

# RÉNYI DIFFERENTIAL PRIVACY IN THE SHUFFLE MODEL: ENHANCED AMPLIFICATION BOUNDS

E Chen<sup>1</sup> Yang Cao<sup>2</sup> Yifei Ge<sup>3</sup>

<sup>1</sup> Zhejiang Lab <sup>2</sup> Hokkaido University <sup>3</sup> Xi'an Jiaotong-Liverpool University

## ABSTRACT

The shuffle model of Differential Privacy has gained significant attention in privacy-preserving data analysis due to its remarkable tradeoff between privacy and utility. It is characterized by adding a shuffling procedure after each user's locally differentially private perturbation, which leads to a *privacy amplification* effect, meaning that the privacy guarantee of a small level of noise, say  $\epsilon_0$ , can be enhanced to  $O(\epsilon_0/\sqrt{n})$  (the smaller, the more private) after shuffling all  $n$  users' perturbed data. Most studies in the shuffle DP focus on proving a tighter privacy guarantee of privacy amplification. However, the current results assume that the local privacy budget  $\epsilon_0$  is within a limited range. In addition, there remains a gap between the tightest lower bound and the known upper bound of the privacy amplification. In this work, we push forward the state-of-the-art by making the following contributions. Firstly, we present the first asymptotically optimal analysis of Rényi Differential Privacy in the shuffle model without constraints on  $\epsilon_0$ . Secondly, we introduce hypothesis testing for privacy amplification through shuffling, offering a distinct analysis technique and a tighter upper bound. Furthermore, we propose a DP-SGD algorithm based on RDP. Experiments demonstrate that our approach outperforms existing methods significantly at the same privacy level.<sup>1</sup>

**Index Terms**— Rényi Differential Privacy, Shuffle Model, Privacy Amplification, Hypothesis Testing

## 1. INTRODUCTION

Rényi Differential Privacy (RDP) [1, 2] is a variant of Differential Privacy (DP) [3, 4], which has become the preferred and more sophisticated framework for ensuring privacy protection. While DP is widely regarded as the standard framework for privacy protection, RDP offers enhanced privacy guarantees and finer control over privacy levels by introducing the Rényi order parameter. Although advanced composition theorems exist for DP [3] to quantify privacy leakage, it should be noted that these bounds may not always be tight.

The interest in the shuffle model has been driven by its privacy amplification effect [5, 6]. This effect becomes no-

tably pronounced because there is often a trade-off between utility and individual privacy protection through Local Differential Privacy (LDP) [7]. The primary focus in this area is to achieve more precise RDP bounds for privacy amplification [8, 9, 10, 11]. Figure 1 illustrates the shuffle model, where the choice between adaptive and non-adaptive approaches is determined by the query's dependency on previous queries.

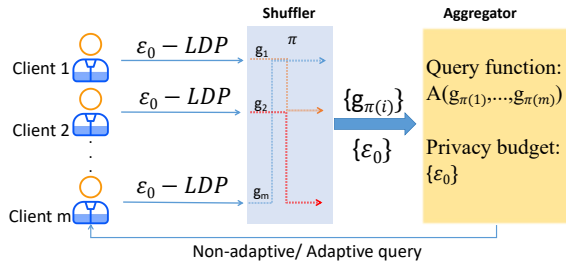
However, it is worth noting that the existing results not only impose limitations on the local privacy budget  $\epsilon_0$  but also leave a considerable gap to reach the lower bound of RDP. This suggests the need for further advancements and exploration in this area to bridge the existing gap.

In this work, we provide the first asymptotically optimal analysis for RDP in the shuffle model without any additional constraints on  $\epsilon_0$ . By transforming the original problem into a simpler task of measuring the distance between two multinomial distributions [10], we improve the RDP bound using hypothesis testing [12, 13]. To provide a clear and convenient comparison, we outline both previous findings and our own results in Table 1. Despite the advancements and continuous improvements in RDP bounds under the shuffle model, previous studies have imposed constraints on the privacy budget  $\epsilon_0$  (such as  $0 < \epsilon_0 < 1/2$  [8]). In contrast, our method eliminates such restrictions and is suitable for all  $\epsilon_0 > 0$ . Furthermore, we introduce a DP-SGD algorithm based on RDP, leveraging the RDP bounds obtained from our asymptotically optimal analysis. The numerical results demonstrate that our proposed algorithm significantly surpasses existing methods in terms of both preserving privacy and maintaining utility.

Methods	Upper Bound	Lower Bound [9]
Erlingsson et al. (SODA, 2019) [8]	$O(\frac{e^{6\epsilon_0\lambda}}{n})$	$O(\frac{e^{\epsilon_0\lambda}}{n})$
Girgis et al. (CCS, 2021) [9]	$O(\frac{e^{2\epsilon_0\lambda}}{n})$	
Feldman et al. (FOCS, 2022) [10]	$O(\frac{64e^{\epsilon_0\lambda}}{n})$	
Feldman et al. (SODA, 2023) [11]		
This work	$O(\frac{2e^{\epsilon_0\lambda}}{n})$	

**Table 1:** Privacy amplification of RDP via shuffling with order  $\lambda$ . For the sake of brevity, we have not listed the constraints on  $\epsilon_0$  found in previous studies.

<sup>1</sup>The full version with proofs can be found on website <https://github.com/EChen233/A-full-version-of-RDP-in-the-shuffle-model>.



**Fig. 1:** The shuffle model with differential privacy

## 2. PRELIMINARIES AND NOTATIONS

This section gives essential terminology, definitions and properties related to differential privacy. Due to space limitations, proofs will be included in the full version.

**Definition 1** ( $\epsilon$ -Local Differential Privacy,  $\epsilon$ -LDP). An randomized algorithm  $\mathcal{R} : \mathcal{D} \rightarrow \mathcal{S}$  satisfies  $\epsilon$ -LDP if for all neighboring datasets  $D_0, D_1 \in \mathcal{D}^n$ ,

$$\mathbb{P}(\mathcal{R}(D_0) \in S) \leq e^\epsilon \mathbb{P}(\mathcal{R}(D_1) \in S). \quad (1)$$

Here  $D_0$  and  $D_1$  are considered neighboring if they differ by exactly one record, and we denote this relationship as  $D_0 \sim D_1$ .

**Definition 2.** (Rényi Divergence) For two random variables  $U$  and  $V$ , the Rényi divergence of  $U$  and  $V$  of order  $\lambda > 1$  is defined as:

$$D^\lambda(U \| V) = \frac{1}{\lambda - 1} \log \mathbb{E}_{x \sim V} \left[ \left( \frac{U(x)}{V(x)} \right)^\lambda \right]. \quad (2)$$

Introduced in [1], Rényi differential privacy (RDP) can be defined based on Rényi divergence.

