Published in L. Breveglieri *et al.*, Eds, *Fault Diagnosis and Tolerance in Cryptography (FDTC 2008)*, pp. 87–91, IEEE Press, 2008.

On the Security of a Unified Countermeasure

Marc Joye

Thomson R&D France
Technology Group, Corporate Research, Security Laboratory
1 avenue de Belle Fontaine, 35576 Cesson-Sévigné Cedex, France
E-mail: marc.joye@thomson.net

Abstract

Implementation attacks are a major threat for cryptographic applications. Recently, Baek and Vasyltsov (ISPEC 2007) proposed a unified countermeasure for protecting elliptic curve implementations against a variety of implementation attacks, including differential power attacks and fault attacks.

This paper studies the security of this countermeasure. In particular, it shows that the fault coverage is less than what was anticipated. Further security weaknesses are also pointed out.

Keywords. Elliptic curve cryptography, fault attacks, differential power attacks, countermeasures.

1. Introduction

The central operation in elliptic cryptography is the point multiplication. Given a point $\boldsymbol{P}$ and a scalar $d \geq 0$, one has to compute $[d]\boldsymbol{P}$, that is, $\boldsymbol{P}+\boldsymbol{P}+\cdots+\boldsymbol{P}$ (d times). Scalar d is typically a secret value. If an attacker can recover it (or a part thereof), he will likely break the underlying cryptosystem. Modern cryptosystems feature provable security: their security can be proved in a given security model. However, existing security models suppose that an attacker gets only access to the input and the output of the cryptosystem. This does not rule out implementation attacks.

The first family of implementation attacks is that of *fault attacks*. They were introduced by Boneh et al. [7]. See also [4, 8, 6] for attacks in the context of elliptic curve cryptography. The goal of the attacker is to induce a fault in order to generate a malfunction. Next, given the faulty output, the attacker tries to infer some secret information. Excellent surveys on fault attacks can be found in [2, 12].

The second family of implementation attacks is that of *side-channel attacks*, introduced by Kocher et al. [13, 14] and applied to elliptic curve cryptography in [10]. Here the attacker monitors some side-channel information (e.g., the power consumption) in order to deduce the inner-workings of a crypto-algorithm and thereby infers some secret information. When there is a single measurement, the attack is referred to as an SPA-type attack. When there are several measurements together with statistical analysis, the attack is referred to as a DPA-type attack. We refer the reader to [15] for a complete treatment of the subject. See also [5, 9] for attacks and countermeasures dedicated to elliptic curve cryptosystems.

In [1], the authors propose a unified countermeasure aimed at protecting point multiplication against both fault attacks and DPA-type attacks. Hence, combined with an SPA-resistant point multiplication algorithm, the so-obtained implementation should resist against known implementation attacks. The countermeasure generalizes to elliptic curves a countermeasure first suggested for RSA by Shamir [17]. The idea is to embed the given elliptic curve in a random extension ring. A similar countermeasure was proposed in [6]. The main differences are (i) the extension is random, and (ii) the curve equation is extended. The aim is to cover a larger class of attacks. This also yields a number of advantages. However, as will become apparent, choosing a random extension rather than a fixed one as in [6] gives rise to several security issues.

The rest of this paper is organized as follows. In the next section, we introduce some background on elliptic curves. We define elliptic curves over a field and over a ring, and present their arithmetic. In Section 3, we review the unified countermeasure of Baek and Vasyltsov. Section 4 is the core of the paper. We give a detailed security analysis of this unified countermeasure. We also compare it with a previous fault countermeasure. Finally, we conclude in Section 5.

