NTRUEncrypt parameters secure against CRYPTO '07 hybrid attacks

- Just finished a large internal assessment of lattice reduction estimates and generalized hybrid MITM techniques.
  - Generalized birthday attacks *are* possible
- Settled on parameters to standardize in X9.98 and IEEE 1363.1
  - Been very conservative!
- Published (today!) on eprint
  - Check it out!!
- Cash prizes!?
  - Currently debating whether to give $1000 for an improvement over our cryptanalysis (anyway there's money to send me down here for a one minute presentation, so …)