Supplementary Material of "Implementing Distributed Dynamical Systems over Encrypted Data using Secure Multi-party Computation"

Seungjoon Lee, Junsoo Kim, and Hyungbo Shim*

April 1, 2020

Abstract

This article is a supplementary material for the submitted paper [1].

1 Derivation of Main Results of [1]

1.1 Auxiliary Lemmas

First, two auxiliary lemmas used for the proof of main results are introduced. Following lemma states the ultimate bounds of the linear system. Proof uses elementary techniques from linear system theory and hence omitted.

Lemma 2. *Consider the discrete-time linear system given by*

$$x[k+1] = Ax[k] + d[k]$$

where $A \in \mathbb{R}^{N\times N}$ and $d[k]$ is the disturbance. Suppose that $A = T\Lambda T^{-1}$ is Schur stable where $T \in \mathbb{R}^{N\times N}$ and $\Lambda \in \mathbb{C}^{N\times N}$ is a diagonal matrix. Also assume that the disturbance is uniformly bounded, i.e., $|d[k]|_\infty < D$ for all $k \geq 0$. Then for all $k \geq 0$, it holds that

$$\begin{aligned} |x[k]|_\infty &\leq \kappa|\lambda|^{k+1}|x[0]|_\infty + \frac{D}{1-|\lambda|} \\ &< \kappa|x[0]|_\infty + \frac{D}{1-|\lambda|}, \end{aligned}$$

where $\kappa := |T|_\infty \cdot |T^{-1}|_\infty$ and $\lambda \in \mathbb{C}$ is the eigenvalue of A with the largest modulus. ◊

Next, consider the discretized solution to the economic dispatch problem [1, Equation (6)]

$$\lambda[k+1] = W\lambda[k] + \epsilon h(\lambda[k]) \tag{S–1}$$

and its quantized version [1, Equation (7)]

$$\lambda^{\mathrm{q}}[k+1] = W\lambda^{\mathrm{q}}[k] + \epsilon h(\lambda^{\mathrm{q}}[k]) + \Delta[k], \tag{S–2a}$$

$$y_i^{\mathrm{q}}[k] = \hat{x}_i^{\mathrm{q}}(\lambda_i^{\mathrm{q}}[k]), \tag{S–2b}$$

*S. Lee, J. Kim, and H. Shim are with ASRI, Department of Electrical and Computer Engineering, Seoul National University, Seoul, Korea. `seungjoon.lee@cdsl.kr, kjs9044@cdsl.kr, hshim@snu.ac.kr`

where the quantization error can be written as

$$\Delta[k] := \lfloor W^{\mathrm{q}}\lambda^{\mathrm{q}}[k]\rfloor_r - W\lambda^{\mathrm{q}}[k] + \lfloor \epsilon^{\mathrm{q}} h^{\mathrm{q}}(\lambda^{\mathrm{q}}[k])\rfloor_r - \epsilon h(\lambda^{\mathrm{q}}[k]).$$

For the analysis, consider the discretized solution for the EDP (S–1) under small perturbation given by

$$\lambda[k+1] = W\lambda[k] + \epsilon h(\lambda[k]) + \beta[k] \tag{S–3}$$

where $\beta[k] := [\beta_1[k]; \cdots ; \beta_N[k]] \in \mathbb{R}^N$ is perturbation. Then, uniform boundedness of (S–3) can be shown as below.

Lemma 3. *Consider the system* (S–3) *and suppose that Assumptions 2 and 3 of [1] hold (i.e., feasibility of the optimization problem and connectedness of the communication network). Also assume that* $|\lambda_i[0]| \le M$ *where* $M := \max_{i=1,\dots,N}(|v_i(\underline{x}_i)|, |v_i(\bar{x}_i)|)$ *and let* $\epsilon > 0$ *be a fixed number. Then for any* $0 < \rho < \gamma\epsilon/N$*, if* $\beta[k]$ *satisfies*

$$|\beta[k]|_\infty \le \rho, \quad \forall k \ge 0,$$

then $\lambda[k]$ *is uniformly bounded. Specifically,* $\lambda[k]$ *satisfies*

$$|\lambda[k]|_\infty \le B_\lambda + \eta(\rho), \quad \forall k \ge 0,$$

where B_λ *is a positive constant and* $\eta(\cdot)$ *is a class-*$\mathcal{K}_\infty$ *function.* $\Diamond$

