A PROOF OF LEMMA 4.4

Let R_1^0, R_1^1, and R_i denote the probability distributions of the random variable $\mathcal{R}_1(x_1^0)$, $\mathcal{R}_1(x_1^1)$, and $\mathcal{R}_i(x_i)$, respectively. We establish the existence of mixture distributions through a constructive proof. Specifically, for any $y \in \mathbb{Y}$ in the output domain, we define the probability distributions of $Q_1^0, Q_1^1, Q_1, Q_2, \ldots$, and Q_n as follows:

$$Q_1^0[y] = \begin{cases} \frac{R_1^0[y]-R_1^1[y]}{(p-1)\alpha}, & \text{if } R_1^0[y] > R_1^1[y]; \\ 0, & \text{else,} \end{cases}$$

$$Q_1^1[y] = \begin{cases} \frac{R_1^1[y]-R_1^0[y]}{(p-1)\alpha}, & \text{if } R_1^0[y] < R_1^1[y]; \\ 0, & \text{else,} \end{cases}$$

$$Q_1[y] = \frac{\min\{R_1^1[y], R_1^0[y]\}}{1-\alpha-p\alpha} - \frac{|R_1^0[y]-R_1^1[y]|}{(p-1)(1-\alpha-p\alpha)},$$

$$Q_i[y] = \frac{R_i[y] - r(Q_1^0[y]+Q_1^1[y])}{1-2r}.$$

We first demonstrate the validity of probability distributions Q_1^0 and Q_1^1. Specifically, for Q_1^0, it can be observed that $Q_1^0[y]$ is non-negative for all $y \in \mathbb{Y}$, and $\sum_{y\in\mathbb{Y}} Q_1^0[y] = \frac{D_1(\mathcal{R}_1(x_1^0)|\mathcal{R}_1(x_1^1))}{(p-1)\alpha} = \frac{\beta'}{\beta'} = 1$, thereby verifying it as a valid probability distribution. Likewise, we establish Q_1^1 as a valid distribution.

Furthermore, we prove that Q_1 is a valid distribution, and we demonstrate that Equations 1 and 2 hold. Applying the (p, β')-variation property, we obtain $\max\{R_1^0[y], R_1^1[y]\} \leq p \cdot \min\{R_1^0[y], R_1^1[y]\}$, thus verifying that $Q_1[y]$ is non-negative. Additionally, since $p\alpha + \alpha + (1 - \alpha - p\alpha) = 1$, it follows that

$$\sum_{y\in\mathbb{Y}} Q_1[y] = \frac{\sum_{y\in\mathbb{Y}} R_1^0[y] - p\alpha Q_1^0[y] - \alpha Q_1^1[y]}{(1-\alpha-p\alpha)} = 1,$$

indicating that Q_1 is indeed a valid distribution.

Next, we demonstrate that Equation 1 holds. When $R_1^0[y] \geq R_1^1[y]$, we have $p\alpha Q_1^0[y] + \alpha Q_1^1[y] + (1-\alpha-p\alpha)Q_1[y] = (R_1^0[y] - R_1^1[y])p/(p-1) + R_1^1[y] - (R_1^0[y] - R_1^1[y])/(p-1) = R_1^0[y]$. When $R_1^0[y] < R_1^1[y]$, we have $p\alpha Q_1^0[y] + \alpha Q_1^1[y] + (1-\alpha-p\alpha)Q_1[y] = (R_1^1[y] - R_1^0[y])/(p-1) + R_1^0[y] - (R_1^1[y] - R_1^0[y])/(p-1) = R_1^0[y]$. Combining these two cases, we obtain Equation 1. Similarly, we can show that Equation 2 holds by symmetry.

Finally, we demonstrate the validity of Q_i and the satisfaction of Equation 3. By invoking the q-ratio property of R_i, we obtain $R_i[y] \geq \max\{R_1^0[y], R_1^1[y]\}/q$. Consequently, we obtain $R_i[y] \geq \max\{p\alpha Q_1^0[y], p\alpha Q_1^1[y]\}/q$. Notably, we can infer that $Q_1^0[y]$ and $Q_1^1[y]$ are never simultaneously greater than 0. As such, we conclude that $R_i[y] \geq p\alpha(Q_1^0[y] + Q_1^1[y])/q \geq r(Q_1^0[y] + Q_1^1[y])$, thereby leading to $Q_i[y]$ being non-negative. Furthermore, we utilize the fact that $r + r + (1-2r) = 1$, which enables us to establish that Q_i is a valid distribution. For the right-hand side of Equation 3, if $Q_1^0[y] \geq Q_1^1[y]$, we obtain $rQ_1^0[y] + rQ_1^1[y] + (1-2r)Q_i[y] = rQ_1^0[y] + R_i[y] - rQ_1^0[y] = R_i[y]$. Alternatively, if $Q_1^0[y] < Q_1^1[y]$, we obtain $rQ_1^0[y] + rQ_1^1[y] + (1-2r)Q_i[y] = rQ_1^1[y] + R_i[y] - rQ_1^1[y] = R_i[y]$. Combining these two conditional results establishes the satisfaction of Equation 3.

Let $c = a + b$, the condition

$$\frac{\mathbb{P}[P_{p,\beta}^q = (a,b)]}{\mathbb{P}[Q_{p,\beta}^q = (a,b)]} = \frac{p\alpha a + \alpha b + (1-\alpha-\alpha p)(n-a-b)\cdot\frac{r}{1-2r}}{\alpha a + p\alpha b + (1-\alpha-\alpha p)(n-a-b)\cdot\frac{r}{1-2r}} > e^{\epsilon'}$$

holds *if and only if* when $a > low_c = \frac{(e^{\epsilon'}p-1)\alpha c+(e^{\epsilon'}-1)f}{\alpha(e^{\epsilon'}+1)(p-1)}$. Let $P = (A, C-A)$, $P_0 = (A+1, C-A)$ and $P_1 = (A, C-A+1)$, then the Hockey-stick divergence becomes:

$$
\begin{aligned}
&D_{e^\epsilon}(P^q_{p,\beta} \| Q^q_{p,\beta}) \\
&= \sum_{a,b\in[0,n]^2} \max\left\{0, \mathbb{P}[P^q_{\beta,p} = (a,b)] - e^\epsilon \mathbb{P}[Q^q_{\beta,p} = (a,b)]\right\} \\
&= \sum_{c\in[0,n]} \sum_{a\in[\lceil low_c \rceil, c]} \mathbb{P}[P^q_{p,\beta} = (a, c-a)] - e^\epsilon \mathbb{P}[Q^q_{p,\beta} = (a, c-a)] \\
&= \sum_{c\in[0,n]} \sum_{a\in[\lceil low_c \rceil, c]} (p - e^\epsilon)\alpha \mathbb{P}[P_0 = (a, c-a)] \\
&\quad + \sum_{c\in[0,n]} \sum_{a\in[\lceil low_c \rceil, c]} (1 - pe^\epsilon)\alpha \mathbb{P}[P_1 = (a, c-a)] \\
&\quad + \sum_{c\in[0,n]} \sum_{a\in[\lceil low_c \rceil, c]} (1 - \alpha - \alpha p)(1 - e^\epsilon) \mathbb{P}[P = (a, c-a)].
\end{aligned}
$$

Pluging into the probability formulas of $\mathbb{P}[P_0 = (a, c-a)], \mathbb{P}[P_1 = (a, c-a)]$ and $\mathbb{P}[P = (a, c-a)]$, we arrive at the conclusion.