**Definition 3** (Rényi Differential Privacy). An randomized mechanism  $\mathcal{R}$  is said to be  $(\lambda, \epsilon(\lambda))$ -RDP if for all neighbouring pairs  $D_0 \sim D_1$ , it holds that

$$D^\lambda(\mathcal{R}(D_0) \| \mathcal{R}(D_1)) \leq \epsilon, \quad (3)$$

Finally, we establish the framework of privacy protection algorithm under consideration in this paper. The notation  $[n]$  represents the set of natural numbers from 1 to  $n$ . For a domain  $\mathcal{D}$ , let  $\mathcal{R}^{(i)} : \mathcal{S}^{(1)} \times \mathcal{S}^{(2)} \times \dots \times \mathcal{S}^{(i-1)} \times \mathcal{D} \rightarrow \mathcal{S}^{(i)}$  ( $i \in [n]$ ) be a sequence of algorithms such that  $\mathcal{R}^{(i)}(z_{1:i-1}, \cdot)$  is an  $\epsilon_0$ -LDP randomizer for all values of auxiliary inputs  $z_{1:i-1} \in \mathcal{S}^{(1)} \times \mathcal{S}^{(2)} \times \dots \times \mathcal{S}^{(i-1)}$  where  $\mathcal{S}^{(i)}$  is the range space of  $\mathcal{R}^{(i)}$ . Let  $\mathcal{A}_R : \mathcal{D} \rightarrow \mathcal{S}^{(1)} \times \mathcal{S}^{(2)} \times \dots \times \mathcal{S}^{(n)}$  represent the algorithm applied to the given dataset  $x_{1:n} \in \mathcal{D}^n$ . The algorithm sequentially computes  $z_i = \mathcal{R}^{(i)}(z_{1:i-1}, x_i)$

for  $i \in [n]$  and outputs  $z_{1:n}$ . We refer to  $\mathcal{A}_R(\mathcal{D})$  as an  $\epsilon_0$ -LDP adaptive process. Alternatively, if we first uniformly sample a permutation  $\pi : [n] \rightarrow [n]$ , and then sequentially compute  $z_i = \mathcal{R}^{(i)}(z_{1:i-1}, x_{\pi_i})$  for  $i \in [n]$ , we say it is a shuffled process and denote it as  $\mathcal{A}_{R,S}(\mathcal{D})$ . Here,  $\pi_i = \pi(i)$  represents the position of  $i$  after permutation.

For the sake of brevity and convenience of notation, we omit  $D$  and use  $\mathcal{A}_R$ ,  $\mathcal{A}_{R,S}$  to represent the adaptive process and the shuffled adaptive process, respectively.

**Proposition 1.** (Feldman et al. [10]) For a domain  $\mathcal{D}$ , let  $\mathcal{A}_R$  be the  $\epsilon_0$ -LDP adaptive process and  $\mathcal{A}_{R,S}$  be the related shuffled  $\epsilon_0$ -LDP adaptive process. Assume  $X_0 = (x_1^0, x_2, \dots, x_n)$  and  $X_1 = (x_1^1, x_2, \dots, x_n)$  be two neighbouring datasets such that for all  $j \neq 1, x_j \notin \{x_1^0, x_1^1\}$ . Suppose that there exists a positive value  $p \in (0, 1]$  such that for all  $i \in [n]$ ,  $x \in \mathcal{D} \setminus \{x_1^0, x_1^1\}$  and  $z_{1:i-1} \in \mathcal{S}^{(1)} \times \mathcal{S}^{(2)} \times \dots \times \mathcal{S}^{(i-1)}$ , there exists a distribution  $LO^{(i)}(z_{1:i-1}, x)$  such that

$$\begin{aligned} \mathcal{R}^{(i)}(z_{1:i-1}, x) &= \frac{p}{2} \mathcal{R}^{(i)}(z_{1:i-1}, x_1^0) + \frac{p}{2} \mathcal{R}^{(i)}(z_{1:i-1}, x_1^1) \\ &\quad + (1-p) LO^{(i)}(z_{1:i-1}, x). \end{aligned} \quad (4)$$

Then there exists a randomized postprocessing algorithm  $f$  such that  $\mathcal{A}_S(X_0)$  is distributed identically to  $f(A + \Delta, C - A + 1 - \Delta)$  and  $\mathcal{A}_S(X_1)$  is distributed identically to  $f(A + 1 - \Delta, C - A + \Delta)$ , where  $p = e^{-\epsilon_0}$ ,  $\Delta \sim \text{Bern}(\frac{e^{\epsilon_0}}{e^{\epsilon_0} + 1})$ ,  $C \sim \text{Bin}(n-1, p)$ ,  $A \sim \text{Bin}(C, 1/2)$ .

The starting point of this paper is Proposition 1, which transforms the original problem into a simpler task of analyzing a non-adaptive protocol. It is worth noting that Proposition 1 mentions the joint distribution of  $A$  and  $C$ , which corresponds to the multinomial distribution  $\text{Multinom}(n-1; p/2, p/2, 1-p)$ . Here,  $A$  and  $C - A$  represent the number of 0s and 1s, respectively.

## 3. PRIVACY AMPLIFICATION BY SHUFFLING BASED ON MULTINOMIAL DISTRIBUTION

### 3.1. The Exact RDP Bound for the Shuffle Model

In order to provide our tighter exact closed-form bound, we employ a combination of maximum likelihood and hypothesis testing methods, leveraging their strengths to derive a more accurate and precise result.

**Theorem 1.** Let  $P = (A, C - A + \Delta)$  and  $Q = (A + \Delta, C - A)$ , where  $p = e^{-\epsilon_0}$ ,  $C \sim \text{Bin}(n-1, p)$ ,  $A \sim \text{Bin}(C, 1/2)$ ,  $\Delta \sim \text{Bern}(p)$ . Then

$$D^\lambda(P \| Q) = \frac{1}{\lambda - 1} \log \int_0^1 |h'(x)|^{1-\lambda} dx.$$

Here,  $h(\alpha)$  can be obtained as follows.

$$h(\alpha) = 1 - \alpha - c_0 \sum_{v=1}^{n-1} \mathbb{P}(B_1(v) < A \leq B_2(v) | C = v) \mathbb{P}(C = v),$$

where

$$\alpha(t) = \mathbb{P}(\Delta = 0)\mathbb{P}\left(\frac{A}{C-A+1} > t\right) + \mathbb{P}(\Delta = 1)\mathbb{P}\left(\frac{A+1}{C-A} > t\right),$$

$$g(\alpha) = \inf_t \{t : \alpha(t) \leq \alpha\}, c_0 = \frac{e^{-\epsilon_0}-1}{e^{-\epsilon_0}+1}, B_1(v) = \frac{g(\alpha)v-1}{g(\alpha)+1}, B_2(v) = \frac{g(\alpha)v-1}{g(\alpha)+1} + 1, \mathbb{P}(C=v) = \binom{n-1}{v} e^{-v\epsilon_0} (1-e^{-\epsilon_0})^{n-1-v}, v = 0, 1, \dots, n-1, P(A=k|C=v) = \binom{v}{k} \left(\frac{1}{2}\right)^k, k = 0, 1, \dots, v.$$

Theorem 1 gives exact RDP bound for the shuffled output, however, since RDP is symmetric, we also need to provide result of  $D^\lambda(Q\|P)$  in a similar way. Without causing any ambiguity, we use notations  $P$  and  $Q$  to represent the same value in Theorem 1 in the following context. In fact, we can obtain the Rényi divergence between two multinomial distributions by numerical computation [10].

