Optimality of the Laplace Mechanism in Differential Privacy

Fragkiskos Koufogiannis, Shuo Han, George J. Pappas

Abstract—In the highly interconnected realm of Internet of Things, exchange of sensitive information raises severe privacy concerns. The Laplace mechanism – adding Laplace-distributed artificial noise to sensitive data – is one of the widely used methods of providing privacy guarantees within the framework of differential privacy. In this work, we present Lipschitz privacy, a slightly tighter version of differential privacy. We prove that the Laplace mechanism is optimal in the sense that it minimizes the mean-squared error for identity queries which provide privacy with respect to the $\ell_1$-norm. In addition to the $\ell_1$-norm which respects individuals’ participation, we focus on the use of the $\ell_2$-norm which provides privacy of high-dimensional data. A variation of the Laplace mechanism is proven to have the optimal mean-squared error from the identity query. Finally, the optimal mechanism for the scenario in which individuals submit their high-dimensional sensitive data is derived.

I. INTRODUCTION

The Internet of Things (IoT) envisions that everyday devices such as smartphones, power meters, and household appliances will exchange information and provide innovative services such as e-health and assisted living [1]. However, when a device communicates sensitive information (e.g. monitored activities, health records) over a vast network of interconnected things, privacy concerns are raised [2]. For example, traffic maps can be constructed from aggregating users’ GPS traces and users can benefit from such published maps by avoiding congested routes. On the other hand publishing statistics of sensitive data of a population while providing privacy guarantees is not trivial. The Netflix prize is an example were, given publicly released information [3], an adversary can partially reconstruct private data [4]. Accurate, privacy-preserving mechanisms are essential for IoT to provide these services while respecting individuals’ privacy [5].

Significant efforts have been made to address these privacy concerns [6], [7], [8], [9], [10], [11], [12]. Intuitively, uncertainty about the private data is introduced by publishing a perturbed response instead of the exact one. In the context of traffic monitoring, virtual trip lines and data cloaking techniques [13], [14] provide privacy against a given adversarial model. In practice, though, an adversary may be more powerful or informed than the model assumptions. Additionally, an information-theoretic framework based on mutual information was introduced [15]. However, this approach provides privacy guarantees in a probabilistic sense and, therefore, rare, but severe, privacy breaches are possible. A rigorous notion of privacy is differential privacy which provides formal privacy guarantees without any assumptions on the adversary’s power [16] and is the notion used in this work. Specifically, while answering queries from private data, artificial noise is injected. This noise is deliberately designed and ensures that an adversary cannot confidently infer any individual’s private data, where an adjacency relation defines the pairs of inputs that are rendered almost indistinguishable. For tight privacy level, increased amounts of noise are required and, consequently, the accuracy of the noisy response degrades. Thus, a trade-off between privacy level and accuracy exists. Ideally, one would like to design optimal mechanisms that satisfy a predefined privacy level and approximate a given query with minimum mean-squared error.

Several methods for constructing differentially private mechanisms have been proposed. In particular, given a score function for every pair of private input and public response, the exponential mechanism [17] provides a powerful way of building a private mechanism, although no performance guarantees were initially provided. The Laplace mechanism is an instance of the exponential mechanism for real, vector-valued private data which adds Laplace-distributed noise $V$ to the private data:

$$P(V = v) \propto e^{-\epsilon\|v\|_1},$$

(1)

where $\epsilon \in (0, \infty)$ is the privacy level — smaller values of parameter $\epsilon$ result to stronger privacy guarantees — and $\|\cdot\|_1$ is the $\ell_1$-norm. Near-optimality of the Laplace mechanism for a single integer-valued linear query was presented in [18], whereas, for linear queries, asymptotic (in the number of users) sub-optimality bounds were derived for a variant of the Laplace mechanism [19]. For single-dimensional private data, the exact optimality of the “staircase” mechanism, a quantized version of the Laplace mechanism, was established in [20]. Moreover, the Laplace mechanism was proven to be an entropy-minimizing private mechanism [21] under a version of differential privacy for metric spaces [22].

In this work, we establish optimality guarantees for the Laplace mechanism – adding Laplace-distributed noise \{1\}. We formalize Lipschitz privacy which is a slightly stronger version of differential privacy for metric spaces and allows us to pose the problem of designing optimal privacy-aware mechanisms as optimization problems where privacy requirements are included as constraints. We, first, prove that the Laplace mechanism optimally approximates...
real-valued private data by achieving the minimum mean-squared error. Besides the $\ell_1$-norm used in (1), we focus on the $\ell_2$-norm as the appropriate adjacency relation that captures the privacy aspects of sensitive signals, such as GPS and power consumption traces. In the $\ell_2$-norm case, we prove the optimality of a variant of the Laplace mechanism. Furthermore, we extend our optimality results to the case of a composite adjacency relation for the scenario when multiple individuals contribute their private signals, e.g., drivers report their GPS traces.

A brief overview of differential privacy is provided in Section II. In Section III, a version of differential privacy for Euclidean spaces is explored and strong connections with differential privacy are established. Section IV establishes the optimal private mechanism for the case of multi-dimensional identity queries under a general adjacency relation. Specifically, we focus on Euclidean spaces and assume each of the $n$ users contributes his $m$-dimensional sensitive data. Let $U = \mathbb{R}^{n \times m}$ and $Y = \mathbb{R}^{n \times m}$ and consider the adjacency relation $A$ defined as:

\[
(u, u') \in A \Leftrightarrow \exists \text{ s.t. } \|u_i - u'_i\|_2 \leq \alpha \text{ and } u_j = u'_j, \forall j \neq i.
\] (2)

Adjacency relation (2) respects privacy of every individual’s sensitive data $u_i$; even if an adversary is aware of every other user’s data $u_j$, $j \neq i$, the adversary cannot confidently extract the value $u_i$.

