Design and Applications of Differentially Private Mechanisms:
Adherence to Query Range Constraints and Obfuscation of Facial Images
Appendix

This document is an appendix for Chapter 5, Section 1 of *Design and Applications of Differentially Private Mechanisms*. We provide here the full proofs to the lemmata and theorems from the main paper.

A1 - Single Infinitely Spanning Constraint

In this section, we provide the full proofs pertaining to Section 5.1.2 of the main paper.

Lemma 1. *For any PDF with a location parameter at distance $i\Delta F > 0$ from the constraint, bounds on the possible values of its scaling parameter are determined by the following four inequalities:*

$$\sigma_2 \leq -\frac{i\Delta F e^{i\epsilon}\sigma_1}{W\left(-\frac{2i\Delta F e^{-i\epsilon} e^{-\frac{i\Delta F e^{-i\epsilon}}{\sigma_1}}}{\sigma_1}\right) e^{i\epsilon}\sigma_1 + i\Delta F} \tag{1}$$

$$\sigma_2 \geq -\frac{i\Delta F e^{i\epsilon}\sigma_1}{W_{-1}\left(-\frac{2i\Delta F e^{-i\epsilon} e^{-\frac{i\Delta F e^{-i\epsilon}}{\sigma_1}}}{\sigma_1}\right) e^{i\epsilon}\sigma_1 + i\Delta F} \tag{2}$$

$$\sigma_2 \geq \frac{i\Delta F}{-W\left(2W\left(-\frac{1}{2e}\right) i\epsilon e^{W\left(-\frac{1}{2e}\right) i\epsilon e^{-i\epsilon+1} - i\epsilon+1}\right) + W\left(-\frac{1}{2e}\right) i\epsilon e^{-i\epsilon+1}} \tag{3}$$

$$\sigma_2 \leq \frac{i\Delta F}{-W_{-1}\left(2W\left(-\frac{1}{2e}\right) i\epsilon e^{W\left(-\frac{1}{2e}\right) i\epsilon e^{-i\epsilon+1} - i\epsilon+1}\right) + W\left(-\frac{1}{2e}\right) i\epsilon e^{-i\epsilon+1}} \tag{4}$$

Proof. Recall from the main text that the privacy guarantee to be satisfied is as shown in Formula (5).

$$\frac{\sigma_2}{\sigma_1}\left(\frac{2 - e^{-\frac{\Delta L_1 + i\Delta F}{\sigma_2}}}{2 - e^{-\frac{\Delta L_1}{\sigma_1}}}\right)\left(\frac{e^{\frac{\Delta L_1 + i\Delta F}{\sigma_2}}}{e^{\frac{\Delta L_1}{\sigma_1}}}\right) \leq e^{i\epsilon} \tag{5}$$

By isolating σ_2 in the privacy guarantee, we obtain Formulae (6) and (7). Given a PDF for database $D_1 \in \mathbb{D}$ with a scaling parameter σ_1, a paired PDF for database $D_2 \in \mathbb{D}$ satisfies the privacy guarantee if its scaling parameter σ_2 falls in the intersection of the two spans given by these inequalities.

$$\sigma_2 \leq -\frac{2\left(e^{\frac{\Delta L_1}{\sigma_1}} - \frac{1}{2}\right) e^{i\epsilon}\sigma_1\left(i\Delta F + \Delta L_1\right)}{-\sigma_1\left(e^{i\epsilon} - 2e^{\frac{i\epsilon\sigma_1 + \Delta L_1}{\sigma_1}}\right) W\left(-\frac{2(i\Delta F + \Delta L_1) e^{-\frac{2i\epsilon\sigma_1 e^{\frac{\Delta L_1}{\sigma_1}} + e^{-i\epsilon} i\Delta F - i\epsilon\sigma_1 + e^{-i\epsilon}\Delta L_1}{\sigma_1\left(2e^{\frac{\Delta L_1}{\sigma_1}} - 1\right)}}}{\sigma_1\left(2e^{\frac{\Delta L_1}{\sigma_1}} - 1\right)}\right) + i\Delta F + \Delta L_1} \tag{6}$$

$$\sigma_2 \geq -\frac{2\left(e^{\frac{\Delta L_1}{\sigma_1}} - \frac{1}{2}\right) e^{i\epsilon}\sigma_1\left(i\Delta F + \Delta L_1\right)}{-\sigma_1\left(e^{i\epsilon} - 2e^{\frac{i\epsilon\sigma_1 + \Delta L_1}{\sigma_1}}\right) W_{-1}\left(-\frac{2(i\Delta F + \Delta L_1)e^{-\frac{2i\epsilon\sigma_1 e^{\frac{\Delta L_1}{\sigma_1}} + e^{-i\epsilon} i\Delta F - i\epsilon\sigma_1 + e^{-i\epsilon}\Delta L_1}{\sigma_1\left(2e^{\frac{\Delta L_1}{\sigma_1}} - 1\right)}}}{\sigma_1\left(2e^{\frac{\Delta L_1}{\sigma_1}} - 1\right)}\right) + i\Delta F + \Delta L_1} \tag{7}$$

In order for this intersection to be a real-valued range, it is necessary for the input to the LambertW functions in the inequalities to always be greater than or equal to $-\frac{1}{e}$. To ensure that this condition is met for all possible values of i, we first take the derivative of the input with respect to i as shown in Formula (8).

$$-\frac{2\left(i\epsilon\Delta F + \epsilon\Delta L_1 - \Delta F\right)\left(-2\sigma_1 e^{\frac{\Delta L_1}{\sigma_1}} + \left(i\Delta F + \Delta L_1\right)e^{-i\epsilon} + \sigma_1\right) e^{-\frac{2i\epsilon\sigma_1 e^{\frac{\Delta L_1}{\sigma_1}} + e^{-i\epsilon} i\Delta F - i\epsilon\sigma_1 + e^{-i\epsilon}\Delta L_1}{\sigma_1\left(2e^{\frac{\Delta L_1}{\sigma_1}} - 1\right)}}}{\left(\sigma_1\right)^2\left(2e^{\frac{\Delta L_1}{\sigma_1}} - 1\right)^2} \tag{8}$$

Three possible zeros for the derivative can be calculated as shown in Formulae (9) (where the variable Z can be replaced with 0 or -1) and (10).

