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

Werner Schindler
Bundesamt für Sicherheit in der Informationstechnik (BSI)
Bonn, Germany

Leuven, June 30, 2015

Outline

- Introduction and motivation
- Attacks on RSA and on general elliptic curves
- Attacks on special elliptic curves
- Conclusion

Introduction

- Exponent blinding (RSA) and scalar blinding (elliptic curves) are well-known countermeasures against side-channel attacks and fault attacks.

- Notation:
- d = long-term key
- k = bit length of d
- R = blinding length
- $r_j \in \{0, \ldots, 2^R - 1\}$, $r_j = j^{\text{th}}$ blinding factor

- $v_j = d + r_j y$ blinded j^{th} exponent / blinded j^{th} scalar
  - *RSA with CRT:* $y = \phi(p)$, $d = d_{(\text{RSA})}(\text{mod}(p-1))$
  - *RSA without CRT:* $y = \phi(n)$
  - *Elliptic curves:* y = order of the base point

Motivation

- $v_1, v_2, \ldots, v_N$ are different with high probability.
- This shall prevent the combination of information on different blinded exponents / blinded scalars.
- If exponent blinding / scalar blinding would achieve this aim perfectly this should lift the resistance of a device against SPA and single trace template attacks to the resistance against any type of power attack.

Attacks on Exponent Blinding

- For RSA without CRT already [2] showed that this hope is invalid in general.
- Reference [2] assumes that the attacker is able to identify some bits from many exponents with certainty, and [1] extends this attack to the case of noisy measurements.
- Exclusive exponent blinding may not even prevent pure timing attacks (cf. [7], scenario: RSA with CRT and Montgomery's multiplication algorithm).

Our Attack Scenario

- An attacker has obtained guesses $\widetilde{v}_1, \ldots, \widetilde{v}_N$ for $v_1, \ldots, v_N$
  - Source of these guesses: SPA, single trace template attacks, or any other side-channel attack on single exponentiations / single scalar multiplications
- $\epsilon_b := \mathrm{Prob}(\widetilde{v}_{j,i} \neq v_{j,i})$ (probability of a wrong bit guess)

The Basic Attack (I) [3, 4]

- The Basic Attack is applicable to RSA (with and without CRT) and to elliptic curves.
- $\widetilde{v}_j = v_j \oplus e_j$ (exponent guess, e_j = error vector)
- Key observation:

$$\mathrm{ham}(\widetilde{v}_j \oplus \widetilde{v}_m) = \mathrm{ham}(\underbrace{v_j \oplus v_m}_{=0 \text{ iff } r_j = r_m} \oplus e_j \oplus e_m)$$

$$E\left(\mathrm{ham}(\widetilde{v}_j \oplus \widetilde{v}_m)\right) \begin{cases} \leq 2\epsilon_b(k+R) & \text{if } r_j = r_m \\ \approx (k+R)/2 & \text{if } r_j \neq r_m \end{cases} \qquad (1)$$

- Combined with a suitable threshold γ observation (1) provides an effective distinguisher between the two cases $(r_j = r_m)$ and $(r_j \neq r_m)$.

The Basic Attack (II)

Algorithm:

1. Apply (1) to divide the guesses $\widetilde{v}_1, \widetilde{v}_2, \ldots$ into classes with identical (yet unknown) blinding factors.
   Terminate when some class ('winning class') contains $t = t(k, R, \epsilon_b)$ elements.
2. Apply bitwise the majority decision rule to the guesses of the winning class $\rightarrow$ guess $\widetilde{v}_c$.
3. Check whether $\widetilde{v}_c$ is correct.
   Otherwise, flip some bits until a valid key has been found (attack successful), or if the number of trials has exceeded a pre-defined threshold (attack fails).

Example: $(k, R) = (1024, 16)$: The basic attack tolerates error rates $\epsilon_b \leq 0.25$.

- Large R make the basic attack impractical because the number of traces and of mutual comparisons 'explode'.

The Enhanced Attack (I) [3, 4]

- The Enhanced Attack is applicable to RSA (with and without CRT) and to elliptic curves ($u = 2, 3, 4$).

