# Side-Channel Attacks in ECC: A General Technique for Varying the Parametrization of the Elliptic Curve

Loren D. Olson

Dept. of Mathematics and Statistics
University of Tromsø
N-9037 Tromsø, Norway

**Abstract.** Side-channel attacks in elliptic curve cryptography occur with the unintentional leakage of information during processing. A critical operation is that of computing $nP$ where $n$ is a positive integer and $P$ is a point on the elliptic curve $E$. Implementations of the binary algorithm may reveal whether $P+Q$ is computed for $P \neq Q$ or $P = Q$ as the case may be. Several methods of dealing with this problem have been suggested. Here we describe a general technique for producing a large number of different representations of the points on $E$ in characteristic $p \geq 5$, all having a uniform implementation of $P + Q$. The parametrization may be changed for each computation of $nP$ at essentially no cost. It is applicable to all elliptic curves in characteristic $p \geq 5$, and thus may be used with all curves included in present and future standards for $p \geq 5$.

**Keywords:** Elliptic curves, ECC, cryptography, side-channel attacks, weighted projective curves, uniform addition formula.

## 1 Introduction

Side-channel attacks in elliptic curve cryptography (ECC) have received considerable attention. They take advantage of information unintentionally leaked from a supposedly tamper-resistant device. Such information is often obtained via measurements of power consumption or timing. In ECC, a fundamental operation is the computation of $nP$ where $n$ is an integer and $P$ is a point on the elliptic curve $E$ at hand. A naive implementation of the binary algorithm for this computation may reveal whether $P + Q$ is computed for $P \neq Q$ or $P = Q$ (doubling). One method of defense against this attack is to find a parametrization of the points on the elliptic curve $E$ such that the implementation of the group law does not reveal any information in this regard. Several authors have suggested specific parametrizations, notably Liardet and Smart ([1]) with the intersection of two quadric surfaces, Joye and Quisquater ([2]) with a Hessian model, and Billet and Joye ([3]) with the Jacobi quartic. The latter provided a great deal of the motivation for the present work.

We discuss a general technique for producing a large number of different representations of the points on an elliptic curve and its group law all having a uniform computation of $P+Q$. This gives rise to a corresponding variation in the implementation of ECC to avoid certain side-channel attacks. Concretely, given an elliptic curve $E$ with identity element $e$ and any point $M \neq e$ on it, we may attach to the pair $(E, M)$ a weighted projective quartic curve $C_M$ which is isomorphic to $E$. On this curve $C_M$, we will be able to compute $P+Q$ in a uniform fashion. The point $M$ and thus the curve $C_M$ may be changed at virtually no cost, so that a new parametrization may be chosen for each computation of $nP$.

## 2 The General Technique

In this section we present the mathematics of our technique. Let $k$ be a field of characteristic different from 2 and 3. Consider an elliptic curve $E \subseteq \mathbb{P}^2$ defined by the homogeneous equation

$$Y^2Z = X^3 + a_4XZ^2 + a_6Z^3 \tag{1}$$

with identity element $e = (0, 1, 0)$. Let $M \neq e$ be a $k$-rational point on $E$ with coordinates $M = (\alpha, \beta, 1)$. Define constants $c_i \in k$ as follows

$$\begin{aligned} c_2 &= -(3\alpha/2) \\ c_3 &= -\beta \\ c_4 &= -(4a_4 + 3\alpha^2)/16 \end{aligned} \tag{2}$$

Let $D_M$ be the affine quartic curve defined by

$$\begin{aligned} W^2 = R(S) &= S^4 + c_2S^2 + c_3S + c_4 \\ &= S^4 - (3\alpha/2)S^2 - \beta S - (4a_4 + 3\alpha^2)/16 \end{aligned} \tag{3}$$

This will be the affine part of the curve we wish to associate to the elliptic curve $E$ and the point $M \neq e$.

