ICRAMCS 2026

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

Generalized Cryptanalysis of a Cubic Pell-Based Cryptosystem

Communication Info

Authors:
Mostafa CHAKER[1]
Mohammed RAHMANI [2]
Siham EZZOUAK[1]

[1] Faculty of sciences, Dhar Al Mahraz, Sidi Mohammed Ben Abdellah University, Fez, Morocco
[2] Faculty of sciences, Mohammed I University, Oujda, Morocco

Keywords:
(1) Cubic Pell RSA Scheme
(2) Lattice basis reduction techniques
(3) Integer factoring problem

Abstract

At AFRICACRYPT 2025, Rahmani and Nitaj introduced a cryptanalytic attack on the cubic Pell RSA scheme defined by the key equation $ed - k(p - 1)^2 (q - 1)^2 = 1$ when the private exponent d is sufficiently small. In this paper, we investigate the generalized relation $eu - k(p - 1)^2 (q - 1)^2 = z$ and present a lattice-based attack demonstrating that, when the parameters u, k, and z are sufficiently small and the difference between the RSA primes p and q is small, the prime factors can be recovered in polynomial time, thereby improving upon all previously known attacks on this class of constructions. Moreover, our method extends to larger private exponents.

References

[1] Coppersmith, D., Small solutions to polynomial equations, and low exponent RSA vulnerabilities. Journal of Cryptology,10(4), 233–260, (1997). [2] Authors, Title Journal, Volume, Year, Pages.
[2] Feng, Y., Nitaj, A., Pan, Y., Partial prime factor exposure attacks on some RSA variants. Theoretical Computer Science, 999, pp. 114549, Elsevier (2024).
[4] Howgrave-Graham, N., Finding small roots of univariate modular equations revisited, In: IMA International Conference on Cryptography and Coding, LNCS 1355, pp. 131–142, Springer, Berlin, Heidelberg (1997).
[5] Rahmani, M., Nitaj, A., Improved Cryptanalysis of an RSA Variant Based on Cubic Pell Curve. In International Conference on Cryptology in Africa. Cham: Springer Nature Switzerland, pp. 113-125, (2025).