Exponent Blinding and Scalar Blinding in the Context of Side-Channel Analysis

Werner Schindler

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185–189
53175 Bonn, Germany
Werner.Schindler@bsi.bund.de

Abstract

In his pioneering paper on timing analysis (1996) Paul Kocher proposed exponent blinding as a possible countermeasure against timing attacks on RSA (without CRT). For the j^{th} exponentiation the secret exponent d then is not used itself but the blinded exponent $v_j := d + r_j\varphi(n)$ where r_j denotes a random number. Exponent blinding may be applied to RSA with CRT as well (with $d_p := d(\bmod p-1)$ in place of d and $v_j := d_p + r_j\varphi(p)$). For ECC applications the scalar multiplication may be blinded analogously by replacing $\varphi(n)$ by the order of the base point.

Exponent blinding and scalar blinding shall prevent an attacker from bringing together information on different blinded exponents, which he has gained e.g. from a side-channel attack. Although exponent blinding and scalar blinding are known as strong countermeasures this goal cannot be ensured entirely in general.

Fouque et al. (2006) showed that for RSA without CRT exponent blinding may be overcome if the attacker knows some exponent bits from all power traces with certainty. However, power attacks and electromagnetic radiation attacks usually allow to guess all exponent bits though with some uncertainty.

Schindler and Itoh (2011) have developed generic attacks on RSA implementations (with CRT and without CRT) and on ECC implementations under the assumption that the particular bit guesses are wrong with some probability $\epsilon_b > 0$. Schindler and Wiemers (2014, 2015) have introduced new attack variants, which allow to tackle larger error rates ϵ_b and larger blinding lengths R. In particular, for elliptic curves for which the order y of the base point is 'slightly' larger than a power 2^n (let's say, $y - 2^n \approx 2^{n/2}$) two extremely efficient attack variants exist.

Moreover, a timing attack on unprotected RSA implementations (RSA with CRT, Montgomery multiplication) could be extended to a timing attack in the presence of exponent blinding (Schindler 2000, 2014).

The talk presents the current state of the art.