Proof. Since W is a symmetric and doubly stochastic matrix, recall that there exist a matrix $T := [(1/N)1_N^\top; R^\top] \in \mathbb{R}^{N\times N}$ and $T^{-1} = [1_N \ Q]$ such that $TWT^{-1} = \mathrm{diag}(0, \sigma_2(W), \dots, \sigma_N(W))$. Then, define the state transformation as

$$\xi := \begin{bmatrix} \bar{\xi} \\ \tilde{\xi} \end{bmatrix} = T\lambda = \begin{bmatrix} \frac{1}{N}1_N^\top\lambda \\ R^\top\lambda \end{bmatrix},$$

where $\bar{\xi} \in \mathbb{R}$ and $\tilde{\xi} \in \mathbb{R}^{N-1}$. Then it follows that

$$\bar{\xi}[k+1] = \bar{\xi}[k] + \frac{\epsilon}{N}\sum_{i=1}^{N} h_i(\bar{\xi}[k]) + \bar{e}(\bar{\xi}, \tilde{\xi}, k), \tag{S–4a}$$

$$\tilde{\xi}[k+1] = \Lambda\tilde{\xi}[k] + \tilde{e}(\bar{\xi}, \tilde{\xi}, k), \tag{S–4b}$$

where $\bar{e}$ and $\tilde{e}$ are defined as

$$\bar{e}(\bar{\xi}, \tilde{\xi}, k) := \frac{1}{N}\sum_{i=1}^{N}\beta_i[k] + \epsilon\Big(h_i(\bar{\xi}[k]) - h_i(\bar{\xi}[k] + Q_i\tilde{\xi}[k])\Big),$$
$$\tilde{e}(\bar{\xi}, \tilde{\xi}, k) := \epsilon R^T h(1_N\bar{\xi}[k] + Q\tilde{\xi}[k]) + R^T\beta[k].$$

In order to show the boundedness of $\tilde{\xi}[k]$ notice that

$$|\tilde{e}(\bar{\xi}, \tilde{\xi}, k)|_\infty \le \epsilon|R|_\infty c + |R|_\infty|\beta[k]|_\infty = \epsilon\cdot c + \rho =: \tilde{e}_\infty,$$

where $c := \max_{i=1,\dots,N}|d_i - \hat{x}_i(\lambda_i[k])|$, which exists since $\hat{x}_i(\cdot)$ is a bounded function. Therefore, it follows from Lemma 2 that $\tilde{\xi}[k]$ satisfies

$$\begin{aligned} |\tilde{\xi}[k+1]|_\infty &\le \lambda_{N-1}(W)^{k+1}|\tilde{\xi}[0]|_\infty + \frac{\tilde{e}_\infty}{1-\sigma_{N-1}(W)} \\ &< M + \frac{\tilde{e}_\infty}{1-\sigma_{N-1}(W)} \\ &=: B_{\tilde{\xi}}, \end{aligned}$$

where we used $|R^\top|_\infty = 1$. Moreover, for any $U_{\tilde{\xi}} > \tilde{e}_\infty/(1-\sigma_{N-1}(W))$, there exists $T_1 > 0$ such that

$$|\tilde{\xi}[k+1]|_\infty \le U_{\tilde{\xi}}, \quad \forall T > T_1 \tag{S–5}$$

where T_1 is given by

$$T_1 := \frac{\ln(U_{\tilde{\xi}} - \frac{\tilde{e}_\infty}{1-\sigma_{N-1}(W)}) - \ln(|\tilde{\xi}(0)|_\infty)}{\ln(\sigma_{N-1}(W))}$$

if $|\tilde{\xi}(0)|_\infty > U_{\tilde{\xi}}$ and $T_1 = 1$ otherwise.

