

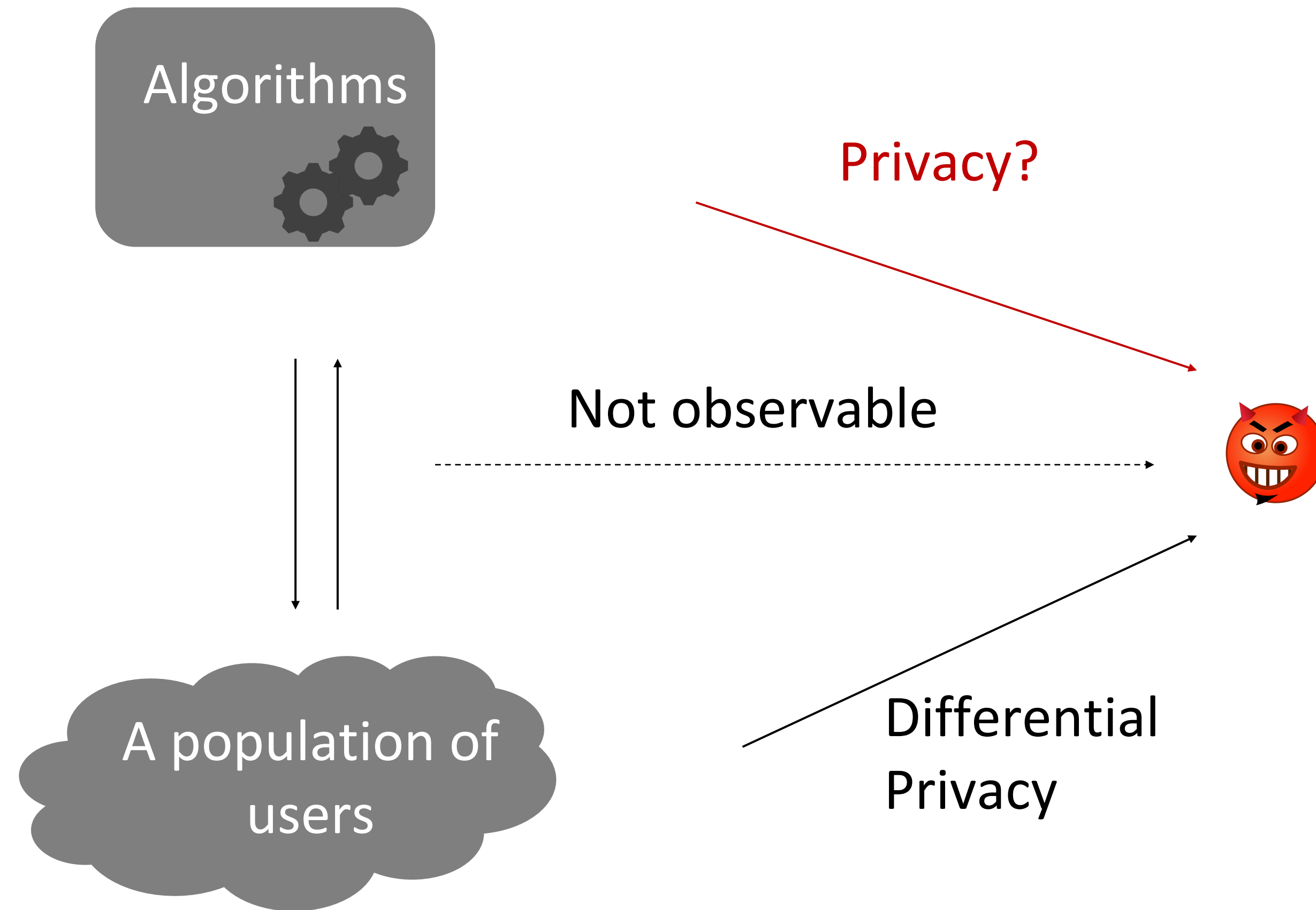
Optimal Query Complexity of Secure Stochastic Convex Optimization

Accepted in NeurIPS'20

Wei Tang, Washington University in St. Louis
Chien-Ju Ho, Washington University in St. Louis
Yang Liu, UC Santa Cruz



UC SANTA CRUZ



➤ For time step $t = 1, \dots, T$:

➤ **Learner** submits query $X_t \in \mathcal{X}$

➤ Learner learns information provided by an oracle $Y_t = \phi(X_t, f)$

➤ **Learner** formulates an estimates \hat{X}_{T+1}

➤ **Adversary** observes $X^T = (X_1, \dots, X_T)$ and formulates an estimator \hat{X}^{adv}

Consider a function class $f \in \mathcal{F}$ and an oracle ϕ :

• Learner's algorithm \mathcal{A} is (ϵ, δ) -accurate if:

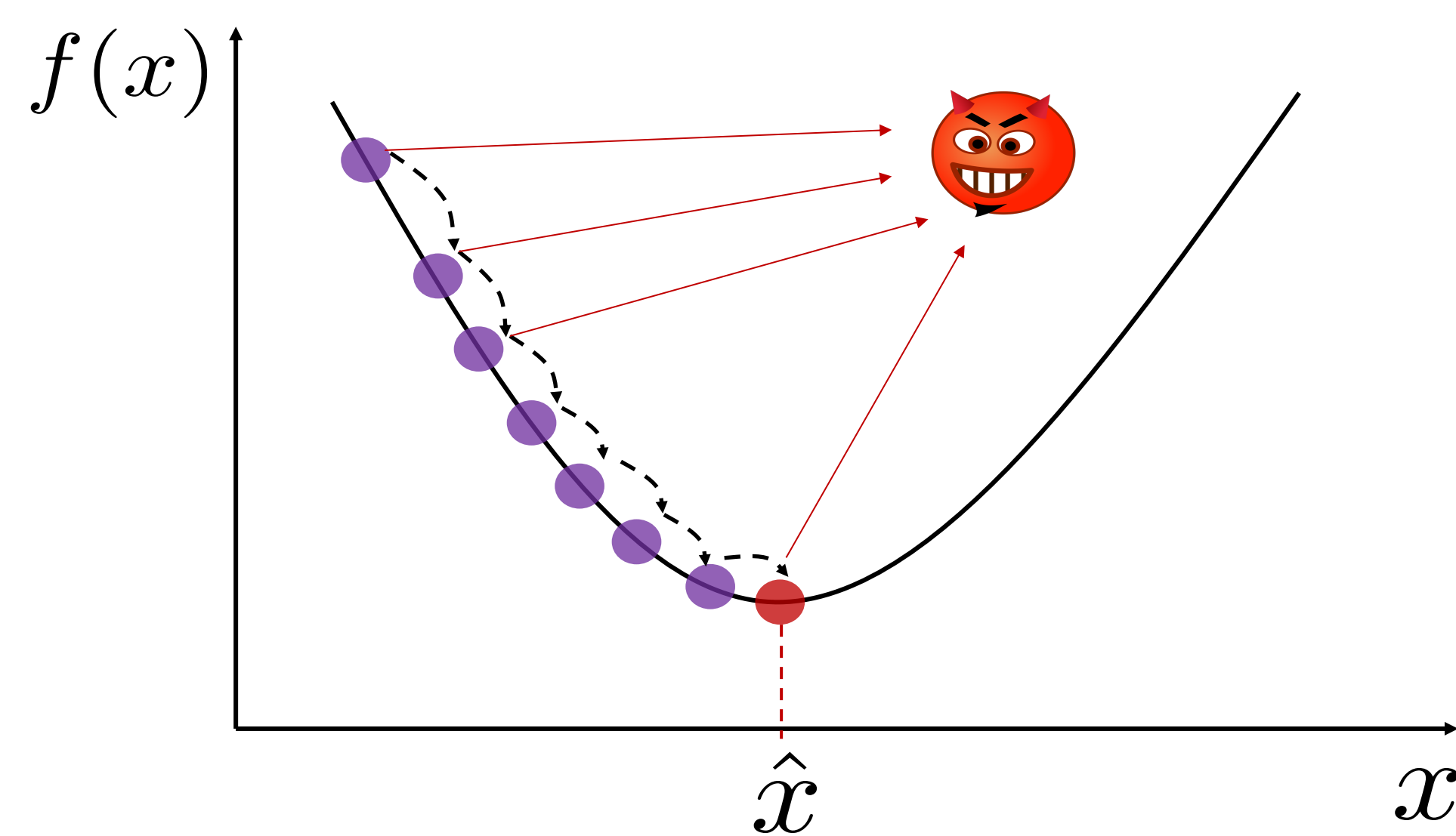
$$\sup_{f \in \mathcal{F}} \mathbb{P} \left(\text{err}_{\mathcal{A}} \left(\hat{X}_{T+1}, f \right) \geq \epsilon \right) \leq \delta$$

• \mathcal{A} is $(\epsilon^{\text{adv}}, \delta^{\text{adv}})$ -private if for any adversary estimator \hat{X}^{adv} , following holds

$$\sup_{f \in \mathcal{F}} \mathbb{P} \left(\text{err} \left(\hat{X}^{\text{adv}}, f \right) \leq \epsilon^{\text{adv}} \right) \leq \delta^{\text{adv}}$$

Summary:

- We study the secure stochastic convex optimization problem, in which the learner aims to optimize the accuracy, i.e., obtain an accurate estimate to the optimal point, while securing her privacy, i.e., preventing an adversary from inferring what she learned.
- We characterize the trade-offs between learner's accuracy and privacy using query complexity.

