Cryptology ePrint Archive: Report 2011/436

Faster Algorithms for Approximate Common Divisors: Breaking Fully-Homomorphic-Encryption Challenges over the Integers

Yuanmi Chen and Phong Q. Nguyen

Abstract: At EUROCRYPT '10, van Dijk, Gentry, Halevi and Vaikuntanathan presented simple fully-homomorphic encryption (FHE) schemes based on the hardness of approximate integer common divisors problems, which were introduced in 2001 by Howgrave-Graham. There are two versions for these problems: the partial version (PACD) and the general version (GACD). The seemingly easier problem PACD was recently used by Coron, Mandal, Naccache and Tibouchi at CRYPTO '11 to build a more efficient variant of the FHE scheme by van Dijk {\em et al.}. We present a new PACD algorithm whose running time is essentially the ``square root'' of that of exhaustive search, which was the best attack in practice. This allows us to experimentally break the FHE challenges proposed by Coron {\em et al.} Our PACD algorithm directly gives rise to a new GACD algorithm, which is exponentially faster than exhaustive search: namely, the running time is essentially the $3/4$-th root of that of exhaustive search. Interestingly, our main technique can also be applied to other settings, such as noisy factoring and attacking low-exponent RSA.

Category / Keywords: public-key cryptography / fully-homomorphic encryption, cryptanalysis

Date: received 12 Aug 2011

Contact author: pnguyen at di ens fr