Privacy-Preserving Flexibility Evaluation via Distributed Energy Resource Aggregation

Zhao Yang, Xiaoting Wang, and Ryan Yunwei Li
Department of Electrical and Computer Engineering, *University of Alberta*
Edmonton, AB, Canada
{zyang21, xiaotin5, yunwei.li}@ualberta.ca

***Abstract*—The rapid proliferation of distributed energy resources (DERs) has increased coordination complexity, calling for efficient feasible region aggregation (FRA) with privacy protection. This paper presents a unified framework combining geometric aggregation and transformation-based encryption (TE) to ensure physical feasibility and data privacy in aggregating DERs dominated by inverter-based resources (IBRs). An affine-transformation (AT) approximation is employed to capture the nonlinear and asymmetric P–Q capability of IBRs under current and modulation constraints, offering a computationally efficient modeling strategy. The TE mapping and optimization processes are redesigned to achieve privacy-resilient aggregation. Theoretical and scenario-based analyses validate the framework's feasibility, optimality, and privacy protection effectiveness.**

***Index Terms*—Distributed energy resource aggregation, P–Q capability charts, privacy preservation.**

I. Introduction

With the growing penetration of distributed energy resources (DERs), device-level modeling and coordination have become increasingly challenging. Feasible region aggregation (FRA) provides a unified representation of heterogeneous DER flexibility, simplifying system operation and enabling market participation. In renewables-dominated grids, short-duration disturbances can induce rapid frequency and voltage deviations, increasing the reliance on FRA to deliver fast and high-magnitude power support [1]. However, most existing feasible-region formulations rely on quasi-static power limits or energy-based constraints to construct power reserve boundaries. Under dynamic operating conditions, such quasi-static boundaries fail to reflect the actual response capability of aggregated DERs. This limitation arises because quasi-static P–Q feasible regions neglect the instantaneous current and modulation constraints of grid-interfacing inverters. An inverter's instantaneous power delivery is tightly restricted by semiconductor current ratings and modulation ratio limits, allowing only a narrow margin for current or voltage deviations [2], [3]. Exceeding these limits leads to PWM saturation or current overload, causing instability of the underlying devices. Hence, explicit modeling of nonlinear coupled P–Q boundaries is vital to represent device-level constraints and ensure physically realizable aggregated flexibility.

A general framework based on the Minkowski sum of individual flexibility sets is computationally intractable. To enhance tractability, various inner-approximation formulations have been developed to eliminate infeasible operating points. Early studies adopt zonotopes [4] or homothets [5], [6] for tractable representations. However, the zonotope-based formulation is restricted by central symmetry, limiting its ability to represent the asymmetric feasible regions characteristic of IBRs. The homothetic framework scales and translates a common prototype polytope, yet cannot adequately capture geometric diversity across heterogeneous devices. The approach in [6] further decomposes individual IBR's flexibility set into a union of hyperrectangles, offering high accuracy at the expense of significant computational complexity. These limitations underscore the need for an aggregation formulation that retains computational efficiency while accurately characterizing the geometric heterogeneity and asymmetry of IBR feasible regions. The affine-transformation framework proposed in [7] establishes a promising basis by generalizing homothetic approximations to broader polyhedral classes. *This paper extends that formulation to inverter-interfaced DERs, accommodating the strong P–Q coupling and nonlinear geometric asymmetry inherent in their feasible regions.*

Centralized aggregation frameworks require DERs to disclose detailed operational information to the aggregator, which raises serious privacy concerns. Although distributed optimization mitigates individual-level risks by decomposing the global problem into local subproblems solved with private data, communication-level privacy remains a major challenge due to iterative exchanges of intermediate variables. To address these risks, several privacy-preserving schemes have been proposed, including differential privacy (DP) [8], [9], homomorphic encryption (HE) [10], and transformation-based encryption (TE) [11], [12]. Compared with DP and HE, TE offers a more concise and computation-efficient approach by masking the original model through random matrix transformations, which yields an equivalent encrypted formulation that preserves optimality while significantly reducing computational burden. Recent studies have verified the effectiveness of TE in distributed optimal power flow problems [12]. Against this background, a fundamental question arises: *Can the TE mechanism be effectively applied to DER aggregation, ensuring privacy preservation while accurately characterizing FRA?*

This paper makes two key contributions:

1) **DER Flexibility Aggregation Framework:** A unified framework is developed to characterize the P–Q feasible region of IBRs under inverter and operational constraints. Geometric aggregation methods are formulated

979-8-3315-8138-1

to construct FRA, capturing device-level heterogeneity.