III. DIFFERENTIAL PRIVACY AS LIPSCHITZ CONSTRAINT

In this section, we reformulate differential privacy for metric spaces as a Lipschitz constraint. This reformulation, which we call Lipschitz privacy, is closely related to the original notion of differential privacy introduced in [22]. In particular, the differential privacy constraint is viewed as a sensitivity constraint. The sensitive data is assumed to be an element of a complete vector space $U$ equipped with a norm $\| \cdot \|$, and the set of possible responses is denoted by $Y$. Formally, we provide the definition of Lipschitz privacy:

Definition 2 (Lipschitz privacy): Let $U$ be a metric space and $Y$ be a set of responses. A mechanism $Q : U \rightarrow \Delta(Y)$ is called $\epsilon$-Lipschitz differentially private if the log-probability function is $\epsilon$-Lipschitz:

\[
|\ln P(Qu \in S) - \ln P(Qu' \in S)| \leq \epsilon \|u - u'\|, \forall u, u' \in U \text{ and } S \subseteq Y.
\] (3)

In practical applications, the space of private data $U = \mathbb{R}^n$ is Euclidean equipped with the $\ell_2$-norm. Assuming the mechanism $Q$ possesses a probability density function $g(u, y) = P(Qu = y)$, where $g(u, y)$ is almost everywhere differentiable in $u$, the Lipschitz condition (3) translates to a point-wise bound on the derivative across the private input $u$ as follows:

$g(\cdot, y)$ is continuous for all $y \in Y$ and,

\[
\|\nabla g(u, y)\|_* \leq cg, \text{ for a.e. } u \in U \text{ and all } y \in Y,
\]

where $\| \cdot \|_*$ is the dual norm of $\| \cdot \|$.

A. A Metric as Adjacency Relation

The adjacency relation $A$ in differential privacy is replaced by the metric $\| \cdot \|$ of the space $U$ of private data. The composite adjacency relation (2) can be captured using $\ell_1$ and $\ell_2$-norms. Specifically, assume that the private data $u = [u_1, \ldots, u_n]$ is an aggregation of $n$ individuals’ high-dimensional data $u_i \in \mathbb{R}^m$. Then, adjacency relation (2) can be relaxed to:

\[
(u, u') \in A \Leftrightarrow \sum_{i=1}^{n} \|u_i - u'_i\|_2 \leq \alpha.
\] (4)
According to the Lipschitz-privacy framework and assuming existence and differentiability of the density of the mechanism, adjacency relation (5) can be viewed as an \( \ell_2 \)-sensitivity constraint that ensures privacy of high-dimensional data. This constraint is encapsulated in an \( \ell_1 \)-sensitivity constraint that respects individuals’ participation in the scheme. Additionally, this expression ensures that privacy of individuals’ sensitive data remains invariant under rotation transformations on the high-dimensional data \( u_i \). This invariance is important in many theoretical and practical case such as privacy of the state of dynamical systems and privacy of GPS traces, respectively.

**B. Connections between Lipschitz and Differential Privacy**

The notion of Lipschitz privacy is closely related to that of differential privacy. Particularly, an \( \epsilon \)-Lipschitz private mechanism is also differential private.

**Proposition 3:** For any \( \alpha > 0 \). Then, an \( \epsilon \)-Lipschitz private mechanism \( Q \) is \( \alpha \)-differentially private:

\[
P(Qu \in S) \leq e^{\epsilon \alpha} P(Qu' \in S), \forall u, u' : \|u - u'\| \leq \alpha.
\]

Many popular differentially private mechanisms, such as the Laplace and the exponential mechanism, are also Lipschitz-differentially private. One exception that fails to satisfy Lipschitz-privacy constraints is the staircase mechanism [20], since the underlying noise distribution is discontinuous and, hence, is not Lipschitz.

**Proposition 4:** Let \( s : U \times \mathcal{Y} \rightarrow \mathbb{R} \) be \( \ell_2 \)-Lipschitz in \( U \). Then, the mechanism \( Q \) with density

\[
P(Qu = y | u) \propto e^{\epsilon s(u, y)}
\]

is \( \epsilon \)-Lipschitz differentially private. In the special case where \( U = \mathcal{Y} = \mathbb{R}^n \) and \( s(u, y) = -\|u - y\|_p \), we recover the Laplace mechanism. Furthermore, Lipschitz privacy inherits the property of resiliency to post-processing. Identically to differential privacy, any further, possibly randomized, post-processing of the output carries the same privacy guarantees.

**Proposition 5 (Post-processing):** Consider an \( \epsilon \)-Lipschitz differentially private mechanism \( Q : U \rightarrow \Delta (\mathcal{Y}) \) and a post-processing of the output \( f : \mathcal{Y} \rightarrow \mathbb{R} \). Then, the mechanism \( f \circ Q \) is \( \epsilon \)-Lipschitz differentially private.

Propositions 3, 4 establish that Lipschitz-differential privacy is a stricter version of differential privacy. Lipschitz privacy has some benefits over the original framework. Firstly, the privacy constraint is simplified; the adjacency relation is now captured by the metric of the space of private data. Furthermore, Lipschitz-differential privacy enables the use of calculus tools in designing and proving properties of mechanisms. Additionally, it provides a unified privacy framework that can support richer privacy-aware applications. Privacy is now viewed as a sensitivity constraint on the mapping between private inputs and published outputs.

