Cryptology ePrint Archive: Report 2011/271

Practical Key-recovery For All Possible Parameters of SFLASH

Charles Bouillaguet and Pierre-Alain Fouque and Gilles Macario-Rat

Abstract: In this paper we present a new practical key-recovery attack on the SFLASH signature scheme. SFLASH is a derivative of the older C^* encryption and signature scheme that was broken in 1995 by Patarin. In SFLASH, the public key is truncated, and this simple countermeasure prevents Patarin's attack. The scheme is well-known for having been considered secure and selected in 2004 by the NESSIE project of the European Union to be standardized.

However, SFLASH was practically broken in 2007 by Dubois, Fouque, Stern and Shamir. Their attack breaks the original (and most relevant) parameters, but does not apply when more than half of the public key is truncated. It is therefore possible to choose parameters such that SFLASH is not broken by the existing attacks, although it is less efficient.

We show a key-recovery attack that breaks the full range of parameters in practice, as soon as the information-theoretically required amount of information is available from the public-key. The attack uses new cryptanalytic tools, most notably pencils of matrices and quadratic forms.

Category / Keywords: public-key cryptography / SFLASH, multivariate cryptography, practical cryptanalysis, key-recovery

Date: received 27 May 2011

Contact author: charles bouillaguet at ens fr