Date: Thu, 11 May 2000 20:04:00 +0900
From: Jun Yajima <jyajima@flab.fujitsu.co.jp>
X-Mailer: Mozilla 4.7 [ja] (WinNT; I)
X-Accept-Language: ja
To: AESround2@nist.gov
Subject: Boolean functions of Serpent S-boxes

Dear Sirs,

We searched Boolean functions of Serpent S-boxes that have the least number of operations by our original method.

Please find attached a summary of our research.

Sincerely yours,

Jun Yajima
FUJITSU LABORATORIES LTD.
jyajima@flab.fujitsu.co.jp

Results of New Boolean Functions Search for Serpent S-boxes

Jun Yajima*, Masahiko Takenaka*, Naoya Torii*, Kouichi Itoh*
FUJITSU LABORATORIES LTD.

We searched boolean functions of Serpent S-boxes that have the least number of operations by our original method [1]. The following table shows our result. It also shows the number of operations by the previous methods [2][3] for comparison. For three S-boxes, we found the boolean functions that have the least number of operations.

Appendix shows a set of the boolean functions of our result.

Table. Number of operations

S-box	**Gladman***[2]	**Osvik**[3]	**Our results**
S_0	15	18(17)	15
S_1	14	18(17)	16
S_2	16	16(14)	15
S_3	16	19(17)	**15#**
S_4	15	20(19)	15
S_5	16	19(18)	16
S_6	15	18(17)	15
S_7	16	20(19)	17
Si_0	15	19(18)	16
Si_1	14	19(18)	16
Si_2	16	19(18)	**15#**
Si_3	15	18(17)	16
Si_4	15	20(19)	16
Si_5	16	19(18)	16
Si_6	15	17(16)	16
Si_7	17	19(18)	**16#**

Note:
#: the least number of operations
*: best results about number of operations
( ): exclude "=" operation

Reference

[1] J.Yajima, M.Takenaka, N.Torii,
"On Efficient Boolean Functions of Serpent S-boxes," (in Japanese)
2000 Symposium on Cryptography and Information Security, Okinawa, Japan 26-28 Jan. 2000, SCIS2000-A47

[2] B.Gladman,
http://www.btinternet.com/~brian.gladman/cryptography_technology/serpent/index.html

[3] D.Osvik,
"Speeding up Serpent," AES3 conference.

*FUJITSU LABORATORIES LTD. 64 Nishiwaki, Ohokubo-cho, Aksahi 674-8555 Japan.
{jyajima, takenaka, torii, kito}@flab.fujitsu.co.jp

