1 Upper Bounds on Degree of the Permutations of Keccak and KNOT

Table 1. The upper bounds on degree of KECCAK-f and its inverse.

Forward			Backward			
#Round	#Bound		#Round	#Bound		
	[2, 1, 3]	Sect.3.3		[2]	[4, 1, 3]	Sect.3.3
1	2	2	1	3	3	3
2	4	4	2	9	9	9
3	8	8	3	27	27	27
4	16	16	4	81	81	81
5	32	32	5	243	243	**229**
6	64	64	6	729	729	**557**
7	128	128	7	1309	1309	**1079**
8	256	**252**	8	1503	1454	**1339**
9	512	**474**	9	1567	1532	**1469**
10	1024	**809**	10	1589	1566	**1534**
11	1408	**1336**	11	1596	1583	**1567**
12	1536	**1512**	12	1598	1591	**1583**
13	1578	**1570**	13	1599	1595	**1591**
14	1592	**1590**	14		1597	**1595**
15	1597	**1596**	15		1598	**1597**
16	1599	**1598**	16		1599	**1598**
17		**1599**	17			**1599**

Table 2. The upper bounds on degree of KNOT-256 and its inverse.

Forward			Backward		
#Round	#Bound		#Round	#Bound	
	[1, 3]	Sect.3.3		[1, 3]	Sect.3.3
1	3	3	1	3	3
2	9	**8**	2	9	**8**
3	27	**17**	3	27	**17**
4	81	**35**	4	81	**36**
5	197	**65**	5	197	**66**
6	236	**104**	6	236	**101**
7	249	**150**	7	249	**141**
8	253	**197**	8	253	**183**
9	255	**229**	9	255	**222**
10		**245**	10		**243**
11		**251**	11		**250**
12		**254**	12		**254**
13		**255**	13		**255**

Table 3. The upper bounds on degree of KNOT-384 and its inverse.

Forward			Backward		
#Round	#Bound		#Round	#Bound	
	[1, 3]	Sect.3.3		[1, 3]	Sect.3.3
1	3	3	1	3	3
2	9	**8**	2	9	**8**
3	27	**17**	3	27	**17**
4	81	**35**	4	81	**36**
5	243	**68**	5	243	**68**
6	337	**112**	6	337	**116**
7	368	**173**	7	368	**183**
8	378	**247**	8	378	**263**
9	382	**317**	9	382	**326**
10	383	**358**	10	383	**361**
11		**377**	11		**375**
12		**379**	12		**380**
13		**382**	13		**382**
14		**383**	14		**383**

Table 4. The upper bounds on degree of KNOT-512 and its inverse.

Forward			Backward		
#Round	#Bound		#Round	#Bound	
	[1, 3]	Sect.3.3		[1, 3]	Sect.3.3
1	3	3	1	3	3
2	9	**8**	2	9	**8**
3	27	**17**	3	27	**17**
4	81	**35**	4	81	**36**
5	243	**68**	5	243	**68**
6	422	**113**	6	422	**115**
7	482	**179**	7	482	**182**
8	502	**264**	8	502	**262**
9	508	**359**	9	508	**350**
10	510	**441**	10	510	**428**
11	511	**485**	11	511	**479**
12		**503**	12		**501**
13		**509**	13		**508**
14		**510**	14		**510**
15		**511**	15		**511**

2 Upper Bounds on the Degree of Trivium and Kreyvium

Table 5. The upper bound on degree of Trivium up to 793 rounds evaluated by numeric mapping.

