The Differential Privacy Frontier
Extended Abstract

Cynthia Dwork

Microsoft Research

Abstract. We review the definition of *differential privacy* and briefly survey a handful of very recent contributions to the differential privacy frontier.

1 Background

Differential privacy is a strong privacy guarantee for an individual's input to a (randomized) function or sequence of functions, which we call a *privacy mechanism.* Informally, the guarantee says that the behavior of the mechanism is essentially unchanged independent of whether any individual opts into or opts out of the data set. Designed for statistical analysis, for example, of health or census data, the definition protects the privacy of individuals, and small groups of individuals, while permitting very different outcomes in the case of very different data sets.

We begin by recalling some differential privacy basics. While the frontier of a vibrant area is always in flux, we will endeavor to give an impression of the state of the art by surveying a handful of extremely recent advances in the field.

Formally, The degree of privacy offered is described by a parameter, ε.

Definition 1. *A randomized function $\mathcal{K}$ gives ε-*differential privacy *if for all data sets D and D' of Hamming distance $d(D, D') \leq 1$ and all $S \subseteq Range(\mathcal{K})$,*

$$\Pr[\mathcal{K}(D) \in S] \leq e^{\varepsilon} \times \Pr[\mathcal{K}(D') \in S] \tag{1}$$

The probability is taken is over the coin tosses of $\mathcal{K}$.

The definition represents a paradigm shift: instead of a simulation-style definition, in which we compare what an adversary can learn about an individual with, versus without, access to the outputs of the privacy mechanism, differential privacy focuses on limiting the additional risk – of anything! – incurred by an individual as a consequence of opting into (or opting out of) a data set. This is no accident, as any "with vs. without access" definition is doomed to fail [5, 9]. The defintion is suited to the real world because it is a property of the mechanism alone, and has no bearing on what the consumer of information produced in a differentially private fashion might or might not know. In consequence the outputs of a differentially private mechanism preserve differential privacy independent of the information and computational power available to an adversary, now or in the future.

Two principal techniques for ensuring differential privacy have appeared, one for the case of (vectors of) real-valued outputs and the other for outputs of arbitrary types [7, 20]; the former is efficient, the latter may not be [10]. These positive results and a key precursor [11] (which used a cumbersome definition now known to imply a natural, mild relaxation of pure differential privacy and which showed that if the number of queries is sublinear in the size of the data set then privacy can be obtained "for free," *i.e.*, with noise smaller than the sampling error) have been used to obtain highly accurate differentially private solutions to a host of problems in datamining, statistics, and learning (see, *e.g.*, [2, 1, 19, 3]). A central concept is the *sensitivity* of a real-valued function mapping data sets to (vectors of) reals:

Definition 2. *Let $\mathcal{D}$ denote the space of all databases. For $f : \mathcal{D} \to R^d$, the* sensitivity *of f is*

$$\Delta f = \max_{D,D'} \|f(D) - f(D)\|_1$$

for all D, D' of distance at most 1.

Roughly speaking, real-valued data analyses that have low sensitivity permit highly accurate differentially private mechanisms [7]. The true answer is computed and Lapalacian (symmetric exponential) noise is added with variance depending on ε and the sensitivity of the query. For analyses whose outcome need not be real (it might be the choice of a color, or a set of locations, or a string), or in cases where the output is real-valued but adding noise makes no sense (the output might be a price when the data set is a collection of bids in an auction), if there is an insensitive function for evaluating the quality of an output (for example, revenue, in the case of an auction), then again high-quality outputs can be obtained in a differentially private fashion [20]. This is done using the *exponential mechanism* which, roughly speaking, weights each possible answer with a density that falls exponentially with its (in)utility, again depending on ε and also the sensitivity, this time, of the utility function[1]. Very recently Ghosh *et al.* considered the question of what it means for a privacy mechanism to be optimal [14]. Intuitively, different users may have different preconceptions before seeing the output of a privacy mechanism, and therefore two users might place different values on the same piece of information. In such a setting what sort of utility function should the mechanism employ? Using a very general notion of utility, and permitting each user to have *her own* utility function, Ghosh *et al.* show that a discretized version of the Laplace distribution used in [7] simultaneously maximizes utility for all users for the case of counting functions ("How many rows in the data set satisfy predicate P?").