$$i = -\frac{\Delta L_1\epsilon + \Delta F W_Z\left(-\frac{\epsilon\sigma_1\left(2e^{\frac{\Delta L_1}{\sigma_1}} - 1\right)e^{-\frac{\Delta L_1\epsilon}{\Delta F}}}{\Delta F}\right)}{\epsilon\Delta F} \tag{9}$$

$$i = -\frac{\Delta L_1\epsilon - \Delta F}{\epsilon\Delta F} \tag{10}$$

Since the substitution of the zero from Formula (9) into the input of the LambertW function does not allow for easy steps of simplification when using -1 as the value of Z, we take an alternate approach to first show that the value of the input to the LambertW function is the same at both zeros defined in Formula (9) (using 0 or -1 as the value of Z). Let the first zero occur at i and the second occur at j. The equality between the values at these zeros is shown in Formulae (11) - (16).

$$-\frac{2\left(i\Delta F + \Delta L_1\right)e^{-\frac{2i\epsilon\sigma_1 e^{\frac{\Delta L_1}{\sigma_1}} + e^{-i\epsilon} i\Delta F - i\epsilon\sigma_1 + e^{-i\epsilon}\Delta L_1}{\sigma_1\left(2e^{\frac{\Delta L_1}{\sigma_1}} - 1\right)}}}{\sigma_1\left(2e^{\frac{\Delta L_1}{\sigma_1}} - 1\right)} = -\frac{2\left(j\Delta F + \Delta L_1\right)e^{-\frac{2j\epsilon\sigma_1 e^{\frac{\Delta L_1}{\sigma_1}} + e^{-j\epsilon} i\Delta F - j\epsilon\sigma_1 + e^{-j\epsilon}\Delta L_1}{\sigma_1\left(2e^{\frac{\Delta L_1}{\sigma_1}} - 1\right)}}}{\sigma_1\left(2e^{\frac{\Delta L_1}{\sigma_1}} - 1\right)} \tag{11}$$

$$-\frac{e^{-i\epsilon}\left(i\Delta F + \Delta L_1\right)e^{-\frac{e^{-i\epsilon}(i\Delta F + \Delta L_1)}{\sigma_1\left(2e^{\frac{\Delta L_1}{\sigma_1}} - 1\right)}}}{\sigma_1\left(2e^{\frac{\Delta L_1}{\sigma_1}} - 1\right)} = -\frac{\left(j\Delta F + \Delta L_1\right)e^{-\frac{e^{-j\epsilon}(j\Delta F + \Delta L_1)}{\sigma_1\left(2e^{\frac{\Delta L_1}{\sigma_1}} - 1\right)}}}{\sigma_1\left(2e^{\frac{\Delta L_1}{\sigma_1}} - 1\right)} \tag{12}$$

$$-\frac{e^{-i\epsilon}\left(i\Delta F+\Delta L_1\right)}{\sigma_1\left(2e^{\frac{\Delta L_1}{\sigma_1}}-1\right)}=-\frac{e^{-j\epsilon}\left(j\Delta F+\Delta L_1\right)}{\sigma_1\left(2e^{\frac{\Delta L_1}{\sigma_1}}-1\right)} \tag{13}$$

$$e^{-i\epsilon}\left(i\Delta F+\Delta L_1\right)=e^{-j\epsilon}\left(j\Delta F+\Delta L_1\right) \tag{14}$$

At this point, we replace i and j with their values as determined by Formula (9) and then we simplify the expression. In the interest of space, we substitute the instances of the LambertW function from Formula (9), using a for the 0 branch and b for the -1 branch.

$$e^{\left(\frac{\Delta L_1\epsilon+\Delta Fa}{\epsilon\Delta F}\right)\epsilon}\left(\left(-\frac{\Delta L_1\epsilon+\Delta Fa}{\epsilon\Delta F}\right)\Delta F+\Delta L_1\right)=e^{\left(\frac{\Delta L_1\epsilon+\Delta Fb}{\epsilon\Delta F}\right)\epsilon}\left(\left(-\frac{\Delta L_1\epsilon+\Delta Fb}{\epsilon\Delta F}\right)\Delta F+\Delta L_1\right) \tag{15}$$

$$ae^a=be^b \tag{16}$$

Since the LambertW functions of a and b both have the same input, the equality of Formula (16) is confirmed to be valid. Now by taking the zero of Formula (9) using 0 as the value for Z, we rewrite the zero in terms of ΔF as shown in Formula (17)

$$\Delta F=\frac{-e^{i\epsilon}\sigma_1+2\sigma_1e^{\frac{i\epsilon\sigma_1+\Delta L_1}{\Delta L_1}}-\Delta L_1}{i} \tag{17}$$

When substituting ΔF in the original LambertW input with the expression in Formula (17), the value of the input becomes $-\frac{2}{e}$ which is outside of the allowable range of input. Since we have shown that the value of the zero using -1 as the value of Z will be the same, both of the potential modes determined by these zeros can be ignored. The function of the input is therefore unimodal and it remains to determine whether the mode is a minimum or a maximum. By setting i to 0 in the derivative, we obtain the expression shown in Formula (18).

$$\frac{2\left(\left(\Delta L_1+\sigma_1\right)e^{-\frac{\Delta L_1}{\sigma_1}}-2\sigma_1\right)e^{\frac{2\Delta L_1}{\sigma_1\left(-2+e^{-\frac{\Delta L_1}{\sigma_1}}\right)}}\left(-\Delta L_1\epsilon+\Delta F\right)}{\left(\sigma_1\right)^2\left(-2+e^{-\frac{\Delta L_1}{\sigma_1}}\right)^2} \tag{18}$$

It is clear that the denominator is always positive as both factors are squared. In the numerator, four factors are present. The first, being the constant 2, and the third, being an exponential function, must always be positive. The sign of the second and fourth factors remains to be determined. We show that the second factor is always negative by proving Formula (19).

$$\left(\Delta L_1+\sigma_1\right)e^{-\frac{\Delta L_1}{\sigma_1}}\leq 2\sigma_1 \tag{19}$$

The derivative of the left-hand side with respect to ΔL_1 is shown in Formula (20).

$$-\frac{e^{-\frac{\Delta L_1}{\sigma_1}}\Delta L_1}{\sigma_1} \tag{20}$$

Since all variables are non-negative, this derivative is always negative meaning that the left-hand side is decreasing as ΔL_1 is increasing. It is therefore maximized when $\Delta L_1=0$. When making this substitution, the inequality reduces to $1\leq 2$, thus proving that the factor is indeed always negative.

