This document provides supplementary materials for the article, including tables containing the results of experiments. All notations are the same as those used in the article itself.

These tables also include data on experiments based on LEC problems of sorting algorithms. Therefore, we have slightly expanded the description of the benchmarks and functions used in Construction 1.

A. Benchmarks description

The first class of benchmarks we considered is a variety of particularly challenging LEC instances for circuits that perform specific arithmetic functions, such as multipliers and sorting algorithms. Specifically, we examined two categories of LEC instances:

1) LEC for two different multiplication algorithms: we considered the "Column multiplier", "Wallace tree", "Karatsuba decomposition", and "Dadda multiplier". These instances are denoted as $\texttt{AvB}_k$, where `A` and `B` represent the multiplication algorithms, and k is the number of bits in the multiplied numbers. For instance, $\texttt{CvK}_{16}$ represents the LEC instance for Column and Karatsuba multiplication algorithms for two 16-bits numbers (`16x16` multiplier). This leads to six classes of LEC instances: $\texttt{CvK}_k$, $\texttt{CvW}_k$, $\texttt{DvC}_k$, $\texttt{DvK}_k$, $\texttt{DvW}_k$, $\texttt{KvW}_k$.
2) LEC for different sorting algorithms: we considered the "bubble sort", "selection sort", and "pancake sort" algorithms. The corresponding LEC instances are denoted by $\texttt{AvB}_{k,l}$, where `A` and `B` represent the sorting algorithms, k is the number of sorted numbers and l is the number of bits in each number. For instance, $\texttt{BvP}_{9,4}$ denotes the LEC for Bubble and Pancake sorting algorithms that sort nine 4-bit numbers. The test instances are denoted by $\texttt{BvP}_{k,l}$ ("Bubble vs Pancake"), $\texttt{SvB}_{k,l}$ ("Selection vs Bubble"), $\texttt{PvS}_{k,l}$ ("Pancake vs Selection").

The second class consists of several (satisfiable) instances related to algebraic cryptanalysis, specifically the SAT encodings of the preimage attack on the reduced-round MD4 compression function. In our experiments, we selected two CNFs (md4_40steps_11.30-32Dobb_one_constr_one_hash, referred to as $\texttt{MD4}_{40}$, and md4_43steps_12Dobb_one_constr_one_hash, referred to as $\texttt{MD4}_{43}$) from the repository[1] presented in [23]. These CNFs correspond to two cryptanalysis instances that are neither too easy nor too difficult.

B. Functions for Construction 1

For Construction 1, we used a partitioning of the set X^{in} into disjoint sets of variables. Function λ_1^j used in Construction 1 was selected experimentally as follows ($\lambda_2^j = \neg\lambda_1^j$ in all cases):

- i-XOR: $\lambda_1^j = (x_1^j \oplus x_2^j \oplus ... \oplus x_i^j)$;
- 2-DIS: $\lambda^1 = x_1 \vee x_2$;
- 3-MAJ: $\lambda_1^j = \texttt{majority}(x_1^j, x_2^j, x_3^j)$, where $\texttt{majority}(a, b, c) = a \wedge b \vee a \wedge c \vee b \wedge c$;
- 4-BENT: $\lambda_1^j = x_1^j \wedge x_3^j \oplus x_2^j \wedge x_4^j$.

Functions λ^j for $j > 1$ are defined over the corresponding subsequent disjoint chunks of inputs, e.g. $\lambda^2 = x_4 \oplus x_5 \oplus x_6$ for `3-XOR`.

C. Tables description

- Tables I to VI contain detailed information on experiments with 12x12 multipliers;
- Table VII provides detailed information on experiments with 16x16 multipliers;
- Table VIII displays the results of an experiment comparing the computation of the decomposition hardness of 12x12 multipliers with different orders of the input variables. For each instance, the hardness was computed using Constructions 1 and 2 for 5 different random orders of input variables;
- Table IX is an extended version of Table III from our article and contains detailed data on the construction of estimates of the decomposition hardness of the non-full-round MD4 inversion problem, relaxed by Dobbertin constraints. This table also shows the exact values of the decomposition hardness of the considered problems w.r.t. to different partitionings;
- Table X contains detailed data on experiments on the decomposition hardness of LEC problems for sorting algorithms.