**Corollary 1.** *The  $\epsilon_0$ -LDP shuffled adaptive process satisfies  $(\lambda, \max\{D^\lambda(P\|Q), D^\lambda(Q\|P)\})$ -RDP, where  $P, Q$  and  $D^\lambda(\cdot\|\cdot)$  are defined in Theorem 1.*

### 3.2. The Asymptotic RDP Bound for the Shuffle Model

Although Corollary 1 provides a RDP bound for the shuffle model, it is excessively complicated and lacks intuitive understanding. In the following context, we provide an asymptotic RDP bound. This approach not only simplifies computations but also facilitates the extension to other privacy definitions based on the relationship between divergences and Gaussian Differential Privacy (GDP) [13].

**Lemma 1.** *Assume  $\xi = (n_0, n_1, n_2)'$  is a random variable which obeys multinomial distribution with parameters  $(n-1; \frac{p}{2}, \frac{p}{2}, 1-p)$ , then  $\xi$  approximately follows the multivariate normal distribution  $N(\tilde{\mu}, \tilde{\Sigma})$  as  $n \rightarrow \infty$ , where  $\tilde{\mu} = \left(\frac{(n-1)p}{2}, \frac{(n-1)p}{2}, (n-1)(1-p)\right)'$  and covariance matrix of  $\xi$  is*

$$\tilde{\Sigma} = (n-1) \begin{pmatrix} \frac{p}{2}(1-\frac{p}{2}) & -\frac{p^2}{4} & -\frac{p(1-p)}{2} \\ -\frac{p^2}{4} & \frac{p}{2}(1-\frac{p}{2}) & -\frac{p(1-p)}{2} \\ -\frac{p(1-p)}{2} & -\frac{p(1-p)}{2} & p(1-p) \end{pmatrix}.$$

Lemma 1 provides the asymptotic normality of the multinomial distribution, which is closely related to GDP. The Berry-Esseen type central limit theorem [14] ensures that the theoretical convergence rate is at most  $O\left(\frac{1}{\sqrt{n}}\right)$  while the numerical calculation confirms a convergence rate of approximately  $O\left(\frac{1}{n}\right)$ .

**Theorem 2.** *For a domain  $\mathcal{D}$ , the shuffled  $\epsilon_0$ -LDP adaptive process approximately satisfies  $\frac{2e^{\epsilon_0/2}}{\sqrt{n-1}}$ -GDP.*

According to the fact that  $\mu$ -GDP implies  $(\lambda, \frac{1}{2}\mu^2\lambda)$ -RDP [13], we have the asymptotic RDP bound of the shuffled output.

**Corollary 2.** *For a domain  $\mathcal{D}$ , the shuffled  $\epsilon_0$ -LDP adaptive process approximately satisfies  $(\lambda, \frac{2e^{\epsilon_0}\lambda}{n-1})$ -RDP for any  $\lambda \geq 2$ .*

### 3.3. Comparison of RDP Bounds under the Shuffle Model

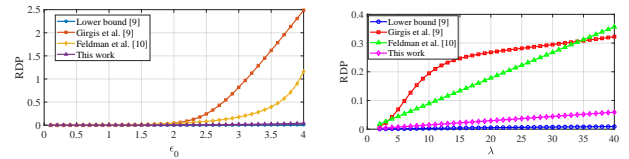
Bounds on RDP for privacy amplification via shuffling were initially introduced by Erlingsson et al. [8]. Girgis et al. [9] gave both an upper bound and a lower bound of RDP for  $\epsilon_0 \geq 0$  and any integer  $\lambda \geq 2$ . That is, the RDP of the shuffled  $\epsilon_0$ -LDP adaptive process is upper-bounded by

$$\epsilon(\lambda) \leq \frac{1}{\lambda-1} \log \left( e^{\lambda^2 \frac{(\epsilon_0-1)^2}{\bar{n}}} + e^{\epsilon_0\lambda - \frac{n-1}{8e^{\epsilon_0}}} \right), \quad (5)$$

where  $\bar{n} = \lfloor \frac{n-1}{2e^{\epsilon_0}} \rfloor + 1$ . And the RDP of the shuffled  $\epsilon_0$ -LDP adaptive process is lower-bounded by

$$\epsilon(\lambda) \geq \frac{1}{\lambda-1} \log \left( 1 + \frac{\lambda(\lambda-1)(e^{\epsilon_0}-1)^2}{2ne^{\epsilon_0}} \right). \quad (6)$$

The exponential term  $e^{\epsilon_0\lambda - \frac{n-1}{8e^{\epsilon_0}}}$  in the upper bound comes from the Chernoff bound, it goes to 0 rapidly as  $n$  increases. If we omit this term, the upper bound is nearly  $\frac{2}{n-1} \frac{\lambda}{\lambda-1} e^{\epsilon_0} (e^{\epsilon_0}-1)^2$ , which is worse than our simplified bound in Corollary 2 by a multiplicative factor of  $\frac{\lambda}{\lambda-1} (e^{\epsilon_0}-1)^2$ . Although the RDP bound has been improved to  $O(\frac{64e^{\epsilon_0}\lambda}{n})$  [11], our proposed RDP bound shows a significantly superior performance.



**Fig. 2:** RDP as a function of  $\epsilon_0$  for  $\lambda = 4$  and  $n = 10^4$  **Fig. 3:** RDP as a function of  $\lambda$  for  $\epsilon_0 = 2$  and  $n = 10^4$

Figure 2 illustrates that our RDP bound provides a significantly tighter bound compared to the existing work for a fixed value of  $\lambda = 4$ . Moreover, it demonstrates that for both  $\epsilon_0 > 1$  and  $\epsilon_0 < 1$ , our bound and the lower bound are in close proximity. Similarly, Figure 3 shows that our RDP bound and the lower bound are close for each  $\lambda \geq 2$ , with a fixed  $\epsilon_0 = 2$ .

## 4. APPLICATION AND EXPERIMENTS

Stochastic gradient descent (SGD) is a crucial algorithm for empirical risk minimization (ERM), which aims to minimize a parameterized function given by  $\mathcal{L}(\theta) = \sum_{i=1}^n \ell(\theta, x_i)$ , where  $\theta \in \mathbb{R}^d$ . Several studies have focused on a differentially private variant of Stochastic Gradient Descent (SGD) [15, 16, 17]. Additionally, researchers have investigated a

deep learning version of SGD tailored for the popular MNIST handwritten digit dataset [2].

In our experiments, we consider a scenario with  $m$  clients, where each client has  $n/m$  samples. Our approach, which incorporates Principle Components Analysis (PCA), achieves an impressive accuracy of 98.18% after approximately 50 epochs in the non-private scenario. This accuracy result is consistent with the findings of a standard neural network trained on the same MNIST dataset [18]. By employing this methodology, we can effectively train a simple classifier that achieves high accuracy in recognizing handwritten digits from the MNIST dataset. Details of the experiment setup can be found in Table 2.

