From: Ralph.Wernsdorf@SIT.rohde-schwarz.com
X-Lotus-FromDomain: SIT@RUS
Sender: Ralph.Wernsdorf@SIT.rohde-schwarz.com
To: AESround2@nist.gov
cc: Henning.Krieghoff@SIT.rohde-schwarz.com,
    Volker.Schneider@SIT.rohde-schwarz.com,
    Volker.Thieszen@SIT.rohde-schwarz.com
Date: Fri, 12 May 2000 09:16:42 +0200
Subject: Properties of the SERPENT algorithm

Dear Sirs,

according to your request for comments on the AES-candidates I send you the following paper:

(See attached file: SERPENTAlternatingGroup0.pdf)

The results in the paper exclude several thinkable regularities of the SERPENT round functions. Thus they support the statement of the SERPENT authors that this algorithm has strong cryptographic properties.

Best regards,

R. Wernsdorf

SIT Gesellschaft für Systeme der Informationstechnik mbH

Dr. Ralph Wernsdorf
Wendenschloßstr. 168 Haus 28
12557   Berlin

Phone: +49 30 65884-280
Fax: +49 30 65884-183

E-Mail: Ralph.Wernsdorf@sit.rohde-schwarz.com
http://www.sit.rohde-schwarz.com

The Round Functions of SERPENT Generate the Alternating Group

Ralph Wernsdorf
SIT GmbH, 12557 Berlin, Germany[1]

1 Introduction

The SERPENT algorithm is a block cipher with a block length of 128 bit that has been submitted for the AES selection process. It was developed by R. Anderson, E. Biham and L. Knudsen [1].

In the following a proof is given that the one round functions of SERPENT 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 SERPENT can be excluded (if the generated group were smaller then this would point to regularities in the algorithm, see for example [4], [5], [8]).

An analogous property is known for the block ciphers DES [6], IDEA(32) [4] and SAFER [2].

2 Definitions and Notations

The notation of the SERPENT round function components will be taken from the SERPENT definition given in [1] (note that the presentation given on the pages 3 - 4 in [1] is used here and **not** the bitslice presentation on the pages 5 - 6 in [1]. For convenience the little ”roofs” on the symbols are omitted here.).

The round functions R_i are defined by:

$$\forall i \in \{0,1,\ldots,30\}\, \forall X \in \{0,1\}^{128} : R_i(X) := L(S_i(X \oplus K)),$$

where ”$\oplus$” denotes the bitwise XOR-operation,

$K \in \{0,1\}^{128}$ denotes the corresponding round subkey,

$S_i : \{0,1\}^{128} \to \{0,1\}^{128}$ denotes the application of the S-box *Si* (*i* mod 8) 32 times in parallel and

$L : \{0,1\}^{128} \to \{0,1\}^{128}$ denotes the linear transformation according to the binary matrix on the pages 19-20 in [1].

The S-Boxes $\{0,1\}^4 \to \{0,1\}^4$ are denoted by *S*0, *S*1, ... , *S*7.

The permutation group *G* considered here is defined by:

$$G := \left\langle \left\{ R_i : \{0,1\}^{128} \to \{0,1\}^{128} \,\middle|\, i \in \{0,1,\ldots,7\}, K \in \{0,1\}^{128} \right\} \right\rangle,$$

where ”$\langle M \rangle$” denotes the closure of a permutation set *M* with respect to concatenation.

Properties of the round subkeys caused by the key scheduling will be neglected here. Therefore the generating set of *G* contains $8 \cdot 2^{128}$ permutations.

[1] Wendenschloßstraße 168, Haus 28, Email: Ralph.Wernsdorf@sit.rohde-schwarz.com

© Rohde&Schwarz SIT GmbH 2000

3 Some Elementary Properties of the Generated Group

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

Proof: By concatenations $R_i^{-1} \circ R_i'$ with suited round subkeys *K*, *K´* each given element of the set $\{0,1\}^{128}$ can obviously be transformed to each other arbitrarily given element of the set $\{0,1\}^{128}$.

■

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

Proof: The mappings $X \to K \oplus X$ are even permutations, because for *K* = (0,0,...,0) we obtain the identity permutation and for $K \neq (0,0,\ldots,0)$ the cycle representation consists of 2^{127} cycles of length 2.

