The Round Functions of RIJNDAEL Generate the Alternating Group

Ralph Wernsdorf

Rohde & Schwarz SIT GmbH, Agastraße 3,
D-12489 Berlin, Germany
Ralph.Wernsdorf@SIT.rohde-schwarz.com

Abstract. For the block cipher RIJNDAEL with a block length of 128 bits group theoretic properties of the round functions are derived. Especially it is shown that these round functions generate the alternating group.
Keywords. RIJNDAEL, permutation groups.

1 Introduction

The RIJNDAEL algorithm with a block length of 128 bits is a block cipher that was selected for a NIST standard [4] in the AES selection process. It was developed by J. Daemen and V. Rijmen [1].

In the following a proof is given that the round functions of RIJNDAEL with a block length of 128 bits generate the alternating group over the set $\{0,1\}^{128}$ of all 128-bit-vectors.

This result implies that from the algebraic point of view some thinkable weaknesses of RIJNDAEL can be excluded (if the generated group were smaller, then this would point to regularities in the algorithm, see for example [2], [5], [9]).

Similar properties are known for the DES ([6]) and for SAFER++ ([7]).

2 Definitions and Notations

The notation of the RIJNDAEL round function components will be similar to the RIJNDAEL definition given in [1]. One exception will be that the states are not given in a matrix form. They are given as 128-bit- or 16-byte-vectors, where the correspondence to the matrices in [1] is defined row by row from left to right. The round functions R_k are defined by

$$\forall k \in \{0,1\}^{128}\ \forall x \in \{0,1\}^{128} : R_k(x) := k \oplus mc(rs(s(x))),$$

where	"$\oplus$"	denotes the bitwise XOR-operation,
	$k \in \{0,1\}^{128}$	denotes the corresponding round subkey,
	$mc : \{0,1\}^{128} \to \{0,1\}^{128}$	denotes the *MixColumn*-transformation according to [1], p. 12,
	$rs : \{0,1\}^{128} \to \{0,1\}^{128}$	denotes the *ShiftRow*-transformation according to [1], p. 11,
	$s : \{0,1\}^{128} \to \{0,1\}^{128}$	denotes the application of the S-box S 16 times in parallel (the *ByteSub*-transformation, [1], p. 11).

The permutation group considered here is defined by:

$$G := \langle \{R_k : \{0,1\}^{128} \to \{0,1\}^{128} \mid k \in \{0,1\}^{128}\} \rangle,$$

where $\langle P \rangle$ denotes the closure of a permutation set P with respect to concatenation. The generating set of G given above contains 2^{128} permutations. Properties of the round subkeys caused by the key scheduling will be neglected here.

3 Some Properties of the Generated Group

Lemma 1. *The group G is transitive on the set $\{0,1\}^{128}$.*

Proof. By concatenations $R_k \circ R_{k'}^{-1}$ (where the transformation with k' is carried out at first) with suitable round subkeys k, k', each given element x of the set $\{0,1\}^{128}$ can obviously be transformed to each other arbitrarily given element x' of the set $\{0,1\}^{128}$. This can be achieved very simply by choosing $k \oplus k' = x \oplus x'$. $\square$

Lemma 2. *The group G contains only even permutations.*

Proof. In the following we will apply the well known fact that a permutation over a set with an even number of elements is even if and only if its cycle representation (including the fixed points) contains an even number of cycles.

The mappings $x \to k \oplus x$ are even permutations since for $k = (0,0,...,0)$ we obtain the identity permutation and for $k \neq (0,0,...,0)$ the cycle representation consists of 2^{127} cycles of length 2.

The linear transformations mc and rs are even permutations since binary one-to-one linear transformations over $\{0,1\}^n, n \geq 3$, are even permutations. This follows from the facts that each regular binary matrix can be obtained from the identity matrix by elementary row transformations (i.e., binary addition of one row to another row), and that these elementary row transformations (considered as linear mappings over $\{0,1\}^n$) are permutations with 2^{n-1} fixed points and 2^{n-2} cycles of length 2.

