

List Privacy Under Function Recoverability

Ajaykrishnan Nageswaran^{ID} and Prakash Narayan^{ID}, *Life Fellow, IEEE*

Abstract—For a given function of user data, a querier must recover with at least a prescribed probability, the value of the function based on a user-provided query response. Subject to this requirement, the user forms the query response so as to minimize the likelihood of the querier guessing a list of prescribed size to which the data value belongs based on the query response. We obtain a general converse upper bound for maximum list privacy. This bound is shown to be tight for the case of a binary-valued function through an explicit achievability scheme that involves an add-noise query response.

Index Terms—Add-noise privacy mechanism, data privacy, function computation, list privacy, query response, recoverability.

I. INTRODUCTION

A (LEGITIMATE) user's data is depicted by a finite-valued random variable (rv) with known probability mass function (pmf). A querier wishes to compute a given function of the data from a query response provided by the user that is a suitably randomized version of the data. The user fashions the query response so as to enable the querier to recover from it the function value with a prescribed accuracy while maximizing “list privacy” of the data. List privacy entails minimizing the likelihood of the querier guessing a list of prescribed size to which the data value belongs based on the query response.

For example, in a movie-streaming application where a user requests a particular movie (data), the identity of that movie is protected, say, by end-to-end encryption. However, the server application could still be interested in the genre of movies that are being streamed (list), which the user wishes to be kept private. The movie requested plays the role of user data, and the server application compiles an estimated list of movies sharing the same genre as the movie. This list should not include the user's movie choice. In another instance, a list of call detail records (list) of multiple users is collected, for example, through a phone records sweep. Then information concerning an individual user (data) needs to be protected, but could be compromised upon whittling down the list using other available information such as phone area codes. In this example, the individual user information constitutes user data, and the call detail records form the list in which the user data should not be contained.

Manuscript received 11 July 2023; revised 13 June 2024; accepted 23 June 2024. Date of publication 1 July 2024; date of current version 20 August 2024. This work was supported by the U.S. National Science Foundation under Grant CCF 1527354. An earlier version of this paper was presented in part at the 2019 International Symposium on Information Theory (DOI: 10.1109/ISIT.2019.8849548). (Corresponding author: Prakash Narayan.)

Ajaykrishnan Nageswaran was with the Department of Electrical and Computer Engineering and the Institute for Systems Research, University of Maryland, College Park, MD 20742 USA. He is now with SandboxAQ, Tarrytown, NY 10591 USA (e-mail: ajaykrishnan.n@gmail.com).

Prakash Narayan is with the Department of Electrical and Computer Engineering and the Institute for Systems Research, University of Maryland, College Park, MD 20742 USA (e-mail: prakash@umd.edu).

Communicated by L. Lai, Associate Editor for Signal Processing and Source Coding.

Digital Object Identifier 10.1109/TIT.2024.3420892

Our contributions, which represent a continuation of our earlier work concerning *data privacy* [15], [16], are as follows. In our formulation, the user forms a query response from which the querier must recover the function value with probability at least ρ , $0 \leq \rho \leq 1$. Under this requirement, we introduce the notion of *list privacy* that is a generalization of data privacy in [15] and [16]. List privacy is measured by the probability that the user data is not contained in a list of prescribed size formed by the querier based on the query response. In fact, list privacy is a more stringent notion than a certain level of data privacy; and, as will be seen below ensuring list privacy for the user guarantees at least the same level of data privacy. We derive a general converse upper bound for maximum list privacy. For the special case of a binary-valued function, the mentioned upper bound is shown to be tight through an achievability scheme based on an explicit query response. A key theoretical insight is described in the second paragraph of Section III below.

A notion of list privacy – in an asymptotic rate-distortion framework – has been considered earlier in a cryptographic context, for instance, in [19]. In [19], a new concept of information-theoretic secrecy is studied in the Shannon cipher system setting where the eavesdropper produces a list of reconstruction sequences, and secrecy is measured by the minimum distortion over the entire list. Of a different nature, our approach is in the spirit of prior works [9], [10], [12], [18], [20] that deal with information leakage of a user's private data with associated nonprivate correlated data. A randomized version of the nonprivate data is released publicly under a constraint on the expected distortion between the nonprivate and public data. The public data is designed such that it minimizes information leakage, which is measured by the mutual information between public and private data, under said distortion constraint. These works are based on principles of rate distortion theory.

In a related data privacy model in [1] and [3], maximum a posteriori (MAP) estimates of private and nonprivate data, that are digital, are formed on the basis of randomized public versions of the latter. The private, nonprivate and public data are assumed to form a Markov chain. Under a constraint on the probability of estimating correctly the private data, mechanisms are sought for said randomization so as to maximize correct MAP estimation of the nonprivate data.

In data privacy, an important movement that has commanded dominant attention over the years is differential privacy, introduced in [4] and [5] and explored further in [2], [11], [13], and [14] among others. Consider a data vector that represents multiple users' data. The notion of differential privacy stipulates that altering a data vector slightly leads only to a near-imperceptible change in the corresponding probability distribution of the output of the data release mechanism, which is a randomized function of the data vector. Upon imposing a differential privacy constraint, there exists a large body of work that seeks to maximize function recoverability by minimizing a discrepancy cost between function value and randomized

query response, a representative sample is [6], [7], [8], [21]. In contrast, our work maximizes privacy under a constraint on recoverability. Also, see [21] for data privacy methods other than differential privacy.

Our model for ρ -recoverable function computation with associated list privacy is described in Section II. List privacy is characterized in Section III and Section IV contains a closing discussion.

II. PRELIMINARIES

Let a (legitimate) user's data be represented by a rv X taking values in a finite set $\mathcal{X}$ with $|\mathcal{X}| = r \geq 2$, say, and of known pmf P_X with $P_X(x) > 0$, $x \in \mathcal{X}$. We shall consider throughout a given mapping $f: \mathcal{X} \rightarrow \mathcal{Z} = \{0, 1, \dots, k-1\}$, $2 \leq k \leq r$. Let f^{-1} denote the inverse image of f , with $f^{-1}(i) \triangleq \{x \in \mathcal{X} : f(x) = i\}$, $i \in \mathcal{Z}$. For a realization $X = x$ in $\mathcal{X}$, a querier – who does not know x – wishes to compute $f(x)$ from a *query response* (QR) $F(x)$ provided by the user, where $F(x)$ is a rv with values in $\mathcal{Z}$. A QR must satisfy the following recoverability condition.

Definition 1: Given $0 \leq \rho \leq 1$, a QR $F(X)$ is ρ -recoverable if

$$P(F(X) = f(x) | X = x) \geq \rho, \quad x \in \mathcal{X}. \quad (1)$$

Condition (1) can be written equivalently in terms of a stochastic matrix $W: \mathcal{X} \rightarrow \mathcal{Z}$ with the requirement

$$W(f(x)|x) \geq \rho, \quad x \in \mathcal{X} \quad (2)$$

which, too, will constitute a ρ -recoverable QR. Such a ρ -recoverable $F(X)$ or W will be termed ρ -QR. Note that ρ -recoverability in (1), (2) does not depend on P_X .