The fourth factor in the numerator of the derivative is the same expression as the numerator of the zero in Formula (10). From this, we can infer that if the zero is at a positive i value, then the derivative is negative when $i = 0$ and if the zero is at a negative i value, then the derivative is positive when $i = 0$. This means that the mode at the zero is a minimum.

Now, we can define a condition on the input to the LambertW function as Formula (21).

$$-\frac{2\left(i\Delta F + \Delta L_1\right) e^{-\frac{2i\epsilon\sigma_1 e^{\frac{\Delta L_1}{\sigma_1}} + e^{-i\epsilon} i\Delta F - i\epsilon\sigma_1 + e^{-i\epsilon}\Delta L_1}{\sigma_1\left(2e^{\frac{\Delta L_1}{\sigma_1}} - 1\right)}}}{\sigma_1\left(2e^{\frac{\Delta L_1}{\sigma_1}} - 1\right)} \geq -\frac{1}{e} \tag{21}$$

By isolating for σ_1, we get Formulae (22) and (23). These inequalities represent disjoint spans where the value of σ_1 is required to fall into their union.

$$\sigma_1 \geq \frac{-\Delta L_1\left(i\Delta F + \Delta L_1\right)}{\left(i\Delta F + \Delta L_1\right) W\left(\frac{2\Delta L_1 W\left(-\frac{1}{2e}\right) e^{\frac{\Delta L_1 W\left(-\frac{1}{2e}\right)e^{i\epsilon} + i\epsilon\left(i\Delta F + \Delta L_1\right)}{i\Delta F + \Delta L_1}}}{i\Delta F + \Delta L_1}\right) - \Delta L_1 W\left(-\frac{1}{2e}\right) e^{i\epsilon}} \tag{22}$$

$$\sigma_1 \leq \frac{-\Delta L_1\left(i\Delta F + \Delta L_1\right)}{\left(i\Delta F + \Delta L_1\right) W_{-1}\left(\frac{2\Delta L_1 W\left(\frac{-1}{2e}\right) e^{\frac{\Delta L_1 W\left(\frac{-1}{2e}\right)e^{i\epsilon} + i\epsilon\left(i\Delta F + \Delta L_1\right)}{i\Delta F + \Delta L_1}}}{i\Delta F + \Delta L_1}\right) - \Delta L_1 W\left(\frac{-1}{2e}\right) e^{i\epsilon}} \tag{23}$$

We substitute i with the zero of the derivative since we must ensure that the inequalities will hold at the minimum value of the input function. This produces Formulae (24) and (25). These inequalities represent bounds on σ_1 values for PDFs with location parameters at a distance of $\Delta L_1 > 0$ away from the constraint.

$$\sigma_1 \geq \frac{-\Delta L_1 \Delta F}{\Delta F W\left(\frac{2\Delta L_1 W\left(\frac{-1}{2e}\right)\epsilon e^{\frac{\Delta L_1 W\left(\frac{-1}{2e}\right)\epsilon e^{-\frac{\Delta L_1\epsilon - \Delta F}{\Delta F}} - \Delta L_1\epsilon + \Delta F}{\Delta F}}}{\Delta F}\right) - \Delta L_1 W\left(\frac{-1}{2e}\right)\epsilon e^{-\frac{\Delta L_1\epsilon - \Delta F}{\Delta F}}} \tag{24}$$

$$\sigma_1 \leq \frac{-\Delta L_1 \Delta F}{\Delta F W_{-1}\left(\frac{2\Delta L_1 W\left(\frac{-1}{2e}\right)\epsilon e^{\frac{\Delta L_1 W\left(\frac{-1}{2e}\right)\epsilon e^{-\frac{\Delta L_1\epsilon - \Delta F}{\Delta F}} - \Delta L_1\epsilon + \Delta F}{\Delta F}}}{\Delta F}\right) - \Delta L_1 W\left(\frac{-1}{2e}\right)\epsilon e^{-\frac{\Delta L_1\epsilon - \Delta F}{\Delta F}}} \tag{25}$$

Finally, since we want to be able to consider the bounds of Formulae (6) and (7) as well as those of Formulae (24) and (25) for σ values of PDFs having the same location parameter, we set $\Delta L_1 = 0$ in Formulae (6) and (7) and we set $\Delta L_1 = i\Delta F$ in Formulae (24) and (25). This produces four inequalities which specify bounds on σ_2 values for PDFs with location parameters at distance $i\Delta F > 0$ from the constraint such that Formulae (1) and (2) are overlapping spans where σ_2 must fall in their intersection and Formulae (3) and (4) are disjoint spans where σ_2 must fall in their union. $\square$

Lemma 2. *Through the selection of an appropriate σ_1 value when $\Delta L_1 = 0$, it is possible to calculate σ_2 values for any PDF with a location parameter at distance $i\Delta F > 0$ away from the constraint such that the inequalities of Lemma 1 are satisfied.*

Proof. By setting $\Delta L_1 = 0$ in Formula (5), we obtain the form in Formula (26).

$$\frac{\sigma_2}{\sigma_1}\left(2 - e^{-\frac{i\Delta F}{\sigma_2}}\right) e^{\frac{i\Delta F}{\sigma_2}} \leq e^{i\epsilon} \tag{26}$$

By isolating for σ_2, we obtain Formulae (27) and (28). As in Lemma 1, the intersection of the spans defined by the inequalities gives the valid range for the σ_2 values.

$$\sigma_2 \leq -\frac{i\Delta F e^{i\epsilon}\sigma_1}{W\left(-\frac{2i\Delta F e^{-i\epsilon} e^{-\frac{i\Delta F e^{-i\epsilon}}{\sigma_1}}}{\sigma_1}\right) e^{i\epsilon}\sigma_1 + i\Delta F} \tag{27}$$

$$\sigma_2 \geq -\frac{i\Delta F e^{i\epsilon}\sigma_1}{W_{-1}\left(-\frac{2i\Delta F e^{-i\epsilon} e^{-\frac{i\Delta F e^{-i\epsilon}}{\sigma_1}}}{\sigma_1}\right) e^{i\epsilon}\sigma_1 + i\Delta F} \tag{28}$$

