# Cryptology ePrint Archive: Report 2011/437

### Approximate common divisors via lattices

*Henry Cohn and Nadia Heninger*

**Abstract:** We analyze the multivariate generalization of Howgrave-Graham's algorithm for the approximate common divisor problem. In the $m$-variable case with modulus $N$ and approximate common divisor of size $N^\beta$, this improves the size of the error tolerated from $N^{\beta^2}$ to $N^{\beta^{(m+1)/m}}$, under a commonly used heuristic assumption. This gives a more detailed analysis of the hardness assumption underlying the recent fully homomorphic cryptosystem of van Dijk, Gentry, Halevi, and Vaikuntanathan. While these results do not challenge the suggested parameters, a $2^{\sqrt{n}}$ approximation algorithm for lattice basis reduction in $n$ dimensions could be used to break these parameters. We have implemented our algorithm, and it performs better in practice than the theoretical analysis suggests.

Our results fit into a broader context of analogies between cryptanalysis and coding theory. The multivariate approximate common divisor problem is the number-theoretic analogue of noisy multivariate polynomial interpolation, and we develop a corresponding lattice-based algorithm for the latter problem. In particular, it specializes to a lattice-based list decoding algorithm for Parvaresh-Vardy and Guruswami-Rudra codes, which are multivariate extensions of Reed-Solomon codes. This yields a new proof of the list decoding radii for these codes.

**Category / Keywords:** foundations / Coppersmith's algorithm, lattice basis reduction, approximate common divisors, fully homomorphic encryption, list decoding, Parvaresh-Vardy codes, noisy polynomial interpolation

**Date:** received 12 Aug 2011, last revised 13 Mar 2012

**Contact author:** nadiah at cs ucsd edu

**Available formats:** PDF | BibTeX Citation

**Version:** 20120314:015506 (All versions of this report)

**Discussion forum:** Show discussion | Start new discussion

---

[ Cryptology ePrint archive ]