Errata to SoK: So, You Think You Know All About Secure Randomized Caches?

I. Introduction

In figure 17 of the SoK paper [1], we used the results of [2] and extended it to our own models. A recent arXiv paper [3] suggested that bugs in the code of [2] could impact our results in figure 17. We verified the claim made by the authors of the arXiv paper [3], and we corroborate the findings for bug-1 and bug-2, highlighted by [3] in the source code of [2], because of which the results shown in Figure 17 change. We thank the authors of the arXiv paper for this effort.

In Section 4 of the SoK paper [1], we extend the analysis carried out by [2]. We *originally* claimed that their findings show that *low-occupancy-based* attacks are possible on Mirage [4]. However, a recent work [3] investigates the low-occupancy-based attack proposed by [2] and finds the following flaws in it:

1) Incorrect indexing of AES traces [2]: The authors [2] apply a check for maximum traces locally per trace file, rather than globally, which leads to it under-reporting the number of AES traces for a given GE by a factor of the number of trace files
2) Bug in Mirage modeling [2]: The authors [2] model Mirage with a fixed seed rather than a random seed. This means that for a given plaintext-ciphertext pair, the timing value obtained is a function of the plaintext-ciphertext pair alone, since the sequence of evictions would be fixed every run. However, theoretically, the sequence of evictions in Mirage should be random and not fixed.

We have thoroughly investigated these claims and concluded that the flaws highlighted [3] are indeed correct. With the corrected attack, the updated Figure 17 from our SoK paper [1] resembles Figure 1. The implication of the change is that Mirage [4] is **not** any more vulnerable to the *low-occupancy-based* attack proposed by [2] than other cache designs.

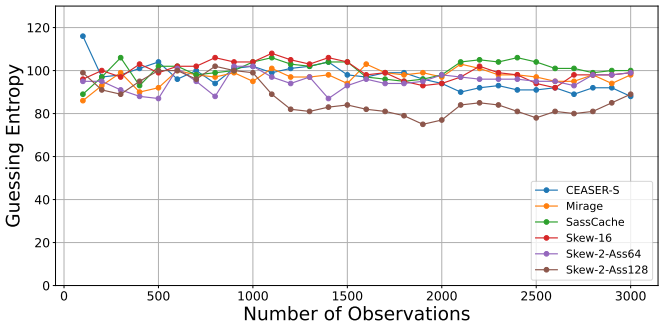

Fig. 1: Updated: Guessing entropy for AES key recovery across a 50% occupancy rate for varying number of observations.

References

[1] A. Bhatla, H. R. Bhavsar, S. Saha, and B. Panda, "Sok: so, you think you know all about secure randomized caches?" in *Proceedings of the 34th USENIX Conference on Security Symposium*, ser. SEC '25. USA: USENIX Association, 2025.

[2] A. Chakraborty, N. Mishra, S. Saha, S. Bhattacharya, and D. Mukhopadhyay, "Systematic evaluation of randomized cache designs against cache occupancy," in *Proceedings of the 34th USENIX Conference on Security Symposium*, ser. SEC '25. USA: USENIX Association, 2025.

[3] C. Cao and G. Saileshwar, "Yet another mirage of breaking mirage: Debunking occupancy-based side-channel attacks on fully associative randomized caches," 2025. [Online]. Available: https://arxiv.org/abs/2508.10431

[4] G. Saileshwar and M. Qureshi, "MIRAGE: Mitigating Conflict-Based cache attacks with a practical Fully-Associative design," in *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, Aug. 2021, pp. 1379–1396. [Online]. Available: https://www.usenix.org/conference/usenixsecurity21/presentation/saileshwar