To the best of our knowledge, the best RDP bound for the shuffled noisy SGD with  $\epsilon_0$ -LDP adaptive process is listed in [9, 10], while Figure 2 and 3 show that the privacy bound in this work is tighter. Furthermore, our technique is based on Laplace mechanism and can be applied to stochastic gradient descent with batch size  $m$ . Figure 4 demonstrates that our method achieves the closest accuracy (96.41%) to the true result (98.18%) when the same total privacy budget (RDP) is applied. This result is natural because a better RDP bound allows for more precise local computations, leading to more accurate results.

**Table 2:** Experiment setting for the shuffled SGD on the MNIST dataset

Parameters/Setting	Value	Explanation
Activation function	ReLU	
Output layer	Softmax	
Loss function	Cross-entropy	
Input layer	60 variables	60 PCA components
$C$	10	Clipping bound
$\epsilon_0$	[0.1, 2]	Privacy budget
$\eta$	0.05	Step size
$m$	100	Batch size
$n$	60,000	Sample size
$T$	50	Epoch count

**Proposition 2** (Composition theorem of GDP [13]). *The  $k$ -fold composition of  $\mu_i$ -GDP mechanisms is  $\sqrt{\mu_1^2 + \dots + \mu_k^2}$ .*

**Proposition 3** (Laplace mechanism [3]). *For a function  $g : D \rightarrow \mathbb{R}^d$ , let  $l_1$  sensitivity be defined as  $\Delta(g) = \max_{D_0 \sim D_1} \|g(D_0) - g(D_1)\|_1$ , then for any  $\epsilon_0 > 0$ , the noisy output  $h(D) = g(D) + \text{Lap}(\Delta(g)/\epsilon)$  satisfies  $\epsilon_0$ -LDP.*

**Theorem 3.** *Algorithm 1 approximately satisfies  $(\lambda, \frac{2Te^{\epsilon_0}\lambda}{m-1})$ -RDP.*

*Proof.* In each epoch, the algorithm is consisted of two main steps splitting and shuffling, let

$$\begin{aligned} & \mathcal{R}^{(i)}(z_{1:i-1}, D_{\pi(i)}) \\ &= \tilde{\theta}_i = \tilde{\theta}_{i-1}(z_{1:i-1}) - \eta_i(\nabla \ell(\tilde{\theta}_{i-1}(z_{1:i-1}), D_{\pi(i)}) + \mathbf{b}_i), \end{aligned}$$

then the output of Algorithm 1 can be seen as post processing of the shuffled  $m$  blocks. Since  $l_1$  sensitivity of each  $\mathcal{R}^{(i)}(z_{1:i-1}, \cdot)$  is  $\frac{2C}{m}$ , then it is  $\epsilon_0$ -LDP according to Proposition 3. Combined with Theorem 2 and Proposition 2, Algorithm 1 approximately satisfies  $\frac{2\sqrt{T}}{\sqrt{m-1}}e^{\frac{\epsilon_0}{2}}$ -GDP. Since  $\mu$ -GDP implies  $(\lambda, \frac{1}{2}\mu^2\lambda)$ -RDP, the proof is completed.  $\square$

---

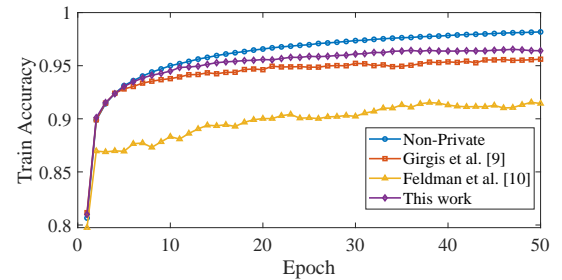
**Algorithm 1** The Shuffled noisy SGD for  $\epsilon_0$ -LDP users

---

**Require:**  $X = (x_1, \dots, x_n), \mathcal{L}(\theta, x), \theta_0, \eta, T, \epsilon_0, d, m, C$   
**Ensure:**  $\hat{\theta}_{T,m}$

- 1: Split  $[n]$  into  $m$  disjoint subsets  $S_1, \dots, S_m$  with equal size  $n/m$
- 2: Choose arbitrary initial point  $\hat{\theta}_{0,m}$
- 3: **for each**  $t \in [T]$  **do**
- 4:    $\tilde{\theta}_0 = \hat{\theta}_{t-1,m}$
- 5:   Choose a random permutation  $\pi$  of  $[m]$
- 6:   **for each**  $i \in [m]$  **do**
- 7:      $\mathbf{b}_i \sim \text{Lap}(0, \frac{2C}{\epsilon_0 m} \mathbf{I}_d)$
- 8:     **for each**  $j \in S_{\pi(i)}$  **do**
- 9:        $\mathbf{g}_i^j = \nabla \ell(\tilde{\theta}_{i-1}, x_j)$
- 10:        $\tilde{\mathbf{g}}_i^j = \mathbf{g}_i^j / \max(1, \|\mathbf{g}_i^j\|_1/C)$
- 11:     **end for**
- 12:      $\tilde{\theta}_i = \tilde{\theta}_{i-1} - \eta(\frac{1}{m} \sum_j \tilde{\mathbf{g}}_i^j + \mathbf{b}_i)$
- 13:   **end for**
- 14:    $\hat{\theta}_{t,m} = \tilde{\theta}_m$
- 15: **end for**
- 16: **return**  $\hat{\theta}_{T,m}$

---



**Fig. 4:** Comparison of train accuracy at the same privacy level of  $(\lambda, 0.008\lambda)$ -RDP

## 5. CONCLUSION

In conclusion, this study focused on Rényi Differential Privacy in the shuffle model for privacy protection. We provide an optimal analysis of RDP without any constraints on the privacy budget for the first time. Furthermore, a superior DP-SGD algorithm based on RDP was proposed, outperforming existing methods within the same privacy budget.