Conversely, consider a quartic plane curve given by the affine equation

$$W^2 = R(S) = S^4 + c_2S^2 + c_3S + c_4 \tag{4}$$

with $c_i \in k$ such that $R(S)$ has no multiple roots. Define

$$\begin{aligned} a_4 &= -[(c_2^2/3) + 4c_4] \\ a_6 &= [2(c_2/3)^3 - 8(c_2c_4/3) + c_3^2] \\ \alpha &= -2c_2/3 \\ \beta &= -c_3 \end{aligned} \tag{5}$$

Then the equation

$$Y^2Z = X^3 + a_4XZ^2 + a_6Z^3 \tag{6}$$

defines an elliptic curve $E$ together with a point $M \neq e$ on $E$ with coordinates $M = (\alpha, \beta, 1)$. There is an isomorphism between $E - \{M, e\}$ and $D_M$ given by

$$\begin{aligned} S &= (Y + \beta)/2(X - \alpha) \\ W &= (X/2) + (\alpha/4) - (Y + \beta)^2/4(X - \alpha)^2 \\ X &= 2W + 2S^2 - (\alpha/2) \\ Y &= 4SW + 4S^3 - 3\alpha S - \beta \end{aligned} \tag{7}$$

These formulas are classical and may be found, for example, in Fricke ([5]); here they are slightly modified to conform with the standard notation for the Weierstrass equation.

If we homogenize equation (4) by introducing a variable $T$ to obtain

$$W^2T^2 = S^4 + c_2S^2T^2 + c_3ST^3 + c_4T^4 \tag{8}$$

this equation will define a projective quartic curve in $\mathbb{P}^2$. This curve has a singular point at infinity and is not very convenient for our purposes. However, a slight variant of this will prove highly useful, as we shall now see.

A very helpful and unifying concept in studying elliptic curves, parametrizations with quartic curves, and various choices of coordinates is that of weighted projective spaces. A good reference for an introduction to the subject is Reid ([4]).

**Definition 1.** *Let $n \geq 1$ and $d_0, \ldots, d_n \geq 1$ be positive integers.* Weighted projective space $\mathbb{P} = \mathbb{P}(d_0, \ldots, d_n)$ *consists of all equivalence classes of $n+1$-tuples $(x_0, \ldots, x_n)$ where not all $x_i$ are zero and $(x_0, \ldots, x_n) \sim (\lambda^{d_0}x_0, \ldots, \lambda^{d_n}x_n)$ for $\lambda \in k^*$. We refer to $(d_0, \ldots, d_n)$ as the* weight system.

This concept then encompasses the standard definition of projective space $\mathbb{P}^n$ with all $d_i = 1$ and provides a natural context for Jacobian coordinates, Chudnovsky coordinates, López-Dahab coordinates, etc. We may speak of weighted homogeneous polynomials and weighted projective varieties.

*Remark 1.* Throughout the remainder of this article *weighted* will refer to the weight system $(1, 1, 2)$ and $\mathbb{P} = \mathbb{P}(1, 1, 2)$. We denote the coordinate system in $\mathbb{P}$ by $(S, T, W)$.

Returning to the material at hand, the weighted homogeneous equation

$$W^2 = S^4 + c_2S^2T^2 + c_3ST^3 + c_4T^4 \tag{9}$$

now defines a weighted quartic projective curve $C_M$ in $\mathbb{P} = \mathbb{P}(1, 1, 2)$. The affine part where $T \neq 0$ is just $D_M$. $C_M$ contains the two points $(1, 0, 1)$ and $(1, 0, -1)$ in addition. $C_M$ is non-singular and is an elliptic curve with $(1, 0, 1)$ as identity element. $E$ is isomorphic to $C_M$ where the isomorphism on $D_M$ is described previously and $e \leftrightarrow (1, 0, 1)$ and $M \leftrightarrow (1, 0, -1)$. We also note the following: If $\beta \neq 0$, then $-M = (\alpha, -\beta) \leftrightarrow (-(3\alpha^2 + 4)/4\beta, 1, (3\alpha/4) - ((3\alpha^2 + 4)/4\beta)^2))$.

