Differential Privacy
A Survery

20398702 HU, JIAJUN
20304086 ZHOU, LEI
Department of Computer Science & Engineering
The Hong Kong University of Science and Technology
May 3, 2017

Abstract

Keywords: differential privacy

1 Introduction

2 Differentail Privacy

Over the past ten years, differentail privacy[1, 2] has emerged to become one of the most powerful approaches to ensure data pricacy. Roughly speaking, differential privacy ensures that the removal or insertion of a single record does not significantly affect the outcome of any analysis conducted on the database, thus making it possible to prevent private information from exposing to attackers. It follows a rigorous mathematical deduction to prove it can reduce the risk of privacy breach while remaining the utility of the data. At the beginning of this section, we will illuminate the concept by leveraging a simple example. Then, we will give the mathematical definition of differential privay and introduce two privacy mechanisms to achieve it.

2.1 A Simple Example

Suppose you have access to a database that allows you to compute the total income of all resident in certain area. You know one of your friends, Mr. White is going to move to another area, so simply computing the total

Name	Annual Income
Mr. Richard	0.5 million
Mr. White	1 million
Mr. Brown	2 million
Ms. Lee	0.35 million
Ms. Jean	0.6 million
...	...
Total income = 50 million	

Name	Annual Income
Mr. Richard	0.5 million
Mr. Brown	2 million
Ms. Lee	0.35 million
Ms. Jean	0.6 million
...	...
Total income = 49 million	

Table 1: The table before and after Mr. White's move.

income of all resident before and after Mr. White's move would allow you to guess his real income. As shown in table 1, the total income of all residents before Mr.White's move is 50 million, while the total income of all residents after Mr.White's move is 49 million. One can compute the real income of Mr.White is 1 millon. So from this example we can see even though we are not allowed to retrieve the information of a particular person, we are still able to get the private informtion through certain opertions. So what could one do to stop this? In the next section, we wil see how differential privacy can help resolve this problem.

2.2 Definition of Differential Privacy

Firstly, let us define some notations.

Definition 2.1. *D and D' are databases, but they must differs on at most one row.*

The reason why D and D' is required to differ on one row is to simulate whether a particular record is in or not in the database.

Definition 2.2. *$f(D)$ is a query on D*

Refer to the previous example, $f(D)$ is the total income of all residents in the database.

Definition 2.3. *$M(D)$ is the privacy mechanism, which is a randomized function that takes the database D as inpiut, and release privatized information with respect to $f(D)$.*

Refer to the previous example, $M(D)$ is the privated total income obtained by adding random noise on the total income.

Definition 2.4. *ϵ - differential privacy A privacy mechanism M gives ϵ - differential privacy if for all data sets D and D' differing on at most one row, and all $C \in Range(M)$,*

$$\frac{Pr[M(D) = C]}{Pr[M(D') = C]} < e^{\epsilon}$$

$\epsilon - differential\ privacy$ is a special case of $(\epsilon, \delta) - differential\ privacy$[3, 4] with $\delta = 0$. Typically, $(\epsilon, \delta) - differential\ privacy$ is simplified to $\epsilon - differential\ privacy$, so we only consider $\epsilon - differential\ privacy$ in this survey. $\epsilon - differential\ privacy$ says that the probability that the privatized result will be C is nearly the same whether or not you are in the database, which means the harm to you is nearly the same regardless of your participation. In the definition, ϵ is the privacy budget, which is a tradeoff that is used to balance the privacy of the result and it's utility. The smaller the ϵ is, the closer $Pr[M(D) = C]$ and $Pr[M(D') = C]$ are, and the stronger protection is.

