Rolling up lattice cryptography primes

Daniel R. L. Brown

March 3, 2022

Abstract

Lattice cryptography uses fixed primes. Kolmogorov's descriptional complexity of the primes might interest the numerically curious.

59 509	48 12289
58 653	53 701
63 677	53 1277
53 701	53 3329
59 761	58 653
58 821	58 821
63 857	58 1013
64 953	58 6343
58 1013	59 509
53 1277	59 761
53 3329	63 677
74 4591	63 857
68 4621	63 7177
78 5167	64 953
58 6343	68 4621
63 7177	74 4591
78 7879	78 5167
48 12289	78 7879
80 8380417	80 8380417

Table 1: Word lengths of roll programs found for lattice cryptography primes

The roll programming language was introduced (in IACR eprint 2020/074) to help measure the descriptional complexity of fixed primes from elliptic

curve cryptography, partially addressing a concern about rigged primes. The analogous concern for lattice primes seems far smaller.

Ad hoc code golfing methods were used to find these roll programs. Existence of shorter roll programs (for each number) should be expected (for example, the program for 5167 uses no other tricks than choosing base three for a radix expansion).

```
509 subs 508 in +1
508 subs 254 in *2
254 subs 127 in *2
127 subs 7 in 2^-1
7   subs 3 in 2^-1
3   subs 2 in 2^-1
2^-1 roll *2+1 up 0
*2+1 subs *2 in +1
*2 roll +2 up 0
2 subs 0 in +2
+2 subs +1 in +1
0 subs in +1
```

```
653 subs 650 in +3
650 subs 130 in *5
130 subs 26  in *5
26  subs 25  in +1
25  subs  5  in *5
5   subs 1   in *5
*5 roll +5 up 0
1 subs in +2
0 subs in +1
+5 subs +3 in +2
+3 subs +2 in +1
+2 subs +1 in +1
```

```
677 subs 675 in +2
675 subs 135 in *5
135 subs 27  in *5
27  subs  9  in *3
9   subs  3  in *3
3   subs  1  in *3
*5 roll +5 up 0
*3 roll +3 up 0
1 subs in +2
0 subs in +1
+5 subs +3 in +2
+3 subs +2 in +1
+2 subs +1 in +1
```

```
701 subs 700 in +1
700 subs  70 in *10
70  subs   7 in *10
*10 roll +10 up 0
7 subs 4 in +3
4 subs in +5
0 subs in +1
+10 subs +5 in +5
+5 subs +3 in +2
+3 subs +2 in +1
+2 subs +1 in +1
```

```
761 subs 756 in +5
756 subs 126 in *6
126 subs  21 in *6
21  subs  18 in +3
18  subs   3 in *6
3   subs   0 in +3
*6  roll  +6 up  0
0 subs in +1
+6 subs +5 in +1
+5 subs +3 in +2
+3 subs +2 in +1
+2 subs +1 in +1
```

```
821 subs 819 in +2
819 subs  91 in *9
91  subs  90 in +1
90  subs  10 in *9
10  subs   9 in +1
9   subs   1 in *9
*9  subs  *3 in *3
*3  roll  +3 up  0
1 subs in +2
0 subs in +1
+3 subs +2 in +1
+2 subs +1 in +1
```

```
857 subs 856 in +1
856 subs 107 in *8
107 subs 104 in +3
104 subs  13 in *8
13  subs  10 in +3
10  subs   2 in +8
*8  roll  +8 up  0
2 subs in +3
0 subs in +1
+8 subs +4 in +4
+4 subs +2 in +2
+3 subs +2 in +1
+2 subs +1 in +1
```

```
953 subs 952 in +1
952 subs 119 in *8
119 subs 112 in +7
112 subs  14 in *8
14  subs   7 in +7
 7  subs   0 in +7
*8  roll  +8 up  0
0 subs in +1
+8 subs +4 in +4
