practical complexity

No Institute Given

Abstract. practical complexity

1 Evaluating practical complexity

most part of the time is spent factoring norms. in practice:

1. trial division
2. pollard's rho
3. ecm

early abort of ECM: as soon as a large factor ($> B$) is found we stop factoring and compute the next norm (same if no factor is found after a number of trials).

how much time is wasted factoring non-smooth norms?

wasted time $\Leftrightarrow$ norm is not smooth but we have intended to factorise it $\Rightarrow$ either 1 large prime or no factor at all was found $\rightarrow$ assume the cheapest option: a large factor was found using ECM

lower bound on practical complexity given by: complexity of the NFS (i.e. number of norm to factor) * complexity of ECM

- NFS: $L_q(1/3, c)$ where c is a constant depending on the degree t of the elements sieved
- ECM (cost of finding a prime factor around B): $L_B(1/2, \sqrt(2)) * \mathrm{Log}(N)$ where N is the norm of the element

$L_q(\alpha, c) = \exp\left((c + o(1))(\log q)^\alpha (\log\log q)^{1-\alpha}\right)$

p a prime, n the extension degree, $q = p^n$, t degree of the sieved elements $c_1 = \frac{4}{3}\left(\frac{3t}{4(t+1)}\right)^{1/3}, B = L_q(1/3, c_1)$

minimal cost of 1 norm factorisation featuring a large prime (without $\log N$):

$$L_B\left(1/2, \sqrt{2}\right) = e^{\left(\sqrt{2}+o(1)\right)(\log B \log\log B)^{1/2}} \tag{1.1}$$

$$= e^{\left(\sqrt{2c_1}+o(1)\right)\left((\log q)^{1/3}(\log\log q)^{2/3}\log(c_1(\log q)^{1/3}(\log\log q)^{2/3})\right)^{1/2}} \tag{1.2}$$

$$= e^{\left(\sqrt{2c_1\frac{\log\left(c_1(\log q)^{1/3}(\log\log q)^{2/3}\right)}{(\log q)^{1/3}(\log\log q)^{2/3}}}+o(1)\right)(\log q)^{1/3}(\log\log q)^{2/3}} \tag{1.3}$$

$$= e^{\left(\sqrt{2\frac{\log\log B}{\log B}c1}+o(1)\right)(\log q)^{1/3}(\log\log q)^{2/3}} \tag{1.4}$$

$$= L_q\left(1/3, \sqrt{2\frac{\log\log B}{\log B}c1}\right) \tag{1.5}$$

C =practical complexity= number of norm sieved to find enough smooth * cost of 1 norm factorisation (with $\log N$):

$$C = L_q(1/3, c) L_q\left(1/3, \sqrt{2\frac{\log\log B}{\log B}c1}\right)\log N \tag{1.6}$$

$$= L_q(1/3, c2)\log N, \text{ with } c2 = c + \sqrt{2\frac{\log\log B}{\log B}c1} \tag{1.7}$$

Remark 1.1. $q \to \infty \Rightarrow B \to \infty \Rightarrow \frac{\log\log B}{\log B} \to 0 \Rightarrow c2 \to c \Rightarrow C \to L_q(1/3, c)\log N \to L_q(1/3, c) =$ NFS asymptotic complexity

2 cryptography

as=asymptotic security, ps=practical security

family-k	p (bits)	ECDLP	t	c	DLP (as)	DLP (ps)
MNT-6	160	80	2	$(256/27)^{1/3}$	93	123
BN-12	256	128	3	$(32/3)^{1/3}$	159	201
KSS-18	512	192	4	$(512/45)^{1/3}$	256	319

family-k	p	balanced ECDLP / DLP (as)
MNT-6	208	104
BN-12	370	185
KSS-18	832	312

family-k	p	balanced ECDLP / DLP (ps)
MNT-6	318	159
BN-12	518	259
KSS-18	1086	407