B PROOF OF THEOREM 5.1

Given $x_2 = x^*, ..., x_n = x^*$, we consider the shuffled messages obtained from applying the mechanism $\mathcal{S}$ to $\mathcal{R}_1(x_1^0), \mathcal{R}_2(x^*)$, ..., $\mathcal{R}_2(x^*)$ and $\mathcal{R}_1(x_1^1), \mathcal{R}_2(x^*), ..., \mathcal{R}_2(x^*)$. Let $g : \mathbb{Y} \mapsto \{0,1\}^2$ be a post-processing function on a single message, where $\mathbb{Y}$ denotes the message space. For any $y \in \mathbb{Y}$, we define $g(y)$ as follows:

$$
g(y) = \begin{cases} (1,0), & \text{if } \mathbb{P}[R_1(x_1^0) = y] > \mathbb{P}[R_1(x_1^1) = y]; \\ (0,1), & \text{if } \mathbb{P}[R_1(x_1^0) = y] < \mathbb{P}[R_1(x_1^1) = y]; \\ (0,0), & \text{else.} \end{cases}
$$

We also define $g_n : \mathbb{Y}^n \mapsto \mathbb{N}^2$ as a function on n shuffled messages S, where $g_n(S) = \sum_{s\in\mathcal{S}} g(s)$ is the vector summation of $g(s)$. It is observed that $g_n(\mathcal{R}_1(x_1^0), \mathcal{R}_2(x^*), ..., \mathcal{R}_2(x^*)) \overset{d}{=} P^{q_0,q_1}_{p_0,\beta}$ and $g_n(\mathcal{R}_1(x_1^1), \mathcal{R}_2(x^*), ..., \mathcal{R}_2(x^*)) \overset{d}{=} Q^{q_0,q_1}_{p_0,\beta}$. By applying the data-processing inequality property of D, we arrive at our conclusion.

C PROOF OF LEMMA 4.5

This lemma generalizes the stronger clone reduction presented in [27, Lemma 3.2], where all local randomizers satisfy LDP and r must equals to α, albeit with a similar underlying proof. Let $x_1^0, \ldots, x_n$ and $x_1^1, \ldots, x_n$ be two neighboring datasets. We define the following distributions for $i \in [1, n]$:

$$
Y_i = \begin{cases} 0 & \text{w.p. } r \\ 1 & \text{w.p. } r \\ i+1 & \text{w.p. } 1-2r \end{cases}, \quad Y_1^0 = \begin{cases} 0 & \text{w.p. } p\alpha \\ 1 & \text{w.p. } \alpha \\ 2 & \text{w.p. } 1-p\alpha-\alpha \end{cases}, \quad Y_1^1 = \begin{cases} 0 & \text{w.p. } \alpha \\ 1 & \text{w.p. } p\alpha \\ 2 & \text{w.p. } 1-p\alpha-\alpha \end{cases}. \tag{5}
$$

We now consider two independent sampling processes: (i) we draw one sample from Y_1^0, and one sample from every Y_i (for $i \in [2, n]$); (ii) we draw one sample from Y_1^1, and one sample from every Y_i (for $i \in [1, n]$). Using the mixture property of $\mathcal{R}_1$ and $\mathcal{R}_i$ (for $i \in [2, n]$), we obtain $\mathcal{S}(\mathcal{R}_1(x_1^0), \ldots, \mathcal{R}_n(x_n))$ and $\mathcal{S}(\mathcal{R}_1(x_1^1), \ldots, \mathcal{R}_n(x_n))$ by post-processing $\mathcal{S}(Y_1^0, Y_2, \ldots, Y_n)$ and $\mathcal{S}(Y_1^1, Y_2, \ldots, Y_n)$ through some function $G : [0, n+1]^n \mapsto \mathbb{Y}^n$.

We now focus on the statistical divergence between $\mathcal{S}(Y_1^0, Y_2, \ldots, Y_n)$ and $\mathcal{S}(Y_1^1, Y_2, \ldots, Y_n)$. Since they differ only in random variables Y_1^0, Y_1^1, and the two distributions differ only in the probability distribution over 0, 1, the 2, 3, ..., $n+1$ terms in $\mathcal{S}(Y_1^0, Y_2, \ldots, Y_n)$ and $\mathcal{S}(Y_1^1, Y_2, \ldots, Y_n)$ can be omitted. Formally, for any distance measure D that satisfies the data processing inequality, our goal is to prove that the following inequalities hold:

$$
\begin{aligned}
D(\mathcal{S}(Y_1^0, Y_2, \ldots, Y_n) \| \mathcal{S}(Y_1^1, Y_2, \ldots, Y_n)) \leq D(P' \| Q'), \\
D(\mathcal{S}(Y_1^0, Y_2, \ldots, Y_n) \| \mathcal{S}(Y_1^1, Y_2, \ldots, Y_n)) \geq D(P' \| Q').
\end{aligned}
$$

For the first inequality, we define the following post-processing function over P' or Q': (1) assume two numbers in P' or Q' are (a, b), uniformly sample $n-a-b$ elements from $[3, n+1]$ (denoted as E); (2) with probability of $\frac{(n-a-b)(1-p\alpha-\alpha)(2r)}{(n-a-b)(1-p\alpha-\alpha)(2r)+(a+b)(p\alpha+\alpha)(1-2r)}$, replace one uniform-random element in E with 2; (3) initialize a list of a-repeat 0s and b-repeat 1s, then append E to the list, finally uniform-randomly shuffle the list. It can be observed that the post-processing result of P' distributionally equals to $\mathcal{S}(Y_1^0, Y_2, \ldots, Y_n)$ and the post-processing result of Q' distributionally equals to $\mathcal{S}(Y_1^1, Y_2, \ldots, Y_n)$. By applying the data processing inequality, we obtain

$D(\mathcal{S}(Y_1^0, Y_2, \ldots, Y_n)\|\mathcal{S}(Y_1^1, Y_2, \ldots, Y_n)) \leq D(P'\|Q')$. For the second inequality, we define the following post-processing function over the output of $\mathcal{S}(Y_1, Y_2, \ldots, Y_n)$ (either $Y_1 = Y_1^0$ or $Y_1 = Y_1^1$): remove all $2, \ldots, n+1$ from the output. Now observe that the number of 0s and 1s in $\mathcal{S}(Y_1^0, Y_2, \ldots, Y_n)$ follows the distribution $P' = (A+\Delta_1, C-A+\Delta_2)$, while the number of 0s and 1s in $\mathcal{S}(Y_1^1, Y_2, \ldots, Y_n)$ follows the distribution $Q' = (A+\Delta_2, C-A+\Delta_1)$. By applying the data processing inequality, we obtain $D(\mathcal{S}(Y_1^0, Y_2, \ldots, Y_n)\|\mathcal{S}(Y_1^1, Y_2, \ldots, Y_n)) \geq D(P'\|Q')$.