## 3 The Group Law on $C_M$

We shall now make explicit the group law on $C_M$, and show that the addition of two points on $C_M$ may be given by formulas independent of whether the two points are equal or not. Let $\phi : E \to C_M$ be the isomorphism given above. We shall compute using coordinates in the two weighted projective spaces $\mathbb{P}^2 = \mathbb{P}(1,1,1)$ and $\mathbb{P}(1,1,2)$, which are the respective ambient spaces for $E$ and $C_M$. First, let $Q = (s, 1, w)$ be a $k$-rational point with $Q \in C_M - \{(1,0,1), \pm(1,0,-1)\}$ and let $-Q = (\bar{s}, 1, \bar{w})$. Then $\bar{s} = -s - (c_3/(2w + s^2 + c_2))$ and $\bar{w} = w + s^2 - \bar{s}^2$. Let $P_i = (x_i, y_i, 1)$ be k-rational points on $E - \{M, e\}$ corresponding to points $Q_i = (s_i, 1, w_i)$ on $D_M - \{(1,0,1), (1,0,-1)\}$ via $\phi$, i.e. $\phi(P_i) = Q_i$. Assume $P_1 \neq -P_2$ and that $P_1 + P_2 = P_3$, so that $Q_1 + Q_2 = Q_3$. We wish to compute the coordinates of $Q_3$ in terms of the coordinates of $Q_1$ and $Q_2$. We will utilize $\phi$ as well as the classical formulas for computing $P_3$ to achieve this. They are given by

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2 \\ y_3 &= \lambda(x_1 - x_3) - y_1 \\ &= \lambda(x_2 - x_3) - y_2 \\ 2y_3 &= \lambda(x_1 + x_2 - 2x_3) - (y_1 + y_2) \end{aligned} \tag{10}$$

where

$$\lambda = \begin{cases} (y_2 - y_1)/(x_2 - x_1) & \text{for } P_1 \neq P_2 \\ (3x_1^2 + a_4)/2y_1 & \text{for } P_1 = P_2 \end{cases}$$

Brier and Joye ([6]) have previously consolidated these two formulas into one single formula for $\lambda$, thus providing a uniform implementation of the computation of $P + Q$ for elliptic curves in Weierstrass form. We briefly recall their computation in the case of $char(k) \geq 5$ as follows:

$$\begin{aligned} y_2^2 &= x_2^3 + a_4 x_2 + a_6 \\ y_1^2 &= x_1^3 + a_4 x_1 + a_6 \\ y_2^2 - y_1^2 &= (x_2^3 - x_1^3) + a_4(x_2 - x_1) \end{aligned}$$

Thus for $P_1 \neq P_2$,

$$\begin{aligned} (y_2 + y_1)\lambda &= (y_2^2 - y_1^2)/(x_2 - x_1) \\ &= (x_2^2 + x_1 x_2 + x_1^2) + a_4 \end{aligned}$$

and

$$\lambda = [(x_2^2 + x_1 x_2 + x_1^2) + a_4]/(y_2 + y_1) \tag{11}$$

On the other hand, if $P_1 = P_2$, then this formula for $\lambda$ reduces to $\lambda = (3x_1^2 + a_4)/2y$ which is precisely the formula given above in the original definition of $\lambda$.

In our case, we are interested in computing $Q_3$ in terms of the coordinates of $Q_1$ and $Q_2$. We begin by computing the quantity $\tau = (w_2 - w_1)/(s_2 - s_1)$. In a fashion similar to the above, we have

$$
\begin{aligned}
w_2^2 &= s_2^4 + c_2 s_2^2 + c_3 s_2 + c_4 \\
w_1^2 &= s_1^4 + c_2 s_1^2 + c_3 s_1 + c_4 \\
w_2^2 - w_1^2 &= (s_2^4 - s_1^4) + c_2(s_2^2 - s_1^2) + c_3(s_2 - s_1) \\
(w_2^2 - w_1^2)/(s_2 - s_1) &= (s_2^2 + s_1^2 + c_2)(s_2 + s_1) + c_3 \\
(w_2 + w_1)\tau &= (s_2^2 + s_1^2 + c_2)(s_2 + s_1) + c_3
\end{aligned}
$$