2.3 Laplace Mechanism

2.4 Exponential Mechanism

Laplace mechanism is applied to query responses which are appropriately measured on the same scale or in the same units and to which certain magnitude of noise of this scale or units is added. On the contrary, exponential mechanism is first proposed by [5] for the situations in which we wish to choose the "best" response. Following the old scheme by adding noise directly to the computed quantity would completely destroy its accuracy. A simple example took by [2] explains the failure of simply adding noise:

Example 2.1. *Suppose in a supermarket a type of chocolate is on sale. The seller has collected a list of bidders: A, B, C, D, where A, B, C each bid* \$1.0 *and D bids* \$3.1*. He wonders how to set the price of the chocolate to maximize the revenue. At* \$3.1*, the revenue is* \$3.1*, at* \$3.0 *and* \$1.0 *the revenue becomes* \$3.0*, but at* \$3.2 *it turns into* \$0.0*.*

The exponential mechanism offers a safe solution to answering queries with arbitrary utilities. Given a query with arbitrary range $\mathcal{R}$, exponential mechanism is defined by range $\mathcal{R}$, the privacy parameter ϵ and a quality function $q : \mathcal{X}^n \times \mathcal{R} \to \mathbb{R}$, which maps outputs to quality scores. Getting back to the chocolate example, the quality with respect to the price $r \in \mathcal{R}$ and database $x \in \mathcal{X}^n$ is just the revenue obtained when the price is set to r. For a fixed database x, the user desires an output that is associated with the maximum quality score. The sensitivity of the quality function, which is a key factor in exponential mechanism, is determined by the database x and the query range $\mathcal{R}$:

$$\triangle = \max_{r \in \mathcal{R}} \max_{x,y:||x-y||_1 \leq 1} |q(x,r) - q(y,r)|. \tag{1}$$

Definition 2.5. *Given a database $x \in \mathcal{X}^n$ and a quality function q with respect to x and query range $\mathcal{R}$, the exponential mechanism $M_E(x, q, \mathcal{R})$ gives the output*

$r \in \mathcal{R}$ based on the probability:

$$Pr[M_E(x,q,\mathcal{R}) = r] \propto exp(\frac{\epsilon q(x,r)}{2\triangle}).$$

Theorem 1. *The exponential mechanism preserves $(\epsilon, 0)-$differential privacy. Proof. Given the query range $\mathcal{R}$, the quality function q and two databases $x, y \in \mathbb{N}^{|\mathcal{X}|}$ differing in at most one record (i.e. $||x-y||_1 \leq 1$), the ratio of probabilities that exponential mechanism produces the same output on two databases is*

$$\begin{aligned}
\frac{Pr(M_E(x,q,\mathcal{R}) = r)}{Pr(M_E(y,q,\mathcal{R}) = r)} &= \frac{\left(\frac{exp(\frac{\epsilon q(x,r)}{2\triangle})}{\sum_{r' \in \mathcal{R}} exp(\frac{\epsilon q(x,r')}{2\triangle})}\right)}{\left(\frac{exp(\frac{\epsilon q(y,r)}{2\triangle})}{\sum_{r' \in \mathcal{R}} exp(\frac{\epsilon q(y,r')}{2\triangle})}\right)} \quad (2)\\
&= \left(\frac{exp(\frac{\epsilon q(x,r)}{2\triangle})}{exp(\frac{\epsilon q(y,r)}{2\triangle})}\right) \cdot \left(\frac{\sum_{r' \in \mathcal{R}} exp(\frac{\epsilon q(y,r')}{2\triangle})}{\sum_{r' \in \mathcal{R}} exp(\frac{\epsilon q(x,r')}{2\triangle})}\right) \quad (3)\\
&\leq exp\left(\frac{\epsilon(q(x,r') - q(y,r'))}{2\triangle}\right) \quad (4)\\
&\cdot \left(\frac{\sum_{r' \in \mathcal{R}} exp(\frac{\epsilon(q(x,r')+\triangle)}{2\triangle})}{\sum_{r' \in \mathcal{R}} exp(\frac{\epsilon q(x,r')}{2\triangle})}\right) \quad (5)\\
&\leq exp(\frac{\epsilon}{2}) \cdot exp(\frac{\epsilon}{2}) \quad (6)\\
&= exp(\epsilon) \quad (7)
\end{aligned}$$

The reason why the exponential mechanism can offer strong quality guarantees is that it discount the probability of outcomes exponentially fast as their quality scores drop. Let $OPT_q(x) = \max_{r \in \mathcal{R}} q(x,r)$ denote the maximum quality score in scope R with regard to database x. The exponential mechanism substantially biases the distribution towards high scoring outputs and brings the expected score close to the optimum $OPT_q(x)$.

