Seeing through MIST Given a Small Fraction of an RSA Private Key

Colin D. Walter

Comodo Research Lab
10 Hey Street, Bradford, BD7 1DQ, UK
Colin.Walter@comodogroup.com www.comodogroup.com

Abstract. In smartcard encryption and signature applications, randomised algorithms are used to increase tamper resistance against attacks based on side channel leakage. MIST is one of these. As is the case with the classical m-ary and sliding windows exponentiation algorithms, the most significant half of the public modulus yields information which can be used to halve the number of key digits which need to be guessed to recover the secret key from a MIST side channel trace. Lattice based methods are used to reduce this to just one quarter of the least significant digits. This enables the strength of the MIST exponentiation algorithm to be guaged more accurately under several threat models.

Key words: Addition chains, division chains, randomized exponentiation, Mist, randomary exponentiation, RSA, side channel leakage, power analysis, SPA, DPA, SEMA, DEMA, blinding, smartcard.

1 Introduction

Smartcards have very limited scope for the inclusion of physical security measures. So tamper resistance should also be built into the component algorithms whenever possible. Because exponentiation is such a major process in many crypto-systems, including RSA, Diffie-Hellman and ECC, it is the main target for improved algorithmic methods. Initial side channel attacks made use of timing differences due to conditional subtractions during modular multiplications. Such differences are now easily avoided. However, because unprotected hardware gates use different amounts of power depending upon whether or not they are switched to a different state, power usage by any chip is also data dependent, and so provides side channel leakage which may enable secret keys to be recovered. Although the first power attacks required averaging over a number of exponentiations in order to reduce the effects of noise and dependence on irrelevant data, recent progress suggests that there is enough data in the trace of a single exponentiation to allow careful averaging to reveal the key. In particular, one can average over subsets of digit-by-digit products within each long integer multiplication rather than the sequential traces of many exponentiations. In addition, electro-magnetic leakage seems to provide a very much more powerful means of obtaining key data than power variation.