For the boundedness of $\bar{\xi}[k]$, let $B_{\bar{\xi}} := M + NB_{\tilde{\xi}}$. Then, it can be verified that

$$h_i(\bar{\xi}[k]) - h_i(\bar{\xi}[k] + Q_i\tilde{\xi}[k]) = 0, \quad \forall |\bar{\xi}[k]| > B_{\bar{\xi}}.$$

Hence, it holds that

$$|\bar{e}(\bar{\xi}, \tilde{\xi}, k)| \le \rho, \quad \forall |\bar{\xi}[k]| > B_{\bar{\xi}}.$$

Also note if $\bar{\xi}[k] > B_{\bar{\xi}}$, then it follows from the definition of $h_i(\cdot)$ that

$$\sum_{i=1}^N h_i(\bar{\xi}[k]) = \sum_{i=1}^N d_i - \bar{x}_i < -\gamma,$$

where the last inequality is due to Assumption 1 of [1]. Similar inequality also holds if $\bar{\xi}[k] < -B_{\bar{\xi}}$. Hence, $\bar{\xi}$ is bounded if $-\gamma\epsilon/N + \rho < 0$, which is equivalent to $\rho < \gamma\epsilon/N$. Finally, bounds of $\lambda[k]$ can be obtained as

$$\begin{aligned}
|\lambda[k]|_\infty &\le |1_N|_\infty |\bar{\xi}|_\infty + |Q|_\infty |\tilde{\xi}|_\infty \\
&= |\bar{\xi}|_\infty + N|\tilde{\xi}|_\infty \\
&\le B_{\bar{\xi}} + NB_{\tilde{\xi}} \\
&= M + NB_{\tilde{\xi}} + NB_{\tilde{\xi}} \\
&= M + 2N\left(M + \frac{\tilde{e}_\infty}{1-\sigma_{N-1}(W)}\right) \\
&= M + 2N\left(M + \frac{\epsilon c + \rho}{1-\sigma_{N-1}(W)}\right) \\
&= \left((2N+1)M + \frac{2N\epsilon c}{1-\sigma_{N-1}(W)}\right) + \frac{2N}{1-\sigma_{N-1}(W)}\rho \\
&=: B_\lambda + \eta(\rho)
\end{aligned}$$

for all $k \ge 0$, where we used $|R|_\infty = 1$ and $|Q|_\infty = N$. This completes the proof. □

1.2 Proof of Lemma 1 of [1]

First, it can be verified that there exists a function $q(r, |\lambda^{\mathrm{q}}[k]|_\infty)$ such that the quantization error $\Delta[k]$ satisfies

$$|\Delta[k]|_\infty \le q(r, |\lambda^{\mathrm{q}}[k]|_\infty), \quad \forall k \ge 0, \tag{S–6}$$

where $q(r, |\lambda^{\mathrm{q}}[k]|_\infty)$ is a class-$\mathcal{K}$ function in the first argument and non-decreasing in the second argument.

Now, define $\alpha(r) := q(r, B_\lambda + \eta(\epsilon\gamma/N))$ and choose r sufficiently small such that

$$\alpha(r) = q(r, B_\lambda + \eta(\epsilon\gamma/N)) < \epsilon\gamma/N, \tag{S–7}$$

where $\eta(\cdot)$ corresponds to the one defined in Lemma 3.

Rest of the proof is done by induction. For $k = 0$, we have $|\lambda_i^{\mathrm{q}}[0]| \leq M < B_\lambda$ and hence $|\Delta[0]| \leq q(r, B_\lambda + \eta(\epsilon\gamma/N)) < \epsilon\gamma/N$. Since the distributed algorithm is causal, applying Lemma 3 with $\beta[k] = \Delta[k]$ implies $|\lambda_i^{\mathrm{q}}[1]| \leq B_\lambda + \eta(\epsilon\gamma/N)$. Hence, it follows from (S–6) that $|\Delta[1]| \leq \epsilon\gamma/N$.

Next, suppose that $|\Delta[k]| \leq \epsilon\gamma/N$ for all $k = 0, \dots, T$. Then, it follows from Lemma 3 and causality that $|\lambda_i^{\mathrm{q}}[T+1]| \leq B_\lambda + \epsilon\gamma/N$ and that $|\Delta_i[T+1]| \leq \epsilon\gamma/N$. Hence, this implies $\lambda_i^{\mathrm{q}}[k]$ satisfies

$$|\lambda_i^{\mathrm{q}}[k]| \leq B_\lambda + \eta(\epsilon\gamma/N) =: B^{\mathrm{q}}, \quad \forall k \geq 0.$$

Therefore, it also follows that

$$|\Delta[k]|_\infty \leq q(r, |\lambda^{\mathrm{q}}[k]|_\infty) \leq q(r, B^{\mathrm{q}}) = \alpha(r), \quad \forall k \geq 0.$$

This concludes the proof.

