Erratum to "LightVeriFL: A Lightweight and Verifiable Secure Aggregation for Federated Learning"

Baturalp Buyukates, Jinhyun So, *Member, IEEE*, Hessam Mahdavifar, *Member, IEEE*, and Salman Avestimehr, *Fellow, IEEE*

I. Introduction

THIS article addresses errors in [1]. Equation (2) contained an error wherein x was not bold. It is corrected below.

$$\sum_{i\in\mathcal{U}_a}\mathbf{x}_i=\sum_{i\in\mathcal{U}_a}(\tilde{x}_{\mathbf{i}}-\mathrm{PRG}(b_i))+\sum_{i\in\mathcal{D}_a}\left(\sum_{j:i<j}\mathrm{PRG}(a_{i,j})-\sum_{j:i>j}\mathrm{PRG}(a_{j,i})\right),\quad(2)$$

The equation numbering in Appendix B contained an error and is corrected below.

II. Proof of (21)

For the input privacy, i.e., hash privacy, we want to show equation (23) shown at the bottom of the page, for an arbitrary set $\mathcal{T}$ of T colluding users and a surviving user set $\mathcal{U}$ such that $\mathcal{U}\subseteq[N]$, $|\mathcal{U}|\geq U$, $U=T+1$. This is the mutual information between individual hashes of the users $\{h_i\}_{i\in[N]}$ and what the server receives from the users during LightVeriFL execution $\{h_i+z_i\}_{i\in[N]}$, $\{\sum_{j\in[N]}[\tilde{z}_j]_i\}_{i\in\mathcal{U}}$, given what the server recovers $\sum_{i\in[N]}h_i$ and receives from the colluding parties $\{h_i\}_{i\in\mathcal{T}}$, $\{z_i\}_{i\in\mathcal{T}}$, $\{[\tilde{z}_j]_i\}_{j\in[N],i\in\mathcal{T}}$. We have equations (24)–(26), shown at the bottom of the page and (27)–(29), shown at the top of the next page

$$I\left(\{h_i\}_{i\in[N]};\{h_i+z_i\}_{i\in[N]},\left\{\sum_{j\in[N]}[\tilde{z}_j]_i\right\}_{i\in\mathcal{U}}\middle|\sum_{i\in[N]}h_i,\{h_i\}_{i\in\mathcal{T}},\{z_i\}_{i\in\mathcal{T}},\left\{[\tilde{z}_j]_i\right\}_{j\in[N],i\in\mathcal{T}}\right)=0,\quad(23)$$

$$I\left(\{h_i\}_{i\in[N]};\{h_i+z_i\}_{i\in[N]},\left\{\sum_{j\in[N]}[\tilde{z}_j]_i\right\}_{i\in\mathcal{U}}\middle|\sum_{i\in[N]}h_i,\{h_i\}_{i\in\mathcal{T}},\{z_i\}_{i\in\mathcal{T}},\left\{[\tilde{z}_j]_i\right\}_{j\in[N],i\in\mathcal{T}}\right)$$

$$=H\left(\{h_i+z_i\}_{i\in[N]},\left\{\sum_{j\in[N]}[\tilde{z}_j]_i\right\}_{i\in\mathcal{U}}\middle|\sum_{i\in[N]}h_i,\{h_i\}_{i\in\mathcal{T}},\{z_i\}_{i\in\mathcal{T}},\left\{[\tilde{z}_j]_i\right\}_{j\in[N],i\in\mathcal{T}}\right)-H\left(\{h_i+z_i\}_{i\in[N]},\left\{\sum_{j\in[N]}[\tilde{z}_j]_i\right\}_{i\in\mathcal{U}}\middle|\{h_i\}_{i\in[N]},\{z_i\}_{i\in\mathcal{T}},\left\{[\tilde{z}_j]_i\right\}_{j\in[N],i\in\mathcal{T}}\right)\quad(24)$$