In order to give additional teeth to our notion of privacy, we assume conservatively that the querier knows the pmf P_X and the ρ -QR F or W .

Definition 2: Let $\mathcal{L}_l$ be the set of all l -sized subsets of $\mathcal{X}$, $1 \leq l < r$. For a given l , $1 \leq l < r$, the (l) -list privacy of a ρ -QR $F(X)$ or W satisfying (1) or (2) is

$$\pi_\rho^{(l)}(F) = \pi_\rho^{(l)}(W) \triangleq \min_g P(X \notin g(F(X))), \quad (3)$$

where the minimum is over all estimators $g: \mathcal{Z} \rightarrow \mathcal{L}_l$. The minimum in (3) is attained by a MAP estimator

$$\begin{aligned} g_{MAP(W)}^{(l)}(i) &= \arg \max_{L \in \mathcal{L}_l} P(X \in L, F(X) = i) \\ &= \arg \max_{L \in \mathcal{L}_l} \sum_{x \in L} P_X(x) W(i|x), \quad i \in \mathcal{Z}. \end{aligned} \quad (4)$$

Ties in (4) are broken arbitrarily. For $0 \leq \rho \leq 1$, the maximum list privacy that can be attained by a ρ -QR is termed *list ρ -privacy* and denoted by $\pi^{(l)}(\rho)$, i.e.,

$$\pi^{(l)}(\rho) \triangleq \max_{W: W(f(x)|x) \geq \rho} \pi_\rho^{(l)}(W).$$

Our objective is to characterize list ρ -privacy, and identify explicitly ρ -QRs that achieve them, $0 \leq \rho \leq 1$. This objective is met below in part for $\pi^{(l)}(\rho)$.

Remark: Our earlier works [15], [16] were concerned primarily with privacy for the data X . The associated concept of ρ -privacy $\pi(\rho)$ for X is a special case of list ρ -privacy $\pi^{(l)}(\rho)$ for list size $l = 1$. Clearly, list privacy is a more stringent notion than (data) privacy since $\pi^{(l)}(\rho) \leq \pi(\rho)$. Also, for $1 \leq l' < l < r$, $\pi^{(l)}(\rho) \leq \pi^{(l')}(\rho)$.

III. LIST ρ -PRIVACY

Our characterization of list ρ -privacy $\pi^{(l)}(\rho)$, $0 \leq \rho \leq 1$, is partial. We provide an upper bound for $\pi^{(l)}(\rho)$, and an achievability proof for the special case of a binary-valued mapping $f: \mathcal{X} \rightarrow \mathcal{Z} = \{0, 1\}$. A general achievability proof is not yet in hand.

Our first main result is a general upper bound for $\pi^{(l)}(\rho)$, $0 \leq \rho \leq 1$. This upper bound below is guided by the following heuristics. When $\rho = 0$, the ρ -QR $F(X)$ gives no actionable information to the querier. Therefore, the querier's best list estimate consists of the l largest P_X -probability elements of the data X in $\mathcal{X}$, and the corresponding list estimation error probability is $\pi^{(l)}(0)$. The other extreme of $\rho = 1$ corresponds to the querier having a full knowledge of $f(X)$. Then, for $f(X) = i$ in $\mathcal{Z}$, the best list estimate for the querier will contain the largest $\min\{l, |f^{-1}(i)|\}$ P_X -probability elements in the subset $f^{-1}(i)$ of $\mathcal{X}$. For any intermediate value of ρ , the querier's optimal choice will be a suitable combination of these two extremes. In other words, the querier's best list estimate will consist of a mix of the highest P_X -probability elements in $\mathcal{X}$ and the highest P_X -probability elements in $f^{-1}(i)$, for $F(X) = i$ in $\mathcal{Z}$; and as ρ increases, the relative size of the latter will increase while the former diminishes.

Specifically, for any $A \subseteq \mathcal{X}$, we denote by $[A]_t$ the set of t largest P_X -probability elements in A , $0 \leq t \leq |A| \leq r$; in particular, $[A]_0 = \emptyset$ and $L_t^* \triangleq [\mathcal{X}]_t$ is the set of t largest P_X -probability elements in $\mathcal{X}$. Define

$$\begin{aligned} \Lambda_\rho &\triangleq \arg \max_{\substack{\Lambda \subseteq \mathcal{X}: \\ 0 \leq |\Lambda| \leq l}} \\ &\left[P_X(\Lambda) + \rho \sum_{i \in \mathcal{Z}} P_X \left([f^{-1}(i) \setminus \Lambda]_{\min\{l-|\Lambda|, |f^{-1}(i) \setminus \Lambda|\}} \right) \right], \\ &0 \leq \rho \leq 1. \end{aligned} \quad (5)$$

Theorem 1: (i) For $0 \leq \rho \leq 1/k$,

$$\pi^{(l)}(\rho) = 1 - P_X(L_l^*). \quad (6)$$

(ii) For $\rho = 1$,

$$\pi^{(l)}(1) = 1 - \sum_{i \in \mathcal{Z}} P_X \left([f^{-1}(i)]_{\min\{l, |f^{-1}(i)|\}} \right). \quad (7)$$

(iii) For $0 \leq \rho \leq 1$, $\pi^{(l)}(\rho)$ is bounded above according to

$$\begin{aligned} \pi^{(l)}(\rho) &\leq \pi_u^{(l)}(\rho) \triangleq 1 - \left[P_X(\Lambda_\rho) + \right. \\ &\left. \rho \sum_{i \in \mathcal{Z}} P_X \left([f^{-1}(i) \setminus \Lambda_\rho]_{\min\{l-|\Lambda_\rho|, |f^{-1}(i) \setminus \Lambda_\rho|\}} \right) \right]. \end{aligned} \quad (8)$$

Remarks:

- (i) In the (uninteresting) regime of low ρ , specifically $0 \leq \rho \leq 1/k$, Theorem 1(i) shows that the ρ -QR $F(X)$ is useless for the querier whose best estimate of a list is L_l^* , i.e., the list of l -largest P_X -probability elements in $\mathcal{X}$.
- (ii) For $\rho = 1$, when the querier has full knowledge of $f(X)$, say $f(X) = i$ in $\mathcal{Z}$, the querier's best list estimate L_l will contain $[f^{-1}(i)]_{\min\{l, |f^{-1}(i)|\}}$. Theorem 1(ii) characterizes the corresponding ρ -privacy $\pi^{(l)}(1)$.

- (iii) As described above, the form of $\pi_u^{(l)}(\rho)$ in (8), (5) affords the following interpretation for the querier's best list estimate: For any intermediate value of ρ , the expression in (8) captures a tradeoff between the extremes in Remarks (i), (ii).
- (iv) The maximizing $\Lambda = \Lambda_\rho$ in (5) need not be unique.
- (v) In the right-side of (8), $\pi_u^{(l)}(\rho)$ is piecewise affine in $\rho \in [0, 1]$. See, for example, Fig. 1.
- (vi) For $l = 1$,

$$\pi_u^{(l)}(\rho) = 1 - \max \left\{ \max_{x \in \mathcal{X}} P_X(x), \rho \sum_{i \in \mathcal{Z}} \max_{x \in f^{-1}(i)} P_X(x) \right\}$$

which, by [16, Theorem 2] equals ρ -privacy $\pi(\rho)$. Thus, Theorem 1 is tight for $l = 1$.

