The Staircase Mechanism in Differential Privacy

Author: 1. Peter Kairouz, 2. Pramod Viswanath and 3. Quan GengSewoong Oh

***Abstract*—Laplacian noise is a standard way to add noise to data to sanitize numerical data in differential privacy mechanisms before publishing it. In this paper, the author proposes another noise-adding called staircase mechanism for differential privacy. He has shown that the staircase mechanism can replace the Laplace mechanism and improve performance, particularly in medium and low privacy regimes. The staircase mechanism is proven to be the optimal noise-adding mechanism in a universal context, subject to a conjectured technical lemma. The paper also discusses that we can balance accuracy and privacy by using staircase mechanisms in differential privacy.**

***Index Terms*—Differential privacy, Staircase mechanism Sensitivity, Probability density function, Geometric mixture, Gamma value**

I. Introduction

Differential Privacy is the mathematical framework for preserving the privacy of individuals in numerical datasets. It prevents the individual records by adding noise to datasets. It can provide a sorority of privacy by allowing numerical data analysis without revealing sensitive information of any individuals. The Staircase is another noise-adding mechanism, a geometric mixture of uniform random variables. It can replace the Laplacian noise-adding mechanisms in every category, such as differential privacy, performance, and much improvement in the medium-low privacy regimes. The staircase mechanism is the optimum/optimal noise-adding mechanism. i.e., the Staircase mechanism is an optimal version of the Laplace Mechanisms.

Є-Differential privacy: If all the datasets differ at most one element – 2. The parameters Є (0 ∞) show the privacy of mechanisms, as the decrease parameter (Є) increases the privacy of the document.

The differential privacy constraint (2) is required for neighbors' datasets; the probability distribution of the randomized mechanism's output is approximately the same. Therefore, the absence and presence of any individual in the datasets do not affect the result of the query function.

Query sensitivity: The sensitivity of the function refers to the maximum absolute difference in the output of the function when the input datasets differ in, at most, one element. Δ is denoted as the query sensitivity.

The standard way to preserve privacy is by adding noise to the query function output.

$$K(D) = q(D) + X,$$

Here, K is the noise-adding mechanism, q is the query function, and X is the noise the mechanism adds.

II. Your Procedure or Your Method

The staircase mechanism is viewed as a geometric mixture of uniform random variables easily generated by algorithms. The staircase mechanisms have three parameters: Є, Δ, and γ. Є – set by differential privacy constraints. Δ is set by the global sensitivity of the query functions, and γ [0, 1] is a free parameter related to the cost function being considered.

A. Algorithms

Generation of uniform random variables with a staircase probability distribution.

Input: Є, Δ and γ [0, 1]

Output: *X(staircase noise)* – random variable (r.v.) with Staircase Distribution using Є, Δ, and γ parameters of the Staircase mechanisms.

1. Generate a r.v. S with *Pr(S=1) = Pr(S=-1) = ½.*
2. Generate Geometric r.v. G with *Pr(G = i) = (1-b) b^i.* For integer $i \geq 0$, $b = e^{-Є}$.
3. Generate a r.v. U uniformly distributed in [0, 1].
4. Generate a binary r.v. B with *Pr(B=0) = γ/ (γ+(1- γ)b) and Pr(B=1) = (1- γ)b/(γ+(1- γ)b).*
5. *X ← S((1-B)((G+ γU) Δ)+B((G+ γ+(1- γ)U) Δ)).*
6. Output X.
   - S shows the sign of noise.
   - G shows the interval of noise lies.
   - B shows the subinterval of noise lies.
   - U helps in the uniform sample of the subinterval.
   - X is the staircase noise that adds to the actual value.

