Supplementary Material for “Lightweight Privacy-Preserving Charging Coordination of Electric Vehicles via Mixed Encryption Communication”

Zhe Zhou, Jiawei Xie, Zhengshuo Li, Xue Li, Shengqi Zhang and Haochen Wu

In the supplementary material, we give the Paillier cryptosystem, the formulation of the event-triggered condition, and the convergence analysis of system-level charging electricity prices for electric vehicles, as discussed in the paper “Lightweight Privacy-Preserving Charging Coordination of Electric Vehicles via Mixed Encryption Communication.”

I. Paillier Cryptosystem

The Paillier cryptosystem, outlined in Algorithm 1, has homomorphic properties, which are shown in the following lemma.

Lemma 1 (Homomorphic Property of Paillier Encryption). *Let m_1 and m_2 be two plaintexts, and $E(m_1)$ and $E(m_2)$ be their corresponding ciphertexts under Paillier encryption. The Paillier encryption scheme possesses the following homomorphic property: $E_{enc}(m_1) \cdot E_{enc}(m_2) = E_{enc}(m_1 + m_2)$ and $E_{enc}(m)^r = E_{enc}(rm)$ for any plaintext m_1, m_2 and m, and positive integer r.*

Remark. *Since the Paillier encryption only works with unsigned integers, any floating-point numbers representing analog signals in practical applications must be converted to their corresponding integer values via quantization. In this paper, we utilize the quantizer described in [S1] without extensive analysis, disregarding quantization errors by appropriately configuring its parameters.*

Algorithm 1 Paillier Cryptosystem

Key Generation (K_p, K_s):
Step 1: Choose two different large prime numbers p_P and q_P such that $\gcd(p_P \cdot q_P, (p_P - 1)(q_P - 1)) = 1$.
Step 2: Compute $n_P = p_P \cdot q_P$ and $\lambda_P = \mathrm{lcm}(p_P - 1, q_P - 1)$.
Step 3: Let g_P be a random selection from $\mathbb{Z}^*_{n_P^2}$ and verify that $\mu_P = \left(L(g_P^{\lambda_P} \mod n_P^2)\right)^{-1} \mod n_P$, where $L(x) = \frac{x-1}{n_P}$ for $x \in \{x < n_P^2 \mid x \equiv 1 \mod n_P\}$.
Step 4: Generate the public and private keys $K_p = (n_P, g_P)$ and $K_s = (\lambda_P, \mu_P)$, respectively.
Encryption $E_{\text{enc}}(\cdot)$:
Step 1: Pick a random $h_P \in \mathbb{Z}^*_{n_P^2}$.
Step 2: Encrypt the plaintext $m_P \in \mathbb{Z}_{n_P}$ as $E_{\text{enc}}(m_P) = g_P^{m_P} \cdot h_P^{n_P} \mod n_P^2$.
Decryption $D_{\text{dec}}(\cdot)$:
Recover the plaintext from ciphertext $c_P \in \mathbb{Z}^*_{n_P^2}$ using $D_{\text{dec}}(c_P) = L(c_P^{\lambda_P} \mod n_P^2) \cdot \mu_P \mod n_P$.

II. The Setting of Event-triggering Condition for EVs

Proof: According to [S2], we define $\boldsymbol{\varphi} = \{\varphi_1, \varphi_2, \cdots, \varphi_N\}$ as the left eigenvector of matrix Q corresponding to eigenvalue 1, which satisfies $\sum_{i=1}^{N} \varphi_i = 1$ and $\varphi_i > 0$. Moreover, we construct the Lyapunov function as follows:

$$V(l) = \sum_{i=1}^{N} \varphi_i \hat{\lambda}_{i,t}^2(l). \tag{1}$$

In our paper, the electricity price for EV i at iteration $l+1$ is deduced as follow:

$$\hat{\lambda}_{i,t}(l+1) = e_{i,t}(l) + \sum_{j \in \mathcal{N}_i}^{N} q_{ij} \hat{\lambda}_{j,t}^e(l) \tag{2}$$