We now take the same process as in Lemma 1 to ensure that the input to the LambertW function is always greater than or equal to $-\frac{1}{e}$. The derivative of the input is shown in Formula (29).

$$-\frac{2\Delta F e^{-i\epsilon} e^{-\frac{i\Delta F e^{-i\epsilon}}{\sigma_1}} (i\epsilon - 1)\left(i\Delta F e^{-i\epsilon} - \sigma_1\right)}{\sigma_1{}^2} \tag{29}$$

We are interested in the modality of the input, thus we calculate the zeros of the derivative. Two possible zeros are given in Formula (30) where Z can be replaced with 0 or -1 and a third is given in Formula (31).

$$i = -\frac{W_Z\left(-\frac{\epsilon\sigma_1}{\Delta F}\right)}{\epsilon} \tag{30}$$

$$i = \frac{1}{\epsilon} \tag{31}$$

For both of the first two zeros in Formula (30), by substituting i with this value in the input of the LambertW function, the value of the input becomes $-\frac{2}{e}$. Since this is outside of the valid range for the input, both of these zeros can be ignored. The third zero allows for the input to fall in the valid range. We can therefore conclude that the input is unimodal as a function of i.

We now turn to identifying whether the zero is a minimum or a maximum. To do so, we examine the value of the derivative when $i = 0$. Since the value is $-\frac{2\Delta F}{\sigma_1}$, and all variables must be non-negative, the function is decreasing at $i = 0$ and since the mode is at $i = \frac{1}{\epsilon}$, it is a minimum. From this, we can now specify that in order for the input of the LambertW to always remain greater than or equal to $-\frac{1}{e}$, the value of the input at its mode must satisfy the same condition. This is represented as Formula (32).

$$-\frac{2\Delta F e^{-1-\frac{\Delta F}{\epsilon e \sigma_1}}}{\epsilon\sigma_1} \geq -\frac{1}{e} \tag{32}$$

Using this inequality, we can now isolate for σ_1 and find that its possible values are given as the union of two disjoint spans defined by Formulae (33) and (34).

$$\sigma_1 \geq -\frac{\Delta F}{W\left(-\frac{1}{2e}\right) e\epsilon} \tag{33}$$

$$\sigma_1 \leq -\frac{\Delta F}{W_{-1}\left(-\frac{1}{2e}\right) e\epsilon} \tag{34}$$

From these two spans, we select the lower bound of Formula (33) as the value to assign to σ_1. Over the course of the remaining lemmas, we will show why this choice is necessary. By substituting the σ_1 of Formulae (1) and (2) with this value, we get the following inequalities:

$$\sigma_2 \leq -\frac{i\Delta F}{-W\left(2W\left(-\frac{1}{2e}\right)i\epsilon e^{W\left(-\frac{1}{2e}\right)i\epsilon e^{-i\epsilon+1}-i\epsilon+1}\right)+W\left(-\frac{1}{2e}\right)i\epsilon e^{-i\epsilon+1}} \tag{35}$$

$$\sigma_2 \geq -\frac{i\Delta F}{-W_{-1}\left(2W\left(-\frac{1}{2e}\right)i\epsilon e^{W\left(-\frac{1}{2e}\right)i\epsilon e^{-i\epsilon+1}-i\epsilon+1}\right)+W\left(-\frac{1}{2e}\right)i\epsilon e^{-i\epsilon+1}} \tag{36}$$

Note that these inequalities are identical to Formulae (3) and (4) except that the directions of the inequality signs are flipped. As a result, by using Formulae (3) and (4) as equalities rather than inequalities, for any distance $i\Delta F > 0$, we can calculate exactly two possible σ_2 values which satisfy all four inequalities of Lemma 1 when using this choice of σ_1. The calculation of σ_2 (with σ_1 left as a variable) is shown in Formula (37).

$$\sigma_2 = -\frac{i\Delta F e^{i\epsilon}\sigma_1}{W_Z\left(-\frac{2i\Delta F e^{-i\epsilon}e^{-\frac{i\Delta F e^{-i\epsilon}}{\sigma_1}}}{\sigma_1}\right)e^{i\epsilon}\sigma_1 + i\Delta F} \tag{37}$$

□

Lemma 3. *The sign of the denominator in the derivative taken with respect to i of the σ_2 calculation of Lemma 2 depends on which branch is indicated by the branch index variable Z.*

Proof. The derivative for the calculation of σ_2 is shown in Formula (38).

$$-\frac{\left(W_Z\left(-\frac{2i\Delta F e^{-i\epsilon}e^{-\frac{i\Delta F e^{-i\epsilon}}{\sigma_1}}}{\sigma_1}\right)+i\epsilon\right)\Delta F e^{i\epsilon}\sigma_1}{\left(W_Z\left(-\frac{2i\Delta F e^{-i\epsilon}e^{-\frac{i\Delta F e^{-i\epsilon}}{\sigma_1}}}{\sigma_1}\right)e^{i\epsilon}\sigma_1 + i\Delta F\right)\left(W_Z\left(-\frac{2i\Delta F e^{-i\epsilon}e^{-\frac{i\Delta F e^{-i\epsilon}}{\sigma_1}}}{\sigma_1}\right)+1\right)} \tag{38}$$

We start by studying the sign of the first factor in the denominator. We will show that it is always negative by proving Formula (39).

$$W_Z\left(-\frac{2i\Delta F e^{-i\epsilon}e^{-\frac{i\Delta F e^{-i\epsilon}}{\sigma_1}}}{\sigma_1}\right)e^{i\epsilon}\sigma_1 < -i\Delta F \tag{39}$$

This can be re-written as:

$$W_Z\left(-\frac{2i\Delta F e^{-i\epsilon}e^{-\frac{i\Delta F e^{-i\epsilon}}{\sigma_1}}}{\sigma_1}\right) < -\frac{i\Delta F e^{-i\epsilon}}{\sigma_1} \tag{40}$$

Since $W_Z(xe^x) = x$, we can replace the right-hand side with the appropriate LambertW function. To do this, we must determine which branch should be used. If the value of x in the aforementioned identity is greater than or equal to -1, the principal branch should be used, otherwise, the -1 branch should be used. To determine which of these should be used, we substitute the σ_1 variable of the right-hand side with its selected value from Lemma 2 and analyze the resulting function of the variable i shown in Formula (41).

