Cryptology ePrint Archive: Report 2012/723

Two Exponentiation Algorithms Resistant to Cross-correlation Power Analysis and to Other Known Attacks

Yaacov Belenky, Zeev Geyzel, Michael Kara-Ivanov and Avraham Entelis

Abstract: In order to prevent the SPA (Simple Power Analysis) attack against modular exponentiation algorithms, a multiply-always implementation is generally used. Witteman et al. introduced in \cite{WI} a new cross-correlation power analysis attack against the multiply-always implementation. We suggest two new algorithms, resistant to this attack and also to other known attacks.

The first algorithm is an alternative approach to exponentiation algorithms used in cryptography, which usually receive as an input some representation (e.g. binary) of the exponent. In our approach both the exponent and the result are functions (not necessarily easily invertible) of the exponentiation algorithm input. We show that this approach can have a good performance and that it is also resistant to several known attacks, especially to the cross-correlation power analysis. It is particularly relevant for cryptographic schemes in which the private exponent can be chosen arbitrarily.

Another exponentiation algorithm that we present here may be preferable for use with RSA in certain settings. It is resistant to the cross-correlation power analysis attack, C safe error attack, and other attacks; although it involves squaring operations.

Category / Keywords: secret-key cryptography / smart cards

Date: received 26 Dec 2012

Contact author: aentelis at nds com