Cyclic Properties of AES Round Functions

Yvo Desmedt[a]

Florida State University

USA

May 10, 2004

* Part of this work was supported by NSF grant CCR-0109425.

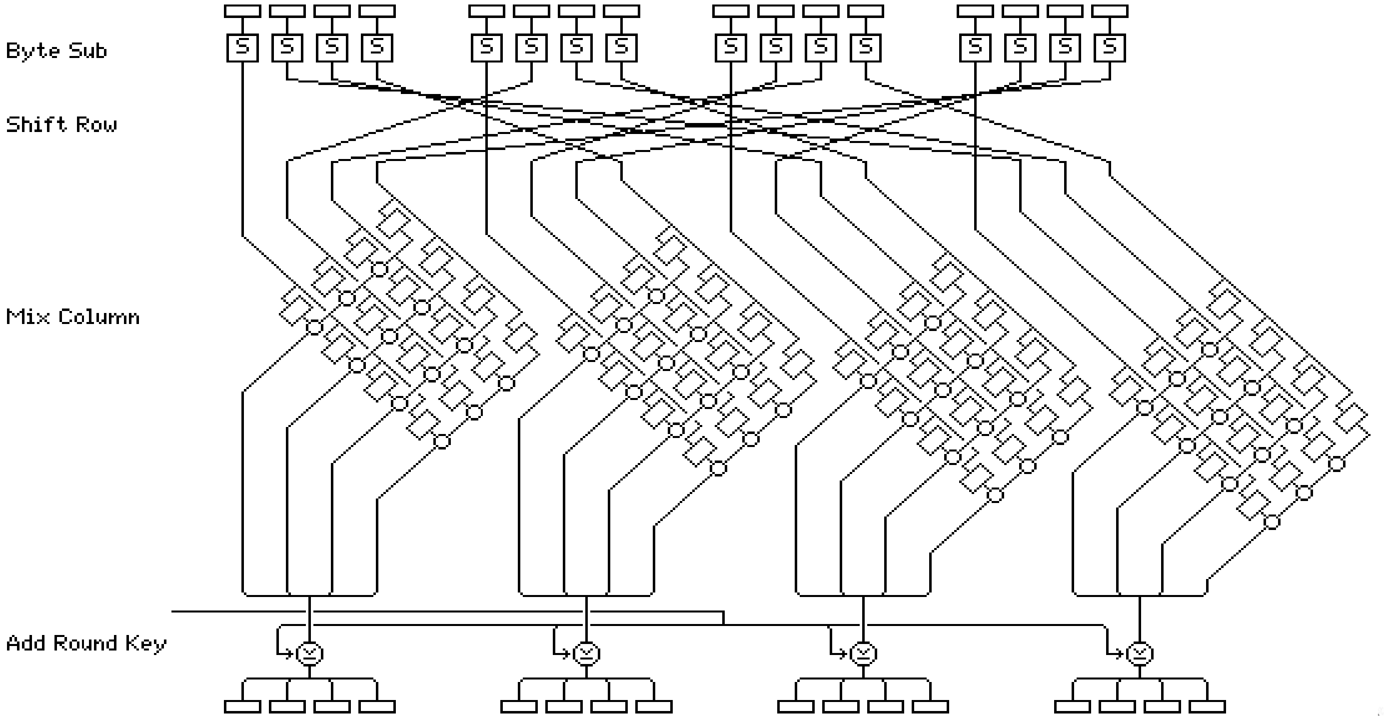
Based on joint work with:

Tri Van Le [1], Rüdiger Sparr [2], Ralph Wernsdorf

[1] Florida State University
Tallahassee, USA

[2] Rohde & Schwarz SIT GmbH,
Berlin, Germany

1. AES ROUND



S-box:

- inversion in the Galois field $GF(2^8)$ modulo $x^8 + x^4 + x^3 + x + 1$, which we denote as I, followed
- by an affine transformation, which we call A.

In the MixColumn operation, each column of the state is considered as a polynomial over $GF(2^8)$ and multiplied modulo $x^4 + 1$ with the polynomial $3x^3 + x^2 + x + 2$.

The ShiftRow, MixColum, AddRoundKey operation is denoted by S, M, and X, respectively.

2. Survey of Known Results

The cyclic order of I, S and X are 2, 4, 2, respectively.
The small size may have troubled many researchers.

At FSE 2003 Song and Seberry showed:

- the cyclic order of M is 4,
- the cycle lengths for $I \circ A$ is 277182,
- the cyclic order of $I \circ A \circ S$ is 554364.

Murphy and Robshaw showed that the order of
$A' \circ S \circ M$ is 16, where
$A'(a)(u) = (u^7 + u^6 + u^5 + u^4 + 1)a(u) \bmod u^8 + 1.$

3. Goal

Since the order of the cycle lengths of individual components of the AES round function are very small, one can wonder how large the cycle length of $I \circ A \circ S \circ M$ is.

Compare with DES!

4. Other cycle properties

Proposition 1 *The cyclic order of the affine transformation A is 4.*

Proof. According to Daemen and Rijmen, the affine transformation A can be written as a mapping of the ring $\mathbb{F}_2[u]/(u^8+1)$

$$A: \ a(u) \mapsto f(u)a(u) + g(u) \bmod u^8 + 1,$$

where $f(u) = u^7 + u^6 + u^5 + u^4 + 1$, and $g(u) = u^7 + u^6 + u^2 + u$.