2. Background on Elliptic Curves

Let p be a prime ≥ 5. An elliptic curve E over the field $\mathbb{F}_p$ is given by the set of points $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$ satisfying

the Weierstraß equation

$$y^2 = x^3 + ax + b \tag{1}$$

where $\gcd(4a^3 + 27b^2, p) = 1$, together with a single element $\boldsymbol{O}_p$ called the 'point at infinity'. The set of points of the elliptic curve over $\mathbb{F}_p$ is noted $E_p(a, b)$ and forms an abelian group under the chord-and-tangent law, with identity element $\boldsymbol{O}_p$ [18]. We have:

1. For all $\boldsymbol{P} \in E_p(a, b)$, $\boldsymbol{P} + \boldsymbol{O}_p = \boldsymbol{O}_p + \boldsymbol{P} = \boldsymbol{P}$;
2. The inverse of $\boldsymbol{P} = (x_1, y_1)$ is $-\boldsymbol{P} = (x_1, -y_1)$;
3. Let $\boldsymbol{P} = (x_1, y_1)$ and $\boldsymbol{Q} = (x_2, y_2) \in E_p(a, b)$ with $\boldsymbol{Q} \neq -\boldsymbol{P}$. Then $\boldsymbol{P} + \boldsymbol{Q} = (x_3, y_3)$ where

$$x_3 = \lambda^2 - x_1 - x_2\,, \quad y_3 = \lambda(x_1 - x_3) - y_1$$

$$\text{with } \lambda = \begin{cases} \frac{3{x_1}^2 + a}{2y_1} & \text{if } x_1 = x_2\,, \\ \frac{y_1 - y_2}{x_1 - x_2} & \text{otherwise}\,. \end{cases}$$

To avoid (costly) field inversions, points are preferably represented using projective Jacobian coordinates. The curve equation then becomes

$$Y^2 = X^3 + aXZ^4 + Z^6 \ . \tag{2}$$

An affine point $\boldsymbol{P} = (x_1, y_1)$ is represented by the triplet $(X_1 : Y_1 : Z_1) = (x_1\theta^2 : y_1\theta^3 : \theta)$ for any $\theta \in \mathbb{F}_p^*$. The point at infinity is the unique point with the Z-coordinate equal to 0, $\boldsymbol{O} = (\theta^2 : \theta^3 : 0)$. Conversely, given a projective Jacobian point $\boldsymbol{P} = (X_1 : Y_1 : Z_1)$ with $Z_1 \neq 0$, its affine representation is recovered as $\boldsymbol{P} = (X_1/{Z_1}^2, Y_1/{Z_1}^3)$. Letting M, S and c respectively denote a multiplication, a squaring and a multiplication by curve parameter a (in $\mathbb{F}_p$), state-of-the-art formulæ [3] require $11\mathsf{M} + 5\mathsf{S}$ for point addition and $1\mathsf{M} + 8\mathsf{S} + 1\mathsf{c}$ for point doubling.

Elliptic curves over rings are defined similarly. The main difference is that they do no longer form an abelian group. Let n be the product of two primes $p, q \geq 5$, and let a, b be such that $\gcd(4a^3 + 27b^2, n) = 1$. An elliptic curve over the ring $\mathbb{Z}_n$ is the set of points $(x, y) \in \mathbb{Z}_n \times \mathbb{Z}_n$ satisfying Weierstraß equation (1) together with the point $\boldsymbol{O}_n$.