Finally, this yields

$$
\tau = [(s_2^2 + s_1^2 + c_2)(s_2 + s_1) + c_3]/(w_2 + w_1) \tag{12}
$$

We now compute $\lambda$ in terms of the coordinates of $Q_1$ and $Q_2$ as follows:

$$
\begin{aligned}
\lambda &= \frac{y_2 - y_1}{x_2 - x_1} \\
&= \frac{[4s_2w_2 + 4s_2^3 - 3\alpha s_2 - \beta] - [4s_1w_1 + 4s_1^3 - 3\alpha s_1 - \beta]}{[2w_2 + 2s_2^2 - (\alpha/2)] - [2w_1 + 2s_1^2 - (\alpha/2)]} \\
&= \frac{[4s_2w_2 - 4s_1w_1] + [(4s_2^3 - 4s_1^3) - 3\alpha(s_2 - s_1)]}{2(w_2 - w_1) + 2(s_2^2 - s_1^2)]} \\
&= \frac{[4s_2w_2 - 4s_1w_2 + 4s_1w_2 - 4s_1w_1] + [(4s_2^3 - 4s_1^3) - 3\alpha(s_2 - s_1)]}{2(w_2 - w_1) + 2(s_2^2 - s_1^2)]} \\
&= \frac{4w_2(s_2 - s_1) + 4s_1(w_2 - w_1) + 4(s_2^2 + s_1s_2 + s_1^2)(s_2 - s_1) - 3\alpha(s_2 - s_1)}{2(w_2 - w_1) + 2(s_2 + s_1)(s_2 - s_1)]} \\
&= \frac{4w_2 + 4s_1\tau + 4(s_2^2 + s_1s_2 + s_1^2) - 3\alpha}{2\tau + 2(s_2 + s_1)} \\
&= \frac{4w_2 + 4s_1\tau + 4(s_2^2 + s_1s_2 + s_1^2) + 2c_2}{2\tau + 2(s_2 + s_1)} \\
&= \frac{2w_2 + 2s_1\tau + 2(s_2^2 + s_1s_2 + s_1^2) + c_2}{\tau + (s_2 + s_1)}
\end{aligned} \tag{13}
$$

By the symmetry of $Q_1$ and $Q_2$, we obtain

$$
\lambda = \frac{(w_1 + w_2) + (s_1 + s_2)\tau + 2(s_2^2 + s_1s_2 + s_1^2) + c_2}{\tau + (s_2 + s_1)} \tag{14}
$$

If we now assume that $Q_1 = Q_2$ (i.e. $P_1 = P_2$) and evaluate the above expressions for $\tau$ and $\lambda$, we obtain

$$\begin{aligned}\tau &= \frac{(2s_1^2 + c_2)(2s_1) + c_3}{2w_1} \\ &= \frac{(2s_1^2 - (3\alpha/2))(2s_1) - \beta}{2w_1} \\ &= \frac{4s_1^3 - 3\alpha s_1 - \beta}{2w_1}\end{aligned} \tag{15}$$

Furthermore,

$$\begin{aligned}\lambda &= \frac{(4w_1 + 12s_1^2 - 3\alpha) + 4s_1\tau}{4s_1 + 2\tau} \\ &= \frac{(8w_1^2 + 24s_1^2 w_1 - 6\alpha w_1) + 4s_1(2w_1\tau)}{2(4s_1w_1 + 2w_1\tau)} \\ &= \frac{(8w_1^2 + 24s_1^2 w_1 - 6\alpha w_1) + 4s_1(4s_1^3 - 3\alpha s_1 - \beta)}{2(4s_1w_1 + 4s_1^3 - 3\alpha s_1 - \beta)} \\ &= \frac{8w_1^2 + 24s_1^2 w_1 - 6\alpha w_1 + 16s_1^4 - 12\alpha s_1^2 - 4\beta s_1}{2y_1} \\ &= \frac{12w_1^2 + 24s_1^2 w_1 + 12s_1^4 - 6\alpha w_1 - 6\alpha s_1^2 + (3\alpha^2/4) + a_4}{2y_1} \\ &= \frac{3[2w_1 + 2s_1^2 - (\alpha/2)]^2 + a_4}{2y_1} \\ &= \frac{3x_1^2 + a_4}{2y_1}\end{aligned} \tag{16}$$

This is exactly the original formula for $\lambda$ in the case $Q_1 = Q_2$ (i.e. $P_1 = P_2$). Hence (14) gives us a single uniform formula for $\lambda$ in terms of $Q_1$ and $Q_2$ analogous to Brier and Joye ([6]) in the Weierstrass case. We shall use formula (14) in the calculation of the coordinates of $Q_3 = Q_1 + Q_2$.

