Unbalanced-Bridge used in PIPO

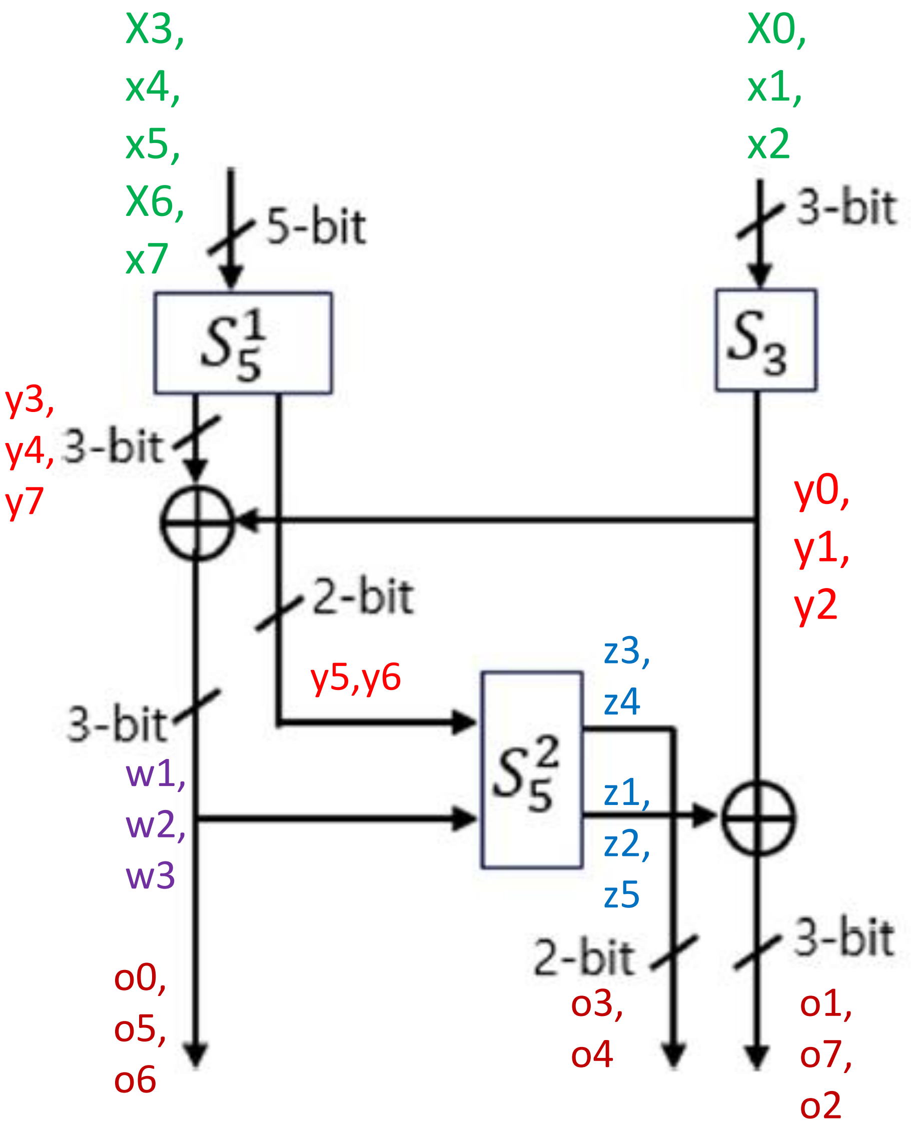
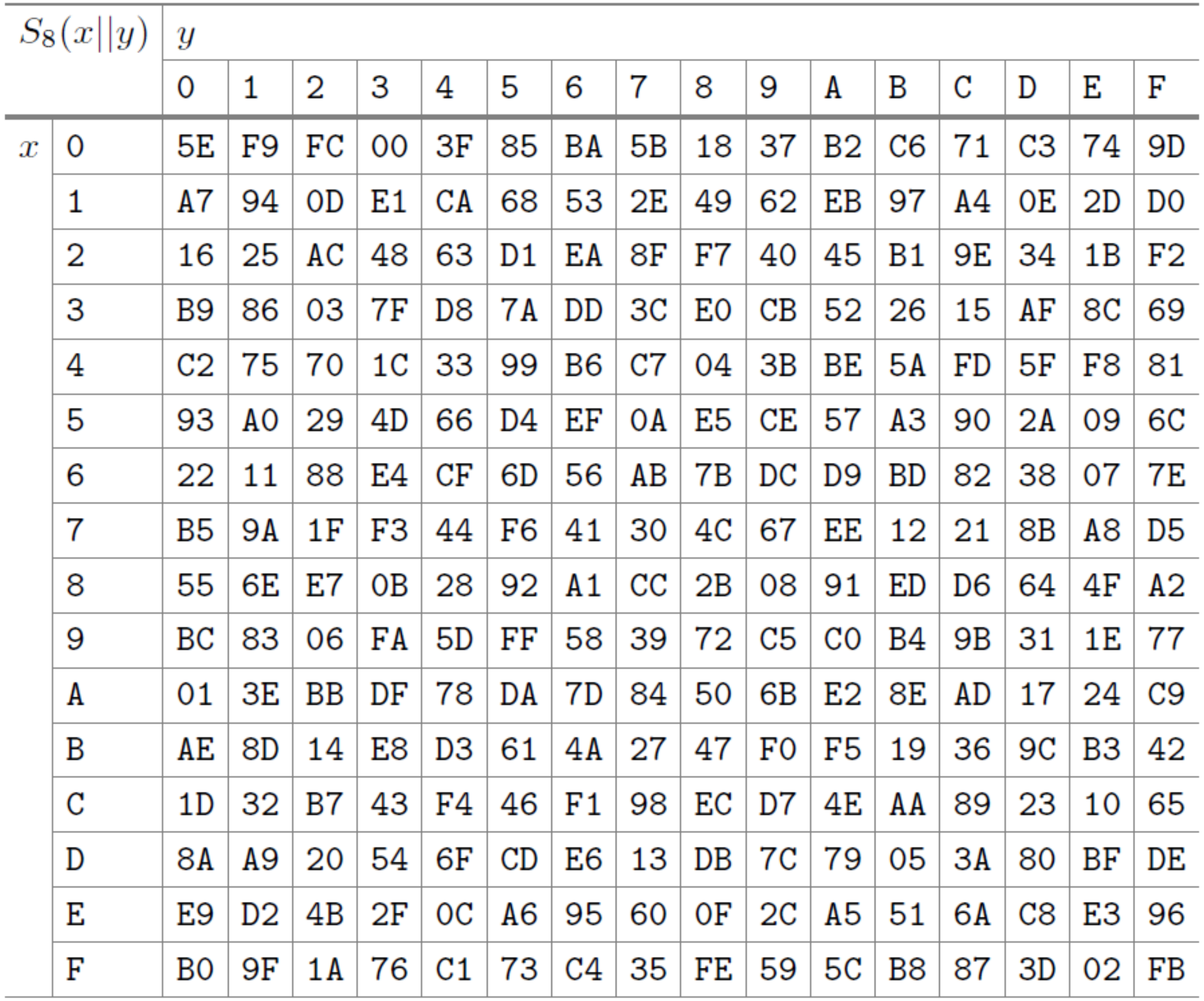


