Dual of New Method for Upper Bounding the Maximum Average Linear Hull Probability for SPNs

Liam Keliher, Henk Meijer
Dept. Comp. & Info. Science
Queen's University at Kingston
Ontario, Canada, K7L 3N6
{keliher,henk}@cs.queensu.ca

Stafford Tavares
Dept. Electrical & Comp. Engineering
Queen's University at Kingston
Ontario, Canada, K7L 3N6
tavares@ee.queensu.ca

1 Introduction

In [3], we present a new algorithm for computing an upper bound on the *maximum average linear hull probability* (MALHP) for the SPN symmetric cipher structure, a value required to make claims about provable security against linear cryptanalysis. This algorithm improves on existing work in that the resulting upper bound is a function of the number of encryption rounds (other upper bounds known to the authors are not), and moreover, it can be computed for an SPN with any linear transformation layer (the best previous result, that of Hong et. al [4], applies only to SPNs with highly diffusive linear transformations).

It is well known that there exists a duality between linear cryptanalysis and differential cryptanalysis which allows certain results related to one of the attacks to be translated into the corresponding results for the other attack [1, 5]. Since this duality applies to our work in [3], we immediately obtain an algorithm for upper bounding the *maximum average differential probability* (MADP) for SPNs (required to make claims about provable security against differential cryptanalysis).

Note: In what follows, we assume familiarity with the notation and results of [3].

2 Dual Result

The algorithm of [3] is found in Theorem 3 and Theorem 4. To obtain the dual algorithm, two changes are required. The first is to replace the table $W[\,]$ (given in Definition 7 of [3]) with the table $W_{\text{diff}}[\,]$, which is defined for all $\gamma, \hat{\gamma} \in \{0,1\}^M$ as

$$W_{\text{diff}}[\gamma, \hat{\gamma}] \stackrel{\text{def}}{=} \#\left\{\Delta\mathbf{x} \in \{0,1\}^N : \gamma_{\Delta\mathbf{x}} = \gamma,\ \gamma_{\Delta\mathbf{y}} = \hat{\gamma},\ \text{ where } \Delta\mathbf{y} = (\mathbf{L}(\Delta\mathbf{x})')'\right\}$$

(note that relative to [3], the roles of $\mathbf{x}$ and $\mathbf{y}$ are exchanged in the equation $\Delta\mathbf{y} = (\mathbf{L}(\Delta\mathbf{x})')'$, and $\mathbf{L}$ is used in place of $\mathbf{L}'$).

The second change is to replace the value q (defined in (4) of [3]), which is the maximum linear probability over all SPN s-boxes, with the value p, the maximum differential probability over all SPN s-boxes, defined as follows: Let S be a bijective $n \times n$ s-box, let $\Delta\mathbf{x}, \Delta\mathbf{y} \in \{0,1\}^n$, and let

$\mathbf{X} \in \{0,1\}^n$ be a uniformly distributed random variable.

$$DP^S(\Delta\mathbf{x} \to \Delta\mathbf{y}) \stackrel{\text{def}}{=} \text{Prob}\{S(\mathbf{X}) \oplus S(\mathbf{X} \oplus \Delta\mathbf{x}) = \Delta\mathbf{y}\}$$
$$p \stackrel{\text{def}}{=} \max_{S \in \text{SPN}} \max_{\Delta\mathbf{x}, \Delta\mathbf{y} \in \{0,1\}^n \setminus \mathbf{0}} DP^S(\Delta\mathbf{x} \to \Delta\mathbf{y}) \ .$$

3 Best Previous Result for SPNs

As for linear cryptanalysis, the best previous upper bound on the MADP for SPNs is due to Hong et al. [4]—in fact, it is the dual of the upper bound on the MALHP given in [4], and is obtained by interchanging p and q. Again, our dual upper bound is more general, in that it applies to any SPN, whereas that of [4] applies only to those SPNs with highly diffusive linear transformation layers. Also, our dual upper bound is a function of the number of encryption rounds; other upper bounds known to the authors are not.

4 Application to Rijndael (AES)

Application of the above dual result to Rijndael (the AES selection) [2] is simple, since for Rijndael $p = 2^{-6} = q$ and $W_{\text{diff}}[\,]$ is identical to $W[\,]$ for the 128-bit LT (this follows from the fact that $W_{\text{diff}}[\,] = W[\,]$ for the 32-bit MDS LT, which was determined by exhaustive search). Therefore the upper bound on the MADP for Rijndael is identical to the upper bound on the MALHP. A plot of this upper bound is given in Figure 1. Note that for $7 \le T \le 10$, the upper bound value is 2^{-75}.

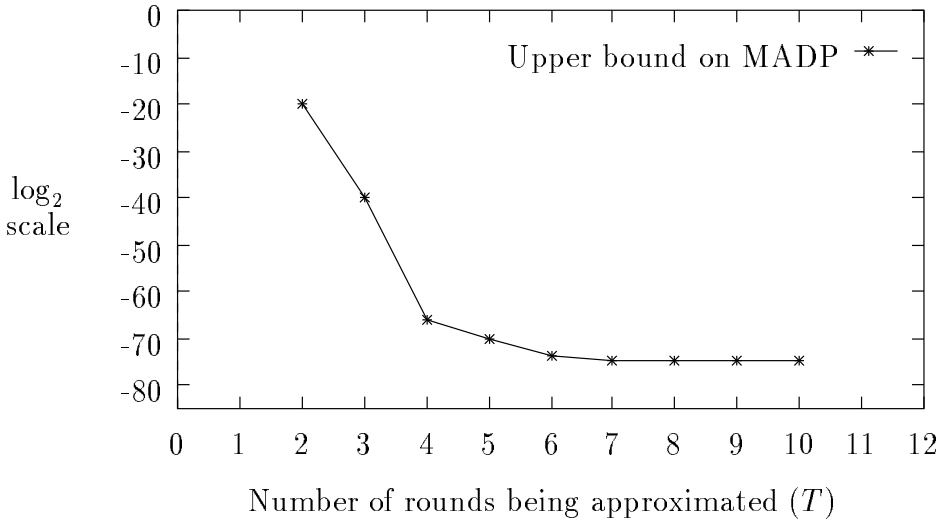

Figure 1: Upper bound on MADP for Rijndael

References

[1] E. Biham, *On Matsui's linear cryptanalysis,* Advances in Cryptology—EUROCRYPT'94, Springer-Verlag, pp. 341–355, 1995.

[2] J. Daemen and V. Rijmen, *AES proposal: Rijndael,* `http://csrc.nist.gov/encryption/aes/round2/AESAlgs/Rijndael/Rijndael.pdf`, 1999.

[3] L. Keliher, H. Meijer, and S. Tavares, *New Method for Upper Bounding the Maximum Average Linear Hull Probability for SPNS,* Advances in Cryptology—EUROCRYPT 2001, LNCS 2045, Springer-Verlag.

[4] S. Hong, S. Lee, J. Lim, J. Sung, and D. Cheon, *Provable security against differential and linear cryptanalysis for the SPN structure,* Fast Software Encryption (FSE 2000), LNCS 1978, Springer-Verlag, 2001.

[5] M. Matsui, *On correlation between the order of s-boxes and the strength of DES,* Advances in Cryptology—EUROCRYPT'94, Springer-Verlag, pp. 366–375, 1995.