Cryptology ePrint Archive: Report 2011/591

A Unified Framework for Small Secret Exponent Attack on RSA

Noboru Kunihiro and Naoyuki Shinohara and Tetsuya Izu

Abstract: We address a lattice based method on small secret exponent attack on RSA scheme. Boneh and Durfee reduced the attack into finding small roots of a bivariate modular equation: $x(N+1+y)+1 ¥equiv 0 mod e)$, where N is an RSA moduli and e is the RSA public key. Boneh and Durfee proposed a lattice based algorithm for solving the problem. When the secret exponent d is less than $N^{0.292}$, their method breaks RSA scheme. Since the lattice used in the analysis is not full-rank, the analysis is not easy. Bl¥"omer and May gave an alternative algorithm. Although their bound $d ¥leq N^{0.290}$ is worse than Boneh--Durfee result, their method used a full rank lattice. However, the proof for their bound is still complicated. Herrmann and May gave an elementary proof for the Boneh--Durfee's bound: $d ¥leq N^{0.292}$. In this paper, we first give an elementary proof for achieving the bound of Bl¥"omer--May: $d ¥leq N^{0.290}$. Our proof employs unravelled linearization technique introduced by Herrmann and May and is rather simpler than Bl¥"omer--May's proof. Then, we provide a unified framework to construct a lattice that are used for solving the problem, which includes two previous method: Herrmann--May and Bl¥"omer--May methods as a special case. Furthermore, we prove that the bound of Boneh--Durfee: $d ¥leq N^{0.292}$ is still optimal in our unified framework.

Category / Keywords: public-key cryptography / lattice techniques, RSA, cryptanalysis

Publication Info: This is a full version of SAC2011 paper.

Date: received 30 Oct 2011

Contact author: kunihiro at k u-tokyo ac jp