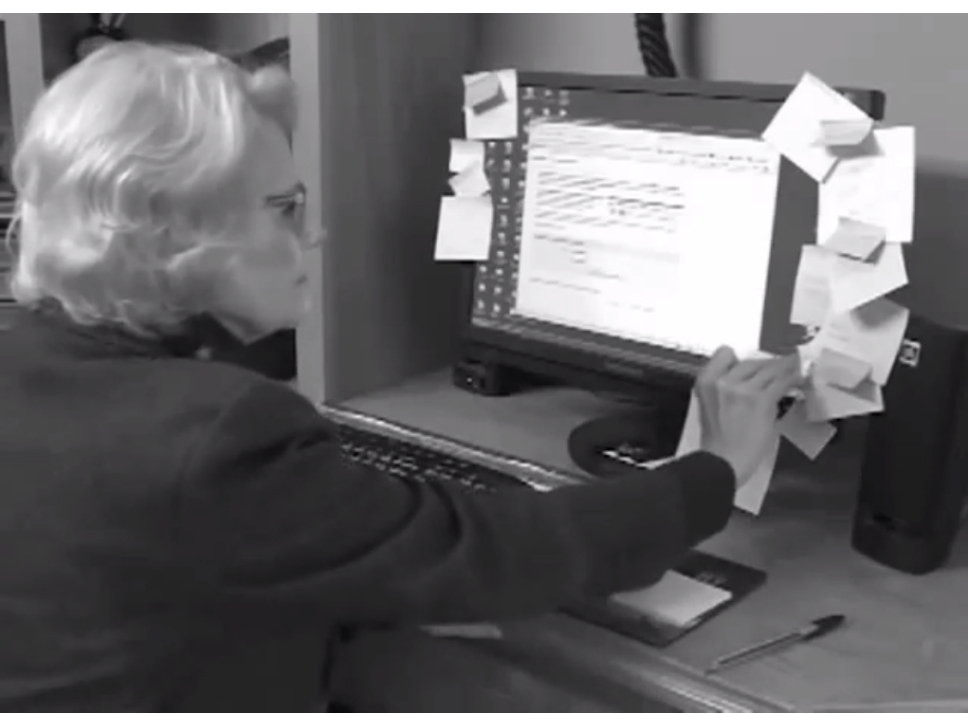


Factoring as a Service

Nadia Heninger



Sign In

What is your e-mail address?

My e-mail address is

Are you having trouble logging in?

☐ No, I am a new customer.

☐ Yes, I have a password:

Private Key Not Found

Sign In Help

Forgot your password? Get a password hint.

Has your e-mail address changed? Update it here.





Factoring in the cloud



Amazon Elastic Compute Cloud

<http://aws.amazon.com/ec2/>



StarCluster

Cluster computing toolkit for ec2

<http://star.mit.edu/cluster/>



CADO-NFS

Crible Algébrique: Distribution, Optimisation - Number Field Sieve

Number field sieve implementation

<http://cado-nfs.gforge.inria.fr/>

The Vision...

```
nadiyah$ ./factor
```

```
StarCluster - (http://star.mit.edu/cluster) (v. 0.94)
```

```
Software Tools for Academics and Researchers (STAR)
```

```
Please submit bug reports to starcluster@mit.edu
```

```
>>> Using default cluster template: highmemcluster
```

```
>>> Validating cluster template settings...
```

```
>>> Cluster template settings are valid
```

```
>>> Starting cluster...
```

```
...
```

```
Info:All done!
```

```
Info:-----
```

```
9738099831990523525967766416518896973138203668314671589842771631
```

```
real 1595m17.334s
```

```
user 0m0.232s
```

```
sys 0m0.032s
```

Info:-----

Info:Duplicate and singleton removal

Info:-----

Info:Removing duplicates...

Error:Command `/home/cado-nfs/build/filter/dup2 -K 59224515 -poly /job/c155.poly -filelist /job/c155.dup2.filelist -renumber /job/c155.renumber.gz -basepath /job/c155.nodup/0 ' terminated unexpectedly with exit status 1.

Error:STDERR Renumbering table: read 92274688 values from file in 12.1s -- 64.5 MB/s

Error:STDERR Renumbering table: read 100663296 values from file in 13.2s -- 64.4 MB/s

Error:STDERR Renumbering table: end of read. Read 108802942 values from file in 14.2s -- 65.1 MB/s

Error:STDERR Renumbering struct: nb_bits=32, sizeof(*table)=4, rat=0 nb_badideals=0 add_full_col=0

Error:STDERR Renumbering struct: nprimes=108802942

Error:STDERR Renumbering struct: first_not_cached=163750

Error:STDERR [checking true duplicates on sample of 592246 cells]

Error:STDERR Allocated hash table of 59224515 entries (225Mb)

Error:STDERR Constructing the two filelists...

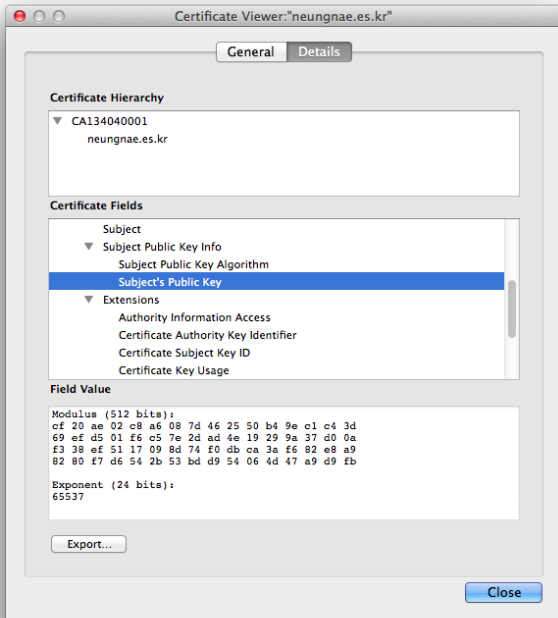
Error:STDERR Error while reading /job/c155.nodup/0/c155.rels.1.0001.gz