$$i\epsilon e^{-i\epsilon+1}W\left(-\frac{1}{2e}\right) \tag{41}$$

To identify what values this function can take on, we first calculate its derivate as shown in Formula (42).

$$\epsilon e^{-i\epsilon+1} W\left(-\frac{1}{2e}\right)(1-i\epsilon) \tag{42}$$

Since the derivative has a single zero at $i = \frac{1}{\epsilon}$, the function is unimodal. The value of the derivative at $i = 0$ is negative therefore, the mode is a minimum. The lowest value that Formula (41) can take on is therefore $W\left(-\frac{1}{2e}\right)$ which is greater than -1. As a result, the principal branch should be used to apply the LambertW identity to Formula (40). This produces Formula (43).

$$W_Z\left(-\frac{2i\Delta F e^{-i\epsilon} e^{-\frac{i\Delta F e^{-i\epsilon}}{\sigma_1}}}{\sigma_1}\right) < W\left(-\frac{i\Delta F e^{-i\epsilon} e^{-\frac{i\Delta F e^{-i\epsilon}}{\sigma_1}}}{\sigma_1}\right) \tag{43}$$

To determine the relationship between the left-hand side and right-hand side, we can compare the input being given to each function:

$$-\frac{2i\Delta F e^{-i\epsilon} e^{-\frac{i\Delta F e^{-i\epsilon}}{\sigma_1}}}{\sigma_1} < -\frac{i\Delta F e^{-i\epsilon} e^{-\frac{i\Delta F e^{-i\epsilon}}{\sigma_1}}}{\sigma_1} \tag{44}$$

This relationship can be simplified to $-2 < -1$. This shows that the input given to the function on the left-hand side will always be less than the input given to the function on the right-hand side. The relationship between the two LambertW functions can now be determined based on which branch the variable Z indicates. If Z is 0 then the left-hand side is less than the right-hand side, making the factor negative. If Z is -1 then the left-hand side will still be less than the right-hand side since the output of the -1 branch is always less than or equal to the output of the principal branch. Therefore, in either case, the factor is negative.

Next, we study the second factor in the denominator of the derivative:

$$W_Z\left(-\frac{2i\Delta F e^{-i\epsilon} e^{-\frac{i\Delta F e^{-i\epsilon}}{\sigma_1}}}{\sigma_1}\right) + 1 \tag{45}$$

Since the output of the principal branch of a LambertW function is always greater than or equal to -1, this factor will always be positive when Z is 0. If Z is -1 then the output of the LambertW function is always less than or equal to -1, making the sign of the factor negative.

Taking the signs of both factors into account, we can see that the sign of the denominator will always be negative for the principal branch and will always be positive for the -1 branch. ☐

Lemma 4. *As a function of i, the σ_2 calculation of Lemma 2 is unimodal for either branch index.*

Proof. Since the sign of the denominator of its derivative cannot change when restricted to the same branch index, the only remaining component that could induce a sign change is the first factor in the numerator:

$$W_Z\left(\frac{2i\Delta F e^{\frac{-i\Delta F}{\sigma_1 e^{i\epsilon}}}}{-\sigma_1 e^{i\epsilon}}\right) + i\epsilon \tag{46}$$

To find when this can be equal to 0, we use the identity of $W_Z(xe^x) = x$, setting the variable x to be $-i\epsilon$. We therefore must find when the following equality is true:

$$-\frac{2i\Delta F e^{-i\epsilon} e^{-\frac{i\Delta F e^{-i\epsilon}}{\sigma_1}}}{\sigma_1} = -i\epsilon e^{-i\epsilon} \tag{47}$$

When $i = 0$, both sides will be equal to 0, however this does not constitute a sign change in the derivative since this is at the beginning of the input range. To find any other zeros, we can isolate i to get:

$$i = -\frac{W_Z\left(\frac{ln\left(\frac{\epsilon\sigma_1}{2\Delta F}\right)\epsilon\sigma_1}{\Delta F}\right)}{\epsilon} \tag{48}$$

Each LambertW branch therefore has its own zero using the corresponding branch index. Since the full derivative has only one sign change when considering W and W_{-1} separately, each of the functions are unimodal. □

Lemma 5. *As a function of i, the input to W_Z in the σ_2 calculation of Lemma 2 is unimodal and is initially decreasing.*

Proof. Recall that the input to the LambertW function is as shown in Formula (49).

$$-\frac{2i\Delta Fe^{-i\epsilon}e^{-\frac{i\Delta Fe^{-i\epsilon}}{\sigma_1}}}{\sigma_1} \tag{49}$$

The input is equal to 0 when $i = 0$. Since all variables used here must be greater than or equal to 0 and there is a negative sign in front of the input, the value will always be less than or equal to 0. We can therefore infer that it must initially be decreasing as i increases. To determine the modality, we study the derivative of the input with respect to i as shown in Formula (50):

$$-\frac{2\Delta Fe^{-i\epsilon}e^{-\frac{i\Delta Fe^{-i\epsilon}}{\sigma_1}}\left(i\epsilon - 1\right)\left(i\Delta Fe^{-i\epsilon} - \sigma_1\right)}{{\sigma_1}^2} \tag{50}$$

From the derivative, we can see that a sign change could occur when any of the following cases occur:

$$i = \frac{1}{\epsilon} \tag{51}$$

$$\sigma_1 = i\Delta Fe^{-i\epsilon} \tag{52}$$

Formula (51) represents a valid point in the span of truncated space and thus constitutes a change in modality.

For Formula (52), we have isolated this in terms of σ_1 in order to study the LambertW function at this point. By substituting σ_1 in Formula (49) with the right-hand side of Formula (52), we obtain the following:

$$-\frac{2i\Delta Fe^{-i\epsilon}e^{-\frac{i\Delta Fe^{-i\epsilon}}{i\Delta Fe^{-i\epsilon}}}}{i\Delta Fe^{-i\epsilon}} \tag{53}$$

After simplification, this expression reduces to $-\frac{2}{e}$. Since the LambertW function only produces real-valued output when the input given is in the range of $[-\frac{1}{e}, \infty)$, we can see that a sign change cannot occur here. The function of Formula (49) is therefore unimodal with its mode occurring at the zero specified in Formula (51). □

Lemma 6. *As a function of i, the mode of the σ_2 calculation of Lemma 2 is a minimum for the principal branch and a maximum for the -1 branch.*

Proof. From Lemma 4, we know that the function is unimodal and that the sign of its rate of change depends on the sign of the function in Formula (46). From Lemma 5, we know that the input to W_Z in Formula (37) is initially decreasing until its mode and is then increasing. This implies that W will also be decreasing until the same mode and then increasing and that W_{-1} will be increasing until the same mode and then decreasing.

