A Compact Bit-Sliced Representation of Kuznyechik S-box

O. Avraamova[1], D. Fomin[2], V. Serov[1], A. Smirnov[1], and V. Shokov[1]

[1] Lomonosov Moscow State University, Russia
[2] Higher School of Economics, Russia

olga.avraamova@gmail.com, dfomin@hse.ru, v_serov_@mail.ru,
asmirnov80@gmail.com, shokov@srcc.msu.ru

September 15, 2020

…Determing the manner of operation of a given switching circuit, is comparatively simple. The inverse problem of finding a circuit satisfying certain given operating conditions, and in particular the *best* circuit is, in general, more difficult and more important from the practical standpoint

---

Claude E. Shannon
The Synthesis of Two-Terminal Switching Circuit, 1949

There are several different "decomposition" the S-box of Kuznyechik[1]:

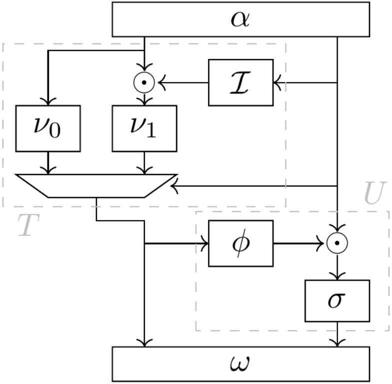


Figure: The TU-decomposition

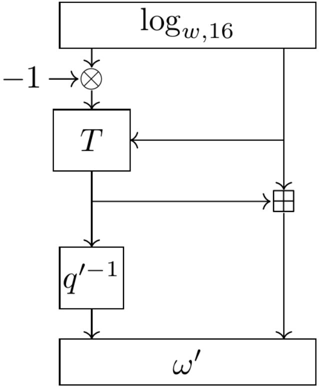


Figure: The log-based decomposition

[1] pictures are from and more details in: Léo Perrin, Partitions in the S-Box of Streebog and Kuznyechik, Cryptology ePrint Archive, Report 2019/092

Piano

→

Lego Piano

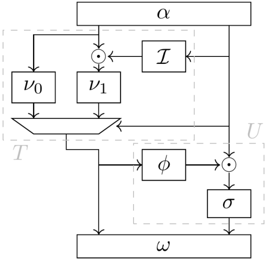
→

Bricks

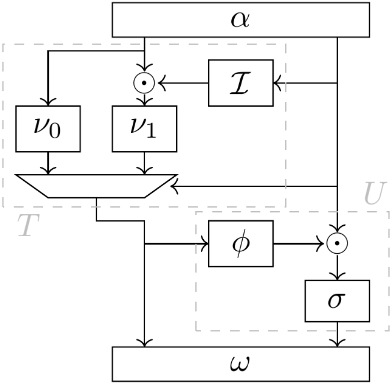
4.1.1 Нелинейное биективное преобразование

В качестве нелинейного биективного преобразования выступает подстановка $\pi = \mathrm{Vec}_8 \pi' \mathrm{Int}_8 \colon V_8 \to V_8$, где $\pi' \colon \mathbb{Z}_{2^8} \to \mathbb{Z}_{2^8}$. Значения подстановки π' записаны ниже в виде массива $\pi' = (\pi'(0), \pi'(1), \ldots, \pi'(255))$:

