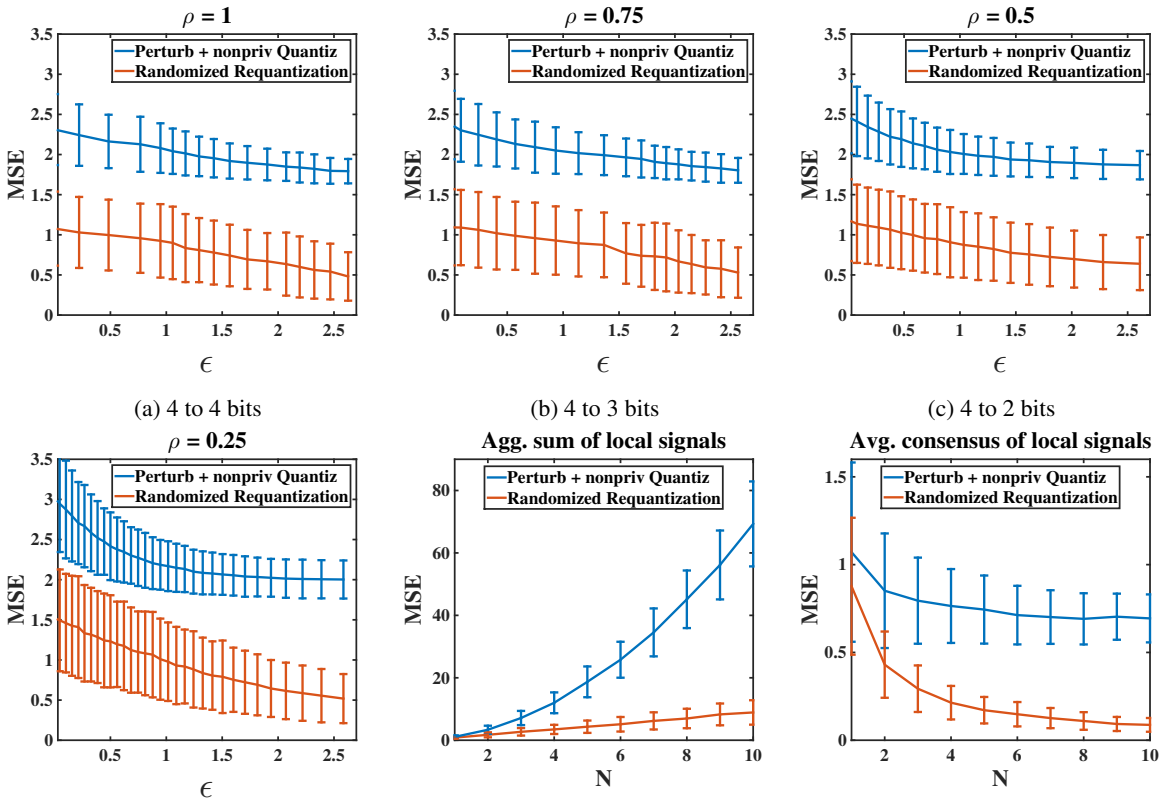
Actually, we can see the objective function e^{ε} as a point-wise maximum of linear fractional functions of Q. Therefore the original problem in (8)-(11) is equivalent to a standard *generalized linear-fractional program*, which can be solved via the bisection method [15].

4. SIMULATION RESULTS

To illustrate our approach, we assumed a lowpass signal class with 15 synthetic i.i.d. Fourier coefficients drawn according to $P=\mathcal{N}(10,2)$ but we optimize over the set $\mathcal{P} = \{\mathcal{N}(\mu,\sigma) : \mu\in[8,12], \sigma\in[1,3]\}$. The initial quantization was to $R=4$ bits, and we found optimal Q matrices via in (8)-(11) for alphabet sizes $\hat{R}=4,3,2,1$, or equivalently, different compression ratios $\rho = 1, 0.75, 0.5, 0.25$ according to (2). The distortion measure used in simulations is the *mean squared error* (MSE): $d(x^n,\hat{x}^n) = \frac{1}{n}\|x^n-\hat{x}^n\|_2^2$.

Figure 1 shows the minimum achievable privacy level ε for a given utility constraint δ on MSE under different compression ratios ρ. The standard privacy-utility tradeoff is demonstrated for any fixed ρ: more randomness (larger δ) guarantees lower privacy risk (smaller ε). Across different ratios ρ, for small distortion the achievable ε are quite close; this means we can halve the bit rate while guaranteeing nearly the same level of privacy.

More importantly, *randomized requantization* has better performance than naïve differentially private perturbation method, even for perturbation in the sparse Fourier transform domain [3]. We include the latter method for comparison. In Fig. (2a)-(2d), the red (lower) curves show the MSE versus ε for our locally differentially private Q; the blue (upper) curves show the same results from directly perturbing Fourier coefficients and quantizing down to the same output rate R'.



(a) 4 to 4 bits (b) 4 to 3 bits (c) 4 to 2 bits

(d) 4 to 1 bits (e) Aggregate Sum (f) Average Consensus

Fig. 2: Comparison between *randomized requantization* and standard perturbation method

We further carry out simulations when applying local quantization to $N = 20$ users having different realizations of the same signal and the goal is to estimate μ. Fig. (2e) and (2f) show the MSE for each case with $\varepsilon = 1, \rho = 0.5$. As the number of users N increases, the total "noise" added by our locally differentially private Q (lower red curve) increases much slower than direct perturbation (upper blue curve) when summing local signals and actually decreases when averaging. Again, in both applications, *randomized requantization* demonstrates better scalability with the network size.