For the special case of binary-valued functions $f : \mathcal{X} \rightarrow \mathcal{Z} = \{0, 1\}$, the upper bound in Theorem 1(iii) is tight. This is shown by identifying a suitable ρ -QR that achieves said bound.

A special form of ρ -QR, termed add-noise ρ -QR in [16, Definition 2], will be pertinent. An *add-noise* ρ -QR $F(X)$ is of the form

$$F(X) = f(X) + N \pmod{k} \quad (9)$$

where N is a $\mathcal{Z}$ -valued rv that satisfies

$$N \text{ --- } f(X) \text{ --- } X \quad (10)$$

whereby readily implying

$$X \text{ --- } f(X) \text{ --- } F(X). \quad (11)$$

As shown in [16, Lemma 1], such an add-noise privacy mechanism corresponds to a stochastic matrix $W : \mathcal{X} \rightarrow \mathcal{Z}$ with identical rows for all $x \in f^{-1}(i)$, $i \in \mathcal{Z}$.

Theorem 2: For $f : \mathcal{X} \rightarrow \mathcal{Z} = \{0, 1\}$, it holds that list ρ -privacy is

$$\pi^{(l)}(\rho) = \pi_u^{(l)}(\rho) = 1 - \left[P_X(\Lambda_\rho) + \rho \sum_{i \in \{0,1\}} P_X \left([f^{-1}(i) \setminus \Lambda_\rho]_{l-|\Lambda_\rho|} \right) \right], \quad 0 \leq \rho \leq 1, \quad (12)$$

and is achieved by an add-noise ρ -QR.

Remark: As noted below in the proof of Theorem 2, the minimum in (8) is attained by $l - |\Lambda_\rho|$.

Example: This example illustrates the remark at the end of Section II. Let X be a $\{0, 1, 2, 3\}$ -valued rv with uniform pmf P_X . Consider the mapping $f : \{0, 1, 2, 3\} \rightarrow \{0, 1\}$ with

$$f(0) = f(1) = 0, \quad f(2) = f(3) = 1.$$

By Remark (vi) after Theorem 1 above,

$$\pi(\rho) = \pi^{(1)}(\rho) = 1 - \max\{0.25, 0.5\rho\}, \quad 0 \leq \rho \leq 1.$$

Next, in (5), we have

$$\Lambda_\rho = \arg \max_{\substack{\Lambda \subset \mathcal{X}: \\ 0 \leq |\Lambda| \leq l}} \left[0.25 |\Lambda| + 0.25 \rho \sum_{i \in \{0,1\}} \min\{l - |\Lambda|, |f^{-1}(i) \setminus \Lambda|\} \right],$$

$$0 \leq \rho \leq 1,$$

and so by Theorem 2,

$$\pi^{(2)}(\rho) = 1 - \max\{0.5, \rho\}, \quad 0 \leq \rho \leq 1,$$

and

$$\pi^{(3)}(\rho) = 1 - \max\{0.75, 0.5 + 0.5\rho\}, \quad 0 \leq \rho \leq 1.$$

Thus, for $0 \leq \rho < 1$,

$$\pi^{(1)}(\rho) > \pi^{(2)}(\rho) > \pi^{(3)}(\rho) > \pi^{(4)}(\rho) = 0,$$

where the last equality is obvious. ■

The following technical lemma, whose proof is relegated to Appendix, states properties of Λ_ρ and $\pi_u^{(l)}(\rho)$ in (5), (8) of pertinence to the proof of Theorem 2.

Lemma 3: (Properties of Λ_ρ and $\pi_u^{(l)}(\rho)$ in (5), (8), (12))

- (i) $\Lambda_\rho = \bigcup_{i \in \mathcal{Z}} (\Lambda_\rho \cap f^{-1}(i)) = \bigcup_{i \in \mathcal{Z}} [f^{-1}(i)]_{|\Lambda_\rho \cap f^{-1}(i)|}$, i.e., $\Lambda_\rho \cap f^{-1}(i)$ consists of $|\Lambda_\rho \cap f^{-1}(i)|$ -largest P_X -probability elements in $f^{-1}(i)$, $i \in \mathcal{Z}$.
- (ii) For $f : \mathcal{X} \rightarrow \mathcal{Z} = \{0, 1\}$, Λ_ρ satisfies

$$l - |\Lambda_\rho| \leq |f^{-1}(i) \setminus \Lambda_\rho|, \quad i \in \{0, 1\}. \quad (13)$$

- (iii) $\pi_u^{(l)}(\rho)$ in (5), (8) is piecewise affine, continuous and nonincreasing in $\rho \in [0, 1]$, with

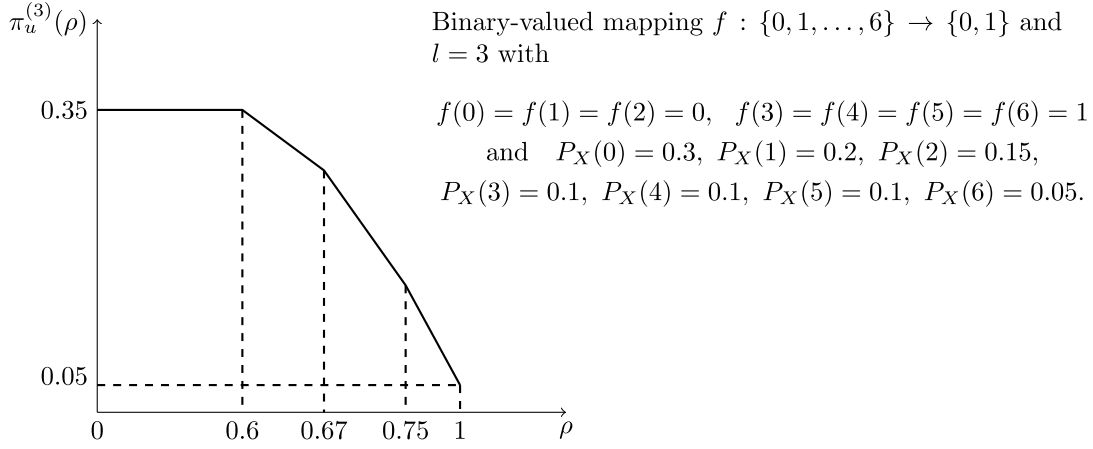
$$\begin{aligned} \pi_u^{(l)}(0) &= 1 - P_X(L_l^*), \\ \pi_u^{(l)}(1) &= 1 - \sum_{i \in \mathcal{Z}} P_X \left([f^{-1}(i)]_{\min\{l, |f^{-1}(i)|\}} \right). \end{aligned} \quad (14)$$