[1] The addition of Laplacian noise to a real-valued output is a special case of the exponential mechanism: the (in)utility of an output is its L_1 distance from the true answer.

2 Differentially Private Synthetic Data Sets and Coresets

A series of negative results concerning privacy, says, roughly, that there is a class of queries with the property that it is blatantly non-private (allowing almost full reconstruction) if "too many" queries receive "overly accurate" responses [4, 8, 12]. These results have been viewed as saying that, in contrast to the sublinear queries work discussed above, one cannot privately answer a small polynomial number of queries, say, n^3 or even n^2, with reasonably small noise (here, n is the number of elements in the data set).

The idea of creating a *synthetic* data set whose statistics closely mirror those of the original data set, but which preserves privacy of individuals, was proposed in the statistics community as far back as 1993 [24]. However, the negative results imply that no such data set can safely provide very accurate answers to too many questions, motivating the interactive approach to private data analysis ([11] *et sequelae*). Intuitively, the advantage of the interactive approach is that only the questions actually asked receive responses, while to offer the same utility in the non-interactive approach all, or at least most, questions must receive very accurate responses, leading to blatant non-privacy.

Against this backdrop, Blum, *et al.* revisited the non-interactive case from a learning theory perspective, and challenged the above interpretation about the necessity of limiting the number of queries [3]. Let X be a universe of data items and $\mathcal{C}$ be a "concept" class consisting of efficiently computable functions $c : X \rightarrow \{0, 1\}$. Given a sufficiently large database $x \in X^n$, Blum *et al.* inefficiently, but with differential privacy, obtain a *synthetic database* that maintains approximately correct fractional counts for *all* concepts in $\mathcal{C}$. That is, letting y denote the synthetic database produced, with high probability over the choices made by the privacy mechanism, for every concept $c \in \mathcal{C}$, the fraction of elements in y that satisfy c is approximately the same as the fraction of elements in x that satisfy c.[2]

This remarkable result has rekindled interest in synthetic databases in particular and non-interactive solutions in general. When can differentially private synthetic databases be constructed efficiently? Very roughly, if either the universe X of data items or the concept class $\mathcal{C}$ is of size superpolynomial in a computation parameter κ, then, under standard computational assumptions, there exists a distribution on databases and a concept class $\mathcal{C}$ for which there is no efficient (in κ) mechanism for privately generating synthetic databases. In contrast, if both the concept class and the data universe are of size polynomial in κ then not only is there an efficient mechanism, but the size of the input database can be surprisingly small, namely $|C|^{o(1)} \cdot \log |X|$ (or even $O(2^{\sqrt{\log |\mathcal{C}|}} \log |X|)$) [10]. Thus $\mathcal{C}$ can be very large, as a function of n (while still polynomial in κ).

[2] This does not contradict the negative results because of the size of the error in the case of attacks using a polynomial number of queries, or the size of the input database in the case of attacks using an exponential number of queries.

Interestingly, for the potentially easier problem of privately generating a data structure (as opposed to a synthetic data set) from which it is possible to approximate counts, there is a tight “if and only if” connection between hardness of sanitization and the existence of *traitor tracing* schemes in cryptography [10].

2.1 Coresets

In computational geometry a coreset for a point set P is a small, weighted, point set C that is useful in computing approximate solutions of problems for P. For example, the queries might consist of a set of k points (not necessarily related to P), and the exact answer to the query might be the sum of the distances from each point $p \in P$ to its closest point in the query set Q; this is a *k-median* query. Coresets enjoy an extensive literature; different techniques are used for creating coresets appropriate for different sorts of queries.
Feldman *et al.* define *private coresets*. These are coresets in the traditional sense, but they are generated from P in a differentially private fashion [13]. Thus, the private coreset problem is similar to the problem of private generation of a synthetic data set, where the class of queries to be handled by the coreset plays a role analagous to the fractional concept class counts. Using similar techniques to those in [3], Feldman *et al.* show how any coreset construction can (ineffeciently) be modified to yield differentially private coresets, and using new techniques they obtain an efficient construction of coresets for k-median queries.