The linear transformation *L* is an even permutation, because binary one-to-one linear transformations over $\{0,1\}^n, n \geq 3$, are always even permutations (see for example [3]; besides this, the author found by computations, that all cycles in the cycle representation of *L* have odd length.)

The permutations S_i are even, because they can be represented as concatenations of parallel applications (32 times) of 2-cycles over $\{0,1\}^4$ (14 fixed points and one cycle of length 2). Such a parallel application of 2-cycles yields a permutation with 14^{32} fixed points and $\frac{2^{128} - 14^{32}}{2} = 2^{127} - 2^{31} \cdot 7^{32}$ cycles of length 2. The number $2^{127} - 2^{31} \cdot 7^{32}$ is even, hence the parallel application of 2-cycles is an even permutation.
Now the proof is complete, since the concatenation of even permutations always yields an even permutation.

■

Lemma 3: For all permutations on $\{0,1\}^4$ the parallel application (32 times) is an element of *G*.

Proof (sketch): We choose round functions with the all zero subkey and consider products of the form $R_i^{-1} \circ R_{i'}$. It is not difficult to check that for example $R_1^{-1} \circ R_0$ and $R_3^{-1} \circ R_0$ can generate all permutations of the required form. (The permutations $S1^{-1} \circ S0$ and $S3^{-1} \circ S0$ generate the symmetric group on $\{0,1\}^4$.)

■

Corollary 4: The linear transformation *L* is an element of *G*.

Proof: We choose an arbitrary round function R_i with the all zero subkey: $R_i(X) = L(S_i(X))$. From Lemma 3 we know that S_i is an element of *G*. This immediately implies $L \in G$.

■

Lemma 5: For all even permutations $P : \{0,1\}^4 \to \{0,1\}^4$ and for all $j \in \{0,1,\ldots,31\}$ we have: The mapping $M : \{0,1\}^{128} \to \{0,1\}^{128}$ defined by:

$$\forall X \in \{0,1\}^{128} : Y := M(X) \text{ with } \begin{cases} (Y_{4j}, Y_{4j+1}, Y_{4j+2}, Y_{4j+3}) = P(X_{4j}, X_{4j+1}, X_{4j+2}, X_{4j+3}), \\ \qquad\qquad Y_i = X_i \qquad \text{else} \end{cases}$$

is an element of *G*.

Proof (sketch): We choose round functions with the all zero subkey (with the exception of the components $K_{4j}, K_{4j+1}, K_{4j+2}, K_{4j+3}$) and consider products of the form $R_i^{-1} \circ R_{i'}$. It is not difficult to check that these products can generate all permutations of the required form.

■

Corollary 6: For all 32-tuples of even permutations $P_j : \{0,1\}^4 \to \{0,1\}^4$, $j = 0,1,\ldots,31$, the mapping $M' : \{0,1\}^{128} \to \{0,1\}^{128}$ defined by:

$$\forall X \in \{0,1\}^{128} : Y := M'(X) \text{ with } \begin{cases} (Y_{4j}, Y_{4j+1}, Y_{4j+2}, Y_{4j+3}) = P_j(X_{4j}, X_{4j+1}, X_{4j+2}, X_{4j+3}), \\ \qquad\qquad j = 0,1,\ldots,31 \end{cases}$$

is an element of *G*.

Proof: Each mapping *M´* of the described form can be represented as a product of mappings *M* of the form described in Lemma 5.

■

4 Proof that the Round Functions Generate the Alternating Group

Lemma 7: The group *G* is doubly transitive on the set $\{0,1\}^{128}$.

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 $\{0,1\}^{128} \setminus \{(0,0,\ldots,0)\}$ (see [7], p. 19).

Let us start with an arbitrary non-zero vector $X \in \{0,1\}^{128}$. With the help of Corollary 6 it can be shown that it is always possible to find an element of the subgroup G_0 that transforms *X* to a vector $X' \neq (0,0,\ldots,0)$ with:

$$\forall j \in \{0,1,\ldots,31\} : (X'_{4j}, X'_{4j+1}, X'_{4j+2}, X'_{4j+3}) \in \{(0,0,0,0), (1,1,1,1)\}.$$

(Choose even permutations P_j that (*) let (0,0,0,0) fixed and that transform the non-all-zero-components $(X_{4j}, X_{4j+1}, X_{4j+2}, X_{4j+3})$ to (1,1,1,1).)