#Round	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**
0		1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
20	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
40	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
60	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	2
80	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
100	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
120	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
140	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
160	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	3	3
180	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
200	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
220	3	3	3	3	3	3	3	3	3	3	4	4	4	4	4	4	4	4	4	4
240	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
260	4	4	4	4	4	4	4	4	4	4	4	4	5	5	5	5	5	5	5	5
280	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
300	5	5	5	5	5	5	5	5	5	6	6	6	6	6	6	6	6	6	6	6
320	6	6	6	6	6	6	7	7	7	7	7	7	7	7	7	7	7	7	7	7
340	7	7	7	7	7	7	7	7	7	7	7	8	8	8	8	8	8	8	8	8
360	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
380	8	8	8	8	8	8	8	9	9	9	9	9	9	9	9	9	9	9	9	9
400	9	9	9	9	9	9	9	9	9	9	9	9	9	9	9	9	9	9	10	10
420	10	10	10	10	10	10	10	10	10	11	11	11	11	11	11	11	11	11	12	12
440	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12
460	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13
480	13	13	13	13	13	13	13	14	14	14	14	14	14	14	14	14	14	14	14	15
500	15	15	15	15	15	15	15	15	15	15	15	16	18	18	18	18	18	18	18	18
520	18	18	18	18	18	18	18	18	18	19	19	19	19	19	19	19	19	19	19	19
540	19	20	20	20	20	20	20	21	21	21	21	21	21	21	22	22	22	22	22	22
560	22	22	22	22	22	22	23	24	24	24	24	24	24	24	24	24	24	24	25	25
580	25	25	25	26	26	26	26	26	26	26	27	29	29	29	29	30	30	30	30	30
600	30	30	30	30	30	30	30	30	31	32	32	32	32	32	32	32	32	32	32	32
620	33	33	33	33	33	33	34	34	34	34	34	34	34	35	35	35	35	35	35	35
640	35	35	35	35	36	36	36	36	36	36	36	36	36	37	37	37	37	37	37	38
660	38	38	38	38	38	38	38	38	39	42	43	43	43	43	43	43	43	44	45	45
680	45	45	45	45	45	45	46	46	46	46	46	46	46	46	46	47	48	48	48	48
700	48	48	49	50	51	51	51	51	51	51	51	52	53	53	53	53	53	53	53	53
720	54	55	55	55	55	55	55	55	55	55	55	55	55	55	55	56	56	56	57	57
740	57	57	57	57	57	57	58	59	60	60	60	60	60	60	60	61	63	64	64	64
760	64	64	64	64	64	64	64	64	65	69	71	71	71	71	71	71	71	71	71	71
780	72	75	76	76	76	76	77	78	78	78	78	78	78	79						

Table 6. The upper bound on degree of Trivium up to 839 rounds evaluated by division property.

#Round	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**
0		1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
20	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
40	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
60	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	2
80	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
100	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
120	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
140	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
160	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	3	3
180	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
200	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
220	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
240	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
260	3	3	3	3	3	4	4	4	4	4	4	4	5	5	5	5	5	5	5	5
280	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
300	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
320	5	5	5	5	5	5	6	6	6	6	6	6	6	6	6	6	6	6	6	6
340	6	6	6	6	6	6	6	6	6	7	7	8	8	8	8	8	8	8	8	8
360	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
380	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
400	8	8	8	8	8	8	8	8	8	8	8	8	8	9	9	9	9	9	9	9
420	10	10	10	10	10	10	10	10	10	11	11	11	11	11	11	11	11	11	12	12
440	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12
460	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13
480	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13
500	13	13	13	13	13	13	13	13	14	14	13	14	14	15	16	16	16	16	16	16
520	16	16	16	16	16	16	16	16	16	17	17	17	17	17	17	17	17	17	18	18
540	18	19	19	19	19	19	19	19	19	20	20	20	20	20	21	21	21	21	21	21
560	21	21	21	21	21	21	21	21	21	21	21	21	21	22	22	22	22	22	22	22
580	23	23	23	23	23	23	23	23	23	24	24	24	24	24	25	26	26	27	27	27
600	27	27	27	27	27	27	27	27	28	29	29	30	30	30	30	30	30	30	31	31
620	32	32	32	32	32	32	32	32	32	32	32	33	33	34	34	34	34	34	34	34
640	34	34	34	34	34	34	34	34	34	34	34	34	35	35	35	35	35	35	35	36
660	36	36	36	36	37	37	37	37	38	38	38	39	39	39	39	39	39	40	40	40
680	41	41	41	42	42	42	43	43	43	43	44	44	44	44	44	45	45	46	46	46
700	47	47	46	47	47	47	48	48	48	49	49	50	50	51	51	51	51	52	51	52
720	52	53	53	54	54	54	54	54	54	54	54	54	54	54	54	54	54	54	55	55
740	56	56	56	56	56	56	56	56	56	57	57	56	56	56	56	56	57	58	57	58
760	58	58	58	58	58	59	59	59	59	59	60	59	59	60	60	60	60	61	61	62
780	62	62	62	63	62	62	63	63	63	64	64	64	64	65	66	66	66	67	67	67
800	67	67	68	68	68	69	69	71	70	71	72	71	71	71	71	72	73	73	73	74
820	75	75	75	76	76	76	76	76	77	78	78	79	79	79	78	78	79	79	79	79

