Tabelle 4 zum Artikel
Zeit-Experimente zur Faktorisierung,
ein Beitrag zur Didaktik der Kryptologie

von Ralph-Hardo Schulz und Helmut Witten

erschienen in LogIn-Heft XXX

Tabelle 4: Ausführlichere Aufstellung der behandelten Zerlegungen von Semiprimzahlen, d.h. Zahlen der Form $n = p * q$ mit p, q prim.

Legende:
S: Rechnung mit Sage (Web-Interface);
CT1a: Rechnung mit CrypTool 1 auf eigenem PC
(2 GByte Hauptspeicher, einer Intel Core 2 CPU und 2,4 GHertz Taktfrequenz);
CT1b: Rechnung mit CrypTool 1 auf eigenem PC bei Wahl des (günstigeren) Algorithmus;
CT2: Rechnung mit CrypTool 2 auf eigenem PC.
P: Pollards (p-1)-Verfahren; **QS**: Quadratisches Sieb; **W**: Williams (p+1)-Verfahren;
$M_p := 2^p - 1$ mit p prim (Mersenne-Zahl)

$l(n)$	t(n) [sec]	$n = p * q$
10	0,00 S 0,047 CT1a (P) 0,016 CT1b 0 CT2	8616460799 (Jevons-Zahl) =89681 * 96079
25	0,01 S; 0,02 S 0,250 CT1a (P) 0,016 CT1b 0 CT2	5018557517866741394046901 =1481124532001 * 3388342714901 (Faktor von $2^{500}+1$ bzw. von $10^{40}+13$)
34	0,03 S 0,187 CT1a (P) 0,016 CT1b 0 CT2	1240819002867598361280210027487189 =538119463428139 * 2305843009213693951
39	0,16 S 4,141 CT1a (QS) 0,859 CT1b 0 CT2	87429758973907681855541983050986592355 1 = 21213434569876541053 * 41214334569876541067
40	0,14 S 3,686 CT1a (QS) 0,766 CT1b 0 CT2	21720290762118698701730547377528215514 83 = 46600033003000345873 * 46610033003024346571

46	0,56 S 0,047 CT1a (W) 0,031 CT1b 0 CT2	142724769270595988043931594750096198971949056 1 = 2305843009213693951 * 6189700196426901374495621 11 = $(2^{61}-1)*(2^{89}-1) = M_{61} * M_{89}$
52	3,00 S 52,921 CT1a (QS) 11,702 CT1b 1 CT2	160002664011088900002765815025218400000011952508308 7 =400003330000000000000345691 * 400003330000000000000345757
52	3,91 S 39,984 CT1a (QS) 10,563 CT1b 1 CT2	435604395611088900004563500624818800000011952093529 9 =660003330000000000000345703 *660003330000000000000345733
55	6,59 S 107 CT1a (QS) 23,734 CT1b 1 CT2	901474623537489407738470176874556221399300013185104851 3 =300245670000000012345612111 1 * 300245670000000123456003338 3
56	5,88 S 78 CT1a (QS) 20,155 CT1b 1 CT2	160002664011088900000027653430212890000000000119484292209 =400003330000000000000345661 * 400003330000000000000345669
56	8,24 S 129 CT1a (QS) 31,312 CT1b 2 CT2	901474623537489074134295234483660265139888804010895744 43= 300245670000000012345612111 1*300245670000000012345600000 13
58	6,64 S; 6,63 S 76 CT1a (QS) 28,094 CT1b 2 CT2	135627354233541693362006500711567604569222738541000763975 1= 257878038725783152726710839*525936039003934785796425018980 9
60	13,24 S 13,21 S; 13,42 S 261 CT1a (QS) 61 CT1b 4 CT2	100433627766186892221372630609062766858404681029709092356097 =6189700196426901374495621 11 * 162259276829213363391578010288127 $= (2^{89}-1)*(2^{107}-1) = M_{89} * M_{107}$
60	16,33 S 16,38 S; 16,28 S 315 CT1a (QS) 303; 309 CT1a (QS) 76 CT1b 4 CT2	267619860332297401900866279382024711037566640405902751004511 =6189700196426901374495621 11 * 432363203127002885506543172618401
61	26,56 S; 35,91 S 426 CT1a (QS) 95 CT1b 5 CT2	262597352418731258300395219707057257009060909209923704725501 7 =197210611666467174983596 81* 133155792276964047936085219707057257 (Faktor von $10^{38}+7$)