π' = (252, 238, 221, 17, 207, 110, 49, 22, 251, 196, 250, 218, 35, 197, 4, 77, 233, 119, 240, 219, 147, 46, 153, 186, 23, 54, 241. 187, 20, 205, 95, 193, 249, 24, 101, 90, 226, 92, 239, 33, 129, 28, 60, 66, 139, 1, 142, 79, 5, 132, 2, 174, 227, 106, 143, 160, 6, 11, 237, 152, 127, 212, 211, 31, 235, 52, 44, 81, 234, 200, 72, 171, 242, 42, 104, 162, 253, 58, 206, 204, 181, 112, 14, 86, 8, 12, 118, 18, 191, 114, 19, 71, 156, 183, 93, 135, 21, 161, 150, 41, 16, 123, 154, 199, 243, 145, 120, 111, 157, 158, 178, 177, 50, 117, 25, 61, 255, 53, 138, 126, 109, 84, 198, 128, 195, 189, 13, 87, 223, 245, 36, 169, 62, 168, 67, 201, 215, 121, 214, 246, 124, 34, 185, 3, 224, 15, 236, 222, 122, 148, 176, 188, 220, 232, 40, 80, 78, 51, 10, 74, 167, 151, 96, 115, 30, 0, 98, 68, 26, 184, 56, 130, 100, 159, 38, 65, 173, 69, 70, 146, 39, 94, 85, 47, 140, 163, 165, 125, 105, 213, 149, 59, 7, 88, 179, 64, 134, 172, 29, 247, 48, 55, 107, 228, 136, 217, 231, 137, 225, 27, 131, 73, 76, 63, 248, 254, 141, 83, 170, 144, 202, 216, 133, 97, 32, 113, 103, 164, 45, 43, 9, 91, 203, 155, 37, 208, 190, 229, 108, 82, 89, 166, 116, 210, 230, 244, 180, 192, 209, 102, 175, 194, 57, 75, 99, 182).



Boolean function minimization basis $\{AND, OR, NOT, XOR\}$



The TU-decomposition was first presented in "Reverse-engineering the SBox of Streebog, Kuznyechik and STRIBOBr1" by Alex Biryukov, Leo Perrin, and Aleksei Udovenko., 2016

It consists of:

- linear transformations $V_8 \to V_8$: α and ω
- non-linear transformations $V_4 \to V_4$: ν_0, ν_1, I, σ, φ
- multiplication in Galois field $GF\left(2^4, \odot, \oplus\right) = GF(2)[x]/(f(x))$ with irreducible polynomial $f(x) = x^4 \oplus x^3 \oplus 1$
- multiplexer (if-else construction)

$$\alpha = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$\boxed{\text{Total } \alpha \text{ and } \omega\text{: 14 XOR}}$

$l = (l_1, l_2, l_3, l_4)$, $r = (r_1, r_2, r_3, r_4)$ be representations of field elements as vectors. Then α has the following Boolean representation:

$$\begin{aligned}
&\alpha_1(l,r) = r_1,\\
&\alpha_2(l,r) = l_2 \oplus r_4,\\
&\alpha_3(l,r) = l_2 \oplus r_3 \oplus r_4 = \alpha_2(l,r) \oplus r_3,\\
&\alpha_4(l,r) = l_1 \oplus l_2 \oplus l_3 \oplus r_1 \oplus r_2 \oplus r_3 \oplus r_4 =\\
&= \alpha_2(l,r) \oplus \alpha_5(l,r) \oplus l_3 \oplus r_2,\\
&\alpha_5(l,r) = l_1 \oplus r_1 \oplus r_3 = l_1 \oplus p_1,\\
&\alpha_6(l,r) = l_2 \oplus r_2,\\
&\alpha_7(l,r) = l_4 \oplus r_1 \oplus r_3 = l_4 \oplus p_1,\\
&\alpha_8(l,r) = l_3,\\
&p_1 = r_1 \oplus r_3.
\end{aligned}$$