5. DISCUSSION AND FUTURE WORK

In this paper, we proposed a novel *randomized requantization* mechanism and empirically showed its effectiveness for joint data privatization and compression while satisfying utility. For low distortion, the achievable ε values are similar, allowing us to control and reduce the storage/bandwidth of sensor nodes. We believe that this approach shows that for IoT systems of sensor nodes, individual sensors can simultaneously reduce their data while ensuring privacy. For a fixed distortion, sensors can trade off bandwidth and privacy, or they can trade off privacy and accuracy at a fixed bandwidth; this approach may also have larger system implications.

There are several major challenges to address to understand these tradeoffs. First, although e^{ε} is quasiconvex, for high bitrates the optimization may become infeasible due to the high dimension of Q: going from 8 bits to 4 bits would result in a 2048-dimensional problem. Structural results can be helpful here: for low distortion the support of output distribution may be reduced. Optimizing over $\hat{\mathcal{X}}$ may yield a modified Lloyd-Max algorithm to alternate between choosing $\hat{\mathcal{X}}$ and Q. Although we motivated this approach and provided a simulation of privately compressing lowpass Fourier signals, we claim that this can hold for many sparse or low-complexity signal classes, provided that the sparse representation lies in a common subspace. For more complex models such as compressed sensing or dictionary learning, the sparsity pattern itself may require privacy protection, in which case approaches from differentially private LASSO [18] may complement the approach here.

Differential privacy gives strong guarantees on the individual identifiability of single samples in the underlying signals. However, it is unclear if meaningful values of ε are possible in all parameter ranges. Understanding the limits of differentially private data sharing will shed light on how and where privacy guarantees should be made for ubiquitous monitoring networks.

6. REFERENCES

[1] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy," *Theoretical Computer Science*, vol. 9, no. 3-4, pp. 211–407, 2013.

[2] C. Dwork and A. Smith, "Differential privacy for statistics: What we know and what we want to learn," *Journal of Privacy and Confidentiality*, vol. 1, no. 2, pp. 2, 2010.

[3] V. Rastogi and S. Nath, "Differentially private aggregation of distributed time-series with transformation and encryption," in *Proceedings of the 2010 ACM SIGMOD International Conference on Management of data*. ACM, 2010, pp. 735–746.

[4] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Theory of Cryptography*, Berlin, Heidelberg, 2006.

[5] L. Fan and L. Xiong, "An adaptive approach to real-time aggregate monitoring with differential privacy," *IEEE Transactions on Knowledge and Data Engineering*, vol. 26, no. 9, pp. 2094–2106, 2014.

[6] C. Dwork, M. Naor, T. Pitassi, and G. N. Rothblum, "Differential privacy under continual observation," in *Proceedings of the Forty-Second ACM symposium on Theory of Computing (STOC)*. ACM, 2010, pp. 715–724.

[7] T.-H. H. Chan, E. Shi, and D. Song, "Private and continual release of statistics," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 3, pp. 26, 2011.

[8] S. Zhou, K. Ligett, and L. Wasserman, "Differential privacy with compression," in *Proceedings of the 2009 International Symposium on Information Theory*, Seoul, South Korea, 2009, pp. 2718–2722.

[9] J. C. Duchi, M. Jordan, and M. J. Wainwright, "Local privacy and statistical minimax rates," in *2013 IEEE 54th Annual Symposium on Foundations of Computer Science (FOCS)*. IEEE, 2013, pp. 429–438.

[10] A. D. Sarwate and L. Sankar, "A rate-disortion perspective on local differential privacy," in *Proceedings of the 52nd Annual Allerton Conference on Communication, Control and Computation*, Monticello, IL, USA, October 2014.

[11] L. Wasserman and S. Zhou, "A statistical framework for differential privacy," *Journal of the American Statistical Association*, vol. 105, no. 489, pp. 375–389, 2010.

[12] P. Kairouz, S. Oh, and P. Viswanath, "The composition theorem for differential privacy," Tech. Rep. arXiv:1311.0776v4 [cs.DS], ArXiV, December 2015.

[13] S. Papadimitriou, F. Li, G. Kollios, and P. S. Yu, "Time series compressibility and privacy," in *Proceedings of the 33rd International Conference on Very Large Data Bases (VLDB)*. VLDB Endowment, 2007, pp. 459–470.

[14] F. D. McSherry, "Privacy integrated queries: an extensible platform for privacy-preserving data analysis," in *Proceedings of the 2009 ACM SIGMOD International Conference on Management of Data*. ACM, 2009, pp. 19–30.

[15] S. Boyd and L. Vandenberghe, *Convex optimization*, Cambridge university press, 2004.

[16] S. P. Lloyd, "Least squares quantization in pcm," *IEEE Transactions on Information Theory*, vol. 28, no. 2, pp. 129–137, March 1982.

[17] J. Max, "Quantization for minimum distortion," *IRE Transactions on Information Theory*, vol. 6, no. 1, pp. 7–12, March 1960.

[18] D. Kifer, A. Smith, and A. Thakurta, "Private convex empirical risk minimization and high-dimensional regression," *Journal of Machine Learning Research*, vol. 1, pp. 41, 2012.