- (iv) $|\Lambda_\rho|$ is nonincreasing in ρ , $0 \leq \rho \leq 1$, with $|\Lambda_0| = l$ and $0 \leq |\Lambda_1| \leq \max\{0, l - \min_{i \in \mathcal{Z}} |f^{-1}(i)|\}$.
- (v) $|\Lambda_\rho|$ is piecewise constant in $0 \leq \rho \leq 1$ with $|\Lambda_\rho| = l - j$ for $\rho \in [\rho_j, \rho_{j+1}]$, $0 \leq j \leq l$, where $\rho_0 = 0 < \rho_1 \leq \dots \leq \rho_l \leq \rho_{l+1} = 1$; and ρ_j , $j = 1, \dots, l$, is the solution to

$$\begin{aligned} & \max_{\substack{\Lambda \subset \mathcal{X}: \\ |\Lambda| = l-j+1}} \left[P_X(\Lambda) \right. \\ & \quad \left. + \rho \sum_{i \in \mathcal{Z}} P_X \left([f^{-1}(i) \setminus \Lambda]_{\min\{j-1, |f^{-1}(i) \setminus \Lambda|\}} \right) \right] \\ &= \max_{\substack{\Lambda' \subset \mathcal{X}: \\ |\Lambda'| = l-j}} \left[P_X(\Lambda') \right. \\ & \quad \left. + \rho \sum_{i \in \mathcal{Z}} P_X \left([f^{-1}(i) \setminus \Lambda']_{\min\{j, |f^{-1}(i) \setminus \Lambda'|\}} \right) \right]. \end{aligned} \quad (15)$$

Proof of Theorem 1: (i) For every ρ -QR $W : \mathcal{X} \rightarrow \mathcal{Z}$ in (2),

$$\begin{aligned} 1 - \pi_\rho^{(l)}(W) &= P \left(X \in g_{MAP(W)}^{(l)}(F(X)) \right) \\ &= \sum_{i \in \mathcal{Z}} P \left(X \in g_{MAP(W)}^{(l)}(F(X)), F(X) = i \right) \\ &= \sum_{i \in \mathcal{Z}} \max_{L \in \mathcal{L}_l} P(X \in L, F(X) = i) \\ &= \sum_{i \in \mathcal{Z}} \max_{L \in \mathcal{L}_l} \sum_{x \in L} P_X(x) W(i|x) \end{aligned} \quad (16)$$

Fig. 1. $\pi_u^{(3)}(\rho)$ vs. ρ .

$$\begin{aligned} &\geq \sum_{i \in \mathcal{Z}} \sum_{x \in L_i^*} P_X(x) W(i|x) \\ &= \sum_{x \in L_i^*} P_X(x) \sum_{i \in \mathcal{Z}} W(i|x) = P_X(L_i^*), \end{aligned}$$

where the inequality above is by choosing $L = L_i^*$ in (16). Therefore,

$$\pi^{(l)}(\rho) \leq 1 - P_X(L_i^*), \quad 0 \leq \rho \leq 1. \quad (17)$$

The upper bound in (17) can be achieved by a ρ -QR $W_0 : \mathcal{X} \rightarrow \mathcal{Z}$, $0 \leq \rho \leq 1/k$, given by

$$W_0(i|x) = \frac{1}{k}, \quad i \in \mathcal{Z}, x \in \mathcal{X}.$$

Using (16),

$$\begin{aligned} \pi_\rho^{(l)}(W_0) &= 1 - \sum_{i \in \mathcal{Z}} \max_{L \in \mathcal{L}_l} \sum_{x \in L} P_X(x) W(i|x) \\ &= 1 - \sum_{i \in \mathcal{Z}} \max_{L \in \mathcal{L}_l} \sum_{x \in L} P_X(x) \frac{1}{k} = 1 - P_X(L_i^*), \end{aligned}$$

which along with (17) yields (6).

(ii) For $\rho = 1$, the only feasible ρ -QR is $W_1 : \mathcal{X} \rightarrow \mathcal{Z}$ given by

$$W_1(i|x) = \begin{cases} 1, & x \in f^{-1}(i), i \in \mathcal{Z} \\ 0, & \text{otherwise.} \end{cases}$$

Then

$$\begin{aligned} 1 - \pi(1) &= 1 - \pi_1^{(l)}(W_1) \\ &= \sum_{i \in \mathcal{Z}} \max_{L \in \mathcal{L}_l} \sum_{x \in L} P_X(x) W_1(i|x), \quad \text{by (16)} \\ &= \sum_{i \in \mathcal{Z}} \max_{L \in \mathcal{L}_l} \sum_{x \in L} P_X(x) \mathbb{1}(i = f(x)) \\ &= \sum_{i \in \mathcal{Z}} P_X([f^{-1}(i)]_{\min\{l, |f^{-1}(i)|\}}), \end{aligned}$$

which gives (7).

(iii) By (16), for every ρ -QR $W : \mathcal{X} \rightarrow \mathcal{Z}$ in (2),

$$\begin{aligned} 1 - \pi_\rho^{(l)}(W) &= \sum_{i \in \mathcal{Z}} \max_{L \in \mathcal{L}_l} \sum_{x \in L} P_X(x) W(i|x) \end{aligned} \quad (18)$$

$$\begin{aligned} &\geq \sum_{i \in \mathcal{Z}} \max_{\substack{\Lambda \subset \mathcal{X}: \\ 0 \leq |\Lambda| \leq l}} \sum_{x \in \Lambda \cup [f^{-1}(i) \setminus \Lambda]_{\min\{l-|\Lambda|, |f^{-1}(i) \setminus \Lambda|\}}} P_X(x) W(i|x) \\ &= \sum_{i \in \mathcal{Z}} \max_{\substack{\Lambda \subset \mathcal{X}: \\ 0 \leq |\Lambda| \leq l}} \left[\sum_{x \in \Lambda} P_X(x) W(i|x) + \right. \\ &\quad \left. \sum_{x \in [f^{-1}(i) \setminus \Lambda]_{\min\{l-|\Lambda|, |f^{-1}(i) \setminus \Lambda|\}}} P_X(x) W(i|x) \right] \\ &\geq \max_{\substack{\Lambda \subset \mathcal{X}: \\ 0 \leq |\Lambda| \leq l}} \sum_{i \in \mathcal{Z}} \left[\sum_{x \in \Lambda} P_X(x) W(i|x) + \right. \\ &\quad \left. \sum_{x \in [f^{-1}(i) \setminus \Lambda]_{\min\{l-|\Lambda|, |f^{-1}(i) \setminus \Lambda|\}}} P_X(x) W(i|x) \right] \\ &\geq \max_{\substack{\Lambda \subset \mathcal{X}: \\ 0 \leq |\Lambda| \leq l}} \left[P_X(\Lambda) + \right. \\ &\quad \left. \rho \sum_{i \in \mathcal{Z}} P_X([f^{-1}(i) \setminus \Lambda]_{\min\{l-|\Lambda|, |f^{-1}(i) \setminus \Lambda|\}}) \right] \end{aligned} \quad (19)$$

which yields (8). $\blacksquare$

Proof of Theorem 2: For $f : \mathcal{X} \rightarrow \{0, 1\}$, we first note by Lemma 3(ii) that $\pi_u^{(l)}(\rho)$ in (8) simplifies to the form of $\pi_u^{(l)}(\rho)$ in the right-side of (12).