Consider the group $\widetilde{E}_n(a, b)$ given by the direct product

$$\widetilde{E}_n(a, b) = E_p(a, b) \times E_q(a, b) \ .$$

By Chinese remaindering, there exists a unique point $\boldsymbol{P} = (x_1, y_1) \in E_n(a, b)$ for every pair of points $\boldsymbol{P}_p = (x_{1p}, y_{1p}) \in E_p(a, b) \setminus \{\boldsymbol{O}_p\}$ and $\boldsymbol{P}_q = (x_{1q}, y_{1q}) \in E_q(a, b) \setminus \{\boldsymbol{O}_q\}$ such that $\boldsymbol{P}_p = \boldsymbol{P} \bmod p$ and $\boldsymbol{P}_q = \boldsymbol{P} \bmod q$. This equivalence is denoted by $\boldsymbol{P} = [\boldsymbol{P}_p, \boldsymbol{P}_q]$. Since $\boldsymbol{O}_n = [\boldsymbol{O}_p, \boldsymbol{O}_q]$, the group $\widetilde{E}_n(a, b)$ consists of all the points of $E_n(a, b)$ and of points of the form $[\boldsymbol{P}_p, \boldsymbol{O}_q]$ or $[\boldsymbol{O}_p, \boldsymbol{P}_q]$. It is easy to see that the chord-and-tangent addition, whenever it is defined, coincides with the group operation on $\widetilde{E}_n(a, b)$.

3. Baek-Vasyltsov Countermeasure

In this section, we review the unified countermeasure proposed by Baek and Vasyltsov. We focus on the (large) prime field case. The binary field case is treated analogously. We refer the reader to [1] for a complete description.

The countermeasure makes use of a curve equation E' of the form

$$Y^2 + pYZ^3 = X^3 + aXZ^4 + bZ^6 \tag{3}$$

defined over the ring $\mathbb{Z}_{pr}$ where p is a (large) prime and r is a positive integer. Remark that $E' \bmod p = E$, as given by Eq. (2).

Let $\boldsymbol{P} = (X_1 : Y_1 : Z_1)$ and $\boldsymbol{Q} = (X_2 : Y_2 : Z_2)$ be two points on E' with $Z_1, Z_2 \neq 0$. In [1], the authors define the operations ADD-JP and DBL-JP given by

$$\text{ADD-JP}(\boldsymbol{P}, \boldsymbol{Q}) = (X_3 : Y_3 : Z_3) \quad \text{for } \boldsymbol{P} \neq \pm\boldsymbol{Q}$$

where

$$\begin{cases} X_3 = R^2 - H^2({X_2}{Z_1}^2 + {X_1}{Z_2}^2) \\ Y_3 = R({X_1}{Z_2}^2H^2 - X_3) \\ \qquad\qquad - (Y_1 + p{Z_1}^3){Z_2}^2H^3 \\ Z_3 = Z_1Z_2H \end{cases} \tag{4}$$

with $R = Y_2{Z_1}^3 - Y_1{Z_2}^3$ and $H = X_2{Z_1}^2 - X_1{Z_2}^2$, and

$$\text{DBL-JP}(\boldsymbol{P}) = (X_3 : Y_3 : Z_3)$$

where

$$\begin{cases} X_3 = M^2 - 2X_1(F + Y_1)^2 \\ Y_3 = M\big(X_1(F + Y_1)^2 - X_3\big) - F(F + Y_1)^3 \\ Z_3 = Z_1(Y_1 + F) \end{cases} \tag{5}$$

with $M = 3{X_1}^2 + a{Z_1}^4$ and $F = Y_1 + p{Z_1}^3$. The respective costs are $15\mathsf{M} + 4\mathsf{S}$ and $7\mathsf{M} + 5\mathsf{S} + 1\mathsf{c}$ over $\mathbb{Z}_{pr}$. This has to be compared with the usual elliptic curve addition law, $11\mathsf{M} + 5\mathsf{S}$ and $1\mathsf{M} + 8\mathsf{S} + 1\mathsf{c}$ over $\mathbb{F}_p$ (cf. Section 2).

We can now describe the countermeasure. Suppose we have to compute $[d]\boldsymbol{P}$ with $\boldsymbol{P} = (x_1 : y_1 : 1)$ on an elliptic curve E defined over $\mathbb{F}_p$. The secure implementation proposed in [1] proceeds as follows:

1. Choose a small random integer r.
2. Compute $B = {y_1}^2 + py_1 - {x_1}^3 - ax_1 \bmod (pr)$ and let $E'_{/\mathbb{Z}_{pr}} : Y^2 + pYZ^3 = X^3 + aXZ^4 + BZ^6$.
3. Compute $(X_d : Y_d : Z_d) = [d](x_1 : y_1 : 1)$ on E' using an SPA-resistant point multiplication algorithm.

