Supplementary material of "Compression-based Privacy Preservation for Distributed Nash Equilibrium Seeking in Aggregative Games"

APPENDIX

A. Useful Lemmas

The following results are used in the proofs.

Lemma 3. *[1] Let $\{u_k\}$, $\{v_k\}$, $\{w_k\}$ and $\{z_k\}$ be the nonnegative sequences of random variables. If they satisfy*

$$\mathbb{E}[u_{k+1}] \leq (1+z_k)u_k - v_k + w_k,$$

$$\sum_{k=0}^{\infty} z_k < \infty \ a.s., \ \textit{and} \ \sum_{k=0}^{\infty} w_k < \infty \ a.s.,$$

then u_k converges almost surely (a.s.), and $\sum_{k=0}^{\infty} v_k < \infty$ a.s..

Lemma 4. *[1] Let $\{u_k\}$ be a non-negative sequence satisfying the following relationship for all $k \geq 0$:*

$$u_{k+1} \leq (1+\gamma_k)u_k + v_k, \tag{16}$$

where sequence $\gamma_k \geq 0$ and $v_k \geq 0$ satisfy $\sum_{k=0}^{\infty} \gamma_k < \infty$ and $\sum_{k=0}^{\infty} v_k < \infty$, respectively. Then the sequence $\{u_k\}$ will converge to a finite value $u > 0$.

Lemma 5. *[2] Let $\{u_k\}$ be a non-negative sequence satisfying the following relationship for all $k \geq 0$:*

$$u_{k+1} \leq (1-\gamma_{1,k})u_k + \gamma_{2,k} \tag{17}$$

where $\gamma_{1,k} \geq 0$ and $\gamma_{2,k} \geq 0$ satisfying

$$\frac{a_1}{(a_2 k+1)^{b_1}} \leq \gamma_{1,k} \leq 1, \ \frac{a_3}{(a_2 k+1)^{b_2}} \leq \gamma_{2,k} \leq 1,$$

for some $c_1, c_2, c_3 > 0$, $0 \leq b_1 < 1$, and $b_1 < b_2$. Then for all $0 \leq b_0 < b_2 - b_1$, we have $\lim_{k\to\infty}(k+1)^{b_0} u_k = 0$.

B. Proof of Lemma 1

Denote $\bar{\mathbf{y}} = \frac{1}{N}\mathbf{1}^\top \mathbf{y}$ and $\Theta = I - \frac{1}{N}\mathbf{1}\mathbf{1}^\top$, then we have $\|\Theta\| \leq 1$ and

$$\|\mathbf{y}_{k+1} - \mathbf{1}\bar{\mathbf{x}}_{k+1}\|^2 = \|\Theta\mathbf{y}_{k+1} + \mathbf{1}\bar{\mathbf{y}}_{k+1} - \mathbf{1}\bar{\mathbf{x}}_{k+1}\|^2 \leq \|\mathbf{y}_{k+1}\|^2, \tag{18}$$

where the inequality follows from (8) in the main article. Therefore, we can complete the proof by showing $\sum_{k=0}^{\infty} \beta_k \mathbb{E}\left[\|\mathbf{y}_k\|^2\right] < \infty$. Since $\sum_{k=1}^{\infty} \beta_k^2 < \infty$, there obviously exists k_1 such that $\beta_k < 1/\lambda_2$, $\forall k > k_1$. We know that $\sum_{k=0}^{k_1} \beta_k \mathbb{E}\left[\|\mathbf{y}_k\|^2\right]$ is always bounded. Therefore, we only need to focus on proving $\sum_{k=k_1+1}^{\infty} \beta_k \mathbb{E}\left[\|\mathbf{y}_k\|^2\right] < \infty$