2) **Privacy-Preserving TE Mechanism:** Structural and theoretical enhancements are introduced to the TE scheme, enabling feasibility preservation, optimality consistency, and numerical stability while maintaining communication efficiency. Theoretical and scenario-based analyses further demonstrate its *privacy effectiveness* against diverse threat models.

II. P-Q Feasible region from DERs

1) P-Q curve for IBR: PV/ESS units are interfaced via inverters subject to physical constraints. The inverter operating region is characterized by two voltage-dependent constraints:

$$\begin{cases} \mathcal{C}_1 : P_i^2 + Q_i^2 \le (V_i^{\mathrm{g}} \overline{I}_i^{\mathrm{rated}})^2, \\ \mathcal{C}_2 : \left(\frac{3V_i^{\mathrm{g}} V_i^{\mathrm{inv}}}{|Z_i|}\right)^2 = \left(P_i + \frac{3V_i^{\mathrm{g}2} R_i}{|Z_i|^2}\right)^2 + \left(Q_i + \frac{3V_i^{\mathrm{g}2} X_i}{|Z_i|^2}\right)^2, \end{cases} \tag{1}$$

where $Z_i = R_i + jX_i$ denotes the filter impedance. Constraint $\mathcal{C}_1$ enforces the current limit, while $\mathcal{C}_2$ represents the PWM saturation boundary, see [2] for details. For different modulation strategies, the inverter output voltage V_i^{inv} depends on the modulation index m_a and the DC-link voltage V_i^{dc}, given by $V_i^{\mathrm{inv}} = \frac{3}{2} m_a V_i^{\mathrm{dc}}/2$ for SPWM and $V_i^{\mathrm{inv}} = \frac{3}{2} m_a V^{\mathrm{dc}}/\sqrt{3}$ for SVPWM.

Since both limits depend on the grid-connected voltage V^{g}, the current constraint is evaluated at $\underline{V}^{\mathrm{g}}$ and the modulation constraint at $\overline{V}^{\mathrm{g}}$, yielding a conservative IBR feasible set as

$$\Phi_i^{\mathrm{IBR}} \triangleq \mathcal{C}_1(\underline{V}^{\mathrm{g}}) \cap \mathcal{C}_2(\overline{V}^{\mathrm{g}}). \tag{2}$$

$\mathcal{C}_1(V)$ tightens with decreasing V and $\mathcal{C}_2(V)$ with increasing V, so an inner valid for $V^{\mathrm{g}} \in [0.95, 1.05]$ is obtained in Fig. 1.

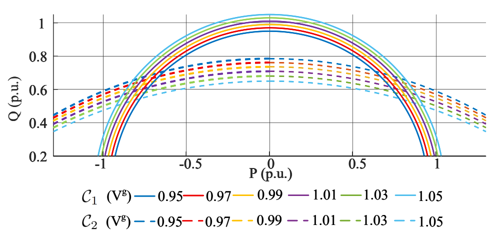

Fig. 1: P–Q capacity curve of IBR under different voltage

2) Regulation Capability: DER capability envelopes must satisfy active power limits, while PV units further comply with power-factor-based reactive limits:

$$\begin{cases} 0 \le P_i^{\mathrm{pv}} \le \overline{P}_i^{\mathrm{pv}}, \\ -\eta_i^{\mathrm{pv}} P_i^{\mathrm{pv}} \le Q_i^{\mathrm{pv}} \le \eta_i^{\mathrm{pv}} P_i^{\mathrm{pv}}, \\ -\overline{P}_i^{\mathrm{ess}} \le P_i^{\mathrm{ess}} \le \overline{P}_i^{\mathrm{ess}}. \end{cases} \tag{3}$$

III. Geometric Aggregation Methodology

A. Aggregation of P–Q Feasible Regions

The intersection of current and PWM constraints in Φ^{IBR} is nonlinear. To obtain a tractable representation, we construct an N-facet inner polyhedral approximation of $(\mathcal{C}_1, \mathcal{C}_2)$ by retaining their intersection points and linearizing the corresponding circular arcs. In general, the approximation accuracy improves as N increases. This accuracy can be quantified by the area ratio $\kappa = \sin(\alpha)/\alpha$, $\alpha = 2\pi/N$. In the case studies, we set $N = 8$, yielding $\kappa \approx 0.90$. By incorporating the regulation limits in (3), the resulting linearized feasible sets of PV and ESS units are denoted by Φ_i^{pv} and Φ_i^{ess}, respectively.