### IV. Optimal Private Mechanisms

In this section, the optimality of the Laplace mechanism is proven. Specifically, we prove that the Laplace mechanism minimizes the mean-squared error among all private mechanisms that use additive and input-independent noise. Initially, the result is derived for the case of a single-dimensional identity query. Next, the result is extended to the case of isotropic multi-dimensional queries under both \( \ell_1 \) and \( \ell_2 \) norms. The \( \ell_1 \)-norm respects individuals’ participation in the aggregation scheme and is related to event counting queries [24]. Moreover, the \( \ell_2 \)-norm is invariant under rotations and is more suitable for high-dimensional private data such as GPS signals and power consumption traces. Finally, the optimal mechanism for the case of multiple individuals contributing their high-dimensional sensitive data is derived from the results for \( \ell_1 \) and \( \ell_2 \) norms.

#### A. Single-Dimensional Identity Query

The exponential mechanism introduced in [17] is a general way of building privacy-preserving mechanisms. Besides the exponential mechanism, specific mechanisms that approximate linear, high-dimensional queries were explored in [24]. However, no optimality guarantees were provided. Under the original framework of differential privacy the staircase mechanism [20] is optimal for one-dimensional identity queries in the sense of mean-squared error. Asymptotic bounds on the sub-optimality of mechanisms approximating linear queries were introduced [19]. In this approach, we are interested in exact optimality results. Specifically, we provide a proof of the optimality of the Laplace mechanism for the case of single-dimensional identity queries. In [21], the Laplace mechanism is proven to be an entropy-minimizer. In this work, we provide a proof that the Laplace mechanism achieves the minimal mean-squared error. In the following subsections, this result is extended to high-dimensional cases.

Initially, we focus on single-dimensional private data and Lipschitz-private mechanisms that add oblivious noise. In this setting, the mean-squared error is minimized when the noise is Laplace-distributed. The problem of designing the optimal private mechanism is initially posed as an infinite-dimensional linear program. Optimality of the Laplace distribution is proven by deriving the dual problem and constructing a dual feasible solution. In particular, the space of private data is the real line \( U = \mathbb{R} \) equipped with the absolute value as a metric. We approximate the identity query \( q(u) = u \) with an \( \epsilon \)-Lipschitz private mechanism \( Q \) that adds input-independent noise with probability measure \( g^*: \)

\[
Qu = u + V, \text{ where } V \sim g \in \Delta (\mathbb{R^n}),
\]

where \( \Delta (\mathcal{Y}) \) denotes the set of probability measures over the set \( \mathcal{Y} \). The following result establishes the optimality of Laplace distribution.

**Theorem 6:** Consider the set of \( \epsilon \)-Lipschitz private mechanisms \( Q : \mathbb{R} \rightarrow \Delta (\mathbb{R^n}), Qu = u + V, \) that approximate the identity query \( q : \mathbb{R} \rightarrow \mathbb{R}, q(u) = u \), where noise \( V \) is input-independent and has probability distribution \( g \). The Laplace
mechanism that adds noise with density \( l(v) = \frac{1}{2} e^{-|v|} \) achieves the minimal mean-squared error:
\[
\mathbb{E} (Qu - q(u))^2 = \mathbb{E} V^2 \geq \mathbb{E} \|V\|^2 = \frac{2}{\epsilon^2}.
\]

Proof: A simplified but intuitive sketch of the proof is presented here. A full proof is presented in the Appendix. By definition, the optimal mechanism is the solution of the following optimization problem:
\[
\begin{align*}
\min_{\eta \in \mathcal{A}(\mathbb{R})} & \quad \mathbb{E} V^2 \\
\text{s.t.} & \quad Q \text{ is } \epsilon \text{-Lipschitz private.}
\end{align*}
\]

The optimization is assumed over the infinite-dimensional space of probability measures over the real line. For a simplified proof, we restrict our attention to probability measures that are continuous and almost everywhere differentiable. This assumption is removed in the technical proof. The privacy constraint is massaged:
\[
Q \text{ is } \epsilon \text{-Lipschitz private } \Rightarrow \frac{d}{du} \ln P(Qu = y) \leq \epsilon, \quad \forall u, y \Leftrightarrow \frac{d}{du} P(V = y - u) \leq \epsilon P(V = y - u), \quad \forall u, y \Leftrightarrow |g'(v)| \leq \epsilon g(v), \quad \forall v.
\]