Table 7. The upper bound on degree of Kreyvium up to 862 rounds evaluated by numeric mapping.

#Round	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**
0		1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
20	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
40	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
60	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2
80	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
100	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
120	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
140	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
160	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3
180	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
200	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
220	3	3	3	3	3	3	3	4	4	4	4	4	4	4	4	4	4	4	4	4
240	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
260	4	4	4	4	4	4	4	4	4	5	5	5	5	5	5	5	5	5	5	5
280	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
300	5	5	5	5	5	5	6	6	6	6	6	6	6	6	6	6	6	6	6	6
320	6	6	6	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7
340	7	7	7	7	7	7	7	7	8	8	8	8	8	8	8	8	8	8	8	8
360	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
380	8	8	8	8	9	9	9	9	9	9	9	9	9	9	9	9	9	9	9	9
400	9	9	9	9	9	9	9	9	9	9	9	9	9	9	9	10	10	10	10	10
420	10	10	10	10	10	10	11	11	11	11	11	11	11	11	11	12	12	12	12	12
440	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	13	13	13
460	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13
480	13	13	13	13	14	14	14	14	14	14	14	14	14	14	14	14	15	15	15	15
500	15	15	15	15	15	15	15	15	16	18	18	18	18	18	18	18	18	18	18	18
520	18	18	18	18	18	18	19	19	19	19	19	19	19	19	19	19	19	19	20	20
540	20	20	20	20	21	21	21	21	21	21	21	22	22	22	22	22	22	22	22	22
560	22	22	22	23	24	24	24	24	24	24	24	24	24	24	24	25	25	25	25	25
580	26	26	26	26	26	26	26	27	29	29	29	29	30	30	30	30	30	30	30	30
600	30	30	30	30	30	31	32	32	32	32	32	32	32	32	32	32	32	33	33	33
620	33	33	33	34	34	34	34	34	34	34	35	35	35	35	35	35	35	35	35	35
640	35	36	36	36	36	36	36	36	36	36	37	37	37	37	37	37	38	38	38	38
660	38	38	38	38	38	39	42	43	43	43	43	43	43	43	44	45	45	45	45	45
680	45	45	45	46	46	46	46	46	46	46	46	46	47	48	48	48	48	48	48	49
700	50	51	51	51	51	51	51	51	52	53	53	53	53	53	53	53	53	54	55	55
720	55	55	55	55	55	55	55	55	55	55	55	55	56	56	56	57	57	57	57	57
740	57	57	57	58	59	60	60	60	60	60	60	60	61	63	64	64	64	64	64	64
760	64	64	64	64	64	65	69	71	71	71	71	71	71	71	71	71	71	72	75	76
780	76	76	76	77	78	78	78	78	78	78	79	82	82	82	82	83	84	84	84	84
800	84	85	85	85	85	85	85	86	87	88	89	89	89	90	90	90	91	91	91	91
820	92	93	93	93	93	94	97	99	99	99	99	100	103	106	107	107	107	108	108	108
840	108	108	108	108	109	114	118	118	118	119	120	120	120	120	120	120	121	124	125	125
860	125	126	127																	

Table 8. The upper bound on degree of Kreyvium up to 897 rounds evaluated by division property.