Appendix:

```
/*                  Boolean Functions of Serpent S-boxes                  */
/*                                                                        */
/*      Copyright (C) 2000 FUJITSU LABORATORIES LIMITED.                  */
/*                         All rights reserved.                           */
/*                                                                        */
/*          Jun Yajima              (jyajima@flab.fujitsu.co.jp)          */
/*          Masahiko Takenaka       (takenaka@flab.fujitsu.co.jp)         */
/*          Naoya Torii             (torii@flab.fujitsu.co.jp)            */
/*          Kouichi Itoh            (kito@flab.fujitsu.co.jp)             */
/*                                                                        */
/*             If you use this information, please contact us.            */
/*                                                                        */
```

```
/* S0: 15 steps */
S_0(x3,x2,x1,x0,y3,y2,y1,y0)
  t7=x0|x3;
  t1=~x0;
  t8=t7^x1;
  t2=t1^x3;
  y3=t8^x2;
  t3=t2|x1;
  t9=x2^t3;
  t4=t3^x3;
  t10=t9^t1;
  t5=t4|x2;
  t11=t10&y3;
  t6=t5^x1;
  y0=t11^t4;
  y2=t6^t2;
  y1=y0^t10;
```

```
/* S1: 16 steps */
S_1(x3,x2,x1,x0,y3,y2,y1,y0)
  t1=~x1;
  t2=t1^x0;
  t3=t2|x3;
  t7=x0|t2;
  t4=t3|x2;
  t8=t7^x2;
  t5=t4^x0;
  t9=t3^t8;
  t6=t5^x3;
  t10=t9|x1;
  t11=x1^t9;
  y1=t10^t6;
  y2=t8^x3;
  y3=t11^y1;
  t12=t6&t11;
  y0=t12^t8;
```

```
/* S2: 15 steps */
S_2(x3,x2,x1,x0,y3,y2,y1,y0)
  t1=~x0;
  t7=x0&x2;
  t4=x1^x2;
  t2=t1&x3;
  t8=t7^x3;
  t9=x1&t8;
  t3=t2^x1;
  t10=t9^t4;
  t5=t4&t3;
  t11=t3^t10;
  t6=t5^x3;
  y0=t8^t4;
  y3=t10^t1;
  y2=x0^t6;
  y1=t11^y2;
```

```
/* S3: 15 steps */
S_3(x3,x2,x1,x0,y3,y2,y1,y0)
  t1=x0|x3;
  t2=x0&x1;
  t6=x2^x3;
  t3=t2^t1;
  t8=x0&x3;
  t4=t3|x2;
  t7=t6|t2;
  t5=t4^x1;
  y3=t8^t5;
  t9=t3|y3;
  y1=t7^t5;
  t10=t9^x0;
  t11=y1&t10;
  y2=y1^t10;
  y0=t11^t3;
```

```
/* S4: 15 steps */
S_4(x3,x2,x1,x0,y3,y2,y1,y0)
  t1=x0^x3;
  t2=t1|x1;
  t3=t2^x0;
  t5=x0&x3;
  t4=t3^x2;
  t6=t5^t4;
  t7=t6|t3;
  t8=t6|x1;
  y3=t8^t1;
  t9=t7^x1;
  t10=y3|t9;
  y0=~t6;
  y2=t9^t1;
  t11=t10^x3;
   y1=t11^t6;
```

```
/* S5: 16 steps */
S_5(x3,x2,x1,x0,y3,y2,y1,y0)
  t1=x0&x1;
  t2=t1^x2;
  t3=~t2;
  t4=t3^x3;
  t5=x1^t4;
  t8=x2|t4;
  t6=t5&x3;
  t9=t8&x0;
  t7=t6^x0;
  t10=t4&t5;
  y1=t7^t4;
  y3=t9^t5;
  t12=x3&y1;
  t11=t2^y3;
  y0=t12^t5;
   y2=t11|t10;
```

```
/* S6: 15 steps */