Based on (2), the difference of $V(l)$ with respect to iteration l is

$$\begin{aligned} \Delta V(l) &= V(l+1) - V(l) \\ &= \sum_{i=1}^{N} \varphi_i \hat{\lambda}_{i,t}^2(l+1) - \sum_{i=1}^{N} \varphi_i \hat{\lambda}_{i,t}^2(l) \\ &= \Delta V_1(l) + \Delta V_2(l). \end{aligned} \tag{3}$$

where

$$\begin{aligned} &\Delta V_1(l) \\ &= \sum_{i=1}^{N} \varphi_i \Big[\sum_{j=1}^{N} q_{ij}^2 (\hat{\lambda}_{j,t}^e(l))^2 - (\hat{\lambda}_{i,t}^e(l))^2 \Big] \\ &\quad + \sum_{i=1}^{N} \varphi_i \Big[\sum_{j=1, j \neq i}^{N} \sum_{k > j, k \neq i}^{N} q_{ij} q_{ik} \Big((\hat{\lambda}_{j,t}^e(l))^2 + (\hat{\lambda}_{k,t}^e(l))^2 \Big) \Big] \\ &\quad + \sum_{i=1}^{N} \varphi_i \Big[\sum_{j=1, j \neq i}^{N} q_{ij} q_{ii} \Big((\hat{\lambda}_{j,t}^e(l))^2 + (\hat{\lambda}_{i,t}^e(l))^2 \Big) \Big] \\ &= \sum_{i=1}^{N} \varphi_i \Big[\sum_{j=1}^{N} q_{ij}^2 (\hat{\lambda}_{j,t}^e(l))^2 - (\hat{\lambda}_{i,t}^e(l))^2 \Big] \\ &\quad + \sum_{i=1}^{N} \varphi_i \Big[\sum_{j=1, j \neq i}^{N} \sum_{k > j, k \neq i}^{N} q_{ij} q_{ik} \Big((\hat{\lambda}_{j,t}^e(l))^2 + (\hat{\lambda}_{k,t}^e(l))^2 \Big) \Big] \\ &\quad + \sum_{i=1}^{N} \varphi_i \Big[\sum_{j<i}^{N} q_{ij} q_{ii} \Big((\hat{\lambda}_{j,t}^e(l))^2 + (\hat{\lambda}_{i,t}^e(l))^2 \Big) \Big] \\ &\quad + \sum_{i=1}^{N} \varphi_i \Big[\sum_{k>i}^{N} q_{ik} q_{ii} \Big((\hat{\lambda}_{k,t}^e(l))^2 + (\hat{\lambda}_{i,t}^e(l))^2 \Big) \Big] \\ &= \sum_{i=1}^{N} \varphi_i \Big[\sum_{j=1}^{N} \sum_{k=1}^{N} q_{ij} q_{ik} (\hat{\lambda}_{j,t}^e(l))^2 - (\hat{\lambda}_{i,t}^e(l))^2 \Big] \\ &= \sum_{j=1}^{N} \varphi_j (\hat{\lambda}_{j,t}^e(l))^2 - \sum_{i=1}^{N} \varphi_i (\hat{\lambda}_{i,t}^e(l))^2 \\ &= 0. \end{aligned} \tag{4}$$

and

$$\Delta V_2(l) = -\sum_{i=1}^{N}\varphi_i\left[\sum_{j=1,j\neq i}^{N} q_{ij}q_{ii}\left(\hat{\lambda}^e_{j,t}(l)-\hat{\lambda}^e_{i,t}(l)\right)^2\right.$$
$$\left.+\sum_{j=1,j\neq i}^{N}\sum_{k>j,k\neq i}^{N} q_{ij}q_{ik}\left(\hat{\lambda}^e_{j,t}(l)-\hat{\lambda}^e_{k,t}(l)\right)\right]^2 \tag{5}$$
$$+2\sum_{i=1}^{N}\varphi_i\left[\sum_{j=1,j\neq i}^{N} q_{ij}e_{i,t}(l)\left(\hat{\lambda}^e_{j,t}(l)-\hat{\lambda}^e_{i,t}(l)\right)\right].$$