Using the standard basis of $GF\left(2^4\right)$ $\{\mathbf{e}_1 = (1000), \mathbf{e}_2 = (0100), \mathbf{e}_3 = (0010), \mathbf{e}_4 = (0001)\}$ it is easy to show that the every coordinate z^k, $k \in \overline{1,4}$, $\mathbf{z} = \mathbf{x} \odot \mathbf{y}$, $x, y, z \in GF\left(2^4\right)$ is a quadratic form:

$$\mathbf{z}^k = (\mathbf{x} \circledcirc \mathbf{y})^k = \left(\left(\sum_{i=1}^{4} x^i \mathbf{e}_i\right) \circledcirc \left(\sum_{j=1}^{4} y^j \mathbf{e}_j\right)\right)^k = \sum_{i,j} x^i \cdot y^j (\mathbf{e}_i \circledcirc \mathbf{e}_j)^k \Rightarrow$$

$$\Rightarrow z^k = (x^1, x^2, x^3, x^4) \begin{pmatrix} c_{11}^k & \dots & c_{14}^k \\ \vdots & \ddots & \vdots \\ c_{41}^k & \dots & c_{44}^k \end{pmatrix} \begin{pmatrix} y^1 \\ y^2 \\ y^3 \\ y^4 \end{pmatrix}.$$

$\mathbf{z} = \mathbf{x} \odot \mathbf{y}$, $\mathbf{z} = \left(z^1, z^2, z^3, z^4\right)$, $\mathbf{x} = \left(x^1, x^2, x^3, x^4\right)$, $\mathbf{y} = \left(y^1, y^2, y^3, y^4\right)$:

$$
\begin{aligned}
z_1 &= \left(P_2 \oplus x_4\right) \cdot y_1 \oplus P_2 \cdot y_2 \oplus P_1 \cdot y_3 \oplus x_1 \cdot y_4, \\
z_2 &= x_1 \cdot y_1 \oplus x_4 \cdot y_2 \oplus x_3 \cdot y_3 \oplus x_2 \cdot y_4, \\
z_3 &= P_1 \cdot y_1 \oplus x_1 \cdot y_2 \oplus x_4 \cdot y_3 \oplus x_3 \cdot y_4, \\
z_4 &= P_2 \cdot y_1 \oplus P_1 \cdot y_2 \oplus x_1 \cdot y_3 \oplus x_4 \cdot y_4, \\
P_1 &= x_1 \oplus x_2, \\
P_2 &= x_1 \oplus x_2 \oplus x_3 = P_1 \oplus x_3.
\end{aligned}
$$

Total: 31 Boolean operations

There is an "if-else" construction in the considered decomposition:
"`2.If` $r = 0$ `then` $l := \nu_0(l)$ `else` $l := \nu_1(l \circledcirc I(r))$"

Let $I_{0,0,0,0}(r)$ be a Boolean function which takes the value 1 in a single point $r = (0,0,0,0)$ then this construction can be expressed by a formula:

$$l^i = I_{0,0,0,0}(r) \cdot \nu_0^i(l) + \overline{I_{0,0,0,0}(r)} \cdot \nu_1^i(l \circledcirc I(r)), \quad i = 1, \ldots, 4.$$

It can be rewriten as follows:

$$l^i = I_{0,0,0,0}(r) \cdot \left(\nu_0^i(l) \oplus \nu_1^i(0)\right) \oplus \nu_1^i(l \circledcirc I(r)), \quad i = 1, \ldots, 4.$$

Branching elimination

Using the fact that

$$I_{0,0,0,0}(r) = \bar{r}_1 \cdot \bar{r}_2 \cdot \bar{r}_3 \cdot \bar{r}_4 = \overline{r_1 + r_2 + r_3 + r_4}.$$

and $\nu_1^i(0) = (0, 0, 1, 0)$ we can implement branching using operations that are given in a table below:

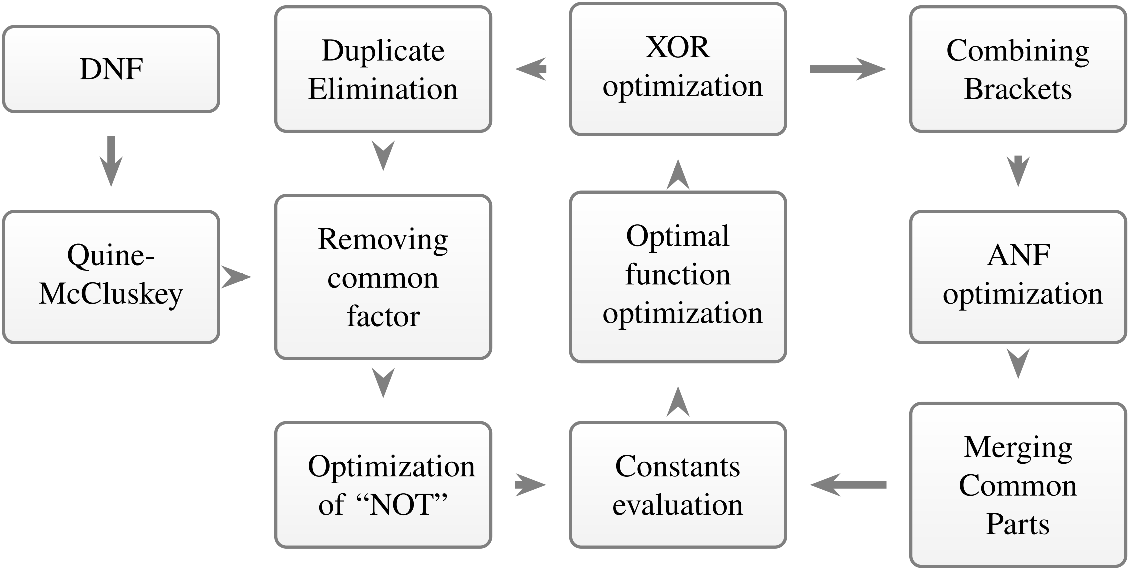
	AND	OR	NOT	XOR	Total
$\overline{I_{0,0,0,0}(r)}$		3			3
$I_{0,0,0,0}(r)$			1		1
Final glue by every coordinate	1			1(2)	
Final glue for all coordinaetes	4			5	9

$\boxed{\text{Total: 13 Boolean operations}}$

There are 5 non-linear elements in the considered decomposition:

I	0, 1, c, 8, 6, f, 4, e, 3, d, b, a, 2, 9, 7, 5
v_0	2, 5, 3, b, 6, 9, e, a, 0, 4, f, 1, 8, d, c, 7
v_1	7, 6, c, 9, 0, f, 8, 1, 4, 5, b, e, d, 2, 3, a
φ	b, 2, b, 8, c, 4, 1, c, 6, 3, 5, 8, e, 3, 6, b
σ	c, d, 0, 4, 8, b, a, e, 3, 9, 5, 2, f, 1, 6, 7

The goal is to represent it as a set of Boolean functions in the basis of logical functions AND, OR, NOT, XOR with the minimal number of operations.


DNF
Quine-McCluskey
Removing common factor
Duplicate Elimination
Optimization of “NOT”
Constants evaluation
Optimal function optimization
XOR optimization
Combining Brackets
ANF optimization
Merging Common Parts

The total complexity of the set of functions is much less than the complexity of non-optimized functions.

Function	Number of operations
I	26
v_0	29
v_1	29
φ	33
σ	31

- We consider the possibility of bit-slicing the non-linear bijective mapping of GOST R 34-12.2015 «Kuznyechik» block cipher.
- It should be noted that in 2016 “A Method of Constructing S-boxes With Minimal Number of Logical Elements” got a patent in Russian Federation. The method protected by this patent allows to realize non-linear mapping of Kuznyechick cipher with complexity of 681 Boolean operations.
- Our results are presented below:

	AND	*OR*	*NOT*	*XOR*	Total
I	8	5	4	9	26
v_0	9	5	6	9	29
v_1	4	3	3	7	17
φ	11	6	8	7	32
σ	11	6	7	9	33
α and ω				14	14
multiplication in $GF\left(2^4\right)$	16			15	31
branchng elimination	4	3	1	5	13
	79	28	29	90	Total: 226

Thank you for your attention!

Questions?