3 Connections to Other Fields of Study

As the study of privacy broadens, differential privacy productively blends, Zelig-like, with a surprising variety of concepts[3]. We have already seen this in the connection between traitor-tracing and non-interactive sanitization. Here we offer four additional examples.

Truthful Mechanisms for Strategic Agents. In a truthful mechanism, reporting one’s true value is a dominant strategy. Designing mechanisms to be truthful simplifies their analysis, making truthful mechanisms a widely studied solution concept in economics. One way of ensuring truthfulness is to arrange that the price paid by an individual is *independent* of his or her reported value. Analogously, if a price is set by a differentially private mechanism, then the price paid by an individual is “almost” independent of her bid. This intuition has been validated: differential privacy can be used to obtain “approximate truthfulness” [20], yielding the first collusion-resilient mechanism; it can also be used to better approximately solve combinatorial public project problems than can be done with any efficient truthful solution (unless $NP \subseteq BPP$) [15]. In each case an agent can gain only slightly by lying.

[3] The Internet Movie Database summarizes Woody Allen’s *Zelig*: “Fictional documentary about the life of human chameleon Leonard Zelig, a man who becomes a celebrity in the 1920s due to his ability to look and act like whoever is around him.”

Additive Combinatorics and Dense Model Theorems. Reingold *et al.* [23] give (almost) the following definition of density: Consider distributions X and Y over a set R. X is e^{ε}-dense in Y if for all $x \in R$, $\Pr[X = x] \leq e^{\varepsilon}\Pr[Y = x]$. Thus, a randomized mechanism f is ε-differentially private if and only if $f(D)$ is e^{ε}-dense in $f(D')$ for all D, D' such that $d(D, D') \leq 1$. This connection between differential privacy and (mutually) dense distributions has been exploited in an investigation of *computational* differential privacy, *i.e.*, differential privacy against a computationally bounded adversary. [21], which extends the dense model theorem in [23] to demonstrate equivalence between two definitions (indistinguishability-based and simulatability-based, respectively) of computational differential privacy,

Robust Statistics and the Influence Function. *Robust statistics* is the subfield of statistics that attempts to cope with outliers. In consequence, in a robust analysis the specific data for any one individual should not greatly affect the outcome of the analysis, suggesting a connection to differential privacy. Indeed, independently of our community and unknown to us, as early as 2005 Heitzig [17] proposed adapting, for the sake of privacy, a specific robust technique for reducing bias and estimating variance, known as the Jackknife [22, 25].
The Jackknife is related to the the *influence function* $\mathrm{IF}(x, T; F)$, which describes how an estimator T applied to samples from distribution F changes if we replace F by a distribution G with an infinitesimal contamination at x: $G = (1 - t)F + t\Delta_x$, for very small t. (See [18, 16].) This, in turn, is related to sensitivity "in a statistical setting" (that is, *whp* over samples from the distribution F). Typically, robust estimators are designed to have bounded influence function, implying *vanishing* sensitivity in a statistical setting. Heitzig's intuition, supported by detailed statistical insight but not made rigorous, was that it should be possible to ensure privacy by reporting an interval for the results of an analysis, rather than the exact value, where the size of the interval is determined by his (randomized) Jackknife-like procedure. Independently of Heitzig, but later, Dwork and Lei were also inspired by the implications of vanishing sensitivity offered by bounded influence functions. They adapted several robust algorithms, for varying statistical tasks, to provably (and always) yield differential privacy, with excellent accuracy whenever certain mild statistical assumptions hold [6].

4 Concluding Remarks

We have surveyed at least six very recent contributions on the differential privacy frontier. In several cases the work has forged links with other fields and communities: statistics, cryptography, complexity, geometry, mechanism design, and optimization. The plethora of new techniques, the formulation of new problems, and the fruitful interplay with other fields provides fertile ground for ebullient growth in an intellectually exciting and socially valuable endeavor.

Acknowledgements. I am grateful to all the authors of the new works for sharing their results with me before publication. Thanks also to Guy

Rothblum for his helpful comments on an early draft of this extended abstract.

