Para-Hash: Design of universal hash functions suitable for vectorial architectures

Avik Chakraborti · Shibam Ghosh
Cuauhtemoc Mancillas-López · Luis A. Pérez-Sarmiento

April 11, 2025

Abstract

Para-Hash is a novel and efficient construction based on ε-universal hash function following *key-then-hash* parallel paradigm. Its main objective is to take advantage of modern architectures. Offering at the same time a generic and adaptable structure for future platforms.

An ε-universal hash function is one in which the probability that two different messages produce the same output is at most, ε. These functions are particularly useful for the construction of Message Authentication Code (MAC).

Para-Hash is a newly proposed ε-universal hash function designed specifically to exploit to vectorized instructions. It begins by adding a secret key to the input blocks. Each resulting key-masked block is then processed using a block function with very low Maximum Image Probability (MIP) and Maximum Differential Probability (MDP). The block function is designed using two public AES rounds, allowing the construction to take full advantage of vectorized instruction sets available in modern processors, such as AVX on x86 platforms and ARMv8-NEON on ARM architectures. Nowadays, most commercially available processors support vectorized AES instructions. This motivates the development of ε-universal hash functions that are optimized for such instruction sets.

We conducted performance tests to evaluate Para-Hash. All experiments were performed using 4KB messages, and the results were measured in Cycles Per Byte (CPB). The implementation achieved 0.63 CPB on an Intel i7-11700, 1.26 CPB on a Cortex-A76 (Raspberry Pi 5), and 0.59 CPB on a Ryzen 3 4300. Each version was optimized to fully utilize the corresponding vectorized instruction set available on the target architecture.