4. Check whether

$$Y_d{}^2 + pY_dZ_d{}^3 \stackrel{?}{\equiv} X_d{}^3 + aX_dZ_d{}^4 + BZ_d{}^6 \pmod{r}$$

and, if not, return $\boldsymbol{O}$ and stop.

5. Return $(X_d : Y_d : Z_d) \bmod p$.

4. Analysis

The point at infinity $\boldsymbol{O}_{pr}$ on extended curve equation (3) for E' is $\boldsymbol{O}_{pr} = (\theta^2 : \theta^3 : 0)$ for any $\theta \in \mathbb{Z}_{pr}^*$. If we evaluate DBL-JP$(\boldsymbol{O}_{pr})$, we get from Eq. (5) $M = 3\theta^4$, $F = \theta^3$ and hence $X_3 = \theta^8$, $Y_3 = \theta^{12}$ and $Z_3 = 0$. Since $(\theta^8 : \theta^{12} : 0) = (\vartheta^2 : \vartheta^3 : 0)$ with $\vartheta = \theta^4$, this implies that the doubling formula remains valid for the point at infinity:

$$\text{DBL-JP}(\boldsymbol{O}_{pr}) = \boldsymbol{O}_{pr} \ . \tag{6}$$

Since $\boldsymbol{O}_{pr} \bmod p = \boldsymbol{O}_p$, this also holds on E.

If we inspect what happens with the addition formula on E' with the point at infinity, ADD-JP$(\boldsymbol{P}, \boldsymbol{O}_{pr})$ for a point $\boldsymbol{P} = (X_1 : Y_1 : Z_1)$, we get from Eq. (4), $R = \theta^3 {Z_1}^3$ and $H = \theta^2 {Z_1}^2$. This yields $X_3 = \theta^6 {Z_1}^6 - \theta^6 {Z_1}^6 = 0$, $Y_3 = \theta^3 {Z_1}^3(-X_3) = 0$ and $Z_3 = 0$. Likewise, if we evaluate ADD-JP$(\boldsymbol{O}_{pr}, \boldsymbol{P})$, we obtain $X_3 = 0$, $Y_3 = 0$ and $Z_3 = 0$. The addition formula is thus not valid for the point at infinity:

$$\left.\begin{array}{l}\text{ADD-JP}(\boldsymbol{P}, \boldsymbol{O}_{pr}) \\ \text{ADD-JP}(\boldsymbol{O}_{pr}, \boldsymbol{P})\end{array}\right\} \begin{array}{l} = (0:0:0) \\ \neq \boldsymbol{P}, \ \forall \boldsymbol{P} \in E' \ .\end{array} \tag{7}$$

Again, noting that $(0:0:0) \bmod p = (0:0:0)$, this also holds for E.

4.1. Security

The previous observations can be generalized. For any prime factor q dividing r, if we let $\boldsymbol{O}_q = \boldsymbol{O}_{pr} \bmod q$ then DBL-JP$(\boldsymbol{O}_{pr}) \bmod q = \boldsymbol{O}_q$ and ADD-JP$(\boldsymbol{P}, \boldsymbol{O}_{pr}) \bmod q = \text{ADD-JP}(\boldsymbol{O}_{pr}, \boldsymbol{P}) \bmod q = (0:0:0)$. More generally:

Proposition 1 *Using the previous notations, for any $\boldsymbol{P}$ and $\boldsymbol{S}$ satisfying Eq.* (3) *such that the Z-coordinate of $\boldsymbol{S} \bmod q$ is zero, we have:*

$$\text{DBL-JP}(\boldsymbol{S}) \equiv \boldsymbol{S} \pmod{q}$$

and

$$\left.\begin{array}{l}\text{ADD-JP}(\boldsymbol{P}, \boldsymbol{S}) \\ \text{ADD-JP}(\boldsymbol{S}, \boldsymbol{P})\end{array}\right\} \equiv (0:0:0) \pmod{q} \ .$$