$$=H\left(\{h_i+z_i\}_{i\in[N]},\sum_{i\in[N]}z_i,\sum_{i\in[N]}n_i\middle|\sum_{i\in[N]}h_i,\{h_i\}_{i\in\mathcal{T}},\{z_i\}_{i\in\mathcal{T}},\left\{[\tilde{z}_j]_i\right\}_{j\in[N],i\in\mathcal{T}}\right)-H\left(\{z_i\}_{i\in[N]},\sum_{i\in[N]}z_i,\sum_{i\in[N]}n_i\middle|\{h_i\}_{i\in[N]},\{z_i\}_{i\in\mathcal{T}},\left\{[\tilde{z}_j]_i\right\}_{j\in[N],i\in\mathcal{T}}\right)\quad(25)$$

$$=H\left(\{h_i+z_i\}_{i\in[N]\setminus\mathcal{T}}\middle|\sum_{i\in[N]}h_i,\{h_i\}_{i\in\mathcal{T}},\{z_i\}_{i\in\mathcal{T}},\left\{[\tilde{z}_j]_i\right\}_{j\in[N],i\in\mathcal{T}}\right)+H\left(\sum_{i\in[N]}z_i,\sum_{i\in[N]}n_i\middle|\{h_i+z_i\}_{i\in[N]\setminus\mathcal{T}},\sum_{i\in[N]}h_i,\{h_i\}_{i\in\mathcal{T}},\{z_i\}_{i\in\mathcal{T}},\left\{[\tilde{z}_j]_i\right\}_{j\in[N],i\in\mathcal{T}}\right)$$

$$-H\left(\{z_i\}_{i\in[N]}\middle|\{h_i\}_{i\in[N]},\{z_i\}_{i\in\mathcal{T}},\left\{[\tilde{z}_j]_i\right\}_{j\in[N],i\in\mathcal{T}}\right)-H\left(\sum_{i\in[N]}z_i,\sum_{i\in[N]}n_i\middle|\{z_i\}_{i\in[N]},\{h_i\}_{i\in[N]},\left\{[\tilde{z}_j]_i\right\}_{j\in[N],i\in\mathcal{T}}\right)\quad(26)$$

Manuscript received 11 June 2024; accepted 11 June 2024. Date of current version 23 August 2024. *(Corresponding author: Baturalp Buyukates.)*

Baturalp Buyukates and Salman Avestimehr are with the Department of Electrical and Computer Engineering, University of Southern California, Los Angeles, CA 90089 USA (e-mail: buyukate@usc.edu; avestime@usc.edu).

Jinhyun So is with the Department of Electrical and Engineering and Computer Science, Daegu Gyeongbuk Institute of Science and Technology, Daegu 42988, South Korea (e-mail: jinhyun@dgist.ac.kr).

Hessam Mahdavifar is with the Department of Electrical and Computer Engineering, Northeastern University, Boston, MA 02115 USA, and also with the Department of Electrical Engineering and Computer Science, University of Michigan at Ann Arbor, Ann Arbor, MI 48109 USA (e-mail: hessam@umich.edu).

Digital Object Identifier 10.1109/JSAIT.2024.3413928

where equation (24) follows from the mutual information definition and equation (25) follows since $\{\sum_{j\in[N]}[\tilde{z}_j]_i\}_{i\in\mathcal{U}}$ is invertible to $\sum_{i\in[N]}z_i$, $\sum_{i\in[N]}n_i$ through the encoding matrix W. Equation (26) follows from the fact that $\{h_i+z_i\}_{i\in\mathcal{T}}$ is a deterministic function of $\{h_i\}_{i\in\mathcal{T}}$, $\{z_i\}_{i\in\mathcal{T}}$ and the chain rule. In equation (27), in the second term, $\sum_{i\in[N]}z_i$ is a deterministic function of $\{h_i+z_i\}_{i\in[N]\setminus\mathcal{T}}$, $\sum_{i\in[N]}h_i$, $\{h_i\}_{i\in\mathcal{T}}$, $\{z_i\}_{i\in\mathcal{T}}$; the third term follows from the independence of h_is and z_is and the fact that, given $\{z_i\}_{i\in\mathcal{T}}$, the remaining uncertainty is in $\{z_i\}_{i\in[N]\setminus\mathcal{T}}$; in the last term, $\sum_{i\in[N]}z_i$ is a function of $\{z_i\}_{i\in[N]}$ and h_is are independent of n_is. In