Combining the previous two paragraphs, we get $D(\mathcal{S}(\mathcal{R}_1(x_1^0), .., \mathcal{R}_n(x_n))\|\mathcal{S}(\mathcal{R}_1(x_1^1), .., \mathcal{R}_n(x_n))) \leq D(\mathcal{S}(Y_1^0, Y_2, \ldots, Y_n)\|\mathcal{S}(Y_1^1, Y_2, \ldots, Y_n)) \leq D(P'\|Q')$.

D PROOF OF LEMMA 4.6

Let us define a post-processing function $g : \mathbb{N}^2 \mapsto \mathbb{N}^2$ as $g(d, e) = (\text{Binomial}(d, \beta'/\beta), \text{Binomial}(e, \beta'/\beta))$. To prove the post-processing inequality of distance measure D, we need to show that $g(P^q_{p,\beta}) \overset{d}{=} P^q_{\beta',p}$ and $g(Q^q_{p,\beta}) \overset{d}{=} Q^q_{\beta',p}$.

We shall use an equivalent sampling process for $P^q_{p,\beta}$ and $Q^q_{p,\beta}$ similar to Equation 5. Let us define the following random variables:

$$G_i = \begin{cases} (1,0) & \text{w.p. } r \\ (0,1) & \text{w.p. } r \\ (0,0) & \text{w.p. } 1-2r \end{cases}, \quad G_1^0 = \begin{cases} (1,0) & \text{w.p. } p\alpha \\ (0,1) & \text{w.p. } \alpha \\ (0,0) & \text{w.p. } 1-p\alpha-\alpha \end{cases}, \quad G_1^1 = \begin{cases} (1,0) & \text{w.p. } \alpha \\ (0,1) & \text{w.p. } p\alpha \\ (0,0) & \text{w.p. } 1-p\alpha-\alpha \end{cases},$$

then $P^q_{p,\beta} \overset{d}{=} G_1^0 + \sum_{i=2}^n G_i$ and $P^q_{p,\beta} \overset{d}{=} G_1^1 + \sum_{i=2}^n G_i$, where the same G_i appearing in the two equations are independently sampled.

Let $G_1^{0'} = g(G_1^0)$, $G_1^{1'} = g(G_1^0)$, and $G_i' = g(G_i)$, they follow distributions:

$$G_i' = \begin{cases} (1,0) & \text{w.p. } r' \\ (0,1) & \text{w.p. } r' \\ (0,0) & \text{w.p. } 1-2r' \end{cases}, \quad G_1^{0'} = \begin{cases} (1,0) & \text{w.p. } p\alpha' \\ (0,1) & \text{w.p. } \alpha' \\ (0,0) & \text{w.p. } 1-p\alpha'-\alpha' \end{cases}, \quad G_1^{1'} = \begin{cases} (1,0) & \text{w.p. } \alpha' \\ (0,1) & \text{w.p. } p\alpha' \\ (0,0) & \text{w.p. } 1-p\alpha'-\alpha' \end{cases},$$

where $\alpha' = \frac{\beta'}{p-1}$ and $r' = \frac{\alpha' p}{q}$. Therefore, we have $g(P^q_{p,\beta}) \overset{d}{=} G_1^{0'} + \sum_{i=2}^n G_i' \overset{d}{=} P^q_{\beta',p}$ and $g(Q^q_{p,\beta}) \overset{d}{=} G_1^{1'} + \sum_{i=2}^n G_i' \overset{d}{=} Q^q_{\beta',p}$, by applying the post-processing inequality of distance measure D.

E DETAILED PROOF OF THEOREM 4.8

According to the definition of Hockey-stick divergence, we have:

$$D_{e^\epsilon}(P^q_{p,\beta}\|Q^q_{p,\beta}) = \sum_{a,b \in [0,n]^2} \max\{0, \mathbb{P}[P^q_{p,\beta} = (a,b)] - e^\epsilon \mathbb{P}[Q^q_{p,\beta} = (a,b)]\}. \tag{6}$$

Recall that $C \sim Binomial(n-1, 2r)$, $A \sim Binomial(C, 1/2)$, and $\Delta_1 = Bernoulli(p\alpha)$ and $\Delta_2 = Bernoulli(1-\Delta_1, \alpha/(1-p\alpha))$. First consider $P = (A, C-A)$, $P_0 = (A+1, C-A)$ and $P_1 = (A, C-A+1)$. Based on the above sampling process, it is derived that

$$\begin{aligned} \frac{\mathbb{P}[P_0 = (a,b)]}{\mathbb{P}[P_1 = (a,b)]} &= \frac{\binom{n-1}{a+b-1}(2r)^{a+b-1}(1-2r)^{n-a-b}\binom{a+b-1}{a-1}(1/2)^{a+b-1}}{\binom{n-1}{a+b-1}(2r)^{a+b-1}(1-2r)^{n-a-b}\binom{a+b-1}{a}(1/2)^{a+b-1}} \\ &= \frac{a}{b}. \end{aligned} \tag{7}$$

Similarly, we have:

$$\begin{aligned} \frac{\mathbb{P}[P = (a,b)]}{\mathbb{P}[P_1 = (a,b)]} &= \frac{\binom{n-1}{a+b}(2r)^{a+b}(1-2r)^{n-a-b-1}\binom{a+b}{a}(1/2)^{a+b}}{\binom{n-1}{a+b-1}(2r)^{a+b-1}(1-2r)^{n-a-b}\binom{a+b-1}{a}(1/2)^{a+b-1}} \\ &= \frac{n-a-b}{a+b} \cdot \frac{2r}{1-2r} \cdot \frac{a+b}{2b}. \\ &= \frac{n-a-b}{b} \cdot \frac{r}{1-2r}. \end{aligned} \tag{8}$$

Now consider two variables $P^q_{p,\beta}$ and $Q^q_{p,\beta}$, we have the probability ratio as:

$$
\begin{aligned}
\frac{\mathbb{P}[P^q_{p,\beta}=(a,b)]}{\mathbb{P}[Q^q_{p,\beta}=(a,b)]} &= \frac{p\alpha\mathbb{P}[P_0=(a,b)]+\alpha\mathbb{P}[P_1=(a,b)]+(1-\alpha-\alpha p)\mathbb{P}[P=(a,b)]}{\alpha\mathbb{P}[P_0=(a,b)]+p\alpha\mathbb{P}[P_1=(a,b)]+(1-\alpha-\alpha p)\mathbb{P}[P=(a,b)]} \\
&= \frac{(p-1)\alpha\mathbb{P}[P_0=(a,b)]+(1-p)\alpha\mathbb{P}[P_1=(a,b)]}{\alpha\mathbb{P}[P_0=(a,b)]+p\alpha\mathbb{P}[P_1=(a,b)]+(1-\alpha-\alpha p)\mathbb{P}[P=(a,b)]} \\
&= 1+\frac{(p-1)\alpha a+(1-p)\alpha b}{\alpha a+p\alpha b+(1-\alpha-\alpha p)\cdot(n-a-b)\cdot\frac{r}{1-2r}}. \\
&= 1+\frac{(p-1)\alpha(a-b)}{\alpha(a+b)+(p-1)\alpha b+(1-\alpha-\alpha p)\cdot(n-(a+b))\cdot\frac{r}{1-2r}}.
\end{aligned}
\tag{9}
$$