The FRA from DERs is obtained through Minkowski sum:

$$\mathbf{\Phi}^{\mathrm{DER}} = \bigoplus_{i \in \mathcal{N}_{\mathrm{pv}}} \Phi_i^{\mathrm{pv}} \oplus \bigoplus_{i \in \mathcal{N}_{\mathrm{ess}}} \Phi_i^{\mathrm{ess}}. \tag{4}$$

Note that the exact Minkowski sums are tractable mainly for homogeneous cases, while they may become prohibitive for heterogeneous portfolios [5]. Accordingly, PV and ESS units are first aggregated separately via affine inner-approximate polytopes to mitigate complexity; for the subsequent cross-type Minkowski sum, scalability can be further improved via polytope order reduction techniques such as facet pruning [13] or vertex sampling with convex-hull compression [14].

B. Inner Approximation via Affine Transformation

PV/ESS type-level feasible region aggregation is approximated by the maximum-volume affine transformation (i.e. scaling, rotation and translation) of a prototype polytope [7]:

$$\mathbf{\Phi}^{\mathrm{pv/ess}\prime} = \mathbf{f}^{\mathrm{pv/ess}} + \mathbf{F}^{\mathrm{pv/ess}} \mathbf{\Phi}_0^{\mathrm{pv/ess}} \subseteq \mathbf{\Phi}^{\mathrm{pv/ess}}. \tag{5}$$

Here, $\mathbf{\Phi}_0^{\mathrm{pv/ess}}$ is the prototype baseset, and $\mathbf{F}^{\mathrm{pv/ess}}, \mathbf{f}^{\mathrm{pv/ess}}$ denote the affine mapping. For notational simplicity, the superscripts of PV/ESS are omitted. AT finds the largest-volume inscribed polytope within all feasible sets of the same type, and all individual DER feasible-region constraints are reformulated under a unified representation. Based on Farkas' Lemma [6], the containment condition leads to the following problem:

$$\begin{aligned} \min_{\mathbf{F} \succ 0,\ \{\mathbf{\Gamma}_i, \boldsymbol{\gamma}_i, \mathbf{\Lambda}_i\}} \quad & -\log\det \mathbf{F} \\ \text{s.t.} \quad & \sum_i \mathbf{\Gamma}_i = \mathbf{F}, \quad \sum_i \boldsymbol{\gamma}_i = \mathbf{f}, \\ & \mathbf{\Lambda}_i \overline{\mathbf{H}} = \mathbf{H}_i \mathbf{\Gamma}_i, \\ & \mathbf{\Lambda}_i \overline{\mathbf{h}} \le \mathbf{h}_i - \mathbf{H}_i \boldsymbol{\gamma}_i, \\ & \mathbf{\Gamma}_i \succeq 0, \ \mathbf{\Lambda}_i \ge 0. \end{aligned} \tag{$\mathcal{P}$}$$

The prototype set Φ_0 in (5) is typically constructed from a conservative feasible region and expanded via homothetic transformation [5]. In our work, Φ_0 is chosen as the intersection of all normalized individual P–Q feasible regions, and the affine transformation further adjusts scale and orientation adaptively to improve the geometric fit while maintaining convexity and tractability. In highly heterogeneous settings, cluster-specific affine approximation can be constructed by grouping similar DER units [15].

C. Privacy-persevering DERs Aggregation

Solving $(\mathcal{P})$ centrally requires each DER to disclose its feasible region $\mathbf{\Phi}_i^{\mathrm{pv/ess}}$, giving rise to two inherent privacy risks: (i) *individual level* — local feasible regions embed inverter parameters and regulation limits, whose disclosure may reveal device characteristics; and (ii) *communication level*

979-8-3315-8138-1

— information exchanged during feasibility aggregation (e.g., individual contributions to the P–Q region) may be intercepted, exposing each DER's flexibility potential.