## 6. REFERENCES

- [1] Ilya Mironov, “Rényi differential privacy,” in *2017 IEEE 30th computer security foundations symposium (CSF)*. IEEE, 2017, pp. 263–275.
- [2] Martin Abadi, Andy Chu, Ian Goodfellow, H Brendan McMahan, Ilya Mironov, Kunal Talwar, and Li Zhang, “Deep learning with differential privacy,” in *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 2016, pp. 308–318.
- [3] Cynthia Dwork, Aaron Roth, et al., “The algorithmic foundations of differential privacy,” *Foundations and Trends® in Theoretical Computer Science*, vol. 9, no. 3–4, pp. 211–407, 2014.
- [4] Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith, “Calibrating noise to sensitivity in private data analysis,” *Journal of Privacy and Confidentiality*, vol. 7, no. 3, pp. 17–51, 2016.
- [5] Borja Balle, James Bell, Adrià Gascón, and Kobbi Nissim, “The privacy blanket of the shuffle model,” in *Advances in Cryptology—CRYPTO 2019: 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18–22, 2019, Proceedings, Part II 39*. Springer, 2019, pp. 638–667.
- [6] Albert Cheu, Adam Smith, Jonathan Ullman, David Zeyer, and Maxim Zhilyaev, “Distributed differential privacy via shuffling,” in *Advances in Cryptology—EUROCRYPT 2019: 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19–23, 2019, Proceedings, Part I 38*. Springer, 2019, pp. 375–403.
- [7] Xingxing Xiong, Shubo Liu, Dan Li, Zhaohui Cai, and Xiaoguang Niu, “A comprehensive survey on local differential privacy,” *Security and Communication Networks*, vol. 2020, pp. 1–29, 2020.
- [8] Úlfar Erlingsson, Vitaly Feldman, Ilya Mironov, Ananth Raghunathan, Kunal Talwar, and Abhradeep Thakurta, “Amplification by shuffling: From local to central differential privacy via anonymity,” in *Proceedings of the Thirtieth Annual ACM-SIAM Symposium on Discrete Algorithms*. SIAM, 2019, pp. 2468–2479.
- [9] Antonious M Girgis, Deepesh Data, Suhas Diggavi, Ananda Theertha Suresh, and Peter Kairouz, “On the renyi differential privacy of the shuffle model,” in *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, 2021, pp. 2321–2341.
- [10] Vitaly Feldman, Audra McMillan, and Kunal Talwar, “Hiding among the clones: A simple and nearly optimal analysis of privacy amplification by shuffling,” in *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*. IEEE, 2022, pp. 954–964.
- [11] Vitaly Feldman, Audra McMillan, and Kunal Talwar, “Stronger privacy amplification by shuffling for rényi and approximate differential privacy,” in *Proceedings of the 2023 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*. SIAM, 2023, pp. 4966–4981.
- [12] Peter Kairouz, Sewoong Oh, and Pramod Viswanath, “The composition theorem for differential privacy,” in *International conference on machine learning*. PMLR, 2015, pp. 1376–1385.
- [13] Jinshuo Dong, Aaron Roth, and Weijie J Su, “Gaussian differential privacy,” *Journal of the Royal Statistical Society Series B: Statistical Methodology*, vol. 84, no. 1, pp. 3–37, 2022.
- [14] Iosif Pinelis and Raymond Molzon, “Optimal-order bounds on the rate of convergence to normality in the multivariate delta method,” *Electronic Journal of Statistics*, vol. 10, no. 1, pp. 1001, 2016.
- [15] Raef Bassily, Adam Smith, and Abhradeep Thakurta, “Private empirical risk minimization: Efficient algorithms and tight error bounds,” in *2014 IEEE 55th annual symposium on foundations of computer science*. IEEE, 2014, pp. 464–473.
- [16] Shuang Song, Kamalika Chaudhuri, and Anand D Sarwate, “Stochastic gradient descent with differentially private updates,” in *2013 IEEE global conference on signal and information processing*. IEEE, 2013, pp. 245–248.
- [17] Antonious Girgis, Deepesh Data, Suhas Diggavi, Peter Kairouz, and Ananda Theertha Suresh, “Shuffled model of differential privacy in federated learning,” in *International Conference on Artificial Intelligence and Statistics*. PMLR, 2021, pp. 2521–2529.
- [18] Yann LeCun, Léon Bottou, Yoshua Bengio, and Patrick Haffner, “Gradient-based learning applied to document recognition,” *Proceedings of the IEEE*, vol. 86, no. 11, pp. 2278–2324, 1998.

## A. APPENDIX

First, we introduce a powerful tool called  $f$ -DP based on hypothesis testing. Readers can refer to the reference [13] for more detailed information.

Let  $U$  and  $V$  denote the probability distributions of  $M(D_0)$  and  $M(D_1)$ , respectively. We consider a rejection rule  $0 \leq \phi \leq 1$ , with type I and type II error rates defined as

$$\alpha_\phi = \mathbb{E}_U[\phi], \quad \beta_\phi = 1 - \mathbb{E}_V[\phi]. \quad (7)$$

**Definition A.1.** (Trade-off function) For any two probability distributions  $U$  and  $V$  on the same space  $\Omega$ , the trade-off function  $T(U, V) : [0, 1] \rightarrow [0, 1]$  is defined as

$$T(U, V)(\alpha) = \inf\{\beta_\phi : \alpha_\phi \leq \alpha\},$$

where the infimum is taken over all measurable rejection rules  $\phi$ , and  $\alpha_\phi = \mathbb{E}_U(\phi)$  and  $\beta_\phi = 1 - \mathbb{E}_V(\phi)$ .

**Definition A.2.** ( $f$ -differential privacy,  $f$ -DP) Let  $f$  be a trade-off function, a mechanism  $M$  is said to be  $f$ -differentially private if

$$T(M(D_0), M(D_1))(\alpha) \geq f(\alpha), \quad (8)$$

for all neighboring data sets  $D_0$  and  $D_1$  and  $0 \leq \alpha \leq 1$ . Under the assumption of no ambiguity, we assume that the trade-off function is a function of  $\alpha$  and denote the abbreviated form of equation (8) as  $T(M(D_0), M(D_1)) \geq f$ .

**Lemma A.1.** [13] If a mechanism  $M$  is  $f$ -DP and  $\inf\{x \in [0, 1] : f(x) = 0\} = 1$ , then it is  $(\lambda, \ell_\lambda^{\text{Rényi}}(f))$ -RDP for any  $\lambda > 1$ . Here,  $\ell_\lambda^{\text{Rényi}}(f) = \frac{1}{\lambda-1} \log \int_0^1 |f'(x)|^{1-\lambda} dx$ .

Here are some useful facts about  $f$ -DP and details can be found in [13].

**Fact 1.** If a mechanism  $M$  is  $f$ -DP, then its post-processing  $\text{Proc} \circ M$  is also  $f$ -DP.

**Fact 2.** A  $f$ -DP mechanism is called  $\mu$ -GDP if  $f$  can be obtained by  $f = T(N(0, 1), N(\mu, 1)) = \Phi(\Phi^{-1}(1 - \alpha) - \mu)$ . In other words, A mechanism is  $\mu$ -GDP if and only if it is  $(\epsilon, \delta(\epsilon))$ -DP for all  $\epsilon \geq 0$ , where

$$\delta(\epsilon) = \Phi(-\frac{\epsilon}{\mu} + \frac{\mu}{2}) - e^\epsilon \Phi(-\frac{\epsilon}{\mu} - \frac{\mu}{2}),$$

where  $\Phi(\cdot)$  is cumulative distribution function of standard normal distribution  $N(0, 1)$ .