Let $Q_i = (S_i, T_i, W_i) = (s_i, 1, w_i)$, so that $s_i = S_i/T_i$ and $w_i = W_i/T_i^2$. We have $Q_3 = (s_3, 1, w_3) = ((y_3+\beta)/2(x_3-\alpha), 1, (x_3/2) + (\alpha/4) - (y_3+\beta)^2/4(x_3-\alpha)^2) = ((y_3+\beta), 2(x_3-\alpha), (2x_3+\alpha)(x_3-\alpha)^2 - (y_3+\beta)^2)$. Let

$$\begin{aligned}G &= w_1 + w_2 + s_1^2 + s_2^2 \\ H &= 2s_1w_1 + 2s_1^3 + 2s_2w_2 + 2s_2^3 + c_2(s_1+s_2) + 2c_3\end{aligned} \tag{17}$$

Then $x_1 + x_2 + \alpha = 2G$ and we have

$$\begin{aligned}2(y_3+\beta) &= \lambda(x_1 + x_2 - 2x_3) - (y_1 + y_2) - 2c_3 \qquad (18) \\ &= \lambda(-2\lambda^2 + 6G + 2c_2) - [4s_1w_1 + 4s_1^3 + 4s_2w_2 + 4s_2^3 + 2c_2(s_1+s_2) + 4c_3] \\ &= \lambda(-2\lambda^2 + 6G + 2c_2) - 2H\end{aligned}$$

Thus

$$\begin{aligned}
\lambda &= \frac{(w_1+w_2)(G+c_2)}{(s_1+s_2)(G+c_2)+c_3} + (s_1+s_2) \\
x_3 - \alpha &= \lambda^2 - 2G \\
2x_3 + \alpha &= 2(\lambda^2 - 2G - c_2) \\
y_3 + \beta &= \lambda(-\lambda^2 + 3G + c_2) - H
\end{aligned} \tag{19}$$

Putting all this together, we can now state the group law on the weighted quartic $C_M$ formally.

**Proposition 1.** *Let $C_M$ be the elliptic curve given by the weighted quartic curve $W^2 = S^4 + c_2S^2T^2 + c_3ST^3 + c_4T^4$ in $\mathbb{P}(1,1,2)$. Let $Q_1 = (s_1, 1, t_1)$ and $Q_2 = (s_2, 1, t_2)$ be k-rational points in $C_M - \{(1,0,1),(1,0,-1)\}$ such that $Q_1 \neq -Q_2, -Q_2 + (1,0,-1)$. Let $Q_1 + Q_2 = Q_3$. Then $Q_3 = (\lambda(-\lambda^2 + 3G + c_2) - H, 2(\lambda^2 - 2G), 2(\lambda^2 - 2G - c_2)(\lambda^2 - 2G)^2 - (\lambda(-\lambda^2 + 3G + c_2) - H)^2)$.*

We note that the proposition accomplishes two objectives:
a.) it gives a uniform description of the group law on the weighted quartic $C_M$, i.e. the addition formula is independent of whether $Q_1 = Q_2$ or not.
b.) the group law is given entirely in terms of the coefficients of the equation for $C_M$ and the coordinates of the $Q_i$'s, making no explicit reference to the curve $E$ and the point $M$ which we had as our starting point. While this is not used in the sequel, it may prove to be of some independent interest.

To make the group law more accessible and to evaluate its usefulness, we provide an algorithm for its computation in the next section.