Next, we present a ρ -QR that achieves the right-side of (12). In particular, this ρ -QR will involve $0 < \rho_1 < 1$ where, by Lemma 3(v), with $j = 1$ in (15), $\rho = \rho_1$ is the solution to

$$P_X(L_i^*) = \max_{\substack{\Lambda' \subset \mathcal{X}: \\ |\Lambda'| = l-1}} \left[P_X(\Lambda') + \rho \sum_{i \in \mathcal{Z}} P_X([f^{-1}(i) \setminus \Lambda']_1) \right],$$

observing that $\Lambda = L_i^*$ is the maximizer in the left-side of (15). Furthermore, the right-side of (12) simplifies for $0 \leq \rho \leq \rho_1$. Specifically, by Lemma 3(v), $|\Lambda_\rho| = l$, $0 \leq \rho \leq \rho_1$, and by the observation above $\Lambda_\rho = L_i^*$, $0 \leq \rho \leq \rho_1$. Hence, by the right-side of (12),

$$\pi_u^{(l)}(\rho) = 1 - P_X(L_i^*), \quad 0 \leq \rho \leq \rho_1. \quad (20)$$

Clearly, by Theorem 1(i), $\rho_1 \geq 1/k$. Consider the add-noise ρ -QR (9)-(11)

$$F(X) = f(X) + N \pmod{2}$$

with

$$P(N = 0 | f(X) = i) = \max\{\rho, \rho_1\}, \quad i \in \{0, 1\}$$

where, in this instance, N is independent of $f(X)$. The ρ -QR above corresponds to $W_o : \mathcal{X} \rightarrow \{0, 1\}$ given by

$$\begin{aligned} W_o(i|x) &= \begin{cases} \max\{\rho, \rho_1\}, & i = f(x) \\ 1 - \max\{\rho, \rho_1\}, & i \neq f(x), \end{cases} \quad x \in \mathcal{X}, \quad i \in \{0, 1\}. \end{aligned} \quad (21)$$

The list privacy afforded by W_o is

$$\begin{aligned} \pi_\rho^{(l)}(W_o) &= 1 - P\left(X \in g_{MAP(W_o)}^{(l)}(F(X))\right) \\ &= 1 - \sum_{i \in \{0, 1\}} \max_{L \in \mathcal{L}_l} \sum_{x \in L} P_X(x) W_o(i|x). \end{aligned} \quad (22)$$

The proof of Theorem 2 is completed upon showing that $\pi_\rho^{(l)}(W_o)$ above equals the right-side of (12) for $0 \leq \rho \leq 1$ (and, in particular, the right-side of (20) for $0 \leq \rho \leq \rho_1$). This is done in the following four steps.

1. Using Lemma 3(i), (ii), we identify the set that attains the maximum in (22) for i in $\{0, 1\}$.
2. We first consider the case $\rho_1 \leq \rho \leq 1$. Using the form of Λ_ρ in (5), we show that the set identified in Step 1 indeed attains the maximum in (22) for i in $\{0, 1\}$.
3. Using Steps 1 and 2, for $\rho_1 \leq \rho \leq 1$, we show that $\pi_\rho^{(l)}(W_o) = \pi_u^{(l)}(\rho)$ in (12).
4. For $0 \leq \rho < \rho_1$, using Steps 1 and 2, we show directly that $\pi_\rho^{(l)}(W_o) = \pi_u^{(l)}(\rho)$ in (12).

Step 1: With Λ_ρ as in (5), and noting by Lemma 3(ii) that $l - |\Lambda_\rho| \leq |f^{-1}(i) \setminus \Lambda_\rho|$, $i \in \{0, 1\}$, we claim that the maxima in (22) are attained by L^i , $i = 0, 1$, in $\mathcal{L}_l$ given by

$$L^i = \Lambda_\rho \cup [f^{-1}(i) \setminus \Lambda_\rho]_{l-|\Lambda_\rho|}, \quad i = 0, 1. \quad (23)$$

For any $A \subseteq \mathcal{X}$, let $[A]^i$ denote the (not necessarily unique) i th-largest P_X -probability element in A , $i = 1, \dots, |A|$. Let $|\Lambda_\rho \cap f^{-1}(i)| = a_i$, $i \in \{0, 1\}$. Using Lemma 3(i) in (23), said claim means that

$$\begin{aligned} L^1 &= [f^{-1}(1)]_{a_1+l-|\Lambda_\rho|} \cup [f^{-1}(0)]_{a_0} \\ L^0 &= [f^{-1}(1)]_{a_1} \cup [f^{-1}(0)]_{a_0+l-|\Lambda_\rho|} \end{aligned}$$

attain the maxima in (22).

Step 2: When $\rho_1 \leq \rho \leq 1$, with the choice of W_o in (21), for the maximum in (22) for $i = 1$ to be attained by L^1 , it suffices if

$$\rho P_X\left([f^{-1}(1)]^{a_1+l-|\Lambda_\rho|}\right) \geq (1 - \rho) P_X\left([f^{-1}(0)]^{a_0+1}\right) \quad (24)$$

and

$$(1 - \rho) P_X\left([f^{-1}(0)]^{a_0}\right) \geq \rho P_X\left([f^{-1}(1)]^{a_1+l-|\Lambda_\rho|+1}\right). \quad (25)$$

If $a_0 = 0$ or $a_1 + l - |\Lambda_\rho| = |f^{-1}(1)|$, then it is enough to show (24), as (25) is vacuous. If $a_0 = |f^{-1}(0)|$ or $a_1 +$

$l - |\Lambda_\rho| = 0$, then again it is adequate to show (25), as (24) is vacuous. Since Λ_ρ attains the maximum for the expression within $[\cdot]$ in (5),

$$\begin{aligned} P_X(\Lambda_\rho) + \rho \sum_{i \in \{0, 1\}} P_X\left([f^{-1}(i) \setminus \Lambda_\rho]_{l-|\Lambda_\rho|}\right) \\ \geq P_X(\Lambda) + \rho \sum_{i \in \{0, 1\}} P_X\left([f^{-1}(i) \setminus \Lambda]_{\min\{l-|\Lambda|, |f^{-1}(i) \setminus \Lambda|\}}\right), \end{aligned}$$

$$\Lambda \subset \mathcal{X}, \quad 0 \leq |\Lambda| \leq l. \quad (26)$$

By choosing $\Lambda = \Lambda_\rho \cup [f^{-1}(0)]^{a_0+1}$ in¹ (26), we get

$$\begin{aligned} P_X(\Lambda_\rho) + \rho \sum_{i \in \{0, 1\}} P_X\left([f^{-1}(i) \setminus \Lambda_\rho]_{l-|\Lambda_\rho|}\right) \\ \geq P_X(\Lambda_\rho \cup [f^{-1}(0)]^{a_0+1}) \\ + \rho \sum_{i \in \{0, 1\}} P_X\left([f^{-1}(i) \setminus (\Lambda_\rho \cup [f^{-1}(0)]^{a_0+1})]_{l-|\Lambda_\rho|-1}\right), \end{aligned}$$

which reduces to (24). Similarly, by choosing $\Lambda = \Lambda_\rho \setminus [f^{-1}(0)]^{a_0}$ in² (26), we get (25).

