# A brief chat about approximate GCDs

Henry Cohn and **Nadia Heninger**

# Approximate GCD problem

**You get:**

A bunch of near multiples of $p$.

**You have to:**

Find $p$.

$pq_1 + r_1$ $\quad$ $pq_2 + r_2$ $\quad$ $pq_3 + r_3$ $\quad$ $pq_m + r_m$

$$\hookrightarrow \quad p$$

**Motivation:** Factoring RSA modulus with partial information. [Howgrave-Graham 01]

# Fully homomorphic encryption over the integers

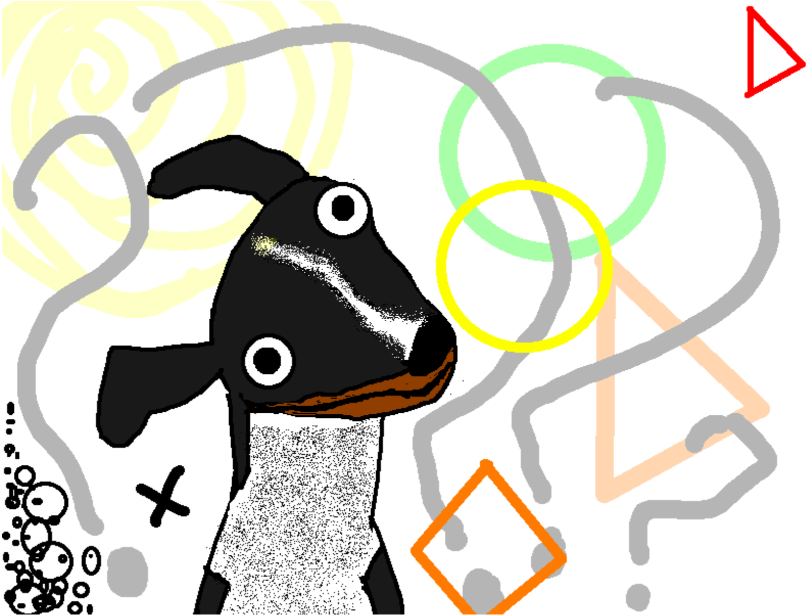
[van Dijk, Gentry, Halevi, Vaikuntanathan Eurocrypt 2010]

[Coron, Mandal, Naccache, Tibouchi Crypto 2011]

## Assumption:

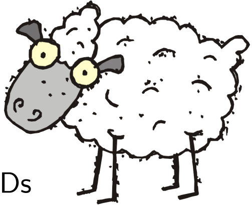
Approximate GCD is as hard for $m$ samples as for 2 samples.

Best way to break is to brute force over noise.

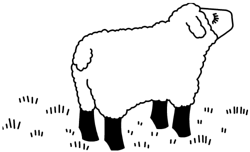


hyperboleandahalf.blogspot.com

# Our work



- Lattice-based algorithm for approximate GCDs with many samples.
- Multivariate extension of Coppersmith/Howgrave-Graham technique.
- As number of samples increases, amount of error tolerated increases.



- (Bonus: New list-decoding algorithm for Parvaresh-Vardy, Guruswami-Rudra, and other error-correcting codes.)

# Applications to fully homomorphic encryption

**Coron et al. key settings:**

Assuming LLL approximation of $1.04^{\dim L}$:

| key size | lattice dimension |
|---|---|
| toy | 165 |
| small | 595 |
| medium | 2211 |
| large | 9591 |

**van Dijk et al. asymptotic settings:**

Lattice approximation of $2^{\dim L^{2/3}}$ breaks suggested parameters.

Any polynomial key setting can be broken by subexponential lattice approximation ($2^{\dim L^{1/c}}$).

(Worst case enumeration takes $2^{\lambda}$ time for security parameter $\lambda$.)

# Approximate common divisors via lattices

http://eprint.iacr.org/2011/437