Since the function of $i\epsilon$ is monotonically increasing, the only way a zero can occur in Formula (46) for the principal branch is if W is initially decreasing faster than $i\epsilon$ is increasing such that the sign of Formula (46) is initially negative. In this way, as the rate of change of W increases, the sign will eventually become positive. This implies that Formula (46) must initially be negative for the principal branch. For the -1 branch, since the input is initially decreasing from 0, W_{-1} will be initially increasing from negative infinity, making Formula (46) initially negative.

Thus, for both branches, the overall sign of the numerator of the derivative is positive prior to the mode. From Lemma 3, we know that the sign of the denominator is negative for the principal branch, making its mode a minimum and that the sign of the denominator is positive for the -1 branch, making its mode a maximum. □

Theorem 1. *The σ calculation method of Lemma 2 provides a solution which optimally satisfies the differential privacy guarantee.*

Proof. Lemma 2, provides a method of calculating σ values that satisfy the bounds identified in Lemma 1. The additional condition that the σ values are monotonically decreasing as i increases must also be proven in order for the worst-case analysis of the continuous random variable (Section 3.5, main document) to be applicable.

When using the σ_1 value of Formula (33), the mode specified in Formula (48) reduces to $i = \frac{1}{\epsilon}$ for both branches of Formula (37). By Lemma 6, the principal branch is decreasing until its mode and that the -1 branch is decreasing after its mode. Thus, by using the principal branch to calculate the values of σ_2 prior to $i = \frac{1}{\epsilon}$ and the -1 branch after this point, all σ values will be monotonically decreasing as i increases.

We must also consider the symmetric form of the privacy guarantee. Let K be a function representing the randomization mechanism. Since the calculations from Lemma 2 make both sides of the privacy guarantee equal to each other, the guarantee written using K would be as shown in Formula (54).

$$\Pr\left(K(D_1) = x\right) = e^{i\epsilon} \Pr\left(K(D_2) = x\right), \qquad \forall D_1, D_2 \in \mathbb{D} : f\left(D_1\right) \geq f\left(D_2\right) \tag{54}$$

To prove the symmetric form of the guarantee, we must show that the condition shown in Formula (55) holds.

$$\Pr\left(K(D_2) = x\right) \leq e^{i\epsilon} \Pr\left(K(D_1) = x\right), \qquad \forall D_1, D_2 \in \mathbb{D} : f\left(D_1\right) \geq f\left(D_2\right) \tag{55}$$

Since ϵ and i must be positive, we know that $e^{i\epsilon} \geq 1$. Therefore, from Formula (54), we can infer Formula (56) which shows that the guarantee for the symmetric form is satisfied.

$$\Pr\left(K(D_2) = x\right) \leq \Pr\left(K(D_1) = x\right), \qquad \forall D_1, D_2 \in \mathbb{D} : f\left(D_1\right) \geq f\left(D_2\right) \tag{56}$$

Finally, we must consider the optimality of the σ values. Since lower σ values are preferable, we will show that it is not possible to calculate lower σ values that could satisfy the privacy guarantee.

By Lemma 1, σ values must fall into one of the two spans specified in Formulae (3) and (4). By Lemma 2, the right-hand sides of Formulae (3) and (4) are equivalent to Formula (37) using the σ_1 value of Formula (33). Therefore, these two bounds are characterized in the same way according to Lemma 6. This implies that that prior to $i = \frac{1}{\epsilon}$ any σ values chosen in the span of Formula (4) would be increasing as i increases which violates the requirement of monotonically decreasing σ values. We are therefore restricted to the span of Formula (3) and since we always select the lowest value in this span, our method of calculating σ values prior to $i = \frac{1}{\epsilon}$ is optimal.

After $i = \frac{1}{\epsilon}$, the σ values we select are on the upper bound of Formula (4). It is therefore possible to select lower σ values in this span without violating the requirement of having monotonically decreasing σ values. However, since we are also selecting σ values that are on the bounds of Formula (2), the only way to select a lower σ value while still satisfying the privacy guarantee is to raise the value of all prior choices. Doing so means that higher σ values must be used at $i = 0$ and $i = \frac{1}{\epsilon}$. The use of a higher σ value at $i = 0$ has the effect of shifting the mode of the right-hand side of Formula (1) to the left on the i-axis. Since the mode used to be at $i = \frac{1}{\epsilon}$, we now end up with a σ value at $i = \frac{1}{\epsilon}$ which is past the mode of Formula (1) and is also higher than that mode. As a result, in order to satisfy the bound of Formula (1), it is necessary that some of the preceding σ values are lower than that at $i = \frac{1}{\epsilon}$, however, this again violates the requirement of having monotonically decreasing σ values as i increases.

Thus, for values of i both smaller and larger than $\frac{1}{\epsilon}$, the σ values calculated in Lemma 2 are optimal. $\square$

A2 - Arbitrary Finite Constraints

In this section, we provide the full proofs pertaining to Section 5.1.3 of the main paper.