62	52,09 S 475 CT1a (QS) 119 CT1b 6 CT2	267426488949013093414928041917346305986801160286423952752520 69 =369646296854333406037717721877 7* 723465894896812414632199608919 7
63	37.42 S; 37,37 S 0,250 CT1a (P) 0,031 CT1b 8 CT2	853380013471994113258399286230448538969180138406196014529097743 =525936039003934785796425018980 9 * 162259276829213363391578010288127 (d.h. $2^{107}-1$, also M_{107})
65	58,39 S 807 CT1a (QS) 206 CT1b 10 CT2	573858262806101867788776494659612345896855544908276527496334225 27 =197210611666467174983596 81 (Faktor von $10^{40}+1$) *290987517333317111147996922713460953196 7
66	77,63 S 1673 CT1a (QS) 473 CT1b 17 CT2	788322734263222118228263763686486830345832185555140314438509745937 =310063097840410523541540703533169 * 254245906640903081460388487745347 3 (Faktoren von $10^{38}+35$ bzw. $10^{38}+40$)
68	81.48 S 1766 CT1a (QS) 496 CT1b 23 CT2	193195977690655836975979094031418921049922767975958383422610482597 37 =254245906640903081460388487745347 3 * 759878419452887537993920972644376 9 (Faktor von $10^{38}+40$)
69	172,6 S 171,68; 173,63 S 0,156 CT1a (P) 0,032 CT1b 27 CT2	894833801006409699304039289958384322031968018318595556994505973936143 =525936039003934785796425018980 9 * 170141183460469231731687303715884105727 (d.h. $2^{127}-1$, also M_{127})
70	189,63 S 3498 CT1a (QS) 1045 CT1b 40 CT2	869565217391304347826086956521739193043478260869565217391304347826 0877 =434782608695652173913043478260869 59 * 200000000000000000000000000000003
71	184,55 S 3455 CT1a (QS) 801 CT1b 32 CT2	111111111111111111111111111111111111111111111111111111111111111111111111111111 = 241573142393627673576957439049 * 459948113478868463102217288952230343018 39
71	188,63 S 1439 CT1b 36 CT2	153040822265873617718240359500687304774978075489107007191112804031243 03 = 525936039003934785796425018980 9 * 290987517333317111147996922713460953196 7 (Faktor von $10^{70}+5$)
71	175,18 S 1235 CT1b 34 CT2	228790021094439944907362920458861266327599855404706668313954818546634 27 = 133155792276964047936085219707057257 * 171821305841924398625429553264604811 (Faktor von $10^{38}+2$)
71	143,66 S 145,31 S 3455 CT1a (QS) 1020 CT1b 37 CT 2	276069853871622551497390234491079316684587161426206011699548030008033 29 =162259276829213363391578010288127 * 170141183460469231731687303715884105727 $=(2^{107}-1)*(2^{127}-1)=M_{107}*M_{127}$