[1] https://github.com/olegzaikin/MD4-CnC

TABLE I
EXPERIMENTAL RESULTS FOR PARTITIONINGS. $\texttt{CvK}_{12}$.

Partitioning (type / size)	Avg ± sd time, s	Min – max time, s	Total time, s
Sequential	—	—	36 864
2-XOR / 4 096	2.87 ± 0.15	2.43 – 3.6	11 751
2-DIS / 4 096	17.35 ± 15.27	1.83 – 218.47	71 075
3-MAJ / 256	21.24 ± 1.12	18.29 – 26.39	5 437
3-XOR / 256	20.76 ± 0.91	18.55 – 23.84	5 314
INT / 32	176.45 ± 20.22	134.32 – 211.85	5 647
INT / 64	74.61 ± 7.01	52.89 – 87.1	4 775
INT / 100	45.19 ± 4.48	28.41 – 55.42	4 520
INT / 128	33.03 ± 3.16	21.26 – 39.18	4 228
INT / 200	21.31 ± 2.2	12.44 – 27.28	4 263
INT / 256	15.71 ± 1.41	9.05 – 18.35	4 021
INT / 300	14.16 ± 1.43	7.44 – 19.95	4 248
INT / 400	10.73 ± 1.06	5.07 – 12.93	4 293
INT / 500	8.8 ± 0.87	4.17 – 10.93	4 401
INT / 512	8.01 ± 0.74	3.71 – 9.72	4 102
INT / 600	7.45 ± 0.79	2.73 – 9.93	4 471
INT / 1 024	4.49 ± 0.46	1.49 – 5.55	4 596
CnC-d8 / 256	16.05 ± 12.22	2.95 – 133.19	4 110
CnC-def. / 56 404	0.15 ± 0.23	0.01 – 11.8	8 358
CnC-n4600 / 273	16.47 ± 30.42	2.12 – 418.31	4 498
CnC-default incremental iGlucose			16 782
CnC-default incremental Cadical v1.5.3			9 427

TABLE II
EXPERIMENTAL RESULTS FOR PARTITIONINGS. $\texttt{CvW}_{12}$.

Partitioning (type / size)	Avg ± sd time, s	Min – max time, s	Total time, s
Sequential	—	—	6 612
2-XOR / 4 096	1.72 ± 0.12	1.34 – 2.14	7 032
2-DIS / 4 096	13.01 ± 14.42	0.17 – 150.52	53 304
3-MAJ / 256	14.98 ± 3.4	3.57 – 24.88	3 836
3-XOR / 256	16.96 ± 1.02	14.62 – 20.21	4 343
INT / 32	140.81 ± 49.68	25.05 – 222.69	4 506
INT / 64	60.0 ± 21.15	6.7 – 99.99	3 840
INT / 100	34.91 ± 10.49	3.39 – 51.01	3 492
INT / 128	25.39 ± 7.79	1.99 – 40.28	3 251
INT / 200	14.97 ± 4.24	1.01 – 25.7	2 995
INT / 256	10.97 ± 3.02	0.57 – 16.92	2 809
INT / 300	9.6 ± 2.64	0.47 – 18.57	2 880
INT / 400	6.88 ± 1.75	0.19 – 11.44	2 751
INT / 500	5.46 ± 1.37	0.16 – 8.34	2 731
INT / 512	5.1 ± 1.32	0.14 – 7.38	2 614
INT / 600	4.48 ± 1.1	0.09 – 7.42	2 686
INT / 1 024	2.53 ± 0.63	0.02 – 3.68	2 589
CnC-d8 / 256	18.66 ± 253.93	0.74 – 4 065.08	4 777
CnC-def. / 73 359	0.06 ± 0.08	0.0 – 3.08	4 074
CnC-n2850 / 261	13.73 ± 30.76	0.62 – 298.97	3 584
CnC-default incremental iGlucose			7 916
CnC-default incremental Cadical v1.5.3			7 592

TABLE III
EXPERIMENTAL RESULTS FOR PARTITIONINGS. $\texttt{DvC}_{12}$.