According to (4) and (5), $\Delta V(l)$ in (3) can be rewritten as follows:

$$\begin{aligned}\Delta V(l) &= \Delta V_2(l)\\ &\leq -\sum_{i=1}^{N}\varphi_i\Bigg[\sum_{j=1,j\neq i}^{N} q_{ij}q_{ii}\Big(\hat{\lambda}^e_{j,t}(l)-\hat{\lambda}^e_{i,t}(l)\Big)^2\\ &+\sum_{j=1,j\neq i}^{N}\sum_{i>j,k\neq i}^{N} q_{ij}q_{ik}\Big(\hat{\lambda}^e_{j,t}(l)-\hat{\lambda}^e_{k,t}(l)\Big)^2\Bigg]\\ &+\sum_{i=1}^{N}\varphi_i\sum_{j=1,j\neq i}^{N} q_{ij}\left[\frac{1}{\iota_i}e^2_{i,t}(l)+\iota_i\left(\hat{\lambda}^e_{j,t}(l)-\hat{\lambda}^e_{i,t}(l)\right)^2\right]\\ &= \Delta V_3(l)+\Delta V_4(l).\end{aligned} \tag{6}$$

where ι_i is a constant and designed later, and

$$\begin{aligned}\Delta V_3(l) &= -\sum_{i=1}^{N}\varphi_i\left[\sum_{j=1,j\neq i}^{N}\sum_{k>j,k\neq i}^{N} q_{ij}q_{ik}\left(\hat{\lambda}^e_{j,t}(l)-\hat{\lambda}^e_{k,t}(l)\right)^2\right].\\ \Delta V_4(l) &= \sum_{i=1}^{N}\varphi_i\left[\sum_{j=1,j\neq i}^{N}\frac{1-q_{ii}}{\iota_i}e^2_{i,t}(l)\right.\\ &\left.-\sum_{j=1,j\neq i}^{N} q_{ij}\left(q_{ii}-\iota_i\right)\left(\hat{\lambda}^e_{j,t}(l)-\hat{\lambda}^e_{i,t}(l)\right)^2\right].\end{aligned} \tag{7}$$

According to the Lyapunov stability theorem, we must ensure that $\Delta V(l) \leq 0$. As shown in (7), it is clear that $\Delta V_3(l) \leq 0$. Therefore, to guarantee that $\Delta V(l) \leq 0$, we must also ensure that $\Delta V_4(l) \leq 0$. The event-triggering condition is thus established as follows:

$$e^2_{i,t}(l) > \frac{\beta\iota_i\left(q_{ii}-\iota_i\right)\sum_{j=1,j\neq i}^{N} q_{ij}\left(\hat{\lambda}^{\mathrm{e}}_{j,t}(l)-\hat{\lambda}^{\mathrm{e}}_{i,t}(l)\right)^2}{1-q_{ii}}. \tag{8}$$

where λ is a parameter ranging from 0 to 1. By adjusting λ, the event-triggering threshold can be regulated, which in turn controls the frequency of event triggers and ensures consistent convergence. To reduce the communication network burden, we set $\iota_i = q_{ii}/2$ to decrease the number of event triggers triggered. Consequently, the event-triggered condition (9) is obtained.

$$e_{i,t}^2(l) > \frac{\lambda q_{ii}^2 \sum_{j=1,j\neq i}^{N} q_{ij}\left(\hat{\lambda}_{j,t}^e(l) - \hat{\lambda}_{i,t}^e(l)\right)^2}{4\left(1-q_{ij}\right)} \tag{9}$$

■

III. Convergence Analysis of System Charging Electricity Prices for EVs

We now prove that, under the event-triggered condition (9), the individual charging prices of electric vehicles converge to a consensus. This consensus determines the system charging price as $\lambda^{m+1} = \frac{1}{N}\sum_{i=1}^{N}\hat{\lambda}_i(0)$.

