Completion of Computation of Improved Upper Bound on the Maximum Average Linear Hull Probability for Rijndael

Liam Keliher[1], Henk Meijer[2], and Stafford Tavares[3]

[1] Department of Mathematics and Computer Science
Mount Allison University, Sackville, New Brunswick, Canada, E4L 1E6
lkeliher@mta.ca
[2] School of Computing
Queen's University at Kingston, Ontario, Canada, K7L 3N6
henk@cs.queensu.ca
[3] Department of Electrical and Computer Engineering
Queen's University at Kingston, Ontario, Canada, K7L 3N6
tavares@ee.queensu.ca

Abstract. This report presents the results from the completed computation of an algorithm introduced by the authors in [11] for evaluating the provable security of the AES (Rijndael) against linear cryptanalysis. This algorithm, later named KMT2, can in fact be applied to any SPN [8]. Preliminary results in [11] were based on 43% of total computation, estimated at 200,000 hours on our benchmark machine at the time, a Sun Ultra 5. After some delay, we obtained access to the necessary computational resources, and were able to run the algorithm to completion. In addition to the above, this report presents the results from the dual version of our algorithm (KMT2-DC) as applied to the AES.

Keywords: Rijndael, AES, SPN, provable security, linear cryptanalysis, differential cryptanalysis

1 Introduction

The *substitution-permutation network* (SPN) [4] is a fundamental block cipher architecture that has been widely studied, and that serves as the basis for a number of important ciphers, most notably the Advanced Encryption Standard (AES) [3] (originally named *Rijndael*). SPNs have been analyzed in terms of their resistance to a large collection of attacks, the most powerful of which are generally considered to be linear cryptanalysis [13] and differential cryptanalysis [1]. In addition, various theoretical and statistical results have demonstrated that certain properties of SPNs converge to the corresponding properties of the *true random cipher* [14] with an increasing number of rounds [2, 5, 12].

Since 2000, several papers have appeared dealing with the *provable security* [15, 16] of SPNs against linear and differential cryptanalysis [6, 7, 9–11, 17–19]. The focus of all these results is to obtain an upper bound on the *maximum* *average linear hull probability* (MALHP) (for linear cryptanalysis) and/or the *maximum expected differential probability* (MEDP) (for differential cryptanalysis), for T core encryption rounds. Most of these results have been applied to the AES, producing a series of successively tighter upper bounds (see [8] for a survey). The authors' algorithm in [9] (now called KMT1) and its dual version in [10] (KMT1-DC) yielded an upper bound of 2^{-75} on the MALHP and MEDP, respectively, for $T \geq 7$ AES rounds—these results established the provable security of the AES against linear and differential cryptanalysis. (The data complexity of each attack is lower bounded by a value that is roughly proportional to the inverse of the relevant upper bound.)

In [11], the authors published an improved algorithm (now called KMT2) for upper bounding the MALHP; the dual version (KMT2-DC) is discussed in Appendix A of [8]. The KMT2 algorithm yielded an upper bound of 2^{-92} on the MALHP for $T \geq 9$ AES rounds. However, only 43% of the computation had completed at the time of publication, out of a total 200,000 hours on a benchmark Sun Ultra 5. The authors stated in [11] that the completed results would be posted on the IACR ePrint Archive, hence the current report.

At the time of this writing, KMT1/KMT1-DC and KMT2/KMT2-DC are the only completely general algorithms for evaluating the provable security of SPNs against linear and differential cryptanlysis—they can be applied to any SPN, and they compute an upper bound that is a function of the number of core encryption rounds being approximated. In contrast, other approaches compute an upper bound that is independent of the number of rounds under consideration, and many assume the use of a particular linear transformation structure.

2 Results from KMT2 as Applied to the AES

The completed results from the application of KMT2 to the AES are given in Table 1. These values are presented in graphical form in Figure 1, where they are contrasted with the results from the KMT1 algorithm. Note that the upper bound for $T = 9$ ($2^{-92.4}$) is marginally tighter than the preliminary value reported in [11] (2^{-92}).

3 Results from KMT2-DC as Applied to the AES

The results from the application of KMT2-DC to the AES are given in Table 2. These are also presented in graphical form in Figure 2, where they are contrasted with the results from KMT1-DC. As noted in [10], KMT1 and KMT1-DC yield identical upper bound values for the AES. However, the values from KMT2-DC are tighter than the values from KMT2 for $2 \leq T \leq 14$. This is due to the difference between the distribution of values in the linear probability table and the distribution of values in the differential probability table for the AES s-box.