The permutation s is even because it can be represented as a concatenation of 16 permutations that carry out the S-box transformation for one byte and leave the other 15 bytes fixed. The cycle representation of each such permutation contains a number of cycles that is a multiple of 2^{120}.

Now the proof is complete since the concatenation of even permutations always yields an even permutation. $\square$

Lemma 3. *The S-box permutation $S : \{0,1\}^8 \to \{0,1\}^8$ is an odd permutation.*

Proof. The cycle representation of S consists of five cycles (with lengths 87, 81, 59, 27, and 2, respectively). Applying the fact mentioned at the beginning of the proof of Lemma 2, it follows that S is an odd permutation. $\square$

Lemma 4. *For all 16-tuples of even permutations $P_j : \{0,1\}^8 \to \{0,1\}^8$, $j = 0,1,...,15$, the mapping*

$$M' : \{0,1\}^{128} \to \{0,1\}^{128}, (x_0,...,x_{127}) \mapsto (y_0,...,y_{127}),$$

defined by

$$(y_{8j}, y_{8j+1}, ..., y_{8j+7}) := P_j\,(x_{8j}, x_{8j+1}, ..., x_{8j+7})$$

for all $j = 0,1,...,15$, is an element of G.

Proof. We consider products of the form $R_k^{-1} \circ R_{k'}$ and $R_k \circ R_{k'}^{-1}$ (where the transformations with k' are carried out first).
Let $j \in \{0,1,...,15\}$ be arbitrarily fixed. Then we have for all $x \in \{0,1\}^{128}$:

If $\forall\, i \in \{0,1,...,127\} \setminus \{8j, 8j+1,...,8j+7\} :\ k_i = k'_i$,
then $R_k \circ R_{k'}^{-1}$ changes no more than the j-th byte of x.
If $\forall\, i \in \{0,1,...,127\} \setminus \{8j, 8j+1,...,8j+7\} :$

$$(rs^{-1}(mc^{-1}(k)))_i = (rs^{-1}(mc^{-1}(k')))_i,$$

then $R_k^{-1} \circ R_{k'}$ changes no more than the j-th byte of x.

This implies that we can define a subgroup of G, namely the group that is generated by all permutations $R_k^{-1} \circ R_{k'}$ and $R_k \circ R_{k'}^{-1}$ with the subkey pairs (k, k') as above. This subgroup acts only on the j-th byte and will therefore be considered as a permutation group on $\{0,1\}^8$. This group is generated by all byte-permutations of the form $x \to k \oplus x$ and all byte-permutations of the form $x \to S^{-1}(k \oplus S(x))$. Therefore it is transitive on this set and it contains only even permutations on this set.

After a random search for the following subkeys $(k^1, k^2, ..., k^8)$ and the following state x, a cycle of the permutation

$$R_{k^8} \circ R_{k^7}^{-1} \circ R_{k^6}^{-1} \circ R_{k^5} \circ R_{k^4} \circ R_{k^3}^{-1} \circ R_{k^2}^{-1} \circ R_{k^1}$$

with length 233 was found (bytes in hexadecimal notation):

$k^1 = k^3 = k^5 = k^7 = (0, 0, ..., 0)$,
the j-th byte of $rs^{-1}(mc^{-1}(k^2))$ is 0xb9, the other 15 bytes are zero,
the j-th byte of k^4 is 0x8b, the other 15 bytes are zero,
the j-th byte of $rs^{-1}(mc^{-1}(k^6))$ is 0xdd, the other 15 bytes are zero,
the j-th byte of k^8 is 0x1f, the other 15 bytes are zero,
the j-th byte of x is 0x9e, the other 15 bytes are randomly chosen.

Since the cycle length 233 is a prime greater than 256/2 and less than 256, the subgroup is primitive on $\{0,1\}^8$ (such a cycle does not match to any structure of imprimitivity, see [7]).

