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

L. V. Kovalchuk[1]

1 National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”

Potential competing interests: No potential competing interests to declare.

<!-- /* Style Definitions */ p.MsoNormal, li.MsoNormal, div.MsoNormal {mso-style-parent:""; margin:0cm; margin-bottom:.0001pt; mso-pagination:widow-orphan; font-size:12.0pt; font-family:"Times New Roman"; mso-fareast-font-family:"Times New Roman";} @page Section1 {size:595.3pt 841.9pt; margin:42.5pt 42.5pt 42.5pt 70.85pt; mso-header-margin:35.4pt; mso-footer-margin:35.4pt; mso-paper-source:0;} div.Section1 {page:Section1;} -->

Review for “WaveBit – Nonbinary Computation…”

This format can't reflect formulas, so I add full reviews in doc and pdf in “Supplementary data”

1. The abstract is very short and does not contain necessary items: the state of the problem, the state of the art, and what the novelty of the proposed results is.

2. The idea of the article seems clear – is it just in replacing “binary basis” with “wave basis”?

If yes, what are the advantages of such replacing? The question about the advantages of the proposed construction is one of the main questions, and it should be highlighted using different numerical comparisons. Why using 7 frequencies to represent 128 Wavebits is better than using 7 positions in the bit vector to represent 128 numbers?

3. There are a lot of typos; the list of some of them is given below.

a) In II. Mathematical aspects, the first paragraph: it should be ”

” instead of ”

”; the same typo is in Example 1 and may be somewhere below.

b) In II. Mathematical aspects, the first paragraph: what are the two arguments of the function

? In the formula in the 3rd row of this part, the dependencies on

are not explained, and neither are the dependencies of delta on its two arguments, which is indirectly meant in the expression

.

b) In Example 1, is

the same as

, which is introduced above? If yes, it's bad practice to define the same value with different letters.

c) In Example 2, I think it should be "

" instead of "

". Anyway, "

" is an incorrect expression.

d) There is confusion with the names of variables in Definition 1. It should be everywhere

instead of

, or everywhere

instead of

, but not to use different names for one variable in the left and right parts of the formula (the same mistakes are in two formulas in this definition).

e) There is confusion with the sums in Definition 1. In the 4^{th} row of the definition, there should be one sum (on

) in the first term, and the other sum (on

) in the second term of the sum, but we see the two sums in the first term and none in the second.

And so on)

3. At the end of Part II, the delta function is introduced. What is the definition of this function? I think it's not the same as the one that was introduced (without explanation) above.

4. Different Algorithms in Part III – do they have inputs/outputs?

5. In the first Algorithm in Part III: “Create the secret key (map) …” – the secret key is a map, really? For what encryption do we use a map as a secret key?

6. In Part IV, in “A. Encoding” – does “Encoding” mean Encryption?

In “B. Decoding” – do “Decoding” and “De-encryption” mean Decryption?

Please use standard terms to avoid misunderstanding.

7. It would be better to extend the Conclusion, specifying the advantages of the proposed approach and giving numerical results for comparison.