Opinion on “Links Between Differential and Linear Cryptanalysis”

This is a very well written thesis on the relations between differential and linear cryptanalysis. Both methods are widely used in cryptography (especially in Symmetric Key Cryptography) and the links between them is an interesting research direction revived recently by Blondeau and Nyberg [7].

Author starts with a good introduction on the topic. In the first few sections he treats the necessary background material in a succint manner. The thesis is rather compact as the author avoids unnecessary material which provides a good read even possibly for the audience stranger to the field.

The main contribution of the paper is the links among the correlation matrix C, matrix of correlation potentials $C^{(2)}$, difference propagation matrix D, incidence matrix P. Author uses a very nice method based on the powerful Discrete Fourier Transform. Although the Discrete Fourier Transform has a lot of power and application areas, it is highly underused in cryptography. This thesis definitely should be praised for its use of the DFT. The author also gives (complete) proofs of previous results which were presented in a less clear fashion.

Finally, the author analyses the equivalence of the above algebraic objects. Although functions having same differential and linear properties are equivalent under a much more general equivalence (called CCZ or code-equivalence, or also extended-affine equivalence) functions with “equivalent” matrices seems to be equivalent under much restricted maps, i.e., $f(x) = g(x + c) + d$. The author also conjectures (but based on data only on very small vector spaces) that this equivalence is best possible.

Apart from the content, the author clearly spent a lot of time on the “appearence” of the thesis as well. There are very few typos and almost no structural problems (a minor criticism: a few concepts used before their definitions). The presentation of the thesis is very well done.

Therefore my opinion on the thesis is very high. I certainly recommend the thesis for acceptance.

Mark (1/Best mark).