Proof: Based on [S3, Theorem 1], the inequality $\Delta V(l) \leqslant \Delta V_3(l) + \Delta V_4(l) \leqslant 0$ holds. By LaSalle's invariance principle, $\hat{\lambda}_{i,t}(l)$ converges to the set $\mathcal{S} = \{\hat{\lambda}_{i,t} \mid \Delta V_3 = 0 \text{ and } \Delta V_4 = 0\}$. This implies $\hat{\lambda}_{i,t} = \hat{\lambda}_{j,t}$ within $\mathcal{S}$. Therefore,

$$\lim_{l\to\infty}\left(\hat{\lambda}_{i,t}(l) - \hat{\lambda}_{j,t}(l)\right) = 0. \tag{10}$$

indicating that all EVs reach consensus under the event-triggered condition (9).

Let $\Gamma(l) = \sum_{i=1}^{N}\varphi_i\hat{\lambda}_{i,t}(l)$, we draw a conclusion that

$$\begin{aligned}
\Delta\Gamma(l) &= \Gamma(l+1) - \Gamma(l) \\
&= \sum_{i=1}^{N}\varphi_i\left(\hat{\lambda}_{i,t}(l+1) - \hat{\lambda}_{i,t}(l)\right) \\
&= \sum_{i=1}^{N}\varphi_i\sum_{j=1}^{N}q_{ij}\left(\hat{\lambda}_{j,t}^e(l) - \hat{\lambda}_{i,t}^e(l)\right) \\
&= \sum_{i=1}^{N}\varphi_i\sum_{j=1}^{N}q_{ij}\hat{\lambda}_{j,t}^e(l) - \sum_{i=1}^{N}\varphi_i\sum_{j=1}^{N}q_{ij}\hat{\lambda}_{i,t}^e(l) \\
&= \sum_{i=1}^{N}\varphi_j\hat{\lambda}_{j,t}^e(l) - \sum_{i=1}^{N}\varphi_i\hat{\lambda}_{i,t}^e(l) \\
&= 0.
\end{aligned} \tag{11}$$

It can be observed that for all alternating cycles l, $\Gamma(l)$ remains constant, with $\Gamma(l) = \Gamma(0) = \sum_{i=1}^{N}\varphi_i\hat{\lambda}_{i,t}(0)$. This implies that in set S, $\hat{\lambda}_{i,t} = \hat{\lambda}_{j,t} = \frac{\sum_{i=1}^{N}\varphi_i\hat{\lambda}_{i,t}(0)}{\sum_{i=1}^{N}\varphi_i}$. Since the graph G is balanced, and according to [S4], we have $\varphi_i = \frac{1}{N}$. Further derivation gives $\lim_{l\to\infty}\hat{\lambda}_{i,t}(l) = \frac{1}{N}\sum_{i=1}^{N}\hat{\lambda}_{i,t}(0)$. Therefore, the system's average electricity price is $\frac{1}{N}\sum_{i=1}^{N}\hat{\lambda}_i(0)$.

■

References

[S1] M. Ruan, H. Gao, and Y. Wang, "Secure and privacy-preserving consensus," *IEEE Transactions on Automatic Control*, vol. 64, no. 10, pp. 4035–4049, 2019.

[S2] R. A. Horn and C. R. Johnson, *Matrix analysis*. Cambridge university press, 2012.

[S3] Z.-G. Wu, Y. Xu, R. Lu, Y. Wu, and T. Huang, "Event-triggered control for consensus of multiagent systems with fixed/switching topologies," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 48, no. 10, pp. 1736–1746, 2017.

[S4] R. Olfati-Saber, J. A. Fax, and R. M. Murray, "Consensus and cooperation in networked multi-agent systems," *Proceedings of the IEEE*, vol. 95, no. 1, pp. 215–233, 2007.