Now Theorem 13.9 in [8], p. 39 can be applied: *"Let p be a prime and G be a group of degree $n = p + k$ with $k \geq 3$. If G contains an element of degree and order p , then G is either alternating or symmetric."* Here the *degree* of a permutation group over a finite set is defined as the number of elements that are changed by at least one permutation of the group. The *degree of a permutation* is defined as the degree of the cyclic group generated by this permutation.

It follows that the considered subgroup equals the alternating group on $\{0,1\}^8$. (Other cycles can be "cancelled" by considering suitable powers of the permutation.)

Since j and the remaining 15 bytes of x were chosen arbitrarily and the considered transformations have no influence on other bytes than the j-th byte, the proof of the Lemma is complete. $\square$

Corollary 1. *The transformation $mc \circ rs \circ h$, where h denotes an arbitrarily fixed parallel application of 16 odd byte-permutations, is an element of G.*

Proof. We choose the round function R_k with the all zero subkey. From Lemma 4 we know that all parallel applications of 16 even byte-permutations are elements of G. Since the S-box is an odd byte-permutation and $mc \circ rs \circ s$ is an element of G, the proof can easily be completed by considering concatenations of group elements. $\square$

4 Proof that the Round Functions Generate the Alternating Group

Lemma 5. *The group G is doubly transitive on the set $\{0,1\}^{128}$, i.e., each pair of different elements from $\{0,1\}^{128}$ can be mapped to each pair of different elements from $\{0,1\}^{128}$.*

Proof. Because the group G is transitive on the set $\{0,1\}^{128}$, it suffices to show that the subgroup G_0 of G containing all elements of G which let the all zero vector fixed, is transitive on $\{0,1\}^8 \setminus \{(0,0,...,0)\}$ (see for example [8], p. 19).

Let us start with an arbitrary non-zero vector $X \in \{0,1\}^{128}$. With the help of Lemma 4, it can be shown that it is possible to find an element of the subgroup G_0 that transforms X to a vector $X' \neq (0,0,...,0)$ with:

$$\forall j \in \{0,1,...,15\} \;:\; (X'_{8j}, X'_{8j+1}, ..., X'_{8j+7}) \in \{0\text{x}00, 0\text{x}01\}.$$

(Choose even permutations P_j that (*) let 0x00 fixed and that transform the non-all-zero-components $(X'_{8j}, X'_{8j+1}, ..., X'_{8j+7})$ to 0x01.)

By computations on a PC (there are only $2^{16} - 1$ such vectors X'), it was verified that it is possible to transform the mentioned X' to the vector $(0x01, 0x01, ..., 0x01)$ by repeated concatenations of $mc \circ rs \circ h'$ and permutations of the form (*) above. Here h' denotes the parallel application of 16 times the odd byte-permutation that changes 0x01 to 0x02, changes 0x02 to 0x01 and lets all other bytes fixed.

Because we have $mc \circ rs \circ h' \in G_0$ (see Corollary 1), it follows that G_0 is transitive on the set $\{0,1\}^{128} \setminus \{(0,0,...,0)\}$. Hence, G is doubly transitive on the set $\{0,1\}^{128}$. □

Theorem 1. *The group G is the alternating group on the set $\{0,1\}^{128}$.*

Proof. From Lemma 4 it follows that the permutation $(P_0, P_1, P_1, ..., P_1)$, where P_1 is the identity permutation on $\{0,1\}^8$ and where the cycle representation of P_0 contains a 3-cycle and 253 fixed points, is an element of G. This permutation lets exactly $253 \cdot 2^{15 \cdot 8}$ elements fixed. Hence, its degree is equal to $3 \cdot 2^{120}$.

The *minimal degree* of a permutation group is the smallest degree of the non-identity-permutations in the group. The minimal degree of G is not greater than $3 \cdot 2^{120}$.