## 4 An Algorithm for the Group Law

We will now give an explicit algorithm for the computation of $Q_3$ in terms of weighted projective coordinates and count the number of multiplications involved. We define quantities $e_i$ and $N_j$ for $i, j = 1, 2, \ldots$ in terms of the $c_i$'s, $S_i$'s, $T_i$'s, and $W_i$'s. The operations used to obtain the $e_i$ will consist of addition/subtraction and multiplication by integer constants $\leq 4$. The operation involved in the computation of the $N_j$ will be a single multiplication. This will enable us to keep track of the number of multiplications involved in a convenient fashion. Define

$$
\begin{aligned}
N_1 &= T_1^2 & N_2 &= T_2^2 \\
N_3 &= T_1T_2 & N_4 &= S_1T_2 \\
N_5 &= S_2T_1 & N_6 &= W_1N_2 \\
N_7 &= W_2N_1 & N_8 &= N_3^2 \\
N_9 &= N_3N_8 & N_{10} &= N_4^2 \\
N_{11} &= N_5^2 & N_{12} &= c_2N_8 \\
N_{13} &= c_3N_9 & e_1 &= N_4 + N_5 \\
e_2 &= N_6 + N_7 & e_3 &= e_2 + N_{10} + N_{11} + N_{12} \\
e_4 &= e_3 + N_{13} & N_{14} &= e_1e_3 + N_{13} \\
e_5 &= N_{13} + N_{14} & N_{15} &= e_2e_3 \\
N_{16} &= e_1N_{14} & e_6 &= N_{15} + N_{16} \\
e_7 &= N_6 + N_{10} & e_8 &= N_7 + N_{11} \\
N_{17} &= N_4e_7 & N_{18} &= N_5e_8 \\
N_{19} &= N_{12}e_1 & e_9 &= 2N_{17} + 2N_{18} + N_{19} + 2N_{13} \\
e_{10} &= N_6 + N_7 + N_{10} + N_{11} & N_{20} &= e_6^2 \\
N_{21} &= N_{14}^2 & N_{22} &= e_{10}N_{21} \\
N_{23} &= N_{12}N_{21} & e_{11} &= -N_{20} + 3N_{22} + N_{23} \\
N_{24} &= e_6e_{11} & e_{12} &= N_{20} - 2N_{22} \\
N_{25} &= N_3e_{12} & N_{26} &= N_{25}^2 \\
e_{13} &= 2N_{25} - 2N_{23} & N_{27} &= e_{13}N_{26} \\
N_{28} &= e_{16}^2 & e_{14} &= N_{27} - N_{28} \\
N_{29} &= N_{25}N_{14} & e_{15} &= 2N_{29} \\
N_{30} &= e_9N_{14} & N_{31} &= N_{30}N_{21} \\
e_{16} &= N_{24} - N_{31}
\end{aligned}
\tag{20}
$$

Some computation yields the following useful formulas

$$
\begin{aligned}
T_1T_2\lambda &= e_6/N_{14} \\
(T_1T_2)^3H &= e_9 \\
(T_1T_2)^2G &= e_{10}
\end{aligned}
\tag{21}
$$

From Proposition 1 and these formulas, we have that $Q_3 = (\lambda(-\lambda^2 + 3G + c_2) - H, 2(\lambda^2 - 2G), 2(\lambda^2 - 2G - c_2)(\lambda^2 - 2G)^2 - (\lambda(-\lambda^2 + 3G + c_2) - H)^2) = ((T_1T_2)^3)(\lambda(-\lambda^2 + 3G + c_2) - H), 2(T_1T_2)^3)(\lambda^2 - 2G), (T_1T_2)^6)[2(\lambda^2 - 2G - c_2)(\lambda^2 - 2G)^2 - (\lambda(-\lambda^2 + 3G + c_2) - H)^2]) = (e_{16}/N_{14}^3, 2N_{25}/N_{14}^2, e_{14}/N_{14}^6) = (e_{16}, 2N_{25}N_{14}, e_{14}) = (e_{16}, e_{15}, e_{14})$.

