



The Hong Kong University of Science and Technology

Department of Mathematics

MPhil THESIS EXAMINATION

**Differential Private Empirical Risk Minimization
by Gradient Descent**

By

Mr. Bingsong GAO

ABSTRACT

This thesis studies differential private empirical risk minimization (ERM) through the lens of gradient-based optimization. We examine three canonical approaches—output perturbation, objective perturbation, and gradient perturbation—and analyze their privacy guarantees and utility bounds. The central contribution is a *sensitivity contraction* framework: under local strong convexity and smoothness, the sensitivity of gradient descent iterates contracts geometrically, allowing a single noise injection at the final iterate rather than at every step. This one-shot mechanism achieves the optimal error rate $O(1/(\mu n))$, matching the minimax lower bound and improving upon the iteration-dependent bounds of noisy gradient descent, while requiring only local strong convexity. The framework extends naturally to constrained and non-smooth regularized problems via nonexpansive projection and proximal operators. Experiments on various types of examples are conducted to confirm that the one-shot mechanism consistently reduces estimation variance compared to noisy gradient descent, especially when privacy cost is non-negligible. The sensitivity contraction framework thus achieves optimal privacy-utility trade-offs under milder assumptions than existing methods.

Date : 10 August 2026, Monday

Time : 3:00 pm

Venue : Room 5506 (Lifts No. 25/26)

Thesis Examination Committee

Chairman : Prof. Rong TANG, MATH /HKUST

Thesis Supervisor : Prof. Dong XIA, MATH/HKUST

Member : Prof. Jianfeng CAI, MATH/HKUST (via online)

(Open to all faculty and students)

The student's thesis is now being displayed on the reception counter in the General Administration Office (Room 3461).