Number of rounds (T)	Upper bound from KMT2	Number of rounds (T)	Upper bound from KMT2
1	–	9	$2^{-92.4}$
2	$2^{-22.6}$	10	$2^{-94.0}$
3	$2^{-40.0}$	11	$2^{-95.2}$
4	$2^{-80.8}$	12	$2^{-96.2}$
5	$2^{-83.4}$	13	$2^{-97.0}$
6	$2^{-84.7}$	14	$2^{-97.8}$
7	$2^{-87.0}$	15	$2^{-98.4}$
8	$2^{-90.6}$	16	$2^{-99.0}$

Table 1. Upper bound from KMT2 for the AES

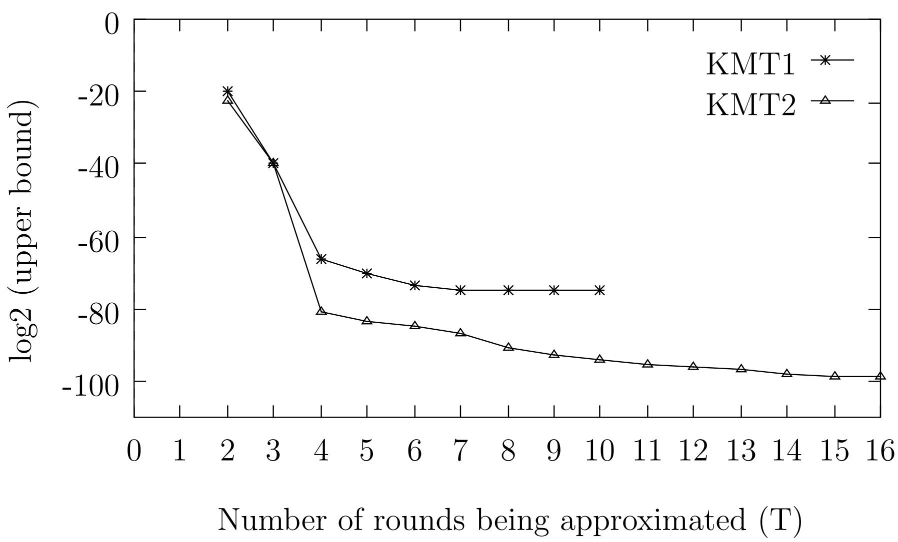

Fig. 1. Upper bounds from KMT1 and KMT2 for the AES

4 Computational Issues

We realized a significant speedup when we moved our computations to faster (Intel-based) workstations. On our new benchmark machine, a 2.8 GHz Pentium 4 (Dell Optiplex GX260, Red Hat Linux 9, Intel C++ Compiler 7.1), KMT2 as applied to the AES required approximately 12,000 hours of computation time (roughly 16 months). Application of KMT2-DC to the AES required approximately 7000 hours of computation time. Although KMT2 and KMT2-DC are essentially the same algorithm, the reduced running time of KMT2-DC is due to the simplistic distribution of values in the differential probability table for the AES s-box.

Number of rounds (T)	Upper bound from KMT2-DC	Number of rounds (T)	Upper bound from KMT2-DC
1	–	9	$2^{-95.1}$
2	$2^{-24.0}$	10	$2^{-96.1}$
3	$2^{-42.0}$	11	$2^{-96.6}$
4	$2^{-88.6}$	12	$2^{-97.1}$
5	$2^{-89.5}$	13	$2^{-97.5}$
6	$2^{-90.7}$	14	$2^{-97.6}$
7	$2^{-92.5}$	15	$2^{-97.7}$
8	$2^{-93.9}$	16	$2^{-97.8}$