Then we have $f(u)^2 = u^6 + u^4 + u^2 \text{ mod } u^8 + 1$ and $f(u)^4 = 1 \bmod u^8 + 1$. Since $f(u)^3 + f(u)^2 + f(u) = 1 \text{ mod } u^8 + 1$, it follows that $A^4(a)(u) = f(u)^4 a(u) + (f(u)^3 + f(u)^2 + f(u) + 1)g(u) = a(u) \bmod u^8 + 1$. $\square$

Proposition 2 *The cyclic order of* $A \circ S$, $S \circ M$, $M \circ X$ *for* $X \neq \mathrm{id}$ *and* $A \circ S \circ M$, $S \circ M \circ X$ *for* $X \neq \mathrm{id}$, *are: 4, 8, 8,* $\leq$ *32, 16, respectively.*

5. Invariances of $I \circ A \circ S \circ M$

A property $P \subseteq \{0,1\}^{128}$, $P \neq \emptyset$, is called an *invariance* of f, if P is preserved by f, i.e., for every $x \in P$ it follows that $f(x) \in P$.

The following proposition can easily be verified.

Proposition 3 *The following sets* $\mathrm{Inv}_1, \ldots, \mathrm{Inv}_6$ *are invariances of the mapping* $I \circ A \circ S \circ M$*.*

$$\mathrm{Inv}_1 = \{(x, x, x, ..., x) | x \in GF(2^8)\},$$

$$\mathrm{Inv}_2 = \{(x, y, x, y, x, y, ..., x, y) | x, y \in GF(2^8)\},$$

$$\mathrm{Inv}_3 = \{(w, x, y, z, w, x, y, z, w, x, y, z, w, x, y, z) | \\ w, x, y, z \in GF(2^8)\},$$

$$\mathrm{Inv}_4 = \{(w, x, w, x, y, z, y, z, w, x, w, x, y, z, y, z) | \\ w, x, y, z \in GF(2^8)\},$$

$$\mathrm{Inv}_5 = \{(w, x, y, z, y, z, w, x, w, x, y, z, y, z, w, x) | \\ w, x, y, z \in GF(2^8)\},$$

$$\mathrm{Inv}_6 = \{(s, t, u, v, w, x, y, z, s, t, u, v, w, x, y, z) | \\ s, t, u, v, w, x, y, z \in GF(2^8)\}. \qquad \square$$

6. Using invariances

Since a cycle starting from a point of an invariance set can only contain points of this set, the cycle length is limited by the size of the invariance set. Because we have $|\mathrm{Inv}_i| \leq 2^{32}$ for $i = 1, ..., 5$, it is possible to compute such cycles on a PC.

Table 1-3 list all cycle lengths according to the invariances $\mathrm{Inv}_1, ..., \mathrm{Inv}_5$. Note that the cycles from the invariance Inv_3 are related to those provided in the Appendix of Song and Seberry.

Table 1. Cycle Lengths for Invariances $\mathrm{Inv}_1, \mathrm{Inv}_2, \mathrm{Inv}_3$

Invariance:	Cycle lengths:
Inv_1	87, 81, 59, 27, 2
$\mathrm{Inv}_2 \setminus \mathrm{Inv}_1$	39488, 16934, 7582, 548, 36, 24, 21, 15, 8, 2
$\mathrm{Inv}_3 \setminus \mathrm{Inv}_2$	1088297796, 637481159, 129021490, 64376666, 11782972, 13548, 10756, 5640, 3560, 1902, 136, 90, 47, 40, 12, 4

Table 2. Cycle Lengths for Invariances Inv_4

Invariance:	Cycle lengths:
$\mathrm{Inv}_4 \setminus \mathrm{Inv}_2$	1219717400, 599556416, 315637164, 4307366, 2990738, 2153683, 1958224, 1606154, 1495369, 975150,803077, 564988, 487575, 86038, 82750, 67324, 21758, 13024, 10902, 5451, 5354, 3340, 2677, 2356, 988, 856, 108, 48, 22, 20, 18, 12, 11, 9, 8, 4

Table 3. Cycle Lengths for Invariances Inv_5

Invariance:	Cycle lengths:
$\mathrm{Inv}_5 \setminus \mathrm{Inv}_2$	1052651234, 737292504, 417828286, 193225414, 96612707, 87601912, 11068518, 9460050, 6486298, 5534259, 4730025, 3243149, 394266, 197133, 42454, 16932, 3166, 3078, 2366, 1583, 1539, 1183, 1160, 1062, 912, 496, 38, 18, 9, 6, 2

The least common multiple of the computed cycle lengths for the invariances $\mathrm{Inv}_1, ..., \mathrm{Inv}_5$ of Table 1-3 is equal to:

15480 20902 25688 03988 20263 80165 33732 81646 22636
91465 18521 79549 12467 08119 71956 75745 56484 49918
71194 74949 82013 75604 65431 85505 89291 91969 54985
57959 09774 73220 08631 61663 54665 95490 84924 52493
78665 19158 83139 45332 15200 0,

which is a number of 206 decimals. Since the least common multiple of the cycle lengths for $\mathrm{Inv}_1, ..., \mathrm{Inv}_5$ is a divisor of the cyclic order of $I \circ A \circ S \circ M$.

7. Some other results

We also have obtained:

- invariances of the mapping $(I \circ A \circ S \circ M)^2$ and $(I \circ A \circ S \circ M)^4$.
- **Proposition 4** *There exist no invariances P of $I \circ A \circ S \circ M \circ X$ such that $P \neq \{0,1\}^{128}$ which hold for all 2^{128} round subkeys.*