Cryptology ePrint Archive: Report 2011/706

Improved Side Channel Attacks on Pairing Based Cryptography

Johannes Blömer and Peter Günther and Gennadij Liske

Abstract: Techniques from pairing based cryptography (PBC) are used in an in- creasing number of cryptographic schemes. With progress regarding efficient implementations, pairings also become interesting for applications on smart cards. With these applications the question of the vulnerability to side channel attacks (SCAs) arises. Several known invasive and non-invasive attacksagainst pairing algorithms only work if the second but not if the &#64257;rst argument of the pairing is the secret. In this paper we extend some of these attacks also to the case where the &#64257;rst argument is the secret. Hence we may conclude that positioning the secret as the &#64257;rst argument of the pairing does not improve the security against SCAs, as it sometimes has been suggested.

Category / Keywords: implementation /

Date: received 27 Dec 2011, last revised 24 Jan 2012

Contact author: peter guenther at uni-paderborn de

Available formats: PDF | BibTeX Citation

Version: 20120124:090118 (All versions of this report)

Discussion forum: Show discussion | Start new discussion
