Crypto/Math Paper

SAND2020-8189R

Complexity of the GNFS

W.R. Cordwell

Sandia National Laboratories

SANDxxxxxx

May 2017

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S.Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.
SAND No. 20XX-XXXX.

General Number Field Sieve Complexity

For factoring an integer N, the complexity of the General Number Field Sieve is believed to be $C = e^{\left(\sqrt[3]{\frac{64}{9}}+o(1)\right)(ln(N))^{\frac{1}{3}}(ln(ln(N)))^{\frac{2}{3}}}$ [1].

Letting $lg(x)$ being the log base 2 of x, and noting that $ln(x) = ln(2) \cdot lg(x)$, we have $C = e^{\left(\sqrt[3]{\frac{64}{9}}+o(1)\right)(ln(2))^{\frac{1}{3}}(lg(N))^{\frac{1}{3}}(ln(2))^{\frac{2}{3}}(lg(ln(N)))^{\frac{2}{3}}}$.

Combining the powers of $ln(2)$ and converting the base, we obtain $C = 2^{\left(\sqrt[3]{\frac{64}{9}}+o(1)\right)(lg(N))^{\frac{1}{3}}(lg(ln(N)))^{\frac{2}{3}}}$.

With the innermost $ln(N) = ln(2) \cdot lg(N)$, and noting that $lg(ln(N)) = lg(ln(2)) + lg(lg(N))$, we see that the constant term can be absorbed into the $o(1)$ term in front, yielding $C = 2^{\left(\sqrt[3]{\frac{64}{9}}+o(1)\right)(lg(N))^{\frac{1}{3}}(lg(lg(N)))^{\frac{2}{3}}}$.

This argument works with any base–the complexity has the same form.

References

[1] Wikipedia, General number field sieve.