S_6(x3,x2,x1,x0,y3,y2,y1,y0)
  t1=x1^x2;
  t2=t1^x0;
  t3=~t2;
  t4=t3^x3;
  t5=t1|t4;
  t8=x2^t4;
  t6=t5^x3;
  t7=t6|x1;
  t9=t8^t6;
  y3=t7^t4;
  t10=t9|y3;
  t11=x0|x3;
  y0=t10^t6;
  y2=t10^t8;
   y1=t11^t4;
```

```
/* S7: 17 steps */
S_7(x3,x2,x1,x0,y3,y2,y1,y0)
  t1=x0^x1;
  t2=x1^x2;
  t3=t1&t2;
  t4=t3^x3;
  t5=t4^x0;
  t6=t5|t2;
  t7=t4&t6;
  y1=t7^x2;
  t8=x0&t5;
  y3=t8^t2;
  t9=x2|x3;
  t10=t9^t8;
  t11=y3&t10;
  y2=t11^t4;
  t12=t1|t9;
  t13=~t12;
   y0=t13^t5;
```

```
/* Si0: 16 steps */
Si_0(x3,x2,x1,x0,y3,y2,y1,y0)
  t1=x1^x2;
  t2=x0^x1;
  t3=t2|x3;
  t4=~t3;
  t5=t4^x0;
  t6=t5|t1;
  t7=x1^x3;
  t8=t7^t3;
  y3=t8^t6;
  t9=t2|t7;
  t10=t9^t1;
  y0=t10^y3;
  t11=x3^t5;
  y2=t11^t10;
  t12=y3&y0;
   y1=t12^t5;
```

```
/* Si1: 16 steps */
Si_1(x3,x2,x1,x0,y3,y2,y1,y0)
  t1=x1^x3;
  t2=t1|x0;
  t3=t2^x3;
  t4=t3&x2;
  t5=~t4;
  t6=t5^x0;
  y2=t1^t6;
  t7=x3&t1;
  t8=t7^x0;
  y3=t8^x2;
  t9=x1^x2;
  t10=t9^t2;
  t11=t10&y3;
  y1=t11^t3;
  t12=~t10;
   y0=t12^y1;
```

```
/* Si2: 15 steps */
Si_2(x3,x2,x1,x0,y3,y2,y1,y0)
 t1=x3&x2;
 t2=x3|x1;
 t3=x0&t2;
 t6=t1^t2;
 t4=t1|t3;
 t7=~t6;
 t5=x2^t4;
 t8=t7^x0;
 y1=x1^t5;
 t9=y1|t6;
 y2=t8^y1;
 t10=t9^x0;
 y0=t10^x3;
 t11=y2&y0;
  y3=t11^t7;
```

```
/* Si3: 16 steps */
Si_3(x3,x2,x1,x0,y3,y2,y1,y0)
 t1=x0|x3;
 t6=x2|x3;
 t2=t1^x2;
 t3=t1^x1;
 t7=t6&x1;
 t4=t3&t2;
 y0=t7^t2;
 t5=t4^x3;
 y2=x0^t5;
 t8=t5^t6;
 t9=x1^y2;
 t10=t9|t8;
 t11=t3&t10;
 y3=t10^x3;
 t12=t11^x0;
  y1=t12^x2;
```

```
/* Si4: 16 steps */
Si_4(x3,x2,x1,x0,y3,y2,y1,y0)
 t1=x0&x1;
 t4=x2|x3;
 t2=t1^x2;
  t5=t4&x0;
 t3=t2^x3;
 y1=t5^t3;
 t8=~x0;
 t6=x3&y1;
 t7=t6^x1;
 t9=t8|y1;
 y3=t7^t3;
 t10=t9^x3;
 t11=y3&t10;
 y0=t10^y3;
 t12=t11^t6;
  y2=t12^t8;
```

```
/* Si5: 16 steps */
Si_5(x3,x2,x1,x0,y3,y2,y1,y0)
 t1=~x0;
 t2=x1|x2;
 t7=x1|t1;
 t3=x3^t2;
  t8=t3&t7;
 t4=t1|t3;
 t9=x0^t8;
 t5=x1^t4;
 y1=x2^t9;
 t10=t5^t7;
 t6=x2|x0;
 y0=y1^t10;
 y3=t5^t6;
 t11=t5|y0;
 t12=t2^t11;
  y2=t1^t12;
```

```
/* Si6: 16 steps */
Si_6(x3,x2,x1,x0,y3,y2,y1,y0)
 t2=x0^x2;
 t1=~x1;
 t3=t2|x3;
 t6=x0&t2;
 t9=t2^t1;
  t7=t6^x3;
 t4=t3^x0;
 t5=t4|t1;
 t8=t7|x1;
 y1=t9^t7;
 t10=t4^t7;
 y0=t8^t5;
 t11=t10^x1;
 t12=t4&t11;
 y3=t11^y0;
  y2=t12^t9;
```

```
/* Si7: 16 steps */
Si_7(x3,x2,x1,x0,y3,y2,y1,y0)
 t1=x2|x3;
 t2=x0&x3;
 t3=t2^t1;
 t9=~x3;
 t4=t3|x1;
  t12=x0|t9;
 t5=t4^x0;
 t6=t5^x2;
 t7=t1&t6;
 t8=t3|t6;
 y2=t7^x1;
 t10=t9^t8;
 y1=t10^y2;
 t11=y2&t10;
 y0=t12^t6;
  y3=t11^t3;
```