For establishing that the maximum in (22) for $i = 0$ is attained by L^0 , similarly it is sufficient to show that

$$\rho P_X\left([f^{-1}(0)]^{a_0+l-|\Lambda_\rho|}\right) \geq (1 - \rho) P_X\left([f^{-1}(1)]^{a_1+1}\right) \quad (27)$$

and

$$(1 - \rho) P_X\left([f^{-1}(1)]^{a_1}\right) \geq \rho P_X\left([f^{-1}(0)]^{a_0+l-|\Lambda_\rho|+1}\right). \quad (28)$$

This is done by choosing $\Lambda = \Lambda_\rho \cup [f^{-1}(1)]^{a_1+1}$ and $\Lambda = \Lambda_\rho \setminus [f^{-1}(1)]^{a_1}$ which give (27) and (28), respectively, by similar calculations as for the case $i = 1$.

Step 3: Finally, upon substituting (23) in (22), the resulting $\pi_\rho^{(l)}(W_o)$ equals the upper bound $\pi_u^{(l)}(\rho)$ in (12). This completes the proof of achievability when $\rho_1 \leq \rho \leq 1$.

Step 4: We now consider the case $0 \leq \rho < \rho_1$. Having established at $\rho = \rho_1$ that $\pi_{\rho_1}^{(l)}(W_o) = \pi_u^{(l)}(\rho_1)$, and using (20), we get $\pi_{\rho_1}^{(l)}(W_o) = \pi_u^{(l)}(\rho_1) = 1 - P_X(L_l^*)$. Then, recalling (21), for $0 \leq \rho < \rho_1$,

$$\pi_\rho^{(l)}(W_o) = \pi_{\rho_1}^{(l)}(W_o) = 1 - P_X(L_l^*) = \pi_u^{(l)}(\rho),$$

where the last equality is by (20). This completes the proof of Theorem 2. ■

Remark: Observe in the proof of Theorem 1(iii) that in obtaining the bound (19), a list of size less than l will be chosen for the second summation in the right-side of (18) if Λ_ρ is such that, for some i in $\mathcal{Z}$, it holds that $l - |\Lambda_\rho| > |f^{-1}(i) \setminus \Lambda_\rho|$. This would suggest an apparent slackness in the upper bound on $\pi(\rho)$. We provide next an example to show that this is not necessarily the case. Consider the mapping $f : \{0, 1, \dots, 4\} \rightarrow \{0, 1, 2\}$ with

$$f(0) = f(1) = 0, \quad f(2) = f(3) = 1 \quad \text{and} \quad f(4) = 2.$$

¹We know that since $\rho > \rho_1$, $|\Lambda_\rho| \leq l - 1$, and therefore, $\Lambda = \Lambda_\rho \cup [f^{-1}(0)]^{a_0+1}$ is a valid choice for Λ in (26). Also, by a straightforward calculation, $l - |\Lambda| \leq |f^{-1}(i) \setminus \Lambda|$, $i = 0, 1$.

²As noted, we only need to show (25) if $a_0 > 0$ and $a_1 + l - |\Lambda_\rho| < |f^{-1}(1)|$. Then with $\Lambda = \Lambda_\rho \setminus [f^{-1}(0)]^{a_0}$, it can be verified easily that if $a_0 > 0$ and $a_1 + l - |\Lambda_\rho| < |f^{-1}(1)|$, then $l - |\Lambda| \leq |f^{-1}(i) \setminus \Lambda|$, $i = 0, 1$.

The list size $l = 2$, and P_X is the uniform pmf on $\mathcal{X}$. By a straightforward calculation, we obtain

$$\pi_u^{(l)}(\rho) = \begin{cases} 1 - \rho, & \frac{1}{2} \leq \rho \leq 1 \\ \frac{4}{5} - \frac{3}{5}\rho, & \frac{1}{3} \leq \rho \leq \frac{1}{2} \\ \frac{3}{5}, & 0 \leq \rho \leq \frac{1}{3}. \end{cases}$$

Observe that for $1/2 \leq \rho \leq 1$, $\Lambda_\rho = \emptyset$, due to which $l - |\Lambda_\rho| = 2 > |f^{-1}(2) \setminus \Lambda_\rho| = 1$. But the ρ -QR $W : \{0, 1, \dots, 4\} \rightarrow \{0, 1, 2\}$ given by

$$W(i|x) = \begin{cases} \rho, & i \in \{0, 1, 2\}, \quad x \in f^{-1}(i) \\ 1 - \rho, & i = 0, \quad x \in \{2, 3\} \\ 1 - \rho, & i = 1, \quad x \in \{0, 1\} \\ \frac{1-\rho}{2}, & i \in \{0, 1\}, \quad x = 4 \\ 0, & \text{otherwise,} \end{cases}$$

has list privacy $1 - \rho$ for $1/2 \leq \rho \leq 1$. Therefore, for $1/2 \leq \rho \leq 1$, $\pi_u^{(l)}(\rho)$ is optimal even though $l - |\Lambda_\rho| = 2 > |f^{-1}(2) \setminus \Lambda_\rho| = 1$.

IV. DISCUSSION

Theorem 1 provides a general upper bound for list ρ -privacy that is tight for the special case of a binary-valued function. What is the exact characterization of list ρ -privacy for functions that are not binary-valued? With regard to the converse, from the derivation of $\pi_u^{(l)}(\rho)$, we get that the querier's best list estimate, based on i in $\mathcal{Z}$, has the structure that it consists of elements from the highest P_X -probability elements in $\mathcal{X}$ and the highest P_X -probability elements in $f^{-1}(i)$. This natural form of the querier list estimate suggests the optimality of $\pi_u^{(l)}(\rho)$. Hence, it promotes the conjecture that list ρ -privacy $\pi^{(l)}(\rho)$ equals $\pi_u^{(l)}(\rho)$. If true, what is the ρ -QR that attains a list privacy of $\pi_u^{(l)}(\rho)$ for functions that are not binary-valued? Our optimal ρ -QR W_o (21) for a binary-valued function involves only ρ_1 . Recalling $\rho_1, \dots, \rho_k$ from Lemma 3(v), what role, if any, will $\rho_2, \dots, \rho_k$ play in the construction of the optimal ρ -QR for functions that are not binary-valued? Further, we note in (21) that W_o corresponding to $f^{-1}(0)$ (resp. $f^{-1}(1)$) are identical. Such a W_o has the attribute that the resulting ρ -QR $F(X)$ satisfies the Markov property $X \dashv\vdash f(X) \dashv\vdash F(X)$, and is termed an "add-noise" ρ -QR in [16, Definition 2]. Will ρ -QRs, not necessarily of the add-noise type, be required for achieving list ρ -privacy in general? These questions are open.