To mitigate these risks, this work adopts two complementary mechanisms: a distributed optimization framework that preserves *individual-level* privacy by solving local subproblems with private data, and a global TE scheme that protects *communication-level* privacy by encrypting exchanged variables via a shared orthogonal matrix $\mathbf{T}$. Defining

$$\tilde{\mathbf{\Gamma}}_i = \mathbf{T}\mathbf{\Gamma}_i\mathbf{T}^\top, \quad \tilde{\mathbf{F}} = \mathbf{T}\mathbf{F}\mathbf{T}^\top, \tag{6}$$

the inner approximation is then solved in the transformed $\sim$-domain. Fig. 2 shows the proposed global TE-sharing distributed scheme for solving $\sim$-domain counterpart ($\tilde{\mathcal{P}}$).

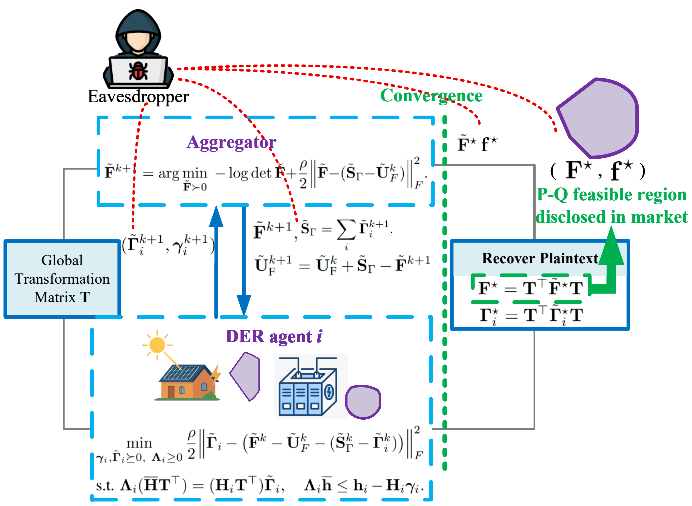

Fig. 2: Global TE Sharing-ADMM with Random Orthogonal Transformation[1]

Remark 1. *The effectiveness of TE relies on congruence transformations, which preserve the positive semidefinite cone and ensure equivalence of feasibility and optimality (Proposition 1). In distributed settings, participants share a common global matrix* $\mathbf{T}$ *to maintain constraint compatibility. In practice, an* orthogonal $\mathbf{T}$ *is often adopted for numerical stability and preserved convergence (Proposition 2).*

In the global orthogonal TE scheme, each DER reports only transformed representations, preventing external eavesdroppers from reconstructing $\mathbf{\Gamma}_i$ from intercepted messages (Proposition 3) and thereby ensuring *communication-level privacy*. The proof is given in the Appendix.

IV. Simulation Results

A. System Configuration

The test system comprises 10 PV inverter types and 10 ESS inverter types with RL filters [2], [16]. All units are three-phase grid-connected converters operating at line voltage of 60 Hz, 690 Vrms. PV inverters employ DC-link voltages of 900–1050 V, while ESS inverters use 750–900 V. Apparent power ratings span 400 kVA–1.5 MVA, with current limits $\overline{I}_i^{\text{rated}} = \overline{S}_i^{\text{rated}}/V_i^{\text{rated}}$, which define the current-bound constraints. The modulation index m_a ranges from 0.75 to 0.98. All IBRs adopt SPWM modulation.

As discussed in Section II, the P–Q feasible region is governed by: (i) inverter parameters σ_i, (ii) active-power ratio $\rho_i = \overline{P}_i/\overline{S}_i^{\text{rated}}$, and (iii) power-factor limit η_i (PV only). ESS heterogeneity originates from inverter-parameter variations, whereas PV heterogeneity arises from ρ_i (sunny/cloudy) and η_i [2]. The evaluation metric is the area ratio between the approximated polytope and the true FRA computed via the MPT toolbox.

B. DER P-Q Feasible Region Aggregation

a) Individual P–Q region approximation: Table I shows that approximation errors grow with heterogeneity, yet AT consistently outperforms HT because it permits non-uniform scaling on the P–Q plane. For ESS, AT reduces errors greatly (e.g., 8% vs. 20% at Level 2). For PV, AT keeps errors below 5% in cloudy (nearly triangular) cases compared with 7–10% for HT, and in sunny (asymmetric polygon) cases it reduces region loss by 2–3%. These geometric differences explain AT's superior accuracy, as corroborated by Table I and Fig. 3.

