Remarks on the Period of *Edon80*

Jin Hong

National Security Research Institute
161 Gajeong-dong, Yuseong-gu, Daejeon, 305-350, Korea
jinhong@etri.re.kr

1 Introduction

In this short note, we point out some undesirable characteristics appearing in the streamcipher *Edon80*. We refer readers to the original paper [1] for all notation and terms.

Our discussion will center mostly on the *key* determining the quasigroup operations $*_i$ $(i = 0, \ldots 79)$ and the *initial state* $(a_0, \ldots, a_{79})$ obtained right after the *IVSetup* operation. These two will be referred to as *key-state* pair from now on.

This note presents many key-state pairs that would lead to a keystream of period 2. We also argue the existence of key-IV pairs that produce keystreams of period extremely smaller than 2^{103}, the value designers had projected as cipher period.

2 Undesirable key-state pairs

We wish to instantiate Table 4 of [1] in such a way that the bottom row is a sequence of period 4. This would produce a keystream of period 2.

2.1 Partial key-state pairs

Consider the following series of quasigroup string e-transformations.

$*_i$		0	1	2	3	0	1	2	3	0	...
$\bullet_2$	1	1	2	2	1	1	2	2	1	1	...
$\bullet_0$	2	3	2	0	2	3	2	0	2	3	...
$\bullet_3$	1	2	2	0	1	2	2	0	1	2	...
$\bullet_0$	1	3	2	1	1	3	2	1	1	3	...
$\bullet_2$	0	3	1	2	0	3	1	2	0	3	...

Notice that the period of each row is 4. Actually, we found $166 \approx 2^{7.38}$ such 5-row key-state pairs of period 4. Through an exhaustive searching program, we counted all d-row key-state pairs of period p, for small values of d and p. The results are gathered in Table 1. The actual numbers written down in the table are logarithms of the counts. So, for example, the first entry states that there are approximately $2^{7.38}$ key-state pairs of period 4, consisting of 5 rows.

d	$p = 4$	$p = 8$	$p = 16$
5	7.38	11.49	13.30
6	9.36	13.58	15.68
7	11.04	15.63	18.01
8	12.97	17.71	20.30
9	14.75	19.76	22.55
10	16.63	21.81	24.77
11	18.44	23.85	26.96
12	20.30	25.88	29.13
13	22.13	27.91	31.29
14	23.97	29.94	33.44
15	25.81	31.96	
16	27.65	33.98	
17	29.49		
18	31.33		

Table 1. d-row period-p key-state pair count

Going down any column, one can see that the numbers increase at almost a constant rate. Extrapolating, we can assume the numbers given in Table 2 to be true for 40-row key-state pairs.

	$p = 4$	$p = 8$	$p = 16$
$d = 40$	71.81	82.46	89.08

Table 2. Expected number of 40-row short period key-states

2.2 Full key-state pairs producing a period-2 keystream

Take any one of the 2^{72} 40-row key-state pair of period 4. Its bottom row, which is a sequence of period 4, is equal to the top initiating sequence $(0, 1, 2, 3, 0, \dots)$ with probability $(1/4)^4$. We have experimentally verified that this roughly holds true at smaller row counts. Hence we can expect there to be approximately 2^{64}-many 40-row key-state pairs having bottom row identical to the initiating sequence. In the appendix, we have written out one such partial key-state pair as an explicit example.

Now fix any such 40-row key-state and attach another copy of the same partial key-state to its bottom. This gives an explicit instantiation for Table 4 of [1]. This attaching is possible since the bottom of the original 40 rows is identical to the top of the copy. We also remark that, in this argument, we did not overlook the fact that the top 40 rows will determine the key completely and hence also the quasigroup operators for the lower 40 rows. Since $*_i = *_{i+40}$ $(i = 0, \dots, 39)$, our choice of using a copy on the bottom 40 rows does not conflict with this structure of the cipher.

Recall that the actual keystream is every other quasigroup element from the bottom row sequence. Hence, we have shown the existence of 2^{64}-many (full) key-state pairs that all produce the identical keystream $(1, 3, 1, 3, \dots)$ of period 2. We make no claims as to whether these key-state pairs may be reached through normal *IVSetup* process.

