Cryptology ePrint Archive: Report 2011/356

An Efficient Attack on All Concrete KKS Proposals

Ayoub Otmani and Jean-Pierre Tillich

Abstract: Kabastianskii, Krouk and Smeets proposed in 1997 a digital signature scheme based on a couple of random error-correcting codes. A variation of this scheme was proposed recently and was proved to be EUF-1CMA secure in the random oracle model. In this paper we investigate the security of these schemes and suggest a simple attack based on (essentially) Stern's algorithm for finding low weight codewords. It efficiently recovers the private key of all schemes of this type existing in the literature. This is basically due to the fact that we can define a code from the available public data with unusual properties: it has many codewords whose support is concentrated in a rather small subset. In such a case, Stern's algorithm performs much better and we provide a theoretical analysis substantiating this claim. Our analysis actually shows that the insecurity of the proposed parameters is related to the fact that the rates of the couple of random codes used in the scheme were chosen to be too close. This does not compromise the security of the whole KKS scheme. It just points out that the region of weak parameters is really much larger than previously thought.

Category / Keywords: public-key cryptography / Code-based cryptography, digital signature, random error-correcting codes, cryptanalysis

Date: received 2 Jul 2011

Contact author: jean-pierre tillich at inria fr