APPENDIX PROOF OF LEMMA 3

(i) We need to show that

$$\Lambda_\rho \cap f^{-1}(i) = [f^{-1}(i)]_{|\Lambda_\rho \cap f^{-1}(i)|}, \quad i \in \mathcal{Z}. \quad (29)$$

Writing the term within $[\cdot]$ in (5) with $\Lambda = \Lambda_\rho$ as

$$\sum_{i \in \mathcal{Z}} \left[P_X \left(\underbrace{\Lambda_\rho \cap f^{-1}(i)} \right) + \rho P_X \left(\underbrace{[f^{-1}(i) \setminus \Lambda_\rho \cap f^{-1}(i)]_{\min\{l - |\Lambda_\rho|, |f^{-1}(i) \setminus \Lambda_\rho|\}}}} \right) \right]. \quad (30)$$

In (30), for each $i \in \mathcal{Z}$, focusing on the term within $[\cdot]$, if (29) is violated, there exists an element in $\underbrace{\cdot}_{\text{higher}}$ of higher

P_X -probability than the minimum P_X -probability element in $\underbrace{\cdot}_{\text{lower}}$. Swapping them would lead to a higher value of $[\cdot]$ since $\rho \leq 1$, thereby contradicting the optimality of Λ_ρ in (5). Therefore, (29) holds.

(ii) Assume

$$l - |\Lambda_\rho| > |f^{-1}(0) \setminus \Lambda_\rho| \quad (31)$$

and

$$l - |\Lambda_\rho| \leq |f^{-1}(1) \setminus \Lambda_\rho|.$$

Let

$$|\Lambda_\rho \cap f^{-1}(i)| = a_i, \quad i \in \{0, 1\},$$

which give

$$|\Lambda_\rho| = \sum_{i \in \{0, 1\}} a_i \quad (32)$$

and

$$|f^{-1}(i) \setminus \Lambda_\rho| = |f^{-1}(i)| - a_i, \quad i \in \{0, 1\}, \quad (33)$$

and using Lemma 3(i),

$$\Lambda_\rho = [f^{-1}(1)]_{a_1} \cup [f^{-1}(0)]_{a_0}. \quad (34)$$

Substituting (32), (33) in (31), we get

$$l - |f^{-1}(0)| > a_1. \quad (35)$$

Consider the set $\tilde{\Lambda}_\rho$ given by

$$\tilde{\Lambda}_\rho = [f^{-1}(1)]_{l - |f^{-1}(0)|} \cup [f^{-1}(0)]_{a_0}. \quad (36)$$

Since $l - |f^{-1}(0)| > a_1 \geq 0$, $|f^{-1}(1)| > l - |f^{-1}(0)|$ and $|\tilde{\Lambda}_\rho| = l - |f^{-1}(0)| + a_0 \leq l$, $\Lambda = \tilde{\Lambda}_\rho$ is a valid choice for the expression within $[\cdot]$ in (5). We claim that choosing $\Lambda = \tilde{\Lambda}_\rho$ gives a larger value for the expression within $[\cdot]$ in (5), thereby contradicting the optimality of Λ_ρ , and, in turn, proving that (31) cannot hold. To establish the claim above, with $\Lambda = \tilde{\Lambda}_\rho$ in the expression within $[\cdot]$ in (5), and using (34), we get

$$\begin{aligned} [\cdot] &= P_X ([f^{-1}(0)]_{a_0}) \\ &+ \rho P_X ([f^{-1}(0) \setminus [f^{-1}(0)]_{a_0}]_{|f^{-1}(0)| - a_0}) \\ &+ P_X ([f^{-1}(1)]_{a_1}) \\ &+ \rho P_X ([f^{-1}(1) \setminus [f^{-1}(1)]_{a_1}]_{l - a_1 - a_0}); \end{aligned} \quad (37)$$

and upon choosing $\Lambda = \tilde{\Lambda}_\rho$ in $[\cdot]$ in (5), and using (36), we get

$$\begin{aligned} [\cdot] &= P_X ([f^{-1}(0)]_{a_0}) \\ &+ \rho P_X ([f^{-1}(0) \setminus [f^{-1}(0)]_{a_0}]_{|f^{-1}(0)| - a_0}) \\ &+ P_X ([f^{-1}(1)]_{l - |f^{-1}(0)|}) \\ &+ \rho P_X ([f^{-1}(1) \setminus [f^{-1}(1)]_{l - |f^{-1}(0)|}]_{|f^{-1}(0)| - a_0}). \end{aligned} \quad (38)$$

Observe that in (37), (38), by (35), $[f^{-1}(1)]_{a_1} \subset [f^{-1}(1)]_{l - |f^{-1}(0)|}$, and since $\rho \leq 1$, the claim holds.

Similar arguments apply if we assume

$$l - |\Lambda_\rho| > |f^{-1}(1) \setminus \Lambda_\rho| \quad \text{and} \quad l - |\Lambda_\rho| \leq |f^{-1}(0) \setminus \Lambda_\rho|$$

or

$$l - |\Lambda_\rho| > |f^{-1}(1) \setminus \Lambda_\rho| \quad \text{and} \quad l - |\Lambda_\rho| > |f^{-1}(0) \setminus \Lambda_\rho|.$$

Therefore, (13) is true.

(iii) Consider $1 - \pi_u^{(l)}(\rho) = \max_{0 \leq l' \leq l} \alpha(\rho, l')$ where

$$\begin{aligned} \alpha(\rho, l') &= \max_{\substack{\Lambda \subset \mathcal{X}: \\ |\Lambda| = l'}} \beta(\rho, l', \Lambda) \\ \beta(\rho, l', \Lambda) &= P_X(\Lambda) \\ &\quad + \rho \sum_{i \in \mathcal{Z}} P_X \left([f^{-1}(i) \setminus \Lambda]_{\min\{l-l', |f^{-1}(i) \setminus \Lambda|\}} \right), \end{aligned}$$

where $|\Lambda| = l'$. For each fixed $0 \leq l' \leq l$ and fixed $\Lambda \subset \mathcal{X}$ with $|\Lambda| = l'$, $\beta(\rho, l', \Lambda)$ is affine and nondecreasing in ρ . Hence, $\alpha(\rho, l')$ – as the maximum of finitely many affine and nondecreasing functions in ρ – is piecewise affine, continuous and nondecreasing in ρ . In turn, $1 - \pi_u^{(l)}(\rho)$ – as the maximum of $l + 1$ such functions $\alpha(\rho, l')$ – also is piecewise affine, continuous and nondecreasing in ρ . The values of $\pi_u^{(l)}(\rho)$ at the end points $\rho = 0$ and $\rho = 1$ in (14) follow from a straightforward calculation.

