Review of: "WaveBit — Nonbinary Computation: I Symmetric Cryptography"

Behrooz Khadem[1]

1 Imam Hossein University

Potential competing interests: No potential competing interests to declare.

The authors presented an alternative method for symmetric encryption and claimed that it is secure against key discovery attacks and known plaintext attacks. They have also explained their algorithm with an example. The abstract, structure, conclusion, and the use of figures and tables are appropriate, and the problem and related premises are also well stated. It seems that the authors should pay attention to the following points.

1- The resistance of the proposed method against the key discovery attack depends on the size of the key space, which needs to be stated in this case.

2- The resistance of the proposed method against known plaintext attacks should be clearly explained.

3- According to Shannon's principles, a necessary condition for the security of the proposed method is that it should include two distinct parts of diffusion and confusion, which is not discussed.

4- The resistance of the method against other common attacks such as frequency attacks and Kasiski attacks should be checked.

5- Comparison of the proposed method with similar symmetric encryption methods in terms of efficiency, speed, and bandwidth consumption should be investigated.