Some Security Aspects of the Mist Randomized Exponentiation Algorithm (Abstract)

Colin D. Walter

Comodo Research Laboratory
10 Hey Street, Bradford, BD7 1DQ, UK
www.comodo.net

Abstract. The Mist exponentiation algorithm [1, 2] is intended for use in embedded crypto-systems to provide protection against power analysis attacks. It generates randomly different addition chains for performing a particular exponentiation. This means that power attacks on RSA decryption or signing which require averaging over a number of exponentiation power traces become impossible. However, averaging over digit-by-digit multiplication traces may allow the detection of operand re-use. Although this provides a handle for an attacker by which the exponent search space might be considerably reduced, the number of possible exponents is shown to be still well outside the range of feasible computation in the foreseeable future.

Key words: Random-ary exponentiation, Mist exponentiation algorithm, division chains, addition chains, power analysis, DPA, DEMA, blinding, smartcard.

1 Introduction

Because smartcards have very limited scope for the inclusion of physical security measures, the existence of side channel leakage from embedded cryptographic systems creates the need for new algorithms which can be implemented in more secure ways than those currently in use. This is particularly true for exponentiation, which is a major process in many crypto-systems such as RSA, Diffie-Hellman and ECC. Initial power attacks required averaging over a number of exponentiations in order to reduce the effects of noise and dependence on uninteresting data. Although the necessary alignment of power traces can be made more difficult by the insertion of obfuscating, random, non-data-dependent operations, the data transfers between operations usually reveal the commencement of every long integer or elliptic curve operation very clearly in each individual trace. So it is usually possible to perform the averaging process and mount an attack to extract meaningful secret data. Fortunately, attacks which require such averaging can be defeated by modifying the exponent d to $d{+}rg$ where r is a random number and g is the order of the (multiplicative) semi-group in which the exponentiation is performed. This results in a different exponentiation procedure being performed every time...

References

1. C. D. Walter, *Improvements in, and relating to, Cryptographic Methods and Apparatus*, UK Patent Application 0126317.7, Comodo Research Laboratory, 2001.
2. C. D. Walter, *MIST: An Efficient, Randomized Exponentiation Algorithm for Resisting Power Analysis*, Topics in Cryptology – CT-RSA 2002, B. Preneel (editor), Lecture Notes in Computer Science, **2271**, Springer-Verlag, 2002, 53–66.