72	263,93 S 39 CT2	10000000000000000000000000000000037000000000000000000000000000000/ 00033 =2000000000000000000000000000000003 * 5000000000000000000000000000000011
72	202,29 S 55 CT2	18240519489995075059737701329733870826842748481476752457910001276836/ 3643 =133155792276964047936085219707057257 * 136986301369863013698630136986301369863013699 (Faktor von $10^{38}+27$)
72	143,42 S 34 CT2	20000000000000000000000000000000016400000000000000000000000000000000/ 0201 =2000000000000000000000000000000003 * 1000000000000000000000000000000067
72	171,47 S 181,05 S 171,91 S 173,73 S 42 CT2	472154241288322308621049626625163020582457972462095711822828862 8/ 7055809 =162259276829213363391578010288127 (d.h. $2^{107}-1$, also M_{107}) * 290987517333317111147996922713460953 1967
73	327,01 S 48 CT2	13698630136986301369863013698630137907808219178082191780821917808 21/ 917833 =1000000000000000000000000000000067 * 136986301369863013698630136986301369 9
73	339,89 S 340,75 S 339,75 S 55 CT2	7463084827204216028562220613553566489786789143432464634026782164675/ 965553 =162259276829213363391578010288127 (d.h. $2^{107}-1$, also M_{107}) * 459948113478868463102217288952230343018 39
74	313,40 S 70 CT2	4987358169131969861275321306209230112106771529895163323045597391567 8/ 019001 =133155792276964047936085219707057257 * 3745505985018109365817766300963131813 93 (Faktoren von $10^{38}+7$ bzw. $M_{257}=2^{257}-1$ (vgl. Ribenboim, P.: The New book of prime numbers. Springer V. [3]1996 p. 168)
75	440,86 S 92 CT2	2330701143294099064817634297477864462642987938826393048870624274017 6/ 5354173 =136986301369863013698630136986301369863013699 (Faktor von $10^{38}+27$) * 17014118346046923173168730371588410572 7 (d.h. $2^{127}-1$, also M_{127})
75	609,14 S 104 CT2	3874667341322464862157082859034100575460307938925861488420236812116 4/ 0834519 =133155792276964047936085219707057257 * 290987517333317111147996922713460953 1967 (Faktor von $10^{70}+5$)
75	518,56 S 114 CT2	5130830116463163514818857946524838102659296734184780176398351919534 3/ 0902707 =136986301369863013698630136986301369863013699 * 3745505985018109365817766300963131813 93 (Faktoren von $10^{38}+2$ bzw. M_{257})

76	905,30 S 912,72 S 116 CT2	39861303744290015225753003111433007297981730093150084932871119059264 9/ 9415933 =13698630136986301369863013698630136 99 * 290987517333317111147996922713460953196 7 (Faktoren von $10^{38}+27$ bzw. $10^{70}+5$)
77	1285,47 S 168 CT2	87559823127501982332389150045831680611025608888715792754305609791/ 773510137213 = 21234567890000012345678900001234567911 9 * 412345678900000123456789000012345679027
78	838.49 S 193 CT2	49508960571314377154846257332881374516938702292313966742076580244/ 4525814275009 =17014118346046923173168730371588410572 7 * 290987517333317111147996922713460953196 7 (d.h. $2^{127}-1$, also M_{127}.)
79	>1800 S Abbruch 223 CT2	58478832962358394007023133319194805678476345264232522756540492000/ 00243098047477 43456780123000000001234000000012340002 41* 134567800000000000012340000000000000197
80	286 CT2	54397374283007096598162903250247112369687146575563003827218692466/ 797770535826811 =57172041969847948494882852983926198671 01* 95146810239340081340814798948974525187 11
81	294 CT2	44051380726241477584622576267609317576149232856019890285449004710/ 7277398468733833 =57172041969847948494882852983926198671 01 * 770505638918298620403838491433690896695 33
81	315 CT2	85808013231160055711124404895753526713291492377512738214227408207/ 7493303918481489 =90184855399052842067889744119596649878199 * 95146810239340081340814798948974525187 11
82	329 CT2	69487939630001582967502516739066716730554875277623530323515959 8/ 066255373611211067 = 90184855399052842067889744119596649878199 * 770505638918298620403838491433690896695 33
83	485 CT2	31002438893320937478780494821167032651007272832579576517541603 55/ 8569409309564222957 = 90184855399052842067889744119596649878199 * 343765466564650473090660258149404961259643
83	568 CT2	70993632717175769303611888257858392829948001145930586761400628 84/ 9295821871112154981 = 92139017719380577000450028148352920574525 7 * 770505638918298620403838491433690896695 33
84	724 CT2	31674212415111461229265557338520329564508886459473370902077525160/ 8265071587292763251 = 92139017719380577000450028148352920574525 7 * 343765466564650473090660258149404961259643

100	30405 CT2	152260502792253336053561837813263742971806811496138068865790849/ 458012296325895289765400035069200613 **RSA-100** =379752279369436739228088727554456278545655365381 99 * 400946909509208810306837352927614683892148997240 61

Adresse der Autoren:

Prof. Dr. Ralph-Hardo Schulz
c/o Inst. f. Mathematik der FU Berlin
Arnimallee 3
14195 Berlin
E-Mail: rhschulz@zedat.fu-berlin.de

StudDir a.D. Helmut Witten
Brandenburgische Straße 23
10707 Berlin

E-Mail: helmut@witten-berlin.de

Berlin, den 29. November 2010