Cryptology ePrint Archive: Report 2013/026

RSA private key reconstruction from random bits using SAT solvers

Constantinos Patsakis

Abstract: SAT solvers are being used more and more in Cryptanalysis, with mixed results regarding their efficiency, depending on the structure of the algorithm they are applied. However, when it comes to integer factorization, or more specially the RSA problem, SAT solvers prove to be at least inefficient. The running times are too long to be compared with any well known integer factorization algorithm, even when it comes to small RSA moduli numbers.

The recent work on cold boot attacks has sparkled again the interest on partial key exposure attacks and in RSA key reconstruction. In our work, contrary to the lattice-based approach that most of these works use, we use SAT solvers. For the special case where the public exponent e is equal to three, we provide a more efficient modeling of RSA as an instance of a satisfiability problem, and manage to reconstruct the private key, given a part of the key, even for public keys of 1024 bits in few seconds.

Category / Keywords: SAT solvers, RSA, partial key exposure, factoring, public-key cryptography

Date: received 18 Jan 2013, last revised 18 Jan 2013

Contact author: patsakik at tcd ie