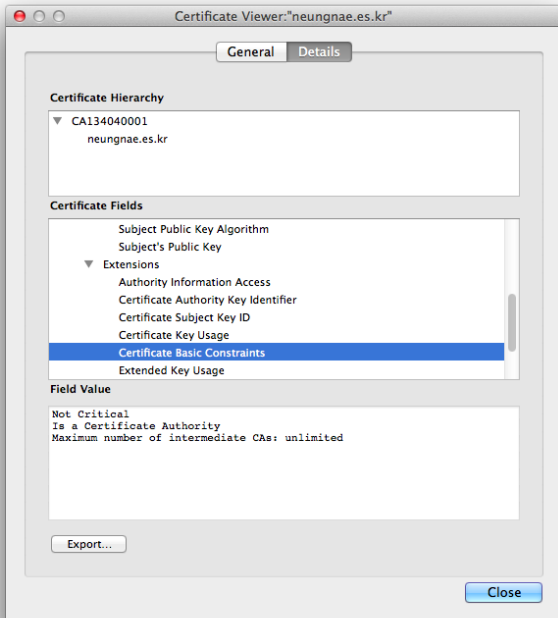

```
top - 18:40:47 up 2 days, 16:13, 1 user, load average: 2.85, 2.10, 1.67
Tasks: 245 total, 1 running, 244 sleeping, 0 stopped, 0 zombie
Cpu(s): 4.0%us, 2.7%sy, 0.0%ni, 93.2%id, 0.0%wa, 0.0%hi, 0.0%si, 0.1%st
Mem: 251649140k total, 73307884k used, 178341256k free, 248164k buffers
Swap: 0k total, 0k used, 0k free, 68952144k cached
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
29174	root	20	0	3577m	267m	3064	S	225	0.1	1086:58	krylov
1	root	20	0	24444	2396	1360	S	0	0.0	0:04.44	init
2	root	20	0	0	0	0	S	0	0.0	0:00.00	kthreadd
3	root	20	0	0	0	0	S	0	0.0	0:00.90	ksoftirqd/0
6	root	RT	0	0	0	0	S	0	0.0	0:00.30	migration/0
7	root	RT	0	0	0	0	S	0	0.0	0:00.99	watchdog/0
8	root	RT	0	0	0	0	S	0	0.0	0:00.32	migration/1
9	root	20	0	0	0	0	S	0	0.0	0:00.00	kworker/1:0
10	root	20	0	0	0	0	S	0	0.0	0:00.44	ksoftirqd/1
11	root	20	0	0	0	0	S	0	0.0	0:03.78	kworker/0:1
12	root	RT	0	0	0	0	S	0	0.0	0:00.81	watchdog/1
13	root	RT	0	0	0	0	S	0	0.0	0:00.32	migration/2

Does anybody still use 512-bit RSA?







Factoring details

44 hours, \$241

- ▶ **Polynomial selection:** 12 minutes (parallel)
- ▶ **Sieving:** 12-14 hours (parallel)
- ▶ **Generating matrix:** 1 hour (single core)
- ▶ **Linear algebra:** 26 hours (partially parallel)
- ▶ **Square root:** 20 minutes (single core)
- ▶ **Recovering from crashes:** 2-3 hours

16 "8x large memory optimized cluster compute spot instances" at
 $\$0.343/\text{hour} = \mathbf{\$5.48/\text{hour}}$

1084815553842551142900520794449806245616824430624988
6906809764553107935080834330292843201597849730250171
094340013101876851402167330796759352537531560876539

=

111399099676390215669316862567320367625
479517670936483804719644527320678472637

x

973809983199052352596776641651889697313
82036683146715898427716312842129869847

현재 페이지는 팝업창을 포함하고 있습니다. 팝업창을 보시겠습니까?

보기 취소

인천능내초등학교
Incheon Neungnae Elementary School

학교안내 알림마당 선생님마당 어린이마당 학부모마당 특색마당 소풍의마당

참고사항: 능내초등학교에서 여가지를 우리 학교로 활용하고 있다. (학생들)은 능내초등학교로 우리들 세상

바른행동, 굳센체력, 알찬학력
오고싶고 머물고 싶은 행복한 학교

학교행사

S	M	T	W	T	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

일정없음

LOGIN

ID

PW

GO

최면가입 비밀번호찾기

Quick menu

인천광역시
교육청
인천광역시
서부교육지원청

매뉴아이

국민권익
위원회

물리산교센터

UCC영상모음

학교환경학생
정화구역도

인천e스쿨

연구학교

업무모텔

공지사항

가정통신문

대회안내

행사안내

+ MORE

- 인천능내초등학교 2013년 9월 ~ 2014년 2월 (08-16)
- 인천능내초등학교 2013년 9월 ~ 2014년 2월 (08-16)
- 능내초등학교 2013학년도 2학기 5.6학년 수 (08-16)

명품 능내 교육활동

사진자료

동영상자료

+ MORE



여름 영어 캠프



꿈과 미래를 향



7.26일 여름방

우리반하기



1학년 홈페이지



2학년 홈페이지



3학년 홈페이지



4학년 홈페이지



5학년 홈페이지



6학년 홈페이지

주간학습안내

1학년

2학년

3학년

4학년

5학년

6학년

열린교장실

독서교육지원시스템

책을 사랑하

1학년

2학년

3학년

4학년

5학년

6학년

<http://www.cis.upenn.edu/~nadiyah/projects/faas/>