Lemma 7. *For each span of truncated space, there exists a value of σ for which the privacy guarantee is satisfied for any pair of PDFs with location parameters within that span.*

Proof. Recall that the privacy guarantee for this constraint configuration class is as shown in Formula (57).

$$\frac{1-\left(L_1 e^{\frac{i\Delta F}{\sigma}}+R_1 e^{-\frac{i\Delta F}{\sigma}}\right)}{1-(L_1+R_1)}\left(e^{\frac{i\Delta F}{\sigma}}\right)\leq e^{i\epsilon} \tag{57}$$

When $i=0$, both sides of Formula (57) will be equal to each other. It is therefore a necessary condition to ensure that the rate of change of the left-hand side with respect to the variable i is initially less than or equal to that of the right-hand side. The derivatives with respect to i of the left-hand side and right-hand side are shown in Formulae (58) and (59) respectively.

$$\frac{\Delta F e^{\frac{i\Delta F}{\sigma}}\left(2L_1 e^{\frac{i\Delta F}{\sigma}}-1\right)}{\sigma\left(L_1+R_1-1\right)} \tag{58}$$

$$\epsilon e^{i\epsilon} \tag{59}$$

Since we must ensure that the derivative of the left-hand is less than or equal to the derivative of the right-hand side when $i=0$, we set all instances of i to 0 and obtain Formula (60).

$$\frac{\Delta F\left(2L_1-1\right)}{\sigma\left(L_1+R_1-1\right)}\leq\epsilon \tag{60}$$

Through rearrangement and application of identities, we can produce Formula (61).

$$\sigma\geq\frac{\Delta F}{\epsilon-\frac{\Delta F(L_1-R_1)}{\sigma(L_1+R_1-1)}} \tag{61}$$

We will consider the use of the lowest σ value that satisfies this inequality. Since this remains a recursive definition of σ, we cannot use this to actually calculate that value. We will show later how to do so. For now, we will simply treat the right-hand side of this inequality as an identity of the required value of σ.

Using this value of σ, we know that both sides of the guarantee will initially have an equal rate of change with respect to i. We must now show that this value of σ preserves the guarantee for higher values of i. We substitute the σ identity into exponential function appearing just before the inequality symbol in Formula (57) to obtain the form shown in Formula (62). Note that we do not substitute this value into the other occurrences of σ. As we will see, any positive value for σ could be applied to those occurrences while still satisfying the guarantee.

$$\frac{1-\left(L_1 e^{\frac{i\Delta F}{\sigma}}+R_1 e^{-\frac{i\Delta F}{\sigma}}\right)}{1-(L_1+R_1)}\left(e^{\frac{i\Delta F}{\frac{\Delta F}{\epsilon-\frac{\Delta F(L_1-R_1)}{\sigma(L_1+R_1-1)}}}}\right)\leq e^{i\epsilon} \tag{62}$$

After simplification, this can be re-written as shown in Formula (63).

$$\frac{1-\left(L_1e^{\frac{i\Delta F}{\sigma}}+R_1e^{-\frac{i\Delta F}{\sigma}}\right)}{1-(L_1+R_1)}\left(e^{i\epsilon-\frac{i\Delta F(L_1-R_1)}{\sigma(L_1+R_1-1)}}\right)\leq e^{i\epsilon} \tag{63}$$

Now by rearranging, we can write the guarantee as shown in Formula (64).

$$\frac{1-\left(L_1e^{\frac{i\Delta F}{\sigma}}+R_1e^{-\frac{i\Delta F}{\sigma}}\right)}{1-(L_1+R_1)}\leq e^{\frac{i\Delta F(L_1-R_1)}{\sigma(L_1+R_1-1)}} \tag{64}$$

Since both sides of the original guarantee were equal to each other when $i=0$, regardless of the choice of σ, the same is true of this version. Furthermore, since we have chosen a value for σ that ensures the rate of change is the same on both sides when $i=0$, the same is true in this version as well. It remains to show that as i increases, the right-hand side will grow more quickly than the left-hand side. To show this, we look at the second derivatives of the left and right sides shown in Formulae (65) and (66) respectively.

$$\frac{\Delta F^2\left(L_1e^{\frac{i\Delta F}{\sigma}}+R_1e^{-\frac{i\Delta F}{\sigma}}\right)}{\sigma^2\left(L_1+R_1-1\right)} \tag{65}$$

$$\frac{\Delta F^2\left(L_1-R_1\right)^2}{\sigma^2\left(L_1+R_1-1\right)^2}\left(e^{\frac{i\Delta F(L_1-R_1)}{\sigma(L_1+R_1-1)}}\right) \tag{66}$$

Since the variables L_1 and R_1 represent the summations of the integrals of the finite constraints to the left and right respectively of the location parameter $f(D_1)$, both of them have a range of $[0,0.5)$. When L_1 and R_1 are restricted to these ranges, the expression in Formula (65) will always be negative and the expression in Formula (66) will always be positive. This means that the derivative of the left-hand side is decreasing and the derivative of the right-hand side is increasing. As such, the left-hand side will always be less than or equal to the right-hand side, meaning that the guarantee is satisfied when using the σ value taken as the lower bound from Formula (61). □

Lemma 8. *Within each span of truncated space, the σ value determined from Lemma 7 acts as a lower bound for the value of σ required to satisfy the privacy guarantee.*

Proof. Starting from the value of σ obtained by using Formula (61) as an equality (as was done in Lemma 7), we can represent a larger value of σ by subtracting some value α from the denominator such that α is not greater than or equal to the original value of the denominator. This form is shown in Formula (67)

$$\sigma\geq\frac{\Delta F}{\epsilon-\frac{\Delta F(L_1-R_1)}{\sigma(L_1+R_1-1)}-\alpha} \tag{67}$$

Using this new σ value, we can repeat the steps of Formulae (62) through (64) to obtain Formula (68).

$$\frac{1-\left(L_1e^{\frac{i\Delta F}{\sigma}}+R_1e^{-\frac{i\Delta F}{\sigma}}\right)}{1-(L_1+R_1)}\leq e^{\frac{i\Delta F(L_1-R_1)}{\sigma(L_1+R_1-1)}+i\alpha} \tag{68}$$

The only difference between Formula (64) and Formula (68) is that the exponent of the right-hand side has become larger, making the guarantee easier to satisfy. It therefore follows that any σ value larger than that which was found to be required will also satisfy the privacy guarantee. □

Lemma 9. *For each finite constraint, there exists a value of σ that satisfies the privacy guarantee for the pair of PDFs with location parameters on the endpoints of the constraint.*

Proof. The guarantee form used thus far has used the same sets of finite constraints to the left and right of both location parameters, implying that they must both lie within the same span of truncated space. We must also be able to show that the privacy guarantee holds for location parameters in different spans of truncated space. To show this, we first consider a pair of PDFs with location parameters that lie on opposite endpoints of a finite constraint (with $f(D_1)$ as always being the point on the right).

