LSBlocFL: A Secure Federal Learning Model Combining Blockchain and Lightweight Cryptographic Solutions Supplementary File

This is the supplementary file for the paper entitled LSBlocFL: A Secure Federal Learning Model Combining Blockchain and Lightweight Cryptographic Solutions.Additional Proof are put into this file and cited by the paper

1 S1 Analysis

Lemma 1 *if* $\eta_t \leq \frac{1}{4\mathrm{L}}$ *,we have*

$$\mathbb{E}\|\overline{v}_{t+1}^{\epsilon} - w^*\|^2 \leq (1-\eta\mathrm{L})\mathbb{E}\|\overline{w_t^{\epsilon}} - w^*\|^2 + \eta^2\mathbb{E}\|g_t^{\epsilon} - \overline{g}_t^{\epsilon}\| + 6\mathrm{L}\eta_t^2 M + 2\mathbb{E}\sum_{k=1}^{N}\rho_k\|\overline{w}_t^{\epsilon} - w_k^t\|^2 \tag{1}$$

where $M = F^* - \sum_{k=1}^{N}\rho_k F_K^*, \overline{v}_{t+1}^{\epsilon} = \overline{w}_t^{\epsilon} - \eta_t g_t^{\epsilon}$.

Proof.

$$\begin{aligned}\left\|\overline{\mathbf{v}}_{t+1}^{\epsilon} - \mathbf{w}^{\star}\right\|^2 &= \|\overline{\mathbf{w}}_t^{\epsilon} - \eta_t\mathbf{g}_t - \mathbf{w}^{\star} - \eta_t\overline{\mathbf{g}}_t^{\epsilon} + \eta_t\overline{\mathbf{g}}_t^{\epsilon}\|^2 \\ &= \|\overline{\mathbf{w}}_t^{\epsilon} - \mathbf{w}^{\star} - \eta_t\overline{\mathbf{g}}_t^{\epsilon}\|^2 \\ &+ 2\eta_t\left\langle\overline{\mathbf{w}}_t - \mathbf{w}^{\star} - \eta_t\overline{\mathbf{g}}_t^{\epsilon}, \overline{\mathbf{g}}_t^{\epsilon} - \mathbf{g}_t\right\rangle \\ &+ \eta_t^2\left\|\mathbf{g}_t - \overline{\mathbf{g}}_t^{\epsilon}\right\|^2\end{aligned} \tag{2}$$

where $2\mathbb{E}\|\eta_t\left\langle\overline{\mathbf{w}}_t - \mathbf{w}^{\star} - \eta_t\overline{\mathbf{g}}_t^{\epsilon}, \overline{\mathbf{g}}_t^{\epsilon} - \mathbf{g}_t\right\rangle\| = 0$

$\|\overline{\mathbf{w}}_t^{\epsilon} - \mathbf{w}^{\star} - \eta_t\overline{\mathbf{g}}_t^{\epsilon}\|^2 = \|\overline{\mathbf{w}}_t^{\epsilon} - \mathbf{w}^{\star}\|^2 - 2\eta_t\left\langle\overline{\mathbf{w}}_t - \mathbf{w}^{\star}, \overline{\mathbf{g}}_t^{\epsilon}\right\rangle + \eta_t^2\left\|\overline{\mathbf{g}}_t^{\epsilon}\right\|^2$.According to the the L-smoothness of $F_k()$,we have

$$\left\|\nabla F_k\left(\mathbf{w}_t^k\right)\right\|^2 \leq 2L\left(F_k\left(\mathbf{w}_t^k\right) - F_k^*\right) \tag{3}$$

According to $\|\cdot\|^2$,we have

$$\left\|\nabla F_k\left(\mathbf{w}_t^k\right)\right\|^2 \leq 2L\eta_t^2\sum_{k=1}^{N}\rho_k\left(F_k\left(\mathbf{w}_t^k\right) - F_k^*\right) \tag{4}$$

Then

$$\begin{gathered}-2\eta_t < \overline{w}_t^{\epsilon} - w^*, \overline{g}_t >= 2\eta_t\sum_{k=1}^{N}\rho_k < \overline{w}_t^{\epsilon} - w^*, \nabla F_K(w_t^k) >= \\ -2\eta_t\sum_{k=1}^{N}\rho_k < \overline{w}_t^{\epsilon} - w_t^k, \nabla F_k(w_t^k) > -2\eta_t\sum_{k=1}^{N}\rho_k < w_t^k - w^*, \nabla F_k(w_t^k) >\end{gathered} \tag{5}$$

