GNFS Factoring Statistics of RSA-100, 110, ..., 150[1]

Kazumaro Aoki*,[2] Yuji Kida† Takeshi Shimoyama‡ Hiroki Ueda*

*NTT Labs †Rikkyo Univ. ‡Fujitsu Labs

April 16, 2004

1 Introduction

GNFS (general number field sieve) algorithm is currently the fastest known algorithm for factoring large integers. Up to the present, several running time estimates for GNFS are announced (ex. [LV00]). These estimates are usually based on the previous factoring results. However, since the previous factoring results were done by various programs and/or computers, it is difficult to compare those running time.

We implemented GNFS and factored 100- to 150-digits number on the same environment. This manuscript describes the statistics of these factorings. We only used lattice sieve[3], and did not use line sieve, because of the use for the interpolation of the results.

We hope that these results will help running time estimation of factoring a large integer.

2 The Numbers to Be Factored

We choose 100- to 150-digit numbers from old RSA Factoring Challenge:

```
RSA-100 =
  1522605027922533360535618378132637429718068114961\
  3
  8068865790849458012296325895289765400035069200613\
  9
= 4009469095092088103068373529276146838921489972406\
  1
* 3797522793694367392280887275544562785456553663819\
  9

RSA-110 =
  3579423417972586877499180783256845540300377802422\
  8
  2261935329081904846702523646774115135161112045040\
  6
  0317568667
= 6122421090493547576937037317561418841225758554253106999
* 5846418214406154678836553182979162384198610505601062333

RSA-120 =
  2270104812954373633342599609474936688958753364608\
```

[1]This work partly supported by the CRYPTREC project which is promoted by Telecommunications Advancement Organization of Japan and other organizations.

[2]Email: maro@isl.ntt.co.jp

[3]Two large primes are used for both algebraic and rational sides.

```
  4780038173258247009162675779735389791151574049166 7\
  47880487470296548479
= 32741455569349801575114630374914148806364240324017146340688 3
* 69334266711083018119732540189970064136196586312733668067301 3

RSA-130 =
  18070820886874048059516561644059055662781025167694\
  01349170127021450056662540244048387341127590812303\
  37178188796656318201321488055 7
= 39685999459597454290161126162883786067576449112810064832555157243
* 45534498646735972188403686897274408864356301263205069600999044599

RSA-140 =
  21290246318258757547497882016271517497806703963277\
  21627823338321538194998405649591136657385302191831\
  67831073879953172308895692308734419364 71
= 33987174230284385545301236276138758356339864959695974234909293027714 79
* 62642001874012850961516549482644422193020371786235090191116606539460 49

RSA-150 =
  15508981247834844050960675437001186177065454583099\
  54306554669457743126327034634659543633350275777290\
  25391453996787414027003501631772186840890795964683
= 34800986710228369548397045104759342483101281735038545688955963754827841 0717
* 44564774490364074153324112578708617600544253629776615349341972453246029 6199
```

3 Notations

N: composite number to be factored (ex. `RSA-120`)

$f(x)$: definition polynomial

M: $f(M) \equiv 0 \pmod{N}$

`rp`: factor base bound for rational side

`rlp`: large prime bound for rational side

`ap`: factor base bound for algebraic side

`alp`: large prime bound for algebraic side

s: skewness

n_q: number of special-q

`qs`: smallest special-q ($\pi(\texttt{ap}) \approx \pi(\texttt{qs}) + n_q$)

4 PCs Used

Pentium 4 (Northwood), 2.53GHz, FSB 533MHz, Intel Desktop Boards D850EMV2, i850e chip set, 1024MB RDRAM, PC800, FreeBSD 4.7-RELEASE-p13

5 Polynomials Used

We generated the definition polynomials except for RSA-140 which is already generated by [CDL+99].

5.1 RSA-100

$$\begin{aligned}\texttt{rsa100} = & \\ & 476148960\ x^5 \\ & +33466236556\ x^4 \\ & -95242541476020\ x^3 \\ & +24540020572973215\ x^2 \\ & -3475579183967599680\ x \\ & -2599927782355220688836 \\ & M = 1261737131078349405\end{aligned}$$

$$\begin{aligned}\texttt{rsa100d4} = & \\ & 11280637368000\ x^4 \\ & +1297331842676166\ x^3 \\ & -6398231616999999973\ x^2 \\ & -3867985592992020706164\ x \\ & -5029809154814976597919529 \\ & M = 3408500839386006478662\end{aligned}$$

$$\begin{aligned}\texttt{rsa100d6} = & \\ & 54885600\ x^6 \\ & -6171978062\ x^5 \\ & -279021830192\ x^4 \\ & +7107344769942\ x^3 \\ & +230170783897105\ x^2 \\ & +12995121899819102\ x \\ & -1211347205408698220 \\ & M = 1739888725534017\end{aligned}$$

