More Detail for a Combined Timing and Power Attack against Implementations of RSA

Werner Schindler[1] and Colin D. Walter[2]

[1] Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189, 53175 Bonn, Germany
Werner.Schindler@bsi.bund.de
[2] Comodo Research Laboratory
10 Hey Street, Bradford, BD7 1DQ, UK
Colin.Walter@comodogroup.com

Abstract. Implementations of Montgomery's modular multiplication algorithm (MMM) typically make conditional subtractions in order to keep the output within register or modulus bounds. For some standard exponentiation algorithms such as m-ary, it has been shown that this yields enough information to deduce the value of the exponent. This has serious implications for revealing the secret key in cryptographic applications without adequate counter-measures. Much more detail is provided here about the distribution of output values from MMM when the output is only reduced to keep it within register bounds, about how implementations of sliding windows can be attacked, and about handling errors.

Key Words. RSA cryptosystem, side channel leakage, power analysis, timing attack, Montgomery modular multiplication, exponentiation, statistical decision problem.

1 Introduction

Side-channel leakage occurs through data dependent variation in the use of resources such as time and hardware. The former results from branching in the code or compiler optimisation [4], and the latter from data causing gate switching in the circuitry. Both manifest themselves measurably through overall current variation as well as local or global electro-magnetic radiation (EMR) [5-7]. Information leaking in these ways might be used by an attacker to deduce secret cryptographic keys which are contained securely inside a smart card.

Timing variation can be measured using overall delay during decryption or signing [1, 4, 11, 13]. However, for successful attacks on keys with limited lifespans for which only a bounded number of decryptions with the same key is allowed, some finer detail may become necessary, such as the time variations for executing component procedures. This detail can be seen by observing delays between the characteristic power consumption wave form for loading instructions and data at the start of the procedure. Here this is applied to the version of Montgomery modular multiplication [9] which contains a final conditional subtraction for reducing the output by only enough to fit within register bounds.