CECS
CENTER FOR EMBEDDED & CYBER-PHYSICAL SYSTEMS
UNIVERSITY OF CALIFORNIA · IRVINE

CECS Seminar

"Poly-Logarithmic Side Channel Rank Estimation via Expontential Sampling"

Liron David

Ph.D. Candidate, Electrical Engineering at Tel-Aviv University

Tuesday, March 12, 2019
10:00 a.m.- 11:00 a.m.
Engineering Hall 5204

Abstract: Rank estimation is an important tool for a side-channel evaluations laboratories. It allows estimating the remaining security after an attack has been performed, quantified as the time complexity and the memory consumption required to brute force the key given the leakages as probability distributions over d subkeys (usually key bytes). These estimations are particularly useful where the key is not reachable with exhaustive search.

We propose ESrank, the first rank estimation algorithm that enjoys provable poly-logarithmic time- and space-complexity, which also achieves excellent practical performance. Our main idea is to use exponential sampling to drastically reduce the algorithm's complexity. Importantly, ESrank is simple to build from scratch, and requires no algorithmic tools beyond a sorting function. After rigorously bounding the accuracy, time and space complexities, we evaluated the performance of ESrank on a real SCA data corpus, and compared it to the currently-best histogram-based algorithm. We show that ESrank gives excellent rank estimation (with roughly a 1-bit margin between lower and upper bounds), with a performance that is on-par with the Histogram algorithm: a run-time of under 1 second on a standard laptop using 6.5 MB RAM.

Biography: Liron David is a Ph.D. candidate in Electrical Engineering at Tel-Aviv University under the supervision of Prof. Avishai Wool. She received her B.Sc. degree in Computer Science and Electrical and Electronics Engineering from Tel-Aviv University and her M.Sc. degree in Electrical Engineering from Tel-Aviv University. Liron has won the Weinstein award for excellence in studies in 2017 ,the Weinstein best paper prize in 2018 and the Tel-Aviv University excellence in teaching in 2018.