Theorem 2. *A database x and a quality function q with respect to x and query range $\mathcal{R}$ are given. Let $\mathcal{R}_{OPT} = \{r \in \mathcal{R} : q(x,r) = OPT_q(x)\}$ denote the set of elements in $\mathcal{R}$ that assume the maximum score. Then:*

$$Pr\left[q(M_E(x,q,\mathcal{R})) \leq OPT_q(x) - \frac{2\triangle}{\epsilon}\left(ln\left(\frac{|\mathcal{R}|}{|\mathcal{R}_{OPT}|}\right) + t\right)\right] \leq e^{-t} \quad (8)$$

Proof.

$$\begin{aligned}
Pr[q(M_E(x,q,\mathcal{R})) \leq c] &\leq \frac{|\mathcal{R}| exp(\epsilon c/2\triangle)}{|\mathcal{R}_{OPT}| exp(\epsilon OPT_q(x)/2\triangle)} \quad (9)\\
&= \frac{|\mathcal{R}|}{|\mathcal{R}_{OPT}|} exp(\frac{\epsilon(c - OPT_q(x))}{2\triangle}) \quad (10)
\end{aligned}$$

Substitute $c = OPT_q(x) - \frac{2\triangle}{\epsilon}\left(ln\left(\frac{|\mathcal{R}|}{|\mathcal{R}_{OPT}|}\right) + t\right)$ *into above inequation 9, and then Q.E.D.*

Since we always have $|\mathcal{R}_{OPT}| \geq 1$, the above theorem can be simplified into the following corollary:

Corollary 2.1. *Given a database x and a quality function q with respect to the x and query range* $\mathcal{R}$*, we have:*

$$Pr[q(M_E(x, q, \mathcal{R})) \geq OPT_q(x) - \frac{2\triangle}{\epsilon}(ln(|\mathcal{R}|) + t)] \geq 1 - e^{-t}. \qquad (11)$$

In other words, the exponential mechanism is a differential private mechanism that outputs an element from the range that has quality score that is nearly as high as possible—excepting an additive term which is linear in the sensitivity of the quality score and logarithmic in the cardinality of the query range.

2.5 BLR Mechanism

BLR mechanism, proposed by Blum, Ligett and Roth [6], is novel mechanism that breaks the limitation of the number of queries to non-interactive databases. Let $D = \{x_1, x_2, ..., x_n\} \in \mathcal{X}^n$ denote an n-row database and $Q = \{q_1, q_2, ..., q_k\}$ denote a set of queries and frequently write $k = |Q|$. The BLR mechanism preserves accuracy and privacy even when $k \gg n$. The lacpace mechanism requires that each query should be accurate and private independently and independent noise is added to each dimension of the output vector. This strategy reveals information increasingly in linearity to the number of queries k. To overcome the rising loss caused by excessive queries, BLR resorts to correlate the noise by projecting the answers to queries in a space of lower dimension. The "projection" is achieved by generating a *synthetic database* that approximately preserves the answers to all queries. Let $\mathcal{X}$ be a universe of data items and $\mathcal{C}$ be a "concept" class consisting of efficiently computable functions $c : \mathcal{X} \rightarrow \{0, 1\}$. As analyzed by Blum et al. [6], the synthetic database has the good property of maintaining approximately correct fractional counts for all concepts in $\mathcal{C}$. In other words, for every concept $c \in \mathcal{C}$, the fraction of elements in synthetic database $\hat{D} \in \mathcal{X}^m$ that satisfy c is approximately the same as the fraction of elements in original database $D \in \mathcal{X}^n$ that satisfy c. It substantially ensures the accuracy of outputs to queries. And after separating the original database from queries, anyone can run any statistic on it as many times as possible.