3 Undesirable key-IV pairs

In this section we shall instantiate Table 4 of [1] in such a way that the bottom row is a sequence of relatively short period. The instantiation will be done in two stages. First, the top 40 rows are filled so that the 40-th row is of period 4, 8, or 16. Then, the rest of rows are filled randomly subject to the restraints caused by the top 40 rows.

3.1 Key-state pairs producing relatively short period keystreams

Fix any 40-row key-state pair of period 4. In particular, the bottom row becomes a sequence of period 4. These 40-rows determine the key completely, and hence also the quasigroup operators for the remaining lower 40 rows. Let us fix these lower row operators accordingly and fill in the remaining 40 initial states $(a_{40}, \dots, a_{79})$ with arbitrary quasigroup elements. Referring to the following quote from Section 4.3 of [1],

> in average, each e-transformation increases the period of an input string by factor of 2.48

we can expect a period of $4 \times (2.48)^{40} \approx 2^{54.41}$ at the bottom 80-th row. This leads to a keystream showing a period of $2^{53.41}$. This is much smaller than the projected period 2^{103} given in [1] and also smaller than even the intended security level 2^{80}.

Since the 40-row key-state pairs were approximately 2^{72} in number (Table 2), and since we have 80-bit freedom coming from the choice of quasigroup elements filling the bottom 40 rows, we can expect the existence of

- 2^{72+80} key-state pairs producing keystreams of period 2^{53}.

If we start with 40-row key-state pairs of period 8, or 16, we obtain

- 2^{82+80} key-state pairs producing period-2^{54} keystreams and
- 2^{89+80} key-state pairs producing period-2^{55} keystreams,

respectively.

3.2 Key-IV pairs producing relatively short period keystreams

It remains to see if any of the discussed key-state pairs producing keystream of short period are reachable by normal *IVSetup* operation.

Notice that the *IVSetup* is a 64-bit to 160-bit mapping for any fixed key. Hence, under the assumption that the *IVSetup* is well-designed, given any key-state pair, the probability of it being reachable by *IVSetup* is 2^{-96}.

Thus we have

- 2^{56} key-IV pairs producing period-2^{53} keystreams,
- 2^{66} key-IV pairs producing period-2^{54} keystreams, and
- 2^{73} key-IV pairs producing period-2^{55} keystreams.

Since there are 2^{80+64} key-IV pairs, the probability of encountering one of these key-IV pairs at random is 2^{-88}, 2^{-78}, and 2^{-71}, respectively. The latter two are larger than 2^{-80} and hence constitutes a valid, although certificatory, attack, if keystreams of such length were allowed in view of the 2^{103} period projected by the cipher designers.

4 Probability-period tradeoffs

4.1 Larger set of key-IVs producing slightly longer keystreams

We do not have to divide the 80 rows appearing in Table 4 of [1] into just top 40 and bottom 40 rows. Extrapolating Table 1, one can come up with Table 3 that gives expected number of, say, 34-row key-state pairs of short period.

	$p = 4$	$p = 8$	$p = 16$
$d = 34$	60.77	70.34	76.24

Table 3. Expected number of 34-row short period key-states

One could start with any of these partial key-state pairs, fill rows 35 to 40 with random key-state values, fill lower 40 row keys as defined by the upper 40 rows, and finally fill the rest of the states with random values. This would gives us $4 \cdot 6 + 80 = 104$ bits of freedom.

Since $4 \times (2.48)^{46} \approx 2^{62.28}$, we have the existence of following key-IV pairs.

- 2^{69} key-IV pairs producing period-2^{61} keystreams.
- 2^{78} key-IV pairs producing period-2^{62} keystreams.
- 2^{84} key-IV pairs producing period-2^{63} keystreams.

All of these periods are still small relative to 2^{103} or 2^{80}, one might take for granted. The probability of encountering one of the 2^{84} key-IV pairs producing keystreams of period 2^{63} is 2^{-60}, much larger than 2^{-80}. Hence if we look for a slightly longer but still short keystream, we have a better chance of encountering one at random.

4.2 Existence of key-IV of very short period

We could also divide the 80 rows into two parts below the 40-th row.