Based on (7b) in the main article, we obtain

$$\begin{aligned}
&\mathbb{E}\left[\|\mathbf{y}_{k+1}\|^2\right] \\
=&\mathbb{E}\left[\|A_k\mathbf{y}_k + \mathbf{x}_{k+1} - \mathbf{x}_k\|^2\right] + \beta_k^2\mathbb{E}\left[\|L\mathbf{e}_k\|^2\right] - \mathbb{E}\left[\beta_k(A_k\mathbf{y}_k + \mathbf{x}_{k+1} - \mathbf{x}_k)^\top L\mathbf{e}_k\right] \\
\leq&\mathbb{E}\left[(\|A_k\mathbf{y}_k\| + \|\mathbf{x}_{k+1} - \mathbf{x}_k\|)^2\right] + \beta_k^2\lambda_M^2 N\sigma^2 \\
\leq&(1+\nu_1)(1-\beta_k\lambda_2)^2\mathbb{E}\left[\|\mathbf{y}_k\|^2\right] + (1+\frac{1}{\nu_1})C^2N\alpha_k^2\beta_k^2 + \lambda_M^2 N\sigma^2\beta_k^2,
\end{aligned} \tag{19}$$

where the first inequality holds from $\mathbb{E}[\mathbf{e}_k] = 0$ and $\mathbb{E}\left[\|\mathbf{e}_k\|^2\right] \leq N\sigma^2$ in Assumption 6, the last inequality uses $(a+b)^2 \leq (1+\nu_1)a^2 + (1+\frac{1}{\nu_1})b^2$ for any $a, b \in \mathbb{R}$ and $\nu_1 > 0$, and λ_2 and λ_M are the second smallest eigenvalue and the eigenvalue with the largest magnitude of L [3], respectively. By setting $\nu_1 = \beta_k\lambda_2$, we further get

$$\begin{aligned}
&\mathbb{E}\left[\|\mathbf{y}_{k+1}\|^2\right] \\
\leq&(1-\beta_k^2\lambda_2^2)(1-\beta_k\lambda_2)\mathbb{E}\left[\|\mathbf{y}_k\|^2\right] + (\alpha_k^2\beta_k^2 + \frac{\alpha_k^2\beta_k}{\lambda_2})C^2N + \lambda_M^2 N\sigma^2\beta_k^2 \\
\leq&(1-\beta_k\lambda_2)\mathbb{E}\left[\|\mathbf{y}_k\|^2\right] + (\alpha_k^2\beta_k^2 + \frac{\alpha_k^2\beta_k}{\lambda_2})C^2N + \lambda_M^2 N\sigma^2\beta_k^2.
\end{aligned} \tag{20}$$

Since $\beta_k\lambda_2 > 0$, we can have the following relationship:

$$\mathbb{E}\left[\|\mathbf{y}_{k+1}\|^2\right] \leq (1+\beta_k^2)\mathbb{E}\left[\|\mathbf{y}_k\|^2\right] - \lambda_2\beta_k\mathbb{E}\left[\|\mathbf{y}_k\|^2\right] + (\alpha_k^2\beta_k^2 + \frac{\alpha_k^2\beta_k}{\lambda_2})C^2N + \lambda_M^2 N\sigma^2\beta_k^2. \tag{21}$$

Since $\sum_{k=k_1+1}^{\infty} \alpha_k^2\beta_k < \infty$ and $\sum_{k=k_1+1}^{\infty} \beta_k^2 < \infty$, it is guaranteed that $\sum_{k=k_1+1}^{\infty}[(\alpha_k^2\beta_k^2 + \frac{\alpha_k^2\beta_k}{\lambda_2})C^2N + \lambda_M^2 N\sigma^2\beta_k^2] < \infty$. Thus, we can conclude that $\sum_{k=k_1+1}^{\infty} \beta_k \mathbb{E}\left[\|\mathbf{y}_k\|^2\right] < \infty$ from Lemma 3.