A key observation is that the above formula of $\frac{\mathbb{P}[P^q_{p,\beta}=(a,b)]}{\mathbb{P}[Q^q_{p,\beta}=(a,b)]}$ monotonically increases with a when $a+b$ is fixed. Therefore, we let $c=a+b$, then the condition $\frac{\mathbb{P}[P^q_{p,\beta}=(a,b)]}{\mathbb{P}[Q^q_{p,\beta}=(a,b)]}=\frac{p\alpha a+\alpha b+(1-\alpha-\alpha p)(n-a-b)\cdot\frac{r}{1-2r}}{\alpha a+p\alpha b+(1-\alpha-\alpha p)(n-a-b)\cdot\frac{r}{1-2r}}>e^{\epsilon'}$ holds *if and only if* when $a>low_c=\frac{(e^{\epsilon'}p-1)\alpha c+(e^{\epsilon'}-1)f}{\alpha(e^{\epsilon'}+1)(p-1)}$. Therefore, the Equation 6 becomes:

$$
\begin{aligned}
D_{e^\epsilon}(P^q_{p,\beta}\|Q^q_{p,\beta}) &= \sum_{c\in[0,n]}\sum_{a\in[\lceil low_c\rceil,c]}\mathbb{P}[P^q_{p,\beta}=(a,c-a)]-e^\epsilon\mathbb{P}[Q^q_{p,\beta}=(a,c-a)] \\
&= \sum_{c\in[0,n]}\sum_{a\in[\lceil low_c\rceil,c]}(p-e^{\epsilon'})\alpha\mathbb{P}[P_0=(a,c-a)] \\
&\quad+\sum_{c\in[0,n]}\sum_{a\in[\lceil low_c\rceil,c]}(1-pe^{\epsilon'})\alpha\mathbb{P}[P_1=(a,c-a)] \\
&\quad+\sum_{c\in[0,n]}\sum_{a\in[\lceil low_c\rceil,c]}(1-\alpha-\alpha p)(1-e^{\epsilon'})\mathbb{P}[P=(a,c-a)] \\
&= (p-e^{\epsilon'})\alpha\sum_{c\in[0,n]}\binom{n-1}{c-1}(2r)^{c-1}(1-2r)^{n-c}\Big(\sum_{a\in[\lceil low_c\rceil,c]}\binom{c-1}{a-1}(1/2)^{c-1}\Big) \\
&\quad+(1-pe^{\epsilon'})\alpha\sum_{c\in[0,n]}\binom{n-1}{c-1}(2r)^{c-1}(1-2r)^{n-c}\Big(\sum_{a\in[\lceil low_c\rceil,c]}\binom{c-1}{a}(1/2)^{c-1}\Big) \\
&\quad+(1-\alpha-\alpha p)(1-e^{\epsilon'})\sum_{c\in[0,n]}\binom{n-1}{c}(2r)^{c}(1-2r)^{n-c-1}\Big(\sum_{a\in[\lceil low_c\rceil,c]}\binom{c}{a}(1/2)^{c}\Big).
\end{aligned}
$$

Notice that the formula $\sum_{c\in[0,n]}\binom{n-1}{c-1}(2r)^{c-1}(1-2r)^{n-c}\Big(\sum_{a\in[\lceil low_c\rceil,c]}\binom{c-1}{a-1}(1/2)^{c-1}\Big)$ equals to:

$$
\sum_{c\in[0,n-1]}\binom{n-1}{c}(2r)^c(1-2r)^{n-c-1}\Big(\sum_{a\in[\lceil low_{c+1}-1\rceil,c]}\binom{c}{a}(1/2)^c\Big)=\mathop{\mathbb{E}}_{c\sim Binom(n-1,2r)}\mathop{\mathsf{CDF}}_{c,1/2}[\lceil low_{c+1}-1\rceil,c];
$$

the formula $\sum_{c\in[0,n]}\binom{n-1}{c-1}(2r)^{c-1}(1-2r)^{n-c}\Big(\sum_{a\in[\lceil low_c\rceil,c]}\binom{c-1}{a}(1/2)^{c-1}\Big)$ equals to:

$$
\sum_{c\in[0,n-1]}\binom{n-1}{c}(2r)^c(1-2r)^{n-c-1}\Big(\sum_{a\in[\lceil low_{c+1}\rceil,c]}\binom{c}{a}(1/2)^c\Big)=\mathop{\mathbb{E}}_{c\sim Binom(n-1,2r)}\mathop{\mathsf{CDF}}_{c,1/2}[\lceil low_{c+1}\rceil,c];
$$

the formula $\sum_{c\in[0,n]}\binom{n-1}{c}(2r)^c(1-2r)^{n-c-1}\Big(\sum_{a\in[\lceil low_c\rceil,c]}\binom{c}{a}(1/2)^c\Big)$ equals to:

$$
\mathop{\mathbb{E}}_{c\sim Binom(n-1,2r)}\mathop{\mathsf{CDF}}_{c,1/2}[\lceil low_c\rceil,c].
$$

Combining these three equations, we have proved the equation about $D_{e^\epsilon}(P^q_{p,\beta}\|Q^q_{p,\beta})$.

As for $D_{e^\epsilon}(Q^q_{p,\beta}\|P^q_{p,\beta})$, a key observation is that $\frac{\mathbb{P}[P^q_{p,\beta}=(a,b)]}{\mathbb{P}[Q^q_{p,\beta}=(a,b)]}$ monotonically decreases with a when $a+b$ is fixed, and the condition $\frac{\mathbb{P}[P^q_{p,\beta}=(a,b)]}{\mathbb{P}[Q^q_{p,\beta}=(a,b)]}=\frac{p\alpha a+\alpha b+(1-\alpha-\alpha p)(n-a-b)\cdot\frac{r}{1-2r}}{\alpha a+p\alpha b+(1-\alpha-\alpha p)(n-a-b)\cdot\frac{r}{1-2r}}<e^{-\epsilon'}$ holds *if and only if* when $a<high_c=\frac{(e^{-\epsilon'}p-1)\alpha c+(e^{-\epsilon'}-1)f}{\alpha(e^{-\epsilon'}+1)(p-1)}$. As with previous procedures, the present analysis derives the equation governing $D_{e^\epsilon}(Q^q_{p,\beta}\|P^q_{p,\beta})$.