TABLE I: Approximation error (%) mean ± std under heterogeneity

DER	Case	AT (mean±std)	HT (mean±std)
ESS	Level 1	4.48 ± 0.42	6.85 ± 0.98
	Level 2	6.03 ± 1.12	13.17 ± 1.80
	Level 3	8.21 ± 1.77	19.65 ± 2.07
PV (ρ_{s0})	$\eta \in \eta_1$	7.52 ± 3.08	10.76 ± 2.10
	$\eta \in \eta_2$	9.75 ± 3.35	11.45 ± 4.13
PV (ρ_{c0})	$\eta \in \eta_1$	2.93 ± 0.85	6.82 ± 0.93
	$\eta \in \eta_2$	4.20 ± 1.51	9.79 ± 3.48

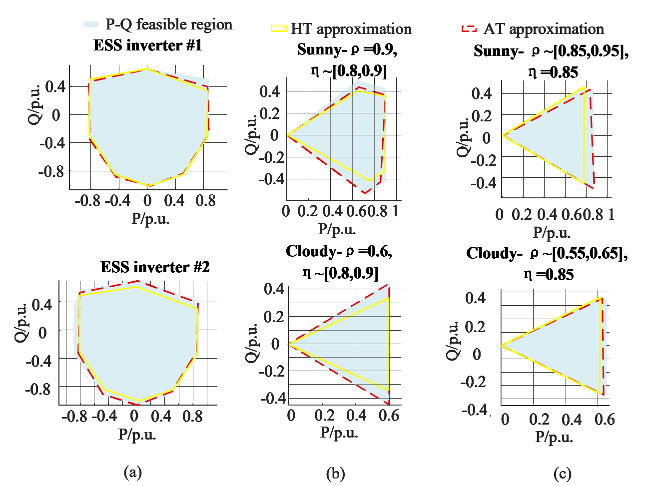

Fig. 3: Comparison of inner approximation methods for representative DER units. Heterogeneity in (a) inverter parameter σ; (b) power factor η; (c) active power limits ρ.

[1]The orthogonal transformation $\mathbf{T}$ is applied exclusively to the matrix variables $(\mathbf{\Gamma}_i, \mathbf{F})$, whereas the vectors γ_i and $\mathbf{f} = \sum_i \gamma_i$ are kept in the original domain. Since $\mathbf{f}$ does not participate in the objective and is obtained via direct aggregation, transforming it would be redundant and could introduce additional linear dependencies that compromise the concealment of $\mathbf{T}$ (Remark 2).

[2]Detailed simulation settings are provided as supplementary material at https://github.com/Joyz0413/Simulation_Setting_Privacy_Preserving_DER_Aggregation.

979-8-3315-8138-1

b) FRA from DERs: To evaluate aggregation performance for a population of 100 DER units, four representative device classes (A–D) are combined into several heterogeneity cases (5:3:1:1, 5:2:2:1, 4:3:2:1, and 4:3:1:2), which is reported in the supplementary simulation setting document. Across all cases, AT consistently outperforms HT. For ESS, its advantage grows with heterogeneity, reducing errors from 29.38% to 17.67%. For PV units, sunny conditions yield larger errors because high ρ produces more irregular feasible regions. Comparing Case 1–2 and Case 1–3 (heterogeneity from ρ vs. η), variations in η have a stronger impact, indicating that power-factor heterogeneity is more critical than active-power-ratio heterogeneity. As shown in Table II, modifying η for ten PV inverters increases error from 5.59% to 9.06%, whereas modifying ρ increases it to 12.52%. The rise from Case 1 to Case 4 further shows that the effect of power-factor heterogeneity is amplified when combined with inverter-type diversity; by comparison, its influence becomes negligible cloudy conditions.

TABLE II: Aggregation errors for FRA (%) of ESS and PV cases

DER Scenario	Case 1		Case 2		Case 3		Case 4	
	AT	HT	AT	HT	AT	HT	AT	HT
ESS	6.80	11.35	8.03	14.12	9.16	15.24	17.67	29.38
PV (Sunny)	5.59	6.89	9.06	13.23	12.52	18.75	19.40	28.76
PV (Cloudy)	1.73	10.88	4.19	15.42	4.88	16.03	5.00	18.75

C. Performance of the distributed privacy protection

In the proposed global TE scheme, DERs jointly share a secret orthogonal matrix $\mathbf{T}$, such that the aggregator operates in the transformed $\sim$-domain rather than in the plaintext domain. As demonstrated in Fig. 4, the orthogonal transformation distorts FRA observable by external entities. Since $\mathbf{T}$ is not uniquely identifiable from $(\mathbf{F}, \tilde{\mathbf{F}})$, adversaries are unable to reconstruct $\boldsymbol{\Gamma}_i$, thereby ensuring the confidentiality of DER-level constraints.