B. Figures

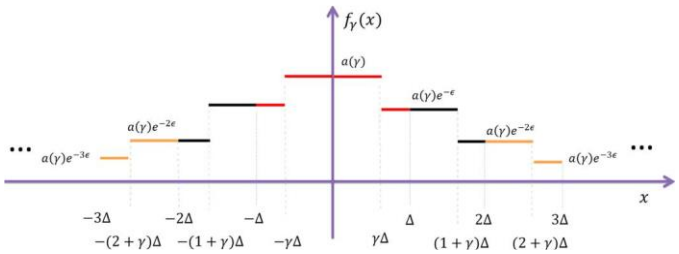


Fig1. 1D Staircase-Shaped Probability Density Functions

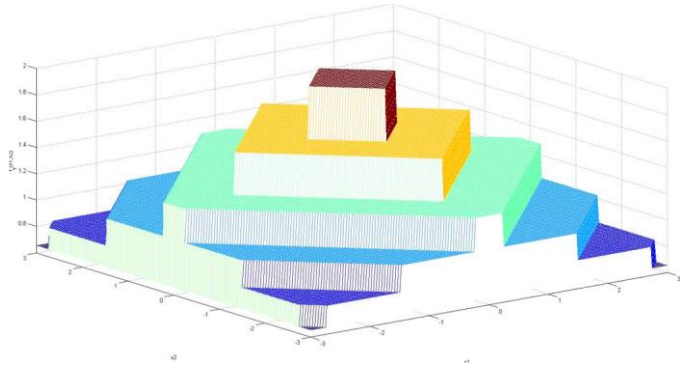


Fig2. 2D Staircase-Shaped Probability Density Functions

III. Optimal Property of Staircase Mechanism

A. *Decrease the noise aptitude.*

ε-differential privacy constraint, the staircase mechanisms minimize the expectation of the noise added to the query output. That means it balances the privacy and accuracy of the individual data.

B. *Staircase Shaped Probability Density Function*

The Staircase Mechanisms have staircase-shaped probability density functions that discrete jump that allows for precise control over privacy guarantees, and privacy amplification occurs at specific intervals, ensuring robust privacy for the differential privacy.

C. *Geometric Mixture*

The Staircase Mechanism is a geometric mixture of random variables that makes it a universal and promising way to make noise and preserve the privacy of individuals in the datasets.

IV. Proof of Main Result

Theorem 1 –

The staircase mechanism has the least cost function among all k-dimensional differentially private mechanisms for the k-dimensional query function under certain technical conditions. This Theorem states that the staircase mechanism is excellent in minimizing the cost function while ensuring k-dimensional differential privacy, making it an optimal choice for preserving privacy in the multi-dimensional.

Proof of Theorem 1

Step 1: Discretization of Probability Distributions

Probability density with symmetric and piecewise constant distribution is considered.

Step 2: Monotonic Decreases

The probability density with symmetric piecewise constant probability distribution is a monotonically decreased density sequence. That shows that the optimal probability distribution should have a monotonically decreasing density sequence.

Step 3: Geometric Decay

probability distributions with monotonically decreasing density sequences and geometrically decay density sequences are considered. It is shown that the optimal probability density function should periodically decay.

Step 4: Staircase-Shaped Probability Density Function

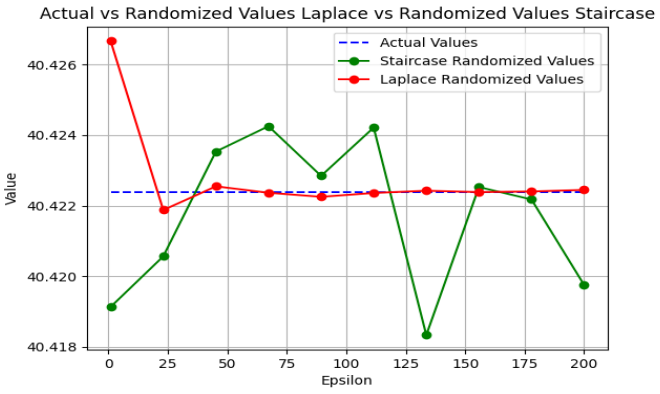
The optimal probability density function is staircase-shaped in the multidimensional setting. The dimension increases, and the probability density function goes to a multidimensional staircase mechanisms function.

Considering the above four steps, we conclude that the Staircase Mechanism is Optimal in preserving individual privacy in the datasets.

