Hi TRIFLE Team,

I observe that there are some structural weakness in TRIFLE S-box. This S-box has 4 fixed points:
0 -> 0
5 -> 5
A -> A
F -> F

What is more worrisome is that these fixed points are forming a subspace (U), that is S(U) = U. Having the design where diffusion depends on the bit permutation and there are only a few places where round constants are being added, this makes a perfect stage for mounting invariant subspace attack.

Please let me know if my understanding is not correct.

Thanks
Sumanta