Specifically, \( g \) should be continuous and \( g' \) should exist almost everywhere. Problem (6) can then, be restated as a linear program:
\[
\begin{align*}
\min_{g : AC(\mathbb{R} \to \mathbb{R}_+)} & \quad \int v^2 g(v) dv \\
\text{s.t.} & \quad \int g(v) dv = 1, \quad (7)
\end{align*}
\]
where \( AC \) denotes the set of absolutely continuous functions. Problem (7) is an infinite-dimensional linear program with uncountably many constraints. We assign the dual variables \( \lambda \in \mathbb{R} \) and \( \kappa, \mu : \mathbb{R} \to \mathbb{R}_+ \) for the two constraints, respectively. The dual of Problem (7) is:
\[
\begin{align*}
\max_{\lambda \in \mathbb{R}, \eta \in \mathbb{C}^1(\mathbb{R} \to \mathbb{R})} & \quad \lambda \\
\text{s.t.} & \quad \eta'(v) + \epsilon |\eta(v)| \leq v^2 - \lambda, \quad \forall v \in \mathbb{R}, \quad (8)
\end{align*}
\]
where \( \mathbb{C}^1(\mathbb{R} \to \mathbb{R}) \) is the set of all continuously differentiable functions. The Laplace distribution \( g(v) = \frac{1}{2} e^{-|v|/\sqrt{2}} \) is a primal feasible solution for Problem (7) with cost \( \sqrt{2} \). Moreover, we construct a dual feasible solution for Problem (8) with cost arbitrarily close to \( \lambda^* = \sqrt{2} \). Specifically, for any \( \lambda < \lambda^* \), we are able to construct a dual feasible solution \( (\lambda, \eta) \) that satisfies the initial value problem:
\[
\eta(0) = 0 \quad \text{and} \quad \eta'(v) + \epsilon |\eta(v)| = v^2 - \lambda, \quad \forall v \in \mathbb{R} \setminus \{0\}. \quad (9)
\]
Figure 1 plots the unique solution \( \eta : \mathbb{R} \to \mathbb{R} \) of the initial value problem (9) for different values of \( \lambda \). For \( \lambda < \lambda^* \), the unique solution \( \eta \) of the initial value problem (9) is feasible since it satisfies the boundary constraints:
\[
\lim_{v \to \infty} \eta(v) \geq 0, \quad \lim_{v \to -\infty} \eta(v) \leq 0.
\]

On the contrary, the dual variable \( \eta \) is infeasible for \( \lambda \geq \lambda^* \). Weak duality establishes the optimality of the Laplace mechanism. Surprisingly, the dual solution \( \eta(v) = -\frac{1}{\epsilon^2} v |v| + 2 \) for the optimal value \( \lambda^* \) is infeasible. The infinite-dimensionality of the problem leads to an open set of feasible solutions for problem (8) and generates this paradox.

The staircase mechanism [20] can be viewed as an approximation of the Laplace mechanism. Although it features better mean-squared error than the Laplace mechanism, the staircase mechanism is not \( \epsilon \)-Lipschitz private for any finite value of \( \epsilon \). Thus, the staircase mechanism is not a feasible solution to Problem (6).

B. High-Dimensional Identity Query under \( \ell_1 \)-norm

Differential privacy is mainly targeted for schemes where individuals contribute their personal data to a single database. In such schemes, the sensitive data \( u \) contains each individual’s private data \( u_i \) at coordinate \( i \). Here, we extend the previous results to high-dimensional identity queries. Privacy-aware approximation of identity queries can be interpreted as synthetic databases which are post-processed to answer any subsequent query. More formally, let the space of sensitive databases which are post-processed to answer any subsequent query be the real space \( U = \mathbb{R}^n \) equipped with the \( \ell_1 \)-norm. We focus on the case of identity queries \( q : \mathbb{R}^n \to \mathbb{R}^n \) with \( q(u) = u \). A generalized version of Theorem 6 establishes optimality of the Laplace mechanism:

Theorem 7: Consider the \( \epsilon \)-Lipschitz private (with respect to the \( \ell_1 \)-norm) mechanism \( Q : \mathbb{R}^n \to \Delta (\mathbb{R}^n) \) of the form \( Qu = u + V \), with \( V \sim g(V) \in \Delta (\mathbb{R}^n) \). Then, the Laplace mechanism that adds oblivious noise with density \( g = \frac{1}{\zeta_n^2} e^{-|v|} \) minimizes mean-squared error:
\[
\mathbb{E}_{V \sim g} \|V\|^2 \geq \mathbb{E}_{V \sim \tilde{g}} \|V\|^2 = \frac{2n}{\epsilon^2}.
\]

Proof: Similarly to the proof of Theorem 6, the optimal mechanism is the solution of the following optimization

\[
\begin{align*}
\min_{\eta \in \mathcal{A}(\mathbb{R})} & \quad \mathbb{E} V^2 \\
\text{s.t.} & \quad Q \text{ is } \epsilon \text{-Lipschitz private.}
\end{align*}
\]
Therefore, the dual Problem (11) admits a feasible solution where
\[
\eta(v) = \mu(v) - \kappa(v),
\]
and \( \kappa : \mathbb{R}^n \times \mathbb{S}^{n-1} \rightarrow \mathbb{R}_+ \), where \( \mathbb{S}^{n-1} = \{ \hat{a} \in \mathbb{R}^n : ||\hat{a}||_2 = 1 \} \). Moreover, set \( \eta(v) = \kappa(v) - \mu(v) \), and formulate the dual problem of Problem (12):
\[
\text{maximize} \quad \lambda \in \mathbb{R}, \kappa \in \mathbb{R}^n \times \mathbb{S}^{n-1} \rightarrow \mathbb{R}_+
\]
\[
\text{s.t.} \quad \nabla \cdot \left( \int_{\mathbb{S}^n} \hat{a} \kappa(v, \hat{a}) d\hat{a} \right) + \epsilon \int_{\mathbb{S}^n} \kappa(v, \hat{a}) d\hat{a} \leq \nu^T v - \lambda,
\]
\[
\lim_{||v||_2 \rightarrow \infty} \int_{\mathbb{S}^n} \hat{a} \cdot v \kappa(v, \hat{a}) d\hat{a} \geq 0.
\]
A feasible solution for the primal problem (12) is:
\[
g(v) = \frac{e^{\epsilon} \Gamma\left(\frac{n}{2} + 1\right)}{\pi^{\frac{n}{2}} (n + 1)} e^{-||v||_2^2},
\]
with mean-square error \( \lambda^* = \frac{n(n+1)}{2\epsilon^2} \). On the other hand, there exists a dual feasible solution for Problem (13) with cost arbitrarily close to \( \lambda^* \). Consider a dual feasible solution of the form:
\[
\kappa(v, \hat{a}) = \left[\eta(||v||_2)\right]^+ \delta \left( \hat{a} + \frac{v}{||v||_2} \right) - \left[\eta(||v||_2)\right]^- \delta \left( \hat{a} - \frac{v}{||v||_2} \right),
\]
where \( \delta \) is Dirac’s delta function on the unit n-sphere \( \mathbb{S}^{n-1} \), \( \eta : \mathbb{R}_+ \rightarrow \mathbb{R} \) is a suitable function, and \( [\cdot]^+ \) and \( [\cdot]^− \) are the positive and negative parts of a function, respectively. Then, we can reduce the feasible region of Problem (13) and rewrite it as
\[
\text{maximize} \quad \lambda \in \mathbb{R}, \eta \in \mathbb{R}, \kappa : \mathbb{R}^n \rightarrow \mathbb{R}_+
\]
\[
\text{s.t.} \quad \eta(r) + \frac{n-1}{r} \eta(r) + \epsilon |\eta(r)| \leq r^2 - \lambda,
\]
\[
\lim_{r \rightarrow \infty} \eta(r) \geq 0.
\]
Similarly to the proof of Theorem 7, a feasible solution \( (\lambda, \eta) \) of Problem (15) of the following form is constructed:
\[
\eta'(r) + \frac{n-1}{r} \eta'(r) + \epsilon |\eta'(r)| = r^2 - \lambda \quad \text{and} \quad \eta(0) = 0(16)
\]
Figure 2 shows the solution of the initial value problem (16) for different values of \( \lambda \). For \( \lambda < \lambda^* \), the solution is feasible and, thus, the optimality of the density (14) for the initial value problem (12) is established.