+7 subs +4 in +3
+4 subs +2 in +2
+3 subs +2 in +1
+2 subs +1 in +1
```

```
1013 subs 1012 in +1
1012 subs 1008 in +4
1008 subs 84 in *12
84 subs 7 in *12
*12 roll +12 up  0
7 subs 3 in +4
3 subs in +4
0 subs in +1
+12 subs +4 in +8
+8 subs +4 in +4
+4 subs +2 in +2
+2 subs +1 in +1
```

```
1277 subs 1275 in +2
1275 subs 51 in *25
51 subs 50 in +1
50 subs 2 in *25
*25 subs *5 in *5
*5 roll +5 up  0
2 subs in +3
0 subs in +1
+5 subs +3 in +2
+3 subs +2 in +1
+2 subs +1 in +1
```

```
3329 subs 3328 in +1
3328 subs 13 in *256
*256 subs *16 in *16
*16 subs *4 in *4
13 subs 12 in +1
12 subs 3 in *4
3 subs in +4
*4 roll +4 up 0
+4 subs +2 in +2
+2 subs +1 in +1
0 subs in +1
```

```
4591 subs 4576 in +15
4576 subs 143 in *32
143 subs 128 in +15
128 subs 4 in *32
4 subs 0 in +4
*32 roll +32 up 0
0 subs in +1
+32 subs +16 in +16
+16 subs +8 in +8
+15 subs +8 in +7
+8 subs +4 in +4
+7 subs +6 in +1
+6 subs +4 in +2
+4 subs +2 in +2
+2 subs +1 in +1
```

```
4621 subs 4620 in +1
4620 subs 4616 in +4
4616 subs  577 in *8
577  subs  576 in +1
576  subs   72 in *8
72   subs    9 in *8
9    subs    8 in +1
8    subs    1 in *8
*8 roll +8 up 0
1 subs in +2
0 subs in +1
+8 subs +4 in +4
+4 subs +2 in +2
+2 subs +1 in +1
```

```
5167 subs 5166 in +1
5166 subs 1722 in *3
1722 subs  574 in *3
574  subs  573 in +1
573  subs  191 in *3
191  subs  189 in +2
189  subs   63 in *3
63   subs   21 in *3
21   subs    7 in *3
7    subs    6 in +1
6    subs    2 in *3
*3 roll +3 up 0
2 subs in +3
0 subs in +1
+3 subs +2 in +1
+2 subs +1 in +1
```

```
6343 subs 6342 in +1
6342 subs 6336 in +6
6336 subs  264 in *24
264  subs   11 in *24
*24 roll +24 up 0
11 subs in +12
0  subs in +1
+24 subs +12 in +12
+12 subs +6 in +6
+6 subs +3 in +3
+3 subs +2 in +1
+2 subs +1 in +1
```

```
7177 subs 7176 in +1
7176 subs 7168 in +8
7168 subs    7 in *1024
*1024 subs *512 in *2
*512  subs *64  in *8
*64   subs *8   in *8
*8 roll +8 up 0
*2 roll +2 up 0
7 subs in +8
0 subs in +1
+8 subs +4 in +4
+4 subs +2 in +2
+2 subs +1 in +1
```

```
7879 subs 7872 in +7
7872 subs  984 in *8
984  subs  123 in *8
123  subs  121 in +2
121  subs   11 in *11
11   subs    1 in *11
*11 roll +11 up 0
*8 roll +8 up 0
1 subs in +2
0 subs in +1
+11 subs +8 in +3
+8 subs +4 in +4
+7 subs +4 in +3
+4 subs +2 in +2
+3 subs +2 in +1
+2 subs +1 in +1
```

```
12289 subs 12288 in +1
12288 subs 3 in *4096
*4096 subs *256 in *16
*256 subs *16 in *16
*16 subs *4 in *4
*4 roll +4 up 0
3 subs in +4
0 subs in +1
+4 subs +2 in +2
+2 subs +1 in +1
```

```
8380417 subs 2^23-2^13 in +1
2^23-2^13 subs 13 2^10-1 in 2^*
2^10-1 subs 10 in 2^-1
2^-1 roll *2+1 up 0
2^* roll *2 up *1
*2+1 subs *2 in +1
*1 roll +1 up 0
13 subs 11 in +2
11 subs 10 in +1
10 subs 5 in *2
*2 roll +2 up 0
5 subs 4 in +1
4 subs 2 in +2
2 subs 0 in +2
+2 subs +1 in +1
0 subs in +1
```