Cryptology ePrint Archive: Report 2011/686

Analysis of some natural variants of the PKP Algorithm

Rodolphe LAMPE and Jacques PATARIN

Abstract: In 1989, Adi Shamir proposed a new zero-knowledge identification scheme based on a NP-complete problem called PKP for Permuted Kernel Problem. For a given prime p, a given matrix A and a given vector V , the problem is to find a permutation \pi such that the permuted vector V_\pi verifies A.V_\pi = 0 mod p. This scheme is still in 2011 known as one of the most efficient identification scheme based on a combinatorial problem. However, we will see in this paper that it is possible to improve this scheme significantly by combining new ideas in order to reduce the total number of computations to be performed and to improve very efficiently the security against side channel attacks using precomputations. We will obtain like this a new scheme that we have called SPKP. Moreover, if we use precomputed values in the scheme SPKP, then the prover will need to perform no computations (i.e. only selection and transmission of precomputed values). This is very interesting for security against side channel attacks because our scheme is zero-knowledge and we don't perform any computations using the key during the identification so we prove that any attacker (even using side channel attacks) being successfully identified implies that he has a solution to the NP-complete problem PKP.

Category / Keywords: public-key cryptography / identification scheme, zero knowledge, permuted kernel problem

Date: received 16 Dec 2011, last revised 4 Jul 2012

Contact author: rodolphe lampe at gmail com

Available formats: PDF | BibTeX Citation

Version: 20120704:182542 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]