$$= H\left(\{h_i + z_i\}_{i\in[N]\setminus\mathcal{T}} \middle| \sum_{i\in[N]} h_i, \{h_i\}_{i\in\mathcal{T}}, \{z_i\}_{i\in\mathcal{T}}, \{[\tilde{z}_j]_i\}_{j\in[N],i\in\mathcal{T}}\right) + H\left(\sum_{i\in[N]} n_i \middle| \{h_i + z_i\}_{i\in[N]\setminus\mathcal{T}}, \sum_{i\in[N]} h_i, \{h_i\}_{i\in\mathcal{T}}, \{z_i\}_{i\in\mathcal{T}}, \{[\tilde{z}_j]_i\}_{j\in[N],i\in\mathcal{T}}\right)$$
$$- H\left(\{z_i\}_{i\in[N]\setminus\mathcal{T}} \middle| \{z_i\}_{i\in\mathcal{T}}, \{[\tilde{z}_j]_i\}_{j\in[N],i\in\mathcal{T}}\right) - H\left(\sum_{i\in[N]} n_i \middle| \{z_i\}_{i\in[N]}, \{[\tilde{z}_j]_i\}_{j\in[N],i\in\mathcal{T}}\right) \tag{27}$$

$$= H\left(\{h_i + z_i\}_{i\in[N]\setminus\mathcal{T}} \middle| \sum_{i\in[N]} h_i, \{h_i\}_{i\in\mathcal{T}}, \{z_i\}_{i\in\mathcal{T}}, \{[\tilde{z}_j]_i\}_{j\in[N],i\in\mathcal{T}}\right) + H\left(\sum_{i\in[N]} n_i \middle| \{h_i + z_i\}_{i\in[N]\setminus\mathcal{T}}, \sum_{i\in[N]} h_i, \{h_i\}_{i\in\mathcal{T}}, \{z_i\}_{i\in\mathcal{T}}, \{[\tilde{z}_j]_i\}_{j\in[N],i\in\mathcal{T}}\right)$$
$$- H(\{z_i\}_{i\in[N]\setminus\mathcal{T}}) - H\left(\sum_{i\in[N]} n_i \middle| \{z_i\}_{i\in[N]}, \{[\tilde{z}_j]_i\}_{j\in[N],i\in\mathcal{T}}\right) \tag{28}$$

$$= 0, \tag{29}$$

equation (28), the third term follows from the fact that $I(\{z_i\}_{i\in[N]\setminus\mathcal{T}}; \{z_i\}_{i\in\mathcal{T}}, \{[\tilde{z}_j]_i\}_{j\in[N],i\in\mathcal{T}}) = 0$, which follows from the T-private MDS condition $I(z_i; \{[\tilde{z}_i]_j\}_{j\in\mathcal{T}}) = 0$ and the independence of z_is. To reach equation (29), we make the following observations: First, in the second term of equation (28), $\sum_{i\in[N]} n_i$ is a function of $\{h_i + z_i\}_{i\in[N]\setminus\mathcal{T}}$, $\sum_{i\in[N]} h_i$, $\{h_i\}_{i\in\mathcal{T}}$, $\{z_i\}_{i\in\mathcal{T}}$, $\{[\tilde{z}_j]_i\}_{j\in[N],i\in\mathcal{T}}$; second, in the fourth term, $\sum_{i\in[N]} n_i$ is a function of $\{z_i\}_{i\in[N]}$, $\{[\tilde{z}_j]_i\}_{j\in[N],i\in\mathcal{T}}$; and finally, we note that z_is are uniformly random, and they have the maximum entropy over $\mathbb{F}_n$ (n is the EC subgroup order). Since the mutual information is non-negative, we reach equation (29).

REFERENCE

[1] B. Buyukates, J. So, H. Mahdavifar, and S. Avestimehr, "LightVeriFL: A lightweight and verifiable secure aggregation for federated learning," *IEEE J. Sel. Areas Inf. Theory*, vol. 5, pp. 285–301, 2024, doi: 10.1109/JSAIT.2024.3391849.