On the Existence of Boolean Functions Resistant Against Non-Linear Invariant Attacks

Nicolas T. Courtois

University College London, Gower Street, London, UK

Recent papers show how to construct polynomial invariant attacks on block ciphers for certain Boolean functions. For example we have proven that:
Theorem 0.1 (A Degree 7 Invariant Attack). If $A, B, C, \ldots$ are 8 polynomials from [1] then (new result not the same as in [1]), let

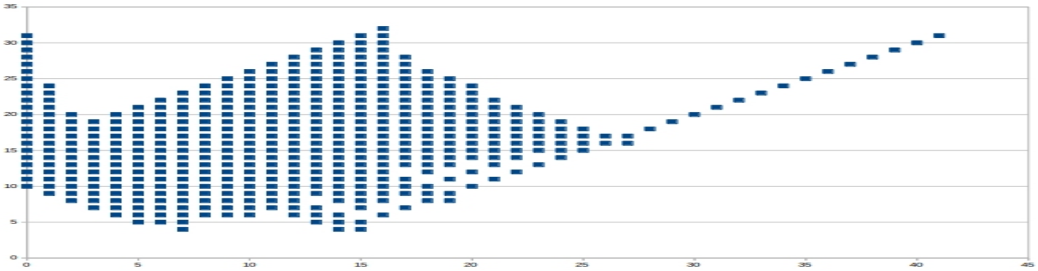
$$\mathcal{P} = (1 + A + H)(B + H)(1 + C + H)(D + H)(E + H)(1 + F + H)(G + H)$$

then assuming a number of technical conditions of the cipher wiring [lack of space] if the Boolean function Z used inside the cipher satisfies:

`(Z+1)*(f+e)(d+a)(b+c)=0     AND     (Z+1)*(f+e+1)(d+a+1)(b+c+1)=0`

then we have $\mathcal{P}(\text{Inputs}) = \mathcal{P}(\text{Outputs})$ for any key and any number of rounds$\square$

A recent paper [1] claims that no Boolean function can resist a similar attack. In fact we are NOT sure that this claim is correct. In this paper we will try to contradict this claim the best we can [or in relative terms] An earlier Thm [cf. Eurocrypt 2003] says that one cannot avoid annihilators of degree 3. However we **can** avoid cubic annihilators of some special form making attacks harder. We are going to show the existence of Boolean functions which seem quite [or more] resistant to such attacks. Success will be measured by the size of the space of long-term keys for which our attack work when Z is fixed. A naive method is by mandating a very low dimension for the annihilator space plus additional criteria. However we show that one cannot have the DimAnn which is too low, or it will degrade the Boolean function so badly that it will become unsuitable for cryptographic applications. One basic fact is shown on the graph below.



On our figure $n = 6$ variables, X axis is the Dim of the annihilator space at degree 3, and $2Y$ is the highest in abs. value coefficient in the Walsh spectrum.

References

1. Nicolas T. Courtois: *Structural Nonlinear Invariant Attacks on T-310: Attacking Arbitrary Boolean Functions*, `https://eprint.iacr.org/2018/1242.pdf`, received 28 Dec 2018.