5.2 RSA-110

$$\begin{aligned}\texttt{rsa110} = & \\ & 2186636760\ x^5 \\ & +7090231275050\ x^4 \\ & -7779420006796361\ x^3 \\ & -7338302252559380692\ x^2 \\ & +2945060505193947891936\ x \\ & +528370695182871756215992 \\ & M = 110358880444076439675\end{aligned}$$

$$\texttt{rsa110d4} = \begin{aligned} &63063320720400 && x^4 \\ &- 108858128876245362 && x^3 \\ &- 333714480816166136741 && x^2 \\ &+ 2151401060734002095936690 && x \\ &- 18550211618518883623239525160 \\ &M = 86797868410535792048781 3 \end{aligned}$$

$$\texttt{rsa110d6} = \begin{aligned} &3356406900 && x^6 \\ &- 129410945870 && x^5 \\ &+ 8416221526418 && x^4 \\ &+ 87105425158528 && x^3 \\ &- 5730778027746978 && x^2 \\ &+ 19623529153740031 && x \\ &+ 1160691112322070568 \\ &M = 46916226934871871 \end{aligned}$$

5.3 RSA-120

$$\texttt{rsa120} = \begin{aligned} &1554355923120 && x^5 \\ &+ 279300728665360 && x^4 \\ &+ 235068853764040024 && x^3 \\ &- 366715788836593094 && x^2 \\ &- 19671660878164914170531 && x \\ &- 694220976163253450117 2599 \\ &M = 2709561965307563001574 \end{aligned}$$

$$\texttt{rsa120d4} = \begin{aligned} &895498088284800 && x^4 \\ &+ 3413868460618755900 && x^3 \\ &- 24034697186813319912433 && x^2 \\ &- 28465301846766247738030 6552 && x \\ &- 37422215960189606744506 7401260 \\ &M = 12618139126842547030090 9327 \end{aligned}$$

$$\texttt{rsa120d6} = \begin{aligned} &6201111840 && x^6 \\ &+ 65538566248 && x^5 \\ &+ 69773963135376 && x^4 \\ &- 578627837775246 && x^3 \\ &- 345217686788156398 && x^2 \\ &+ 1982291106588495261 && x \\ &- 730068578237501089 20 \\ &M = 1822200063999191027 \end{aligned}$$

5.4 RSA-130

$$\texttt{rsa130} = \begin{aligned} &147039132240 && x^5 \\ &+ 871623037904469 && x^4 \\ &+ 3086117472198489675 && x^3 \\ &- 7719799519497061434782 && x^2 \\ &- 9743342795049257456352467 && x \\ &+ 1153631581220084102198819 4190 \\ &M = 4148670947469419004577 67 \end{aligned}$$

5.5 RSA-140

$$\begin{aligned}\texttt{rsa140} = \\ 439682082840\ x^5 \\ +\ 390315678538960\ x^4 \\ -\ 7387325293892994572\ x^3 \\ -\ 19027153243742988714824\ x^2 \\ -\ 63441025694464617913930613\ x \\ +\ 31855391707147435039222350749 4 \\ M = 34435657809242536951779007\end{aligned}$$

5.6 RSA-150

$$\begin{aligned}\texttt{rsa150} = \\ 39579179880240\ x^5 \\ +\ 118091572936301268\ x^4 \\ +\ 9988203749276316477 0\ x^3 \\ -\ 56447112339915941335654 51\ x^2 \\ -\ 17749003945730989474189029270\ x \\ +\ 14495606942348552079748145328451 \\ M = 13140845099321381544918138 36\end{aligned}$$

6 Parameters and Statistics

We show the parameters for sieving in Table 1, and their statistics are as follows.

Table 1: Parameters for Sieving

	rp	rlp	ap	alp	s	qs
rsa100	300e3	18e6	1981711	40e6	369	424247
rsa100d4	1200e3	18e6	12474757	40e6	1200	282797
rsa100d6	300e3	12e6	4992019	160e6	53	1422221
rsa110	800e3	40e6	3995743	80e6	848	1069603
rsa110d4	2400e3	40e6	3773773	80e6	2812	589759
rsa110d6	600e3	20e6	8072513	320e6	23	1496549
rsa120	1600e3	92e6	12474757	184e6	321	2264707
rsa120d4	4800e3	100e6	10322033	140e6	5886	1363513
rsa120d6	1200e3	48e6	13379207	640e6	58	2060059
rsa130	3e6	215e6	20319361	430e6	1882	4107643
rsa140	6e6	500e6	19153333	1e9	3992	4505773
rsa150	12e6	2e9	52864993	2e9	4049	14830997