From this we see that the algorithm sketched above requires 31 multiplications including all necessary multiplications by the $c_i$'s. In contrast, the algorithm given in Brier and Joye ([6]) for elliptic curves in Weierstrass form requires 17 multiplications plus 1 multiplication with a constant from the equation.

## 5 Applications to Side-Channel Attacks

In the previous sections, we showed how to attach to any elliptic curve $E$ and any $k$-rational point $M \neq e$ on $E$ an isomorphic elliptic curve $C_M$ which is given as a weighted quartic projective curve.

The first advantage of this representation is that the addition $P + Q$ of two points may be expressed by formulas independent of whether or not $P$ and $Q$ are different. This uniformity defends against SPA.

Standard techniques of defending against DPA involve either using projective coordinates or changing the representation of the elliptic curve. The method outlined offers both of these features. The addition may be carried out with projective coordinates as indicated above.

Another advantage is that this representation is available for all elliptic curves. Thus, it may be applied to all curves included in present and future standards.

Each elliptic curve admits of a large number of such representations, which can be changed at virtually no cost.

## 6 Examples

A crucial point with this approach is that we may choose *any* point $M \neq e$ on $E$ to obtain a new parametrization. Some applications may not mandate this and it is of some interest to examine certain special examples. We begin by looking at the work of Billet and Joye ([3]) which sparked our interest to begin with.

*Example 1.* (Billett-Joye). An important example of our construction is to be found in the Jacobi model of Billett and Joye ([3]) and its application to side-channel attacks. They begin with an elliptic curve $E$ defined by the affine Weierstrass equation

$$Y^2 = X^3 + aX + b \tag{22}$$

and a $k$-rational point $M = (\theta, 0)$ of order 2. Applying the procedure outlined above, we obtain the curve

$$\begin{aligned} W^2 &= S^4 - (3\theta/2)S^2 - (4a + 3\theta^2)/16 \\ &= S^4 - 2\delta S^2 + \epsilon \end{aligned} \tag{23}$$

where $\delta = 3\theta/4$ and $\epsilon = -(4a + 3\theta^2)/16$. A simple change of variables then gives the equation

$$y^2 = \epsilon x^4 - 2\delta x^2 + 1 \tag{24}$$

used by Billet and Joye.

*Example 2.* A situation which leads to a particularly simple quartic is the use of a point $M = (\alpha, \beta) = (0, \beta)$ where the $X$-coordinate of $M$ is 0. This yields the quartic

$$W^2 = R(S) = S^4 - \beta S - a_4/4 \tag{25}$$

## References


1. Liardet, P.-V., Smart, N.B.: *Preventing SPA/DPA in ECC Systems Using the Jacobi Form.* In: Ç.K. Koç, D. Naccache, and C Paar, editors, Cryptographic Hardware and Embedded Systems – CHES 2001, Volume 2162 of Lecture Notes in Computer Science, pages 391-401. Springer-Verlag, 2001.
2. Joye, M., Quisquater, J.-J.: *Hessian Elliptic Curves and Side-Channel Attacks.* In: Ç.K. Koç, D. Naccache, and C Paar, editors, Cryptographic Hardware and Embedded Systems – CHES 2001, Volume 2162 of Lecture Notes in Computer Science, pages 402-410. Springer-Verlag, 2001.
3. Billet, O., Joye, M.: *The Jacobi Model of an Elliptic Curve and Side-Channel Analysis.* In: Fossorier, M.,Høholdt, T.,Poli, A., editors, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Volume 2643 of Lecture Notes in Computer Science, pages 34-42, Springer-Verlag, 2003.
4. Reid, M. *Graded rings and varieties in weighted projective space.* Manuscript, M. Reid's Web page (www.maths.warwick.ac.uk/˜miles/surf/more/grad.pdf), Jan. 2002.
5. Fricke, R. *Die elliptische Funktionen und ihre Anwendungen*, B.G. Teubner, 1922.
6. Brier, É., Joye, M.: *Weierstraß Elliptic Curves and Side-Channel Attacks.* In: Naccache, D and Paillier, P., editors, Public Key Cryptography 2002, Volume 2274 of Lecture Notes in Computer Science, pages 335-345. Springer-Verlag, 2002.