Observation:

- If $r_{j_1} + \cdots + r_{j_u} = r_{i_1} + \cdots + r_{i_u}$ (Case A) then $\mathrm{ham}(\mathrm{NAF}((\widetilde{v}_{j_1} + \cdots + \widetilde{v}_{j_u}) - (\widetilde{v}_{i_1} + \cdots + \widetilde{v}_{i_u})))$ is 'small'.
- If $r_{j_1} + \cdots + r_{j_u} \neq_{i_1} + \cdots + r_{i_u}$ (Case B) then $\mathrm{ham}(\mathrm{NAF}((\widetilde{v}_{j_1} + \cdots + \widetilde{v}_{j_u}) - (\widetilde{v}_{i_1} + \cdots + \widetilde{v}_{i_u}))) \approx \frac{k+R}{3}$

- Combined with a suitable threshold β this observation provides a distinguisher (2) between Case A and Case B.

The Enhanced Attack (II)

- Each decision for Case A yields a linear equation in the blinding factors.

  The attack falls into three phases

  1. Apply decision rule (2) to index vectors $(j_1, \ldots, j_u)$ and $(i_1, \ldots, i_u)$ with $j_1, \ldots, j_u, i_1, \ldots, i_u \in \{1, \ldots, N\}$ until $N-2$ linearly independent equations have been found.
  2. Solve this system of linear equations
  3. Apply an error detection and correction algorithm. This algorithm returns y (RSA) or $d + ry$ (ECC).

- Phase 1 dominates the workload of the enhanced attack.

The Enhanced Attack (III)

Numerical examples: RSA with CRT, 1024-bit primes

1. $(R, u, \epsilon_b) = (32, 2, 0.11)$: $N \approx 5000$, $\approx 1.7 \cdot 2^{45}$ mutual comparisons.
2. $(R, u, \epsilon_b) = (48, 3, 0.07)$: $N \approx 2400$, $\approx 2^{61}$ mutual comparisons.
3. $(R, u, \epsilon_b) = (64, 4, 0.05)$: $N \approx 2000$, $\approx 2^{77}$ mutual comparisons.

- Note: For elliptic curves y is known, and for RSA without CRT the upper half of $y = \phi(n)$. This allows more efficient attacks ($\rightarrow$ variants of the enhanced attack, alternate attacks).

RSA with CRT – New Results [5]

- The limiting factor of the enhanced attack is not the number of traces but the number of comparisons. Paper [5] introduces two improvements:
  - A pre-step ('sieving step') to the enhanced attack increases the ratio of Case A-situations ($\rightarrow$ linear equation), thereby reducing the number of mutual of comparisons.
  - A pre-step based on continued fractions allows to adapt a variant of the alternate attack [4].
- Compared to [4] both variants improve the attack efficiency on RSA with CRT.

Attacks on Elliptic Curves [6]

- Both the basic attack and the enhanced attack are applicable to elliptic curves.
- In [6] two new attacks against special elliptic curves are introduced.
- All these attacks assume that the scalar multiplications are carried out with blinded long-term keys.
- ECDSA is not concerned.

- Applications of Static Scalar Multiplications
  - static Diffie Hellman
  - ECIES
  - signature-less authentication process for TLS 1.3 (proposal of H. Krawczyk)
  - deterministic signatures

Special Elliptic Curves

- $y = 2^k \pm y_0$ with $y_0 = 2^t + \cdots + 1$ and $t \approx k/2$ (concerns in particular elliptic curves over GF(p) when $p \approx 2^{k+b}$ with cofactor 2^b, $b \geq 0$)
- Examples: NIST P-384, ED448, M-511, Curve41417, Curve25519.

- 'gap' $g := k - t - 1$
- Note: If $y = 2^k + y_0$ then $g = \#$ of zeroes between the two most significant '1's in the binary representation of y.

The Attack Idea

- Paper [6] introduces two attacks on such special curves, the so-called *Wide Window Attack* and the *Narrow Window Attack*.

Key observation: (for $y = 2^k + y_0$)

- $v_j = d + r_j y = r_j 2^k + (d + r_j y_0)$
- If $R \leq g - 7$, for instance, a carry of $(d + r_j y_0)$ from bit $k - 1$ to k is rather unlikely.
- $\Longrightarrow \widetilde{v}_{j;k}, \ldots, \widetilde{v}_{j;k+R-1}$ may serve as initial bit guesses for $r_{j;0}, .., r_{j;R-1}$ (error probability ϵ_b).

- Note: Both attacks work even for $R \leq g - 2$ (!)