	hc	hd	q_end	#rel
rsa100	2 048	2 048	112 000	3 053 728
rsa100d4	2 048	2 048	95 000	2 736 929
rsa100d6	2 048	2 048	240 000	5 329 204
rsa110	2 048	2 048	200 000	6 752 059
rsa110d4	4 096	2 048	220 000	6 185 022
rsa110d6	4 096	2 048	430 000	10 228 570
rsa120	4 096	2 048	650 000	14 225 875
rsa120d4	4 096	4 096	580 000	13 145 521
rsa120d6	4 096	4 096	720 000	19 304 631
rsa130	4 096	4 096	1 000 000	26 975 303
rsa140	8 192	8 192	904 000	51 340 137
rsa150	8 192	8 192	2 200 000	124 804 557

	#dup	#uniq	#lost	total time(sec)
rsa100	391 235	2 662 493	0	54 271
rsa100d4	357 714	2 379 215	0	55 155
rsa100d6	584 401	4 744 803	0	145 247
rsa110	948 123	5 803 935	0	193 676
rsa110d4	956 470	5 228 552	0	250 945
rsa110d6	1 273 191	8 955 379	0	461 685
rsa120	2 389 912	11 835 963	0	790 138
rsa120d4	2 088 586	11 056 935	0	1 320 933
rsa120d6	2 370 817	16 933 814	0	1 517 888
rsa130	3 407 897	23 567 406	0	2 315 347
rsa140	4 982 485	46 357 652	0	6 726 258
rsa150	12 666 924	112 137 633	305	20 597 260

	#free rel	presc #rel	presc #FB	#alprime0	#rlprime0
rsa100	5 273	2 667 766	2 664 811	1 713 274	951 535
rsa100d4	24 960	2 404 175	2 557 942	1 580 867	977 074
rsa100d6	954	4 745 757	5 233 152	4 468 920	765 319
rsa110	11 442	5 815 377	5 443 581	3 407 556	2 036 022
rsa110d4	55 263	5 283 815	5 365 601	3 281 038	2 084 611
rsa110d6	1 574	8 956 953	9 784 707	8 534 027	1 251 490
rsa120	24 169	11 860 132	11 738 886	7 463 338	4 275 555
rsa120d4	126 435	11 183 370	10 928 533	6 178 137	4 750 423
rsa120d6	3 524	16 937 338	18 512 122	15 707 493	2 805 427
rsa130	47 433	23 614 839	24 521 904	15 300 885	9 221 041
rsa140	85 613	46 443 265	50 556 075	31 063 425	19 492 644
rsa150	207 286	112 344 614	125 001 514	66 430 003	58 571 503

	after 1-pass		after sc		after sc	
	#rel	#FB	#rel	#FB	total w	ave. w

rsa100	1 850 290	1 704 727	574 926	573 925	10 087 790	17.546
rsa100d4	1 594 376	1 585 057	724 636	723 634	12 848 598	17.731
rsa100d6	2 552 375	2 545 446	1 092 722	1 091 719	18 881 757	17.280
rsa110	4 207 271	3 581 036	891 802	890 801	16 518 559	18.527
rsa110d4	3 688 857	3 481 925	1 271 853	1 270 846	23 381 040	18.383
rsa110d6	4 776 194	4 729 413	1 884 183	1 883 182	34 029 045	18.060
rsa120	8 302 289	7 540 430	2 279 188	2 278 185	43 910 886	19.266
rsa120d4	8 207 377	7 471 071	2 455 106	2 454 102	45 839 280	18.671
rsa120d6	9 089 129	9 053 515	3 530 459	3 529 458	64 431 664	18.250
rsa130	15 596 081	14 838 636	4 563 119	4 562 121	87 722 757	19.224
rsa140	28 512 843	28 193 867	7 789 491	7 788 488	158 573 057	20.357
rsa150	66 795 889	66 782 788	16 361 279	16 360 278	332 343 491	20.312

				after 20-way merge		
	#lprime	#alprime	#rlprime	#rel	#FB	total w
rsa100	5	365 142	208 778	190 616	189 614	16 664 599
rsa100d4	8	403 691	319 937	215 271	214 257	20 079 506
rsa100d6	5	789 496	302 222	336 137	335 114	33 891 248
rsa110	7	565 076	325 720	304 917	303 916	31 889 185
rsa110d4	9	714 237	556 602	384 185	383 169	42 320 324
rsa110d6	7	1 366 085	517 090	528 397	527 389	67 209 440
rsa120	9	1 460 541	817 635	687 247	686 239	101 496 903
rsa120d4	8	1 375 986	1 078 108	741 068	740 055	103 481 516
rsa120d6	6	2 509 741	1 019 711	904 269	903 253	139 815 927
rsa130	8	2 868 381	1 693 732	1 249 886	1 248 880	209 107 002
rsa140	8	4 734 617	3 053 863	1 842 573	1 841 554	348 263 555
rsa150	8	9 898 427	6 461 843	4 061 097	4 060 083	749 694 248