Let us go back to Section 2.2. Fill the top 40 rows with any one of the 2^{64}-many 40-row period-4 key-state pairs that has the $(0, 1, 2, 3, 0, \dots)$ initiating sequence at the bottom 40-th row. As before, add another copy below, but fill the quasigroup elements $a_{64}, \dots, a_{79}$ for the last 16 rows at random, so that we have an extra 32-bit degree of freedom.

Since $4 \times (2.48)^{16} \approx 2^{20.97}$, we have the existence of 2^{64+32} key-IV pairs producing period-2^{20} keystreams. Recalling that probability of one of these being reachable by normal *IVSetup* process is 2^{-96}, one can expect the existence of a single key-IV pair that leads to a keystream of extremely short period 2^{20}.

Although this single key-IV pair is hard to reach at random through normal use of this cipher, it still does pose a threat. Also, regardless of how realistic a threat this is, it shows that our understanding of *Edon80*'s period is far from satisfactory.

5 Conclusion

For the streamcipher *Edon80*, we have shown that there are quite a large number of key-state pairs that produce the same sequence of period 2. We have also shown that there is a 2^{-71} probability of a random key-IV pair to produce a keystream of period 2^{55}. A period-2^{63} keystream occurs for a random key-IV pair with probability 2^{-60} and there even exists one key-IV pair producing a period-2^{20} keystream.

All of these periods are very small relative to 2^{103}, which the cipher designers had projected as cipher period. These numbers are smaller than even 2^{80}, which many would take for granted on a 80-bit security cipher, unless explicitly stated otherwise.

Even though these results do not break *Edon80* completely and does not give us any information about how to recover keys, it does show that the period of *Edon80* is far from being well understood. We leave it up to the readers to decide on how serious to take these results.

References

1. D. Gligoroski, S. Markovski, L. Kocarev, and M. Gušev, *Edon80* - Hardware synchoronous stream cipher. *Symmetric Key Encryption Workshop*, Århus, Denmark, May, 2005.

A 40-row key-state pair

Here is an explicit key-state pair consisting of 40 rows that contains the initial sequence $(0, 1, 2, 3, 0, \dots)$ at the bottom row. This is not a concatenation of smaller such partial key-state pairs.

	$*_i$		0	1	2	3
0:	$\bullet_1$	2	2	0	0	2
1:	$\bullet_1$	0	0	1	0	0
2:	$\bullet_2$	2	3	3	0	2
3:	$\bullet_0$	0	3	1	2	0
4:	$\bullet_0$	3	1	1	3	3
5:	$\bullet_0$	0	2	3	1	0
6:	$\bullet_0$	3	2	2	3	3
7:	$\bullet_0$	0	1	3	1	0
8:	$\bullet_0$	1	1	0	2	1
9:	$\bullet_0$	0	2	1	3	0
10:	$\bullet_0$	0	1	1	0	0
11:	$\bullet_0$	1	1	1	2	1
12:	$\bullet_1$	3	2	0	0	3
13:	$\bullet_0$	0	1	2	1	0
14:	$\bullet_1$	0	3	1	1	0
15:	$\bullet_1$	1	3	2	0	1
16:	$\bullet_0$	2	2	0	0	2
17:	$\bullet_1$	0	0	1	0	0
18:	$\bullet_2$	2	3	3	0	2
19:	$\bullet_0$	0	3	1	2	0
20:	$\bullet_0$	3	1	1	3	3
21:	$\bullet_0$	0	2	3	1	0
22:	$\bullet_0$	3	2	2	3	3
23:	$\bullet_0$	0	1	3	1	0
24:	$\bullet_0$	2	3	1	1	2
25:	$\bullet_1$	2	1	1	1	2
26:	$\bullet_1$	0	3	2	0	0
27:	$\bullet_1$	2	1	2	2	2
28:	$\bullet_1$	1	1	2	3	1
29:	$\bullet_0$	0	2	0	3	0
30:	$\bullet_3$	1	3	2	1	1
31:	$\bullet_1$	1	3	1	1	1
32:	$\bullet_0$	2	2	3	0	2
33:	$\bullet_0$	2	0	3	3	2
34:	$\bullet_1$	3	3	0	2	3
35:	$\bullet_1$	2	1	0	0	2
36:	$\bullet_3$	0	2	0	3	0
37:	$\bullet_3$	1	3	2	1	1
38:	$\bullet_3$	1	2	2	3	1
39:	$\bullet_3$	3	0	1	2	3