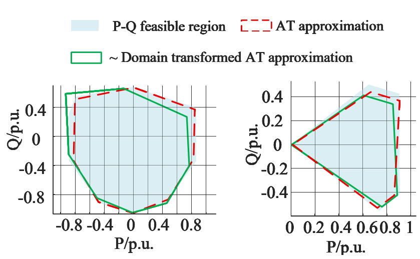

Fig. 4: Representative DER P-Q feasible region approximation perceived by external eavesdropper.

Fig. 5 further shows that the TE-based distributed algorithm converges within 160 iterations, attaining only a 1.9% deviation from the centralized benchmark. In this case study, the FRA is obtained via a cross-type Minkowski sum of the PV- and ESS-level polytopes. Both the convergence trajectory and rate closely resemble those of standard ADMM, consistent with the theoretical equivalence established in the Appendix.

For comparison, a DP approach is implemented by injecting Gaussian noise into $(\boldsymbol{\Gamma}_i^{k+1}, \gamma_i^{k+1})$. While effective in preserving communication-level privacy, this approach deteriorates convergence performance, leading to a 2.2% deviation, 2.65 $(\text{p.u.})^2$, from the optimal FRA value and increasing the average approximation error from 6.45% to 7.97%.

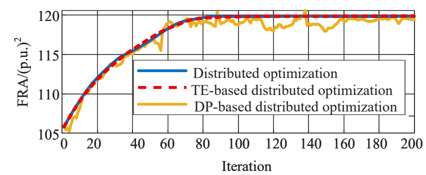

Fig. 5: Iteration trajectory with privacy protection scheme.

TABLE III: Comparison of Different Algorithm

	Cen.	Dist.	TE-Dist.	DP-Dist.
FRA / $(\text{p.u.})^2$	121.53	119.32	119.10	118.88
Avg. AT Error / %	6.45	6.52	6.50	7.97

V. Conclusion

This paper applies and extends the affine-transformation approximation to the aggregation of inverter-based DERs. Compared with the conventional homothetic approach, the AT method more effectively captures geometric asymmetry and strong P–Q coupling in inverter feasible regions, leading to improved adaptability and tighter aggregation accuracy. The proposed P–Q coupling is consistent with practical inverter limits (e.g., current and PWM saturation), while the framework can be extended to incorporate time-coupled energy constraints by introducing additional linear multi-period constraints in future work. In addition, a TE mechanism is integrated to achieve privacy-preserving distributed optimization. Experimental results demonstrate that the TE scheme protects sensitive information without compromising convergence or optimality, confirming the practicality of the proposed framework for secure and efficient DER aggregation.

VI. Appendix

A. TE's Applicability

Proposition 1 (Optimality guarantee)**.** *Under the congruence transformation (6), $(\mathcal{P})$ and $(\tilde{\mathcal{P}})$ are equivalent—objective values are preserved, feasible sets are in bijection, and optimizers map to each other.*

Proof. Objective function. For any $\mathbf{F} \succ 0$,

$$-\log\det\tilde{\mathbf{F}} = -\log\det(\mathbf{T}\mathbf{F}\mathbf{T}^\top) = -\log\det\mathbf{F} - 2\log|\det\mathbf{T}|,$$

which differs from $-\log\det\mathbf{F}$ only by a constant independent of variables. Thus, minimizers coincide under the change of variables.

Feasible set. Since the transformation matrix is invertible, the mapping between original and transformed variables is bijective. Moreover, congruence transformations preserve the positive semidefinite cone [17], which guarantees that feasibility is preserved.