1.3 Proof of Theorem 1 of [1]

The proof is motivated by [2] which analyzed the continuous-time algorithm. Define the set $\Lambda^*(z) := \{\lambda \in \mathbb{R} \mid |\sum_{i=1}^N h_i(\lambda)| < z\}$ and suppose the quantized algorithm (S–2) is transformed as in (S–4). We claim there exists $\epsilon > 0$ and $r > 0$ such that $\bar{\xi}[k]$ converges to the set $\Lambda^*(\theta)$ given a constant $\theta > 0$ (bounds for θ is determined at the end of the proof). First, suppose that $r < r_1^*$ where r_1^* is a sufficiently small constant such that the results of Lemma 1 of [1] hold. Then, we have

$$\frac{1}{N}\sum_{i=1}^N |\Delta[k]| + \epsilon \left| h_i(\bar{\xi}[k]) - h_i(\bar{\xi}[k] + Q_i\tilde{\xi}[k]) \right| \leq \alpha(r) + \frac{\epsilon}{N}\sum_{i=1}^N \bar{L}|Q_i||\tilde{\xi}[k]|, \quad \forall k \geq 0,$$

where $\bar{L} := \max_{i=1,\dots,N} L_i$ and L_i is the Lipschitz constants of h_i. For simplicity, we only consider the case when $\bar{\xi}[k] > 0$. Suppose that $k > T_1$ and $\bar{\xi}[k]$ is on the right of the set $\Lambda^*(\theta/2)$, then the dynamics of $\bar{\xi}[k]$ satisfies

$$\begin{aligned}
\bar{\xi}[k+1] - \bar{\xi}[k] &= \frac{\epsilon}{N}\sum_{i=1}^N h_i(\bar{\xi}[k]) + \frac{1}{N}\sum_{i=1}^N \Delta[k] + \epsilon\Big(h_i(\bar{\xi}[k]) - h_i(\bar{\xi}[k] + Q_i\tilde{\xi}[k])\Big), \\
&\leq -\frac{\epsilon}{N}\frac{\theta}{2} + \alpha(r) + \epsilon\bar{L}\sqrt{N}U_{\tilde{\xi}} \\
&= -\frac{\epsilon}{N}\frac{\theta}{2} + \alpha(r) + \epsilon\bar{L}\sqrt{N}\cdot 2\frac{\epsilon c + \alpha(r)}{1 - \sigma_{N-1}(W)}
\end{aligned} \tag{S–8}$$

where we use $U_{\tilde{\xi}} = 2\tilde{e}_\infty/(1 - \sigma_{N-1}(W))$. Hence, $1 > \epsilon > 0$ and $r > 0$ can be chosen sufficiently small such that

$$\begin{aligned}
-\frac{\epsilon}{N}\frac{\theta}{2} + \alpha(r) + \epsilon\bar{L}\sqrt{N}2\frac{\epsilon c + \alpha(r)}{1 - \sigma_{N-1}(W)} &= \epsilon\left[-\frac{1}{N}\frac{\theta}{2} + \frac{2\epsilon c\bar{L}\sqrt{N}}{1 - \sigma_{N-1}(W)}\right] + \alpha(r)\left[1 + \frac{2\epsilon\bar{L}\sqrt{N}}{1 - \sigma_{N-1}(W)}\right] \\
&< -\frac{1}{4}\frac{\epsilon\theta}{N}.
\end{aligned} \tag{S–9}$$

Specifically, choose $0 < \epsilon < 1$ and $0 < r < r_2^*$ such that

$$\epsilon^2\frac{2c\bar{L}\sqrt{N}}{1 - \sigma_{N-1}(W)} < \frac{\epsilon\theta}{8N}, \quad \alpha(r)\left[1 + \frac{2\bar{L}\sqrt{N}}{1 - \sigma_{N-1}(W)}\right] < \frac{\epsilon\theta}{8N}, \tag{S–10}$$

where r_2^* is such that $\alpha(r_2^*) < 1$. Hence, let $r < \min(r_1^*, r_2^*)$ such that the result of Lemma 1 of [1] hold as supposed at the start of the proof.

