Further Comments on the Structure of Rijndael

Sean Murphy and Matt Robshaw
Information Security Group, Royal Holloway,
University of London, Egham, Surrey, TW20 0EX, U.K.
S.P.Murphy@rhbnc.ac.uk mrobshaw@supanet.com

Preliminary Draft

17 August, 2000

1 Introduction

In a note titled *New observations on Rijndael* [3] we presented the results of an investigation into the diffusion layer of one of the AES finalists Rijndael [1]. The designers of Rijndael then provided a response entitled *Answer to "new observations on Rijndael"* [2]. In this short note we take the opportunity to respond to the criticisms that were levelled at our original posting.

It is important to recognise that our original note gives details of some surprising structural observations on Rijndael, nothing more. However we feel that it is also important to recognise that the level of algebraic structure in Rijndael is unequalled by any of the other AES finalists. Thus we feel that our observations are more than merely being an "alternative representation of the Rijndael structure".

2 Summary of observations

Here we summarise the main results from our original note [3]. Recall that Rijndael consists of 16 parallel, byte-wise S-box transformations, a linear mixing layer across the block, and a key-addition layer.

The S-box (as described in [1]) consists of three components. A transformation $x \to x^{-1}$, the use of a linear transformation (which provides some additional mixing within the byte since $x \to x^{-1}$ is algebraically simple [1]), and the addition of a constant (which is intended to remove fixed points [1]). Our observations are merely these.

1. The additive constant in the original S-box can be viewed as a component of a modified key schedule. The constant was chosen so that the S-Box had

no fixed and no "opposite fixed" points [1]. Thus, by itself, in re-writing Rijndael it is not clear that this stated design aim has been satisfied.

2. The linear transformation that was presented as the second component of the S-box can now be viewed as part of the linear diffusion layer instead. We feel that this yields a more natural presentation of Rijndael, which is given below.

   - *S-box Layer.* The entirety of the non-linear operations are presented in one algebraically simple layer (the 16 parallel mappings $x \to x^{-1}$)
   - *Linear Diffusion Layer.* All other transformations not involving subkeys (including all interaction between the S-boxes) are presented in an augmented linear layer.
   - *Subkey Layer.* The addition of subkey.

3. The augmented linear layer M is **very** structured ($M^{16} = I$).

   - It should be expected that any structure sufficient enough to give $M^{16} = I$ will also have considerable structure over a single iteration of M.
   - The open question, therefore, is how this structure manifests itself over a single iteration of M, and how this structure interacts with the other parts of the cipher.
     - A simple example of the insight that such an analysis of M yields is that for any key, Rijndael encryption is always an even permutation on the set of input blocks.

3 Response to specific comments in [2]

Here we list what seem to be the main statements in [2].

1. *For most ciphers it holds that if you take out all components except for the key addition the cipher will become an involution.* (The implication being that this operation has exponent two yet we still use it without worry.)

   - Every component has its function. A simple key addition layer like the one just described is typically not designed to provide diffusion. Thus we are not concerned that it has order two. Similarly, we are not criticising the linear diffusion layer of Rijndael because it does not introduce any secret key information. However, the linear diffusion layer in Rijndael is there to provide the **only** interaction between the S-boxes from one round to the other.

2. *A structure with 12 active S-boxes per round does not appear to be threatening to security.*

    - The case of 12 active S-boxes was offered as an example of how there are inputs to the diffusion layer that are not "diffused". Likewise there are large sets of inputs that are only mapped to themselves by the linear diffusion in Rijndael.

3. *It should not surprise many readers that such equations [parity checks] can be found over a linear mapping.*

    - It is the fact that so many of these parity equations are fixed across the only diffusive component in Rijndael that is interesting. It is trivial to specify very simple diffusion matrices that do not have this property.

4. *The fact that the matrix can be brought to a simple form by means of a change of basis, ..., is a very basic theorem of linear algebra.*

    - It is true that we have used a very basic theorem of linear algebra. The surprise is not that we have used the theorem, but rather the exceptionally simple form of the matrix that is derived.

5. *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.*

    - The reason to change basis between matrices is to show the structure within the corresponding linear map more clearly. The simpler form R reveals much of the inner structure of M. It is not the intention to use R instead of M.

6. *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.*

    - This technique is particularly applicable to block ciphers that rely on a layer of linear diffusion.

3.1 The comparison with DES

Daemen and Rijmen [2] give an alternative representation of DES in which the linear diffusion layer is particularly simple (as we crudely measure it by exponent). They claim that the exponent of this alternative linear diffusion layer is 12 in comparison to the exponent for the linear diffusion layer of Rijndael of 16. In fact the exponent of the alternative linear diffusion given in [2] appears to be 30. However, the point being made is a valid one. There are indeed many

equivalent representations of DES that may be obtained by linearly transforming the outputs of the DES S-boxes.

The representation we chose to use for Rijndael was one in which the S-Box was as algebraically simple as possible and all other components of Rijndael (and arguably all the accessible diffusive components) were moved into the augmented diffusion layer. This representation into naturally coherent layers actually makes the linear diffusion more complicated than in the original specification (which has exponent 8) and yet it remains remarkably simple with exponent 16.

We feel it would be a mistake to let our comparison with DES detract from our comments on Rijndael. As we repeatedly stated [3], we believe that the comparison with DES is over-simplistic. In particular, it took no account of the role of the expansion function in DES for providing diffusion, a function for which there is no parallel in Rijndael.

4 Conclusions

Clearly it is a question of interpretation, but we do find it surprising that a linear diffusion layer that is intended to "guarantee high diffusion over multiple rounds" fixes so many inputs and sets. Our conclusion remains unchanged from before [3].

> The consequences described in this note [3] are ones that immediately come to mind and demonstrate the structure in the linear diffusion layer. Even if these particular properties offer little advantage to conventional differential and linear cryptanalysis, it remains an open question whether the cryptanalyst can find a more novel way to combine the rich structure in the diffusion layer of Rijndael with the highly structured inverse map.

References

[1] J. Daemen and V. Rijmen. AES Proposal: Rijndael. Version 2. 1999. Available via `csrc.nist.gov/aes/`.

[2] J. Daemen and V. Rijmen. Answer to "new observations on Rijndael". August 11, 2000. Available via `csrc.nist.gov/aes/`.

[3] S. Murphy and M. Robshaw. New observations on Rijndael. August 7, 2000. Available via `csrc.nist.gov/aes/`.