Now, let us suppose that G is smaller than the alternating group. Then, (because of Lemma 5 G is doubly transitive) according to Theorem 15.1 in [8], p. 42 : *"Let G be a a k-ply transitive group, neither alternating nor symmetric. Let n be its degree, m its minimal degree. If $k \geq 2$, then $m \geq \frac{n}{3} - \frac{2\sqrt{n}}{3}$."*, we obtain the contradiction:

$$3 \cdot 2^{120} \geq \frac{2^{128}}{3} - \frac{2^{65}}{3}.$$

From this together with the result of Lemma 2, it follows that G is the alternating group on the set $\{0,1\}^{128}$. □

5 Conclusions and Remarks

By the result stated in the Theorem, several thinkable regularities like the existence of nontrivial factor groups or a too small diversity of occurring permutations in the RIJNDAEL algorithm can be excluded (the alternating group is a large, simple, primitive and $(2^{128} - 2)$-transitive permutation group).

With respect to the Markov approach to differential cryptanalysis, we obtain [2]: For all corresponding Markov ciphers the chain of differences is irreducible and aperiodic, i.e., after sufficiently many RIJNDAEL rounds all differences will be almost equally probable. If the hypothesis of stochastic equivalence holds for a part of the corresponding Markov ciphers, then for all of these Markov ciphers RIJNDAEL is secure against differential cryptanalysis attacks after a sufficient number of rounds.

The results give evidence that the S-box and the other transformations are well chosen from the algebraic point of view. Especially the results of [3] have no consequences with respect to the sizes of the considered permutation groups.

In the following remarks some generalizations (with proof sketches) are given:

Remark 1. Let us take a set of 129 pairwise different round subkeys that includes a basis of the binary vector space $\{0,1\}^{128}$. Then the 129 corresponding round functions suffice to generate the alternating group. This follows from the fact that all round functions can be represented as concatenations of these 129 round functions and their inverses.

Remark 2. Let us take a byte permutation S' such that all byte-permutations of the form $x \to k \oplus x$ and all byte-permutations of the form $x \to S'^{-1}(k \oplus S'(x))$ generate the alternating group on $\{0,1\}^8$. Then the round functions of (modified) RIJNDAEL with the S-box S' also generate the alternating group. For odd permutations S' this can be derived from the proofs given above. For even permutations S' Lemma 5 can be proved in a similar way and the other steps are the same (the result of Corollary 1 is not needed here).

References

1. Daemen, J. and Rijmen, V.: *AES-proposal RIJNDAEL, Version 2*, September 8, 1999. Available at `http://www.esat.kuleuven.ac.be/~rijmen/rijndael/`.
2. Hornauer, G., Stephan, W., and Wernsdorf, R.: Markov Ciphers and Alternating Groups. In *Advances in Cryptology - EUROCRYPT'93*, Lecture Notes in Computer Science, vol. 765, Springer 1994, 453-460.
3. Murphy, S. and Robshaw, M.: *New Observations on Rijndael, Preliminary Draft*, August 7, 2000.
4. National Institute of Standards and Technology (U.S.): *Advanced Encryption Standard (AES)*, FIPS Publication 197, November 26, 2001. Available at `http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf`.
5. Paterson, K. G.: Imprimitive Permutation Groups and Trapdoors in Iterated Block Ciphers. In *Fast Software Encryption - FSE'99*, Lecture Notes in Computer Science, vol. 1636, Springer 1999, 201-214.
6. Wernsdorf, R.: The One-Round Functions of the DES Generate the Alternating Group. In *Advances in Cryptology - EUROCRYPT'92*, Lecture Notes in Computer Science, vol. 658, Springer 1993, 99-112.
7. Wernsdorf, R.: *IDEA, SAFER++ and Their Permutation Groups*, Second Open NESSIE Workshop, Royal Holloway University of London, Egham, September 2001.
8. Wielandt, H.: *Finite Permutation Groups.* Academic Press, New York and London, 1964.
9. Zieschang, T.: Combinatorial Properties of Basic Encryption Operations. In *Advances in Cryptology - EUROCRYPT'97*, Lecture Notes in Computer Science, vol. 1233, Springer 1997, 14-26.