By Cauchy-Schwarz inequality and AM-GM inequality, we have

$$-2\left\langle\overline{\mathbf{w}}_t^{\epsilon} - \mathbf{w}_t^k, \nabla F_k\left(\mathbf{w}_t^k\right)\right\rangle \leq \frac{1}{\eta_t}\left\|\overline{\mathbf{w}}_t^{\epsilon} - \mathbf{w}_t^k\right\|^2 + \eta_t\left\|\nabla F_k\left(\mathbf{w}_t^k\right)\right\|^2 \tag{6}$$

By the µ-strong convexity of Fk(·), we have

$$-\left\langle \mathbf{w}_t^k-\mathbf{w}^\star, \nabla F_k\left(\mathbf{w}_t^k\right)\right\rangle \leq -\left(F_k\left(\mathbf{w}_t^k\right)-F_k\left(\mathbf{w}^*\right)\right)-\frac{\mu}{2}\left\|\mathbf{w}_t^k-\mathbf{w}^\star\right\|^2 \tag{7}$$

Then

$$\begin{aligned}
\left\|\overline{\mathbf{w}}_t^\epsilon-\mathbf{w}^\star-\eta_t\overline{\mathbf{g}}_t^\epsilon\right\|^2 \leq & \left\|\overline{\mathbf{w}}_t^\epsilon-\mathbf{w}^\star\right\|^2+2L\eta_t^2\sum_{k=1}^N \rho_k\left(F_k\left(\mathbf{w}_t^k\right)-F_k^*\right) \\
& +\eta_t\sum_{k=1}^N \rho_k\left(\frac{1}{\eta_t}\left\|\overline{\mathbf{w}}_t^\epsilon-\mathbf{w}_k^t\right\|^2+\eta_t\left\|\nabla F_k\left(\mathbf{w}_t^k\right)\right\|^2\right) \\
& -2\eta_t\sum_{k=1}^N \rho_k\left(F_k\left(\mathbf{w}_t^k\right)-F_k\left(\mathbf{w}^*\right)+\frac{\mu}{2}\left\|\mathbf{w}_t^k-\mathbf{w}^\star\right\|^2\right) \\
= & \left(1-\mu\eta_t\right)\left\|\overline{\mathbf{w}}_t^\epsilon-\mathbf{w}^\star\right\|^2+\sum_{k=1}^N p_k\left\|\overline{\mathbf{w}}_t^\epsilon-\mathbf{w}_k^t\right\|^2 \\
& +4L\eta_t^2\sum_{k=1}^N \rho_k\left(F_k\left(\mathbf{w}_t^k\right)-F_k^*\right)-2\eta_t\sum_{k=1}^N \rho_k\left(F_k\left(\mathbf{w}_t^k\right)-F_k\left(\mathbf{w}^*\right)\right)
\end{aligned} \tag{8}$$

Then $\pi=2\eta(1-2L\eta_t), \eta_t \leq \frac{1}{4L}, \eta \leq\leq 2\eta_t$.Then we have

$$\begin{aligned}
4L\eta_t^2\sum_{k=1}^N \rho_k\left(F_k\left(\mathbf{w}_t^k\right)-F_k^*\right)-2\eta_t\sum_{k=1}^N \rho_k\left(F_k\left(\mathbf{w}_t^k\right)-F_k\left(\mathbf{w}^*\right)\right) = & -2\eta_t\left(1-2L\eta_t\right)\sum_{k=1}^N \rho_k\left(F_k\left(\mathbf{w}_t^k\right)-F_k^*\right) \\
& +2\eta_t\sum_{k=1}^N \rho_k\left(F_k\left(\mathbf{w}^*\right)-F_k^*\right) \\
= & -\pi_t\sum_{k=1}^N \rho_k\left(F_k\left(\mathbf{w}_t^k\right)-F^*\right) \\
& +\left(2\eta_t-\pi_t\right)\sum_{k=1}^N \rho_k\left(F^*-F_k^*\right) \\
= & -\pi_t\sum_{k=1}^N p_k\left(F_k\left(\mathbf{w}_t^k\right)-F^*\right)+4L\eta_t^2 M
\end{aligned} \tag{9}$$

