ICRAMCS 2026

THE EIGHTH EDITION OF THE INTERNATIONAL CONFERENCE ON RESEARCH IN APPLIED MATHEMATICS AND COMPUTER SCIENCE
April 23-24-25, 2026 | Marrakech, Morocco

An Enhanced Small Private Exponent Attack Against RSA

Communication Info

Authors:
Brahim CHNIOUNE [1]
Mohammed RAHMANI [1]
Mhammed ZIANE [1]

[1] *Mohammed I University, Oujda, Morocco*

Keywords:
(1) RSA
(2) Lattices
(3) Coppersmith's algorithm
(4) Factoring problem

Abstract

In their seminal work [1], Boneh and Durfee introduced a small private exponent attack on the RSA cryptosystem by solving the key equation $ed - k(p - 1)(q - 1) = 1$, and proved that RSA can be broken whenever the private exponent satisfies $d < N^{0.292}$. Notably, more than twenty-eight years later, no subsequent small private exponent attack has improved this bound. In this paper, we demonstrate that if the prime factors share a portion of their most significant bits, then a stronger bound exceeding $N^{0.292}$ can be achieved; moreover, under these conditions, the RSA primes can be recovered in polynomial time.

References

[1] Boneh, D., Durfee, G.: Cryptanalysis of RSA with private key d less than N0.292, Advances in Cryptology-Eurocrypt'99, Lecture Notes in Computer Science 1592, pp. 1–11,Springer, Berlin, Heidelberg, (1999).
[2] Boneh, D.: Twenty years of attacks on the RSA cryptosystem. Not. Am. Math. Soc. 46(2), 203–213 (1999)
[3] Jochemsz, E., May, A.: A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants, In: ASIACRYPT 2006, LNCS 4284, pp. 267–282, Springer-Verlag (2006)
[4] Coppersmith, D.: Small solutions to polynomial equations, and low exponent RSA vulnerabilities. J. Cryptol. 10(4), 233–260 (1997)