F PROOF OF THEOREM 4.2

Recall that $C \sim Binomial(n-1, 2r)$, $A \sim Binomial(C, 1/2)$, and $\Delta_1 = Bernoulli(p\alpha)$ and $\Delta_2 = Bernoulli(1-\Delta_1, \alpha/(1-p\alpha))$. Similar to proof for Theorem 4.8, we first consider $P = (A, C-A)$, $P_0 = (A+1, C-A)$ and $P_1 = (A, C-A+1)$. Use the fact that $C = a+b$ or $C = a+b-1$ and $|A - C/2| < \sqrt{C/2\log(4/\delta)}$ holds with probability $1-\delta/2$ (by the Hoeffding's inequality), we have the probability ratio upper bounded as:

$$
\begin{aligned}
\frac{\mathbb{P}[P^q_{p,\beta} = (a,b)]}{\mathbb{P}[Q^q_{p,\beta} = (a,b)]} &= \frac{p\alpha\mathbb{P}[P_0 = (a,b)] + \alpha\mathbb{P}[P_1 = (a,b)] + (1-\alpha-\alpha p)\mathbb{P}[P = (a,b)]}{\alpha\mathbb{P}[P_0 = (a,b)] + p\alpha\mathbb{P}[P_1 = (a,b)] + (1-\alpha-\alpha p)\mathbb{P}[P = (a,b)]} \\
&= 1 + \frac{(p-1)\alpha\mathbb{P}[P_0 = (a,b)] + (1-p)\alpha\mathbb{P}[P_1 = (a,b)]}{\alpha\mathbb{P}[P_0 = (a,b)] + p\alpha\mathbb{P}[P_1 = (a,b)] + (1-\alpha-\alpha p)\mathbb{P}[P = (a,b)]} \\
&= 1 + \frac{(p-1)\alpha((a+b)-2b)}{\alpha(a+b) + (p-1)\alpha b + (1-\alpha-\alpha p)\cdot(n-(a+b))\cdot\frac{r}{1-2r}}. \\
&\le 1 + \frac{(p-1)\alpha(C+1-2b)}{\alpha C + (p-1)\alpha b + (1-\alpha-\alpha p)\cdot(n-1-C)\cdot\frac{r}{1-2r}} \\
&\le 1 + \frac{(p-1)\alpha(2\sqrt{C/2\log(4/\delta)}+1)}{\alpha C + (p-1)\alpha(C/2 - \sqrt{C/2\log(4/\delta)}) + (1-\alpha-\alpha p)\cdot(n-1-C)\cdot\frac{r}{1-2r}}.
\end{aligned}
$$

Based on the induced formula in the last line (denoted as $1 + F(C)$), if the coefficient $\alpha + (p-1)\alpha/2 - (1-\alpha-\alpha p)r/(1-2r)$ of C in the denominator is no less than 0, the derivative $\frac{\mathrm{d}F}{\mathrm{d}C}$ is lower than 0 when $C > \frac{2p(\beta+1+(\beta-1)p)(n-1)+\beta}{q+p(\beta-1+(\beta+1)p)-pq}$. Now focus on the variable C, according to the multiplicative Chernoff bound and Hoeffding's inequality, it is derived that $C \ge (n-1)2r - \sqrt{\min\{6r, 1/2\}(n-1)\log(4/\delta)}$ holds with probability at least $1-\delta/2$. Therefore, if $\Omega = (n-1)2r - \sqrt{\min\{6r, 1/2\}(n-1)\log(4/\delta)} \ge \frac{2p(\beta+1+(\beta-1)p)(n-1)+\beta}{q+p(\beta-1+(\beta+1)p)-pq}$, then with probability at least $1-\delta/2$, the $F(C) \le F(\Omega)$ and hence $\frac{\mathbb{P}[P^q_{p,\beta}=(a,b)]}{\mathbb{P}[Q^q_{p,\beta}=(a,b)]} \le e^{\epsilon}$ holds.

Similarly, we have the probability ratio lower bounded as:

$$
\begin{aligned}
\frac{\mathbb{P}[P^q_{p,\beta} = (a,b)]}{\mathbb{P}[Q^q_{p,\beta} = (a,b)]} &= \frac{p\alpha a + \alpha b + (1-\alpha-\alpha p)\cdot(n-a-b)\cdot\frac{r}{1-2r}}{\alpha a + p\alpha b + (1-\alpha-\alpha p)\cdot(n-a-b)\cdot\frac{r}{1-2r}} \\
&= 1/(\frac{\alpha a + p\alpha b + (1-\alpha-\alpha p)\cdot(n-a-b)\cdot\frac{r}{1-2r}}{p\alpha a + \alpha b + (1-\alpha-\alpha p)\cdot(n-a-b)\cdot\frac{r}{1-2r}}) \\
&= 1/(1 + \frac{(p-1)\alpha((a+b)-2a)}{\alpha(a+b) + (p-1)\alpha a + (1-\alpha-\alpha p)\cdot(n-(a+b))\cdot\frac{r}{1-2r}}) \\
&\ge 1/(1 + \frac{(p-1)\alpha(C+1-2a)}{\alpha C + (p-1)\alpha a + (1-\alpha-\alpha p)\cdot(n-1-C)\cdot\frac{r}{1-2r}}) \\
&\ge 1/(1 + \frac{(p-1)\alpha(2\sqrt{C/2\log(4/\delta)}+1)}{\alpha C + (p-1)\alpha(C/2 - \sqrt{C/2\log(4/\delta)}) + (1-\alpha-\alpha p)\cdot(n-1-C)\cdot\frac{r}{1-2r}}).
\end{aligned}
$$

Then under the same condition about C, we have $\frac{\mathbb{P}[P^q_{p,\beta}=(a,b)]}{\mathbb{P}[Q^q_{p,\beta}=(a,b)]} \ge e^{-\epsilon}$ holds.

G PROOF OF THEOREM 4.3

According to multiplicative Chernoff bound and Hoeffding's inequality, we have $|C - (n-1)2r| < \sqrt{\min\{6r, 1/2\}(n-1)\log(4/\delta)}$ holds with probability at least $1-\delta/2$; according to Hoeffding's inequality, $|A - C/2| < \sqrt{C/2\log(4/\delta)}$ holds with probability $1-\delta/2$. Specifically, when $n \ge \frac{8\log(2/\delta)}{r}$, both $\sqrt{\min\{6r, 1/2\}(n-1)\log(4/\delta)} < \min\{r, \sqrt{r}/4, 1-2r\}(n-1)$ and $\sqrt{C/2\log(4\delta)} < C/4$ hold. The remaining proof conditions on these events.

It is observed that:

$$
\begin{aligned}
\frac{n-a-b}{b}\cdot\frac{r}{1-2r} &= \frac{n-C}{C-A}\cdot\frac{r}{1-2r}\\
&\geq \frac{n-C}{C}\cdot\frac{4r}{3(1-2r)}\\
&\geq \frac{n-(n-1)2r-\min\{r,\sqrt{r}/4,1-2r\}(n-1)}{(n-1)2r+\min\{r,\sqrt{r}/4,1-2r\}(n-1)}\cdot\frac{4r}{3(1-2r)}\\
&\geq \frac{1-2r-\min\{r,\sqrt{r}/4,1-2r\}}{2r+\min\{r,\sqrt{r}/4,1-2r\}}\cdot\frac{4r}{3(1-2r)}\\
&\geq \frac{4(1-3r)}{9(1-2r)}.
\end{aligned} \tag{10}
$$

By symmetry of a and b, we also have $\frac{n-a-b}{a}\cdot\frac{r}{1-2r}\geq\frac{4(1-3r)}{9(1-2r)}$. We use c_r to denote $\max\{0,\frac{4(1-3r)}{9(1-2r)}\}$.

