Answer to "new observations on Rijndael"

Joan Daemen Vincent Rijmen

August 11, 2000

1 Introduction

The note [1] presents an interesting view on alternative representations of the Rijndael structure. The application of mathematical techniques is refreshing. The purpose of this reply is to clarify that the observations made do not contradict the security claims we made. While we are sure that the authors are fully aware of the merits and limitations of their results, we feel that a less experienced reader might easily draw wrong conclusions.

From the beginning, our design strategy was to use as simple as possible components, to define clear evaluation criteria, and to use simple components with easily provable properties where possible.

This paper is organised as folows. We start in Section 2 with a few comments on the used terminology. In Section 3 we restate our evaluation criterium for 'diffusion' and show that the results of [1] compare to it. In Section 4 we explain the advantages of using simple components, with provable properties. In Section 5 we explain the advantages of using a simple structure. This is illustrated with an analysis of the DES that contradicts the results of [1].

2 Block ciphers versus block cipher components

The authors of [1] claim to discuss unusual properties for the block cipher, that hold for *any* number of rounds. However, they study the *linear* components of the round only. Therefore, it is equally valid to state that the results hold for a **fraction of one round** only: in the real cipher, applications of the linear layer are alternated with applications of the nonlinear layer. Since the authors cannot extend their results over a nonlinear layer, they do not study even a single round.

We think it is good practice to study the individual components of a cipher, but one should be careful when drawing conclusions about the cipher's security, because the cipher's security is based on an interaction of the components. As an illustration: for most ciphers, it holds that if you take out all components except for the key addition, the cipher will become an involution. "Any input text is mapped to itself after at most two iterations of the key addition." This property holds for any number of rounds. Nevertheless, most designers still use a simple key addition, because despite this 'unusual property', it fulfills its function: in combination with the other block cipher components, it can make the cipher resistant to cryptanalysis.

3 Properties of the diffusion layer

The note [1] questions the suitability of Rijndael's diffusion layer, because 16 applications of the linear mapping gives the identity mapping. We restate here that we defined 'diffusion' as the minimum number of active S-boxes in a linear or differential characteristic. The observed property may be untuitively unsettling, but has no impact on the number of active S-boxes. Our definition for 'diffusion' is based on extensive experience with block cipher cryptanalysis: almost all known cryptanalytic attacks have a complexity that depends on the number of active S-boxes and the input/output correlation of individual S-boxes.

Secondly, the authors find input differences for a differential that make "only" 12 S-boxes active. This should be understood as 12 S-boxes *per round*. Since our own security claims are based on the (provable) lower bound of 25 S-boxes for every 4 rounds, a structure with 12 active S-boxes per round does not appear to be threatening to the security. Note that for the DES, there are many differential characteristics with only 3 active S-boxes for every 2 rounds.

Another remark of the authors is the existence of 2^{16} so-called parity check equations over the linear mapping. It should not surprise many readers that such equations can be found over a linear mapping. Indeed, it is exactly the function of the nonlinear layer to destroy these properties.

The fact that the matrix describing the linear diffusion layer can be brought to a simple form by means of a change of basis, as described in the note, is a very basic theorem of linear algebra. However, when a cryptanalyst wants to use this simple matrix in an attack, he has to take into consideration the effect of this change of basis on the nonlinear layer as well: a change of basis in $\mathrm{GF}(2)^{128}$ will transform the neat 16 parallel instances of the S-box into one huge S-box with 128 inputs, thus making further analysis non-trivial. It remains to be seen whether this technique —which is by the way applicable to *all* block ciphers– can lead to results on a block cipher, or even a block cipher reduced to a small number of rounds.

In short, the authors of [1] list several properties of the diffusion layer, but fail to show any impact on the cipher's security.

4 The use of simple components

In the Rijndael design, we opted to use simple components, with properties that can be proven and verified very easily. Our documentation includes proofs (or references) for any security result that we claim. E.g., the linear diffusion layer results in provable lower bounds on the number of active S-boxes; the S-boxes have provable lower bounds for the nonlinear order, the difference to linear functions, and the resistance to linear and differential cryptanalysis [2].

The advantage of using simple components becomes perhaps more clear when one considers the problems experienced by the other design teams: both the Serpent design team and the MARS design team did not produce S-boxes that are in accordance with their own design criteria [3, 4]; the key dependent S-boxes of Twofish have made it apparently very difficult to determine the security of the cipher [5].

5 The use of a simple structure

Rijndael has an easily understandable mathematical structure, that can easily be split in its components. This property should not be confused with the question whether it can easily be broken. Exactly because of Rijndael's 'rich algebraic structure', the cipher's security can more easily be assessed in the limited time frame available, compared to other designs that require a lot of thinking and searching "where all the bits go".

