World Academy of Science, Engineering and Technology
International Journal of Information and Communication Engineering
Vol:16, No:03, 2022

Search for APN Permutations in Rings □_2×□_2^k

Authors : Daniel Panario, Daniel Santana de Freitas, Brett Stevens

Abstract : Almost Perfect Nonlinear (APN) permutations with optimal resistance against differential cryptanalysis can be found in several domains. The permutation used in the standard for symmetric cryptography (the AES), for example, is based on a special kind of inversion in GF(28). Although very close to APN (2-uniform), this permutation still contains one number 4 in its differential spectrum, which means that, rigorously, it must be classified as 4-uniform. This fact motivates the search for fully APN permutations in other domains of definition. The extremely high complexity associated to this kind of problem precludes an exhaustive search for an APN permutation with 256 elements to be performed without the support of a suitable mathematical structure. On the other hand, in principle, there is nothing to indicate which mathematically structured domains can effectively help the search, and it is necessary to test several domains. In this work, the search for APN permutations in rings ℤ2×ℤ2k is investigated. After a full, exhaustive search with k=2 and k=3, all possible APN permutations in those rings were recorded, together with their differential profiles. Some very promising heuristics in these cases were collected so that, when used as a basis to prune backtracking for the same search in ℤ2×ℤ8 (search space with size 16! □244), just a few tenths of a second were enough to produce an APN permutation in a single CPU. Those heuristics were empirically extrapolated so that they could be applied to a backtracking search for APNs over ℤ2×ℤ16 (search space with size 32! □2117). The best permutations found in this search were further refined through Simulated Annealing, with a definition of neighbors suitable to this domain. The best result produced with this scheme was a 3-uniform permutation over ℤ2×ℤ16 with only 24 values equal to 3 in the differential spectrum (all the other 968 values were less than or equal 2, as it should be the case for an APN permutation). Although far from being fully APN, this result is technically better than a 4-uniform permutation and demanded only a few seconds in a single CPU. This is a strong indication that the use of mathematically structured domains, like the rings described in this work, together with heuristics based on smaller cases, can lead to dramatic cuts in the computational resources involved in the complexity of the search for APN permutations in extremely large domains.

Keywords : APN permutations, heuristic searches, symmetric cryptography, S-box design
Conference Title : ICISC 2022 : International Conference on Information Security and Cryptography
Conference Location : Paris, France
Conference Dates : March 28-29, 2022