C. Proof of Theorem 1

Obviously, there exists k_0 such that $\beta_k < 1, \forall k > k_0$, to satisfy $\sum_{k=0}^{\infty} \beta_k^2 < \infty$. According to the dynamics in (7a), it can be verified that the following relationship holds:

$$\begin{aligned}
&\mathbb{E}\left[\|\mathbf{x}_{k+1} - \mathbf{x}^*\|^2\right] \\
=&\mathbb{E}\left[\|\mathbf{P}_{\mathcal{X}}[\mathbf{x}_k - \alpha_k\beta_k G(\mathbf{x}_k, \mathbf{y}_k)] - \mathbf{P}_{\mathcal{X}}[\mathbf{x}^* - \alpha_k\beta_k G(\mathbf{x}^*, \mathbf{1}\bar{\mathbf{x}}^*)]\|^2\right] \\
\leq&\mathbb{E}\left[\|\mathbf{x}_k - \mathbf{x}^* - \alpha_k\beta_k(G(\mathbf{x}_k, \mathbf{y}_k) - G(\mathbf{x}^*, \mathbf{1}\bar{\mathbf{x}}^*))\|^2\right] \\
=&\mathbb{E}\left[\|\mathbf{x}_k - \mathbf{x}^*\|^2\right] + \alpha_k^2\beta_k^2\mathbb{E}\left[\|G(\mathbf{x}_k, \mathbf{y}_k) - G(\mathbf{x}^*, \mathbf{1}\bar{\mathbf{x}}^*)\|^2\right] \\
&- 2\alpha_k\beta_k\mathbb{E}\left[(\mathbf{x}_k - \mathbf{x}^*)^\top(G(\mathbf{x}_k, \mathbf{y}_k) - G(\mathbf{x}^*, \mathbf{1}\bar{\mathbf{x}}^*))\right] \\
\leq&\mathbb{E}\left[\|\mathbf{x}_k - \mathbf{x}^*\|^2\right] + 4C^2N\alpha_k^2\beta_k^2 - 2\alpha_k\beta_k\mathbb{E}[(\mathbf{x}_k - \mathbf{x}^*)^\top(G(\mathbf{x}_k, \mathbf{y}_k) - G(\mathbf{x}^*, \mathbf{1}\bar{\mathbf{x}}^*))], \qquad (22)
\end{aligned}$$

where the first inequality holds from the non-expansive property of the projection operation and the last inequality is followed by Assumption 5. For the last term of (22), we have

$$\begin{aligned}
&- 2\alpha_k\beta_k(\mathbf{x}_k - \mathbf{x}^*)^\top(G(\mathbf{x}_k, \mathbf{y}_k) - G(\mathbf{x}^*, \mathbf{1}\bar{\mathbf{x}}^*)) \\
=&- 2\alpha_k\beta_k(\mathbf{x}_k - \mathbf{x}^*)^\top(G(\mathbf{x}_k, \mathbf{y}_k) - G(\mathbf{x}_k, \mathbf{1}\bar{\mathbf{x}}) + G(\mathbf{x}_k, \mathbf{1}\bar{\mathbf{x}}) - G(\mathbf{x}^*, \mathbf{1}\bar{\mathbf{x}}^*)) \\
=&- 2\alpha_k\beta_k(\mathbf{x}_k - \mathbf{x}^*)^\top(G(\mathbf{x}_k, \mathbf{y}_k) - G(\mathbf{x}_k, \mathbf{1}\bar{\mathbf{x}})) - 2\alpha_k\beta_k(\mathbf{x}_k - \mathbf{x}^*)^\top(\Phi(\mathbf{x}_k) - \Phi(\mathbf{x}^*)) \\
\leq&2L_g\alpha_k\beta_k\|\mathbf{x}_k - \mathbf{x}^*\|\|\mathbf{y}_k - \mathbf{1}\bar{\mathbf{x}}_k\| - 2m\alpha_k\beta_k\|\mathbf{x}_k - \mathbf{x}^*\|^2 \qquad (23) \\
\leq&\frac{1}{\nu_2}L_g^2\alpha_k^2\beta_k\|\mathbf{x}_k - \mathbf{x}^*\|^2 + \nu_2\beta_k\|\mathbf{y}_k - \mathbf{1}\bar{\mathbf{x}}_k\|^2,
\end{aligned}$$