Based on the classical clone reduction [27, Lemma A.3], when $n\geq\frac{8\log(2/\delta)}{r}$, it is derived that the following two inequalities hold with $\epsilon'=\log(1+\sqrt{\frac{32\log(4/\delta)}{r(n-1)}}+\frac{4}{rn})$:

$$
e^{-\epsilon'}\leq\frac{\mathbb{P}[P_0=(a,b)]}{\mathbb{P}[P_1=(a,b)]}\leq e^{\epsilon'},
$$

Now notice that $P^q_{p,\beta}=p\alpha P_0+\alpha P_1+(1-\alpha-\alpha p)P$ and $Q^q_{p,\beta}=\alpha P_0+p\alpha P_1+(1-\alpha-\alpha p)P$, we have:

$$
\begin{aligned}
\frac{\mathbb{P}[P^q_{p,\beta}=(a,b)]}{\mathbb{P}[Q^q_{p,\beta}=(a,b)]} &= \frac{p\alpha\frac{\mathbb{P}[P_0=(a,b)]}{\mathbb{P}[P_1=(a,b)]}+\alpha+(1-\alpha-\alpha p)\frac{\mathbb{P}[P=(a,b)]}{\mathbb{P}[P_1=(a,b)]}}{\alpha\frac{\mathbb{P}[P_0=(a,b)]}{\mathbb{P}[P_1=(a,b)]}+p\alpha+(1-\alpha-\alpha p)\frac{\mathbb{P}[P=(a,b)]}{\mathbb{P}[P_1=(a,b)]}}\\
&= 1+\frac{(p-1)\alpha\frac{\mathbb{P}[P_0=(a,b)]}{\mathbb{P}[P_1=(a,b)]}+(1-p)\alpha}{\alpha\frac{\mathbb{P}[P_0=(a,b)]}{\mathbb{P}[P_1=(a,b)]}+p\alpha+(1-\alpha-\alpha p)\frac{\mathbb{P}[P=(a,b)]}{\mathbb{P}[P_1=(a,b)]}}\\
&\leq 1+\frac{(p-1)\alpha\frac{a}{b}+(1-p)\alpha}{\alpha\frac{a}{b}+p\alpha+(1-\alpha-\alpha p)\cdot\frac{n-a-b}{b}\cdot\frac{r}{1-2r}}\\
&\leq 1+\frac{(p-1)\alpha\frac{a}{b}+(1-p)\alpha}{\alpha\frac{a}{b}+p\alpha+(1-\alpha-\alpha p)\cdot c_r}\\
&\leq 1+\frac{(p-1)\alpha e^{\epsilon'}+(1-p)\alpha}{\alpha e^{\epsilon'}+p\alpha+(1-\alpha-\alpha p)\cdot c_r}\\
&\leq 1+\frac{(p-1)\alpha}{\alpha+p\alpha+(1-\alpha-\alpha p)\cdot c_r}\cdot(e^{\epsilon'}-1)\\
&\leq 1+\frac{\beta}{\alpha+p\alpha+(1-\alpha-\alpha p)\cdot c_r}\cdot(e^{\epsilon'}-1).
\end{aligned} \tag{11}
$$

Besides, we have:

$$
\begin{aligned}
\frac{\mathbb{P}[P^q_{p,\beta}=(a,b)]}{\mathbb{P}[Q^q_{p,\beta}=(a,b)]} &= \frac{p\alpha\frac{a}{b}+\alpha+(1-\alpha-\alpha p)\cdot\frac{n-a-b}{b}\cdot\frac{r}{1-2r}}{\alpha\frac{a}{b}+p\alpha+(1-\alpha-\alpha p)\cdot\frac{n-a-b}{b}\cdot\frac{r}{1-2r}}\\
&= 1/(\frac{\alpha\frac{a}{b}+p\alpha+(1-\alpha-\alpha p)\cdot\frac{n-a-b}{b}\cdot\frac{r}{1-2r}}{p\alpha\frac{a}{b}+\alpha+(1-\alpha-\alpha p)\cdot\frac{n-a-b}{b}\cdot\frac{r}{1-2r}})\\
&= 1/(\frac{\alpha+p\alpha\frac{b}{a}+(1-\alpha-\alpha p)\cdot\frac{n-a-b}{b}\cdot\frac{r}{1-2r}\frac{b}{a}}{p\alpha+\alpha\frac{b}{a}+(1-\alpha-\alpha p)\cdot\frac{n-a-b}{b}\cdot\frac{r}{1-2r}\frac{b}{a}})\\
&\geq 1/(\frac{\alpha+p\alpha e^{\epsilon'}+(1-\alpha-\alpha p)\cdot\frac{n-a-b}{a}\cdot\frac{r}{1-2r}}{p\alpha+\alpha e^{\epsilon'}+(1-\alpha-\alpha p)\cdot\frac{n-a-b}{a}\cdot\frac{r}{1-2r}})\\
&\geq 1/(1+\frac{(p-1)\alpha}{p\alpha+\alpha+(1-\alpha-\alpha p)c_r}\cdot(e^{\epsilon'}-1))\\
&\geq 1/(1+\frac{\beta}{p\alpha+\alpha+(1-\alpha-\alpha p)c_r}\cdot(e^{\epsilon'}-1)).
\end{aligned} \tag{12}
$$

By combining Equations 11 and 12, it follows that, with a probability of $1-\delta$, the inequality $\frac{\mathbb{P}[P^q_{p,\beta}=(a,b)]}{\mathbb{P}[Q^q_{p,\beta}=(a,b)]} \in [e^{-\epsilon}, e^{\epsilon}]$ holds. The value of ϵ is defined as $\log(1+\frac{\beta}{\beta(1+p)/(p-1)+(1-\beta(1+p)/(p-1))c_r})(\sqrt{\frac{32\log(4/\delta)}{r(n-1)}}+\frac{4}{rn}))$.

H PROBABILITY RATIO OF $P^{q_0,q_1}_{p_0,\beta}$ AND $Q^{q_0,q_1}_{p_0,\beta}$

Recall that for $p_0 > 1, \beta \in [0, \frac{p_0-1}{p_0+1}], q_0, q_1 \in [1, +\infty)$ such that $q_0 \leq p_0 q_1$ and $q_1 \leq p_0 q_0$, we define α as $\frac{\beta}{(p_0-1)}$, r_0 as $\frac{\alpha p_0}{q_0}$ and r_1 as $\frac{\alpha p_0}{q_1}$, and $C \sim Binom(n-1, r_0+r_1)$, $A \sim Binom(C, r_0/(r_0+r_1))$, and $\Delta_1 = Bernoulli(p_0\alpha')$ and $\Delta_2 = Bernoulli(1-\Delta_1, \alpha/(1-p_0\alpha))$. The random variable $P^{q_0,q_1}_{p_0,\beta}$ corresponds to $(A+\Delta_1, C-A+\Delta_2)$ and the $Q^{q_0,q_1}_{p_0,\beta}$ corresponds to $(A+\Delta_2, C-A+\Delta_1)$ from two independent samplings.