Again, for \( \lambda = \lambda^* \), the dual solution \( \eta(r) = -\frac{r(r^2 + n+1)}{2\epsilon^2} \) is infeasible as a result of the infinite-dimensional nature of problem (16).

Sample from distribution (14) can be efficiently generated. The magnitude \( r = ||v||_2 \) of the noise is drawn from the Gamma distribution \( r \sim \frac{\epsilon}{\Gamma(n)} e^{-\epsilon r} r^{n-1} \) and the direction \( \hat{v} = \frac{v}{||v||_2} \) is uniformly sampled from the sphere \( \mathbb{S}^{n-1} \).

D. Multiple Users with High-Dimensional Private Data

In this section, the case of multiple users contributing their high-dimensional sensitive data is explored. Specifically, consider \( n \) individuals. Each individual contributes his \( m \)-dimensional sensitive data \( u_i \in \mathbb{R}^n \), \( i \in \{1, \ldots, n\} \). Furthermore, we are interested in releasing a privacy-aware version of the sensitive data under an adjacency relation that
preserves both individual’s participation and each user’s data. These aspects of privacy are captured by adjacency relation \(\Psi\) derived earlier.

In particular, let the space of private data be \(\mathcal{U} = \mathbb{R}^{n\times m}\) and consider private mechanisms \(Q\) that add input-independent noise \(V \sim g\) to the private data \(u\). Similarly to the previous case, a version of the Laplace mechanism provides the optimal mean-squared error.

**Theorem 9:** Consider the \(\epsilon\)-Lipschitz private (with respect to the adjacency relation \(\Psi\)) mechanism \(Q : \mathbb{R}^{n \times m} \rightarrow \Delta(\mathbb{R}^{n \times m})\) of the form \(Q u = u + V\), with \(V \sim g \in \Delta(\mathbb{R}^{n \times m})\). Then, the Laplace mechanism that adds oblivious noise with density \(g = I_{n\times m}(v) \rightarrow e^{-\epsilon \sum_{i=1}^{m} \|v_i\|_2}\) minimizes the mean-squared-error:

\[
\mathbb{E}_{V \sim g} \|V\|^2 \geq \mathbb{E}_{V \sim I_{n\times m}} \|V\|^2 = \frac{n^2(m + 1)}{\epsilon^2}.
\]

**Proof:** The primal optimization problems is as follows

\[
\text{minimize}_{g:AC(\mathbb{R}^{n \times m} \rightarrow \mathbb{R}_+)} \int_{\mathbb{R}^{n \times m}} g(v) v^T v d\nu
\]

\[
\text{s.t.} \int_{\mathbb{R}^{n \times m}} g(v) dv = 1,
\]

\[
\|\nabla_i g(v)\|_2 \leq \epsilon g(v), \forall i \in [n], \forall v \in \mathbb{R}^n,
\]

where \(\nabla_i g = [\frac{\partial g}{\partial u_{i,1}}, \ldots, \frac{\partial g}{\partial u_{i,m}}]\) and \([n] = \{1, \ldots, n\}\). The dual problem is formulated:

\[
\text{maximize}_{\lambda \in \mathbb{R}, \eta : \mathbb{R}^n \rightarrow \mathbb{R}_+} \lambda
\]

\[
\text{s.t.} \sum_{i=1}^{n} \left\{ \eta_i(r_i) + \frac{n - 1}{r_i} \eta_i(r_i) + \epsilon |\eta_i(r_i)| \right\} \leq \sum_{i=1}^{n} r_i^{-2} - \lambda, \text{ and } \lim_{r_i \to \infty} \eta_i(r_i) \geq 0, \forall i
\]

A pair of feasible primal and dual solutions is constructed:

\[g = \frac{e^m T(m+1)}{m \pi^2} \frac{1}{\Gamma(m)} n e^{-\epsilon \sum_{i=1}^{m} \|v_i\|_2},\]

\[\eta_i(r_i) = \eta_{\epsilon \ell_2}(r_i), \text{ and } \lambda = n \lambda_{\epsilon \ell_2},\]

where \((\lambda_{\epsilon \ell_2}, \eta_{\epsilon \ell_2})\) is the dual solution of Theorem 8. Weak duality establishes the optimality of the solution.