**Fact 3.** The  $k$ -fold composition of  $\mu_i$ -GDP mechanisms is  $\sqrt{\mu_1^2 + \dots + \mu_k^2}$ .

**Lemma A.2.** Given observation  $(a, b)$ , the likelihood function between  $H_0 : P = (A, C - A + 1)$  and  $H_1 : Q = (A + 1, C - A)$  is  $\Lambda = \frac{\mathcal{L}_{H_1}}{\mathcal{L}_{H_0}} = \frac{\mathbb{P}(Q=(a,b))}{\mathbb{P}(P=(a,b))} = \frac{a}{b}$ , where  $C \sim \text{Bin}(n-1, p)$ ,  $A \sim \text{Bin}(C, 1/2)$ .

*Proof.* Since  $C \sim \text{Bin}(n-1, p)$ , we can obtain that  $\mathbb{P}(C = k) = \binom{n-1}{k} p^k (1-p)^{n-1-k}$ ,  $k = 0, 1, \dots, n-1$ . Then  $\mathbb{P}(Q = (a, b)) = \mathbb{P}(C = a+b-1) \mathbb{P}(A = a-1 | C = a+b-1) = \mathbb{P}(C = a+b-1) \mathbb{P}(A = a | C = a+b-1) = \frac{a}{b} \mathbb{P}(P = (a, b))$ , which indicates that  $\Lambda = \frac{\mathcal{L}_{H_1}}{\mathcal{L}_{H_0}} = \frac{a}{b}$ .  $\square$

**Lemma A.3.** (Neyman-Pearson lemma) For a hypothesis test between null hypothesis  $H_0$ : The sample distribution is  $P$  and alternative hypothesis  $H_1$ : The sample distribution is  $Q$ , let  $\Lambda = \frac{\mathcal{L}_{H_1}}{\mathcal{L}_{H_0}}$ , then the optimal reject region for  $\omega \in \Omega$  (sample space) is defined as follows:

$$\phi(\omega) = \begin{cases} 1, & \Lambda > t, \\ 0, & \Lambda \leq t. \end{cases} \quad (9)$$

**Lemma A.4.** Assume  $\mu_0, \mu_1 \in \mathbb{R}^d$ ,  $\mathbf{I}_d \in \mathbb{R}^{d \times d}$  is an identity matrix and  $\Sigma \in \mathbb{R}^{d \times d}$  is a positive definite matrix, then

$$T(N(\mathbf{0}, \mathbf{I}_d), N(\mu, \mathbf{I}_d)) = \Phi(\Phi^{-1}(1 - \alpha) - \sqrt{\mu' \mu}),$$

and

$$\begin{aligned} T(N(\mu_0, \Sigma), N(\mu_1, \Sigma)) \\ = \Phi(\Phi^{-1}(1 - \alpha) - \sqrt{(\mu_1 - \mu_0)' \Sigma^{-1} (\mu_1 - \mu_0)}), \end{aligned}$$

where  $\alpha \in [0, 1]$  represents type I error.

*Proof.* Notice that likelihood function between  $H_0 : N(\mathbf{0}, \mathbf{I}_d)$  and  $H_1 : N(\mu, \mathbf{I}_d)$  is

$$\frac{L_{H_1}}{L_{H_0}} = \frac{\prod_{j=1}^d (2\pi)^{-\frac{d}{2}} e^{-\frac{1}{2}(\mathbf{x} - \mu)'(\mathbf{x} - \mu)}}{\prod_{j=1}^d (2\pi)^{-\frac{d}{2}} e^{-\frac{1}{2}\mathbf{x}'\mathbf{x}}} = e^{-\frac{1}{2}\mu'\mu + \mu'\mathbf{x}}, \quad (10)$$

according to Lemma A.3, the reject rule is defined as follows:

$$\phi(\omega) = \begin{cases} 1, & \mu'\mathbf{x} > t, \\ 0, & \mu'\mathbf{x} \leq t. \end{cases} \quad (11)$$

Hence, type I error  $\alpha(t) = \mathbb{P}(\mu'\mathbf{x} > t)$ , where  $\mathbf{x} \sim N(0, \mathbf{I}_d)$ , which indicates that  $\mu'\mathbf{x} \sim N(0, \mu'\mu)$ . Therefore,

$$\alpha(t) = \mathbb{P}\left(\frac{\mu'\mathbf{x}}{\sqrt{\mu'\mu}} > \frac{t}{\sqrt{\mu'\mu}}\right) = 1 - \Phi\left(\frac{t}{\sqrt{\mu'\mu}}\right), \quad (12)$$

which indicates that  $t = \sqrt{\mu'\mu} \Phi^{-1}(1 - \alpha)$ . In addition, we can calculate type II error

$$\begin{aligned} \beta(t) &= \mathbb{P}(\mu'(\mathbf{x} + \mu) \leq t) \\ &= \mathbb{P}\left(\frac{\mu'\mathbf{x}}{\sqrt{\mu'\mu}} \leq \frac{t}{\sqrt{\mu'\mu}} - \sqrt{\mu'\mu}\right) \\ &= \Phi\left(\frac{t}{\sqrt{\mu'\mu}} - \sqrt{\mu'\mu}\right) = \Phi(\Phi^{-1}(1 - \alpha) - \sqrt{\mu'\mu}). \end{aligned} \quad (13)$$

Based on simple calculation, we can find that

$$\begin{aligned} & T(N(\boldsymbol{\mu}_0, \boldsymbol{\Sigma}), N(\boldsymbol{\mu}_1, \boldsymbol{\Sigma})) \\ &= T(N(\mathbf{0}, \mathbf{I}_d), N(\boldsymbol{\Sigma}^{-1/2}(\boldsymbol{\mu}_1 - \boldsymbol{\mu}_0), \mathbf{I}_d)) \\ &= \Phi(\Phi^{-1}(1 - \alpha) - \sqrt{(\boldsymbol{\mu}_1 - \boldsymbol{\mu}_0)' \boldsymbol{\Sigma}^{-1}(\boldsymbol{\mu}_1 - \boldsymbol{\mu}_0)}). \end{aligned}$$

□

When  $d = 1$ , we have  $T(N(0, 1), N(\mu, 1)) = \Phi(\Phi^{-1}(1 - \alpha) - \mu)$ , which is consistent with the conclusion in Fact 2.

### A.1. Proof of Theorem 1

**Lemma A.5.** Let  $P = (A, C - A + 1)$  and  $Q = (A, C - A)$ , where  $p = e^{-\epsilon_0}$ ,  $C \sim \text{Bin}(n - 1, p)$ ,  $A \sim \text{Bin}(C, 1/2)$ , then

$$T(P, Q) \geq h.$$

Here,  $\alpha(t)$ ,  $\beta(t)$  and  $h(\alpha)$  can be obtained as follows.

$$\alpha(t) = \sum_{v=1}^{n-1} \mathbb{P}(A > \frac{tv + t}{tv - 1}) \mathbb{P}(C = v),$$

$$g(\alpha) = \inf_t \{t : \alpha(t) \leq \alpha\},$$

$$\beta(t) = h(\alpha) = 1 - \alpha - \sum_{v=1}^{n-1} \mathbb{P}(A = \lceil \frac{g(\alpha)v - 1}{g(\alpha) + 1} \rceil) \mathbb{P}(C = v).$$