Partitioning (type / size)	Avg ± sd time, s	Min – max time, s	Total time, s
Sequential	—	—	3 299
2-XOR / 4 096	1.63 ± 0.11	1.34 – 2.11	6 673
2-DIS / 4 096	10.5 ± 10.23	0.23 – 151.78	42 992
3-MAJ / 256	13.49 ± 2.09	5.51 – 19.95	3 455
3-XOR / 256	13.95 ± 1.0	11.48 – 16.83	3 571
INT / 32	96.46 ± 30.92	17.33 – 157.67	3 087
INT / 64	43.11 ± 12.1	4.7 – 62.38	2 759
INT / 100	26.74 ± 7.28	2.14 – 40.42	2 675
INT / 128	20.02 ± 5.28	1.73 – 30.75	2 563
INT / 200	12.41 ± 3.08	0.69 – 19.59	2 482
INT / 256	8.87 ± 2.19	0.36 – 12.92	2 272
INT / 300	8.29 ± 2.17	0.34 – 14.32	2 488
INT / 400	5.93 ± 1.48	0.15 – 10.46	2 372
INT / 500	4.76 ± 1.15	0.08 – 9.18	2 379
INT / 512	4.34 ± 1.05	0.08 – 6.62	2 224
INT / 600	3.97 ± 0.94	0.04 – 6.67	2 384
INT / 1 024	2.19 ± 0.54	0.01 – 3.38	2 247
CnC-d8 / 256	9.66 ± 20.28	1.16 – 275.34	2 474
CnC-def. / 80 956	0.05 ± 0.08	0.0 – 3.02	4 054
CnC-n2800 / 250	11.07 ± 30.81	0.57 – 262.87	2 767
CnC-default incremental iGlucose			6 205
CnC-default incremental Cadical v1.5.3			5 893

TABLE IV
EXPERIMENTAL RESULTS FOR PARTITIONINGS. $\texttt{DvK}_{12}$.

Partitioning (type / size)	Avg ± sd time, s	Min – max time, s	Total time, s
Sequential	—	—	36 224
2-XOR / 4 096	2.89 ± 0.17	2.46 – 3.76	11 824
2-DIS / 4 096	18.66 ± 16.95	1.84 – 235.98	76 414
3-MAJ / 256	23.3 ± 1.64	19.16 – 30.39	5 966
3-XOR / 256	22.96 ± 1.12	21.02 – 27.28	5 879
INT / 32	191.41 ± 15.84	162.17 – 217.88	6 126
INT / 64	83.39 ± 8.07	58.91 – 100.33	5 338
INT / 100	49.93 ± 5.21	34.96 – 64.33	4 993
INT / 128	35.73 ± 3.24	24.25 – 43.33	4 574
INT / 200	23.62 ± 2.88	11.74 – 36.04	4 724
INT / 256	16.99 ± 1.72	10.15 – 21.59	4 349
INT / 300	15.57 ± 1.95	7.38 – 21.77	4 672
INT / 400	11.32 ± 1.22	4.81 – 14.1	4 530
INT / 500	9.45 ± 1.06	3.7 – 12.7	4 726
INT / 512	8.51 ± 0.96	3.6 – 11.22	4 355
INT / 600	7.83 ± 0.88	2.8 – 11.08	4 697
INT / 1 024	4.69 ± 0.55	1.44 – 6.15	4 806
CnC-d8 / 256	17.04 ± 11.8	0.17 – 65.03	4 362
CnC-def. / 68 995	0.13 ± 0.19	0.01 – 9.94	8 639
CnC-n4450 / 246	20.16 ± 39.43	2.06 – 463.09	4 959
CnC-default incremental iGlucose			16 767
CnC-default incremental Cadical v1.5.3			9 759

TABLE V
EXPERIMENTAL RESULTS FOR PARTITIONINGS. $\texttt{DvW}_{12}$.