Optimality. As the transformation is linear and cone-preserving, KKT conditions map directly between $(\mathcal{P})$ and $(\tilde{\mathcal{P}})$, ensuring that optimizers correspond one-to-one. $\square$

Lemma 1 (Equivariance under orthogonal transformation)**.** *Proximal mappings and Euclidean projections commute with orthogonal transformations (see [18]).*

Proposition 2 (Convergency analysis)**.** *By Lemma 1, each ADMM update in the transformed domain is the orthogonal image of its plaintext counterpart. Consequently, the primal and dual residual norms remain identical, and the convergence trajectory and rate are preserved in both domains.*

B. Privacy Protection

Threat models is premised on the possibility that the plaintext aggregate $\mathbf{F}, \mathbf{f}$ becomes observable to adversaries (e.g., when disclosed in market interactions). On this basis, the following additional threat factors are considered:

1) **Passive eavesdropper:** Intercepts communication channels and observes transformed messages $(\tilde{\mathbf{\Gamma}}_i, \gamma_i, \tilde{\mathbf{F}}, \mathbf{f})$ exchanged during optimization.
2) **Multi-instance attacker:** Accumulates multiple observations of $(\mathbf{F}, \tilde{\mathbf{F}})$ across different optimization runs to reduce the ambiguity of $\mathbf{T}$.
3) **Partial disclosure attacker:** Possesses a subset of original DER parameters $(\tilde{\mathbf{\Gamma}}_i, \mathbf{\Gamma}_i)$ and leverages both the exposed $\mathbf{F}$ and transformed data to infer private information of other DERs.

Lemma 2 (Non-uniqueness of transformation recovery)**.** *Given* $(\mathbf{F}, \tilde{\mathbf{F}})$ *with* $\tilde{\mathbf{F}} = \mathbf{T}\mathbf{F}\mathbf{T}^\top$ *and* $\mathbf{F} \succ 0$*, the set of feasible* $\mathbf{T}$ *is infinite: for any* $\mathbf{U} \in O(n)$*,* $\mathbf{T}' = \tilde{\mathbf{F}}^{1/2}\mathbf{U}\mathbf{F}^{-1/2}$ *satisfies* $\tilde{\mathbf{F}} = \mathbf{T}'\mathbf{F}\mathbf{T}'^\top$.

Remark 2 (Design choice for $\mathbf{T}$ protection)**.** *In the TE design, only the matrix variables* $(\mathbf{\Gamma}_i, \mathbf{F})$ *are transformed by* $\mathbf{T}$*, while the vector variables* γ_i *remain untransformed. This prevents* γ_i *from acting as an additional linear clue that could help an adversary infer* $\mathbf{T}$*. By leaving* γ_i *in plaintext, the uncertainty of* $\mathbf{T}$ *as established in Lemma 2 is preserved, thereby strengthening individual privacy.*

Proposition 3 (Individual-level feasible-region privacy of DERs)**.** *Even if an adversary observes both* $(\mathbf{F}, \tilde{\mathbf{F}})$*, Lemma 2 ensures that the true* $\mathbf{T}$ *cannot be uniquely determined. Since recovering local data requires* $\mathbf{\Gamma}_i = \mathbf{T}^{-1}\tilde{\mathbf{\Gamma}}_i\mathbf{T}^{-\top}$*, any individual* $\mathbf{\Gamma}_i$ *remains non-identifiable without the exact* $\mathbf{T}$*. This directly protects against a* passive eavesdropper*, who only observes transformed exchanges during optimization. For stronger adversaries, additional measures are required:* ***periodic refreshing of*** $\mathbf{T}$ *prevents from linking* multiple instances attacks.

Discussions on key exposure. Proposition 3 considers a passive eavesdropper who observes transformed exchanges but does not obtain the transformation matrix $\mathbf{T}$. If $\mathbf{T}$ is compromised (or inferred via partial disclosure of $(\tilde{\mathbf{\Gamma}}_i, \mathbf{\Gamma}_i)$ from a subset of DERs), the global transformation alone cannot guarantee individual-level privacy, corresponding to a stronger key-exposure threat model. This risk can be mitigated by the following enhancements:

- **Group-wise transformations:** DERs are partitioned into multiple groups with independent keys $\{\mathbf{T}_g\}$, such that disclosure of a single $\mathbf{T}_g$ only affects DERs within the compromised group.
- **Secure aggregation:** DERs transmit messages using pairwise random masks that cancel out during aggregation [11]. As a result, the coordinator observes only aggregated sums, while individual $\mathbf{\Gamma}_i$ and $\boldsymbol{\gamma}_i$ remain non-identifiable even if the transformation matrix is disclosed.