Fig. 3. The unbalanced-Bridge structure

W2 = y0 + y4 → o5
W3 = y1 + y7 → o0
W1 = y2 + y3 → o6

o1 = y0 + z1
o7 = y1 + z2
o2 = y2 + z5

z3 → o4
z4 → o3



$S_8(x\|\|y)$		y															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x	0	5E	F9	FC	00	3F	85	BA	5B	18	37	B2	C6	71	C3	74	9D
	1	A7	94	0D	E1	CA	68	53	2E	49	62	EB	97	A4	0E	2D	D0
	2	16	25	AC	48	63	D1	EA	8F	F7	40	45	B1	9E	34	1B	F2
	3	B9	86	03	7F	D8	7A	DD	3C	E0	CB	52	26	15	AF	8C	69
	4	C2	75	70	1C	33	99	B6	C7	04	3B	BE	5A	FD	5F	F8	81
	5	93	A0	29	4D	66	D4	EF	0A	E5	CE	57	A3	90	2A	09	6C
	6	22	11	88	E4	CF	6D	56	AB	7B	DC	D9	BD	82	38	07	7E
	7	B5	9A	1F	F3	44	F6	41	30	4C	67	EE	12	21	8B	A8	D5
	8	55	6E	E7	0B	28	92	A1	CC	2B	08	91	ED	D6	64	4F	A2
	9	BC	83	06	FA	5D	FF	58	39	72	C5	C0	B4	9B	31	1E	77
	A	01	3E	BB	DF	78	DA	7D	84	50	6B	E2	8E	AD	17	24	C9
	B	AE	8D	14	E8	D3	61	4A	27	47	F0	F5	19	36	9C	B3	42
	C	1D	32	B7	43	F4	46	F1	98	EC	D7	4E	AA	89	23	10	65
	D	8A	A9	20	54	6F	CD	E6	13	DB	7C	79	05	3A	80	BF	DE
	E	E9	D2	4B	2F	0C	A6	95	60	0F	2C	A5	51	6A	C8	E3	96
	F	B0	9F	1A	76	C1	73	C4	35	FE	59	5C	B8	87	3D	02	FB

8-bit S-box of PIPO
(Example: S(C2)=B7)

We have used the “bitsliced implementation of the S8 (in C code)” in [1] to get the table of three S-boxes in the bridge structure.

The bridge.py code verifies the compliance of the obtained S-boxes in the bridge structure with the 8-bit PIPO S-box table.

7~0	7	6	5	4	3	2	1	0	X[0]
15~8	15	14	13	12	11	10	9	8	X[1]
23~16	23	22	21	20	19	18	17	16	X[2]
31~24	31	30	29	28	27	26	25	24	X[3]
39~32	39	38	37	36	35	34	33	32	X[4]
47~40	47	46	45	44	43	42	41	40	X[5]
55~48	55	54	53	52	51	50	49	48	X[6]
63~56	63	62	61	60	59	58	57	56	X[7]

[1]. Kim, Hangi, et al. "A new method for designing lightweight S-boxes with high differential and linear branch numbers, and its application." *IEEE Access* 9 (2021): 150592-150607.