A note on the Edon80 S-box

T.E. Bjørstad

The Selmer Center, Department of Informatics,
University of Bergen, Pb. 7800, N-5020 Bergen, Norway.
Email : tor.bjorstad@ii.uib.no

Abstract. Edon80 [1] is one of the Phase 3 candidates in eSTREAM, the ECRYPT stream cipher project. This note examines the structure of the Edon80 quasigroup permutation, when viewed as an S-box or a pair of boolean functions. Although some structure is found, it is unclear how this can be applied to attack the full cipher.

1 Introduction

The Edon80 stream cipher consists of 80 pipelined stages. Each stage has 4 bits of internal state: two fixed bits $k = (k_1, k_0)$ which are part of the secret key, and two dynamic state bits $s = (s_1, s_0)$ which are updated every clock cycle. The key bits are used to select one of four quasigroup permutations $\star_i$. During keystream generation, the state bits s of stage i at time t are updated by the rule

$$s_{i,t+1} = s_{i,t} \star_i s_{i-1,t}. \tag{1}$$

The initial stage takes as input the periodic string $01230123\ldots0123\ldots$, while the last stage outputs its current s as keystream every other cycle. Key and IV setup is described in further detail in [1]. In the following, we denote the input

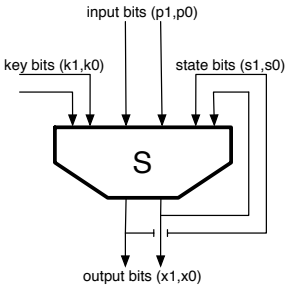

Fig. 1. The Edon80 S-box

coming from the previous stage as $p = (p_1, p_0)$, and the output of the S-box (the new state) as $x = (x_1, x_0)$. The most significant bit of each value is the first, so the notation $p = 2$ and $p_1 = 1, p_0 = 0$ will be used interchangably. We shall refer to a single application of the quasigroup transformation as a *round*.

2 The Edon80 Quasigroups

The four Edon80 quasigroups are shown in Fig. 2. According to [1] the permutations have been chosen among 64 "good" choices among the 576 possible quasigroups.

$\star_0$	0	1	2	3
0	0	2	1	3
1	2	1	3	0
2	1	3	0	2
3	3	0	2	1

$\star_1$	0	1	2	3
0	1	3	0	2
1	0	1	2	3
2	2	0	3	1
3	3	2	1	0

$\star_2$	0	1	2	3
0	2	1	0	3
1	1	2	3	0
2	3	0	2	1
3	0	3	1	2

$\star_3$	0	1	2	3
0	3	2	1	0
1	1	0	3	2
2	0	3	2	1
3	2	1	0	3

Fig. 2. The Edon80 quasigroup permutations

Instead of taking a group-theoretical approach, we consider the quasigroup transformation as an S-box mapping a 6 bit input to 2 bits of output. We denote this map $S : \{0,1\}^6 \rightarrow \{0,1\}^2$, where the individual bits $(k_1k_0s_1s_0p_1p_0) \mapsto (x_1x_0)$. Alternately, S may be viewed as an ordered pair of boolean functions $f(x)$ and $g(x)$, which map 6 input bits to x_1 and x_0 respectively.

2.1 Boolean functions

It may readily be confirmed that the functions $f(x)$ and $g(x)$ are of degree four.

$$\begin{aligned} f(x) = {} & p_0 + s_0 + k_1 \\ & + k_0s_0 + k_0s_1 + k_1p_1 \\ & + k_0s_0p_0 + k_0s_0p_1 + k_1s_1p_1 + k_1k_0p_0 + k_1k_0s_0 \\ & + k_1k_0s_0p_0 + k_1k_0s_0p_1 + k_1k_0s_1p_0 + k_1k_0s_1p_1 \end{aligned} \tag{2}$$

$$\begin{aligned} g(x) = {} & p_1 + s_1 + k_0 \\ & + s_0p_0 + k_0s_0 + k_1p_0 + k_1p_1 + k_1s_0 \\ & + k_0s_0p_1 + k_1s_0p_0 + k_1s_1p_1 \\ & + k_1k_0s_0p_1 + k_1k_0s_1p_1 \end{aligned} \tag{3}$$

The following are the best affine approximations to f and g. Both hold with probability 11/16 (bias 3/16). Thes approximations are not independent as they depend on the same variables; the probability that *both* approximations hold is 7/16.

$$\begin{aligned} f(x) &\approxeq k_1 + s_0 + p_0 \\ &\approxeq k_1 + k_0 + s_0 + p_0 \end{aligned} \tag{4}$$

$$\begin{aligned} g(x) &\approxeq k_1 + s_1 + p_0 \\ &\approxeq k_1 + k_0 + s_1 + p_0 + 1 \end{aligned} \tag{5}$$

The four approximations all depend on bits from all three inputs, k, s and p.