Proof. The Z-coordinate of $\boldsymbol{S} \bmod q$ being zero implies that either $\boldsymbol{S} \bmod q = (0:0:0)$ or $\boldsymbol{S} \bmod q = \boldsymbol{O}_q$. If $\boldsymbol{S} \bmod q = (0:0:0)$, it is easy to see that the proposition holds by inspecting Eqs (4) and (5). If $\boldsymbol{S} \bmod q = \boldsymbol{O}_q$, the proposition is a straightforward application of the Chinese Remainder Theorem. □

Although not a valid projective point, triplet $(0:0:0)$ satisfies Eq. (3). This explains the correctness of Baek-Vasyltsov countermeasure: Step 4 of the countermeasure (cf. Section 3) will always be satisfied — when there is no fault.

Let us analyze the reverse direction. Suppose that a fault occurred during the computation of $(X_d : Y_d : Z_d) = [d]\boldsymbol{P}$. The expected probability that faulty point $(X_d : Y_d : Z_d)$ passes verification step

$$Y_d{}^2 + pY_dZ_d{}^3 \stackrel{?}{\equiv} X_d{}^3 + aX_dZ_d{}^4 + BZ_d{}^6 \pmod{r} \tag{8}$$

is about, *at best*, of $2^{-|r|_2}$ where $|r|_2$ denotes the bit-length of random integer r. Unfortunately, the proposed countermeasure is not perfect. The above verification step (Eq. (8)) checks that triple $(X_d : Y_d : Z_d)$ belongs to elliptic curve E' over the ring $\mathbb{Z}_r$, or, as shown earlier, that it is $(0:0:0)$. If q denotes the largest factor of r such that $(X_d : Y_d : Z_d) \equiv (0:0:0) \pmod{q}$ then a random fault will go through the verification with a probability of about $2^{-|r/q|_2} \approx 2^{-|r|_2+|q|_2}$. Hence, we deduce that the "effective" bit-length of r is roughly $(|r|_2 - |q|_2)$.

We carried out experiments to estimate the average value of $|q|_2$ with the collection of elliptic curves recommended by NIST for U.S. federal government use [11, Appendix 6]. The next table gives the average effective bit-length of random integer r.

$\lvert r\rvert_2$	P-192	P-224	P-256	P-384	P-521
20	10.7	10.3	10.1	9.6	9.2
32	22.7	22.3	22.1	21.6	21.2
40	30.7	30.3	30.1	29.6	29.2

Table 1. Effective randomization bit-length

NIST-recommended curves are denoted P-xxx and define elliptic curves over fields $\mathbb{F}_p$ where p is an xxx-bit prime. We see that for recommended cryptographic sizes (192 bits to 521 bits) the loss in effectiveness is approximatively of 10 bits. We also see that larger field sizes imply slightly larger loss in effectiveness. This follows from the fact that $(X_d : Y_d : Z_d) = [d]\boldsymbol{P}$ with $d \in [1, \#E[$ and $p + 1 - 2\sqrt{p} \leq \#E \leq p + 1 + 2\sqrt{p}$. Finally, Table 1 confirms that the loss in effectiveness is independent of the bit-length of r. The conclusion is that roughly 10 more bits for random integer r are needed.

It is also important to study the probability that $q = r$, that is, that $(X_d : Y_d : Z_d) \equiv (0 : 0 : 0) \pmod{r}$. When this occurs, a fault will not be detected by the proposed countermeasure. Table 2 presents the probability that $q = r$ or, equivalently, the average proportion of undetected faults.