Partitioning (type / size)	Avg ± sd time, s	Min – max time, s	Total time, s
Sequential	—	—	10 373
2-XOR / 4 096	1.74 ± 0.13	1.42 – 2.16	7 118
2-DIS / 4 096	14.19 ± 14.76	0.19 – 199.22	58 129
3-MAJ / 256	17.16 ± 3.22	4.36 – 26.92	4 392
3-XOR / 256	18.79 ± 1.11	16.16 – 22.4	4 810
INT / 32	155.89 ± 48.06	30.02 – 225.99	4 989
INT / 64	70.88 ± 21.88	7.9 – 104.63	4 537
INT / 100	42.48 ± 12.81	2.75 – 68.47	4 249
INT / 128	31.0 ± 9.52	2.47 – 49.06	3 969
INT / 200	18.37 ± 5.33	0.9 – 30.43	3 675
INT / 256	12.92 ± 3.69	0.59 – 20.11	3 308
INT / 300	11.39 ± 3.16	0.4 – 19.23	3 418
INT / 400	8.02 ± 2.24	0.21 – 13.02	3 209
INT / 500	6.27 ± 1.65	0.12 – 10.12	3 138
INT / 512	5.8 ± 1.61	0.11 – 10.14	2 972
INT / 600	5.13 ± 1.35	0.06 – 8.95	3 078
INT / 1 024	2.81 ± 0.79	0.02 – 4.83	2 880
CnC-d8 / 256	15.85 ± 135.66	1.21 – 2 176.97	4 058
CnC-def. / 53 954	0.08 ± 0.17	0.0 – 21.06	4 210
CnC-n2650 / 293	13.24 ± 34.91	0.63 – 374.09	3 880
CnC-default incremental iGlucose			10 320
CnC-default incremental Cadical v1.5.3			9 710

TABLE VI
EXPERIMENTAL RESULTS FOR PARTITIONINGS. $\texttt{KvW}_{12}$.

Partitioning (type / size)	Avg ± sd time, s	Min – max time, s	Total time, s
Sequential	—	—	37 339
2-XOR / 4 096	2.88 ± 0.16	2.52 – 3.76	11 781
2-DIS / 4 096	20.35 ± 19.44	1.72 – 275.52	83 356
3-MAJ / 256	24.58 ± 2.55	19.36 – 35.41	6 292
3-XOR / 256	24.47 ± 1.05	21.95 – 29.35	6 264
INT / 32	229.09 ± 20.46	192.35 – 262.83	7 331
INT / 64	94.81 ± 9.25	70.89 – 114.68	6 068
INT / 100	57.85 ± 6.79	40.61 – 77.49	5 785
INT / 128	41.38 ± 4.44	26.5 – 49.68	5 298
INT / 200	26.14 ± 2.97	13.47 – 37.02	5 229
INT / 256	18.9 ± 2.12	10.17 – 24.08	4 839
INT / 300	16.77 ± 1.85	7.67 – 23.22	5 030
INT / 400	12.33 ± 1.39	5.42 – 16.3	4 931
INT / 500	10.12 ± 1.15	4.85 – 16.36	5 058
INT / 512	9.28 ± 1.11	4.05 – 12.4	4 750
INT / 600	8.41 ± 0.99	3.28 – 11.98	5 044
INT / 1 024	4.97 ± 0.62	1.5 – 6.97	5 091
CnC-d8 / 256	19.72 ± 21.87	0.16 – 227.13	5 048
CnC-def. / 57 516	0.15 ± 0.25	0.01 – 28.66	8 828
CnC-n4550 / 217	26.16 ± 48.27	2.26 – 524.06	5 677
CnC-default incremental iGlucose			17 716
CnC-default incremental Cadical v1.5.3			11 981

TABLE VII
EXPERIMENTAL RESULTS FOR PARTITIONINGS. MULTIPLIERS 16X16.

