Cryptology ePrint Archive: Report 2011/329

Hardness of Computing Individual Bits for Pairing-based One-way Functions

Alexandre Duc and Dimitar Jetchev

Abstract: We prove that if one can predict any of the bits of the input to a classical pairing-based one-way function with non-negligible advantage over a random guess then one can efficiently invert this function and thus, solve the Fixed Argument Pairing Inversion problem (FAPI-1/FAPI-2). The latter has implications for the security of various pairing-based schemes such as the identity-based encryption scheme of Boneh--Franklin, Hess' identity-based signature scheme, as well as Joux's three-party one-round key agreement protocol. Moreover, if one can solve FAPI-1 and FAPI-2 in polynomial time then one can solve the Computational Diffie--Hellman problem (CDH) in polynomial time. Our result implies that all the bits of the pairing-based one-way function are hard--to--compute, assuming that CDH is hard. Our argument uses a list-decoding technique via discrete Fourier transforms due to Akavia--Goldwasser--Safra.

Category / Keywords: foundations / One-way function, hard--to--compute bits, bilinear pairings, fixed argument pairing inversion problem, Fourier transform.

Date: received 17 Jun 2011

Contact author: dimitar jetchev at epfl ch

Available formats: Postscript (PS) | Compressed Postscript (PS.GZ) | PDF | BibTeX Citation

Version: 20110622:200705 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]