$\lvert r \rvert_2$	P-192	P-224	P-256	P-384	P-521
20	23.2%	27.3%	28.9%	33.8%	37.3%
32	2.4%	3.1%	3.6%	5.0%	6.2%
40	0.4%	0.6%	0.7%	1.0%	1.4%

Table 2. Proportion of undetected faults

Quite surprisingly, we observe that for 20-bit random integers r, the average proportion of undetected faults ranges from 23.2% to 37.3% (!). For 32- or 40-bit random integers r, the proportion of undetected faults is smaller but still remains non-negligible. Of course, the use of larger values for r yields better results (i.e., protection) but also significantly impacts the overall performance.

Remark. The previous analysis focuses on elliptic curves defined over prime fields. In [1], the authors adapt their countermeasure to elliptic curves over binary fields. A similar analysis applies to this setting as well.

4.2. Comparison

In [6], building on Shamir's countermeasure, Blömer et al. devised another strategy to prevent fault attacks. Rather than forming the combined curve on-the-fly over a random extension ring, they suggest to pre-compute and store a *fixed prime-order elliptic curve* $E_r(a_r, b_r)$ over prime field $\mathbb{F}_r$ along with a point $\boldsymbol{P}_r$ on E_r. The evaluation of $\boldsymbol{Q} = [d]\boldsymbol{P}$ on $E_p(a, b)$ then goes as $\boldsymbol{Q'} = [d]\boldsymbol{P'}$ on E' and next, if $\boldsymbol{Q'} \equiv [d \bmod \#E_r]\boldsymbol{P'} \pmod{r}$, $\boldsymbol{Q} = \boldsymbol{Q'} \bmod p$ where

$$E'_{/\mathbb{Z}_{pr}} : Y^2 = X^3 + \mathrm{CRT}(a, a_r)X\,Z^4 + \mathrm{CRT}(b, b_r)\,Z^6$$

and

$$\boldsymbol{P'} = \mathrm{CRT}(\boldsymbol{P}, \boldsymbol{P}_r) \ .$$

Compared to the countermeasure of Baek and Vasyltsov, the order of point $\boldsymbol{P}_r = \boldsymbol{P'} \bmod r$ is always the largest possible prime, namely $\#E_r$. As a consequence, the success probability of the aforementioned attacks is minimal.

4.3. Further results

Since the last intermediate values may no longer be randomized (i.e., as soon as $(X_d : Y_d : Z_d) \equiv (0 : 0 : 0) \pmod{r}$), the bits of k appearing at the end of the algorithm can be recovered through a DPA-type attack [10] on the output of the algorithm by reversing the computations. This can be combined with the attack of [16]. To prevent such attacks, the proposed countermeasure should be modified by returning the result point in affine coordinates, $(X_d/{Z_d}^2, Y_d/{Z_d}^3)$ or, alternatively, by returning a random projective representation thereof, $(X_d\,\theta^2 : Y_d\,\theta^3 : \theta)$ for some non-zero $\theta \in \mathbb{F}_p$.

5. Conclusion

In this paper, we analyzed the security of a unified countermeasure recently proposed by Baek and Vasyltsov. In particular, we pointed out that the overhead incurred by the countermeasure is larger than what could be thought at first sight: *on average*, 10 additional bits are required for the randomizer in cryptographic applications. Moreover, and somewhat more surprisingly, we observed that a *non-negligible proportion* of faults is undetected if the randomizer is an integer in the range $2^{20} \sim 2^{40}$. We conducted extensive experiments on NIST-recommended curves to support our investigations.

As a conclusion, our results show that the countermeasure of Baek and Vasyltsov should be used with care. They also underline the necessity of using larger randomizers, at the cost of performance losses.

References

[1] Y.-J. Baek and I. Vasyltsov. How to prevent DPA and fault attacks in a unified way for ECC scalar multiplication: Ring extension method. In E. Dawson and D. Wong, editors, *Information Security Practice and Experience − ISPEC 2007*, volume 4464 of *Lecture Notes in Computer Science*, pages 225–237. Springer-Verlag, 2007.