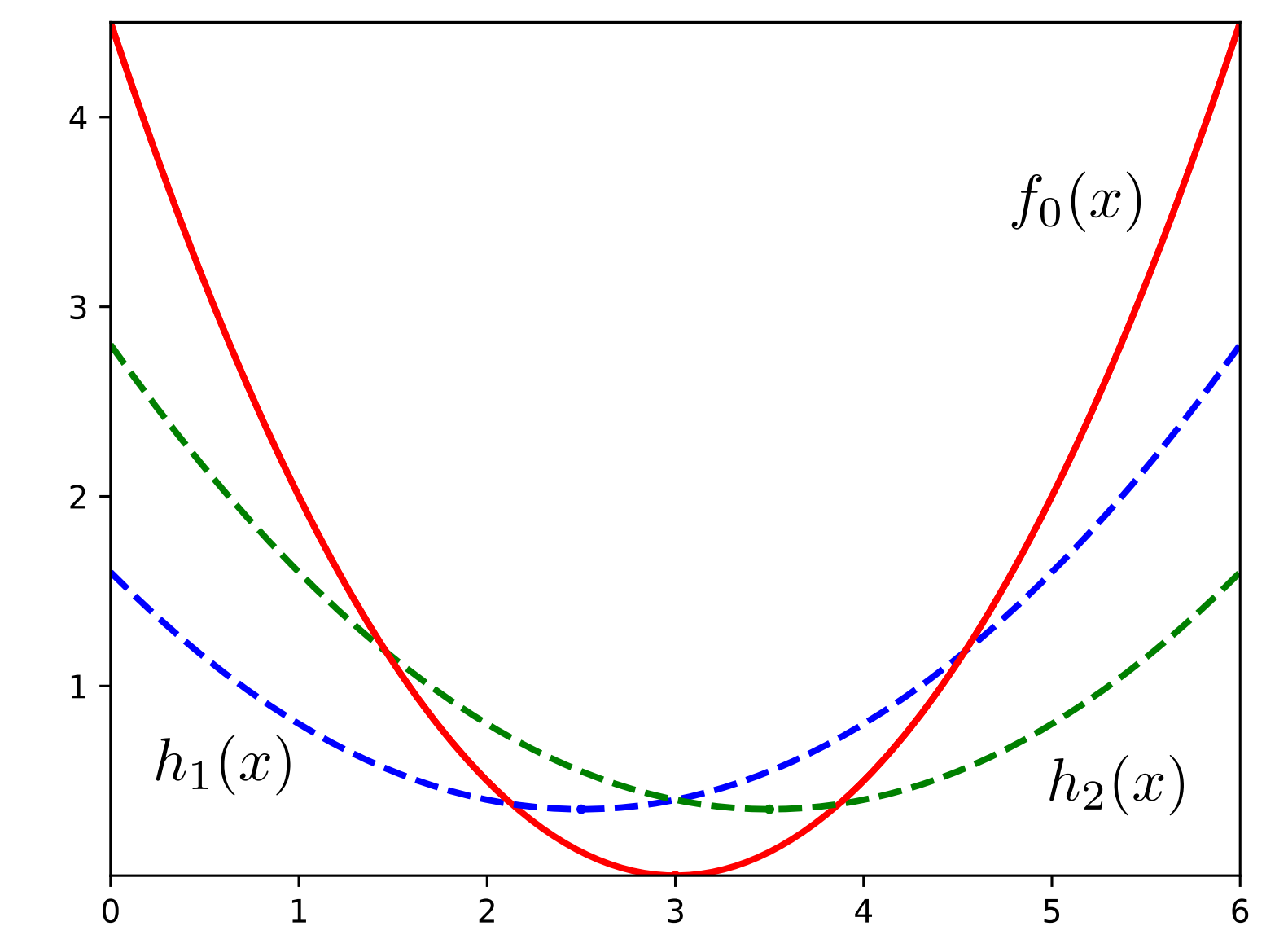


Fix a problem instance $(\mathcal{X}, \mathcal{F}, \phi)$. Define **Secure Query Complexity**:

- **smallest** number of queries needed for a learner's algorithm to be (ϵ, δ) -accurate and $(\epsilon^{\text{adv}}, \delta^{\text{adv}})$ -private for any $f \in \mathcal{F}$.

Lower Bounds (Secure Query Complexity):

- $\Omega \left(\frac{(1-\delta)\sigma^2}{\delta^{\text{adv}}\epsilon^2} \right)$ for Convex Lipschitz
- $\Omega \left(\frac{(1-\delta)\sigma^2}{\delta^{\text{adv}}\epsilon} \right)$ for Strongly convex, Lipschitz functions



An algorithm with matching upper bound:

- Secure learning protocol: a mix of (secure but non-efficient) uniform query protocol and (efficient but non-secure) standard methods from the optimization literature