We start with the observation that for every database D and query set Q, there exists a synthetic database with a small number of rows that preserves the answers to every query in Q.

Theorem 3. *For every $D \in \mathcal{X}^n$ and every set of counting queries Q, there exists a synthetic database $\hat{D} \in \mathcal{X}^m$, for $m \in \frac{8logk}{\alpha^2}$, such that*

$$max_{i\in[k]}|q_i(D) - q_i(\hat{D})| \leq \alpha.$$

Proof. Consider a database $\hat{D} \in \mathcal{X}^m$ formed by taking $m < n$ random samples from $D \in \mathcal{X}^n$. Then by a union bound and a Chernoff bound

$$\begin{aligned} Pr\left[max_{q_i\in Q}|q_i(D) - q_i(\hat{D})| > \alpha\right] &\leq k \cdot Pr\left[|q_1(D) - q_1(\hat{D})| > \alpha\right] && (12) \\ &\leq k \cdot exp\left(\frac{-\alpha^2 m}{4}\right) && (13) \\ &= k \cdot exp(-2logk) && (14) \\ &< 1 && (15) \end{aligned}$$

It suggests that there must exists some $\hat{D} \in \mathcal{X}^m$ that preserves the answers to every query $q \in Q$ up to an additive error term of α.

The above theorem has kindled interest in synthetic databases [6, 7]. But how to construct the differentially private synthetic databases efficiently? The BLR mechanism [6] presents a classical paradigm that instantiates the exponential mechanism to build up the synthetic database:

- Let $\mathcal{R} = \mathcal{X}^m$ for $m = \frac{32logk}{\alpha^2}$,
- Let the quality function $q(D, \hat{D}) = -max_{f\in Q}|f(D) - f(\hat{D})|$ for every $D \in \mathcal{X}^n$ and $\hat{D} \in \mathcal{X}^m$. Note that we make the quality function inversely related to the error so that better accuracy implies higher score.
- The sensitivity of the quality function $\triangle = 1/n$, because it is simply the maximum error over a set of counting queries, and a counting query has global sensitivity $1/n$.
- Sample and output $\hat{D} \in \mathcal{X}^m$ with the exponential mechanism $M_E(D, q, \mathcal{R})$.

Conclusion

References

1. Cynthia Dwork. Differential privacy: A survey of results. In *International Conference on Theory and Applications of Models of Computation*, pages 1–19. Springer, 2008.

2. Cynthia Dwork, Aaron Roth, et al. The algorithmic foundations of differential privacy. *Foundations and Trends® in Theoretical Computer Science*, 9(3–4):211–407, 2014.

3. Cynthia Dwork. Differential privacy. In *Encyclopedia of Cryptography and Security*, pages 338–340. Springer, 2011.

4. Cynthia Dwork, Krishnaram Kenthapadi, Frank McSherry, Ilya Mironov, and Moni Naor. Our data, ourselves: Privacy via distributed noise generation. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 486–503. Springer, 2006.

5. Frank McSherry and Kunal Talwar. Mechanism design via differential privacy. In *Foundations of Computer Science, 2007. FOCS'07. 48th Annual IEEE Symposium on*, pages 94–103. IEEE, 2007.

6. Avrim Blum, Katrina Ligett, and Aaron Roth. A learning theory approach to noninteractive database privacy. *Journal of the ACM (JACM)*, 60(2):12, 2013.

7. Cynthia Dwork, Moni Naor, Omer Reingold, Guy N Rothblum, and Salil Vadhan. On the complexity of differentially private data release: efficient algorithms and hardness results. In *Proceedings of the forty-first annual ACM symposium on Theory of computing*, pages 381–390. ACM, 2009.