[2] H. Bar-El, H. Choukri, D. Naccache, M. Tunstall, and C. Whelan. The sorcerer's apprentice guide to fault attacks. *Proceedings the IEEE*, 94(2):370–382, 2006. Earlier version in Proc. of FDTC 2004.

[3] D. J. Bernstein and T. Lange. Explicit-formulas database. `http://www.hyperelliptic.org/EFD/jacobian.html`.

[4] I. Biehl, B. Meyer, and V. Müller. Differential fault analysis of elliptic curve cryptosystems. In M. Bellare, editor, *Advances in Cryptology − CRYPTO 2000*, volume 1880 of *Lecture Notes in Computer Science*, pages 131–146. Springer-Verlag, 2000.

[5] I. F. Blake, G. Seroussi, and N. P. Smart, editors. *Advances in Elliptic Curve Cryptography*, volume 317 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, 2005.

[6] J. Blömer, M. Otto, and J.-P. Seifert. Sign change fault attacks on elliptic curve cryptosystems. In L. Breveglieri, I. Koren, D. Naccache, and J.-P. Seifert, editors, *Fault Diagnosis and Tolerance in Cryptography − FDTC 2006*, volume 4236 of *Lecture Notes in Computer Science*, pages 36–52. Springer-Verlag, 2006.

[7] D. Boneh, R. A. DeMillo, and R. J. Lipton. On the importance of eliminating errors in cryptographic computations. *Journal of Cryptology*, 14(2):110–119, 2001. Extended abstract in Proc. of EUROCRYPT '97.

[8] M. Ciet and M. Joye. Elliptic curve cryptosystems in the presence of permanent and transient faults. *Designs, Codes and Cryptography*, 36(1):33–43, 2005.

[9] H. Cohen and G. Frey, editors. *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, volume 34 of *Discrete Mathematics and Its Applications*. Chapman & Hall/CRC, 2005.

[10] J.-S. Coron. Resistance against differential power analysis for elliptic curve cryptosystems. In Ç. K. Koç and C. Paar, editors, *Cryptographic Hardware and Embedded Systems (CHES '99)*, volume 1717 of *Lecture Notes in Computer Science*, pages 292–302. Springer-Verlag, 1999.

[11] FIPS PUB 186-2. Digital signature standard. Federal Information Processing Standard Publication 186-2, National Institute of Standards and Technology, Jan. 2000.

[12] C. Giraud and H. Thiebeauld. A survey on fault attacks. In J.-J. Quisquater, P. Paradinas, Y. Deswarte, and A. A. El Kalam, editors, *Smart Card Research and Advanced Applications VI (CARDIS 2004)*, pages 159–176. Kluwer, 2004.

[13] P. Kocher. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In N. Koblitz, editor, *Advances in Cryptology − CRYPTO '96*, volume 1109 of *Lecture Notes in Computer Science*, pages 104–113. Springer-Verlag, 1996.

[14] P. Kocher, J. Jaffe, and B. Jun. Differential power analysis. In M. Wiener, editor, *Advances in Cryptology − CRYPTO '99*, volume 1666 of *Lecture Notes in Computer Science*, pages 388–397. Springer-Verlag, 1999.

[15] S. Mangard, E. Oswald, and T. Popp. *Power Analysis Attacks: Revealing the Secrets of Smart Cards*. Springer, 2007.

[16] D. Naccache, N. P. Smart, and J. Stern. Projective coordinates leak. In C. Cachin and J. Camenisch, editors, *Advances in Cryptology − EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 257–267. Springer-Verlag, 2004.

[17] A. Shamir. How to check modular exponentiation. Presented at the rump session of EUROCRYPT '97, Konstanz, Germany, May 13, 1997.

[18] J. H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, 1986.