The inequality implies that $\bar{\xi}[k]$ converges to the set $\Lambda^*(\theta/2)$ with speed of at least $-\epsilon\theta/(4N)$ if $\bar{\xi}[k]$ is on the right side of $\Lambda^*(\theta/2)$. Also notice that if $\bar{\xi}[k] \in \Lambda^*(\theta/2)$, it holds that

$$|\bar{\xi}[k+1]|_{\Lambda^*(\theta/2)} \leq \left| \xi[k] + \frac{\epsilon}{N}\frac{\theta}{2} + \alpha(r) + \epsilon \bar{L}\sqrt{N} \cdot 2\frac{\epsilon c + \alpha(r)}{1-\sigma_{N-1}(W)} \right|_{\Lambda^*(\theta/2)} \leq \frac{\theta}{2} + \frac{\epsilon\theta}{2} \leq \theta. \tag{S–11}$$

The first inequality of (S–11) follows from the dynamics of $\bar{\xi}$. The second inequality of (S–11) is obtained by using the inequality (S–10), fact that $(\epsilon/N)|\sum_{i=1}^N h_i(\bar{\xi}[k])| \leq \epsilon\theta/2$ since $\bar{\xi}[k] \in \Lambda^*(\theta/2)$, and since $\bar{\xi}[k]$ is on the right of the set $\Lambda^*(\theta/2)$. Finally, the last inequality of (S–11) holds since $\epsilon < 1$. In conclusion, we obtain $\bar{\xi}[k] \in \Lambda^*(\theta)$ for all $k > T_1 + T_2$ where

$$T_2 := \frac{8B^{\mathrm{q}}}{\epsilon\theta} > |\bar{\xi}[T_1]|_{\Lambda^*} \cdot \left(\frac{1}{4}\epsilon\theta\right)^{-1}.$$

The distance to the optimal solution can be bounded as

$$|h_i(\lambda_i^{\mathrm{q}}[k]) - h_i(\lambda^*)| \leq \sum_{j=1}^N |h_j(\lambda_i^{\mathrm{q}}[k]) - h_j(\lambda^*)| = \left|\sum_{j=1}^N h_j(\lambda_i^{\mathrm{q}}[k]) - h_j(\lambda^*)\right| = \left|\sum_{j=1}^N h_j(\lambda_i^{\mathrm{q}}[k])\right| \leq \theta$$

for all $k > T_1 + T_2$. Since $h_i(\lambda^*) = d_i - x_i^*$, it follows that

$$|x_i^{\mathrm{q}}(\lambda_i^{\mathrm{q}}[k]) - x_i^*| \leq |x_i^{\mathrm{q}}(\lambda_i^{\mathrm{q}}[k]) - x_i(\lambda_i^{\mathrm{q}}[k])| + |x_i(\lambda_i^{\mathrm{q}}[k]) - x_i^*|.$$

Hence, choose r sufficiently small such that $|x_i^{\mathrm{q}}(z) - x_i(z)| < \theta$ for all $|z| \leq B^{\mathrm{q}}$. Then, we obtain

$$|x_i^{\mathrm{q}}(\lambda_i^{\mathrm{q}}[k]) - x_i(\lambda_i^{\mathrm{q}}[k])| + |x_i(\lambda_i^{\mathrm{q}}[k]) - x_i^*| \leq 2\theta, \quad \forall k > T_1 + T_2.$$

Finally, to show constraint violation is bounded, note

$$\left|\sum_{i=1}^N d_i - x_i^{\mathrm{q}}(\lambda_i^{\mathrm{q}}[k])\right| = \left|\sum_{i=1}^N d_i - x_i^{\mathrm{q}}(\lambda_i^{\mathrm{q}}[k]) \pm x_i^*\right| \leq \sum_{i=1}^N |x_i^* - x_i^{\mathrm{q}}(\lambda_i^{\mathrm{q}}[k])| = 2N\theta, \quad \forall k > T_1 + T_2.$$

Finally, choose θ such that $\max(2\theta, 2N\theta) = 2N\theta < \delta$ to obtain the desired result. ■

References

[1] S. Lee, J. Kim, and H. Shim, "Implementing Distributed Dynamical Systems over Encrypted Data using Secure Multi-party Computation", submitted to CDC 2020.

[2] H. Yun, H. Shim, and H. S. Ahn, "Initialization-free privacy guaranteed distributed algorithm for economic dispatch problem," *Automatica*, vol. 102, pp. 86–93, 2019.