(iv) For $l' = 0$, $\alpha(\rho, 0)$ is linear in ρ with $\alpha(0, 0) = 0$ and $\alpha(1, 0) = \sum_{i \in \mathcal{Z}} P_X \left([f^{-1}(i)]_{\min\{l, |f^{-1}(i)|\}} \right)$; and for $l' = l$, $\alpha(\rho, l) \equiv P_X(L^*)$. And for $0 < l' < l$, $\alpha(\rho, l')$ is piecewise affine, continuous and nondecreasing in $\rho \in [0, 1]$ as noted in the proof of (iii). Further, observe that for $0 \leq l'_1 < l'_2 \leq l$,

$$\alpha(0, l'_1) \leq \alpha(0, l'_2) \quad \text{while} \quad \alpha(1, l'_1) \geq \alpha(1, l'_2)$$

where the latter is immediate upon examining

$$\begin{aligned} \alpha(1, l') &= \\ &\max_{\substack{\Lambda \subset \mathcal{X}: \\ |\Lambda| = l'}} \left[P_X(\Lambda) + \sum_{i \in \mathcal{Z}} P_X \left([f^{-1}(i) \setminus \Lambda]_{\min\{l-l', |f^{-1}(i) \setminus \Lambda|\}} \right) \right] \end{aligned}$$

and observing that $\alpha(1, l') \leq \alpha(1, l' - 1)$, etc. The claim in (iv) follows.

(v) The claim follows readily from $|\Lambda_\rho|$ taking values in $\{0, 1, \dots, l\}$, property (iv), and ρ ranging continuously in $[0, 1]$. ■

ACKNOWLEDGMENT

The authors thank Himanshu Tyagi for a helpful discussion of data privacy [16] that motivated the concept of list privacy. They also thank two anonymous referees for their constructive suggestions which made for an improved presentation of their results.

REFERENCES

- [1] S. Asodeh, M. Diaz, F. Alajaji, and T. Linder, "Estimation efficiency under privacy constraints," *IEEE Trans. Inf. Theory*, vol. 65, no. 3, pp. 1512–1534, Mar. 2019.
- [2] R. Bassily, A. Groce, J. Katz, and A. Smith, "Coupled-world privacy: Exploiting adversarial uncertainty in statistical data privacy," *Found. Comput. Sci.*, vol. 1, pp. 439–448, Oct. 2013.
- [3] M. Diaz, H. Wang, F. P. Calmon, and L. Sankar, "On the robustness of information-theoretic privacy measures and mechanisms," *IEEE Trans. Inf. Theory*, vol. 66, no. 4, pp. 1949–1978, Apr. 2020.
- [4] N. O. Attah-Okine, "Differential privacy," in *Big Data and Differential Privacy: Analysis Strategies for Railway Track Engineering*. Cham, Switzerland: Springer, 2017, pp. 241–247.
- [5] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Theory of Cryptography*. Cham, Switzerland: Springer, 2006, pp. 265–284.
- [6] Q. Geng, W. Ding, R. Guo, and S. Kumar, "Tight analysis of privacy and utility tradeoff in approximate differential privacy," in *Proc. Int. Conf. Artif. Intell. Statist.*, 2020, pp. 89–99.
- [7] Q. Geng and P. Viswanath, "The optimal noise-adding mechanism in differential privacy," *IEEE Trans. Inf. Theory*, vol. 62, no. 2, pp. 925–951, Feb. 2016.
- [8] M. Hardt and K. Talwar, "On the geometry of differential privacy," in *Proc. 42nd ACM Symp. Theory Comput.*, Jun. 2010, pp. 705–714.
- [9] F. du Pin Calmon and N. Fawaz, "Privacy against statistical inference," in *Proc. 50th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Oct. 2012, pp. 1401–1408.
- [10] C. Huang, P. Kairouz, X. Chen, L. Sankar, and R. Rajagopal, "Context-aware generative adversarial privacy," *Entropy*, vol. 19, no. 12, p. 656, Dec. 2017.
- [11] S. P. Kasiviswanathan and A. Smith, "On the 'Semantics' of differential privacy: A Bayesian formulation," *J. Privacy Confidentiality*, vol. 6, no. 1, pp. 1–16, Jun. 2014.
- [12] A. Makhdoumi and N. Fawaz, "Privacy-utility tradeoff under statistical uncertainty," in *Proc. 51st Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Oct. 2013, pp. 1627–1634.
- [13] F. McSherry and K. Talwar, "Mechanism design via differential privacy," in *Proc. 48th Annu. IEEE Symp. Found. Comput. Sci. (FOCS)*, Oct. 2007, pp. 94–103.
- [14] I. Mironov, "Renyi differential privacy," in *Proc. IEEE 30th Comput. Secur. Found. Symp. (CSF)*, Aug. 2017, pp. 263–275, doi: 10.1109/CSF.2017.11.
- [15] A. Nageswaran and P. Narayan, "Data privacy for a ρ -recoverable function," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2018, pp. 1046–1050.
- [16] A. Nageswaran and P. Narayan, "Data privacy for a ρ -recoverable function," *IEEE Trans. Inf. Theory*, vol. 65, no. 6, pp. 3470–3488, Jun. 2019.
- [17] A. Nageswaran and P. Narayan, "Predicate privacy and list privacy for a ρ -Recoverable function," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2019, pp. 2139–2143.
- [18] L. Sankar, S. R. Rajagopalan, and H. V. Poor, "Utility-privacy tradeoffs in databases: An information-theoretic approach," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 6, pp. 838–852, Jun. 2013.
- [19] C. Schieler and P. Cuff, "The henchman problem: Measuring secrecy by the minimum distortion in a list," *IEEE Trans. Inf. Theory*, vol. 62, no. 6, pp. 3436–3450, Jun. 2016.
- [20] Y. Wang, S. Aeron, A. S. Rakin, T. Koike-Akino, and P. Moulin, "Robust machine learning via privacy/rate-distortion theory," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2021, pp. 1320–1325.
- [21] L. Wasserman and S. Zhou, "A statistical framework for differential privacy," *J. Amer. Stat. Assoc.*, vol. 105, no. 489, pp. 375–389, Mar. 2010.

Ajaykrishnan Nageswaran received the Bachelor of Technology degree in electronics and communication engineering from the National Institute of Technology Karnataka, India, in 2015, and the Ph.D. degree in electrical engineering from the Department of Electrical and Computer Engineering and the Institute for Systems Research, University of Maryland, College Park, in 2023. He is currently a Research Scientist Resident with SandboxAQ, Tarrytown, NY, USA.

Prakash Narayan (Life Fellow, IEEE) received the Bachelor of Technology degree in electrical engineering from Indian Institute of Technology, Madras, in 1976, and the M.S. degree in systems science and mathematics and the D.Sc. degree in electrical engineering from Washington University, St. Louis, MO, USA, in 1978 and 1981, respectively.

He is currently a Professor of electrical and computer engineering with the University of Maryland, College Park, with a joint appointment with the Institute for Systems Research. His research interests include network information theory, coding theory, communication theory, communication networks, statistical learning, and cryptography.