References

1. B. Barak, K. Chaudhuri, C. Dwork, S. Kale, F. McSherry, and K. Talwar. Privacy, accuracy, and consistency too: A holistic solution to contingency table release. In *Proceedings of the 26th Symposium on Principles of Database Systems*, pages 273–282, 2007.
2. A. Blum, C. Dwork, F. McSherry, and K. Nissim. Practical privacy: The SuLQ framework. In *Proceedings of the 24th ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems*, June 2005.
3. A. Blum, K. Ligett, and A. Roth. A learning theory approach to non-interactive database privacy. In *Proceedings of the 40th ACM SIGACT Symposium on Thoery of Computing*, 2008.
4. I. Dinur and K. Nissim. Revealing information while preserving privacy. In *Proceedings of the Twenty-Second ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems*, pages 202–210, 2003.
5. C. Dwork. Differential privacy. In *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming (ICALP)(2)*, pages 1–12, 2006.
6. C. Dwork and J. Lei. Differential privacy and robust statistics. Manuscript, November 2008.
7. C. Dwork, F. McSherry, K. Nissim, and A. Smith. Calibrating noise to sensitivity in private data analysis. In *Proceedings of the 3rd Theory of Cryptography Conference*, pages 265–284, 2006.
8. C. Dwork, F. McSherry, and K. Talwar. The price of privacy and the limits of lp decoding. In *Proceedings of the 39th ACM Symposium on Theory of Computing*, pages pp. 85–94, 2007.
9. C. Dwork and M. Naor. On the difficulties of disclosure prevention in statistical databases or the case for differential privacy. Manuscript, 2008.
10. C. Dwork, M. Naor, O. Reingold, G. Rothblum, and S. Vadhan. When and how can privacy-preserving data release be done efficiently? Manuscript, November 2008.
11. C. Dwork and K. Nissim. Privacy-preserving datamining on vertically partitioned databases. In *Proceedings of CRYPTO 2004*, volume 3152, pages 528–544, 2004.
12. C. Dwork and S. Yekhanin. New efficient attacks on statistical disclosure control mechanisms. In *Proceedings of CRYPTO 2008*, pages 468–480, 2008.
13. D. Feldman, A. Fiat, H. Kaplan, and K. Nissim. Private coresets. Manuscript, November 2008.
14. A. Ghosh, T. Roughgarden, and M. Sundarajan. Universally utility-maximizing privacy mechanisms. Manuscript, November 2008.
15. A. Gupta, K. Ligett, F. McSherry, A. Roth, and K. Talwar. Differentially private approximation algorithms. Manuscript, November 2008.

16. F. Hampel, E. Ronchetti, P. Rousseeuw, , and W. Stahel. *Robust Statistics: The Approach Based on Influence Functions.* John Wiley, New York, 1986.
17. J. Heitzig. The "jackknife" method: Confidentiality protection for complex statistical analyses. In *Proceedings of the Joint UN-ECE/Eurostat work session on statistical data confidentiality*, 2005.
18. P. Huber. *Robust statistics.* John Wiley & Sons, 1981.
19. S. Kasiviswanathan, H. Lee, K. Nissim, S. Raskhodnikova, and A. Smith. What can we learn privately? In *Proceedings of FOCS 2008*, 2008.
20. F. McSherry and K. Talwar. Mechanism design via differential privacy. In *Proceedings of the 48th Annual Symposium on Foundations of Computer Science*, 2007.
21. I. Mironov, O. Pandey, O. Reingold, and S. Vadhan. Computational differential privacy. Manuscript, November 2008.
22. M. Quenouille. Notes on bias in estimation. *Biometrika*, 43:353–360, 1956.
23. O. Reingold, L. Trevisan, M. Tulsiani, and S. Vadhan. Dense subsets of pseudorandom sets. In *Proceedings 49th Annual IEEE Symposium on Foundations of Computing*, 2008.
24. D. Rubin. Discussion: Statistical disclosure limitation. *Journal of Official Statistics*, 9:462–468, 1993.
25. J. Tukey. Bias and confidence in not-quite large samples (abstract). *Ann. Math. Statist.*, 29, 1958.