*Proof.* Consider the reject rule in Lemma A.3, then type I error

$$\begin{aligned} \alpha(t) &= \mathbb{P}(\frac{A}{C - A + 1} > t) \\ &= \sum_{v=1}^{n-1} \mathbb{P}(A > \frac{tv + t}{tv - 1}) \mathbb{P}(C = v), \end{aligned}$$

and type II error

$$\begin{aligned} \beta(t) &= \mathbb{P}(\frac{A + 1}{C - A} \leq t) \\ &= \sum_{v=1}^{n-1} \mathbb{P}(A \leq \frac{tv - 1}{t + 1}) \mathbb{P}(C = v) \\ &= 1 - \alpha(t) - \sum_{v=1}^{n-1} \mathbb{P}(\frac{tv - 1}{t + 1} < A \leq \frac{tv - 1}{t + 1} + 1) \mathbb{P}(C = v). \end{aligned}$$

Since  $\alpha(t)$  is non-increasing, then for each  $\alpha$ , there exists unique  $t$  such that  $t = g(\alpha)$ , where  $g(\alpha) = \inf_t \{t : \alpha(t) \leq \alpha\}$ .

Hence,  $\beta(t) = h(\alpha) = 1 - \alpha - \sum_{v=1}^{n-1} \mathbb{P}(A = \lceil \frac{g(\alpha)v - 1}{g(\alpha) + 1} \rceil) \mathbb{P}(C = v)$ . □

### Proof of Theorem 1

*Proof.* Similar in proof of Lemma A.5, we can obtain that

$$\begin{aligned} \alpha(t) &= \mathbb{P}(\frac{A + \Delta}{C - A + 1 - \Delta} > t) \\ &= \mathbb{P}(\Delta = 0) \mathbb{P}(\frac{A}{C - A + 1} > t) + \mathbb{P}(\Delta = 1) \mathbb{P}(\frac{A + 1}{C - A} > t), \end{aligned}$$

$$\begin{aligned} \beta(t) &= \mathbb{P}(\frac{A + 1 - \Delta}{C - A + \Delta} \leq t) \\ &= \mathbb{P}(\Delta = 0) \mathbb{P}(\frac{A + 1}{C - A} \leq t) + \mathbb{P}(\Delta = 1) \mathbb{P}(\frac{A}{C - A + 1} \leq t). \end{aligned}$$

Let  $g(\alpha) = \inf_t \{t : \alpha(t) \leq \alpha\}$  and substitute the probability function of the  $A$  and  $C$  into the expression, we can obtain that

$$\begin{aligned} \beta(t) &= h(\alpha) \\ &= 1 - \alpha - c_0 \sum_{v=1}^{n-1} \mathbb{P}(B_1(v) < A \leq B_2(v) | C = v) \mathbb{P}(C = v), \end{aligned} \tag{14}$$

where  $c_0 = \frac{e^{-\epsilon_0} - 1}{e^{-\epsilon_0} + 1}$ ,  $B_1(v) = \frac{g(\alpha)v - 1}{g(\alpha) + 1}$ ,  $B_2(v) = \frac{g(\alpha)v - 1}{g(\alpha) + 1} + 1$ ,  $\mathbb{P}(C = v) = \binom{n-1}{v} e^{-v\epsilon_0} (1 - e^{-\epsilon_0})^{n-1-v}$ ,  $v = 0, 1, \dots, n - 1$ ,  $P(A = k | C = v) = \binom{v}{k} (\frac{1}{2})^k$ ,  $k = 0, 1, \dots, v$ . Then it follows that the mechanism  $M$  satisfies  $h$ -DP. By combining this with Lemma A.1, the proof is completed. □

### A.2. Proof of Lemma 1

Consider the following two multinomial distributions  $P_1$  and  $Q_1$ , where  $P_1 := (n_0 + 1, n_1, n_2)$ ,  $Q_1 := (n_0, n_1 + 1, n_2)$  and  $(n_0, n_1, n_2) \sim \text{MultiNom}(n - 1; \frac{p}{2}, \frac{p}{2}, 1 - p)$ ,  $p = e^{-\epsilon_0}$ . It is easy to check that  $T(P, Q) = T(P_1, Q_1)$ , where  $P$  and  $Q$  are distributions defined in Lemma A.2. In addition, if  $P_2$  and  $Q_2$  are distributions defined in Theorem 1, then we need to calculate  $T(P_2, Q_2)$ , where  $P_2 = (n_0 + 1 - \Delta, n_1 + \Delta, n_2)$  and  $Q_2 = (n_0 + \Delta, n_1 + 1 - \Delta, n_2)$ ,  $\Delta \sim \text{Bern}(p)$ . The following lemma is a basic property of multinomial distribution.

**Lemma A.6.** Assume  $\xi = (n_0, n_1, n_2)'$  is a random variable which obeys  $\text{MultiNom}(n - 1; \frac{p}{2}, \frac{p}{2}, 1 - p)$ , then expectation of  $\xi$  is  $\tilde{\boldsymbol{\mu}} = (\frac{(n-1)p}{2}, \frac{(n-1)p}{2}, (n-1)(1-p))'$  and covariance matrix of  $\xi$  is

$$\tilde{\boldsymbol{\Sigma}} = (n - 1) \begin{pmatrix} \frac{p}{2}(1 - \frac{p}{2}) & -\frac{p^2}{4} & -\frac{p(1-p)}{2} \\ -\frac{p^2}{4} & \frac{p}{2}(1 - \frac{p}{2}) & -\frac{p(1-p)}{2} \\ -\frac{p(1-p)}{2} & -\frac{p(1-p)}{2} & p(1 - p) \end{pmatrix}$$

This lemma can be obtained from simple calculation directly. Next, we prove that the multinomial distribution approximately obeys the multivariate normal distribution.

### Proof of Lemma 1

*Proof.* Since  $\xi = (n_0, n_1, n_2)'$  obeys  $MultiNom(n-1; p_0, p_1, p_2)$  with  $p_0 = p/2, p_1 = p/2$  and  $p_2 = 1-p$ , the characteristic function

$$\phi_\xi(t_0, t_1, t_2) = E(e^{it_0 n_0 + it_1 n_1 + it_2 n_2}), \quad (15)$$

then

$$\begin{aligned} \phi_\xi(t_0, t_1, t_2) &= \sum_{n_0, n_1, n_2=0}^{n-1} \frac{n!}{n_0! n_1! n_2!} p_0^{n_0} p_1^{n_1} p_2^{n_2} e^{it_0 n_0 + it_1 n_1 + it_2 n_2} \\ &= (p_0 e^{it_0} + p_1 e^{it_1} + p_2 e^{it_2})^{n-1}. \end{aligned} \quad (16)$$

Let  $\tilde{\xi} = (\frac{n_0 - (n-1)p_0}{\sqrt{n-1}}, \frac{n_1 - (n-1)p_1}{\sqrt{n-1}}, \frac{n_2 - (n-1)p_2}{\sqrt{n-1}})'$ , then we have  $\phi_{\tilde{\xi}}(t_0, t_1, t_2) =$

$$(p_0 e^{\frac{it_0}{\sqrt{n-1}}} + p_1 e^{\frac{it_1}{\sqrt{n-1}}} + p_2 e^{\frac{it_2}{\sqrt{n-1}}})^{n-1} e^{-\sqrt{n-1}i(p_0 t_0 + p_1 t_1 + p_2 t_2)}.$$

