Abstract of Dissertation Presented to the Graduate School
of the University of Florida in Partial Fulfillment of the
Requirements for the Degree of Doctor of Philosophy

DATA STRUCTURES IN ADVERSARIAL ENVIRONMENTS

By

Sam A. Markelon

August 2025

Chair: Vincent Bindschaedler
Major: Computer Science

This dissertation investigates the security of widely-used data structures under adversarial conditions, with a particular focus on compact frequency estimators (CFEs) and probabilistic skipping-based data structures (PSDS). These structures, though efficient and fundamental to many modern systems, have historically been analyzed primarily through the lens of performance and operational efficiency, with security considerations treated as an afterthought.

Compact probabilistic data structures (CPDS), such as Bloom filters, Count-min sketch (CMS), and HeavyKeeper (HK), are designed to provide compact representations of large datasets, supporting approximate queries with bounded error probabilities. However, existing correctness guarantees implicitly assume non-adaptive adversaries. This dissertation reveals that adaptive adversaries can severely degrade the accuracy of these structures. In particular, it presents both theoretical and experimental attacks against CMS and HK that exploits a mixture of fixed randomness and past query responses, leading to significant frequency estimation errors. To counteract these vulnerabilities, the dissertation introduces Count-Keeper, a novel CFE that offers improved accuracy for honest data streams, resilience against adaptive attacks, and a native mechanism for flagging suspicious estimates.

Beyond theoretical analysis, this work evaluates CFE implementations in Redis, a widely deployed in-memory database system. Redis's reliance on non-cryptographic hash functions and deviations from standard CFE designs enable novel attacks that surpass those possible against

generic versions. This analysis highlights the critical need for secure implementations in practice and proposes countermeasures to mitigate these threats.

Probabilistic skipping-based data structures (e.g., hash tables, skip lists, and treaps) also exhibit vulnerabilities under adversarial conditions. While these structures achieve efficient operations by leveraging randomness, adaptive adversaries can force worst-case performance, causing exponential degradation in their operational efficiency. This dissertation presents attacks on these structures and proposes robust, performant variants. The robustness of these variants is formalized through the Adaptive Adversary Property Conservation (AAPC) framework, which quantifies deviation from expected performance under adversarial influence. Analytical proofs and experimental validation confirm the efficacy of these designs.

Collectively, this dissertation advances the security analysis of data structures from theoretical constructs to real-world implementations, bridging the gap between performance and provable security.