Computational aspects of the expected differential probability of 4-round AES and AES-like ciphers

MARIO LAMBERGER, Institute for Applied Information Processing and Communication, TU Graz

Joint work with Joan Daemen, Norbert Pramstaller, Vincent Rijmen and Frederik Vercauteren

Although symmetric key primitives such as block ciphers are ubiquitously deployed throughout all cryptosystems, they do not come with a formal proof of security. This makes a continuous analysis and evaluation a necessity. In 2001, the block cipher Rijndael [2] has become the new *Advanced Encryption Standard (AES)* by NIST. Therefore, it has been subjected to various modern cryptanalytic techniques such as differential cryptanalysis [1, 6] and linear cryptanalysis [7].

In this talk we want to focus on the security of AES against differential cryptanalysis. Provable security against differential cryptanalysis of so called *Substitution-Permutation-Networks* (SPNs) (of which the AES is the most prominent example) has been investigated recently in [4, 5, 9, 10].

The goal of this talk is to show how to improve on the results achieved so far.

A *differential* (cf. [6]) of a function $f : \{0,1\}^n \to \{0,1\}^n$ is a pair $(a, b) \in \{0,1\}^n \times \{0,1\}^n$ such that $f(x) \oplus f(x \oplus a) = b$ for some x. We call a the input difference and b the output difference. The *differential* probability $DP(a, b)$ of a differential (a, b) (with respect to f) is defined as

$$DP(a,b) = 2^{-n} \cdot \#\{x \in \{0,1\}^n \mid f(x \oplus a) \oplus f(x) = b\}.$$

If f is a function parameterized by a key k, we can also define the differential probability $DP[k](a, b)$ in a straight-forward manner.

Then, the *expected differential probability (EDP)* of a differential (a, b) is defined as

$$EDP(a,b) = 2^{-|\mathcal{K}|} \sum_{k \in \mathcal{K}} (DP[k](a,b)),$$

that is, the mean over all keys k where we assume the keys to be uniformly distributed.

Finally, the *maximum expected differential probability (MEDP)* of a differential (a, e) is

$$\max_{a,e \neq \mathbf{0}} EDP(a,e)$$

In order to prove the security of an R-round block cipher against differential cryptanalysis, the standard procedure is to show that the MEDP of T rounds is sufficiently small for certain values of $T \leq R$. It is known from [8] that the effort (the number of known plaintext/ciphertext pairs) for a differential cryptanalytic attack to succeed is proportional to the inverse of the MEDP. From [4, 10] we know that in the case of AES and related SPNs, if p_u is an upper bound for the MEDP of two rounds, p_u^4 is an upper bound for the MEDP of $T \geq 4$ rounds.

Let $B[k](x)$ denote a function composed of R steps $f^i[k](x)$ parameterized by a key k:

$$B[k](x) = (f^R[k] \circ \cdots \circ f^1[k])(x)$$

A *characteristic* through $B[k]$ is a vector $Q = (a, b_1, \ldots, b_R)$ with $a, b_i \in \{0,1\}^n$ for $i = 1, \ldots, R$ such that

$$f^1[k](x) \oplus f^1[k](x \oplus a) = b_1$$

$$\vdots$$

$$(f^R[k] \circ \cdots \circ f^1[k])(x) \oplus (f^R[k] \circ \cdots \circ f^1[k])(x \oplus a) = b_R.$$

A characteristic $Q = (a', b_1, \ldots, b_R)$ is *in* a differential (a, e) if $a' = a$ and $b_R = e$. Then, it is well known from [6] that

$$EDP(a, e) = \sum_{Q \in (a,e)} EDP(Q)$$

and that for so called Markov ciphers, the EDP of a characteristic can be computed as the product of the DPs of the underlying S-boxes. These S-boxes ("substitution boxes") provide for the non-linearity in the design of SPNs. The S-box employed in AES can be described as a mapping $S(x)$ from $GF(2^8)$ to $GF(2^8)$ where

$$S(x) = L^{-1}(x^{-1}) + q.$$

Here, x^{-1} means inversion in $GF(2^8)$ (where additionally, 0 is mapped to 0), L is a $GF(2)$-linear transformation and q is a constant. In the following, we will always consider 8-bit values to be in $GF(2^8) = GF(2)[\theta]/(\theta^8 + \theta^4 + \theta^3 + \theta + 1)$. For the remainder of this extended abstract, we will make use of a slightly simplified function $S(x)$, namely, we take $S(x) = x^{-1}$ in $GF(2^8)$ (with $S(0) = 0$). This has the advantage of exhibiting a nice mathematical structure and is commonly used as an approximation of the real S-box (cf. [3, 4, 10]).

In [3], the AES *super box* was introduced to investigate two rounds of AES. The super box maps $a = [a_0, \ldots, a_3] \in \left(\{0,1\}^8\right)^4$ to $e = [e_0, \ldots, e_3] \in \left(\{0,1\}^8\right)^4$ via a sequence of four transformations:

- **SubBytes** $b_i = S(a_i)$ for $i = 0, \ldots, 3$
- **MixColumns** $c = \mathbf{M} \cdot b$ with $\mathbf{M} \in \mathcal{M}(4 \times 4, GF(2^8))$
- **AddRoundKey** $d = c \oplus k$ with k a 4-byte round key
- **SubBytes** $e_i = S(d_i)$ for $i = 0, \ldots, 3$

Two rounds of AES can be described by four parallel instances of such a super box and it can be seen that the differential probabilities over this structure are equivalent to two rounds of AES.