To see how the algorithm works, we put forth following analyses on the two variables. According to the sampling process, we have:

$$\begin{aligned}\mathbb{P}[P^{q_0,q_1}_{p_0,\beta} = (a,b)] =& p\alpha\binom{n-1}{a+b-1}(r_0+r_1)^{a+b-1}(1-r_0-r_1)^{n-a-b}\binom{a+b-1}{a-1}\frac{(r_0)^{a-1}(r_1)^b}{(r_0+r_1)^{a+b-1}}\\ &+\alpha\binom{n-1}{a+b-1}(r_0+r_1)^{a+b-1}(1-r_0-r_1)^{n-a-b}\binom{a+b-1}{a}\frac{(r_0)^{a}(r_1)^{b-1}}{(r_0+r_1)^{a+b-1}}\\ &+(1-\alpha-p_0\alpha)\binom{n-1}{a+b}(r_0+r_1)^{a+b}(1-r_0-r_1)^{n-a-b-1}\binom{a+b}{a}\frac{(r_0)^{a}(r_1)^{b}}{(r_0+r_1)^{a+b}}.\end{aligned}$$

Similarly, we have:

$$\begin{aligned}\mathbb{P}[Q^{q_0,q_1}_{p_0,\beta} = (a,b)] =& \alpha\binom{n-1}{a+b-1}(r_0+r_1)^{a+b-1}(1-r_0-r_1)^{n-a-b}\binom{a+b-1}{a-1}\frac{(r_0)^{a-1}(r_1)^b}{(r_0+r_1)^{a+b-1}}\\ &+p_0\alpha\binom{n-1}{a+b-1}(r_0+r_1)^{a+b-1}(1-r_0-r_1)^{n-a-b}\binom{a+b-1}{a}\frac{(r_0)^{a}(r_1)^{b-1}}{(r_0+r_1)^{a+b-1}}\\ &+(1-\alpha-p_0\alpha)\binom{n-1}{a+b}(r_0+r_1)^{a+b}(1-r_0-r_1)^{n-a-b-1}\binom{a+b}{a}\frac{(r_0)^{a}(r_1)^{b}}{(r_0+r_1)^{a+b}}.\end{aligned}$$

Then, it is observed that:

$$\frac{\binom{n-1}{a+b-1}(r_0+r_1)^{a+b-1}(1-r_0-r_1)^{n-a-b}\binom{a+b-1}{a}\frac{(r_0)^{a}(r_1)^{b-1}}{(r_0+r_1)^{a+b-1}}}{\binom{n-1}{a+b-1}(r_0+r_1)^{a+b-1}(1-r_0-r_1)^{n-a-b}\binom{a+b-1}{a-1}\frac{(r_0)^{a-1}(r_1)^{b}}{(r_0+r_1)^{a+b-1}}} = \frac{r_0 b}{r_1 a},$$

$$\frac{\binom{n-1}{a+b}(r_0+r_1)^{a+b}(1-r_0-r_1)^{n-a-b-1}\binom{a+b}{a}\frac{(r_0)^{a}(r_1)^{b}}{(r_0+r_1)^{a+b}}}{\binom{n-1}{a+b-1}(r_0+r_1)^{a+b-1}(1-r_0-r_1)^{n-a-b}\binom{a+b-1}{a-1}\frac{(r_0)^{a-1}(r_1)^{b}}{(r_0+r_1)^{a+b-1}}} = \frac{r_0(n-a-b)}{(1-r_0-r_1)a}.$$

Consequently, we get:

$$\frac{\mathbb{P}[P^{q_0,q_1}_{p_0,\beta} = (a,b)]}{\mathbb{P}[Q^{q_0,q_1}_{p_0,\beta} = (a,b)]} = \frac{p_0\alpha a/r_0 + \alpha b/r_1 + (1-\alpha-p_0\alpha)(n-a-b)/(1-r_0-r_1))}{\alpha a/r_0 + p_0\alpha b/r_1 + (1-\alpha-p_0\alpha)(n-a-b)/(1-r_0-r_1))}. \tag{13}$$

I NUMERICAL LOWER BOUNDS

We proceed to numerically compute the lower bound for privacy amplification. While a naive approach would involve enumerating the entire output space of $P^{q_0,q_1}_{p,\beta}$ and $Q^{q_0,q_1}_{p,\beta}$ with $O(Tn^2)$ complexities, we propose a more efficient implementation. Assuming $q_0/q_1 \in [1/p, p]$, and with $a+b$ fixed, we observe that the ratio $\frac{\mathbb{P}[P^{q_0,q_1}_{p,\beta}=(a,b)]}{\mathbb{P}[Q^{q_0,q_1}_{p,\beta}=(a,b)]}$ monotonically increases with a (see Appendix H for details). Specifically, let g denote $(1-\alpha-\alpha p)(n-c)\cdot\frac{1}{1-r_0-r_1}$, then if $a > low$, where $low = \frac{(e^{\epsilon'}p-1)\alpha c/r_1+(e^{\epsilon'}-1)g}{\alpha(p/r_0-1/r_1+e^{\epsilon'}(p/r_1-1/r_0))}$, the ratio exceeds e^{ϵ}. If $a < high$, where $high = \frac{(e^{-\epsilon'}p-1)\alpha c/r_1+(e^{-\epsilon'}-1)g}{\alpha(p/r_0-1/r_1+e^{-\epsilon'}(p/r_1-1/r_0))}$, the ratio is lower than $e^{-\epsilon}$. We present the divergence in an expectation form in Proposition I.1 and provide an efficient implementation in Algorithm 3 with $\tilde{O}(Tn)$ complexities (see Appendix J).

Proposition I.1 (Divergence bound as an expectation). *For $p > 1, \beta \in [0, \frac{p-1}{p+1}], q_0, q_1 \in [1, \infty)$ that $q_0/q_1 \in [1/p, p]$, let $\alpha = \frac{\beta}{p-1}$, $r_0 = \frac{\alpha p}{q_0}$, and $r_1 = \frac{\alpha p}{q_1}$, let $low_c = \frac{(e^{\epsilon}p-1)\alpha c/r_1+(e^{\epsilon}-1)(1-\alpha-\alpha p)(n-c)/(1-r_0-r_1)}{\alpha(p/r_0-1/r_1+e^{\epsilon}(p/r_1-1/r_0))}$ and $high_c = \frac{(e^{-\epsilon}p-1)\alpha c/r_1+(e^{-\epsilon}-1)(1-\alpha-\alpha p)(n-c)/(1-r_0-r_1)}{\alpha(p/r_0-1/r_1+e^{-\epsilon}(p/r_1-1/r_0))}$,* *then for any $\epsilon \in \mathbb{R}$:*

$$D_{e^\epsilon}(P^{q_0,q_1}_{p,\beta} \| Q^{q_0,q_1}_{p,\beta}) = \mathop{\mathbb{E}}_{c\sim Binomial(n-1,r_0+r_1)} \Big[(p-e^\epsilon)\alpha \cdot \mathop{\mathrm{CDF}}_{c,\frac{r_0}{r_0+r_1}}[\lceil low_{c+1}-1\rceil, c] + (1-pe^\epsilon)\alpha \cdot \mathop{\mathrm{CDF}}_{c,\frac{r_0}{r_0+r_1}}[\lceil low_{c+1}\rceil, c] + (1-e^\epsilon)(1-\alpha-p\alpha)\cdot \mathop{\mathrm{CDF}}_{c,\frac{r_0}{r_0+r_1}}[\lceil low_{c}\rceil, c]\Big],$$

$$D_{e^\epsilon}(Q^{q_0,q_1}_{p,\beta} \| P^{q_0,q_1}_{p,\beta}) = \mathop{\mathbb{E}}_{c\sim Binomial(n-1,r_0+r_1)} \Big[(1-pe^\epsilon)\alpha \cdot \mathop{\mathrm{CDF}}_{c,\frac{r_0}{r_0+r_1}}[0, \lfloor high_{c+1}-1\rfloor] + (p-e^\epsilon)\alpha \cdot \mathop{\mathrm{CDF}}_{c,\frac{r_0}{r_0+r_1}}[0, \lfloor high_{c+1}\rfloor] + (1-e^\epsilon)(1-\alpha-p\alpha)\cdot \mathop{\mathrm{CDF}}_{c,\frac{r_0}{r_0+r_1}}[0, \lfloor high_{c}\rfloor]\Big].$$