---

**REFERENCES**

[1] Luigi Atzori, Antonio Iera, and Giacomo Morabito. The internet of things: A survey. *Computer networks*, 54(15):2787–2805, 2010.

[2] Rolf H Weber. Internet of things–new security and privacy challenges. *Computer Law & Security Review*, 26(1):23–30, 2010.

[3] James Bennett and Stan Lanning. The netflix prize. In *Proceedings of KDD cup and workshop*, volume 2007, page 35, 2007.

[4] Arvind Narayanan and Vitaly Shmatikov. How to break anonymity of the netflix prize dataset. *arXiv preprint cs/0610105*, 2006.

[5] Daniele Miorandi, Sabrina Sicari, Francesco De Pellegrini, and Imrich Chlamtac. Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, 10(7):1497–1516, 2012.

[6] Parv Venkitasubramaniam. Privacy in stochastic control: A markov decision process perspective. In *Communication, Control, and Computing (Allerton), 2013 51st Annual Allerton Conference on*, pages 381–388, IEEE, 2013.

[7] Shao Han, Ufuk Topcu, and George J Pappas. Differentially private distributed constrained optimization. *arXiv preprint arXiv:1411.4105*, 2014.

[8] Marci Meingast, Tanya Roosta, and Shankar Sastry. Security and privacy issues with health care information technology. In *Engineering in Medicine and Biology Society, 2006. EMBS’06. 28th Annual International Conference of the IEEE*, pages 5453–5458, IEEE, 2006.

[9] Alvaro A Cárdenas, Saurabh Amin, Galina Schwartz, Roy Dong, and Shankar Sastry. A game theory model for electricity theft detection and privacy-aware control in ami systems. In *Communication, Control, and Computing (Allerton), 2010 50th Annual Allerton Conference on*, pages 1830–1837. IEEE, 2012.

[10] Pradeep Chathuranga Weeraddana, Georgios Athanasiou, Carlo Fischione, and John S Baras. Per-se privacy preserving solution methods based on optimization. In *Proceedings of the 52nd IEEE Conference on Decision and Control (CDC)*, pages 206–211, 2013.

[11] Edward S Canepa and Christian G Claudel. A framework for privacy and security analysis of probe-based traffic information systems. In *Proceedings of the 2nd ACM international conference on High confidence networked systems*, pages 25–32. ACM, 2013.

[12] Jerome Le Ny and George J Pappas. Differentially private filtering. *Automatic Control, IEEE Transactions on*, 59(2):341–354, 2014.

---

**V. Discussion**

In this work, we explored Lipschitz privacy, which is a version of differential privacy that is adapted for metric spaces. Moreover, we proved that, for a given privacy level, the Laplace mechanism minimizes the mean-squared error among all single-dimensional mechanisms that add input-independent noise. The design of the optimal private mechanism is initially formulated as a linear program. Then, the optimality of the Laplace mechanism is established by constructing a pair of primal and dual feasible solutions with zero duality gap. Next, the result is extended to high-dimensional real spaces equipped with the \(\ell_1\)-norm. The case of \(\ell_1\)-norm corresponds to the case of providing privacy guarantees with respect to participation of any individual. Furthermore, the optimality of a variation of the Laplace mechanism is established for real spaces equipped with the \(\ell_2\)-norm. In this case, the privacy guarantees are invariant under rotations and, thus, this choice of norm captures the case where every individual provides high-dimensional sensitive data. A combination of the two results provides the optimal privacy-aware approximation of the aggregation of high-dimensional sensitive data of multiple individuals. Future directions include optimality guarantees for more general classes of queries beyond identity queries. Moreover, it is useful to study optimality results for other composite adjacency relations such as that proposed in [25].
Then:

\[ u \text{ is absolutely continuous.} \]

For any measurable \( S \), \( V = u + S \) holds. Hence, \( V \) possesses density. Abusing notation, we denote the density of the noise \( V \) with \( g \).

We now provide a technical proof of Theorem 6:

**Proof:** Consider the \( \epsilon \)-Lipschitz differential private mechanisms that use additive, oblivious noise \( V \) with probability measure \( g \):

\[ Q : \mathbb{R} \rightarrow \Delta(\mathbb{R}), \quad Qu = u + V, \]  

where \( V \sim g \).

Solving for the optimal, in the mean-squared error sense, probability measure is posed as a linear, but infinite-dimensional program:

\[
\begin{align*}
\text{minimize} & \quad \mathbb{E}_{V \sim g} V^2 \\
\text{s.t.} & \quad \sum_{v \in \Delta(\mathbb{R})} g(v) v^2 = 1, \quad g(v) \geq 0, \forall v, \\
& \quad -eg(v) \leq \lim inf_{\nu \rightarrow 0} \frac{g(v + \nu) - g(v)}{\nu}, \forall v, \\
& \quad \lim sup_{\nu \rightarrow 0} \frac{g(v + \nu) - g(v)}{\nu} \leq eg(v), \forall v.
\end{align*}
\]

(17)

