Column-parity mixing layers

Joan Daemen

Mixing layers, such as MixColumns in the AES, are an essential ingredient of the wide trail strategy. You can find them in the round function of most modern block ciphers and permutations. We study a generalization of the mixing layer in Keccak-f, the permutation underlying the NIST standard SHA-3 and the authenticated encryption schemes Keyak and Ketje. We call this generalization column-parity mixing layers and investigate their algebraic and diffusion properties and implementation cost. We demonstrate their competitiveness by presenting a fully specified 256-bit permutation with strong bounds for differential and linear trails.