It is worth noting that the upper bound of indistinguishability between $P^{q_0,q_1}_{p,\beta}$ and $Q^{q_0,q_1}_{p,\beta}$, which refers to the minimum value of ϵ' that satisfies $\max[D_{e^{\epsilon'}}(P^{q_0,q_1}_{p,\beta} \| Q^{q_0,q_1}_{p,\beta}), D_{e^{\epsilon'}}(Q^{q_0,q_1}_{p,\beta} \| P^{q_0,q_1}_{p,\beta})] \le \delta$, can be obtained in a similar manner as that of the lower bound. The only difference is that, in Algorithm 3, we return ϵ_H instead of ϵ_L at the last line. This would be useful to derive precise amplification upper bounds for specific randomizers that are not tight in Theorem 4.7, such as randomized response on 2 options [73], local hash with length $l = 2$ [68], and exponential mechanism for metric LDP on 3 options [50].

J EFFICIENT SEARCH OF THE INDISTINGUISHABLE LOWER BOUND

The efficient implementation in Algorithm 3 relies on Proposition I.1, which expresses the divergence as an expectation.

Algorithm 3: Efficient Search of the indistinguishable lower bound of $P^{q_0,q_1}_{p_0,\beta}$ and $Q^{q_0,q_1}_{p_0,\beta}$

Input: privacy parameter δ, number of clients n, property parameters $p_0 > 1, \beta \in [0, \frac{p_0-1}{p_0+1}]$ and $q_0, q_1 \ge 1$ that $q_0/q_1 \in [1/p_0, p_0]$, number of iterations T.

Output: A lower bound of ϵ'_c that $\max[D_{\epsilon'_c}(P^{q_0,q_1}_{p_0,\beta} \| Q^{q_0,q_1}_{p_0,\beta}), D_{\epsilon'_c}(Q^{q_0,q_1}_{p_0,\beta} \| P^{q_0,q_1}_{p_0,\beta})] \ge \delta$ holds.

$\alpha = \frac{\beta}{p_0-1},\ r_0 = \frac{\alpha p_0}{q_0},\ r_1 = \frac{\alpha p_0}{q_1}$

Procedure `Delta`(ϵ')

  $\delta'_0 \leftarrow 0, \quad \delta'_1 \leftarrow 0$

  $w_c = \binom{n-1}{c}(2r)^c(1-2r)^{n-1-c}$

  $low_c = \frac{(e^{\epsilon'}p_0-1)\alpha c/r_1 + (e^{\epsilon'}-1)g}{\alpha(p/r_0-1/r_1+e^{\epsilon'}(p_0/r_1-1/r_0))}$

  $high_c = \frac{(e^{-\epsilon'}p_0-1)\alpha c/r_1 + (e^{-\epsilon'}-1)g}{\alpha(p_0/r_0-1/r_1+e^{-\epsilon'}(p_0/r_1-1/r_0))}$

  for $c \in [0, n]$ **do**

    $\delta'_0 \leftarrow \delta'_0 + w_c\Big((p_0-e^\epsilon)\alpha \cdot \mathop{\mathrm{CDF}}_{c,\frac{r_0}{r_0+r_1}}[\lceil low_{c+1}-1\rceil, c] + (1-p_0e^\epsilon)\alpha \cdot \mathop{\mathrm{CDF}}_{c,\frac{r_0}{r_0+r_1}}[\lceil low_{c+1}\rceil, c] + (1-e^\epsilon)(1-\alpha-p_0\alpha)\cdot \mathop{\mathrm{CDF}}_{c,\frac{r_0}{r_0+r_1}}[\lceil low_c\rceil, c]\Big)$

    $\delta'_1 \leftarrow \delta'_1 + w_c\Big((1-p_0e^\epsilon)\alpha \cdot \mathop{\mathrm{CDF}}_{c,\frac{r_0}{r_0+r_1}}[0, \lfloor high_{c+1}-1\rfloor] + (p_0-e^\epsilon)\alpha \cdot \mathop{\mathrm{CDF}}_{c,\frac{r_0}{r_0+r_1}}[0, \lfloor high_{c+1}\rfloor] + (1-e^\epsilon)(1-\alpha-p\alpha)\cdot \mathop{\mathrm{CDF}}_{c,\frac{r_0}{r_0+r_1}}[0, \lfloor high_c\rfloor]\Big)$

  end

  return $\max(\delta'_0, \delta'_1)$

$\epsilon_L \leftarrow 0, \quad \epsilon_H \leftarrow \log(p_0)$

for $t \in [y]$ **do**

  $\epsilon_t \leftarrow \frac{\epsilon_L+\epsilon_H}{2}$

  if `Delta`(ϵ_t) $> \delta$ **then**

    $\epsilon_L \leftarrow \epsilon_t$

  else

    $\epsilon_H \leftarrow \epsilon_t$

  end

end

return ϵ_L

K COMPLEMENTARY AMPLIFICATION PARAMETERS OF ϵ-LDP MECHANISMS

Zhu *et al.*[79, Proposition 8] proved that for any given privatization mechanism, there always exists a *tightly* dominating pair of distributions. Therefore, the tight upper bound on pairwise total variation (i.e., hockey-stick divergence with $e^{\epsilon} = 1$) can be computed from the tightly dominating pair.

Table 6: Additional amplification parameters of ϵ-LDP randomizers.

randomizer	param. p	param. β	param. q
general mechanisms	e^{ϵ}	$\frac{e^{\epsilon}-1}{e^{\epsilon}+1}$	e^{ϵ}
Duchi *et al.* [20] for $[-1,1]^d$	e^{ϵ}	$\frac{e^{\epsilon}-1}{e^{\epsilon}+1}$	e^{ϵ}
Harmony mechanism for $[-1,1]^d$ [53]	e^{ϵ}	$\frac{e^{\epsilon}-1}{e^{\epsilon}+1}$	e^{ϵ}
k-subset exponential on s in d options [61]	e^{ϵ}	$\frac{(e^{\epsilon}-1)(\binom{d-s}{k}-\binom{d-2s}{k})}{e^{\epsilon}(\binom{d}{k}-\binom{d-s}{k})+\binom{d-s}{k}}$	e^{ϵ}
PrivKV on s in d keys ($\epsilon_1+\epsilon_2=\epsilon$) [76]	e^{ϵ}	$\frac{2s\max\{\frac{e^{\epsilon_1}(e^{\epsilon_2}-1)}{e^{\epsilon_2}+1}, e^{\epsilon_1}-1+\frac{e^{\epsilon_2}-1}{2(e^{\epsilon_2}+1)}\}}{d(e^{\epsilon_1}+1)}$	e^{ϵ}