Problem (18) is an infinite-dimensional linear program with infinite many constraints, thus, it is unclear though whether the minimum is achievable. The Laplace distribution \( l_{\epsilon}(v) = \frac{\epsilon}{2} e^{-\frac{\epsilon}{2}|v|} \) is a feasible solution with mean error \( \frac{\epsilon}{2} \). We now discretize, dualize and take limits in order to compute the dual problem. As a result, we prove that the dual variable is differentiable and we retrieve the formulation of the dual problem. Consider \( N \) discrete points:

\[ v_i = -M + i \cdot \nu, \quad i \in \{1, \ldots, N\} \]

where \( \nu = \frac{2M}{N - 1} \) is the discretization step and \( M \) is the truncation limit. For \( g_i = g(v_i) \), the original optimization is now approximated by its discretized version:

\[
\begin{align*}
\text{minimize} & \quad \sum_{i=1}^{N} g_i v_i^2 + \nu \\
\text{s.t.} & \quad \sum_{i=1}^{N} g_i v_i = 1, \quad g_i \geq 0, \forall i, \\
& \quad -\epsilon \cdot \frac{g_i + g_{i+1}}{2} \leq \frac{g_{i+1} - g_i}{\nu} \leq \epsilon \cdot \frac{g_i + g_{i+1}}{2}, \forall i.
\end{align*}
\]

Problem (18) is an infinite-dimensional linear program with infinite many constraints, thus, it is unclear though whether the minimum is achievable. The Laplace distribution \( l_{\epsilon}(v) = \frac{\epsilon}{2} e^{-\frac{\epsilon}{2}|v|} \) is a feasible solution with mean error \( \frac{\epsilon}{2} \). We now discretize, dualize and take limits in order to compute the dual problem. As a result, we prove that the dual variable is differentiable and we retrieve the formulation of the dual problem. Consider \( N \) discrete points:

\[ v_i = -M + i \cdot \nu, \quad i \in \{1, \ldots, N\} \]

where \( \nu = \frac{2M}{N - 1} \) is the discretization step and \( M \) is the truncation limit. For \( g_i = g(v_i) \), the original optimization is now approximated by its discretized version:

\[
\begin{align*}
\text{minimize} & \quad \sum_{i=1}^{N} g_i v_i^2 + \nu \\
\text{s.t.} & \quad \sum_{i=1}^{N} g_i v_i = 1, \quad g_i \geq 0, \forall i, \\
& \quad -\epsilon \cdot \frac{g_i + g_{i+1}}{2} \leq \frac{g_{i+1} - g_i}{\nu} \leq \epsilon \cdot \frac{g_i + g_{i+1}}{2}, \forall i.
\end{align*}
\]

(17)

Appendix

Theorem 6 establishes the optimality of the Laplace mechanism for a single-dimensional identity query. A more technical proof is presented here. First, we prove that, for Lipschitz differential privacy guarantees to hold, the additive noise should possess density.

**Lemma 10:** Consider the \( \epsilon \)-Lipschitz private mechanism \( Q \) that uses oblivious, additive noise \( V \). Specifically, let \( Qu = u + V \), where \( V \) has probability measure \( g \in \Delta(V) \). Then \( V \) possesses density.

**Proof:** We prove that the cumulative density function \( G \) of \( V \)

\[ G(x) = \mathbb{P}(V \leq x) \]

is absolutely continuous. For any measurable \( S \subseteq \mathbb{R} \) and any \( u_1, u_2 \in \mathbb{R} \), Lipschitz privacy dictates that:

\[ |\ln \mathbb{P}(QU_1 \in S) - \ln \mathbb{P}(QU_2 \in S)| \leq \epsilon|u_1 - u_2| \]

Let \( S = (-\infty, 0] \), \( u_1 = -x \), and \( u_2 = -y \), with \( x < y \). Then:

\[ |\ln \mathbb{P}(V \leq x) - \ln \mathbb{P}(V \leq y)| \leq \epsilon|x - y| \Rightarrow \]

\[ |\mathbb{P}(V \leq x) - \mathbb{P}(V \leq y)| \leq \mathbb{P}(V \leq x)\epsilon|x - y| \Rightarrow \]

\[ |G(x) - G(y)| \leq \epsilon|x - y| \]

Therefore, \( G \) is absolutely continuous and, hence, \( V \) possesses density. Abusing notation, we denote the density of the noise \( V \) with \( g \).
computed and minimized over \( \{g_i\}_{i=1}^N \in \mathbb{R}_+^N \):

\[
\mathcal{L}(g, \lambda, \kappa, \mu) = \sum_{i=1}^N g_i v_i^2 \nu + \lambda - \lambda \sum_{i=1}^N g_i \\
+ \sum_{i=1}^{N-1} \left[ -\epsilon \kappa_i \frac{g_i + g_{i+1}}{2} - \frac{\kappa_i g_{i+1} - g_i}{\nu} \right] \\
+ \sum_{i=1}^{N-1} \left[ \mu_i \frac{g_{i+1} - g_i}{\nu} - \epsilon \mu_i \frac{g_i + g_{i+1}}{2} \right]
\]

Thus, the dual problem is the following:

maximize \( \lambda \) subject to

\[
\epsilon \frac{\kappa_{i-1} + \kappa_i}{2} + \epsilon \frac{\mu_{i-1} + \mu_i}{2} - \frac{\kappa_i - \kappa_{i-1}}{\nu} \\
+ \frac{\mu_i - \mu_{i-1}}{\nu} \leq v_i^2 \nu - \lambda \nu_i, \forall i \in \{2, \ldots, N-1\},
\]

\[
v_1^2 \nu - \lambda \nu - \epsilon \frac{\kappa_1 + \mu_1}{2} - \frac{\mu_1 - \kappa_1}{\nu} \geq 0,
\]

\[
v_N^2 \nu - \lambda \nu - \epsilon \frac{\kappa_{N-1} + \mu_{N-1}}{2} \geq 0,
\]

\[
\kappa_i \geq 0 \text{ and } \mu_i \geq 0, \quad \forall i \in \{1, \ldots, N\}
\]

