Cryptology ePrint Archive: Report 2011/057

Another Look at RSA Signatures With Affine Padding

Jean-Sébastien Coron and David Naccache and Mehdi Tibouchi

Abstract: It is well-known that, due to the homomorphic properties of the RSA function, textbook RSA signatures are insecure, and a common workaround is to encode messages with a so-called padding function mu before applying the RSA{} function.

The simplest padding functions are probably affine paddings, and a significant amount of work has been devoted to assess their security, so as to better understand the properties of the RSA function. It turns out that RSA signatures with affine padding can be forged in polynomial time if the size of the message m is too large---a thread of publications progressively reduced the size of m for which a forgery can be constructed, down to the current bound of $1/3$ of the bit size of the public modulus N. Improving this bound further to 1/4 has been an elusive open problem for the past decade.

This paper presents several new results on the security of RSA signatures with affine padding which constitute some progress towards a solution to this longstanding open problem.

First, we show that affine RSA signatures can be forged in polynomial time on messages of larger bit size, but whose entropy is only 1/4 of the modulus size. We also show how a multiplicative relation between the affine paddings of four messages, three of which are of bit size 1/4 and the fourth is of size 3/8, can be obtained faster than factoring.

Finally, we show than $(1/4)$-forgeries can be obtained in some special scenarios, including one in which one can sign with two independent paddings, and another in which the most significant bits of the public modulus are chosen maliciously.

Category / Keywords: RSA, digital signature, forgery, padding

Date: received 31 Jan 2011, last revised 1 Sep 2011

Contact author: david naccache at ens fr