By computations on a PC it has been verified that it is always possible to transform the mentioned *X´* to the all-one-vector by repeated concatenations of *L* and permutations of the form (*) above. (There are only 2^{32}–1 such vectors *X´*.)
Because we have $L \in G_0$ it follows that G_0 is transitive on the set $\{0,1\}^{128} \setminus \{(0,0,\ldots,0)\}$.

Hence, *G* is doubly transitive on the set $\{0,1\}^{128}$.

■

Theorem: The group G equals the Alternating group over the set $\{0,1\}^{128}$.

Proof: For the proof we apply a part of Theorem 15.1 in [7], p. 42:

”Let G be a k-ply transitive group, neither alternating nor symmetric. Let n be its degree, m its minimal degree. If $k \geq 2$*, then* $m \geq \frac{n}{3} - \frac{2\sqrt{n}}{3}$ *.”.*

Here the minimal degree is the smallest degree of the non-identity-permutations in the group, where the degree of a permutation is the number of the elements that are not fixed by the permutation.

From Corollary 6 it follows that the permutation $(P_0, P_1, P_1, \ldots, P_1)$, where P_1 is the identity permutation on $\{0,1\}^4$ and where the cycle representation of P_0 contains a 3-cycle and 13 fixed points, is an element of G. This permutation lets exactly $13 \cdot 2^{31 \cdot 4}$ elements of $\{0,1\}^{128}$ fixed. Hence, its degree is equal to $3 \cdot 2^{124}$ and the minimal degree of G is not greater than $3 \cdot 2^{124}$.
Now, let us suppose that G is smaller than the alternating group. Then, (because of Lemma 7 G is doubly transitive) according to Theorem 15.1 in [7] we obtain the inequality:

$$3 \cdot 2^{124} \geq \frac{2^{128}}{3} - \frac{2^{65}}{3}.$$

Thus, we obtained a contradiction. From this together with the result of Lemma 2 it follows that G equals the Alternating group over the set $\{0,1\}^{128}$.

■

5 Conclusions and Remarks

By the result stated in the Theorem several thinkable regularities in the SERPENT 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 [4]:
For all corresponding Markov ciphers the chain of differences is irreducible and aperiodic, i.e. after sufficiently many 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 SERPENT is secure against differential cryptanalysis attacks after a sufficient number of rounds.

The results give evidence that the S-boxes and the transformation L are well chosen from the algebraic point of view.

It would be interesting to find out the group generated by the 32 round cipher mappings, but this seems to be very difficult, since the key scheduling must be taken into consideration.

The author would like to thank Mr. R. Gretmann for the careful preparation of the programs for the mentioned computations.

6 References

[1] Anderson, R.; Biham, E.; Knudsen, L.
SERPENT – A Proposal for the Advanced Encryption Standard
1998, http://www.nist.gov/aes

[2] Dittmar, R.; Hornauer, G.; Wernsdorf, R.
SAFER, DES and FEAL: Algebraic Properties of the Round Functions
Proc. PRAGOCRYPT ’96, ISBN 80-01-01502-5, Prague 1996, 55-66

[3] Even, S.; Goldreich, O.
DES-like Functions can Generate the Alternating Group
IEEE Transactions on Information Theory IT-29, No. 6, 1983, 863-865

[4] Hornauer, G.; Stephan, W.; Wernsdorf, R.
Markov Ciphers and Alternating Groups
Proc. EUROCRYPT ’93, LNCS 765, 1994, 453-460

[5] Paterson, K.G.
Imprimitive Permutation Groups and Trapdoors in Iterated Block Ciphers
Proc. Fast Software Encryption FSE ‘99, LNCS 1636, 1999, 201-214

[6] Wernsdorf, R.
The One-Round Functions of the DES Generate the Alternating Group
Proc. EUROCRYPT ’92, LNCS 658, 1993, 99-112

[7] Wieland, H.
Finite Permutation Groups
Academic Press, New York and London 1964

[8] Zieschang, T.
Combinatorial Properties of Basic Encryption Operations
Proc. EUROCRYPT ’97, LNCS 1233, 1997, 14-26