Misarsky, Jean-François

A multiplicative attack using LLL algorithm on RSA signatures with redundancy. (English)

Zbl 0882.94024

Kaliski, Burton S. jun. (ed.), Advances in Cryptology - CRYPTO '97. 17th annual international cryptology conference. Santa Barbara, CA, USA. August 17–21, 1997. Proceedings. Berlin: Springer. Lect. Notes Comput. Sci. 1294, 221-234 (1997).

Summary: We show that some RSA signature schemes using fixed or modular redundancy and dispersion of redundancy bits are insecure. Our attack is based on the multiplicative property of an RSA signature function and extends old results of [*W. De Jonge* and *D. Chaum*, "Attacks on some RSA Signatures", Advances in Cryptology, Crypto '85, Lect. Notes Comput. Sci. 218, 18-27 (1986)] as well as recent results of [*M. Girault* and *J. F. Misarsky*, "Selective Forgery of RSA Signatures Using Redundancy", Advances in Cryptology-Eurocrypt '97, Lect. Notes Comput. Sci. 1233, 495-507 (1997)]. Our method uses the lattice basis reduction and algorithms of *László Babai* [Combinatorica 6, 1-13 (1986; Zbl 0593.68030) also see Zbl 0569.10015]. Our attack is valid when the length of redundancy is roughly less than half the length of the public modulus. We successfully apply our attack to a scheme proposed for discussion inside ISO. Afterwards, we also describe possible adaptations of our method to attack schemes using mask or different modular redundancies. We explain limits of our attack and how to defeat it.

For the entire collection see [Zbl 0870.00047].

MSC:

94A60 Cryptography
11Y16 Number-theoretic algorithms; complexity
11H06 Lattices and convex bodies (number-theoretic aspects)
90C10 Integer programming

Keywords:

RSA signature schemes; lattice basis reduction