From the first two conditions in (9), we can derive that $\lim_{k\to\infty}\alpha_k = 0$. Thus, there exists $k' > 0$ such that $\alpha_{k'} < 1$ and we can only focus on the the sequence $\{\mathbf{x}_k\}_{k\geq k'}$. By combining (22) and (23) , we obtain the following expression:

$$\begin{aligned}
&\|\mathbf{x}_{k+1} - \mathbf{x}^*\|^2 \\
\leq&\|\mathbf{x}_k - \mathbf{x}^*\|^2 + 4C^2N\alpha_k^2\beta_k^2 - 2m\alpha_k\beta_k\|\mathbf{x}_k - \mathbf{x}^*\|^2 + 2L_g\alpha_k\beta_k\|\mathbf{x}_k - \mathbf{x}^*\|\|\mathbf{y}_k - \mathbf{1}\bar{\mathbf{x}}_k\| \\
\leq&\|\mathbf{x}_k - \mathbf{x}^*\|^2 + 4C^2N\alpha_k^2\beta_k^2 - 2m\alpha_k\beta_k\|\mathbf{x}_k - \mathbf{x}^*\|^2 + \frac{1}{\nu}L_g^2\alpha_k^2\beta_k^2\|\mathbf{x}_k - \mathbf{x}^*\|^2 + \nu\|\mathbf{y}_k - \mathbf{1}\bar{\mathbf{x}}_k\|^2,
\end{aligned}$$

where the last inequality holds from Young's inequality. By letting $\nu = \frac{L_g^2\alpha_k\beta_k}{m}$, we further get

$$\begin{aligned}
&\|\mathbf{x}_{k+1} - \mathbf{x}^*\|^2 \\
\leq&\|\mathbf{x}_k - \mathbf{x}^*\|^2 + 4C^2N\alpha_k^2\beta_k^2 - m\alpha_k\beta_k\|\mathbf{x}_k - \mathbf{x}^*\|^2 + \frac{L_g^2\alpha_k\beta_k}{m}\|\mathbf{y}_k - \mathbf{1}\bar{\mathbf{x}}_k\|^2. \qquad (24)
\end{aligned}$$

Taking expectation and summing both side of (24) from $k = k'$ to T, we have the following relationship:

$$\begin{aligned}&\sum_{k=k'}^{T} m\alpha_k\beta_k\mathbb{E}\left[\|\mathbf{x}_k-\mathbf{x}^*\|^2\right]\\ \leq&\|\mathbf{x}_0-\mathbf{x}^*\|^2-\mathbb{E}\left[\|\mathbf{x}_{T+1}-\mathbf{x}^*\|^2\right]+4C^2N\sum_{k=k'}^{T}\alpha_k^2\beta_k^2+\frac{L_g^2}{m}\sum_{k=k'}^{T}\alpha_k\beta_k\mathbb{E}\left[\|\mathbf{y}_k-\mathbf{1}\bar{\mathbf{x}}_k\|^2\right].\end{aligned}\tag{25}$$

When $T\to\infty$, $4C^2N\sum_{k=k'}^{T}\alpha_k^2\beta_k^2$ is bounded and $\|\mathbf{x}_{T+1}-\mathbf{x}^*\|^2$ is bounded due to the bounded constraint. Moreover, $\sum_{k=k'}^{\infty}\alpha_k\beta_k\mathbb{E}\left[\|\mathbf{y}_k-\mathbf{1}\bar{\mathbf{x}}_k\|^2\right]\leq\sum_{k=k'}^{\infty}\beta_k\mathbb{E}\left[\|\mathbf{y}_k-\mathbf{1}\bar{\mathbf{x}}_k\|^2\right]<\infty$ by Lemma 1. Therefore, the right-hand side of (25) is always bounded when $T\to\infty$. With $\sum_{k=k'}^{\infty}\alpha_k\beta_k=\infty$, we can conclude that $\mathbb{E}\left[\|\mathbf{x}_k-\mathbf{x}^*\|^2\right]$ converges to zero.