Inst.	Partitioning (type / size)	Avg ± sd time, s	Min – max time, s	Total time, s
$\texttt{CvK}_{16}$	Sequential	—	—	>864 000
	2-XOR / 65 536	33.24 ± 1.4	26.26 – 40.68	2 178 663
	3-MAJ / 2 048	2 093 ± 655	1 195 – 3 556	4 284 519
	3-XOR / 2 048	2 441 ± 235	1 753 – 3 243	4 998 083
	INT / 1 024	3 955 ± 573	1 422 – 5 894	4 049 359
	INT / 2 048	1 450 ± 197	460 – 2 235	2 968 692
	INT / 4 096	553 ± 59	189 – 728	2 264 599
	INT / 8 192	219 ± 22	48 – 340	1 792 975
	INT / 16 384	90 ± 7.8	9.1 – 119	1 467 434
	INT / 32 768	39.8 ± 3.7	0.9 – 54.5	1 305 053
	INT / 65 536	18.6 ± 2.2	0.01 – 26.5	1 223 521
	INT / 131 072	10.1 ± 1.2	0.01 – 14.4	1 321 271
	CnC-d16 / 65 536	22.8 ± 17.7	0.11 – 253.8	1 491 116
	CnC-n7500 / 72 617	25.2 ± 161	0.25 – 28 755	1 825 959
$\texttt{CvW}_{16}$	Sequential	—	—	>864 000
	2-XOR / 65 536	21.64 ± 1.93	15.78 – 31.41	1 418 200
	3-MAJ / 2 048	1 514 ± 734	122 – 4 394	3 098 645
	3-XOR / 2 048	2 111 ± 145	1 633 – 2 601	4 322 038
	INT / 65 536	13.37 ± 3.74	0.01 – 23.61	875 967
	INT / 131 072	6.39 ± 1.43	0.01 – 10.34	837 069
	CnC-n4500 / 51 350	27.12 ± 151	0.05 – 13 532	1 392 715
$\texttt{DvC}_{16}$	Sequential	—	—	>864 000
	2-XOR / 65 536	19.88 ± 2.11	12.44 – 29.6	1 302 856
	3-MAJ / 2 048	1 120 ± 411	257 – 2 507	2 293 699
	3-XOR / 2 048	1 221 ± 102	803 – 1 562	2 499 298
	INT / 65 536	9.12 ± 2.25	0.01 – 16.61	597 799
	INT / 131 072	4.73 ± 0.98	0.01 – 8.01	619 720
	CnC-d16 / 65 534	12.35 ± 36.08	0.01 – 2 798	809 517
	CnC-n4500 / 52 602	18.99 ± 106	0.01 – 9 240	999 001
$\texttt{DvK}_{16}$	Sequential	—	—	>864 000
	2-XOR / 65 536	35.11 ± 1.76	28.37 – 45.25	2 301 015
	3-MAJ / 2 048	2 196 ± 685	1 218 – 3 625	4 496 446
	3-XOR / 2 048	2 525 ± 212	1 977 – 3 327	5 170 873
	INT / 65 536	20.26 ± 2.55	0.01 – 31.43	1 327 640
	CnC-d16 / 65 535	25.03 ± 28.35	0.01 – 919	1 640 023
	CnC-n7400 / 58 308	33.38 ± 184	0.05 – 26 851	1 946 050
$\texttt{DvW}_{16}$	Sequential	—	—	>864 000
	2-XOR / 65 536	24.34 ± 2.16	17.69 – 36.11	1 595 147
	3-MAJ / 2 048	1 677 ± 747	147 – 4 450	3 432 961
	3-XOR / 2 048	2 145 ± 191	1 473 – 2 807	4 391 977
	INT / 65 536	13.51 ± 3.67	0.01 – 27.4	885 363
	CnC-n4300 / 54 347	24 ± 113	0.01 – 8 063	1 304 537
$\texttt{KvW}_{16}$	Sequential	—	—	>864 000
	2-XOR / 65 536	35.77 ± 1.73	28.5 – 48.46	2 344 223
	3-MAJ / 2 048	2 515 ± 799	1 310 – 4 614	5 149 410
	3-XOR / 2 048	2 816 ± 186	2 287 – 3 642	5 765 837
	INT / 65 536	21.72 ± 2.91	0.01 – 30.97	1 423 759
	CnC-d16 / 65 536	29.76 ± 93.37	0.1 – 20 495	1 950 390
	CnC-n7500 / 70 469	30.65 ± 109	0.23 – 11 294	2 159 532

TABLE VIII

EXPERIMENTAL RESULTS FOR PARTITIONINGS. MULTIPLIERS 12X12. 5 DIFFERENT RANDOM INPUT VARIABLES ORDERS FOR EVERY PARTITIONING.

