On the propagation of linear relations through an Sbox

Christina Boura[1,2] and Anne Canteaut[1]

[1] SECRET Project-Team - INRIA Paris-Rocquencourt - B.P. 105
78153 Le Chesnay Cedex - France
[2] Gemalto
6 rue de la Verrerie, 92190 Meudon, France
Christina.Boura@inria.fr, Anne.Canteaut@inria.fr

In several cryptographic primitives, Sboxes are used to provide confusion. The resistance of such Sboxes against several cryptographic attacks, such as linear or differential attacks, has been widely studied. In this work, a different property is investigated.

Definition 1. *Let S be a function from $\mathbf{F}_2^n$ into $\mathbf{F}_2^m$. Then, S is said to be (v, w)-linear if there exist two linear subspaces $V \subset \mathbf{F}_2^n$ and $W \in \mathbf{F}_2^m$ with $\dim V = v$ and $\dim W = w$ such that, for all $\lambda \in W$, S_λ has degree at most 1 on all cosets of V, where S_λ is the Boolean function $x \mapsto \lambda \cdot S(x)$.*

This property is strongly related to the algebraic degree of the coordinates of S, to their non-linearities and also to the notion of (weak)-normality. In particular, if S is (v, w)-linear, then it has w coordinates S_i such that $\deg S_i \leq n + 1 - v$ and $\mathcal{L}(S_i) \geq 2^v$. Moreover, (v, w)-linear Sboxes can be completely characterized in some cases.

We show in the sequel that the use of an Sbox which is (v, w)-linear for some high values of v or of w can introduce a weakness in a symmetric cryptosystem. Let us consider a function F based on the SPN construction where such an Sbox is used in the confusion layer, together with a linear diffusion layer. Then, this property may help find a restriction F' of F, obtained by fixing some input variables, such that several output coordinates of F' have degree 1 on a subspace and all its cosets. This situation can then be exploited for finding preimages of F faster than the generic attack, as shown by Thomas Fuhr in [1] where this algorithm is applied to the compression function of the SHA-3 candidate Hamsi. Here, we show that the attack presented by Thomas Fuhr exploits both the slow diffusion and the fact that one of the coordinates of the 4×4 Sbox is $(3, 1)$-linear, and also that another one is $(2, 1)$-linear. We have searched for all subspaces V such that a coordinate of S is linear on V and all its cosets. By exploiting these properties in a systematic way, we are able to find a higher number of linear relations for the input and the output of the compression function of Hamsi and thus slightly improve the complexity of the attack in [1].

References

1. T. Fuhr. Finding second preimages of short messages for Hamsi-256. In *ASIACRYPT 2010*, volume 6477 of *Lecture Notes in Computer Science*, pages 20–37. Springer, 2010.