#Round	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**
0		1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
20	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
40	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
60	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2
80	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
100	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
120	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
140	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
160	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3
180	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
200	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
220	3	3	3	3	3	3	3	4	4	4	4	4	4	4	4	4	4	4	4	4
240	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
260	4	4	4	4	4	4	4	4	4	5	5	5	5	5	5	5	5	5	5	5
280	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
300	5	5	5	5	5	5	6	6	6	6	6	6	6	6	6	6	6	6	6	6
320	6	6	6	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7
340	7	7	7	7	7	7	7	7	8	8	8	8	8	8	8	8	8	8	8	8
360	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
380	8	8	8	8	9	9	9	9	9	9	9	9	9	9	9	9	9	9	9	9
400	9	9	9	9	9	9	9	9	9	9	9	9	9	9	9	10	10	10	10	10
420	10	10	10	10	10	10	11	11	11	11	11	11	11	11	11	12	12	12	12	12
440	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	13	13	13
460	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13
480	13	13	13	13	13	13	13	13	13	13	13	13	13	14	14	14	15	15	15	15
500	15	15	15	15	15	15	15	15	16	17	18	18	18	18	18	18	18	18	18	18
520	18	18	18	18	18	18	19	19	19	19	19	19	19	19	19	19	19	19	20	20
540	20	20	20	20	21	21	21	21	21	21	21	22	22	22	22	22	22	22	22	22
560	22	22	22	22	22	23	23	23	23	23	23	23	23	23	23	24	25	25	25	25
580	25	26	26	26	26	26	26	27	28	29	29	29	30	30	30	30	30	30	30	30
600	30	30	30	30	30	31	31	32	32	32	32	32	32	32	32	32	32	33	33	33
620	33	33	33	34	34	34	34	34	34	34	35	35	35	35	35	35	35	35	35	35
640	35	36	36	36	36	36	36	36	36	36	37	37	37	37	37	37	69	38	38	38
660	38	38	38	38	38	38	39	40	41	41	42	42	42	42	42	43	43	44	44	44
680	44	44	44	44	45	45	45	45	46	46	46	46	46	47	47	47	47	48	48	48
700	49	49	50	50	50	51	51	51	51	52	52	52	53	53	53	53	53	53	53	54
720	54	55	55	55	55	55	55	55	55	55	55	55	55	55	55	56	56	57	57	57
740	57	57	57	57	58	58	59	59	60	60	60	60	60	60	60	61	62	62	62	63
760	63	63	63	63	63	63	64	64	64	64	64	65	65	66	66	66	67	67	68	68
780	68	68	69	69	70	71	71	72	72	72	72	73	74	75	75	76	76	77	77	78
800	78	78	78	79	79	79	80	80	81	81	81	82	82	83	84	84	85	85	86	86
820	87	87	88	88	89	89	90	91	91	93	93	93	93	93	94	95	95	96	96	96
840	97	97	98	98	98	99	99	100	101	102	102	102	102	103	103	104	104	105	106	107
860	108	108	108	109	110	111	111	111	112	112	113	114	114	115	115	115	116	117	117	117
880	118	118	119	120	120	121	121	122	122	123	123	123	124	125	125	126	127	127		

References

1. Christina Boura and Anne Canteaut. On the influence of the algebraic degree of F^{-1} on the algebraic degree of $G \circ F$. *IEEE Trans. Inf. Theory*, 59(1):691–702, 2013.
2. Christina Boura, Anne Canteaut, and Christophe De Cannière. Higher-order differential properties of Keccak and *Luffa*. In Antoine Joux, editor, *Fast Software Encryption - 18th International Workshop, FSE 2011, Lyngby, Denmark, February 13-16, 2011, Revised Selected Papers*, volume 6733 of *Lecture Notes in Computer Science*, pages 252–269. Springer, 2011.
3. Claude Carlet. Graph indicators of vectorial functions and bounds on the algebraic degree of composite functions. *IEEE Trans. Inf. Theory*, 66(12):7702–7716, 2020.
4. Ming Duan and Xuejia Lai. Improved zero-sum distinguisher for full round Keccak-f permutation. *IACR Cryptology ePrint Archive*, 2011:23, 2011.