Inst.	Partitioning (type / size)	Avg ± sd time, s	Min – max time, s	Total time, s
CvK_{12}	INT / 256	17.21 ± 0.85	14.99 – 19.86	4 406
	INT / 256	17.04 ± 0.96	14.88 – 21.17	4 362
	INT / 256	17.84 ± 1.14	14.72 – 21.88	4 568
	INT / 256	17.54 ± 0.97	14.86 – 20.68	4 491
	INT / 256	17.85 ± 0.93	15.42 – 20.62	4 570
	3-XOR / 256	21.25 ± 0.68	19.79 – 23.84	5 439
	3-XOR / 256	20.83 ± 0.97	19.04 – 24.86	5 333
	3-XOR / 256	20.95 ± 0.98	19.28 – 25.87	5 363
	3-XOR / 256	21.52 ± 0.88	19.25 – 25.88	5 510
	3-XOR / 256	20.73 ± 0.87	19.01 – 24.65	5 309
CvW_{12}	INT / 256	12.12 ± 2.33	4.81 – 17.61	3 103
	INT / 256	11.46 ± 2.62	3.13 – 16.07	2 934
	INT / 256	12.02 ± 2.49	3.95 – 15.75	3 078
	INT / 256	11.93 ± 2.33	2.73 – 17.39	3 054
	INT / 256	11.73 ± 2.78	3.58 – 17.22	3 004
	3-XOR / 256	16.73 ± 0.91	14.95 – 20.05	4 283
	3-XOR / 256	15.77 ± 1.2	13.31 – 20.61	4 037
	3-XOR / 256	16.16 ± 1.19	12.88 – 19.84	4 138
	3-XOR / 256	17.11 ± 0.88	15.13 – 19.77	4 380
	3-XOR / 256	15.28 ± 1.13	13.39 – 20.09	3 912
DvC_{12}	INT / 256	9.74 ± 1.08	5.43 – 12.96	2 494
	INT / 256	8.98 ± 1.38	4.05 – 13.03	2 298
	INT / 256	9.69 ± 1.16	5.7 – 11.99	2 481
	INT / 256	9.68 ± 0.98	4.91 – 11.86	2 479
	INT / 256	9.95 ± 0.99	6.39 – 13.15	2 548
	3-XOR / 256	13.42 ± 0.91	11.73 – 17.27	3 436
	3-XOR / 256	12.91 ± 0.84	11.48 – 17.03	3 305
	3-XOR / 256	12.97 ± 0.71	11.64 – 16.11	3 321
	3-XOR / 256	12.94 ± 0.76	11.37 – 15.86	3 312
	3-XOR / 256	12.68 ± 0.72	11.51 – 16.91	3 246
DvK_{12}	INT / 256	18.12 ± 1.07	15.44 – 21.9	4 640
	INT / 256	18.97 ± 0.95	16.16 – 21.87	4 858
	INT / 256	18.43 ± 0.86	15.85 – 21.08	4 719
	INT / 256	17.86 ± 0.91	14.45 – 21.1	4 572
	INT / 256	18.17 ± 1.04	15.66 – 21.56	4 653
	3-XOR / 256	24.91 ± 1.02	22.68 – 28.38	6 379
	3-XOR / 256	23.86 ± 1.07	21.77 – 27.87	6 109
	3-XOR / 256	23.59 ± 1.05	21.09 – 27.62	6 038
	3-XOR / 256	23.89 ± 1.11	21.57 – 28.5	6 117
	3-XOR / 256	24.69 ± 1.1	22.33 – 28.55	6 320
DvW_{12}	INT / 256	13.55 ± 1.87	6.41 – 18.4	3 469
	INT / 256	13.33 ± 1.74	6.74 – 17.11	3 414
	INT / 256	12.82 ± 2.39	4.25 – 16.74	3 283
	INT / 256	13.36 ± 2.36	4.76 – 18.16	3 420
	INT / 256	13.61 ± 2.23	6.03 – 18.35	3 485
	3-XOR / 256	18.59 ± 0.99	16.2 – 22.34	4 760
	3-XOR / 256	18.32 ± 0.87	15.96 – 21.37	4 690
	3-XOR / 256	18.98 ± 0.92	16.97 – 21.7	4 861
	3-XOR / 256	18.35 ± 0.9	16.02 – 21.36	4 698
	3-XOR / 256	19.17 ± 0.99	17.09 – 23.29	4 909
KvW_{12}	INT / 256	20.52 ± 1.41	15.83 – 26.37	5 253
	INT / 256	19.79 ± 1.19	16.07 – 23.83	5 067
	INT / 256	20.0 ± 1.21	15.39 – 23.08	5 120
	INT / 256	19.84 ± 1.09	16.76 – 22.2	5 081
	INT / 256	20.12 ± 1.77	13.23 – 25.41	5 151
	3-XOR / 256	25.69 ± 1.13	23.27 – 30.11	6 578
	3-XOR / 256	26.22 ± 1.04	23.74 – 29.65	6 713
	3-XOR / 256	25.33 ± 1.11	22.91 – 29.2	6 484
	3-XOR / 256	25.89 ± 1.17	23.07 – 31.05	6 629
	3-XOR / 256	25.62 ± 0.84	23.88 – 28.05	6 559

TABLE IX

EXPERIMENTAL RESULTS FOR PARTITIONINGS. MD4. SAMPLE SIZE FOR ESTIMATES IS 1000 SUBTASKS.