Based on Taylor expansion of  $e^y = 1 + y + \frac{y^2}{2} + o(y^2)$  near point 0, we can derive that

$$\begin{aligned} &p_0 e^{\frac{it_0}{\sqrt{n-1}}} + p_1 e^{\frac{it_1}{\sqrt{n-1}}} + p_2 e^{\frac{it_2}{\sqrt{n-1}}} \\ &= 1 + i \frac{a}{\sqrt{n-1}} - \frac{b}{2(n-1)} + o(\frac{1}{n-1}), \end{aligned}$$

where  $a = \sum_{j=0}^2 p_j t_j, b = \sum_{j=0}^2 p_j t_j^2$ . In addition, since  $\log(1 + y) = 1 - \frac{y^2}{2} + o(y^2)$  when  $y \rightarrow 0$ , we can obtain that  $\ln(\psi_{\tilde{\xi}}(t)) \rightarrow -\frac{b-a^2}{2}$  and

$$\begin{aligned} -\frac{b-a^2}{2} &= -\frac{1}{2} \left[ \sum_{j=0}^2 p_j (1-p_j) t_j^2 - \sum_{j=0, j \neq k}^2 \sum_{k=0}^2 p_j p_k t_j t_k \right] \\ &= -\frac{1}{2} t' \tilde{\Sigma} t, \end{aligned}$$

which is the logarithm of the characteristic function of multivariate normal distribution  $N(\mathbf{0}, \tilde{\Sigma})$ , where  $\tilde{\Sigma}$  is defined in Lemma A.6. According to the uniqueness of the characteristic function,  $\tilde{\xi} \sim N(\mathbf{0}, \tilde{\Sigma})$  when  $n$  is sufficiently large, which indicates that  $\xi$  approximately follows  $N(\tilde{\mu}, \tilde{\Sigma})$ .  $\square$

### A.3. Proof of Theorem 2

*Proof.* According to Proposition 1, the key component is to measure distance between two distributions  $P_2$  and  $Q_2$ , where  $P_2 = (n_0+1-\Delta, n_1+\Delta, n_2)$  and  $Q_2 = (n_0+\Delta, n_1+1-\Delta)$ ,  $(n_0, n_1, n_2) \sim MultiNom(n-1; \frac{p}{2}, \frac{p}{2}, 1-p)$ ,  $\Delta \sim Bern(p)$  and  $p = e^{-\epsilon_0}$ . Let  $P = (n_0+1, n_1, n_2)$  and  $Q = (n_0, n_1+1, n_2)$ , we first prove that

$$T(P, Q) = T(Q, P) \geq \Phi \left( \Phi^{-1}(1-\alpha) - \frac{2}{\sqrt{n-1}} e^{\frac{\epsilon_0}{2}} \right) \quad (17)$$

approximately. If the inequality (17) holds, then

$$T(P_2, Q_2) = \mathbb{P}(\Delta = 0)T(P, Q) + \mathbb{P}(\Delta = 1)T(Q, P),$$

which indicates that

$$T(P_2, Q_2) = (\mathbb{P}(\Delta = 0) + \mathbb{P}(\Delta = 1))T(P, Q) = T(P, Q) \quad (18)$$

by using the fact that  $T(P, Q) = T(Q, P)$ .

We will now prove that the inequality (17) holds. Combined with Lemma 1, the key is to prove the following formula,

$$T(N(\tilde{\mu}_0, \tilde{\Sigma}), N(\tilde{\mu}_1, \tilde{\Sigma})) \geq \Phi \left( \Phi^{-1}(1-\alpha) - \frac{2}{\sqrt{n-1}} e^{\frac{\epsilon_0}{2}} \right), \quad (19)$$

where  $\tilde{\mu}_0 = \mathbb{E}(P)$ ,  $\tilde{\mu}_1 = \mathbb{E}(Q)$ , and  $\tilde{\Sigma} = Cov(P) = Cov(Q)$ . However,  $\tilde{\Sigma}$  is not irreversible because there exists a linear relationship between sub-vectors:  $n_0 + n_1 + n_2 = n-1$ . Hence, we need to combine postprocessing properties of  $f$ -DP and the fact that sub-vector of a multivariate normal variable is still a multivariate normal variable.

Since  $P = (n_0+1, n_1, n_2)'$  and  $Q = (n_0, n_1+1, n_2)'$ , we can use sub-vector  $P_2 = (n_0+1, n_1)'$  and  $Q_2 = (n_0, n_1+1)'$  to construct  $P$  and  $Q$  by formula  $n_2 = n-1-n_0-n_1$ . Then,  $P = Proc(P_2)$  and  $Q = Proc(Q_2)$ , which indicates that  $T(P, Q) \leq T(P_2, Q_2)$  by Fact 1.

From another perspective, it is obvious that  $P_2 = Proc(P)$  and  $Q = Proc(Q)$  if we take  $Proc(\cdot)$  as a projection, then  $T(P, Q) \geq T(P_2, Q_2)$ . Notice that  $P_2$  obeys  $N(\mu_0, \Sigma)$  and  $Q_2$  obeys  $N(\mu_1, \Sigma)$ , where  $\mu_0 = (\frac{(n-1)p}{2} + 1, \frac{(n-1)p}{2})'$ ,  $\mu_1 = (\frac{(n-1)p}{2}, \frac{(n-1)p}{2} + 1)'$  and

$$\Sigma = (n-1) \begin{pmatrix} \frac{p}{2}(1-\frac{p}{2}) & -\frac{p^2}{4} \\ -\frac{p^2}{4} & \frac{p}{2}(1-\frac{p}{2}) \end{pmatrix}.$$

After simple algebraic operation, we can obtain that

$$\Sigma^{-1} = \frac{1}{n-1} \begin{pmatrix} \frac{2-p}{p(1-p)} & \frac{1}{1-p} \\ \frac{1}{1-p} & \frac{2-p}{p(1-p)} \end{pmatrix},$$

and

$$\begin{aligned} &(\mu_1 - \mu_0)' \Sigma^{-1} (\mu_1 - \mu_0) \\ &= (-1, 1) \frac{1}{n-1} \begin{pmatrix} \frac{2-p}{p(1-p)} & \frac{1}{1-p} \\ \frac{1}{1-p} & \frac{2-p}{p(1-p)} \end{pmatrix} \begin{pmatrix} -1 \\ 1 \end{pmatrix} \quad (20) \\ &= \frac{4}{(n-1)p}. \end{aligned}$$

Then  $T(P, Q) = \Phi(\Phi^{-1}(1-\alpha) - \frac{2}{\sqrt{(n-1)p}})$ , and the inequality (17) can be obtained immediately by using Lemma A.4.  $\square$