References

[1] V. Häberle, A. Tayyebi, X. He, E. Prieto-Araujo, and F. Dörfler, “Grid-forming and spatially distributed control design of dynamic virtual power plants,” *IEEE Transactions on Smart Grid*, vol. 15, no. 2, pp. 1761–1777, 2023.

[2] H. S. Das, S. Li, B. Lu, J. Wang, S. Rahman, and X. Fu, “Exploring dynamic pq capability and abnormal operations of inverter-based resources,” *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 12, no. 2, pp. 1608–1618, 2024.

[3] L. Streitmatter, T. Joswig-Jones, and B. Zhang, “Geometry of the feasible output regions of grid-interfacing inverters with current limits,” *IEEE Control Systems Letters*, 2025.

[4] F. L. Müller, J. Szabó, O. Sundström, and J. Lygeros, “Aggregation and disaggregation of energetic flexibility from distributed energy resources,” *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 1205–1214, 2017.

[5] L. Zhao, W. Zhang, H. Hao, and K. Kalsi, “A geometric approach to aggregate flexibility modeling of thermostatically controlled loads,” *IEEE Transactions on Power Systems*, vol. 32, no. 6, pp. 4721–4731, 2017.

[6] M. S. Nazir, I. A. Hiskens, A. Bernstein, and E. Dall’Anese, “Inner approximation of minkowski sums: A union-based approach and applications to aggregated energy resources,” in *2018 IEEE Conference on Decision and Control (CDC)*. IEEE, 2018, pp. 5708–5715.

[7] F. Al Taha, T. Vincent, and E. Bitar, “An efficient method for quantifying the aggregate flexibility of plug-in electric vehicle populations,” *IEEE Transactions on Smart Grid*, 2024.

[8] V. Dvorkin, F. Fioretto, P. Van Hentenryck, P. Pinson, and J. Kazempour, “Differentially private optimal power flow for distribution grids,” *IEEE Transactions on Power Systems*, vol. 36, no. 3, pp. 2186–2196, 2020.

[9] M. Huang, X. Cui, and Y. Wang, “Distributed differentially private energy management of virtual power plants,” *Electric Power Systems Research*, vol. 234, p. 110687, 2024.

[10] T. Wu, C. Zhao, and Y.-J. A. Zhang, “Privacy-preserving distributed optimal power flow with partially homomorphic encryption,” *IEEE Transactions on Smart Grid*, vol. 12, no. 5, pp. 4506–4521, 2021.

[11] Z. Hou, S. Lu, Y. Xu, H. Qiu, W. Gu, Z. Y. Dong, and S. Ding, “Privacy-preserved aggregate thermal dynamic model of buildings,” *IEEE Transactions on Smart Grid*, vol. 15, no. 6, pp. 5653–5664, 2024.

[12] M. Jia, G. Hug, Y. Su, and C. Shen, “Chance-constrained opf: A distributed method with confidentiality preservation,” *IEEE Transactions on Power Systems*, vol. 38, no. 4, pp. 3373–3387, 2022.

[13] Y. Wen, Z. Hu, S. You, and X. Duan, “Aggregate feasible region of ders: Exact formulation and approximate models,” *IEEE Transactions on Smart Grid*, vol. 13, no. 6, pp. 4405–4423, 2022.

[14] S. Wang and W. Wu, “Aggregate flexibility of virtual power plants with temporal coupling constraints,” *IEEE Transactions on Smart Grid*, vol. 12, no. 6, pp. 5043–5051, 2021.

[15] M. Huang, W. Lin, J. Ma, and Y. Wang, “Performance-integrated virtual power plant management in the frequency regulation market,” *IEEE Transactions on Smart Grid*, 2025.

[16] Z. Quan, Y. W. Li, Y. Pan, C. Jiang, Y. Yang, and F. Blaabjerg, “Reconsideration of grid-friendly low-order filter enabled by parallel converters,” *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 9, no. 3, pp. 3177–3188, 2020.

[17] S. P. Boyd and L. Vandenberghe, *Convex optimization*. Cambridge university press, 2004.

[18] N. Parikh, S. Boyd *et al.*, “Proximal algorithms,” *Foundations and trends® in Optimization*, vol. 1, no. 3, pp. 127–239, 2014.