	after 20-way merge	after cut96		after cut96	
	ave. w	#rel	#FB	total w	ave. w
rsa100	87.425	190 616	189 518	13 181 907	69.15
rsa100d4	93.275	215 271	214 161	16 089 914	74.74
rsa100d6	100.826	336 137	335 018	27 513 589	81.85
rsa110	104.583	304 917	303 820	25 682 013	84.23
rsa110d4	110.156	384 185	383 073	34 490 578	89.78
rsa110d6	127.195	528 397	527 293	56 904 354	105.80
rsa120	147.686	687 247	686 143	84 825 348	123.43
rsa120d4	139.638	741 068	739 959	87 282 307	117.78
rsa120d6	154.6168	904 269	903 157	120 238 399	132.97
rsa130	167.301	1 249 886	1 248 784	178 678 686	142.96
rsa140	189.108	1 841 611	1 840 496	302 854 189	164.45
rsa150	184.604	4 061 097	4 059 987	653 770 042	160.98

processing time for block Lanczos with block width 128
(16 PCs are connected thru 100baseT full-duplex)

	hhh:mm:ss
rsa100	00:07:19
rsa110	00:28:49
rsa120	02:24:15
rsa130	08:47:28
rsa140	15:07:39
rsa150	101:31:17

We used the following abbreviation in the table.

`hc` sieving width for lattice sieve

`hd` sieving height for lattice sieve

`q_end` n_q

`#rel` number of output relations by lattice sieve

`#dup` number of discarded relation in the uniqueness confirmation step

`#uniq` number of unique relations

`#lost` number of lost relations which should be zero but exists because of disk full or other reason

`total time(sec)` total sieving time scaled to one PC in seconds

`#free rel` number of free relations

`presc #rel` $\#\texttt{uniq} + \#\texttt{freerel} - \#\texttt{lost}$

`presc #FB` number of factor bases including large primes after uniqueness confirmation

`#alprime0 presc #FB` for algebraic side

`#rlprime0 presc #FB` for rational side

`after 1-pass #rel` number of relations after 1-pass singleton discarding

`after 1-pass #FB` number of factor bases after 1-pass singleton discarding

`after sc #rel` number of survived relations after singleton and clique operations

`after sc #FB` number of survived factor bases after singleton and clique operations

`after sc total w` total weight in the relation $\times$ factor base matrix

`after sc ave. w` average weight in the relation $\times$ factor base matrix

`#lprime` number of factors of the leading coefficient of the definition polynomial, which is included in the factor bases

`#alprime` factor bases for algebraic side after singleton and clique operations

`#rlprime` factor bases for rational side after singleton and clique operations

`after 20-way merge #rel` number of relation-sets after 20-way merge

`after 20-way merge #FB` number of factor bases after 20-way merge

`after 20-way merge total w` total weight in the matrix after 20-way merge

`after 20-way merge ave. w` average weight in the matrix after 20-way merge

`after cut96 #rel` number of relation-sets in the matrix after 20-way merge whose heavy 96 factor bases are removed, and it equals to `after 20-way merge #rel`

`after cut96 #FB` number of factor bases in the matrix after 20-way merge whose heavy 96 factor bases are removed

`after cut96 total w` total weight in the matrix after 20-way merge whose heavy 96 factor bases are removed

`after cut96 ave. w` average weight of the relation-sets in the matrix after 20-way merge whose heavy 96 factor bases are removed

References

[CDL+99] S. Cavallar, B. Dodson, A. K. Lenstra, P. Leyland, W. Lioen, P. L. Montgomery, B. Murphy, H. te Riele, and P. Zimmermann. Factorization of RSA-140 Using the Number Field Sieve. In K. Y. Lam, E. Okamoto, and C. Xing, editors, *Advances in Cryptology — ASIACRYPT'99*, Volume 1716 of *Lecture Notes in Computer Science*, pp. 195–207. Springer-Verlag, Berlin, Heidelberg, New York, 1999.

[LV00] A. K. Lenstra and E. R. Verheul. Selecting Cryptographic Key Sizes. In H. Imai and Y. Zheng, editors, *Public Key Cryptography — Third International Workshop on Practice and Theory in Public Key Cryptosystems, PKC 2000*, Volume 1751 of *Lecture Notes in Computer Science*, pp. 446–465. Springer-Verlag, Berlin, Heidelberg, New York, 2000.