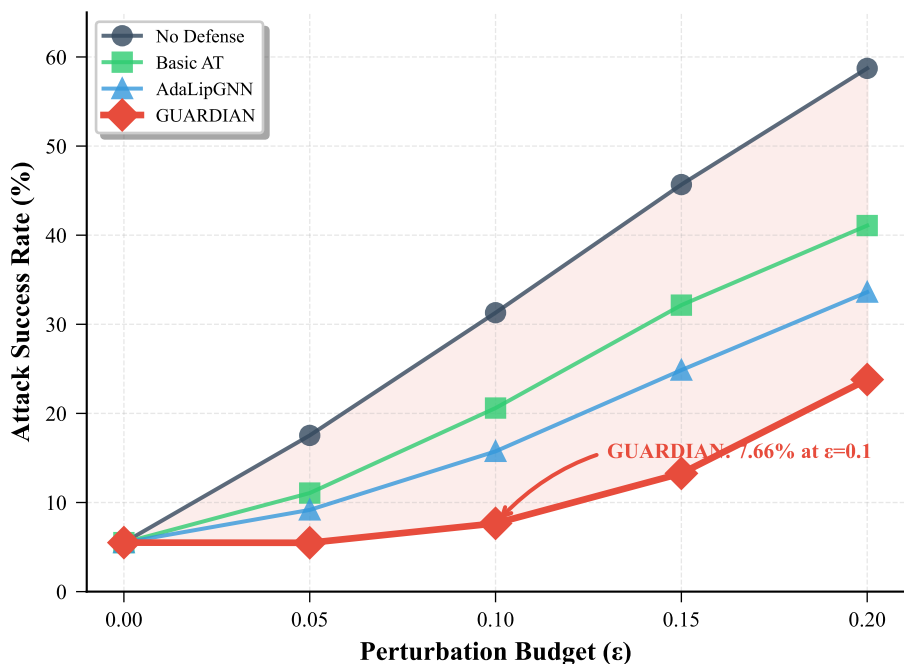
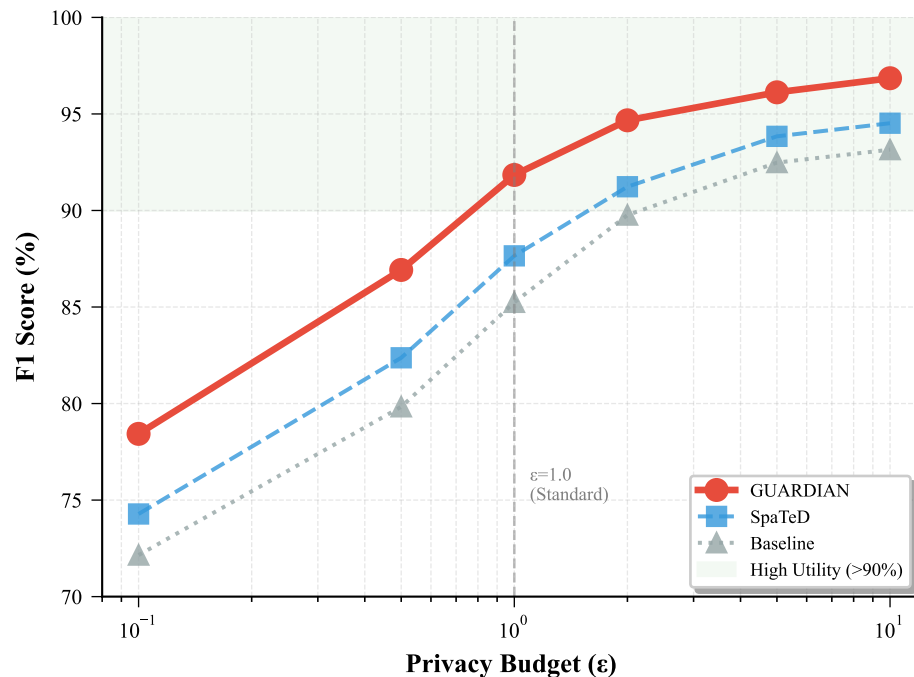


Security Evaluation: Adversarial Robustness and Privacy Protection

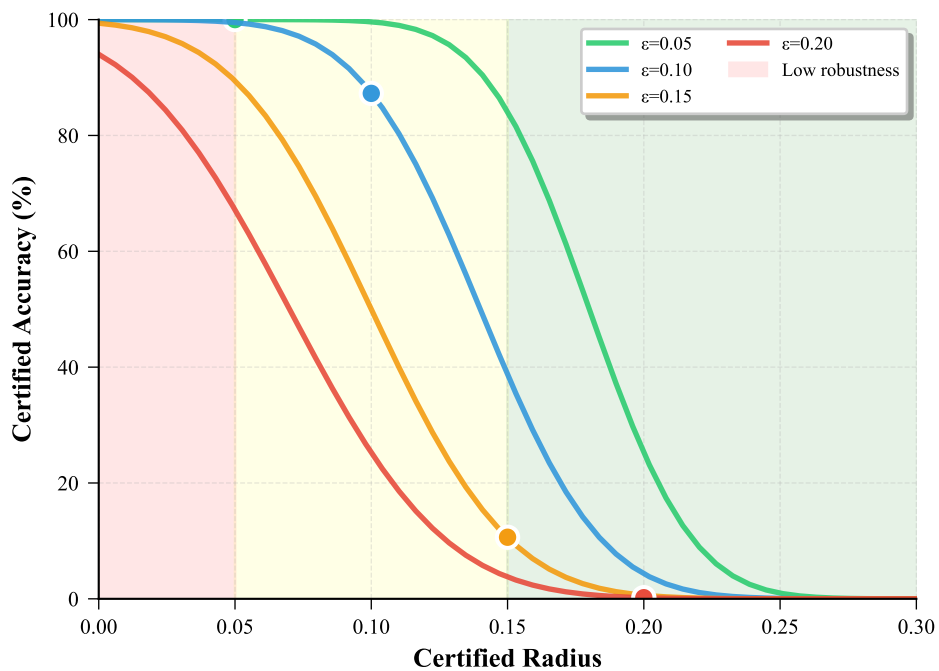
(a) Adversarial Attack Success Rates



(b) Privacy-Utility Tradeoff



(c) Certified Robustness Distribution



(d) Membership Inference Attack Resistance