The Narrow Window Attack

- **Phase 1** Guess iteratively the R least significant bits of the long-term key d and the blinding factors $r_1, \ldots, r_N$. (Within Phase 1 the trace j may be removed if some intermediate guess for $r_j (\bmod 2^w)$ is assumed to be false.)
- **Phase 2** Identify those guesses of blinding factors, which are correct. Remove the other guesses.
- **Phase 3** Guess the bits $R, \ldots, k-1$ of d from the guesses $\widetilde{r}_{j_1}, \widetilde{r}_{j_2}, \ldots, \widetilde{r}_{j_u}$, which have survived Phase 2.

Experimental Results (I)

curve	R	ϵ_b	N	success rate
Curve25519	64	0.12	400	9/10
Curve25519	120	0.10	700	19/20
Curve25519	120	0.12	5,000	19/20
Curve25519	120	0.13	15,000	23/30
Curve25519	120	0.14	60,000	18/30
Curve25519	120	0.15	400,000	5/10
Curve25519	125	0.10	1000	10/10
Curve25519	125	0.12	6,000	16/20
Curve25519	125	0.13	17,000	8/10
Curve25519	125	0.14	60,000	14/30

Table: $g = 127$

Experimental Results (II)

curve	R	ϵ_b	N	success rate
M-511	250	0.07	500	10/10
M-511	250	0.10	30,000	9/10
M-511	253	0.10	40,000	8/10
ED448	220	0.10	30,000	10/10
ED448	220	0.11	120,000	9/10
ED448	220	0.12	700,000	9/10
Curve41417	200	0.07	400	10/10
Curve41417	200	0.10	7,000	8/10
NIST P-384	190	0.10	4,000	10/10
NIST P-384	190	0.12	70,000	9/10

Table: $g = 255$ (M-511), $g = 222$ (ED448), $g = 206$ (Curve41417), $g = 194$ (NIST P-384)

Efficiency and Countermeasure

- For the above parameter sets the attack essentially costs from $O(2^{29})$ to $O(2^{34})$ operations (each consisting of several inexpensive basic operations).
- Both the Wide Window Attack and the Narrow Window Attack are very efficient.
- To prevent these attacks the blinding factors must at least exceed the gap, i.e. $R \geq g \approx k/2$.

Conclusion

- Exponent blinding and scalar blinding are well-known countermeasures against implementation attacks.
- Several attacks on RSA and ECC implementations have shown that exponent blinding and scalar blinding are not as strong as it had been believed.
- The basic attack, the enhanced attack and its improvements, the alternate attacks, and the attacks on special elliptic curves can be prevented by sufficiently long (attack-indivual!) blinding factors.
- The attacks against elliptic curves over $\mathrm{GF}(p)$ for special primes p and cofactor 2^b are very efficient. It requires extremely large blinding factors to thwart these attacks. This feature at least reduces their efficiency gain over general elliptic curves.

Contact

Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn, Germany

Werner Schindler

P.O. Box 200363, 53133 Bonn, Germany
Tel.: +49 (0)228-9582-5652
Fax: +49 (0)228-10-9582-5652

Werner.Schindler@bsi.bund.de

https://www.bsi.bund.de

https://www.bsi-fuer-buerger.de

[1] S. Bauer: Attacking Exponent Blinding in RSA without CRT. COSADE 2012, Springer, LNCS 7275, 82–88.

[2] P. Fouque, S. Kunz-Jacques, G. Martinet, F. Muller, F. Valette: Power Attack on Small RSA Public Exponent. CHES 2006, Springer, LNCS 4249, 339 - 353.

[3] W. Schindler, K. Itoh: Exponent Blinding Does not Always Lift (Partial) SPA Resistance to Higher-Level Security. ACNS 2011, Springer, LNCS 6715, 73 – 90.

[4] W. Schindler, A. Wiemers: Power Attacks in the Presence of Exponent Blinding. J Cryptogr Eng 4 (2014), 213-236.
online http://dx.doi.org/10.1007/s13389-014-0081-y

- [5] W. Schindler, A. Wiemers: Generic Power Attacks on RSA with CRT and Exponent Blinding — New Results. Submitted.
- [6] W. Schindler, A. Wiemers: Efficient Side-Channel Attacks on Scalar Blinding on Elliptic Curves with Special Structure. In: Proceedings of the Workshop on Elliptic Curve Cryptography Standards, NIST, Gaithersburg, 2015.
- [7] W. Schindler: Exclusive Exponent Blinding May Not Suffice to Prevent Timing Attacks on RSA. To appear in the Proceedings of CHES 2015.
  Preversion: http://eprint.iacr.org/2014/869