Table 2. Upper bound from KMT2-DC for the AES

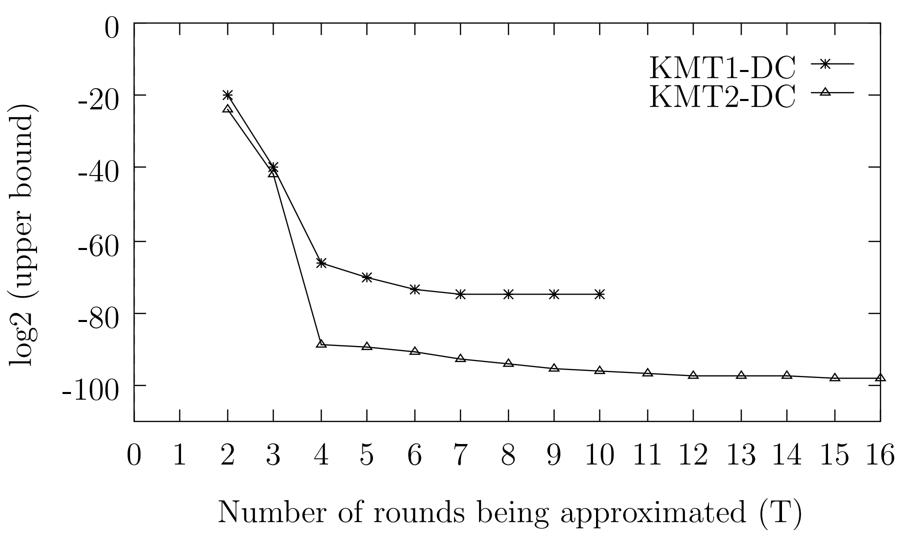

Fig. 2. Upper bounds from KMT1-DC and KMT2-DC for the AES

Acknowledgement

Much of the computation involved in this research was carried out on the Mount Allison Cluster for Advanced Research (`www.mta.ca/torch`) and the High Performance Computing Virtual Laboratory (`www.hpcvl.org`).

References

1. E. Biham and A. Shamir, *Differential cryptanalysis of DES-like cryptosystems,* Journal of Cryptology, Vol. 4, No. 1, pp. 3–72, 1991.
2. Z.G. Chen and S.E. Tavares, *Towards provable security of substitution-permutation encryption networks,* Fifth Annual International Workshop on Selected Areas in Cryptography (SAC'98), LNCS 1556, pp. 43–56, Springer-Verlag, 1999.
3. J. Daemen and V. Rijmen, *The Design of Rijndael: AES—The Advanced Encryption Standard,* Springer-Verlag, 2002.
4. H. Feistel, *Cryptography and computer privacy,* Scientific American, Vol. 228, No. 5, pp. 15–23, May 1973.
5. H.M. Heys and S.E. Tavares, *Avalanche characteristics of substitution-permutation encryption networks,* IEEE Transactions on Computers, Vol. 44, No. 9, pp. 1131–1139, September 1995.
6. 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, pp. 273–283, Springer-Verlag, 2001.
7. J.-S. Kang, S. Hong, S. Lee, O. Yi, C. Park, and J. Lim, *Practical and provable security against differential and linear cryptanalysis for substitution-permutation networks,* ETRI Journal, Vol. 23, No. 4, December 2001.
8. L. Keliher, *Linear cryptanalysis of substitution-permutation networks,* Ph.D. Thesis, Queen's University, Kingston, Canada, 2003.
9. 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, pp. 420–436, Springer-Verlag, 2001.
10. L. Keliher, H. Meijer, and S. Tavares, *Dual of new method for upper bounding the maximum average linear hull probability for SPNs,* Technical Report, IACR ePrint Archive (`http://eprint.iacr.org`, Paper # 2001/033), 2001.
11. L. Keliher, H. Meijer, and S. Tavares, *Improving the upper bound on the maximum average linear hull probability for Rijndael,* Eighth Annual International Workshop on Selected Areas in Cryptography (SAC 2001), LNCS 2259, pp. 112–128, Springer-Verlag, 2001.
12. L. Keliher, H. Meijer, and S. Tavares, *Toward the true random cipher: On expected linear probability values for SPNs with randomly selected s-boxes,* chapter in Communications, Information and Network Security, V. Bhargava, H. Poor, V. Tarokh, and S. Yoon (Eds.), pp. 123-146, Kluwer Academic Publishers, 2003.
13. M. Matsui, *Linear cryptanalysis method for DES cipher,* Advances in Cryptology—EUROCRYPT'93, LNCS 765, pp. 386–397, Springer-Verlag, 1994.
14. A.J. Menezes, P.C. van Oorschot, and S.A. Vanstone, *Handbook of Applied Cryptography,* CRC Press, 1997.
15. K. Nyberg, *Linear approximation of block ciphers,* Advances in Cryptology—EUROCRYPT'94, LNCS 950, pp. 439–444, Springer-Verlag, 1995.
16. K. Nyberg and L. Knudsen, *Provable security against a differential attack,* Journal of Cryptology, Vol. 8, No. 1, pp. 27–37, 1995.

17. S. Park, S.H. Sung, S. Chee, E-J. Yoon, and J. Lim, *On the security of Rijndael-like structures against differential and linear cryptanalysis,* Advances in Cryptology—ASIACRYPT 2002, LNCS 2501, pp. 176–191, Springer-Verlag, 2002.
18. S. Park, S.H. Sung, S. Lee, J. Lim, *Improving the upper bound on the maximum differential and the maximum linear hull probability for SPN structures and AES,* Fast Software Encryption (FSE 2003), LNCS 2887, pp. 247–260, Springer-Verlag, 2003.
19. F. Sano, K. Ohkuma, H. Shimizu, and S. Kawamura, *On the security of nested SPN cipher against the differential and linear cryptanalysis,* IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E86-A, No. 1, pp. 37–46, 2003.