D. Proof of Corollary 1

If ω_1 and ω_2 satisfy the conditions in Corollary 1, then α_k and β_k will satisfy the conditions in Theorem 1 to ensure that $\mathbb{E}\left[\|\mathbf{x}_k-\mathbf{x}^*\|^2\right]$ converges to zero. According to (20), we have the following relationship when k is large enough:

$$\mathbb{E}\left[\|\mathbf{y}_{k+1}\|^2\right]\leq(1-\beta_k\lambda_2)\mathbb{E}\left[\|\mathbf{y}_k\|^2\right]+\eta_k,$$

where $\eta_k=\frac{c_4}{(c_2k+1)^{\omega_3}}$ for some $c_4>0$ and $\omega_3=\min\{2\omega_1+\omega_2,2\omega_2\}$. Therefore, we have

$$\lim_{k\to\infty}(k+1)^{\omega_4}\mathbb{E}\left[\|\mathbf{y}_k\|^2\right]=0\tag{26}$$

based on Lemma 5, where $0\leq\omega_4<\omega_3-\omega_2$.

Based on (25) and (18), we have

$$\frac{\sum_{k=0}^{T}m\alpha_k\beta_k\mathbb{E}\left[\|\mathbf{x}_k-\mathbf{x}^*\|^2\right]}{\sum_{k=0}^{T}\alpha_k\beta_k}\tag{27}$$

$$\begin{aligned}\leq&\frac{\|\mathbf{x}_0-\mathbf{x}^*\|^2-\mathbb{E}\left[\|\mathbf{x}_{T+1}-\mathbf{x}^*\|^2\right]}{\sum_{k=0}^{T}\alpha_k\beta_k}+\frac{4C^2N\sum_{k=0}^{T}\alpha_k^2\beta_k^2}{\sum_{k=0}^{T}\alpha_k\beta_k}\\&+\frac{\frac{\bar{L}^2}{m}\sum_{k=0}^{T}\alpha_k\beta_k\mathbb{E}\left[\|\mathbf{y}_k\|^2\right]}{\sum_{k=0}^{T}\alpha_k\beta_k}.\end{aligned}\tag{28}$$

Equation (26) indicates that $\mathbb{E}\left[\|\mathbf{y}_k\|^2\right]$ is in the same order of α_k^2 or β_k, and thus, the third term of (28) converges to zero with a rate $O\left(\frac{1}{(T+1)^{\omega}}\right)$, where $\omega=\min\{2\omega_1,\omega_2\}$. Moreover, the second term of (28) converges to zero with a rate $O\left(\frac{1}{(T+1)^{\omega_1+\omega_2}}\right)$. Since $\omega_1+\omega_2>\omega$, (27) will decay with a rate ω.

E. Proof of Theorem 2

It can be easily inferred that $\mathbb{E}[\mathcal{C}(x)] = x$ and $\mathbb{E}\left[\|\mathcal{C}(x) - x\|^2\right] \leq \frac{\theta^2}{4}$, fulfilling the requirements of Assumption 6. Furthermore, $\sum_{k=0}^{\infty} \frac{c_4}{c_5 k+1} = \infty$ satisfies the first condition in (9). Thus, this stochastic compressor enables convergence accuracy when the step sizes satisfy other conditions in (9).

From Algorithm 1, it can be seen that given initial state $\{\mathbf{x}_0, \mathbf{y}_0\}$, the network topology W and the function set $\mathcal{F}$, the observation sequence $\{\mathcal{O}_k\}_{k\geq 0}$ is uniquely determined by the compression scheme. For any pair of adjacent objective function sets $\{\mathcal{F}\}$ and $\{\mathcal{F}'\}$, the eavesdropper is assumed to know the initial states of the algorithm. Thus, $\mathbf{x}_0 = \mathbf{x}'_0$ and $\mathbf{y}_0 = \mathbf{y}'_0$ based on the same observation. Furthermore, the two function sets generate the same outputs, i.e., $\mathcal{C}(y_{i,k})$ and $\mathcal{C}(y'_{i,k})$ for all $i \in \mathcal{N}$. The compression errors are independently and identically distributed. Similarly to the nosie-based privacy analysis [4], we can conclude that $x_{i,k} = x'_{i,k}$ and $y_{i,k} = y'_{i,k}$ for $i \neq i_0$ and for all non-negative k. According to (6), we have the following relation for i_0:

$$\begin{aligned} y_{i_0,k+1} =& y_{i_0,k} + \beta_k \sum_{j\in\mathcal{N}_i} w_{i,j}(\mathcal{C}(y_{j,k}) - \mathcal{C}(y_{i_0,k})) - \alpha_k\beta_k g_{i_0,k}, \\ y'_{i_0,k+1} =& y'_{i_0,k} + \beta_k \sum_{j\in\mathcal{N}_i} w_{i,j}(\mathcal{C}(y'_{j,k}) - \mathcal{C}(y'_{i_0,k})) - \alpha_k\beta_k g'_{i_0,k}. \end{aligned}$$

Therefore, we have

$$\Delta y_{i_0,k+1} = y_{i_0,k+1} - y'_{i_0,k+1} = \Delta y_{i_0,k} - \alpha_k\beta_k \Delta g_{i_0,k},$$

where $\Delta g_{i_0,k} = g_{i_0,k} - g'_{i_0,k}$. Since $\Delta y_{i_0,0} = 0$, there is

$$\|\Delta y_{i_0,k}\| \leq \sum_{s=0}^{k-1} \alpha_s\beta_s \|\Delta g_{i_0,s}\| \leq 2C \sum_{s=0}^{k-1} \alpha_s\beta_s \leq \frac{2Cc_4}{c_5} \ln(c_5 k + 1). \tag{29}$$

Without generality, suppose the attacker's observation at k for $y_{i(j)}, y'_{i(j)}$ is $l\theta$. Similar to the proof of Theorem 3 in Wang and Başar [5], we can obtain that $\delta_k = \mathbb{P}[\mathcal{C}(y_{i(j)}) = l\theta | y_i] - \mathbb{P}[\mathcal{C}(y'_{i(j)}) = l\theta | y'_i] \leq \frac{\|\Delta y_{i_0,k}\|_1}{\theta}$ depends on $\|\Delta y_{i_0,k}\|_1$. Due to the same observation, there is $|\Delta y_{i_0(j),k}| \leq 2\theta$ from Fig. 1 and $\|\Delta y_{i_0,k}\|_1 = \sum_{j=1}^{n} |\Delta y_{i_0(j),k}| \leq 2n\theta$. Additionally, according to (29), we have $\|\Delta y_{i_0,k}\|_1 \leq \sqrt{n}\|\Delta y_{i_0,k}\| \leq \frac{2Cc_4\sqrt{n}}{c_5} \ln(c_5 k + 1)$. Moreover, it should be noted that in DP, δ_k should be a small parameter in $(0, 1)$. Hence, we derive the expression of δ_k shown in (12).

$$\delta_k \leq \frac{\|\Delta y_{i_0,k}\|_1}{\theta} \leq \min\left\{1, \frac{2Cc_4\sqrt{n}}{c_5\theta} \ln(c_5 k + 1)\right\}.$$

REFERENCES

[1] H. Robbins and D. Siegmund, "A convergence theorem for nonnegative almost supermartingales and some applications," in *Optimizing methods in statistics*. Elsevier, 1971, pp. 233–257.

[2] S. Kar and J. M. Moura, "Convergence rate analysis of distributed gossip (linear parameter) estimation: Fundamental limits and tradeoffs," *IEEE Journal of Selected Topics in Signal Processing*, vol. 5, no. 4, pp. 674–690, 2011.

[3] S. Kar, J. M. Moura, and H. V. Poor, "Distributed linear parameter estimation: Asymptotically efficient adaptive strategies," *SIAM Journal on Control and Optimization*, vol. 51, no. 3, pp. 2200–2229, 2013.

[4] M. Ye, G. Hu, L. Xie, and S. Xu, "Differentially private distributed Nash equilibrium seeking for aggregative games," *IEEE Transactions on Automatic Control*, vol. 67, no. 5, pp. 2451–2458, 2021.

[5] Y. Wang and T. Başar, "Quantization enabled privacy protection in decentralized stochastic optimization," *IEEE Transactions on Automatic Control*, 2022.