In this talk, we want to extend the approach outlined in [3] in order to understand the EDP of the simplified super box. Contrary to [4, 9, 10], we are not only interested in the MEDP of the super box (that is, two rounds of AES) but we want to understand the intrinsic structure of the EDP distribution in order to derive a tighter bound on the MEDP over 4 rounds.

Due to the diffusion properties of the matrix $\mathbf{M}$ it can be shown that for the super box, there exist characteristics with 5,6,7, or 8 active S-boxes. Here, active S-box just means that the input difference to the S-box is non-zero.

Let $N_{32}(a, e)$ be the number of 32-bit (simplified super box) characteristics Q in (a, e) having $EDP(Q) > 0$. This number is closely related to the $EDP_{32}(a, e)$, the EDP of (a, e) over the super box.

In the case of 5 active S-boxes, we were able to compute the complete distribution of $EDP_{32}(a, e)$ for $a = (a_0, 0, 0, 0)$ and $e = (e_0, \ldots, e_3)$ via

$$\mathrm{N}_{32}(a, e) = 2^{8-\dim V} - 1,$$

where $V = \{a_0, (\theta e_0)^{-1}, e_1^{-1}, e_2^{-1}, ((1+\theta)e_3)^{-1}\}$ is a vector space over $GF(2)$.

In the case of 6 active S-boxes the problem becomes computationally quite involved, since we get

$$N_{32}(a, e) = \sum_{t \in I} \left(2^{8-\dim V(t)} - 1\right),$$

where the vector space $V(t)$ is defined for $a = (1, a_1, 0, 0)$ and $e = (e_0, \ldots, e_3)$ by

$$V(t) = \{1, (ta_1)^{-1}, ((\theta + (1+\theta)t)e_0)^{-1}, ((1+\theta t)e_1)^{-1}, ((1+t)e_2)^{-1}, (((1+\theta)+t)e_3)^{-1}\}$$

and $t \in I = GF(2^8) \setminus \{0, 1, 1+\theta, \theta^{-1}, \theta(1+\theta)^{-1}\}$. This additional parameter t comes into play because of the sixth active S-box.

We will show methods how to compute bounds for $EDP_{32}(a,e)$ for such a 6-box differential (a,e) of the form:

$$1.60469 \cdot 2^{-130} \leq \sum_{e_0,\ldots,e_3} (\mathrm{N}_{32}(a,e) \cdot 2^{-42}))^5 \leq 1.58991 \cdot 2^{-124}$$

References

[1] Eli Biham and Adi Shamir, *Differential Cryptanalysis of DES-like Cryptosystems*, CRYPTO (Alfred Menezes and Scott A. Vanstone, eds.), Lecture Notes in Computer Science, vol. 537, Springer, 1990, pp. 2–21.

[2] Joan Daemen and Vincent Rijmen, *The Design of Rijndael: AES - The Advanced Encryption Standard*, Springer, 2002.

[3] ______, *Understanding Two-Round Differentials in AES*, SCN (Roberto De Prisco and Moti Yung, eds.), Lecture Notes in Computer Science, vol. 4116, Springer, 2006, pp. 78–94.

[4] Seokhie Hong, Sangjin Lee, Jongin Lim, Jaechul Sung, Dong Hyeon Cheon, and Inho Cho, *Provable Security against Differential and Linear Cryptanalysis for the SPN Structure*, FSE (Bruce Schneier, ed.), Lecture Notes in Computer Science, vol. 1978, Springer, 2000, pp. 273–283.

[5] Liam Keliher, *Refined Analysis of Bounds Related to Linear and Differential Cryptanalysis for the AES*, AES Conference (Hans Dobbertin, Vincent Rijmen, and Aleksandra Sowa, eds.), Lecture Notes in Computer Science, vol. 3373, Springer, 2004, pp. 42–57.

[6] Xuejia Lai, James L. Massey, and Sean Murphy, *Markov Ciphers and Differential Cryptanalysis*, Advances in cryptology—EUROCRYPT '91 (Brighton, 1991), Lecture Notes in Comput. Sci., vol. 547, Springer, Berlin, 1991, pp. 17–38. MR MR1227793

[7] Mitsuru Matsui, *Linear Cryptoanalysis Method for DES Cipher*, EUROCRYPT, 1993, pp. 386–397.

[8] Kaisa Nyberg and Lars R. Knudsen, *Provable security against a differential attack*, J. Cryptology **8** (1995), no. 1, 27–37.

[9] Sangwoo Park, Soo Hak Sung, Seongtaek Chee, E-Joong Yoon, and Jongin Lim, *On the Security of Rijndael-Like Structures against Differential and Linear Cryptanalysis*, ASIACRYPT (Yuliang Zheng, ed.), Lecture Notes in Computer Science, vol. 2501, Springer, 2002, pp. 176–191.

[10] Sangwoo Park, Soo Hak Sung, Sangjin Lee, and Jongin Lim, *Improving the Upper Bound on the Maximum Differential and the Maximum Linear Hull Probability for SPN Structures and AES*, FSE (Thomas Johansson, ed.), Lecture Notes in Computer Science, vol. 2887, Springer, 2003, pp. 247–260.