For two such location parameters, the sets of constraints that lie to their left and right now differ by exactly one constraint span, the one that separates them. We can still indicate the distances between the location parameter $f(D_2)$ and the constraints to its left in terms of the set of constraints to the left of $f(D_1)$. However, we must omit the separating constraint from the summation in L_1 for the normalization factor of D_2. This can be done by subtracting the value of its integral from the summation. Logically, that same value would be added to the summation in R_1 of constraints to the right of $f(D_2)$, however, we must account for how the distance between $f(D_2)$ and the separating constraint differs from the cases with the other constraints. Normally, $f(D_2)$ is $i\Delta F$ farther from the each constraint to its right than $f(D_1)$ is but in this case, since the two location parameters are each on an endpoint of the separating constraint, they are both at a distance of 0 from the constraint. This means that the value of the separating integral is identical for both PDFs. As a result, rather than adding this value to the summation in R_1 for the normalization factor of D_2 (which would cause the integral to be scaled down), it is added independently to the total summation of integral values. Using a variable S as defined in Formula (69) to represent the integral of the separating constraint, this modified version of the privacy guarantee can be written as shown in Formula (70).

$$S = \frac{1 - e^{-\frac{i\Delta F}{\sigma}}}{2} \tag{69}$$

$$\frac{1 - \left(e^{\frac{i\Delta F}{\sigma}}\left(L_1 - S\right) + R_1 e^{-\frac{i\Delta F}{\sigma}} + S\right)}{1 - (L_1 + R_1)} \left(e^{\frac{i\Delta F}{\sigma}}\right) \leq e^{i\epsilon} \tag{70}$$

We know from Lemma 7 that a sufficiently high value of σ can satisfy the guarantee without the modification made here and from Lemma 8 that raising the value of σ beyond the requirement causes the difference between the left and right sides of the guarantee to grow more quickly. We can also see that increasing σ reduces the influence of S by causing the value of S to asymptotically approach 0. It therefore follows that a sufficiently high value of σ will also satisfy this form of the privacy guarantee. ☐

Lemma 10. *All lower bounds on σ identified in Lemmas 7 and 9 are less than $\frac{2\Delta F}{\epsilon}$.*

The proof of this is provided in the appendix. The calculations for lower bounds on σ can be handled by treating Formulae (61) and (70) as equalities and solving for σ. We can identify bounds on the possible values of σ by studying the bounds on the variables L_1 and R_1. Since L_1 represents the sum of the integrals of the constraints to the left of $f(D_1)$ it can be as low as 0 (if no constraints are present to the left of $f(D_1)$) and can approach but not reach 0.5 (since half of the integral exists on the left hand side). The bounds on R_1 are characterized in the same way. By studying the the ranges of the lower bounds for σ, it can be shown that for bounds from both equations, σ will fall in the range of $\left(0, \frac{2\Delta F}{\epsilon}\right)$.

Theorem 2. *The optimal σ value that satisfies the privacy guarantee for all pairs of databases can be found by taking the maximum out of $3n + 2$ lower bounds, where n is the number of finite constraints.*

Proof. Lemma 7 provides a lower bound on σ for pairs of PDFs with location parameters in the same span of truncated space. This applies to a form of the privacy guarantee in which $f(D_2) \leq f(D_1)$ holds. The symmetric case can be handled in the same way after an application of horizontal reflection to the configuration. Since the same value of σ must be used everywhere, it is necessary to select the maximum of the lower bounds. By Lemma 8, the privacy guarantee is still satisfied within each span of truncated space under the use of a value of σ greater than the lower bound.

Lemma 9 provides an additional bound on σ for PDFs with location parameters on opposite endpoints of a constraint. In Formula (70), if the fraction on the left-hand side is inversed, as it would be in a symmetric form, the left-hand side decreases. Thus if the form in Formula (70) is satisfied, the symmetric form will be as well.

For n constraints, there are $n+1$ lower bounds on σ in Lemma 7 from the regular form of the privacy guarantee and an additional $n+1$ lower bounds for the symmetric form. From Lemma 9, there are n lower bounds, giving a total of $3n+2$. By selecting the largest of these, the guarantee is satisfied for all pairs of PDFs with location parameters in any same span of truncated space and for all pairs of PDFs with location parameters on opposite endpoints of a constraint. Since each of the lower bounds must be adhered to, it is not possible to select a lower value of σ than this.

It remains to be shown that any arbitrary pair of databases is also protected. This follows as a transitive property of multiple applications of the guarantee forms used throughout the lemmas. For any pair of PDFs with location parameters at arbitrary points in truncated space, it is possible to represent this as a sequence of points where each adjacent pair of points in the sequence corresponds to a pair of PDF location parameters in the configuration used in either Lemma 7 or Lemma 9. The multiplicative bound for the arbitrary pair is therefore the product of the bounds of the adjacent pairs in the sequence. Since each of the adjacent pairs satisfy the privacy guarantee, the product will also satisfy the guarantee for the arbitrary pair. ☐

Theorem 3. *The optimal value of σ for any configuration of n arbitrary finite constraints can be calculated to a precision of d decimal places in $O\left(n^2\left(d+\log\left(\frac{\Delta F}{\epsilon}\right)\right)\right)$ time.*

Proof. As stated in Theorem 2, σ must be chosen as the maximum value out of the $O(n)$ lower bounds calculated from Formulae (61) and (70). The variables L_1 and R_1 in these inequalities represent summations of $O(n)$ exponential functions where each function contains an instance of σ in the denominator of its exponent. We know of no method to isolate σ for such configurations. It therefore takes $O\left(n^2\right)$ time to check whether a given value of σ is above all lower bounds.

From Lemmas 8 and 9, we know that any value of σ larger than the required value will also satisfy the privacy guarantee. This tells us that once the inequality is satisfied, increasing σ further will never violate the inequality. Lemma 10 indicates that the value of σ will always be between 0 and $\frac{2\Delta F}{\epsilon}$, meaning that for a decimal precision of d, there are $\frac{2\left(10^d\right)\Delta F}{\epsilon}$ possible values for σ. By performing a binary search for the optimal value, the logarithm of the number of possible values of σ must be checked, leading to an overall time complexity of $O\left(n^2\left(d+\log\left(\frac{\Delta F}{\epsilon}\right)\right)\right)$. In most cases, the values of d and ΔF are likely to be small, making $O\left(n^2\right)$ a more practical representation of the time complexity. ☐