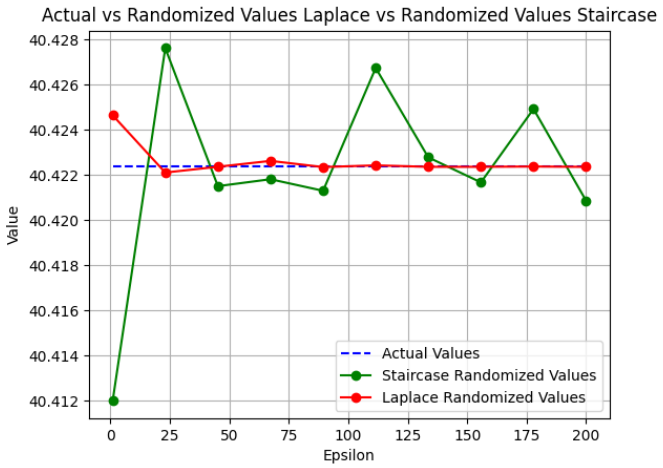
V. Results

Actual Mean value: 40.422382375824085

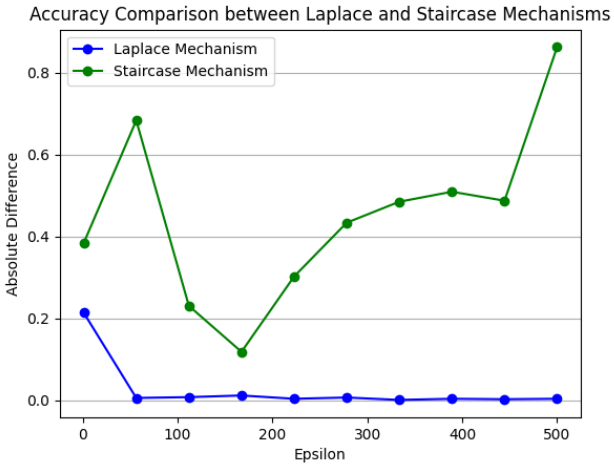
Staircase value	Laplace value
40.4255058642949	40.4265092996485
40.41854646089413	40.422590271379576
40.42180985380181	40.42251369757598
40.416383770202515	40.422366207509356
40.42051871563272	40.4224488802245
40.42000370411114	40.42240116236695
40.4270966109369	40.422391900285696
40.41908102841123	40.42244124155878
40.42257926536507	40.422381221890134
40.42183085205012	40.42239321153611



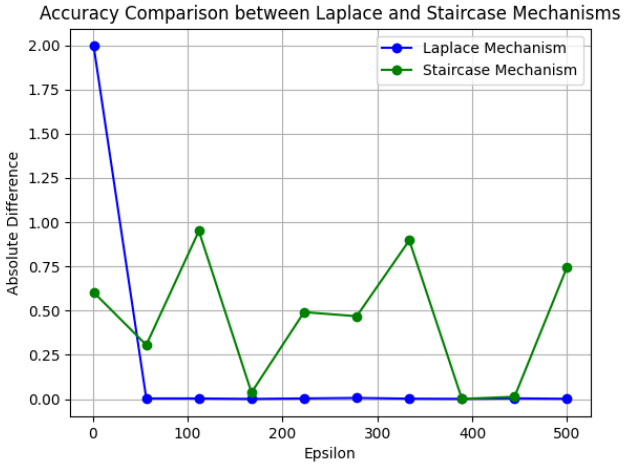
Comparison: Actual vs Staircase vs Laplace at Gamma value: 0



Comparison: Actual vs Staircase vs Laplace at Gamma value:1



Accuracy Comparison: Laplace vs Staircase at Gamma value: 0



Accuracy Comparison: Laplace vs Staircase at Gamma value: 1

VI. Conclusion

I have concluded the study of Laplace and the Staircase Mechanisms. I saw the staircase use different distributions (staircase distribution) to calculate the noise to sanitize individual data. If we implement that in both C++ programming, we found the staircase mechanisms are much faster than the Laplace mechanisms. It's almost two times faster. As discussed in the report above[I], staircase mechanisms perform better in the medium-low data regimes.

VII. Acknowledgment

I want to thank the authors of "The Staircase Mechanism in Differential Privacy" who analyzed the Laplace classical Mechanisms and proposed another optimal mechanism that can ensure differential privacy in the optimal way as of Laplace Mechanisms. That means Staircase Mechanisms is the optimal version of Laplace Mechanisms. The staircase mechanism takes less time to generate noise by using unique algorithms that are discussed above[II]

VIII. References

[1] https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7093132

[2] https://www.cs.ru.nl/bachelors-theses/2018/Jelle_Loman__4573382___Comparing_the_performance_of_the_Laplace_and_Staircase_mechanisms_in_differential_privacy.pdf