Inst.	Partitioning (type / size)	Avg ± sd time, s	Min – max time, s	Time, s
$MD4_{40}$	CnC / 400 509	26 ± 274	0.01 – 39 087	10 550 880
(est.)	INT / 10k	1 721 ± 2 156	8.46 – 26 114	17 206 801
(est.)	INT / 20k	711 ± 801	0.07 – 6 750	14 213 201
(est.)	INT / 50k	252 ± 315	0.1 – 3 915	12 590 001
(est.)	INT / 60k	222 ± 253	0.09 – 3 074	13 306 201
(est.)	INT / 70k	183 ± 210	0.08 – 1 928	12 747 001
(est.)	INT / 80k	153 ± 163	0.07 – 1 458	12 205 601
(est.)	INT / 90k	140 ± 149	0.09 – 1 292	12 550 500
(est.)	INT / 100k	119 ± 141	0.09 – 1 002	11 898 001
(est.)	INT / 110k	105 ± 114	0.08 – 1 382	11 511 501
(est.)	INT / 120k	100 ± 107	0.1 – 882	11 888 401
(est.)	INT / 130k	95 ± 104	0.09 – 931	12 288 901
(est.)	INT / 140k	92 ± 90	0.09 – 690	12 794 601
(est.)	INT / 150k	84 ± 86	0.09 – 659	12 480 001
(full)	INT / 90k	137 ± 156	0.07 – 2 595	12 301 214
(full)	INT / 110	112 ± 124	0.06 – 2 210	12 250 123
$MD4_{43}$	CnC / 54 611	31 ± 52	0.01 – 2 236	1 686 960
(est.)	INT / 10k	357 ± 380	7.26 – 5 110	3 561 401
(est.)	INT / 20k	170 ± 162	0.1 – 1 453	3 399 401
(est.)	INT / 30k	107 ± 90	0.1 – 842	3 205 801
(est.)	INT / 40k	90 ± 81	0.09 – 957	3 594 001
(est.)	INT / 50k	65 ± 53	0.08 – 371	3 241 000
(est.)	INT / 60k	65 ± 59	0.1 – 628	3 877 201
(est.)	INT / 70k	53 ± 38	0.08 – 341	3 696 701
(est.)	INT / 80k	46 ± 34	0.08 – 251	3 666 401
(est.)	INT / 90k	82 ± 65	0.15 – 744	7 379 101
(est.)	INT / 100k	76 ± 66	0.15 – 1 087	7 581 001
(est.)	INT / 110k	41 ± 32	0.1 – 310	4 507 801
(est.)	INT / 120k	36 ± 28	0.08 – 207	4 280 401
(est.)	INT / 130k	33 ± 22	0.08 – 164	4 213 301
(est.)	INT / 140k	32 ± 23	0.08 – 157	4 461 801
(est.)	INT / 150k	31 ± 20	0.08 – 126	4 630 501
(est.)	INT / 200k	26 ± 17.2	0.08 – 115	5 016 001
(est.)	INT / 300k	20 ± 12.8	0.09 – 80	5 931 001
(est.)	INT / 400k	16.5 ± 11	0.09 – 80	6 592 001
(est.)	INT / 500k	14.3 ± 9.3	0.08 – 73.9	7 125 001
(est.)	INT / 1kk	9.5 ± 6.2	0.1 – 44.3	9 490 001
(full)	INT / 20k	166 ± 163	0.08 – 3 134	3 313 451
(full)	INT / 30k	112 ± 104	0.07 – 1 910	3 349 802
(full)	INT / 50k	71 ± 60	0.07 – 1 002	3 526 129
(full)	INT / 60k	61 ± 48.8	0.07 – 988	3 627 241
(full)	INT / 90k	43.9 ± 33.2	0.07 – 699	3 956 652

TABLE X
EXPERIMENTAL RESULTS FOR PARTITIONINGS. SORTING ALGORITHMS.

