LDP definition (General):

The randomized algorithm M is said to be ε-LDP if for all pairs of user's possible data input x, x' and any output S:

$$\frac{Pr[F(x) \in S]}{Pr[F(x') \in S]} \le e^{\varepsilon}.$$

In our case:

we flip a 0 to 1 w/ probability α.

we flip a 1 to 0 w/ probability β.

- If $x = 0$ originally.

$$F(x) = \begin{cases} 1 & \text{w/ probability } \alpha. \\ 0 & \text{w/ probability } 1-\alpha \text{ (unchanged)} \end{cases}$$

- If $x = 1$ originally:

$$F(x) = \begin{cases} 1 & \text{w/ probability } 1-\beta \text{ (unchanged)} \\ 0 & \text{w/ probability } \beta. \end{cases}$$

For randomized algorithm $F(x)$ to satisfy LDP:

$$\frac{Pr[F(x=0) = 1]}{Pr[F(x=1) = 1} \le e^{\varepsilon}.$$

$$\frac{\alpha}{1-\beta} \le e^{\varepsilon}.$$

$$\boxed{\ln\left(\frac{\alpha}{1-\beta}\right) \le \varepsilon}. \quad (1)$$

OR: $$\frac{Pr[F(x=0)=0]}{Pr[F(x=1)=0]} \le e^{\varepsilon}.$$

$$\boxed{\ln\left(\frac{1-\alpha}{\beta}\right) \le \varepsilon} \quad (2)$$

ε can be calculate by either $\ln\left(\frac{\alpha}{1-\beta}\right)$ or $\ln\left(\frac{1-\alpha}{\beta}\right)$, whichever yields to tighter bound. where α is probability of flipping 0 to 1 and β is probability of flipping 1 to 0.

If we want to maintain the number of 0 bits & 1 bits the same as original binary data after flipping:

This means # 1's flipped = # 0's flipped. Assume we have m 1's and n 0's in binary data originally. To satisfy our constraint, if we flip k one-bits, we also need to flip k zero-bits.

$\therefore$ Pr (0 flipped to 1) $= \alpha = \frac{k}{n}$.

Pr (1 flipped to 0) $= \beta = \frac{k}{m}$.

According to (1) & (2), to satisfy ε-LDP, we need to find α (probability of flipping 0 to 1) & β (probability of flipping 1 to 0), so that:

$$\ln\left(\frac{\alpha}{1-\beta}\right) \le \varepsilon \quad \text{and} \quad \ln\left(\frac{1-\alpha}{\beta}\right) \le \varepsilon$$

In the second case:

$$\alpha = \frac{k}{n}, \quad \beta = \frac{k}{m}$$

$$\therefore \ln\left(\frac{\frac{k}{n}}{1-\frac{k}{m}}\right) \le \varepsilon \qquad \ln\left(\frac{1-\frac{k}{n}}{\frac{k}{m}}\right) \le \varepsilon$$

$$\ln\left(\frac{\frac{k}{n}}{\frac{m-k}{m}}\right) \le \varepsilon \qquad \ln\left(\frac{\frac{n-k}{n}}{\frac{k}{m}}\right) \le \varepsilon$$

$$\ln\left(\frac{mk}{n(m-k)}\right) \le \varepsilon \quad (3) \qquad \ln\left(\frac{m(n-k)}{nk}\right) \le \varepsilon \quad (4).$$

In second case, ε is controlled by:

m: number of 1's in the original binary data.

n: number of 0's in the original binary data.

k: number of 1's to flip. & number of 0's to flip (note: flip $2k$ bits in total).

QED