where,$M=\sum_{k=1}^N p_k\left(F^*-F_k^*\right)=F^*-\sum_{k=1}^N p_k F_k^*$

Then

$$\begin{aligned}
\sum_{k=1}^N \rho_k\left(F_k\left(\mathbf{w}_t^k\right)-F^*\right) = & \sum_{k=1}^N \rho_k\left(F_k\left(\mathbf{w}_t^k\right)-F_k\left(\overline{\mathbf{w}}_t^\epsilon\right)\right)+\sum_{k=1}^N \rho_k\left(F_k\left(\overline{\mathbf{w}}_t^\epsilon\right)-F^*\right) \\
\geq & \sum_{k=1}^N \rho_k\left\langle\nabla F_k\left(\overline{\mathbf{w}}_t^\epsilon\right), \mathbf{w}_t^k-\overline{\mathbf{w}}_t^\epsilon\right\rangle+\left(F\left(\overline{\mathbf{w}}_t^\epsilon\right)-F^*\right) \\
\geq & -\frac{1}{2}\sum_{k=1}^N \rho_k\left[\eta_t\left\|\nabla F_k\left(\overline{\mathbf{w}}_t^\epsilon\right)\right\|^2+\frac{1}{\eta_t}\left\|\mathbf{w}_t^k-\overline{\mathbf{w}}_t^\epsilon\right\|^2\right]+\left(F\left(\overline{\mathbf{w}}_t^\epsilon\right)-F^*\right) \\
\geq & -\sum_{k=1}^N \rho_k\left[\eta_t L\left(F_k\left(\overline{\mathbf{w}}_t^\epsilon\right)-F_k^*\right)+\frac{1}{2\eta_t}\left\|\mathbf{w}_t^k-\overline{\mathbf{w}}_t^\epsilon\right\|^2\right]+\left(F\left(\overline{\mathbf{w}}_t^\epsilon\right)-F^*\right)
\end{aligned} \tag{10}$$

where the first inequality results from the convexity of $F_k(\cdot)$, the second inequality from AM-GM inequality and the third inequality from (3)

Then

$$
\begin{aligned}
& -\pi_t \sum_{k=1}^{N} \rho_k \left(F_k\left(\mathbf{w}_t^k\right)-F^*\right)+4L\eta_t^2 M \\
& =\pi_t \sum_{k=1}^{N} \rho_k(\eta_t L\left(F_k\left(\overline{\mathbf{w}}_t^\epsilon\right)-F_k^*\right)+\frac{1}{2\eta_t}\left\|\mathbf{w}_t^k-\overline{\mathbf{w}}_t^\epsilon\right\|^2)-\pi_t\left(F\left(\overline{\mathbf{w}}_t\right)-F^*\right)+4L\eta_t^2 M \\
& =\pi_t\left(\eta_t L-1\right) \sum_{k=1}^{N} \rho_k\left(F_k\left(\overline{\mathbf{w}}_t^\epsilon\right)-F^*\right)+\left(4L\eta_t^2+\pi_t\eta_t L\right) M+\frac{\pi_t}{2\eta_t} \sum_{k=1}^{N} \rho_k\left\|\mathbf{w}_t^k-\overline{\mathbf{w}}_t^\epsilon\right\|^2 \\
& \leq 6L\eta_t^2 M+\sum_{k=1}^{N} \rho_k\left\|\mathbf{w}_t^k-\overline{\mathbf{w}}_t^\epsilon\right\|^2
\end{aligned}
\tag{11}
$$

where we use the following facts $(1)\eta_t L-1 \leq -\frac{1}{4} \leq 0, \sum_{k=1}^{N} \rho_k(F_k(\overline{w}_t)-F^*) \geq 0, (2)M \geq 0, 4L\eta_t^2+\pi_t\eta_t L \leq 6\eta_t^2 L, (3)\frac{\pi_t}{2\eta_t} \leq 1$

Then

$$
\left\|\overline{\mathbf{w}}_t^\epsilon-\mathbf{w}^\star-\eta_t\overline{\mathbf{g}}_t^\epsilon\right\|^2 \leq\left(1-\mu\eta_t\right)\left\|\overline{\mathbf{w}}_t^\epsilon-\mathbf{w}^\star\right\|^2+2\sum^{N} \rho_k\left\|\overline{\mathbf{w}}_t^\epsilon-\mathbf{w}_k^t\right\|^2+6\eta_t^2 LM \tag{12}
$$

Using $\left\|\overline{\mathbf{w}}_t^\epsilon-\mathbf{w}^\star-\eta_t\overline{\mathbf{g}}_t^\epsilon\right\|^2=\left\|\overline{\mathbf{w}}_t^\epsilon-\mathbf{w}^\star\right\|^2-2\eta_t\left\langle\overline{\mathbf{w}}_t-\mathbf{w}^\star, \overline{\mathbf{g}}_t^\epsilon\right\rangle+\eta_t^2\left\|\overline{\mathbf{g}}_t^\epsilon\right\|^2$ and (12),taking expectation on both sides of equation,we complete the proof.

□