Inst.	Partitioning (type / size)	Avg ± sd time, s	Min – max time, s	Total time, s
$\mathtt{BvP}_{9,4}$	Sequential	—	—	7 960
	2-XOR / 262 144	19.4 ± 4.88	5.01 – 67.4	5 098 809
	3-MAJ / 4 096	249 ± 64.7	86.5 – 773	1 016 054
	3-XOR / 4 096	1 642 ± 141	1 224 – 2 169	6 722 151
	4-BENT / 512	998 ± 389	180 – 2 509	510 585
	4-XOR / 512	2 790 ± 544	880 – 4 017	1 428 411
	5-XOR / 256	6 570 ± 449	5 276 – 7 945	1 681 715
	6-XOR / 64	9 283 ± 742	7 860 – 11 106	594 053
	INT / 2	6 781 ± 256	6 601 – 6 961	13 561
	INT / 4	5 959 ± 884	4 775 – 6 894	23 835
	INT / 8	4 537 ± 495	3 623 – 5 097	36 292
	INT / 16	2 166 ± 755	883 – 3 455	34 646
	INT / 32	1 942 ± 675	695 – 3 550	62 113
	INT / 64	1 571 ± 508	623 – 2 746	100 482
	INT / 128	1 051 ± 354	348 – 2 056	134 461
	INT / 256	517 ± 211	137 – 1 057	132 261
	INT / 512	443 ± 175	118 – 972	226 324
	INT / 1 024	347 ± 129	94.9 – 771	354 567
	INT / 4 096	108 ± 46.6	17.2 – 247	441 666
	CnC-d12 / 3 799	2.66 ± 6.79	0.01 – 143	10 091
	CnC-def. / 2 013	4.52 ± 8.75	0.01 – 166	9 108
	CnC-n7250 / 4 064	2.83 ± 4.32	0.01 – 128	11 498
$\mathtt{BvS}_{9,4}$	Sequential	—	—	2 472
	3-MAJ / 4 096	99.3 ± 43.2	19.2 – 434	406 853
	3-XOR / 4 096	869 ± 73.3	657 – 1 241	3 557 590
	4-BENT / 512	342 ± 109	140 – 932	174 657
	4-XOR / 512	899 ± 248	310 – 1 390	459 943
	INT / 16	650 ± 102	435 – 828	10 385
	INT / 32	542 ± 86.7	388 – 727	17 339
	INT / 64	434 ± 64.9	271 – 601	27 715
	INT / 128	310 ± 55.2	152 – 455	39 639
	INT / 256	164 ± 32.3	85.0 – 253	41 909
	INT / 512	140 ± 28.9	52.2 – 237	71 248
	INT / 1 024	110 ± 24.0	48.9 – 175	112 290
	INT / 4 096	36.4 ± 10.2	10.1 – 68.8	148 922
	CnC-d12 / 3 041	2.71 ± 7.66	0.01 – 141	8 234
	CnC-def. / 16 227	0.62 ± 3.54	0.01 – 259	10 115
	CnC-n6500 / 4 043	2.78 ± 4.37	0.01 – 69	11 229
$\mathtt{PvS}_{9,4}$	Sequential	—	—	41 901
	3-MAJ / 4 096	690 ± 200	236 – 2 163	2 822 841
	3-XOR / 4 096	6 096 ± 486	4 727 – 8 246	24 967 143
	4-BENT / 512	3 228 ± 1 353	866 – 8 103	1 652 400
	4-XOR / 512	11 000 ± 2 432	3 712 – 17 003	5 631 961
	INT / 16	10 338 ± 3 042	6 900 – 14 935	165 400
	INT / 32	8 220 ± 2 117	5 409 – 13 782	263 026
	INT / 64	6 044 ± 1 663	3 337 – 9 575	386 799
	INT / 128	4 074 ± 1 212	1 839 – 7 196	521 411
	INT / 256	1 983 ± 772	575 – 3 937	507 463
	INT / 512	1 559 ± 587	492 – 3 124	797 966
	INT / 1 024	1 104 ± 407	317 – 2 528	1 130 096
	INT / 4 096	299 ± 122	45.0 – 738	1 223 049
	CnC-d12 / 3 044	22.32 ± 92.85	0.02 – 1 643	67 933
	CnC-def. / 3 156	21.65 ± 61.29	0.02 – 1 854	68 315
	CnC-n11750 / 4 037	16.7 ± 38.36	0.02 – 865	67 418