

Runtime (ms)

p	r	h / r	A	B	C	D	Total	Nb Permutations
53	3	2	2,81	12,77	0,13	36,78	82,23	2809
		3	5,98	13,93	0,12	36,54	56,57	
		4	11,19	41,76	0,16	35,88	89	
		5	18,98	64,47	0,2	38,88	122,52	
		6	27,24	94,21	0,24	38,35	160,04	
		7	38,35	162,77	0,29	37,52	238,93	
		8	52,06	260,83	0,27	36,3	349,46	
		9	66,76	269,13	0,37	35,8	372,06	
		10	84,39	418,92	0,39	36,68	540,38	
	4	2	4,23	14,15	0,11	37,1	55,59	
		3	10,28	15,64	12	36,65	62,69	
		4	19,39	16,88	0,13	38,35	74,76	
		5	32,89	55,13	0,18	38,38	126,58	
		6	48,91	62,32	0,17	40,04	151,43	
		7	70,11	111,24	0,19	39,26	220,8	
		8	92,18	142,5	0,24	39,78	274,7	
		9	120,64	217,36	0,24	36,2	374,44	
		10	152,26	239,48	0,27	36,5	428,51	
		11	183,83	298,29	0,29	36,06	518,46	
		12	226,47	413,92	0,36	35,36	676,12	
251	3	4	28,63	199,05	0,38	3558,34	3786,4	63001
		6	72,95	450,43	0,57	3554,24	4078,2	
		8	137,46	1256,63	0,83	3572,09	4967,01	
		10	229,97	2033,79	1,25	3564,4	5829,43	
		12	357,6	3155,66	1,75	3550,48	7065,5	
		14	511,4	4946,56	2,37	3537,78	8998,11	
		16	709	6191	2,7	3521,27	10425,15	
	4	5	86,85	268,4	0,44	3576,28	3934,09	
		10	450,99	1186,84	0,78	3565,75	5204,36	
		15	1230,17	3340,35	1,41	3570,03	8141,96	
		20	2489,44	7706,98	2,43	3589,95	13788,8	
	5	5	134,97	101,44	0,31	3559,9	3796,63	
		10	750,95	930,73	0,6	3544,34	5226,61	
		15	2120,06	2905,3	1,1	3557,56	8584,02	
		20	4363,62	6882,45	1,95	3538,7	14786,72	

A Precomputation

B Construction of M

C Sidelnikov Shestakov attack

D Generation of possible permutations