As an example of the fact that more complicated structures usually have the same (but somewhat hidden) properties as simple structures, we had a closer look at the results of Section 3.3 in [1]: 'Comparison with DES'. This example also serves to illustrate the limitations of the used analysis technique and the care one has to apply when drawing conclusions.

In [1], the diffusion properties of the DES are studied by taking out the expansion and the S-boxes, as defined in the usual way. However, also for the DES, a cryptanalyst can benefit from using other representations. In the definition of the S-boxes of the DES, we can arbitrarily reorder the output bits of individual S-boxes. Provided we compensate for this reordering adequately in the definition of the permutation P, the final results will be equal. The reordering of the output bits of S-box i can be represented by a permutation l_i. Denoting the combination of the eight l_i permutations with $L_{1...8}$, we get:

$$\begin{aligned} P \circ S_{1...8} &= (P \circ L_{1...8}^{-1}) \circ (L_{1...8} \circ S_{1...8}) \\ &= P' \circ S'_{1...8} \end{aligned}$$

This representation for the DES is equally valid as the original one.

Now, in a subsequent step, we can apply the same technique as in [1] for the 'diffusion analysis' of the DES: we leave out the expansion and the S-boxes, concentrating on P' and the Feistel Structure. The *surprising* result of this exercize is that for a suitable choice of L, the diffusion layer of the DES will give the identity after only 12 applications (instead of 1020, as in [1]). For completeness, we give this choice of L in the Appendix. Note that we expect it is possible to get this number down to 8 applications only, but the search can no longer be done by hand.

There are two conclusions to be drawn here:

1. Also for complicately interwoven designs like the DES, 'unusual' properties can be determined, but

2. these unusual properties are no sign of inherent weaknesses in the design.

6 Conclusion

Rijndael is a cipher with a simple and elegant structure. It shows an adequate security margin against cryptanalytic attacks, not only against linear and differential cryptanalysis, as remarked in [1, p. 3, Section 3], but also against 'more opportunistic attacks' [7, 8, 9, 10].

Some people argue that an encryption algorithm should not only produce output without apparent structure, but should also hide its own structure by using complex components. This approach is different from ours. This difference in approach by itself should not be seen as a weakness of a design.

References

[1] S. Murphy, M. Robshaw. New observations on Rijndael, version of August 7, 2000. Available from URL: http://isg.rhbnc.ac.uk/mrobshaw .

[2] K. Nyberg. Differentially uniform mappings for cryptography. Proceedings of Eurocrypt '93, LNCS 765, Springer-Verlag, 1994, pp. 55–64.

[3] L. Burnett, G. Carter, E. Dawson, W. Millan. Efficient methods for generating MARS-like S-boxes. Presented at FSE2000.

[4] T. Shimoyama. The nonlinear order of the Serpent S-boxes. Presented at the recent result session of AES2.

[5] The Twofish Team. A Second Twofish Retreat. Presented at the recent result session of AES3.

[6] *Data Encryption Standard,* Federal Information Processing Standard (FIPS), Publication 46, National Bureau of Standards, U.S. Department of Commerce, Washington D.C., January 1977.

[7] The Twofish Team. Improved cryptanalysis of Rijndael. Presented at FSE2000.

[8] S. Lucks. Attacking 7 rounds of Rijndael under 192-bit and 256-bit keys. Presented at AES3.

[9] H. Gilbert, M. Minier. A collision attack on 7 rounds of Rijndael. Presented at AES3.

[10] M. Sugita, K. Kobara, K. Uehara, S. Kubota, H. Imai. Relationships among differential, truncated differential, impossible differential cryptanalyses against word-oriented block ciphers like Rijndael, E2. Presented at AES3.

A An equivalent representation of the DES that appears to have unusual properties

We give the 8 bit permutations, using the same notation as in [6].

$$
\begin{array}{lcccc}
l_1^{-1}: & 2 & 1 & 3 & 4 \\
l_2^{-1}: & 4 & 1 & 2 & 3 \\
l_3^{-1}: & 3 & 4 & 2 & 1 \\
l_4^{-1}: & 4 & 1 & 3 & 2 \\
l_5^{-1}: & 4 & 1 & 2 & 3 \\
l_6^{-1}: & 1 & 2 & 4 & 3 \\
l_7^{-1}: & 4 & 2 & 3 & 1 \\
l_8^{-1}: & 4 & 1 & 2 & 3
\end{array}
$$

The reader can verify that $P \circ L^{-1}$ has one cycle of order 2 and 10 cycles of order 3. Together with the Feistel structure, this results in an order of 12 for the linear diffusion. Probably, there exists L mappings with cycles of order 4 only, which would give the linear diffusion order 8.