Issues of Security with the Oswald-Aigner Exponentiation Algorithm

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, randomized algorithms can be used to increase tamper resistance against attacks based on averaging data-dependent power or EMR variations. Oswald and Aigner describe such an algorithm for point multiplication in elliptic curve cryptography (ECC). Assuming an attacker can identify and distinguish additions and doublings during a single point multiplication, it is shown that the algorithm is insecure for repeated use of the same secret key without blinding of that key. Thus blinding should still be used or great care taken to minimise the differences between point additions and doublings.

Key words: Addition-subtraction chains, randomized exponentiation, elliptic curve cryptography, ECC, point multiplication, power analysis, SPA, DPA, SEMA, DEMA, blinding, smartcard.

1 Introduction

Side channel attacks [6,7] on embedded cryptographic systems show that substantial data about secret keys can leak from a *single* application of a cryptographic function through data-dependent power variation and electro-magnetic radiation [12,13]. This is particularly true for crypto-systems which use the computationally expensive function of exponentiation, such as RSA, ECC and Diffie-Hellman. Early attacks required averaging over a number of exponentiations [9] to extract meaningful data, but improved techniques mean that single exponentiations using traditional algorithms may be insecure. In particular, it should be assumed that the pattern of squares and multiplies can be extracted fairly accurately from side channel leakage, perhaps by using Hamming weights to identify operand re-use. Where the standard binary "square-and-multiply" algorithm is used, this pattern reveals the secret exponent immediately.

In this context, Oswald and Aigner proposed a randomized point multiplication algorithm [10] for which there is no bijection between scalar key values and sequences of curve operations. They randomly switch to a recoding procedure so that multiplications appear to occur for zero bits but not for one bits. This alternative corresponds to a standard recoding of the input bits to remove long sequences of 1s and introduces other non-zero digits such as $\bar{1}$. On the one hand, the pattern of squares and multiplications is no longer fixed, so that averaging