Complementary slackness of the primal problem suggests that, for each \( i \), either \( \kappa_i = 0 \) or \( \mu_i = 0 \). Therefore, we seek dual feasible solutions such that \( \eta_i = \mu_i - \kappa_i \) and \( \eta_i = \mu_i + \kappa_i \):

maximize \( \lambda \) subject to

\[
\epsilon \frac{\eta_{i-1} + |\eta_i|}{2} + \frac{\eta_i - \eta_{i-1}}{\nu} \leq v_i^2 \nu - \lambda \nu_i, \forall i \in \{2, \ldots, N-1\},
\]

\[
v_1^2 \nu - \lambda \nu - \frac{\eta_1}{\nu} \geq 0,
\]

\[
v_N^2 \nu - \lambda \nu - \frac{\eta_{N-1}}{\nu} \geq 0.
\]

We first set \( N = \frac{2M}{\nu} + 1 \) and let \( M \to \infty \) and, then, let \( \nu \to 0 \). The discretized dual problem convergences to the continuous one:

maximize \( \lambda \) subject to

\[
\epsilon \frac{\eta_{i-1} + |\eta_i|}{2} + \frac{\eta_i - \eta_{i-1}}{\nu} \leq v_i^2 \nu - \lambda \nu_i, \forall i \in \{2, \ldots, N-1\},
\]

\[
v_1^2 \nu - \lambda \nu - \frac{\eta_1}{\nu} \geq 0,
\]

\[
v_N^2 \nu - \lambda \nu - \frac{\eta_N}{\nu} \geq 0.
\]

The last step of the proof includes building a feasible dual solution for \( \lambda = \frac{2-\delta}{\nu} \), for small, positive values of \( \delta \). Specifically, we fix \( \lambda = \frac{2-\delta}{\nu} \) and solve the initial value problem:

\[
\eta'(v) + \epsilon |\eta(v)| = v^2 - \lambda, \quad \text{and } \eta(0) = 0
\]

Existence and uniqueness of solutions for the initial value problem [19] implies that the unique solution only needs to be checked that it satisfy the boundary constraints. Some technical analysis proves that, for small and positive values of \( \delta \), the solution \( \eta \) to the initial value problem [19] indeed satisfies the constraints:

\[
\lim_{v \to -\infty} \eta(v) \geq 0 \quad \text{and} \quad \lim_{v \to +\infty} \eta(v) \leq 0
\]

Due to symmetry, we focus only on the case of \( v \geq 0 \). Table I summarizes the signs of \( \eta \) and its derivatives. Specifically, the solution \( \eta \) is negative until \( \hat{v}_3 \). While \( \eta \) remains negative, it satisfies the initial value problem:

\[
\eta'(v) - \epsilon |\eta(v)| = v^2 - \lambda \quad \text{and} \quad \eta(0) = 0
\]

The single root of the second derivative is analytically computed:

\[
\hat{v}_1 = \frac{\ln 2 - \ln \delta}{\epsilon}
\]

At \( \hat{v}_3 \), the dual function \( \eta \) becomes positive and satisfies the initial value problem [20]:

\[
\eta'(v) + \epsilon |\eta(v)| = v^2 - \lambda \quad \text{and} \quad \eta(\hat{v}_3) = 0
\]

The value \( \hat{v}_3 \) can become arbitrarily large. Indeed, it holds that \( \hat{v}_3 \geq \hat{v}_1 \) and, for small enough values of \( \delta \), \( \hat{v}_3 \) can become as large as needed. Therefore, for small enough values of \( \delta \), the derivative of Equation [20] remains positive:

\[
\eta'(v) = \epsilon v(v - 1) + \epsilon (v_3 - v)(\delta - 2v_3\epsilon + v_3^2\epsilon^2) \geq 0,
\]

for \( v \geq \hat{v}_3 \).

The cost of the constructed dual feasible solution is \( \lambda = \frac{2-\delta}{\nu} \) and can be made as close to the cost of the Laplace distribution. Weak duality completes the proof.

Remark 2: For \( \lambda = \frac{2}{\nu} \), we consider the dual solution \( \eta(v) = -\frac{1}{v^2} v(\epsilon |v| + 2) \) which satisfies the differential equation. However, it fails to satisfy the boundary conditions since it quadratically explodes. Instead, for \( \lambda > \frac{2}{\nu} \), the dual feasible explodes exponentially. Despite the qualitative difference between the two cases, they are both infeasible.

Fig. 3: The dual solution \( \eta \) for small values of \( \delta \). The function \( \eta \) changes curvature at \( \hat{v}_1 \), becomes increasing at \( \hat{v}_2 \), and is zero at \( \hat{v}_3 \). For small values of \( \delta \), once \( \eta \) becomes positive, it remains increasing and, thus, positive.

| \( v \) | 0 | \( v_1 \) | \( v_2 \) | \( v_3 \) |
|---|---|---|---|---|
| \( \eta'' \) | 0 | 0 | 0 | 0 |
| \( \eta' \) | 0 | 0 | 0 | 0 |
| \( \eta \) | 0 | 0 | 0 | 0 |

TABLE I: Elementary analysis on the behaviour of function \( \eta(v) \) for small and positive values of \( \delta \).