COMMENTS AND CORRECTIONS

Comments on “On the Design of
Chaos-Based S-Boxes”

DRAGAN LAMBIĆ
Faculty of Education, University of Novi Sad, 21102 Novi Sad, Serbia
e-mail: dragan.lambic@pef.uns.ac.rs

I. INTRODUCTION
In the above article [1], chaos-based S-box design methods are analyzed in order to reassess the nonlinearity of some previous S-box examples. As a result of the analysis, it is concluded that the majority of cited articles in [1] focus only on the average nonlinearity of S-box coordinates, while remaining S-box components are ignored. On the basis of such analysis, it is concluded that the majority of studies analyzed in [1] should be re-evaluated and used with a considerable caution. However, the analysis in the above article [1] is made based on a major oversight in reviewing previous literature regarding the nonlinearity of S-boxes, which caused a wrong conclusion regarding most of the articles cited in [1].

In Section II of this article, different criteria for measuring the nonlinearity of an S-box are discussed with the aim to point out the oversight made in the analysis from the article [1]. Conclusions of this article are summarized in Section III.

II. S-BOX CRITERIA RELATED TO THE NONLINEARITY
In the above article [1], a major oversight is made in the review and the analysis of the previous references, such as [2]–[4] and many others, because the author failed to see that the MELP criterion used in these articles is equivalent to the “actual” nonlinearity, as it is called in the article [1]. For example, we can see that in the article [3], the formula for the nonlinearity of a single S-box coordinate is given in Section 4.1, while the formula for MELP (or actual nonlinearity, how it is called in the article [1]) is given in Section 4.5. We can easily see that the only difference between sums calculated in both formulas is the letter “b” which enables us to calculate nonlinearities of all combinations of S-box coordinates.

In order to prove that the “actual nonlinearity” is equivalent to the MELP from articles [2]–[4], we need to calculate these values for S-boxes from these articles. The “actual nonlinearity” of S-boxes from articles [2] and [3] is 94, while the S-box from [4] has a value of 104. The value of 94 is the value of a single combination of coordinates of an S-box from [3] which represents the minimal nonlinearity which corresponds to some specific value of b. If we use N(f) = 94 in the formula in Section 4.1. of [3], it is easy to calculate that the value of sum in that formula (in absolute brackets) is equal to 68. If we use that the sum is equal to 68 in the formula in Section 4.5. of article [3], we get L(f) = (68/256)^2 = 0.070556640625 which is the value of the MELP criteria shown in Section 4.5 in [6]. The same value of MELP is obtained in [2], while in [4], the MELP value of 0.03515625 shown in table 11 of that article corresponds to the “actual nonlinearity” of 104.

Based on the previous calculation, it is obvious that the value of the “actual nonlinearity” is equivalent to the MELP and therefore is provided in articles such as [2]–[4].

For this reason, claims stated in [1] that cited articles in [1] focus only on the average nonlinearity of S-box coordinates, while remaining S-box components are ignored and that these articles should be re-evaluated and used with a considerable caution, are not correct because all required measures exist in most of these articles.

In addition, in [1], the differences between random (very fast methods such as the method presented in [4] intended mostly for cryptosystems with dynamical S-boxes) and heuristic S-box design methods (slower but with higher quality) are not taken into the consideration and these two types are compared only in the context of cryptosystems with fixed S-boxes which portray biased picture in favor of heuristic methods.

III. CONCLUSION
Claims from the above article [1] regarding the lack of nonlinearity data of most of the cited articles are not correct because these articles include all required nonlinearity criteria. For this reason, the literature review from the above article [1] should be carefully re-evaluated in order to gain correct picture about existing S-box design methods and their usability in both fixed and dynamical S-box cryptosystems.

REFERENCES
[1] M. M. Dimitrov, “On the design of chaos-based S-boxes,” *IEEE Access*, vol. 8, pp. 117173–117181, 2020.
[2] D. Lambić, “S-box design method based on improved one-dimensional discrete chaotic map,” *J. Inf. Telecommun.*, vol. 2, no. 2, pp. 181–191, Apr. 2018.
[3] D. Lambić, “A novel method of S-box design based on discrete chaotic map,” *Nonlinear Dyn.*, vol. 87, no. 4, pp. 2407–2413, Mar. 2017.
[4] D. Lambić, “A novel method of S-box design based on chaotic map and composition method,” *Chaos, Solitons Fractals*, vol. 58, pp. 16–21, Jan. 2014.

**Digital Object Identifier** 10.1109/ACCESS.2021.3067821