2.2 Other linear relations

A simple search reveals four additional relations between input- and output bits in the S-box that hold with probability 11/16.

$$\begin{aligned} s_1 + p_1 + x_1 + x_0 + 1 &= 0 \\ k_0 + s_1 + p_1 + x_1 + x_0 + 1 &= 0 \\ k_1 + s_0 + p_1 + p_0 + x_1 + x_0 + 1 &= 0 \\ k_1 + k_0 + s_0 + p_1 + p_0 + x_1 + x_0 &= 0 \end{aligned} \tag{6}$$

It it interesting to note that the first relation does not involve k at all.

2.3 Restrictions on the boolean functions

In some cases we have partial knowledge of the input to the S-box. Situations where this is always true include the final S-box (where the state s is output as keystream every other cycle), the first S-box (whose input p is known during key generation), and during the IV setup (where the states s of stages 0-39 are initialised using the IV and the fixed string 32100123). In these cases, the restriction of the boolean functions f and g to the remaining free variables is of lower degree, and better affine approximations to f and g exist. The following table gives a list of "good" affine approximations and their respective probabilities of being correct. Some of the approximations (particularly those with probability 3/4) are not unique.

Restriction	f-approximation	Prob.	g-approximation	Prob.
$k = 0$	$s_0 + p_0$	1	$s_1 + p_1$	3/4
$k = 1$	$s_1 + s_1 + p_0$	3/4	$s_1 + p_0$	3/4
$k = 2$	$s_0 + p_0 + 1$	3/4	$s_0 + p_0$	3/4
$k = 3$	$s_0 + p_1 + 1$	3/4	$s_1 + p_0 + 1$	1
$s = 0$	p_0	3/4	$k_0 + p_1$	3/4
$s = 1$	p_1	3/4	$k_1 + p_0$	7/8
$s = 2$	$k_1 + k_0 + p_0$	7/8	$k_0 + p_1 + 1$	3/4
$s = 3$	$k_1 + p_0 + 1$	3/4	$k_1 + p_0 + 1$	3/4
$p = 0$	$k_1 + s_0$	3/4	$k_0 + s_1$	3/4
$p = 1$	$k_1 + k_0 + s_0 + 1$	7/8	$k_1 + s_1 + 1$	3/4
$p = 2$	$s_1 + s_0$	7/8	$k_1 + k_0 + s_1 + 1$	7/8
$p = 3$	$k_0 + s_0 + 1$	3/4	$k_0 + s_1 + s_0 + 1$	3/4

Fig. 3. Restricted approximations to the S-box

Of particular note is the fact that some values of k yield *linear* functions.

2.4 Multiround approximations

A natural question when making linear approximations of the S-box, is whether it is possible to find good linear approximations to multiple "rounds" of Edon80,

preferably of low weight. If we consider each round as independent random functions that admit linear approximations of bias 3/16, the accumulated bias of our linear relation after 80 rounds would be on the order of 2^{-114}, which is not very useful.

We have used exhaustive computer search to find linear relations with greater bias across 2, 3 and 4 S-box iterations. The results are somewhat encouraging, as we do obtain relations with larger biases than predicted using the Piling-up Lemma and the one-round approximations discussed earlier. However, the best 4-round relation (approximating $f\big[k^{'''}, s^{'''}, S\big(k^{''}, s^{''}, S[k^{'}, s^{'}, S(k, s, p)]\big)\big]$) only has a bias only 9/512, and depends on 10 of the 20 different input, output, key and state variables. By the Piling-up Lemma, a bias of 9/512 over 4 rounds yields an estimated bias of roughly 2^{-97} for the corresponding linear relation over 80 S-box iterations. Furthermore, other highly biased linear relations found generally depend on *more* than 10 variables.

There are still some slight improvements to be made. The approximation of the first group of S-boxes can be treated as a special case, since we know the input seed at all times during key generation. This allows us to find better approximations for this particular transformation. As an example, the best 4-round approximation given the input value $p = 0$ has bias of 49/2048.

Finally, since the key bits used in round 40-79 are identical to the key bits in round 0-39, it seems likely that a linear approximation to the full cipher can be constructed in such a way that these bits *cancel* (since they contribute twice, both in S-box i and $i + 40$). Nevertheless, the author is not able to find linear relations of sufficiently high bias and low weight to allow an efficient attack to be made against the full Edon80 stream cipher.

3 Conclusion

We have examined some biases and structural oddities in the Edon80 S-box, but they do not appear large enough to lead to attacks against the full cipher. It might be interesting to look at a scaled-down version of Edon80, to determine more accurately how many cipher rounds are needed to make linear distinguishing attacks infeasible.

References

1. D. Gligoroski, S. Markovski, L. Kocarev, and M. Gusev. Edon80. eSTREAM - ECRYPT Stream Cipher Project, Report 2005/007, 2005.